Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

"Security Is Our First Priority"

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: certin, Cyber Swachhta Kendra, NIC, www.cyberswachhtakendra.gov.in, Cyber Safe Girl | Implemented by: ISEA, C-DAC

www.InfoSecawareness.in

Brochure

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Fake Social Media Profiles

What is it ?

Creating fake profiles is a cyber offence wherein the culprit creates profiles with the name & identity of victim, also he may use social bots (automatic computer programs) to create a fake profile with a false randomly selected picture and details.

The culprit may operate with a fake profile to spread false or fake information to damage the reputation of the victim, and may also send / add friend requests to other friends of victim.

Why should we be concerned ?

A fake social media profile created on anyone's name can damage their public reputation. Also any communication made by the culprit to the friends and family of the actual account holder through this fake account, can make them vulnerable to attacks like phishing, financial scams etc., as they can be tricked into providing their information by the fraudster.

Important Tips :

- Always save the screen shots of the online incidents as proof to support your claim or complaint with relevant evidence. Also make a note of the persons mobile number and other details of the suspect or

culprit.

- Refer to the information given in the site related to various cyber crimes and related evidences to be submitted for the same.

How do we safeguard ourselves ?

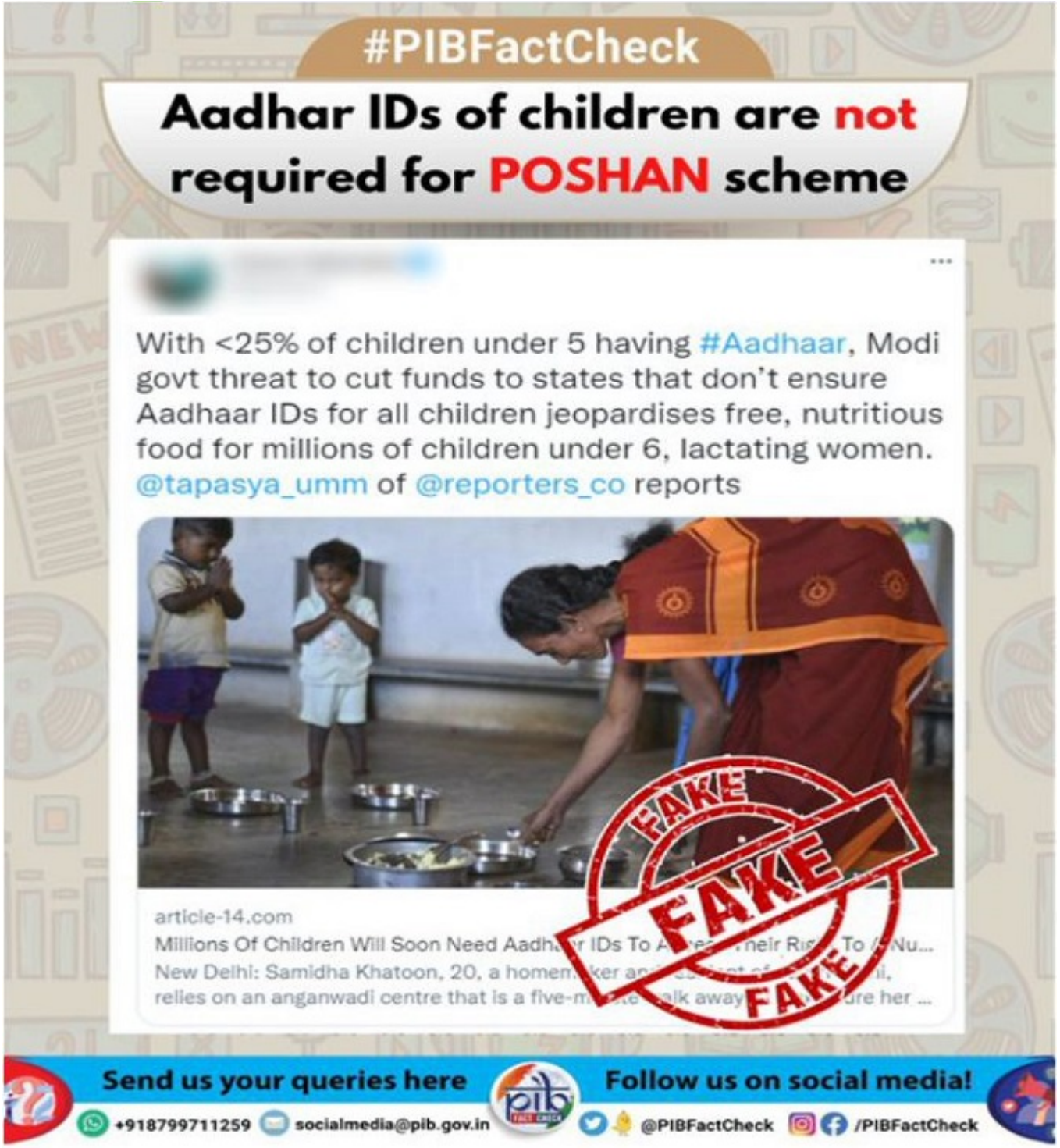
As this type of offence can damage your online reputation and public image, through false information spread by culprit, you should take care of the following aspects to safeguard yourself against this cyber offence.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in


#PIBFactCheck
Aadhar IDs of children are not required for POSHAN scheme
With <25% of children under 5 having #Aadhaar, Modi govt threat to cut funds to states that don't ensure Aadhaar IDs for all children jeopardises free, nutritious food for millions of children under 6, lactating women. @tapasya_umm of @reporters_co reports
article-14.com
FAKE
FAKE
FAKE
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

"Black Basta" Ransomware

Virus Type: Ransomware

It is reported that a new ransomware called "Black Basta", is spreading across the globe. The variants of this ransomware are focused on Windows platform, however, new variants targeting ESXi virtual machines running on Linux servers that facilitates the attackers with encrypting multiple servers with one command are also developed. For attacking ESXi servers, ransomware looks for the /vmfs/volumes; the location where VMs are stored in compromised ESXi servers.

The ransomware steals the sensitive data of the system before starting system encryption. Threat actors maintain the 'Black Basta Blog' or 'Basta News' site on Tor where the data leak information of victims is handled.

Infection Mechanism:

The ransomware requires administrative privileges for its encryption functionalities. Upon execution, the encryptor deletes the shadow volume files using vssadmin.exe so to make Windows recovery difficult. The malware also changes the desktop wallpaper and encrypted file icons as shown:

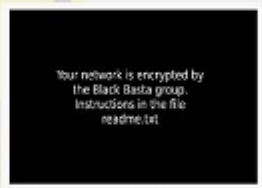


Fig 1 Desktop wallpaper created by encryptor (source: Bleeping Computer)

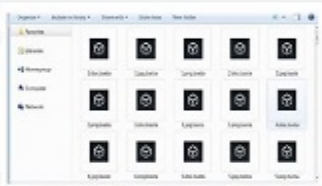
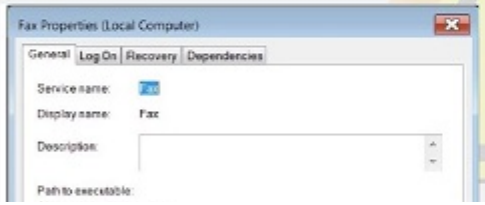
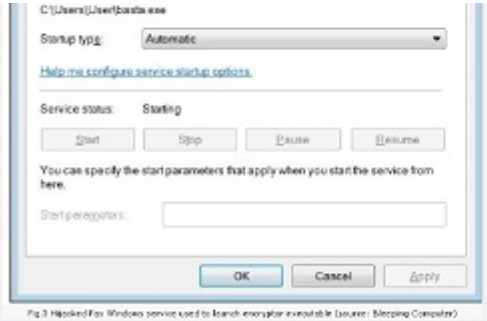


Fig 2 Encrypted Files (source: Bleeping Computer)



The ransomware also has capabilities to hijack existing genuine Windows FAX service and creating a malicious service named 'FAX'. The figure below shows the hijacked/malicious FAX service:

Countermeasures:



- Maintain offline backups of data, and regularly maintain backup and restoration. This practice will ensure the organization will not be severely interrupted, have irretrievable data.
- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted) and covers the entire organization's data infrastructure
- Implement all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to have strong, unique passwords.

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2022-1993

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in), Cyber Safe Girl, I4C | Implemented by: ISEA

www.InfoSec awareness.in

TOOLS

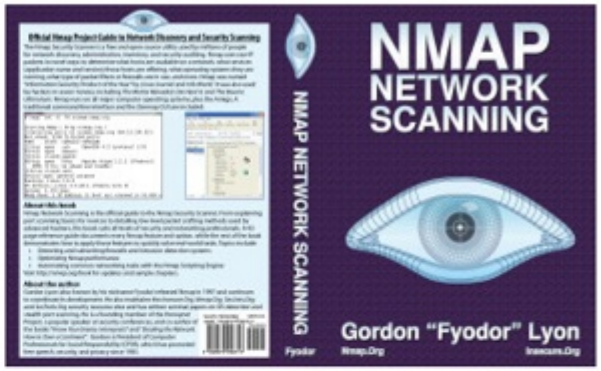
National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Nmap:

Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing. It is a very useful tool for many systems and network administrators for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. It uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.



A representative Nmap scan

```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

Target Specification

Everything on the Nmap command-line that isn't an option (or option argument) is treated as a target host specification. The simplest case is to specify a target IP address or hostname for scanning.

When a hostname is given as a target, it is resolved via the Domain Name System (DNS) to determine the IP address to scan. If the name resolves to more than one IP address, only the first one will be scanned. To make Nmap scan all the resolved addresses instead of only the first one, use the --resolve-all option.

For more details visit : *https://nmap.org/*

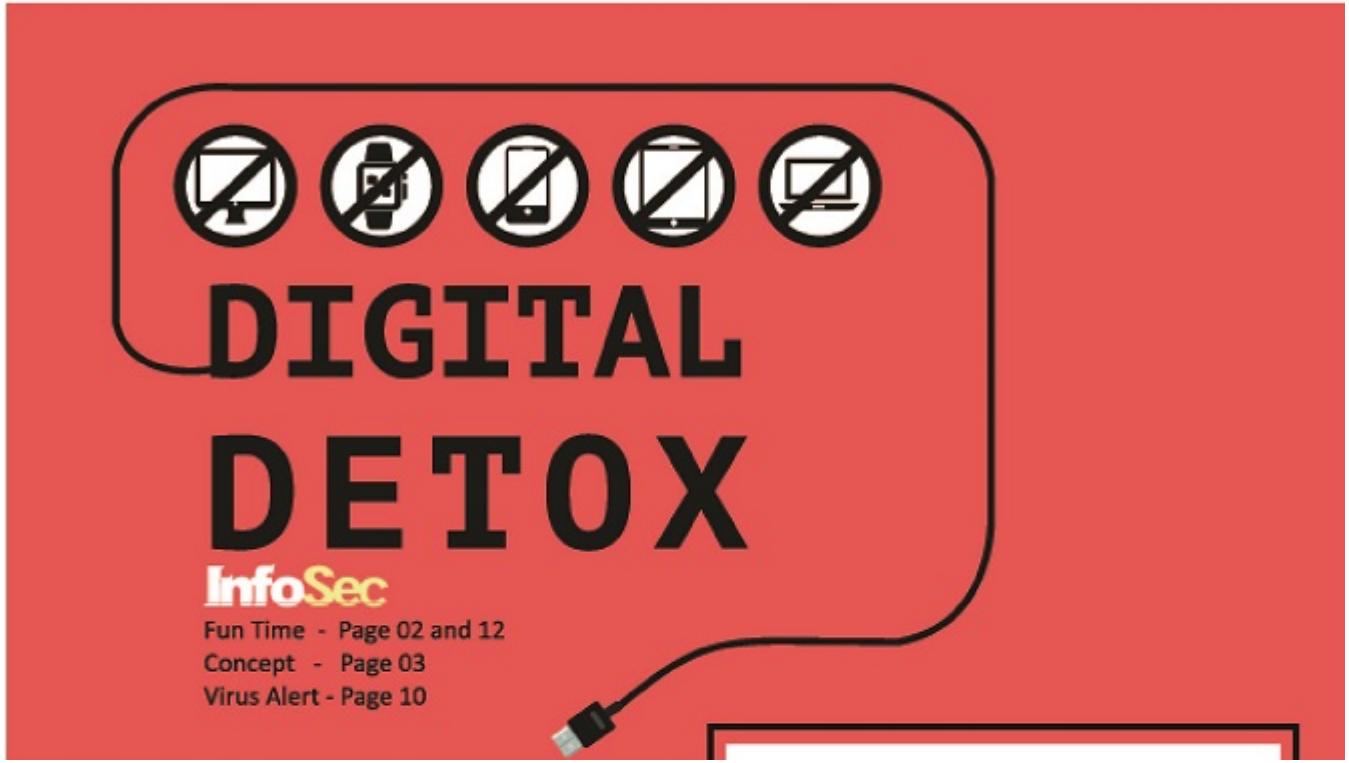
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, साइबर स्वच्छता केन्द्र Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C | Implemented by: C-DAC


A security flaw has been uncovered in the Google Chrome browser version prior to 104.0.5112.101, making it necessary for the Chrome users to update their web browser to latest version immediately.
About the threat
Indian Computer Emergency Response Team (CERT-In) has issued a high-severity alert to the Google Chrome users in view of the multiple vulnerabilities which were observed by them in Google Chrome version prior to 104.0.5112.101 .
The critical security flaws detected in some versions of the web browser can potentially put the users at risk. The flaw can allow fraudsters to execute malicious code by overriding security restrictions on targeted systems.
Advisory
It is advised that users running an older version of Google Chrome update their browser version with relevant patches immediately.
How to download the latest Google Chrome update?
Open the Google Chrome browser
Click on the three dots in the top right hand corner of the browsing window
Choose the option "settings" from the drop down list
Click on the "About Chrome" option that is available in the bottom of the menu on left side
The page mentions if it is updated, otherwise click 'Update Google Chrome'.
(Note: If you can't find this button, you're on the latest version)
Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India
Supported by : Ministry of Home Affairs (MHA), Govt. of India

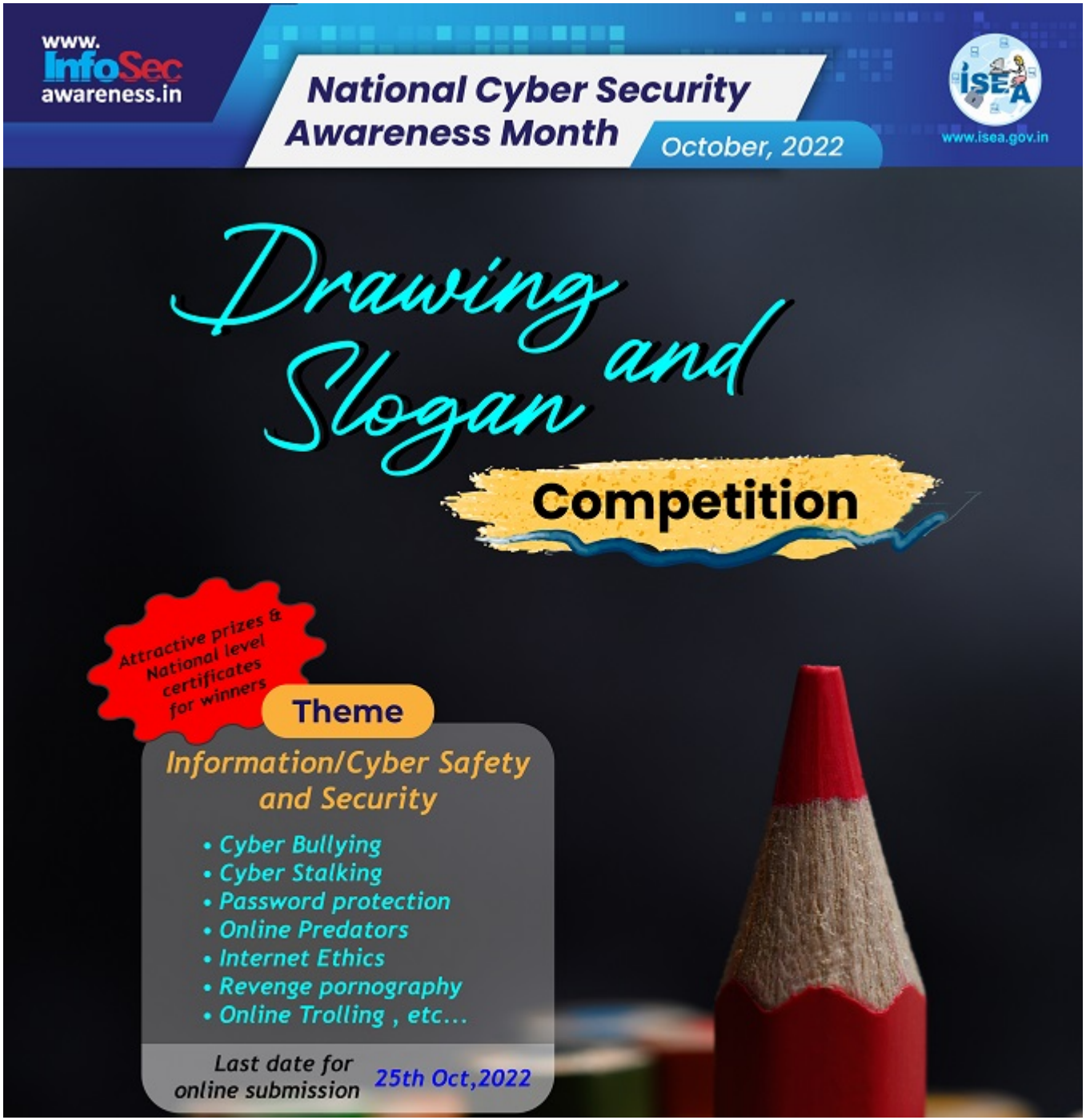
ISEA awareness Newsletters on DIGITAL DETOX




Scan and Download
https://infosecawareness.in/newsletter/edition1-2022
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
certm
NIC National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by
CDAC


www.
InfoSec
awareness.in
National Cyber Security Awareness Month
October, 2022
ISEA
www.isea.gov.in
"See Yourself in Cyber"


Drawing and Slogan Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
Cyber Bullying
Cyber Stalking
Password protection
Online Predators
Internet Ethics
Revenge pornography
Online Trolling , etc...
For more topics, please visit www.infosecawareness.in
www.isea.gov.in
www.infosecawareness.in
infosecawarenesss
infosec_awareness
InfoSecAwa
InformationSecurityAwareness
Join 2-hour course on Cyber Hygiene Practices
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
www.cyberswachhtakendra.gov.in
Implemented by


www.
InfoSec
awareness.in
National Cyber Security
Awareness Month
October, 2022
ISEA
www.isea.gov.in
Drawing and
Slogan
Competition
Attractive prizes &
National level
certificates
for winners
Theme
Information/Cyber Safety
and Security
• Cyber Bullying
• Cyber Stalking
• Password protection
• Online Predators
• Internet Ethics
• Revenge pornography
• Online Trolling , etc...
Last date for
online submission
25th Oct,2022


For more information visit: www.infosecawareness.in/article/national-level-competitions2022
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
MINISTRY OF EDUCATION
Supported by
certin
www.cyberswachhtakendra.gov.in
Implemented by


OCTOBER
2022
National Cyber Security Awareness Month
"See Yourself in Cyber"
SECURITY TIPS FOR SOCIAL MEDIA USAGE
• Block profiles from public searches.
• Log out after each session.
• Never Share social media credentials with any one.
• Never accept friend request from unknown person.


• Avoid mentioning home or work address.
• Never click on suspicious links.
• Keep the privacy settings of social media profile at the most restricted levels, especially for public/ others.
• Apply maximum caution while sharing photographs, status, comments etc. These may together reveal enough about users.
"Security is our first Priority"
certin
Enhancing Cyber Security in India
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre


www.InfoSec awareness.in
National Cyber Security Awareness Month
October, 2022
ISEA
www.isea.gov.in
"See Yourself in Cyber"
Drawing and Slogan
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
Cyber Bullying
Cyber Stalking
Password protection
Online Predators
Internet Ethics
Revenge pornography

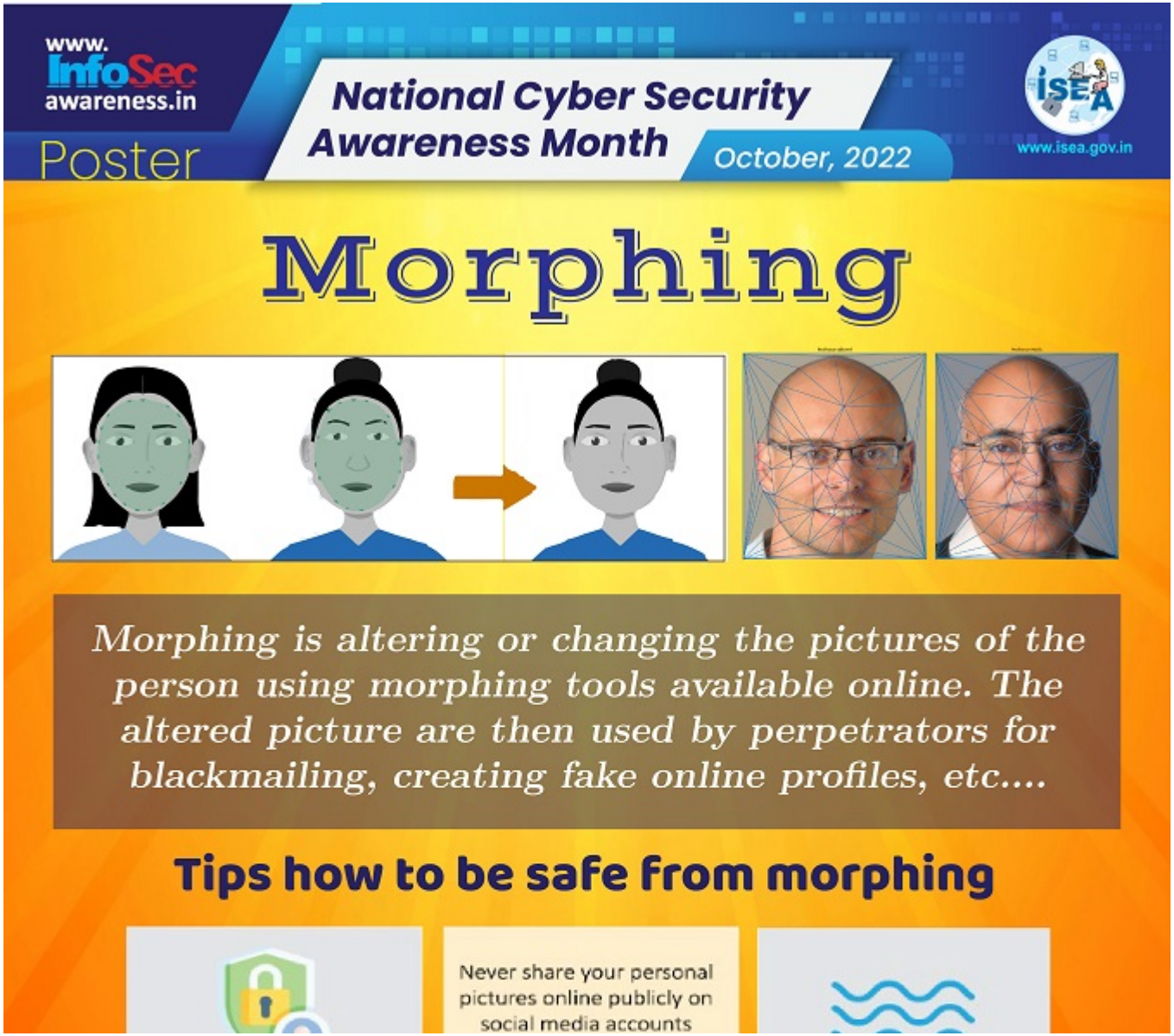

Competition
Online Trolling ,
etc...
For more topics, please visit
www.infosecawareness.in
www.isea.gov.in
www.infosecawareness.in
infosecawarenesss
infosec_awareness
InfoSecAwa
InformationSecurityAwareness
Join 2-hour course on
Cyber Hygiene Practices
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
www.cyberswachhtakendra.gov.in
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

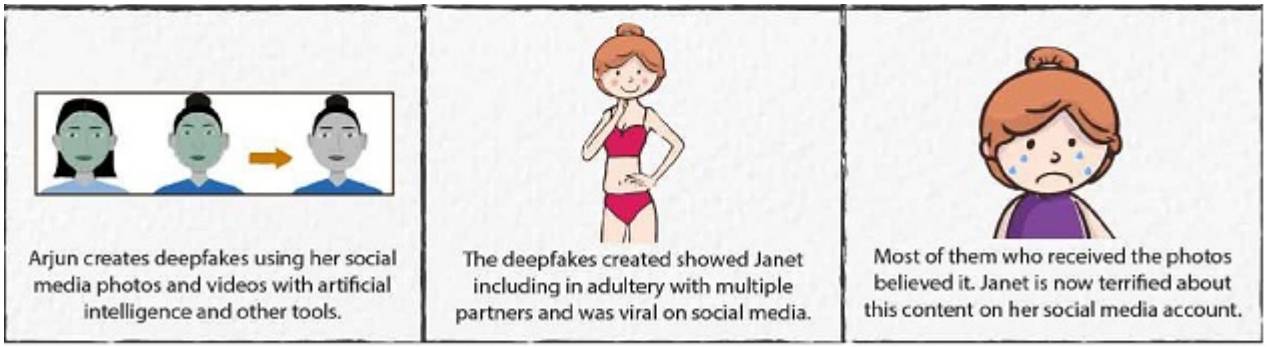
सत्यमेव जयते

"SECURITY is incomplete without U and I"



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Why should we be concerned ?

Morphing can damage your online reputation and cause emotional trauma, you can be prone to threats from perpetrators and may fall prey to their attempts at blackmailing you.

How can we safeguard ourselves against such offence ?

Morphing can cause social stigma and can have damaging effect on you. It is therefore important to understand the measures that can help you stay safe.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in


NOT being done Through WhatsApp
Agnipath Scheme 2022
Online Registeration Via Whatsapp
MYGOV
AGNIPATH SCHEME 2022
ADD WHATSAPP NUMBER
+919608439688
Click to interact with
MyGov Angipath Scher
bit.ly/Mygov-Agnipa -Sc me-202
Last Date For Re
15 Au 20
FAKE
FAKE
FAKE
Helpline Number
Phone:+919608439688
Toll Free Number:0911
#IndiaFight #JoinIndianArmy
#PIBFactCheck
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in

HIVE RANSOMWARE

Virus Type: Ransomware

It has been reported that Hive ransomware isemploying a wide variety of tactics, techniques, and procedures (TTPs) to compromise business networks. Hive RaaS owners build personalized ransomware kit, customized for various operating systems.

Infection Mechanism:

Hive affiliates resort to various initial compromise methods, such as vulnerable RDP servers, compromised VPN credentials, as well as phishing emails with malicious attachments. Hive generally uses applications like Cobalt Strike, ConnectWise, ADrecon during the attack. Hive ransomware attempts to dump credentials, cache clear text credential data and use tools like ADrecon to "map, traverse, and enumerate" the Active Directory (AD) environment. It seeks processes related to backups, anti-virus/anti-spyware, and file copying and terminates them to facilitate file encryption. The encrypted files commonly end with a .hive extension.

Best Practices and Recommendations:

- Maintain offline backups of data, and regularly maintain backup and restoration. This practice will ensure the organization will not be severely interrupted, have irretrievable data.

- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted) and covers the entire organization's data infrastructure.

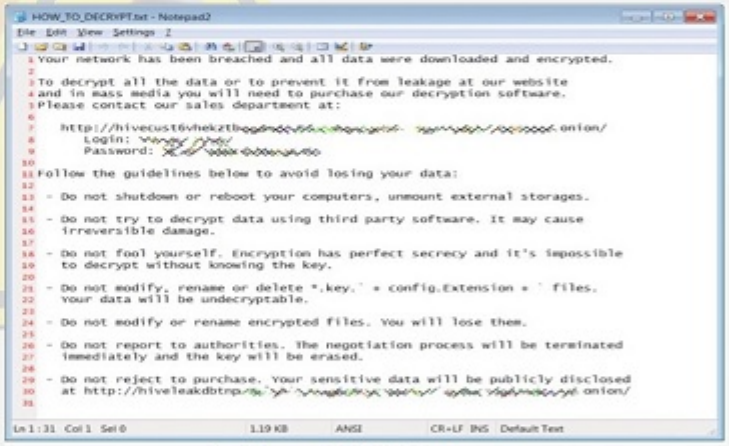


Fig .1 Ransom note by Hive Ransomware

- Implement all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to have strong, unique passwords.

- Implement multi-factor authentication for all services to the extent possible, particularly for web-mail, virtual private networks, and accounts that access critical systems.

- Remove unnecessary access to administrative shares

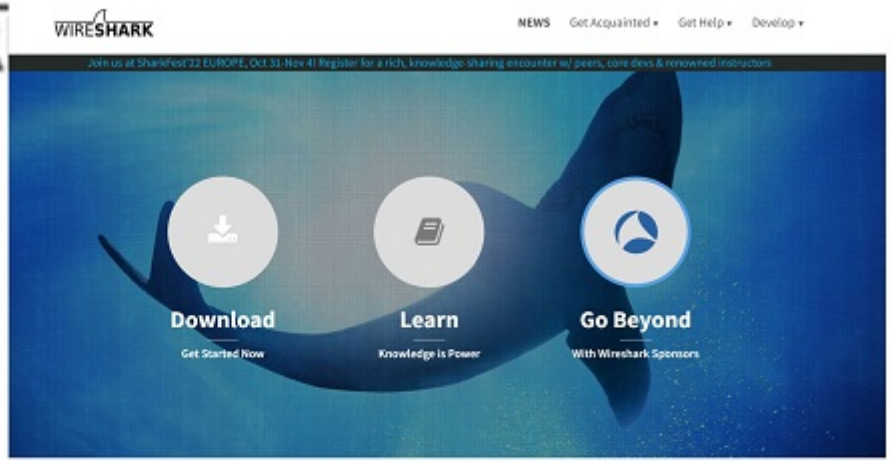
For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2022-1973

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

WIRESHAR

Wireshark is a free and open-source tool for network protocol analysis. This tool enables security professionals to observe the network at a minute level by viewing the traffic, dumping specific packets, checking the packet format and finding network issues this way. It allows for deep inspection of hundreds of protocols. It also supports live capture and offline analysis of



data and offers decryption for multiple protocols such as for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP and WPA/WPA2.

Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text

For more details visit : *https://www.wireshark.org/*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in


Drawing and Slogan
Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
• Cyber Bullying
• Cyber Stalking
• Password protection
• Online Predators
• Internet Ethics
• Revenge pornography
• Online Trolling , etc...
Last date for online submission 25th Oct,2022
For more information visit: www.infosecawareness.in/article/national-level-competitions2022
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
MINISTRY OF EDUCATION
certmc
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by


www.
InfoSec


awareness.in
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
"See Yourself in Cyber"
Drawing and Slogan Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
Cyber Bullying
Cyber Stalking
Password protection
Online Predators
Internet Ethics
Revenge pornography
Online Trolling , etc...
For more topics, please visit www.infosecawareness.in
www.isea.gov.in
www.infosecawareness.in
infosecawarenesss
infosec_awareness
InfoSecAwa
InformationSecurityAwareness
Join 2-hour course on
Cyber Hygiene Practices


Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
certin
NIC
National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by
CDAC

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Think Before You Click"

anonymous persons who comment on your social media posts

Also disable your location on your social media account.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: certin, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA www.cyberswachhtakendra.gov.in, CYBER SAFE GIRL

Implemented by: ISEA, CDAC

www.InfoSecawareness.in

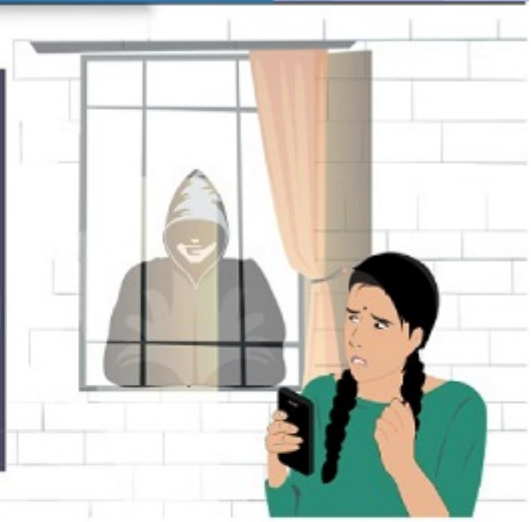
Brochure

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Cyber Stalking



What is it ?

A cyber stalker makes use of internet and electronic means to monitor your online activities and track your whereabouts to harass, intimidate, embarrass, accuse, threaten, commit identity theft or malware attack.

The cyber stalker starts harassing you anonymously using online means like your email, social networks, instant messaging etc.,. They can intrude on your privacy and can track your physical location and cause harm. They can take control of your online accounts and can spread false rumors about you online.

Why should we be concerned ?

Cyber stalking can not only be disturbing and stressful but it can also put you in danger of being attacked by the stalker either online or offline.

Important Tips :

- ✓ *Always save the screen shots of the online messages, comments, conversations or communication as proof to support your claim or complaint with relevant evidence. Also make a note of the persons*

mobile number and other details of the suspect or culprit.

✓ *Refer to the information given on the site cybercrime.gov.in related to various cyber crimes and related evidences to be submitted for the same.*

How can you safeguard yourself against cyber stalking?

Cyber stalking can cause extreme mental distress and can cause post-traumatic stress disorder because of the harassment of the stalker, hence it is important that you know about measures to protect yourself.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: certin, NIC National Informatics Centre, साइबर स्वच्छता केंद्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, CYBER SAFE GIRL

Implemented by

pib FACT CHECK

राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022


FAKE ALERT!
No such aid is being given by Finance Ministry
वित्त मंत्रालय
MINISTRY OF
FINANCE
सत्यमेव जयते
FAKE
FAKE
FAKE
After taking into consideration the financial cr
by the Indian people, the Ministry of Finance decided to give every citizen an amount of (INR 30,628) to reduce the severity of the crisis
Register for support
#PIBFactCheck
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

LockBit 2.0 Ransomware

Virus Type: Ransomware

It has been reported that the LockBit2.0 ransomware, which operates as an affiliate-based Ransomware-as-a-Service (RaaS) ramped up its targeted attacks.

Infection Mechanism:

LockBit 2.0 is spreading through a variety of techniques, including, but not limited to, purchased access, unpatched vulnerabilities, insider access, and zero day exploits.LockBit 2.0 also developed a Linux-based malware that takes advantage of vulnerabilities within VMWare ESXi virtual machines.

Ransom note by LockBit 2.0 ransomware

The following are the tools and components that ensure LockBit's smooth execution:

- delsvc.bat ensures that crucial processes, such as MySQL and QuickBooks, are unavailable. It also stops Microsoft Exchange and disables other related services.
- AV.bat uninstalls the antivirus program ESET.
- LogDelete.bat clears Windows Event Logs.
- Defoff.bat disables Windows Defender features such as real-time monitoring.

The malware comes with a hidden debug window that can be activated during the infection process using the SHIFT + F1 keyboard shortcut.

Best Practices and Recommendations:

- Maintain offline backups of data, and regularly maintain backup and restoration. This practice will ensure the organization will not be severely interrupted, have irretrievable data.
- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted) and covers the entire organization's data infrastructure
- Implement all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to have strong, unique passwords

Screen Capture of Hidden Window

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2022-1953

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in), Cyber Safe Girl, I4C | Implemented by: C-DAC

www.InfoSec awareness.in

TOOLS

National Cyber Security Awareness Month

October, 2022

ISEA www.isea.gov.in

Greenbone OpenVAS

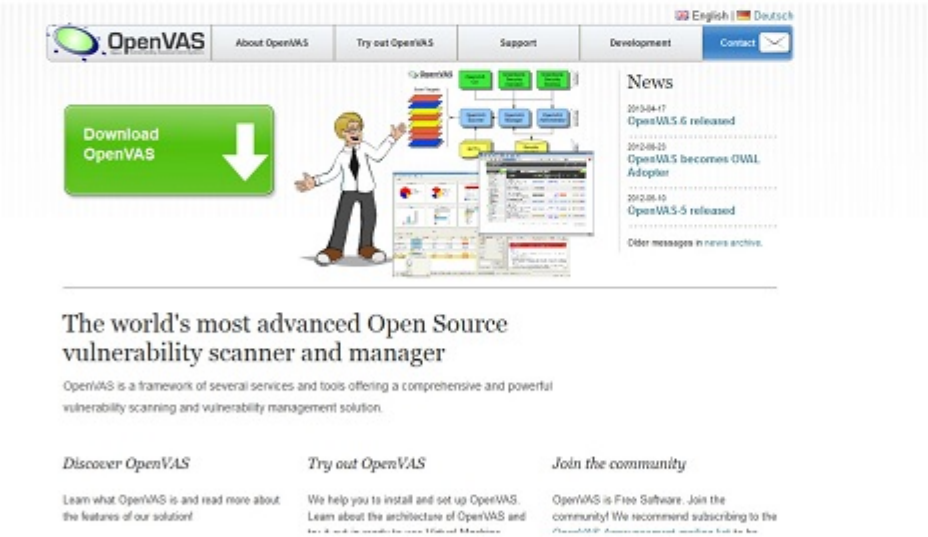
Open Vulnerability Assessment Scanner

Open Vulnerability Assessment Scanner

OpenVAS is an all-in-one vulnerability scanner that comprehensively tests for security holes, misconfigured systems and outdated software. The scanner gets the tests for detecting vulnerabilities from a feed with daily updates. Its capabilities include unauthenticated and authenticated testing, high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.

Installation

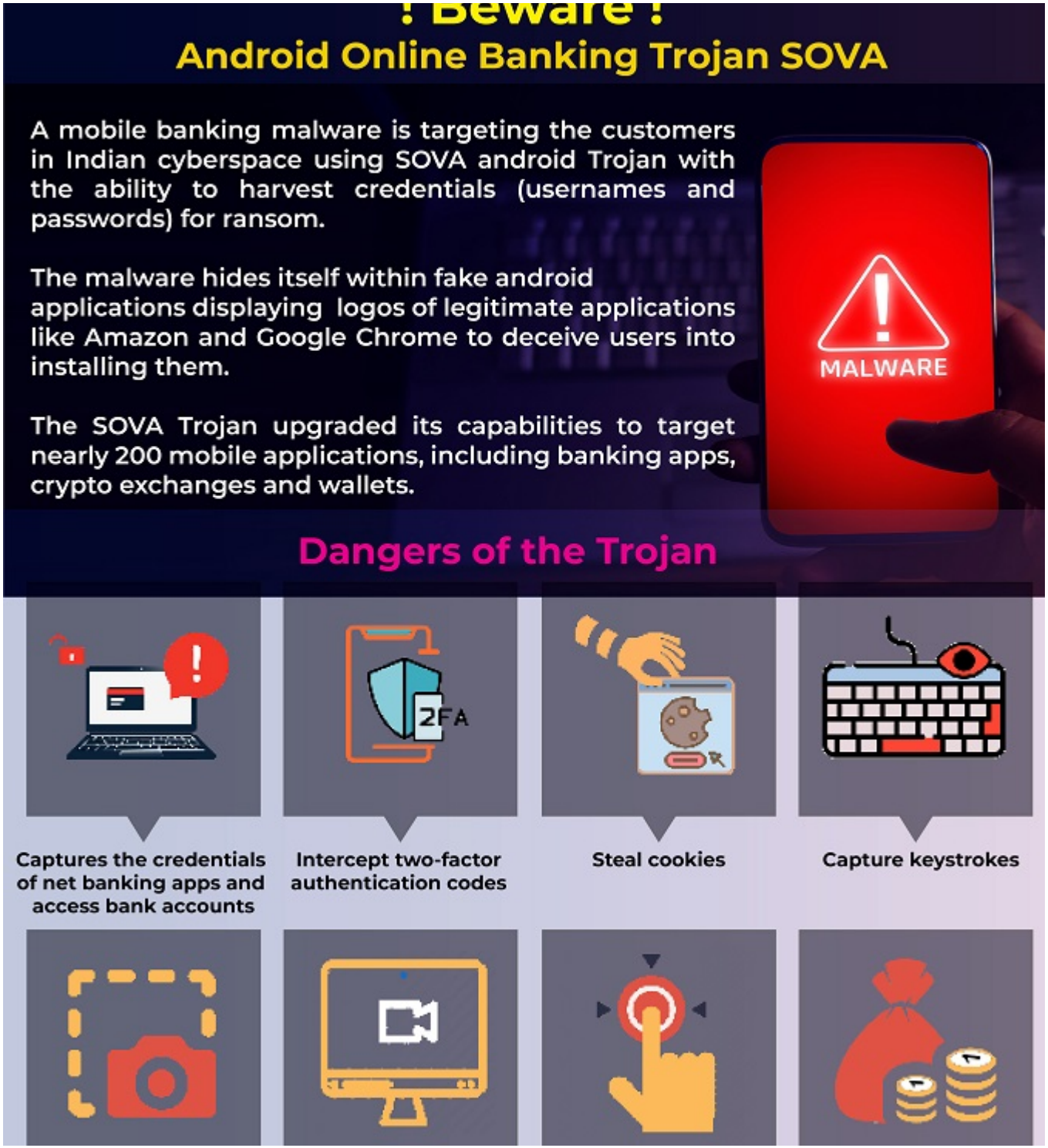
OpenVAS is an all-in-one vulnerability scanner that comprehensively tests for security holes, misconfigured systems and outdated software. The scanner gets the tests for detecting vulnerabilities from a feed with daily updates. Its capabilities include unauthenticated and authenticated testing, high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.



For more details visit : *https://openvas.org/*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in


! Beware !
Android Online Banking Trojan SOVA
A mobile banking malware is targeting the customers in Indian cyberspace using SOVA android Trojan with the ability to harvest credentials (usernames and passwords) for ransom.
The malware hides itself within fake android applications displaying logos of legitimate applications like Amazon and Google Chrome to deceive users into installing them.
The SOVA Trojan upgraded its capabilities to target nearly 200 mobile applications, including banking apps, crypto exchanges and wallets.
MALWARE
Dangers of the Trojan
2FA
Captures the credentials of net banking apps and access bank accounts
Intercept two-factor authentication codes
Steal cookies
Capture keystrokes

Takes screenshots

Records video

Perform gestures like screen click, swipe etc

May lead to large-scale financial frauds

Modus Operandi

Trojan will be installed /distributed via message

Send details of applications installed on the device

Communicate with command and control server

Advisory

Download applications only from trusted sources like legitimate websites or authorized app store

Avoid downloading apps from SMS, APIs, social media messages, or by clicking advertisements

Be cautious about allowing any permissions during the installation of the applications

Properly verify the app details in the developer's website before downloading it

Avoid installing mobile

Pay attention to reviews


Avoid installing mobile applications that have typo graphical/ grammatical mistakes in its descriptions
Pay attention to reviews and comments of the users, before installing any applications
Use a trusted anti-virus software for mobile security to stay safe from android malware


Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by


www.
InfoSec
awareness.in
National Cyber Security Awareness Month
October, 2022
ISEA
www.isea.gov.in
"See Yourself in Cyber"
Drawing and Slogan
Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
Cyber Bullying
Cyber Stalking
Password protection
Online Predators
Internet Ethics
Revenge pornography
Online Trolling ,
etc...
For more topics, please visit
www.infosecawareness.in


www.isea.gov.in
www.infosecawareness.in
infosecawarenesss
infosec_awareness
InfoSecAwa
InformationSecurityAwareness
Join 2-hour course on
Cyber Hygiene Practices
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by
www.cyberswachhtakendra.gov.in


www.
InfoSec
awareness.in
National Cyber Security
Awareness Month
October, 2022
www.isea.gov.in
Drawing


Slogan and
Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
• Cyber Bullying
• Cyber Stalking
• Password protection
• Online Predators
• Internet Ethics
• Revenge pornography
• Online Trolling , etc...
Last date for online submission
25th Oct,2022
For more information visit: www.infosecawareness.in/article/national-level-competitions2022
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
MINISTRY OF EDUCATION
Supported by
certin
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

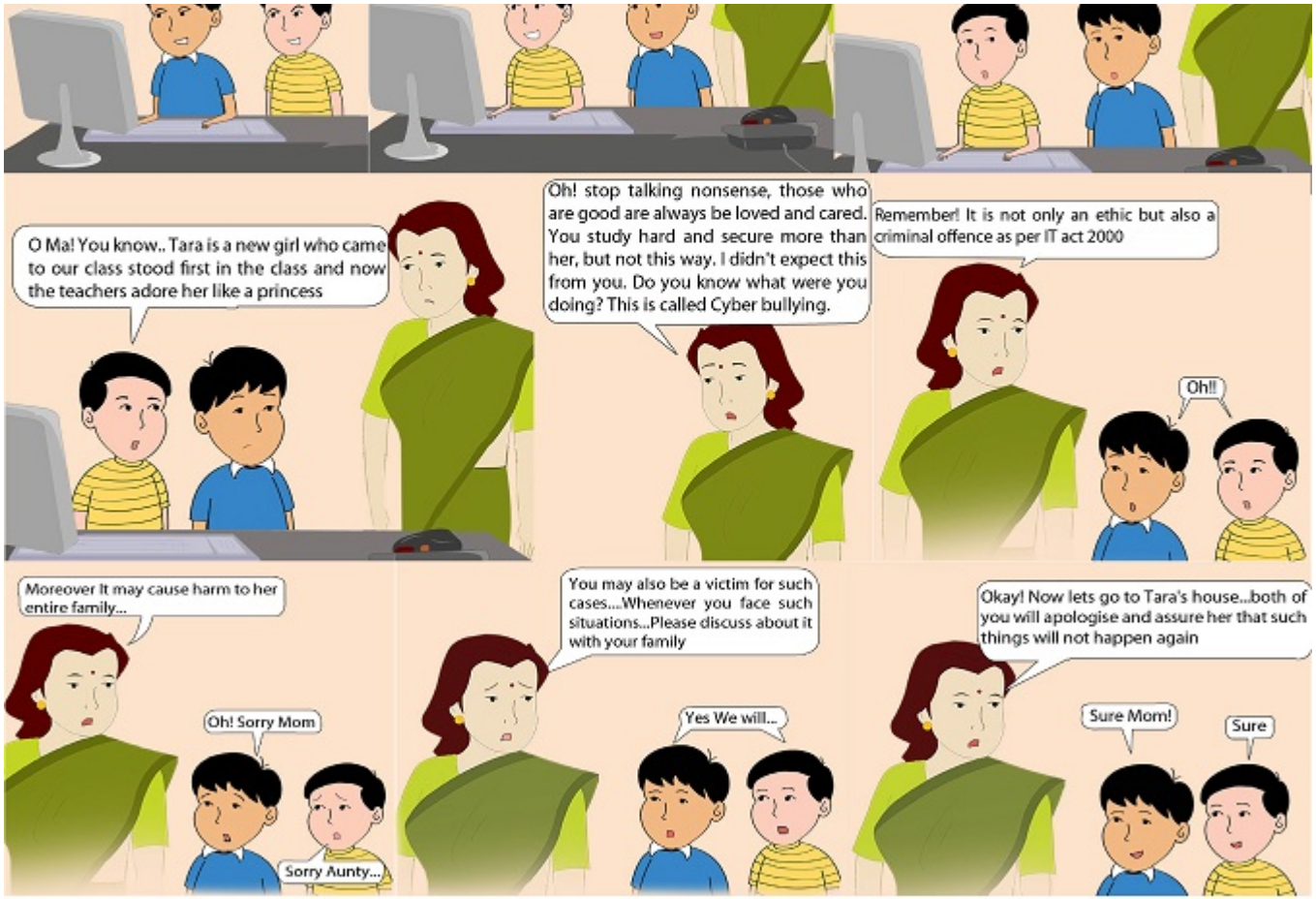
"Stronger the Password, Stronger the security"

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in), Cyber Safe Girl | Implemented by: C-DAC


This Appointment Letter issued in the name of CBIC is FAKE
CENTRAL BOARD OF INDIRECT TAXES AND CUSTOMS
केंद्रीय अप्रत्यक्ष कर और सीमा शुल्क बोर्ड
DEPARTMENT OF REVENUE
राजस्व विभाग
MINISTRY OF FINANCE
वित्त मंत्रालय
GOVERNMENT OF INDIA
भारत सरकार
Website: http://www.mumbaicustomszone1.gov.in/ E-mail: [redacted] Telephone:022-22610027
Dept_HRD/78(5)/NEW/2021-2022/38
Date : 14-07-2022
Office Order No. 609/12/20/6064/377
Sub : Joining of Candidates in Clerk (LDC)
under Customs Department .
Having accepted the terms and condition stipulated vide this office offer of appointment letter of even No. dates 29/06/2022 and having been declared medically fit, the under mentioned candidates for appointment under Customs Office, Ministry of
Central Board of Indirect Taxes & Customs
2016 and posted to mentioned against him.
Sl NO.
Name/Father's Name/Caste/S/St
Date of Birth
01
Mitesh Patel S/O- Narendrabhai
27-07-1999
FAKE
FAKE
FAKE
#PIBFactCheck
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

www.InfoSec awareness.in

Malware Alerts

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

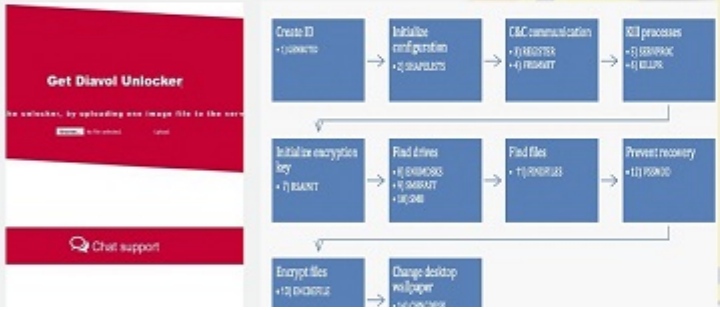
Diavol Ransomware

Virus Type: Ransomware

It has been reported that a newly surfaced malware named "Diavol Ransomware" compiled with Microsoft Visual C/C++ Compiler is encrypting files using user-mode Asynchronous Procedure Calls (APCs) with an asymmetric encryption algorithm. Recently, it has been reported that the Diavol malware has been spreading via email, which includes a link to OneDrive. The OneDrive link, directs the user to download a zipped file which included an ISO file containing a LNK file and a DLL. Once opened (mounted) on the users system, the LNK file masqueraded as a Document entices the user to click/open it. Once the user executes the LNK file, the malware infection will be initiated.

Infection Mechanism:

Once executed, the Diavol malware carries out pre-processing on the victim system including registering the victim device with a remote server, terminating running processes, finding local drives and files in the system to encrypt, and preventing recovery by deleting shadow copies. Then, the files are locked and desktop wallpaper is changed with a ransom message.



Best Practices and Recommendations:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the targets of most attacks.

- Scan all incoming and outgoing emails to detect threats and filter executable

files from reaching end users.

- Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.

- Restrict users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.

- Configure firewalls to block access to known malicious IP addresses.

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2021-1933

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Nikto2

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible, and is obvious in log files or to an IPS/IDS. However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your IDS system).

Not every check is a security problem, though most are. There are some items that are "info only" type checks that look for things that may not have a security flaw, but the webmaster or security engineer may not know are present on the server. These items are usually marked appropriately in the information printed. There are also some checks for unknown items which have been seen scanned for in log files.

Features

- SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's
- Perl/NetSSL)
- Full HTTP proxy support
- Checks for outdated server components
- Save reports in plain text, XML, HTML, NBE or CSV
- Template engine to easily customize reports
- Scan multiple ports on a server, or multiple servers via input file (including nmap output)
- LibWhisker's IDS encoding techniques
- Easily updated via command line
- Identifies installed software via headers, favicons and files
- Host authentication with Basic and NTLM
- Subdomain guessing
- Apache and cgiwrap username enumeration
- Mutation techniques to "fish" for content on web servers
- Scan tuning to include or exclude entire classes of vulnerability
- checks
- Guess credentials for authorization realms (including many default id/pw combos)
- Authorization guessing handles any directory, not just the root
- directory
- Enhanced false positive reduction via multiple methods: headers,
- page content, and content hashing
- Reports "unusual" headers seen
- Interactive status, pause and changes to verbosity settings
- Save full request/response for positive tests
- Replay saved positive requests
- Maximum execution time per target
- Auto-pause at a specified time
- Checks for common "parking" sites
- Thorough documentation

For more details visit : *https://cirt.net/Nikto2*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in


"See Yourself in Cyber"
Drawing and Slogan Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
Cyber Bullying
Cyber Stalking
Password protection
Online Predators
Internet Ethics
Revenge pornography
Online Trolling ,
etc...
For more topics, please visit www.infosecawareness.in
www.isea.gov.in
www.infosecawareness.in
infosecawarenesss
infosec_awareness
InfoSecAwa
InformationSecurityAwareness
Join 2-hour course on
Cyber Hygiene Practices
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in


Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
certin
NIC
National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by
CDAC


www.
InfoSec
awareness.in
National Cyber Security
Awareness Month
October, 2022
ISEA
www.isea.gov.in
Drawing and Slogan
Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
• Cyber Bullying
• Cyber Stalking
• Password protection
• Online Predators
• Internet Ethics
• Revenge pornography
• Online Trolling , etc...

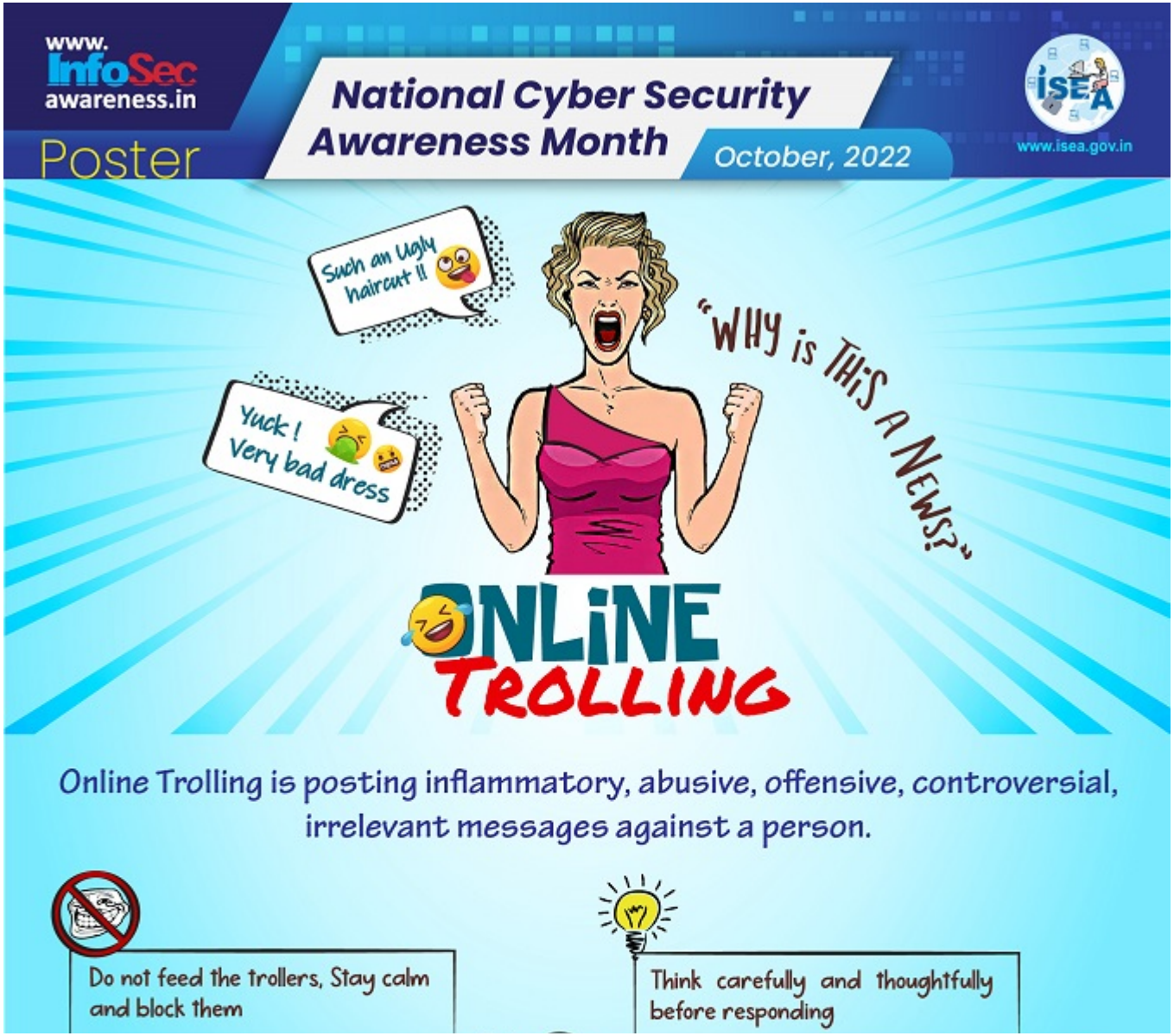

Last date for online submission
25th Oct,2022
For more information visit: www.infosecawareness.in/article/national-level-competitions2022
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
MINISTRY OF EDUCATION
Supported by
certin
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

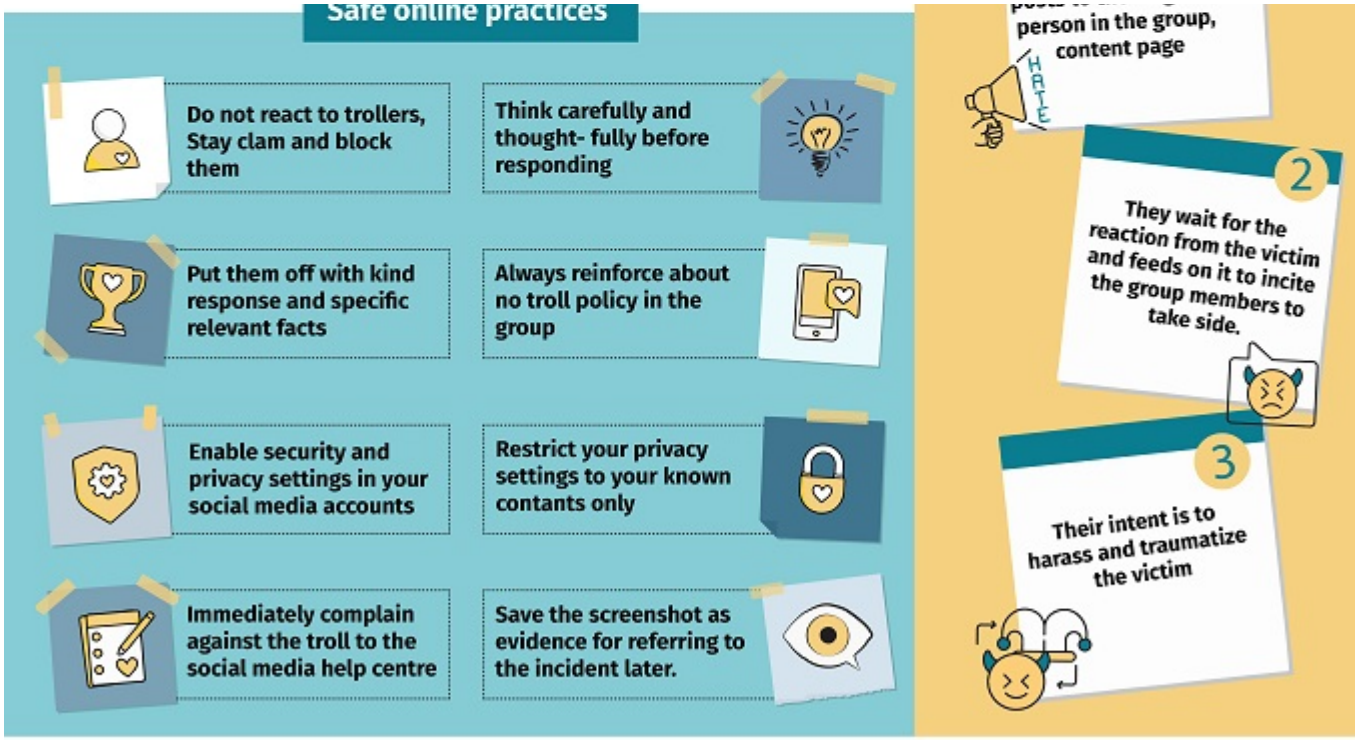
सत्यमेव जयते

"Be Updated and Stay Protected"




Put them off with humor or very kind response with specific relevant facts
Take screenshot as an evidence and immediately file complaint against the troller
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by


www.InfoSec awareness.in
Brochure
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
ONLINE TROLLING
Danielle says:
Did anyone else see what Jess was wearing to @jeremy's party last night? #whatajoke
Like · Comment · Share
Dangers
Stress
Depression
Self-harm
Suicidal thoughts
Points to identify the troll
Spelling & grammar mistakes
Exaggeration
Acting entitled
Making it personal
Online trolling is posting inflammatory, abusive, offensive, controversial, irrelevant messages against a person.
Trolling can start off a heated battle of words among the members in the group against each other while the person who started it enjoys the frustrated responses.
Modus Operandi
1
The troll sends provocative messages/ posts to the targeted



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: certin, CSK, NIC National Informatics Centre, साइबर स्वच्छता केंद्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, CYBER SAFE GIRL, I4C

Implemented by: CDAC

PIB FACT CHECK

राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022


#PIBFactCheck
The Ministry of Finance has not issued this Memorandum!
No. 1/2/2022-E-II (B)
Government of India
Ministry of Finance
Department of Expenditure
North Block, New Delhi Dated the 23 August 2022.
OFFICE MEMORANDUM
Subject: Grant of Dearness Allowance to Central Government employees - Revised Rates effective from 01.07.2022.
The undersigned is directed to refer to this Ministry's Office Memorandum No. 1/4/2021-E-II (B) dated 25th October, 2021 on the subject mentioned above and to say that the President is pleased to decide that the Dearness Allowance payable to Central Government employees shall be enhanced from the existing rate of 34% to 38%of the Basic Pay with effect from 1st July, 2022.
2. The term 'Basic Pay' in the revised pay structure means the pay drawn in the prescribed Level in the Pay Matrix as per 7th CPC recommendations accepted by the Government, but does not include any other type of pay like special pay, etc.
3. The Dearness Allowance will continue to be a distinct
and will not be treated as pay within the ambit of FR 9(21).
4. The payment on account of Dearness Allowance
above m
be rounded to the next higher rupee and the fraction
50 paise m
ored.
5. The payment of arrears of Dearness Allowance
the d
disbursement of salary of September 2022.
6. These orders shall also apply to the civi
Ser
es
Estimates and the expenditure will be char
to the
he Def
e Ser
es
Estimates. In respect of Armed Forces perso
l and Railwa
es, separat
ers
be
issued by the Ministry of Defence and Ministry
ailways,
ly.
7. In so far as the persons serving in the India
Accounts D
ncerned,
these orders are issued in consultation with the Comptro
Aud
of India, as
mandated under Article 148(5) of the Constitution of India.
(Nirmala Dev)
Director
To,
All Ministries/Departments of the Government of India (as per standard distribution list)
Copy to: C&AG, UPSC, etc, as per standard endorsement list.
FAKE
FAKE
FAKE
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

BotenaGo Malware

Virus Type: Backdoor/Malware Botnet

It has been reported that a newly surfaced malware written in Google's open-source programming language Golang, is targeting Linux-embedded routers and Internet of Things (IoT) devices through botnets. The malware is utilizing 33 different exploits to compromise routers and IoT devices. It works by creating a backdoor to the device and then waits to either receive a target to attack from a remote operator through port 19412 or from another related module running on the same machine.

Infection Mechanism:

The new Golang-based malware botnet incorporates more than 30 exploits for a variety of routers,modems, and Network-attached Storage (NAS) devices. As listed by Alien Labs, the vulnerabilities with CVE numbers, which can be exploited by new BotenaGo malware are listed below. In addition, some of the vulnerabilities have also been disclosed without CVE.

The malware botnet deploys a backdoor on the compromised device, and then waits for commands - either from a remote operator or a malicious module on the device - to initiate an attack.As part of a typical BotenaGo attack, the malware first maps potential targets to attack functions, then queries the target with a GET request, after which it searches the returned data, and only then it attempts to exploit the vulnerable target.

VULNERABILITY	AFFECTED DEVICES
CVE-2020-8515	DrayTek Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, and Vigor3008 1.3.3_Beta, 1.4.2.1_Beta, and 1.4.4_Beta devices
CVE-2015-2051	D-Link DIR-645 Wired/Wireless Router Rev. Ax with firmware 1.04b12 and earlier
CVE-2016-1555	Netgear WN604 before 3.3.3 and WNB02Tv2, WNAP210v2, WNAP320, WNDAP350, WNDAP360, and WNDAP660 before 3.5.5.0
CVE-2017-6077	NETGEAR DGN2200 devices with firmware through 10.0.0.50
CVE-2016-6277	NETGEAR R6250 before 1.0.4.6_Beta, R6400 before 1.0.1.18_Beta, R6700 before 1.0.1.14_Beta, R6900, R7000 before 1.0.7.6_Beta, R7100LG before 1.0.0.28_Beta, R7300DST before 1.0.0.46_Beta, R7900 before 1.0.1.8_Beta, R8000 before 1.0.3.26_Beta, D6220, D6400, D7000
CVE-2013-10561	GPON home routers

Best Practices and Recommendations:

- It is recommended to keep the software up to date with latest security up-

dates.

- Install the latest firmware and use a properly configured firewall.
- Ensure minimal exposure to the Internet on Linux servers and IoT devices.
- Monitor network traffic, outbound port scans, and unreasonable bandwidth usage.
- It is advised to carry out timely patching of internet-connected devices to avoid becoming a victim of BotenaGo or any other IoT botnets.

CVE-2013-10562	
CVE-2013-3307	Linksys X3000 1.0.03 build 001
CVE-2020-9377	D-Link DIR-610
CVE-2016-11021	D-Link DCS-930L devices before 2.12
CVE-2016-10088	XiongMai uc-httpd 1.0.0
CVE-2020-10173	Comtrend VR-3033 DE11-416SSG-C01_R02.A2pvl042j1.d26m
CVE-2013-5223	D-Link DSL-2760U Gateway
CVE-2020-8958	Guangzhou IOE CNU V2801RW 1.9.1-181203 through 2.9.0-181024 and V2804R0W 1.9.1-181203 through 2.9.0-181024
CVE-2019-19824	TOTOLINK Realtek SDK based routers, this affects A3002RU through 2.0.0, A702R through 2.1.3, N301RT through 2.1.6, N302R through 3.4.0, N300RT through 3.4.0, N200RE through 4.0.0, N150RT through 3.4.0, and N100RE through 3.4.0.
CVE-2020-10987	Tenda AC15 AC1900 version 15.03.05.19
CVE-2020-9054	Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.2, Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 device. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2
CVE-2017-18368	ZyXEL P660HN-T1A v1 TCLinux Fw §7.3.15.0 v001 / 3.40(ULM.0)b31 router distributed by TrueOnline
CVE-2014-2321	ZTE F460 and F660 cable modems
CVE-2017-6334	NETGEAR DGN2200 devices with firmware through 10.0.0.50

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2021-1914

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: certin, CERT-In, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C | Implemented by: C-DAC

OSSEC

OSSEC is a free program for cybersecurity professionals that's been touted as one of the most popular systems for intrusion detection and prevention. Made up of multiple components including a server, agent and router monitor. OSSEC is capable of rootkit detection, system integrity checking, threat alerts and response. One of OSSEC's highlights is its comprehensive log analysis tool, empowering users to compare and contrast log events from many different sources.

OSSEC is a scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS)

OSSEC Features

Log based Intrusion Detection (LIDs)
Actively monitors and analyzes data from multiple log data points in real-time

Rootkit and Malware Detection
Process and file level analysis to detect malicious applications and rootkits

Active Response
Respond to attacks and changes on the system in real time through multiple mechanisms including firewall policies, integration with 3rd parties such as CDN's and support portals, as well as self-healing actions

Compliance Auditing
Application and system level auditing for compliance with many common standards such as PCI-DSS, and CIS benchmarks

File Integrity Monitoring (FIM)
For both files and windows registry settings in real time not only detects changes to the system, it also maintains a forensic copy of the data as it changes over time.

System Inventory
Collects system information, such as installed software, hardware, utilization, network services, listeners and other information.

Used By Almost Everyone

OSSEC is a growing project, with more 500,000 downloads a year. It is used by everyone from large enterprises to small businesses to governments agencies as their primary server intrusion detection system — both on premise and in the cloud. In addition to being deployed for server protection, OSSEC , is commonly used strictly as a log analysis tool, monitoring and analyzing firewalls, IDSs, web servers and authentication logs.

For more details visit : *https://www.ossec.net/*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

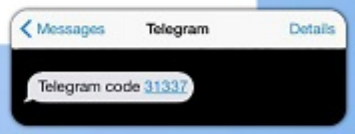
For more information visit: www.isea.gov.in and www.infosecawareness.in

Instant Messaging (IM) Apps have become popular medium of communication among individuals. Fraudsters have targeted the app users and have managed to device ways and means to take over or hijack their IM accounts to commit cyber offences by impersonating them. Users need to be aware and alert about these frauds with necessary safety measures against the same.

How does Telegram Hijacking happen?

The user receives a message from Telegram application containing a 5-digit login code to open a Telegram account.

The user receives a message from a fraudster, requesting a screenshot of their Telegram chat with a 5-digit login code.

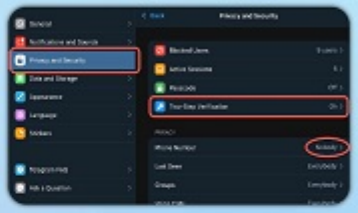


The login code will be visible to the fraudster, to hijack the user account.

Using the hijacked Telegram account, the fraudster will contact people in the user's contact list and use various methods to request for money to be transferred

Precautions

- Never share verification codes with anyone, even if you know them.
- Beware of unusual requests received over Telegram or other messaging apps.
- Turn off notification preview for SMS. Anyone who can see the verification code on your phone can easily hijack your account.
- Enable "Two-Step Verification' for your Telegram account. ***Go to Settings > Privacy and Security > Enable Two-Step Verification***



- Log out of Telegram web/ desktop when you finish using it.
- If your Telegram account has been hijacked Inform your family and friends that your account has been hacked, and they should not respond to any Telegram messages that appear to be from you.
- Warn others not to share their verification codes or any other confidential information.
- Report to Telegram regarding your stolen account. ***https://telegram.org/support***
- Complain at ***www.cybercrime.gov.in***

How to secure your Telegram account

- Use Two-Step Verification
- Make your phone number private


• Once enabled, you will need both an SMS code and a password to log in.
• If any third party doesn't know which phone number you are using on your account, it will be more difficult to breach your account privacy.
• Secret Chats: Telegram secret chat uses end-to-end encryption so no one can see your conversation even if they have access to your account.


Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by
www.cyberswachhtakendra.gov.in
www. InfoSec awareness.in
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
"See Yourself in Cyber"
Drawing and Slogan Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
Cyber Bullying
Cyber Stalking
Password protection
Online Predators
Internet Ethics
Revenge pornography
Online Trolling ,
etc...
For more topics, please visit www.infosecawareness.in


www.isea.gov.in
www.infosecawareness.in
infosecawarenesss
infosec_awareness
InfoSecAwa
InformationSecurityAwareness
Join 2-hour course on
Cyber Hygiene Practices
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by
www.cyberswachhtakendra.gov.in
www.
InfoSec
awareness.in
National Cyber Security
Awareness Month
October, 2022
www.isea.gov.in
Drawing


Slogan and
Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
• Cyber Bullying
• Cyber Stalking
• Password protection
• Online Predators
• Internet Ethics
• Revenge pornography
• Online Trolling , etc...
Last date for online submission
25th Oct,2022
For more information visit: www.infosecawareness.in/article/national-level-competitions2022
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
MINISTRY OF EDUCATION
Supported by
certm
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Protection is better than mitigation"

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in


SCAM
ALERT
#PIBFactCheck
यह योजना फर्जी है
Forwarded
प्रधानमंत्री बेरोजगारी भत्ता योजना 2022
1800 रुपये प्राप्त करें
rebrand.ly
सरकार का नया फैसला
अब बेरोजगार युवाओं को 6000 रुपये हर महीने जीवन यापन के लिए दिए जायेंगे।
प्रधानमंत्री बेरोजगार भत्ता योजना के लिए रजिस्ट्रेशन शुरू हो गए हैं, इस योजना के अंतर्गत बेरोजगार युवाओं को
हर महीने दिए जायेंगे।
फेक
https://rebrand.ly/
bhatta-yojna
संदिग्ध जानकारी यहाँ साझा करें
+918799711259
socialmedia@pib.gov.in
सोशल मीडिया पर हमें फॉलो करें
@PIBFactCheck
/PIBFactCheck

REvil Aka Sodinikibi Ransomware

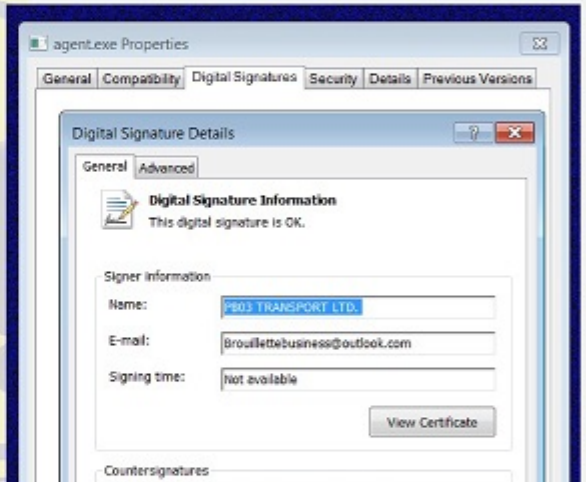
Virus Type: Ransomware

It has been reported that the ransomware strain attributed to REvil is again highly active/ spreading. The attack vector includes Ransomware-as-a-service (RaaS) operation, operating since April 2019. In the recent supply-chain ransomware attack against Kaseya VSA and the multiple managed service providers (MSPs), VSA software (a software platform designed to help manage IT services remotely) used to deliver payload (REvil ransomware) via a Kaseya update and using the platform's administrative privileges to infect systems. Once MSPs are infected, their systems may be used to attack clients that they provide remote IT services for (network management, system updates, backups and others). As per reports, the notorious REvil ransomware already linked to attacks on Acer and meat supplier JBS earlier this year.

Countermeasures:

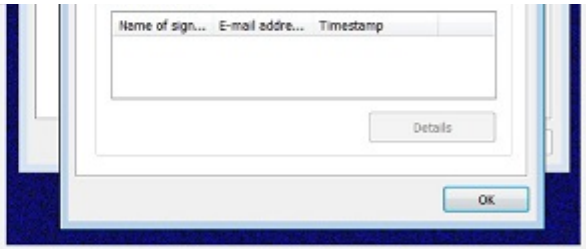
- KASEYA VSA advised their customers/users to IMMEDIATELY shutdown and SHOULD CONTINUE TO REMAIN DOWN UNTIL FURTHER INSTRUCTIONS FROM KASEYA ABOUT WHEN IT IS SAFE TO RESTORE OPERATIONS. KASEYA VSA UPDATED notice will be issued HERE

- Users are advised to disable their RDP if not in use, if required it should be placed behind the firewall and users are to bind with proper policies while using the RDP.



- Restrict execution of Power shell /WSCRIPT in enterprise environment Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled. Script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

Reference:https://www.fireeye.com/blog/-threat-research/2016/02/greater_visibilityt.html



The agent.exe is signed using a certificate from "PB03 TRANSPORT LTD" and includes an embedded 'MsMpEng.exe' and 'mpsvc.dll,' with the DLL being the REvil encryptor.

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2021-1894

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

www.InfoSec awareness.in

TOOLS

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Snort

Snort is an open-source network intrusion prevention and intrusion detection system capable of real-time traffic analysis and logging. It uses a series of rules to identify malicious network activity, find the packets and generate alerts. This packet sniffer is managed by Cisco. It actively searches and analyses networks to detect probes, attacks and intrusions. Snort accomplishes this by fusing a sniffer, packet logger and intrusion detection engine into a single package.


More Adaptable
Snort 3 is redesigned in C++ which makes the code base more modular and easier to maintain on your network.
More Efficient
Threading and shared memory allow you to scale Snort 3 to your network and create a much faster start-up. This allows multiple packet processing to free up more memory for more packet processing power.
More Customizable
Plugins with Luajit allows users to write their own plugins much easier than before to do things like add your own Snort Rule options, in-depth file processing, and more.
Better Performance
Snort Rule Syntax has been updated to make it easier to write and to understand, especially for new users. The rule syntax is more concise with fewer rule parts which will allow rules to run quicker.
For more details visit : https://www.snort.org/
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by
www.InfoSec awareness.in
National Cyber Security Awareness Month
October, 2022
ISEA
www.isea.gov.in


"See Yourself in Cyber"
Drawing and Slogan Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
Cyber Bullying
Cyber Stalking
Password protection
Online Predators
Internet Ethics
Revenge pornography
Online Trolling ,
etc...
For more topics, please visit www.infosecawareness.in
www.isea.gov.in
www.infosecawareness.in
infosecawarenesss
infosec_awareness
InfoSecAwa
InformationSecurityAwareness
Join 2-hour course on
Cyber Hygiene Practices
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in


Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
certin
NIC
National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by


www.
InfoSec
awareness.in
National Cyber Security
Awareness Month
October, 2022
ISEA
www.isea.gov.in
Drawing and
Slogan
Competition
Attractive prizes &
National level
certificates
for winners
Theme
Information/Cyber Safety
and Security
• Cyber Bullying
• Cyber Stalking
• Password protection
• Online Predators
• Internet Ethics
• Revenge pornography
• Online Trolling , etc...


Last date for online submission
25th Oct,2022
For more information visit: www.infosecawareness.in/article/national-level-competitions2022
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
MINISTRY OF EDUCATION
Supported by
certin
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"If you don't know the sender, it might be a pretender."

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in


purpose is to use this information to commit identity theft and other types of fraud.
theft can happen through the photocopies of ID proof documents handed over to strangers for various purposes.
purchase their product or divulge your personal information.
Child Identity theft
Personal Information of a child is used by criminals to apply for government benefits, open bank and credit card accounts and apply for loan.
Skimming
Special electronic devices are inserted in ATM and credit and debit card processing machines to obtain credit and debit card details.
Dumpster Diving
It is a way of getting hold of invoices, financial records or other documents containing personal information from the dustbin.
Pretexting
Fraudsters use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.
Tax Identity Theft
PAN card number which is personal information of an individual is stolen for the purpose of filing fraudulent tax return in the victim's name and also in 'unauthorized' transactions, purchase of luxury cars, etc.
Medical Identity Theft
Personal Information like Name or Medicare Number stolen to submit fraudulent claims to Medicare and other health insurers without your authorization.
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in


www.InfoSec awareness.in
Storyboard
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
Hide personal information
One day, Meena turns on the computer and starts creating her User ID for Facebook
Her brother Nikhil enters the room and said....

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology

Supported by: CERT-In, NIC, साइबर स्वच्छता केन्द्र Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, Cyber Safe Girl

Implemented by

PIB FACT CHECK

राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022


This Warning was NOT issued by IMD Chennai
Time News
Home News World Business Entertainment Health Sport
time.news
The earth is moving away from the sun.. It will be very cold from today.. There is a chance of fever Chennai Meteorological department warns about heavy cold wave
Delhi: The Meteorological Department has announced that as the Earth moves further away from the Sun, it will get colder from today.
All the planets including earth revolve around the sun. The Earth moves to its furthest point from the Sun once a year. This is called abelian.
FAKE
FAKE
FAKE
#PIBFactCheck
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

"Crackonosh" Malware

Virus Type: Cryptocurrency Miner

It is reported that a new strain of cryptocurrency miner dubbed as Crackonosh is spreading through abusing windows Safe mode in its attack and escape detection. The malware is distributed through illegal and cracked copies of popular software. Crackonosh has been circulating since at least June 2018.

Infection Mechanism:

The infection chain starts with an installer and a script that is deployed along with pirated/cracked software and modifies Windows registry to allow critical malware executable to run in Safe mode. The infected system boot in Safe mode in next start up. The malware encase itself in password protected archive and unpack during installation process. While system is in Safe mode, AV software doesn¿t work and this can enable the malicious Serviceinstaller.exe to disable/delete Windows defender. It also uses WQL to query all antivirus software installed. Command listed below:

SELECT * FROM AntiVirusProduct

The malware also able to disable the anti-virus software from other popular companies including Avast, Kaspersky, Norton, McAfee's scanner and Bitdefender etc. with the following command:

"rd < AV directory > /s /q" (here < AV directory > is the default directory name that a specific antivirus software uses.)

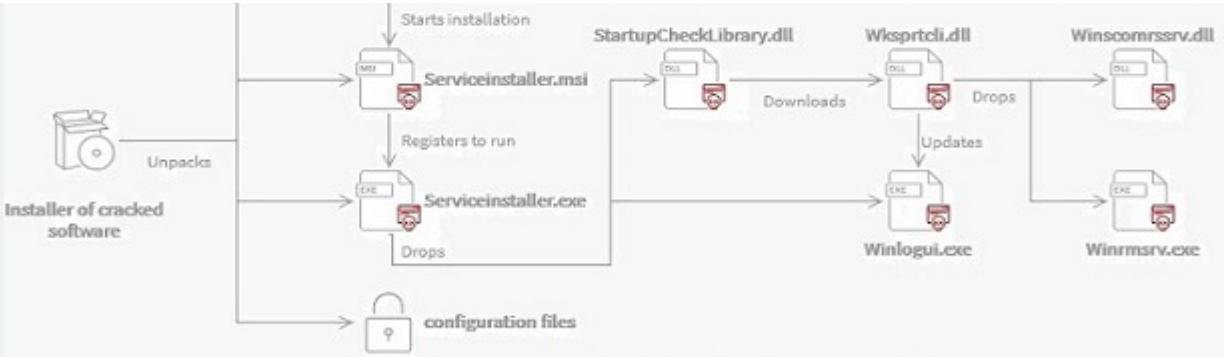


Fig.1 "Crackonosh" installation process. (source:avast)

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2021-1895

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in), Cyber Safe Girl, I4C | Implemented by: ISEA, CDAC

www.InfoSec awareness.in

TOOLS

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

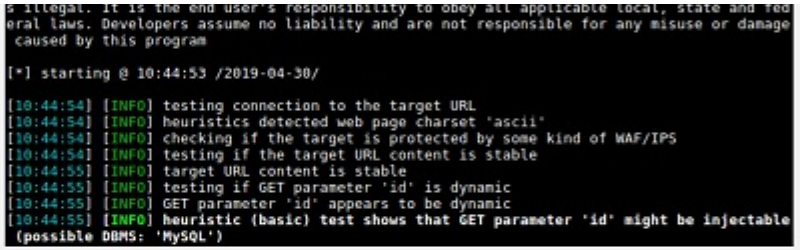
Sqlmap

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Features

- Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server,

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
                         {1.3.4.44#dev}
                         http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
```



Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, HSQLDB, H2, MonetDB, Apache Derby, Amazon Redshift, Vertica, Mckoi, Presto, Altibase, MimerSQL, CrateDB, Greenplum, Drizzle, Apache Ignite, Cubrid, InterSystems Cache, IRIS, eXtremeDB, FrontBase, Raima Database Manager, YugabyteDB and Virtuoso database management systems.

- Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band.
- Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
- Support to enumerate users, password hashes, privileges, roles, databases, tables and columns.
- Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack.
- Support to dump database tables entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.
- Support to search for specific database names, specific tables across all databases or specific columns across all databases' tables. This is useful, for instance, to identify tables containing custom application credentials where relevant columns' names contain string like name and pass.
- Support to download and upload any file from the database server underlying file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.

For more details visit : *https://www.snort.org/*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

OTP Theft

OTP fraud is executed by fraudsters by deceiving digital users into sharing OTP in following ways :

- Over a call posing with fake identities
- In person with fake identities and fake reasons
- Malware infested links to users to download malware that can read OTP

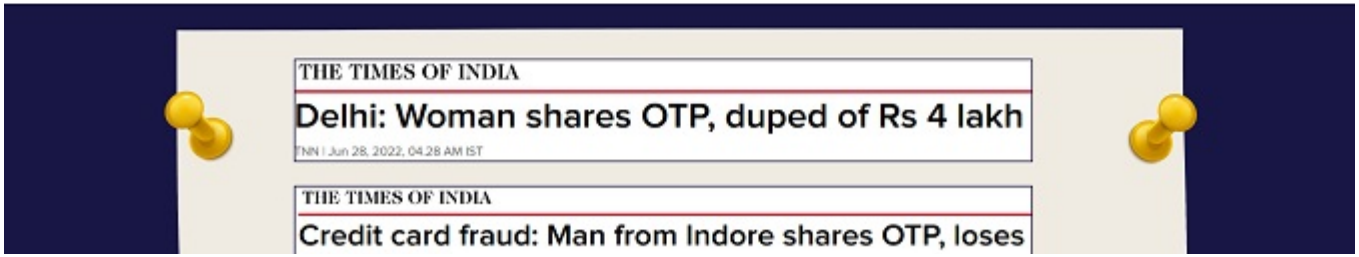
Dangers


FINANCIAL LOSS


BREACH OF DATA


MALWARE ATTACK


MOBILE & SYSTEM HACK



over ₹36K

TNN | Jun 23, 2022, 08.36 AM IST

Modus Operandi

Fraudsters impersonating as executives from companies/ agencies/ institutions

Call/meet individual users on different fake pretexts like

Free gifts/ offers/ discounts
Easy loans
KYC updation
Online shopping executive
Credit limit enhancement
Food delivery executives
etc.,

They convince them to share OTP for providing service

Fraudsters adopting various social engineering techniques to con people into revealing OTP

Advisory

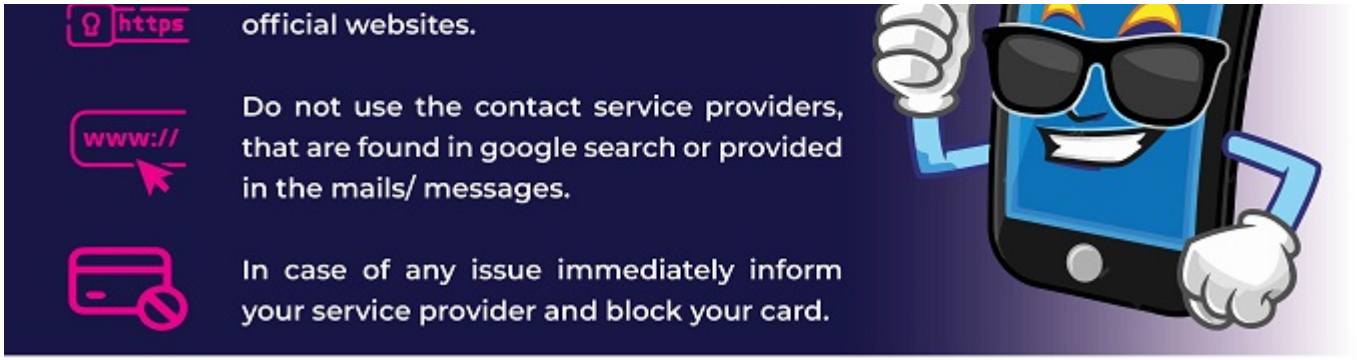
Never share or disclose OTP with anyone.

Do not share details by filling up forms.

Do not download any third party apps.

Avoid clicking on the links received from unknown sources.

Always use the contact details provided in


https
official websites.
www://
Do not use the contact service providers, that are found in google search or provided in the mails/ messages.
In case of any issue immediately inform your service provider and block your card.


Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
certin
NIC
National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by
www.
InfoSec
awareness.in
National Cyber Security Awareness Month
October, 2022
ISEA
www.isea.gov.in
"See Yourself in Cyber"
Drawing and Slogan Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
Cyber Bullying
Cyber Stalking
Password protection
Online Predators
Internet Ethics
Revenge pornography
Online Trolling ,
etc...
For more topics, please visit
www.infosecawareness.in


www.isea.gov.in
www.infosecawareness.in
infosecawarenesss
infosec_awareness
InfoSecAwa
InformationSecurityAwareness
Join 2-hour course on
Cyber Hygiene Practices
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
certin
NIC
National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
www.
InfoSec
awareness.in
National Cyber Security
Awareness Month
October, 2022
ISEA
www.isea.gov.in
Drawing


Slogan and
Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
• Cyber Bullying
• Cyber Stalking
• Password protection
• Online Predators
• Internet Ethics
• Revenge pornography
• Online Trolling , etc...
Last date for online submission
25th Oct,2022
For more information visit: www.infosecawareness.in/article/national-level-competitions2022
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
MINISTRY OF EDUCATION
Supported by
certm
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Smart devices without security can become slave devices"

Identity Theft

3 Properly dispose of documents with personal data.

4 Limit how much information you share.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | certin | NIC National Informatics Centre

Supported by: साइबर स्वच्छता केंद्र Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) www.cyberswachhtakendra.gov.in | Cyber Safe Girl | I4C

Implemented by: C-DAC

www.InfoSecawareness.in

Brochure

National Cyber Security Awareness Month

October, 2022

ISEA www.isea.gov.in

Online Sextortion

What is it ?

Online Sextortion occurs when online predator threatens to circulate your private and sensitive material online, if you do not provide images of a sexual nature, sexual favors, or money.

Why should we be concerned ?

You are blackmailed and sexually exploited or harassed by the online predator while being threatened to leak your private /sexual posts, pictures etc., online. This can be an extremely traumatic and devastating experience for you

Important Tips :

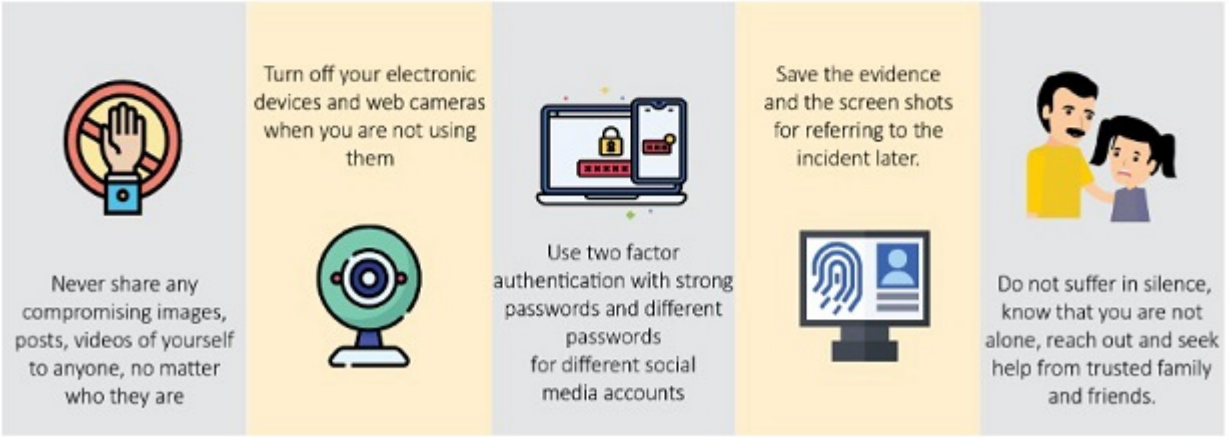
✓ *Always save the screen shots of the online incidents, messages, emails etc., as proof to support your claim or complaint with relevant evidence. Also make a note of the persons mobile num-*

ber and other details of the suspect or culprit.

✓ *Refer to the information given on the site cybercrime.gov.in related to various cyber crimes and related evidences to be submitted for the same.*

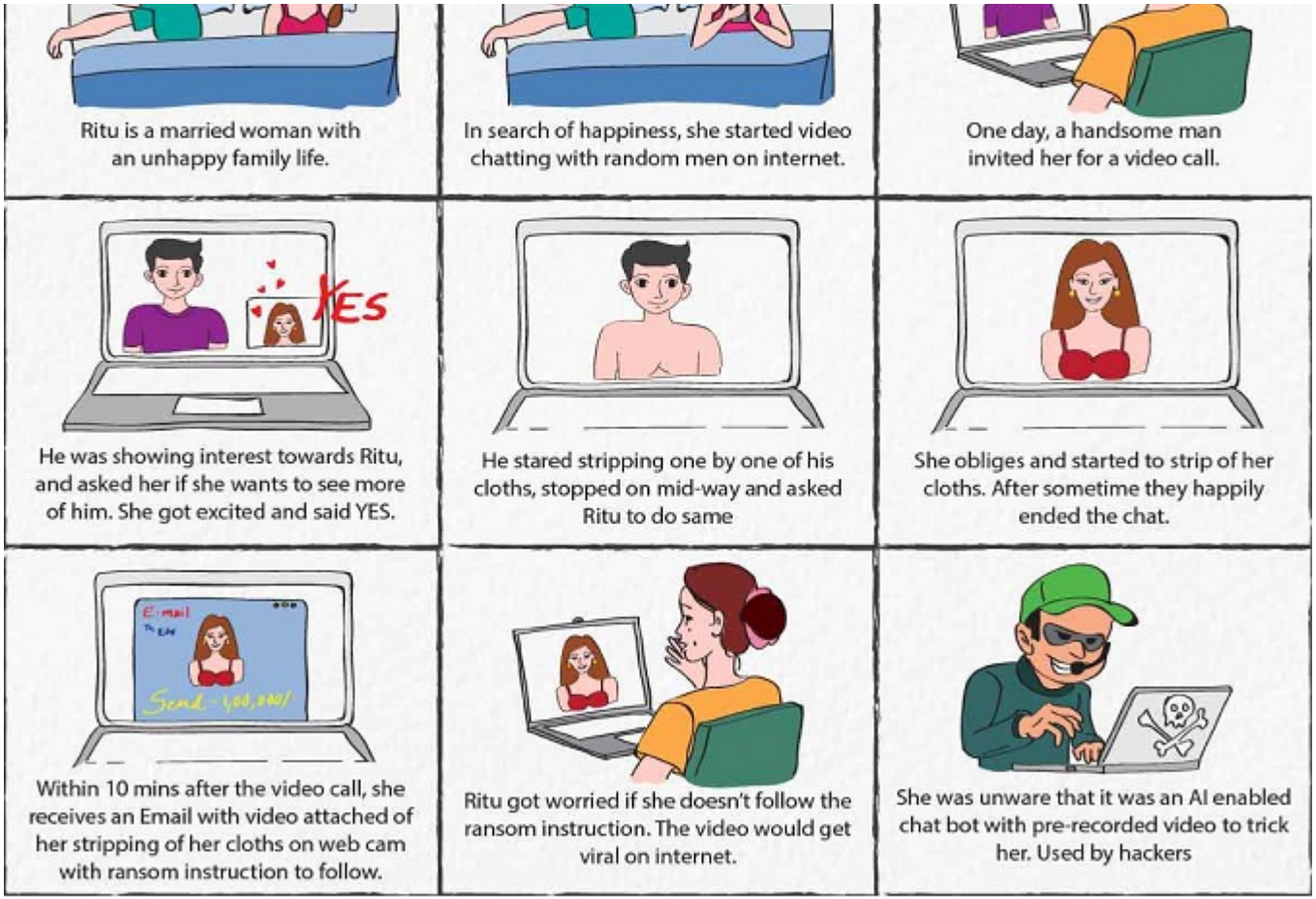
How can we safeguard ourselves against online sextortion ?

This kind of offence can cost you your peace of mind, they can drain you emotionally and cause negative mental/psychological effects effecting your health and well being. It is therefore important to understand the measures to protect yourself from it.



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: certin, NIC National Informatics Centre, साइबर स्वच्छता केंद्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, CYBER SAFE GIRL

Implemented by

pib FACT CHECK

राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022

Indian Railways
Lifeline to the nation...

Indian Railways Government Transport Subsidy! 26 May, 2022

Congratulations!

Indian Railways Government Transport Subsidy!

Through the questionnaire, you will have a chance to get 6000 Rupee .

Question 1 of 4 : Do you know Indian Railways ?

yes

no

"Siloscape" Malware

Virus Type: Malware Targeting Windows Containers

It has been reported that a new category of malware is targeting misconfigured Kubernetes clusters through Windows containers to compromise cloud environments. The malware variant gains initial access by exploiting vulnerabilities in common cloud applications or a vulnerable web page or database and then utilizes windows container escape techniques, executes code on underlying node and then spreads in poorly configured Kubernetes clusters to open a backdoor in order to run/deploy malicious containers. Once cluster is compromised, the attacker might be able to steal critical information such as usernames and passwords, an organization¿s confidential and internal files or even entire databases hosted in the cluster. This malware can leverage the computing resources in a Kubernetes cluster for cryptojacking and potentially exfiltrate sensitive data from hundreds of applications running in the compromised clusters.

Behaviour:

- Uses Windows container escape techniques to escape the container and gain code execution on the underlying node.
- Attempts to abuse the node's credentials to spread in the cluster.
- Siloscape uses the Tor proxy and an ".onion" domain to anonymously connect to its command and control (C2) server.

Best practices and Countermeasures:

- Kubernetes cluster configuration should restrict node privileges such that creation of new deployments is not possible. (It means that any process running in Windows Server containers should not have the same privileges as admin). Malware is ineffective in this case

- It is advised to follow Microsoft's recommendation of discarding use of Windows containers as a security feature. Hyper-V containers should be employed for operations that rely on containerization as a security boundary and it is recommended to move applications running in Windows Server containers to Hyper-V containers.

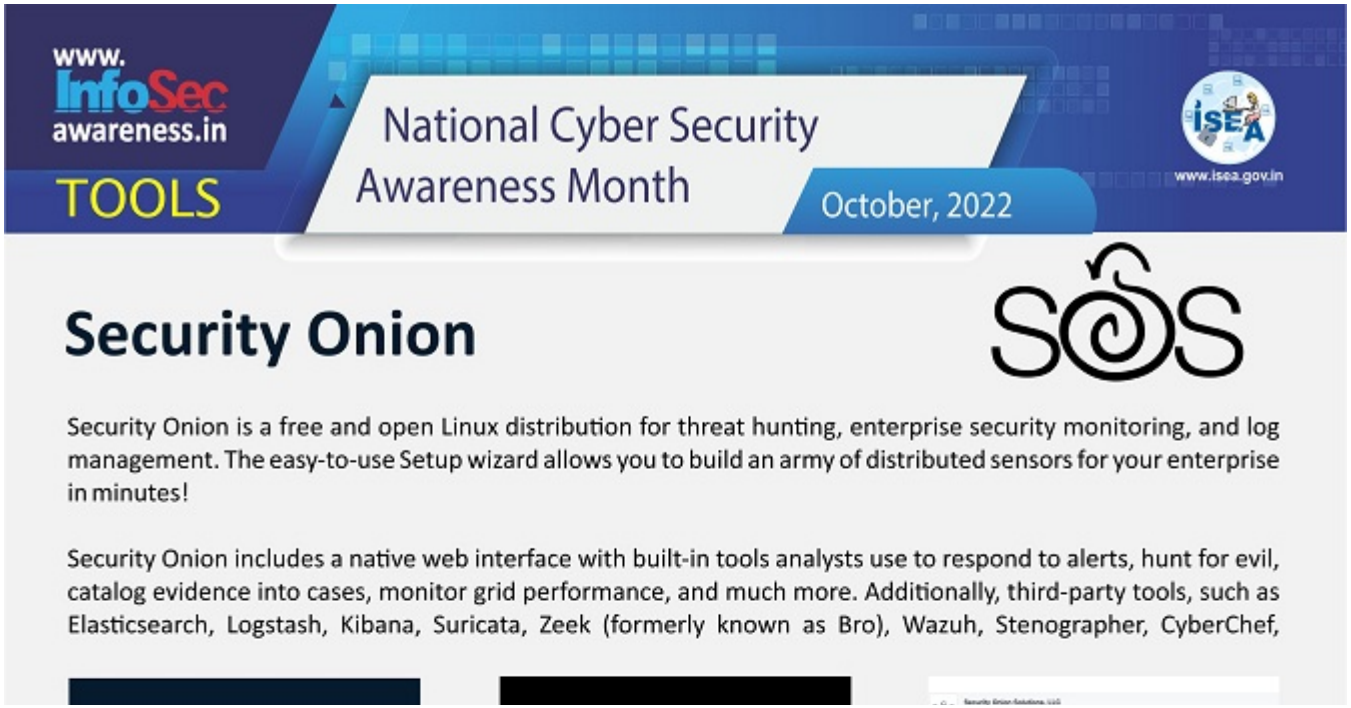
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.

- Check regularly for the integrity of the information stored in the databases.

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2021-1893

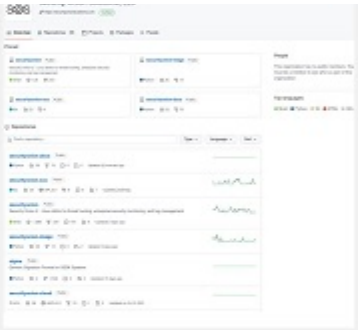
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in



Security Onion is a free and open Linux distribution for threat hunting, enterprise security monitoring, and log management. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

Security Onion includes a native web interface with built-in tools analysts use to respond to alerts, hunt for evil, catalog evidence into cases, monitor grid performance, and much more. Additionally, third-party tools, such as Elasticsearch, Logstash, Kibana, Suricata, Zeek (formerly known as Bro), Wazuh, Stenographer, CyberChef,



Use Cases

NIDS
Collect network events from Zeek, Suricata, and other tools for complete coverage of your network. Cast a wide net to catch the bad guys quickly and easily.

HIDS
Security Onion supports several host-based event collection agents including Wazuh, Beats, and osquery. Just point them to your installation and it's off to the races.

Static Analysis (PCAP and EVTX Import)
Use Security Onion to import full packet capture files for quick static analysis and case studies. Spin up a virtual machine quickly and get started in just a few minutes. Includes support for Windows Event logs.

SOC Workstation
A workstation install option is also available for SOC analysts to use local Linux tools to perform analysis of network and host events. No need to install extra tools, we bundle all the apps you might need.

For more details visit : *https://securityonionsolutions.com/software*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in


"See Yourself in Cyber"
Drawing and Slogan Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
Cyber Bullying
Cyber Stalking
Password protection
Online Predators
Internet Ethics
Revenge pornography
Online Trolling ,
etc...
For more topics, please visit www.infosecawareness.in
www.isea.gov.in
www.infosecawareness.in
infosecawarenesss
infosec_awareness
InfoSecAwa
InformationSecurityAwareness
Join 2-hour course on
Cyber Hygiene Practices
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in


Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
certin
NIC
National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by


www.
InfoSec
awareness.in
National Cyber Security
Awareness Month
October, 2022
ISEA
www.isea.gov.in
Drawing and
Slogan
Competition
Attractive prizes &
National level
certificates
for winners
Theme
Information/Cyber Safety
and Security
• Cyber Bullying
• Cyber Stalking
• Password protection
• Online Predators
• Internet Ethics
• Revenge pornography
• Online Trolling , etc...

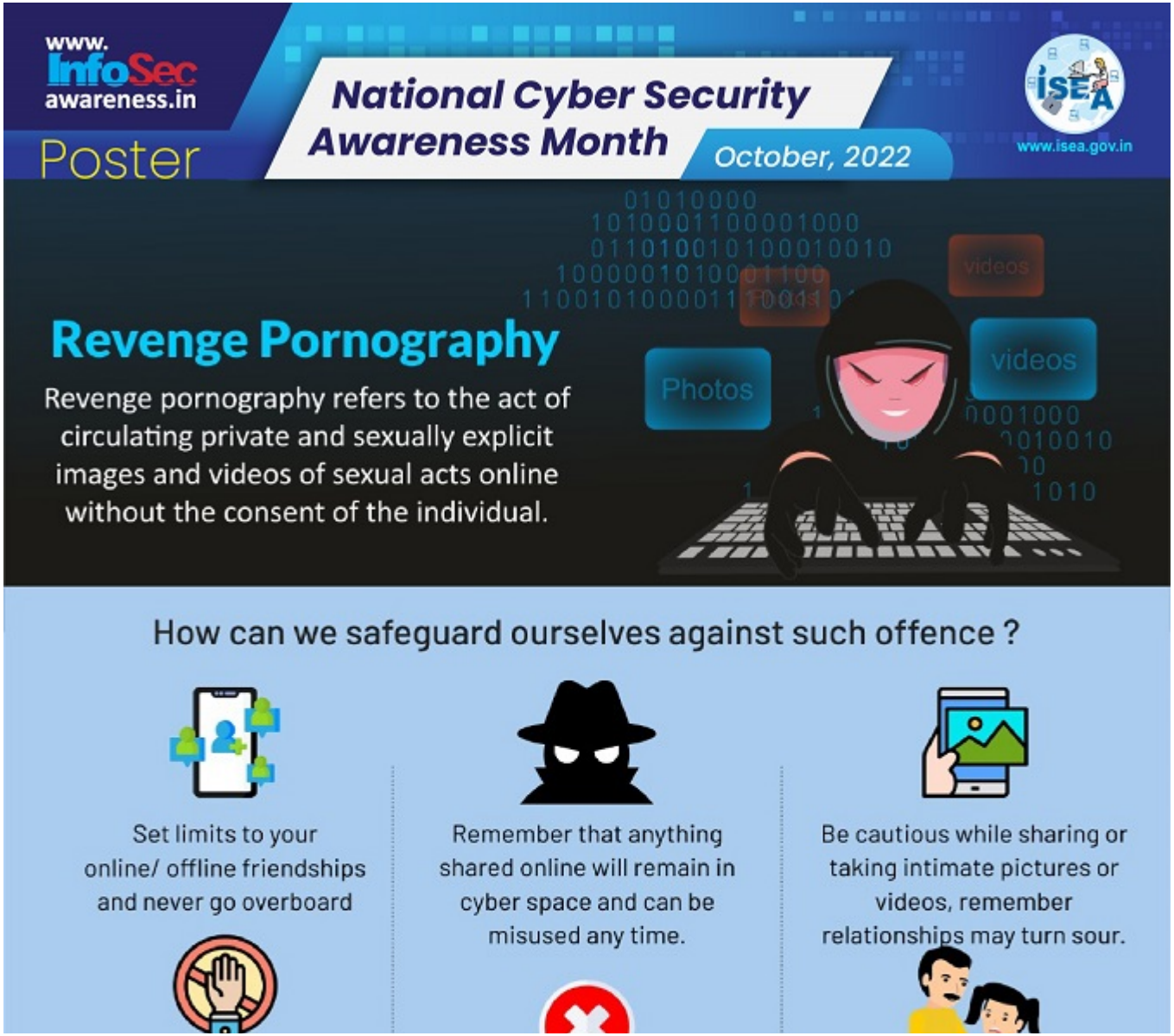

Last date for online submission
25th Oct,2022
For more information visit: www.infosecawareness.in/article/national-level-competitions2022
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
MINISTRY OF EDUCATION
Supported by
certin
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Keep your sensitive data out of reach, to prevent security breach"



Do not pursue or engage in maintaining relation with someone who pressurizes you to share personal intimate pictures or videos.

Do not forward any sexual pictures or images as it is violation of trust and in case can be a serious crime too.

In case of threats Don't suffer in silence, reach out for help from family and friends

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: certin, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra www.cyberswachhtakendra.gov.in, Cyber Safe Girl | Implemented by: ISEA, C-DAC

www.InfoSecawareness.in

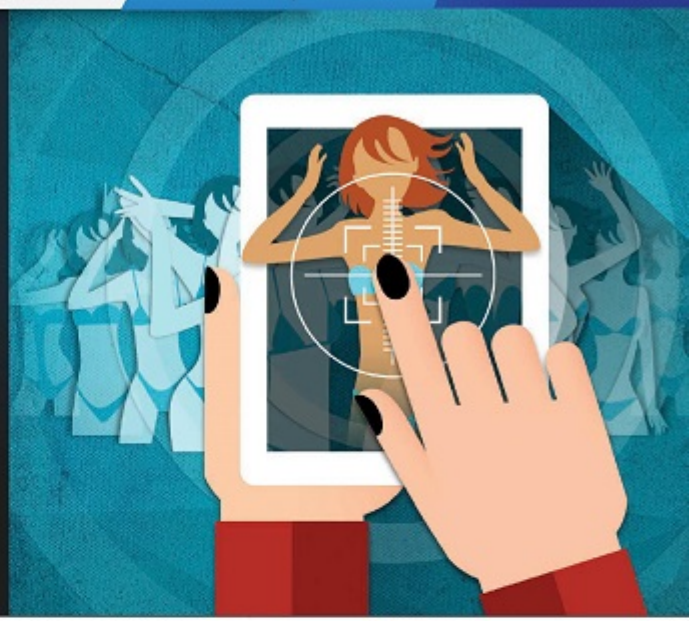
Brochure

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Revenge Pornography



What is it ?

Revenge pornography refers to the act of circulating private and sexually explicit images and videos of sexual acts online without the consent of the individual.

The private sexual act recorded by an intimate partner is used to intimidate, humiliate, blackmail, coerce, commit sextortion or punish the victim as an act of revenge, on a public platform. .

Why should we be concerned ?

Revenge pron damages your social image & reputation, you face humiliating, degrading remarks and messages and are trolled mercilessly, it leaves you emotionally, mentally and psychologically scarred for life.

How can we safeguard ourselves against such offence ?

It is quite important to understand and be aware of the possible dangers of the offence and take appropriate care and caution before hand to protect yourself. Mentioned below are few helpful tips-

Set limits to your online/ offline friendships and never go overboard

Remember that anything shared online will remain in cyber space and can be misused any time.

Be cautious while sharing or taking intimate pictures or videos, remember relationships may turn sour.

Do not pursue or engage in maintaining relation with someone who pressurizes you to share personal intimate pictures or videos.

Do not forward any sexual pictures or images as it is violation of trust and in case can be a serious crime too.

In case of threats Don't suffer in silence, reach out for help from family and friends

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: certin, Cyber Swachhta Kendra, NIC, CyberSafeGirl | Implemented by: ISEA

www.InfoSec awareness.in

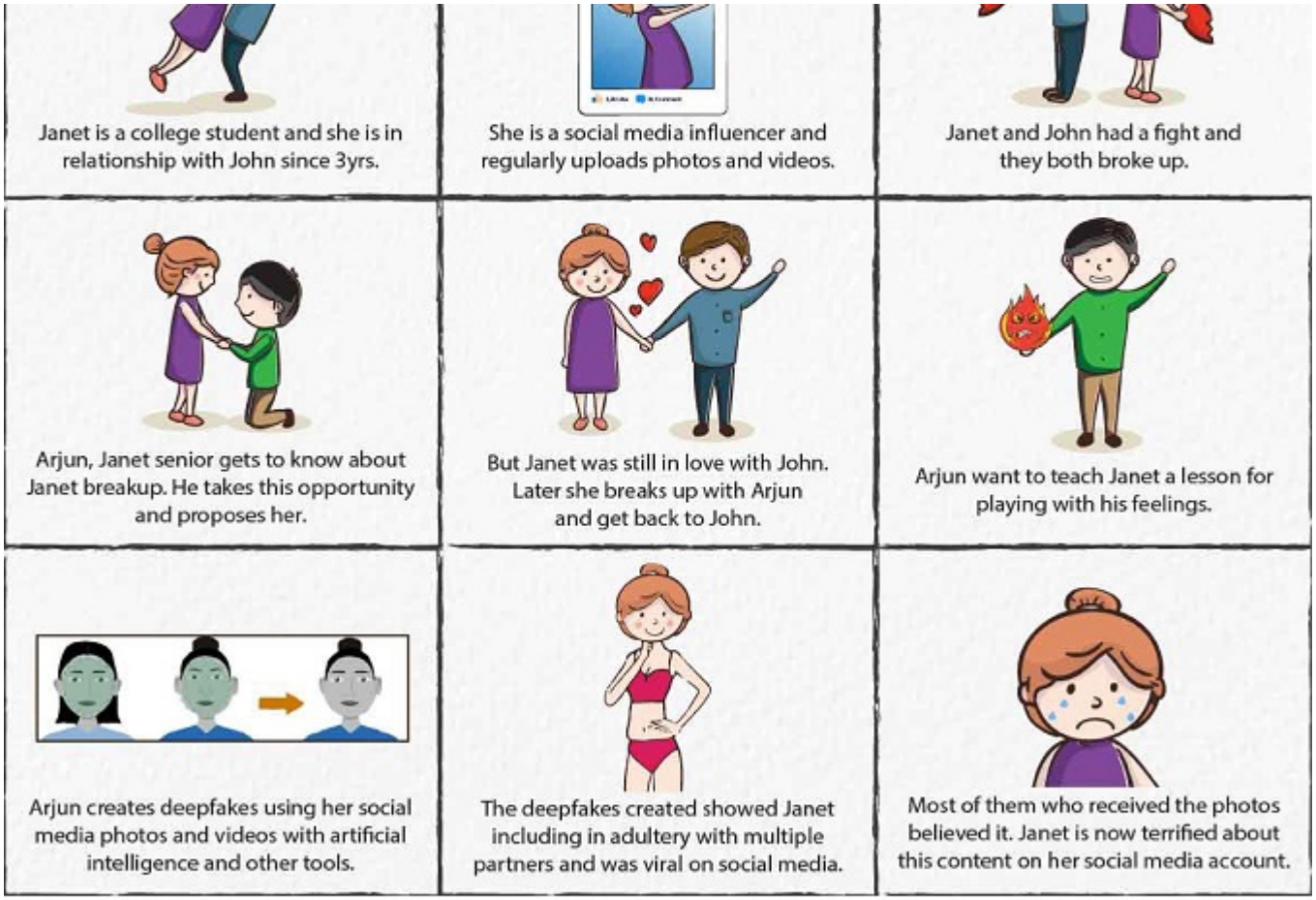
Storyboard

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Beware of Revenge Pornography



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in


FAKE ALERT!
Labour Ministry is NOT running such offer!
कर्मचारी राज्य बीमा निगम
Employees' State Insurance Corporation
Azadi Ka Amrit Mahotsav
श्रम एवं रोजगार मंत्रालय
GOVERNMENT OF INDIA
MINISTRY OF LABOUR EMPLOYMENT
सत्यमेव जयते
Those who worked btween 1990 and 2022 have the right to withdraw (Rs 155,000)
from Ministry Of Labour And Employment.
Check if your name is on the list of those who are entitled to withdraw these funds.
FAKE
FAKE
FAKE
#PIBFactCheck
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

Sarbloh Ransomware

Virus Type: Ransomware

It has been reported that a new ransomware named "Sarbloh" is spreading via specially crafted malicious documents sent as spear phishing email attachments. Malicious document is embedded with Marco with a heavily obfuscated VBA code, which downloads original payload (Sarbloh Ransomware) from an AWS URL silently. Once executed, it encrypts files on affected system (Audio, images, video, databases, and other document files) and renames the encrypted files with the ".sarbloh" extension to make them unusable. The ransom note ("README_SARBLOH.txt") states that the user's files are encrypted and will not be recovered until Sarbloh's creator's demands are fulfilled.

Best Practices and remedial measures:

Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection/attacks:

- Maintain updated Antivirus software on all systems
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Do not open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser
- Do not enable Macros if prompted by document received from untrusted sources.

- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.

- Check regularly for the integrity of the information stored in the databases.

- If not required consider disabling, PowerShell / windows script hosting.

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2021-1873

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in), Cyber Safe Girl, I4C | Implemented by: ISEA, C-DAC

www.InfoSec awareness.in

TOOLS

National Cyber Security Awareness Month

October, 2022

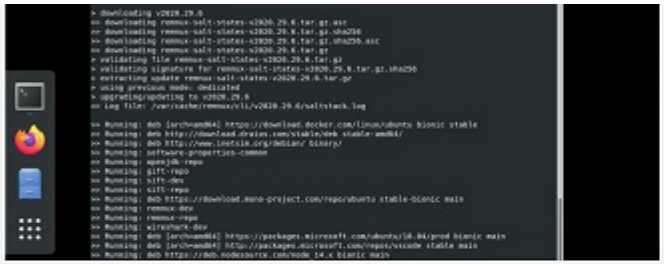
www.isea.gov.in

REMnux

A Linux Toolkit for Malware Analysis

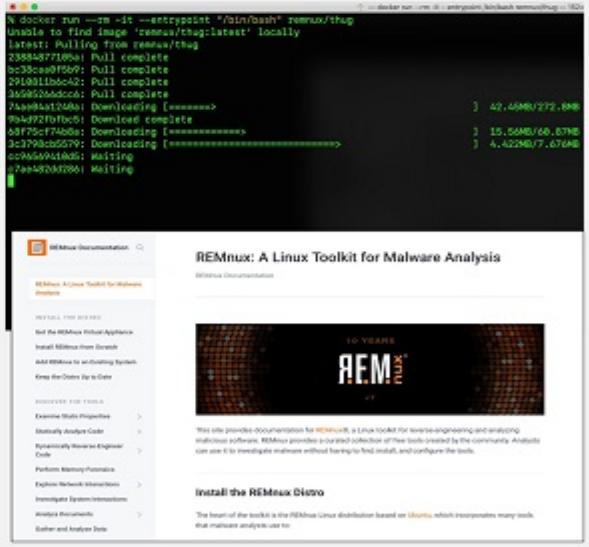
REMnux® is a Linux toolkit for reverse-engineering and analyzing malicious software. REMnux provides a curated collection of free tools created by the community. Analysts can use it to investigate malware without having to find, install, and configure the tools.

The easiest way to get the REMnux distro is to download the REMnux virtual machine in the OVA format, then import it into your hypervisor.



You can also install the distro from scratch on a dedicated host or add it to an existing system running a compatible version of Ubuntu.

The REMnux toolkit also offers Docker images of popular malware analysis tools, making it possible to run the them as containers without having to install the tools directly on the system. You can even run the REMnux distro as a container.



Docker is installed as part of the REMnux distro. If you're planning to run REMnux Docker images on another system, you may need to install Docker. The first time you run an image (e.g., using the docker run command), Docker will automatically download the image from Docker Hub, run it locally as an active container. Your system will need to be connected to the internet to retrieve the image; afterwards, Docker will use a locally cached copy. You can use the docker pull command to update the cached version of the image

For more details visit : *https://remnux.org/*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) www.cyberswachhtakendra.gov.in, Cyber Safe Girl | Implemented by: ISEA


! Fraud Alert !
Fake messages about Government subsidy/offers
Are you receiving such messages !!!
Indian Railways
Congratulations!
Indian Railways Government Transport Subsidy!
Through the questionnaire, you will have a chance to get 6000 Rupee .
Question 1 of 4 : Do you know Indian Railways ?
yes
no
Comment
Neha Kale
I thought it was a joke, but it was delivered this morning! So surprised! @Indian Railways is the
Indian Railways Government Transport Subsidy!
India Post Government subsidies!
Every citizen can enjoy government sub...
www.indiapost.gov.in
http://particularrim.top/indiapost/tb.php
Get your new coronavirus subsidy
50000 INR
Click to receive
klbwa.001esport.com
Digital users 'Beware', fake links and messages are being spread across instant messaging apps and social media platforms by fraudsters.
These messages are sent on pretext of subsidies/grants/offers by government to lure people into clicking on fake links.
The fraudsters aim to siphon money, hack your accounts/passwords, install
Warning Sings
Koogle .com
Tweaked website/ URL/ Links
Dear ALL
Impersonalized/ generic message/mail
Requesting for unrelated PII
(Personal Identifiable Information)

victim of cyber-attacks through such fake links/messages.

Can sound too good to be true

Modus Operandi

User receives messages / links/ posts about government subsidies/cash offers etc.,

User is prompted to click on the link or participate in survey or register

Redirects the user to malicious sites

Leads to data leak, malware/ virus attacks

Advisory

- Immediately block the number & report against such fake offers
- Install antivirus on your digital devices for security & protection
- Do not forward fake messages, links & mails to people without proper verification
- Be aware & alert about such attempts of cyber criminals by keeping track of the latest news
- Never share your personal or financial details like login credentials/ passwords/credit
- Always ensure to verify the information by visiting the official government website,


or debit card details
for any authorized notification
Never believe such posts, messages, mails regarding government subsidies/ cash offers etc., with links to register, these are usually used as bait by cyber fraudsters
Never click on unknown links or download unauthorized apps or software on your digital devices as it can install malicious software on your device
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by
www.cyberswachhtakendra.gov.in
www. InfoSec awareness.in
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
ISEA awareness Newsletters on SEXUAL CYBER CRIME
InfoSec
Activity
Page 2
Concept
Page 4
Virus Alert
Page 15
Cuber Offences that are


Sexual in Nature -Vol II
Scan and Download
https://infosecawareness.in/newsletter/nov21
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC
National Informatics Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by
www.
InfoSec


awareness.in
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
"See Yourself in Cyber"
Drawing and Slogan Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
Cyber Bullying
Cyber Stalking
Password protection
Online Predators
Internet Ethics
Revenge pornography
Online Trolling , etc...
For more topics, please visit www.infosecawareness.in
www.isea.gov.in
www.infosecawareness.in
infosecawarenesss
infosec_awareness
InfoSecAwa
InformationSecurityAwareness
Join 2-hour course on
Cyber Hygiene Practices


Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
Implemented by
www.cyberswachhtakendra.gov.in
www. InfoSec awareness.in
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
Drawing and Slogan
Competition
Attractive prizes & National level certificates for winners
Theme
Information/Cyber Safety and Security
• Cyber Bullying
• Cyber Stalking
• Password protection
• Online Predators


• Internet Ethics
• Revenge pornography
• Online Trolling , etc...
Last date for online submission
25th Oct,2022
For more information visit: www.infosecawareness.in/article/national-level-competitions2022
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
MINISTRY OF EDUCATION
Supported by
cert-in
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

"Don't be safety blinded, be safety minded."

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

In the current digital age, the usage of mobile has become essential and inevitable. From simple communication to managing sensitive online transactions, it is put to use for almost every possible

activity in our daily life. This extensive usage of mobile has made it an attractive target for malicious attacks by cyber fraudsters, that can compromise with users security & privacy or even gain complete control over the device.

Safety Guidelines for securing mobile devices

Never leave your mobile device unattended

Always update your devices with the latest software

Report lost or stolen devices immediately to the nearest Police Station

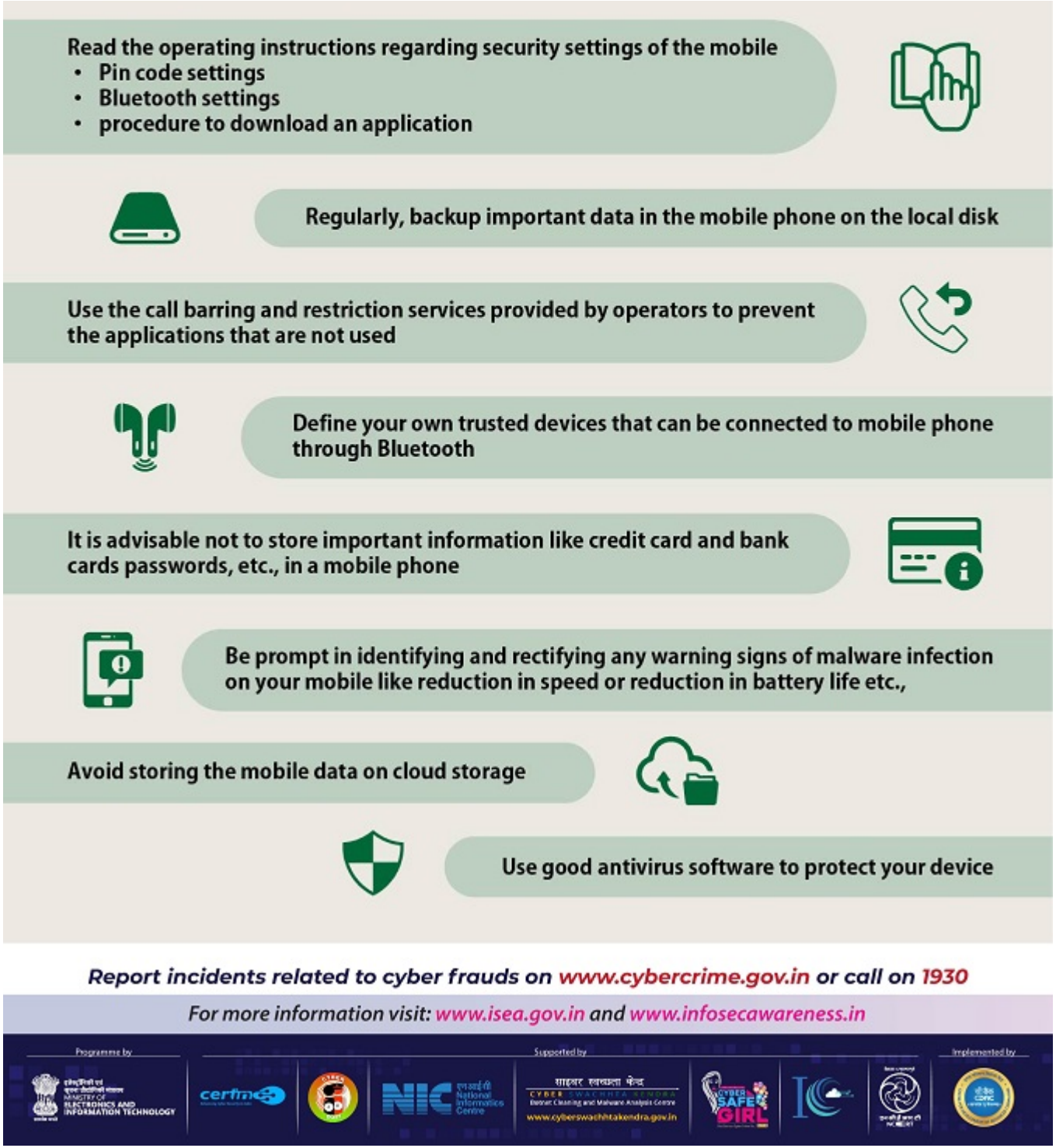
Use Wi-Fi only when required. It is advisable to switch off the service when not in use

Avoid downloading content from untrusted sources

Be careful while downloading applications through Bluetooth or as MMS attachments as they may contain harmful software

Keep the Bluetooth connection in a hidden or non-discoverable mode

Choose a PIN that is unpredictable yet easy to remember for you


Read the operating instructions regarding security settings of the mobile
• Pin code settings
• Bluetooth settings
• procedure to download an application
Regularly, backup important data in the mobile phone on the local disk
Use the call barring and restriction services provided by operators to prevent the applications that are not used
Define your own trusted devices that can be connected to mobile phone through Bluetooth
It is advisable not to store important information like credit card and bank cards passwords, etc., in a mobile phone
Be prompt in identifying and rectifying any warning signs of malware infection on your mobile like reduction in speed or reduction in battery life etc.,
Avoid storing the mobile data on cloud storage
Use good antivirus software to protect your device
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
www.cyberswachhtakendra.gov.in
Implemented by

www.InfoSec awareness.in

Storyboard

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Be aware of Juice Jacking

Nidhi is staying in delhi with her parents. She useds her father phone for playing games and watching youtube

She is traveling to her grandparents house for a family function.

She ran out of charge in her father phone, so she used free airport charging station to charge phone

Her father found out that his phone suddenly got slower and hotter

Then he delete unwanted file and scanned with antivirus which showed dangerous malware that reduced his phone performance

He thought malware might be injected into phone via charging cable at charging station

Later he found that her confidential office data were stolen from the phone via Juice Jacking

He thought many people might be using charging station daily and being victim of Juice Jacking

So he decied to report to cyber crime regarding this issuse he faced and he uses power bank in futher

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930


For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by
PIB FACT CHECK
राष्ट्रीय साइबर सुरक्षा
जागरूकता माह - अक्टूबर 2022
यह मैसेज फ़र्ज़ी है
Amrit Mahotsav
श्रम एवं रोजगार मंत्रालय
GOVERNMENT OF INDIA
MINISTRY OF LABOUR
EMPLOYMENT
सत्यमेव जयते
Sabka Saath
Sabka Vikas
Sabka Vishwas
Sabka Prayas
Those who worked between 1990 and 2022 have
the right to withdraw (Rs 155,000)
#PIBFactCheck


from Ministry Of Labour And Employment.
Check if your name is on the list of those who are entitled to withdraw these funds.
Send us your queries here
pib FACT CHECK
Follow us on social media!
+9187997 11259
socialmedia@pib.gov.in
@PIBFactCheck
/PIBFactCheck


Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
www.isea.gov.in
साइबर स्वच्छता केन्द्र
www.cyberswachhtakendra.gov.in
Implemented by


www.InfoSec awareness.in
Malware Alerts
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
Adrozek Malware
Virus Type: Browser Modifiers
It has been reported that a new malware named Adrozek is affecting user's device globally. It infects the device and then proceeds to modify web browsers and their settings in order to inject ads into search results pages.
Infection Mechanism:
The malware is distributed via classic drive-by download schemes. Users are typically redirected from legitimate sites to shady domains
Distribution infra
Installer
Server
Ad injection scripts
Injects ads into search results

where they are tricked into installing malicious software. The software installs the Adrozek malware, which then proceeds to obtain reboot persistence with the help of a registry key. The malware looks for locally installed browsers such as Microsoft Edge, Google Chrome, Mozilla Firefox, Yandex Browser and attempts to force-install an extension by modifying the browser's AppData folders.

Best practices for prevention:

- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- Users are advised to update their devices with patches as & when released by respective OEM.
- If devices found infected, it is recommended to re-install the browsers.
- Be aware of the risks of downloading and installing software from untrusted sources and clicking ads or links on suspicious websites.

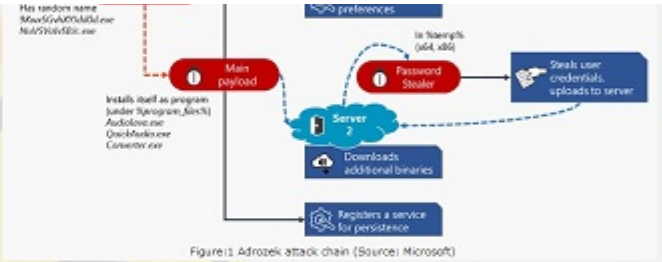


Figure 1: Adrozek attack chain (Source: Microsoft)

It also modifies some of the browsers' DLL files to change browser settings and disable security features to make sure that browser's security features doesn't detect unauthorized modifications, modifications performed by Adrozek include:

- Disabling browser updates.
- Disabling file integrity checks.
- Disabling the Safe Browsing feature.
- Registering and activating the extension they added in a previous step.
- Allowing their malicious extension to run in incognito mode.
- Allowing the extension to run without obtaining the appropriate permissions.
- Hiding the extension from the toolbar.
- Modifying the browser's default home page.
- Modifying the browser's default search engine.

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1853

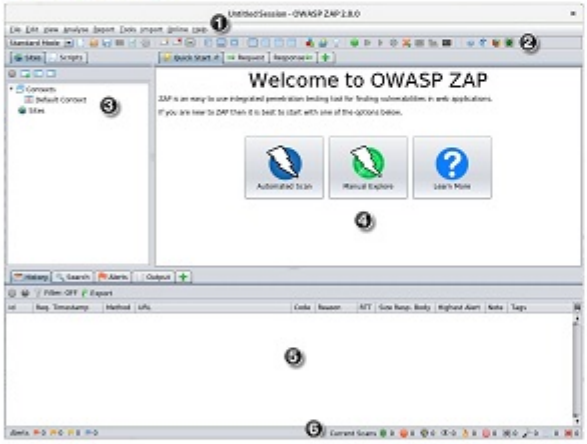
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

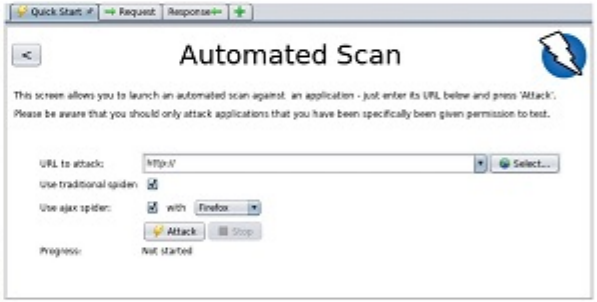
For more information visit: www.isea.gov.in and www.infosecawareness.in

Zed Attack Proxy (ZAP)

ZAP is an open source penetration testing tool designed specifically for testing web applications. It is known as a "man-in-the-middle proxy," where it intercepts and inspects messages sent between browsers and web applications. ZAP provides functionality for developers, testers new to security testing and security testing specialists. There are also versions for each major operating system and Docker. Additional functionality is available via add-ons in the ZAP Marketplace.

ZAP Desktop UI





The easiest way to start using ZAP is via the Quick Start tab. Quick Start is a ZAP add-on that is included automatically when you installed ZAP.

To run a Quick Start Automated Scan :

- Start ZAP and click the Quick Start tab of the Workspace Window.
- Click the large Automated Scan button.
- In the URL to attack text box, enter the full URL of the web application you want to attack.
- Click the Attack

For more details visit : *https://www.zaproxy.org/*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930


For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
cert-in
NIC
National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

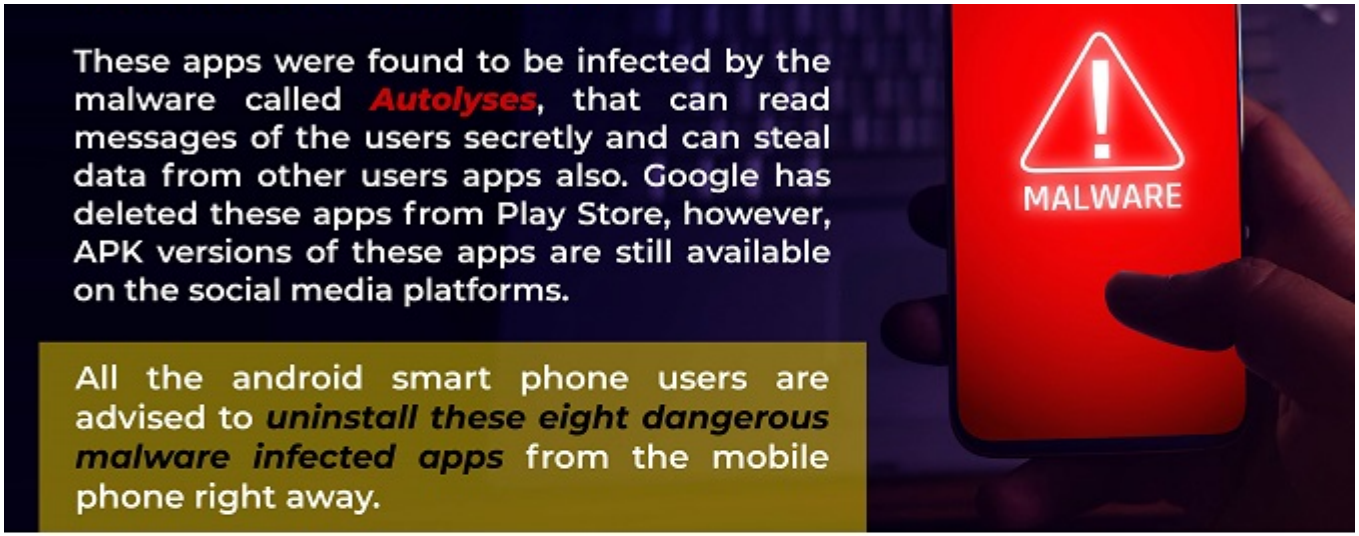
"Do not use computers to harm others"

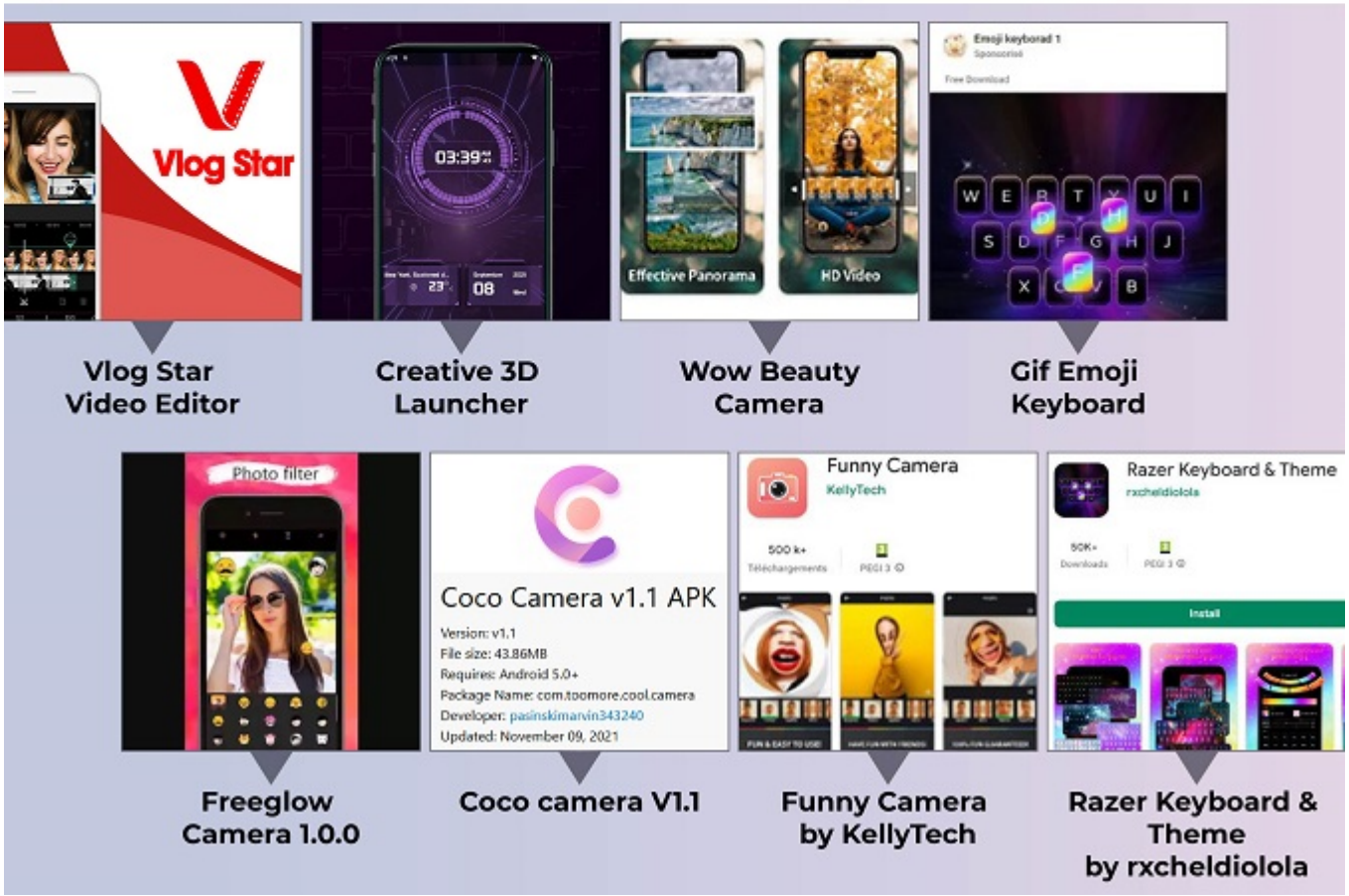

Reset your phone to factory settings to remove any malware
Do good research about apps and their developers by reading the reviews
Make sure you review and manage permissions for each app you download
Avoid installing apps by clicking on links in emails, social media etc.,
Always keep an updated anti virus security solution installed
Look at the publish date. A fake app will have a recent publish date
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC
www.cyberswachhtakendra.gov.in
Implemented by

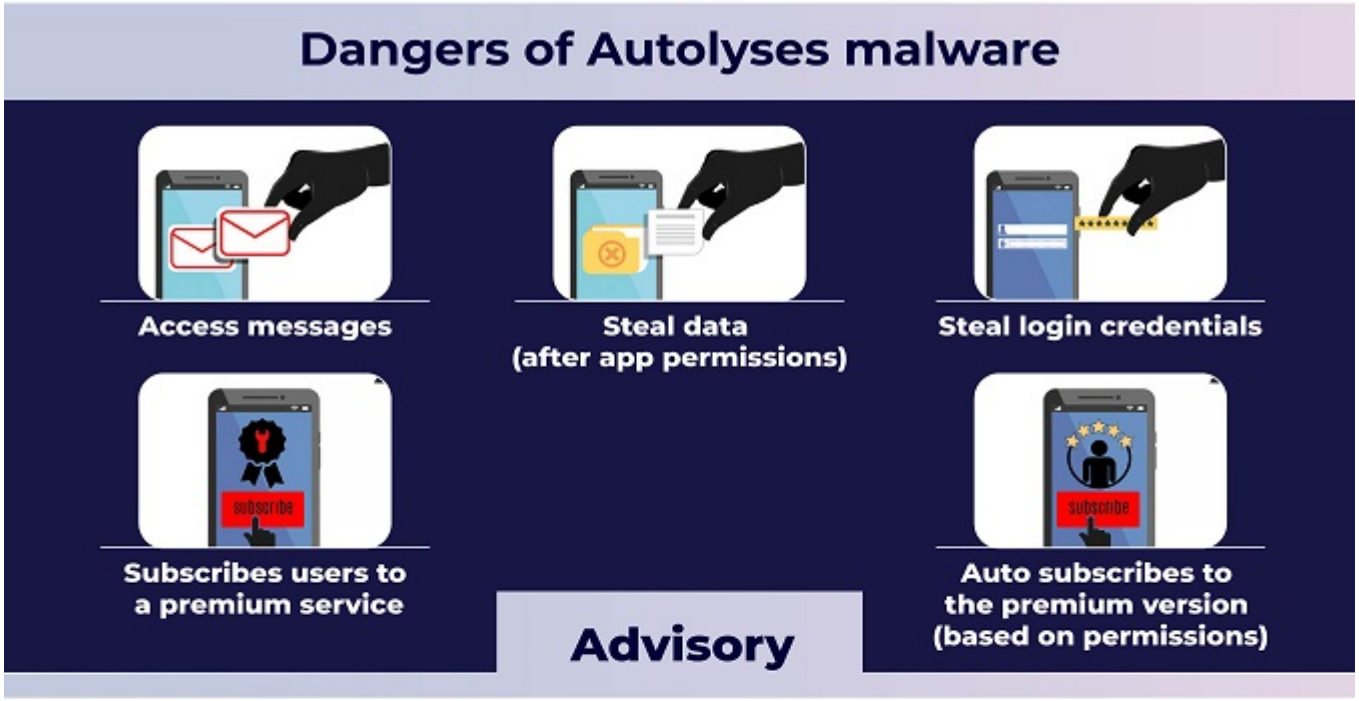

www.InfoSec awareness.in
Poster
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
Mobile Application Security
user reviews
good
very good
excellent
poor
Available on the App Store
Google play
Use only official stores for downloading Apps
Do good research about apps and their developers by reading the reviews
Check for spelling


Reset your phone to factory settings to remove any malware
Make sure you review and manage permissions for each app you download
Uninstall apps when you no longer use
mistakes in the title or description
Beware of apps that promise shopping discounts
Avoid installing apps by clicking on links in emails, social media etc.,
Terms & Conditions
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by


www.InfoSec awareness.in
Advisory
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
! Beware ! MALICIOUS APPS DETECTED
A security alert is issued to all the android smart phone users about dangerous malware found in 8 android Mobile Apps.


These apps were found to be infected by the malware called Autolyses, that can read messages of the users secretly and can steal data from other users apps also. Google has deleted these apps from Play Store, however, APK versions of these apps are still available on the social media platforms.
All the android smart phone users are advised to uninstall these eight dangerous malware infected apps from the mobile phone right away.
MALWARE


Vlog Star
Vlog Star Video Editor
Creative 3D Launcher
Effective Panorama
HD Video
Wow Beauty Camera
Gif Emoji Keyboard
Photo filter
Freeglow Camera 1.0.0
Coco Camera v1.1 APK
Version: v1.1
File size: 43.86MB
Requires: Android 5.0+
Package Name: com.toomore.cool.camera
Developer: pasinskimarvin343240
Updated: November 09, 2021
Coco camera V1.1
Funny Camera
KellyTech
Funny Camera by KellyTech
Razer Keyboard & Theme
rxcheldiolola
Install
Razer Keyboard & Theme by rxcheldiolola



Download applications only from trusted sources

Avoid downloading apps from SMS, APIs, social media messages, or by clicking advertisements

Google Play Protect

Before downloading a mobile app. check for play protect feature on Google Play Store

Properly verify the app details in the developer's website before downloading it

AD

Avoid installing mobile applications which contains advertisements

Pay attention to reviews and comments of the users, before installing any applications

Be cautious about allowing any permissions during the installation of the applications

Use a trusted anti-virus software for mobile security to stay safe from android malware

UNINSTALL

Ensure that you immediately uninstall these android apps

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in), Cyber Safe Girl, I4C | Implemented by: C-DAC

www.InfoSecawareness.in

TOOLS

National Cyber Security Awareness Month

October, 2022

ISEA www.isea.gov.in

Browser JSGuard

Protects from JavaScript based Threats

About Browser JSGuard

In the recent times, most of the systems connected to Internet are getting infected with malware and some of these systems are even becoming zombies for the attacker. When user knowingly or unknowingly visits a malware website, his system gets infected. Attackers do this by exploiting vulnerabilities in web browser and it is possible to acquire control over the underlying Operating System. Once attacker compromises the user's web browser, he can instruct the browser to visit the attacker's website by using number of redirections. During the process, user's web browser downloads the malware without the intervention of the user. Once the malware is downloaded, it would be placed in the file system and responds as per the instructions of the attacker. These types of attacks mostly happen through JavaScript and malicious HTML tags. Browser JSGuard detects and defends from such attacks made through the web browser. It blocks access to the harmful, inappropriate and dangerous websites that may contain malicious content.

Salient Features

- Content/Heuristic based JS & HTML malware protection
- Alerts the User on visiting Malicious Web pages
- Provides detailed analysis of webpage threats
- Ease of installation / maintenance

- Suitable for both home and office usage
- Signed by Mozilla Add-on community

JavaScript & HTML threats detected by Browser JSGuard

- Client side Redirections
- Redirections through DOM changing functions
- Runtime JavaScript Injections

System Requirements

- Operating Systems : Windows and Linux
- Browsers
  - Mozilla Firefox (Version >= 21.0)
  - Google Chrome (Version >= 21.0)

Download links

- For Firefox web browser: https://addons.mozilla.org/en-US/firefox/addon/browser-jsguard/
- For Google chrome web browser: https://chrome.google.com/webstore/detail/browserjsguard/ncpkigeklafkopcelcegambndlhkcbhb

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: certin, CYBER SWACHHTA KENDRA, Botnet Cleaning and Malware Analysis Centre, www.cyberswachhtakendra.gov.in, NIC National Informatics Centre, CYBER SAFE GIRL

Implemented by: C-DAC


ONLINE GAS AGENCY
DEALERSHIP
सत्यमेव जयते
BHARAT PETROLEUM CORPORATION LTD.
WEBSITE: www.ujjwalagasagency.in
OFFICIAL MAIL: info@ujjwalagasagency.in
ADD: Ujjwala Gas Agency vitarak kendra Block G-13 Bandra Kurla complex Mumbai 400051, INDIA.
REG.NO. MV7541GA
APPROVAL LETTER
Date-
Mr.
LPG VITRAK CHAYAN is Installing Gas Agency D ship under UJJWALA YOJANA across India. We are informing you that Ujjwala has agreed to vide BHARAT GAS agency ership w reference number PMUY/GADS/10661/477IG on the la referred by you at pin 202526. On basis of your documents and suitability of your land sp the iss based on ms and conditions will be according to policies of the pany in the fi of the agre ent.
After issue of your NOC CERTIFICATE through our area m ger will appoint a date for Site verification and Agree purpose of our terms and co ions on your property, along the period of deal compan ct 1956 n case of any legal pr ure.
For registration procedures you need to depo registration fees of Rs. 12,500/- only ompany's account through NEFT/RTGS/IMPS or online we don't accept cash deposit th gh the bank or any other method.
Once the deal begins and agency gets installation don ur land th sche t be terminated before maturity period of 25 years. Delay by you may te ne whole issues get condemned.
Dear Applicant kindly deposit your registration fees for the further procedures, within 24 hours of issue of approval letter. The deposited amount will be refunded.
फेक
#PIBFactCheck
संदिग्ध जानकारी यहाँ साझा करें
+918799711259
socialmedia@pib.gov.in
सोशल मीडिया पर हमें फॉलो करें
@PIBFactCheck
/PIBFactCheck
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
www.isea.gov.in
www.cyberswachhtakendra.gov.in
Implemented by

www.InfoSec awareness.in

Storyboard

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Keep Safe & Limited Mobile Applications

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology

Supported by: certin, CERT-In, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C

Implemented by: Data Security Council of India, CDAC

www.InfoSec awareness.in

Malware Alerts

National Cyber Security Awareness Month

October, 2022

ISEA www.isea.gov.in

Mozi IoT Botnet

Virus Type: IoT Botnet

It has been reported that a new malware named Mozi is affecting IoT devices globally. Affected IoT devices are being assembled into an IoT botnet which could be employed by botnet owner for launching distributed denial-of-service (DDoS) attacks, data exfiltration and payload execution.

According to the reports, Mozi malware is comprised of source code from Gafgyt, Mirai, and IoT Reaper; malware families which are targeting IoT devices. Mozi could compromise embedded Linux device with an exposed telnet. It mainly targets home routers and DVRs which are either unpatched, loosely configured or have weak/default telnet credentials. The infected devices form a peer-to-peer (P2P) botnet and uses a distributed hash table (DHT) to communicate with other infected host systems.

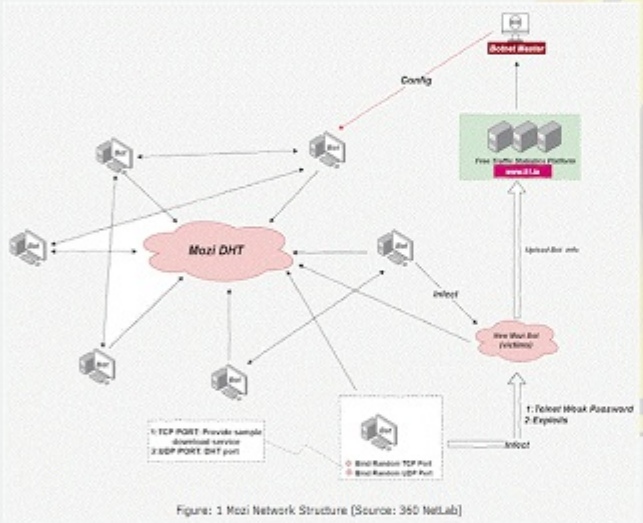


Figure: 1 Mozi Network Structure (Source: 360 NetLab)

VULNERABILITY	AFFECTED DEVICES
Eir D1000 Wireless Router RCI	Eir D1000 Router
Vacron NVR RCE	Vacron NVR devices
CVE-2014-8361	Devices using the Realtek SDK
Netgear cig-bin Command Injection	Netgear R7000 and R6400
Netgear setup.cgi unauthenticated RCE	DGN1000 Netgear routers
JAWS Webserver unauthenticated shell command execution	MVPower DVR
CVE-2017-17215	Huawei Router HG532
HNAP SoapAction-Header Command Execution	D-Link Devices
CVE-2018-10561, CVE-2018-10562	GPON Routers
UPnP SOAP TelnetD Command Execution	D-Link Devices
CCTV/DVR Remote Code Execution	CCTV DVR

Best practices for prevention:

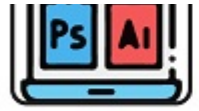

best practices for prevention:
• Users are advised to update their devices with patches as & when released by respective OEM of devices
• If devices found infected, it is recommended to reset device firmware or restore it from trusted backup.
• Monitor or block UDP traffic from the device to Bit Torrent DHT bootstrap nodes
• Block outgoing TCP traffic with destination ports 22, 23, 2323, 80, 81, 5555, 7574, 8080, 8443, 37215, 49152, and 52869, if not in use.
For more details visit: https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1833
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Respect the privacy of others"



Use Licensed Software and always Backup your data

Keep Login Credential Secure

Always use updated firewall and Windows Defender

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology; cert-in; Supported by: NIC National Informatics Centre; साइबर स्वच्छता केन्द्र Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in; Cyber Safe Girl; Implemented by

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, साइबर स्वच्छता केंद्र Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, Cyber Safe Girl | Implemented by: C-DAC

राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022

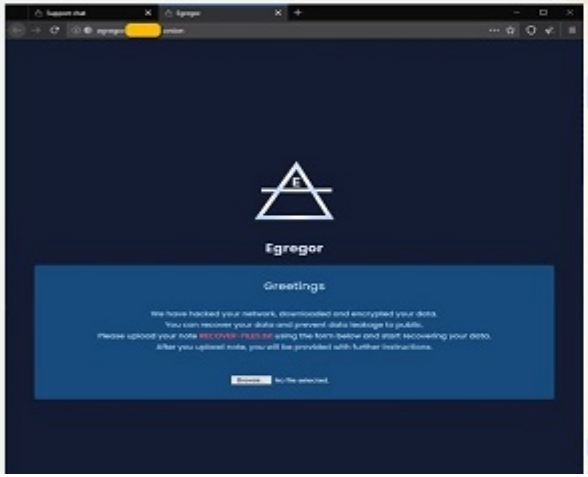

FAKE ALERT!
MTNL NEVER SENDS SUCH MESSAGES
12:46 PM
Dear MTNL user your MTNL KYC Has been Expired call immediately for verific
will be blocked within 24
ir MTNL
FAKE
FAKE
FAKE
#PIBFactCheck
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck
/PIBFactCheck

Egregor Ransomware

Virus Type: Ransomware

It has been reported that a new ransomware, named as Egregor is affecting organizations globally. The modus operandi used is typically breaking into organizations, stealing sensitive data, and running the malware to encrypt their files and threatens "Mass-Media" Release of Corporate Data if ransom not paid in due time. It uses double extortion tactics generally used by NetWalker ransomware families.

Initial Infection vector and propagation mechanism is still unknown, it is anticipated that Egregor ransomware may infiltration via spam email attachments or maliciously crafted link shared via email/instant messaging chats.



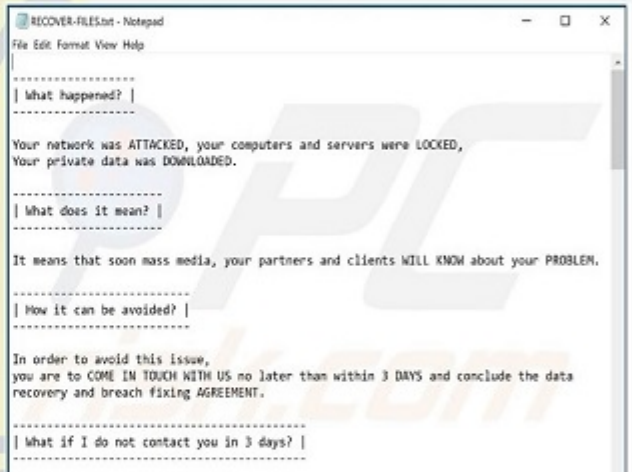


Figure:2 Egregor ransomware web page

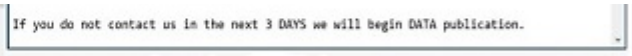


Figure:1 Ransom note by Egregor ransomware

Best practices for prevention:

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Check regularly for the integrity of the information stored in the databases.
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1813

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

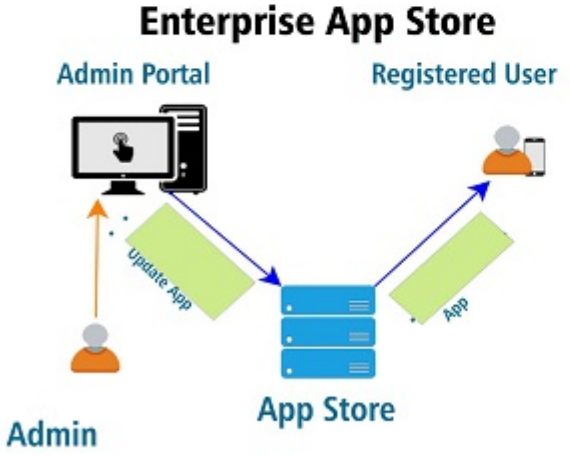
For more information visit: www.isea.gov.in and www.infosecawareness.in

allows to remotely lock and wipe the devices through a single, easy-to-use interface.

App store with Enterprise approved mobile apps makes application distribution easier and more streamlined. It gives users the freedom to choose and install only required corporate-approved apps. For an enterprise, it could lower the device vulnerability to unnecessary downloads and other security related threats.

Features of Enterprise App Store

- Private/Trusted application store for Enterprise Applications
- Remote administration of Enterprise mobile devices or BYOD devices
  - Remote Lock & Wipe
  - Remote app update
  - Remote policy enforcement
- Option to integrate with custom hardened Android platform
- Web console for managing the users & devices
  - User Registration
  - Device Registration
- Secure communication between the Enterprise app store and registered devices



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Encourage family to use internet safely"

against viruses, Trojans, worms, etc. use anti-virus software

attachments and files before downloading them to your system

strong unique passwords for all of your accounts

on Web links sent by someone you do not know

suspicious emails and requesting confidential information

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: certin, CISO, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra, www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C | Implemented by: CDAC

www.InfoSecawareness.in

Brochure

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Data Security measures for Desktop/Laptop

Data security refers to the protection of data from unauthorized access, use, change, disclosure and destruction. There are different types of data security measures such as data backup, encryption and antivirus software, which will ensure the security of your sensitive data.

1. Enable Auto-updates of your Operating System and update it regularly.

2. Download Anti-Virus Software from a Trusted Website and Install. Make sure it automatically gets updated with latest

virus signatures.

3 **Backup :** Periodically backup your computer data on CD / DVD or USB drive etc.. in case it may get corrupted due to HardDisk failures or when reinstalling/format ting the system.

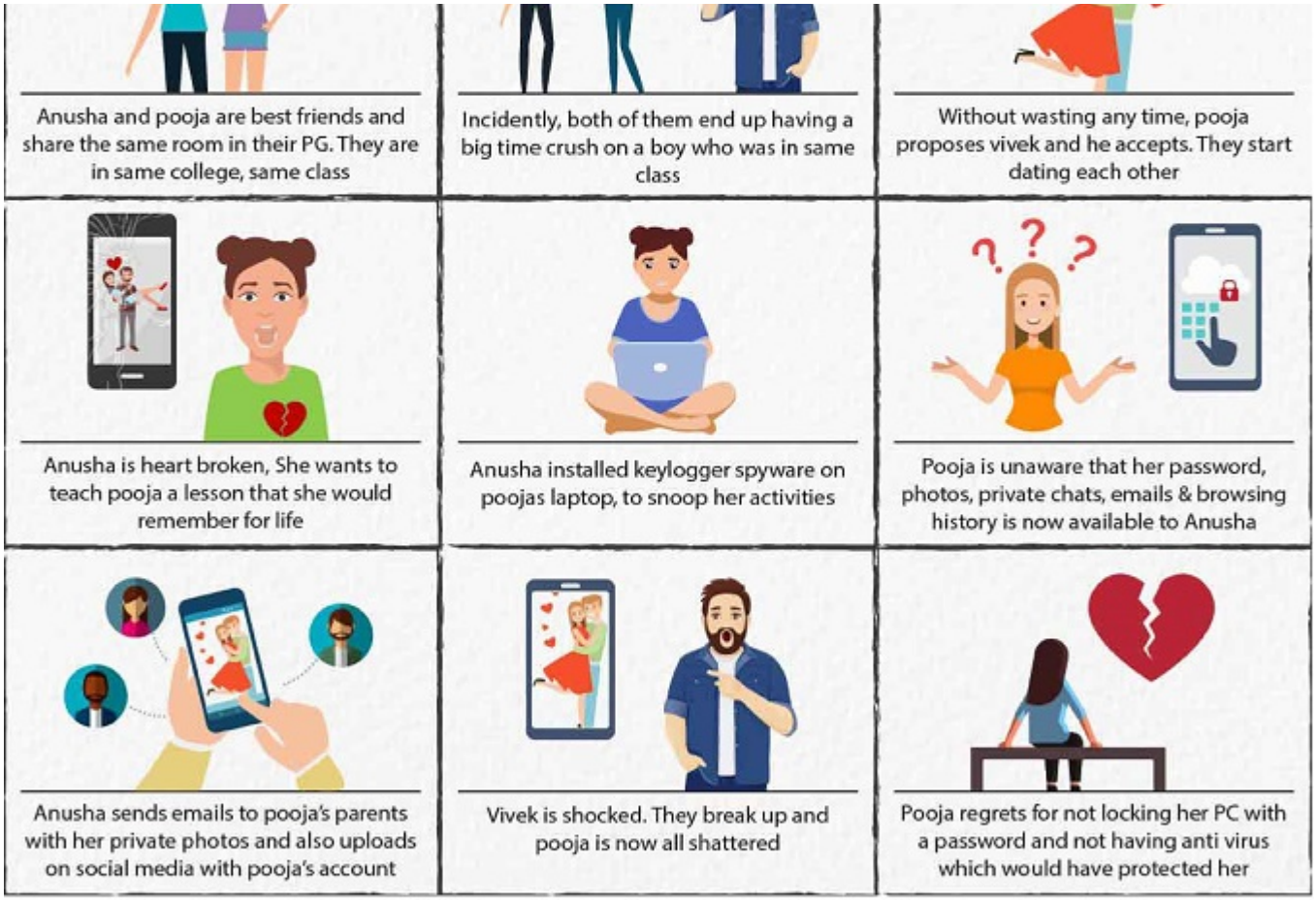
4 **Recovery Disk:** Always keep recovery disk suplied by Manufacturer / Vendor of the Computer System to recover the Operating System in the event of boot failures due to system changes such as uncerificated Drivers/unknown Software pub- lisher.

5 Strong password should be used for "Admin" Account on computer and for other important applications like E-mail client, Financial Applications (accounting etc).

6 Download Anti-Spyware Software from a Trusted Website and Install. Make sure it automatically updates with latest definitions.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in


#PIBFactCheck
This statement has not been issued by the RBI
सत्यमेव जयते
Important Message from RBI
- A very useful tip while withdrawing funds from an ATM.
- Press 'cancel' button twice before inserting the card. If anyone has set up the key pad to steal your PIN code, this will cancel
FAKE
FAKE
FAKE
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

Doki

Virus Type: Backdoor

It has been observed that a new sophisticated Linux OS based backdoor named "Doki" is spreading. The attackers are exploiting the booming cloud computing infrastructure which is usually based on Linux architecture to attack Linux systems and servers. The attackers target publically accessible Docker servers hosted with popular cloud platforms, including, AWS, Azure and Alibaba Cloud. Docker is a famous platform-as-a-service (PaaS) solution for developers to create, test and run their applications in a loosely isolated environment called container. This attack is very dangerous due to the fact the attacker uses container escape techniques to gain full control of the victim's infrastructure.

Infection Mechanism:

The attackers are abusing misconfigured Docker API ports, where attackers scan for publicly accessible Docker servers and exploit them in order to set up their own containers and execute malware on the victim's infrastructure. Doki uses a complex mechanism to contact its operator by abusing the Dogecoin cryptocurrency blockchain to generate dynamic addresses.

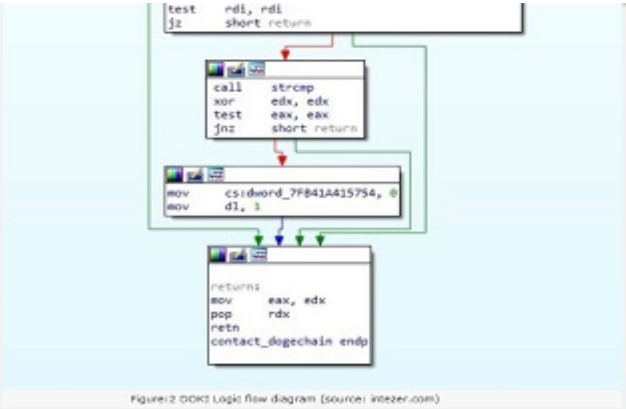


Figure:2 DOKI Logic flow diagram (source: intezer.com)

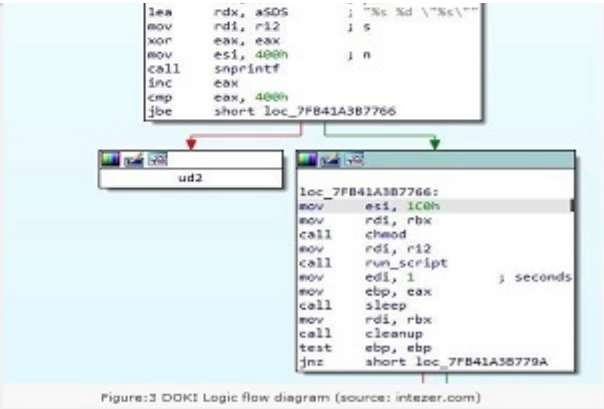


Figure:3 DOKI Logic flow diagram (source: intezer.com)

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1794

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

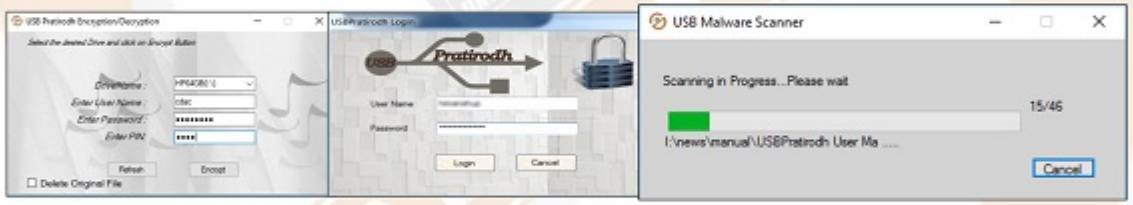
Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in), Cyber Safe Girl, I4C | Implemented by: ISEA, C-DAC

Device Control

All USB devices are uniquely identified. User can add or remove the devices to the database. User can bind one or more USB devices to be accessed using enabled username. Any unauthorized new USB device cannot be accessed, unless it is registered.

User Authentication

Whenever a USB device gets plugged in, the user is asked to authenticate with username and password. Only authenticated user can access the device. If the user fails to authenticate, user gets access denied message.



Secure Storage

Data on the USB storage devices can be encrypted.

Malware Detection

USB Pratirodh scans the plugged USB device for malware. Detected malware can be deleted by the user to keep his PC free from malware.

BENEFITS

- USB device control with password protection
- Data Encryption on USB devices
- Auto run protection and Malware Detection
- Configurable read / write privilege protection

SYSTEM REQUIREMENTS

Works with Microsoft Windows 7 and Windows 10

Download Link : www.cdac.in/usbpratirodh

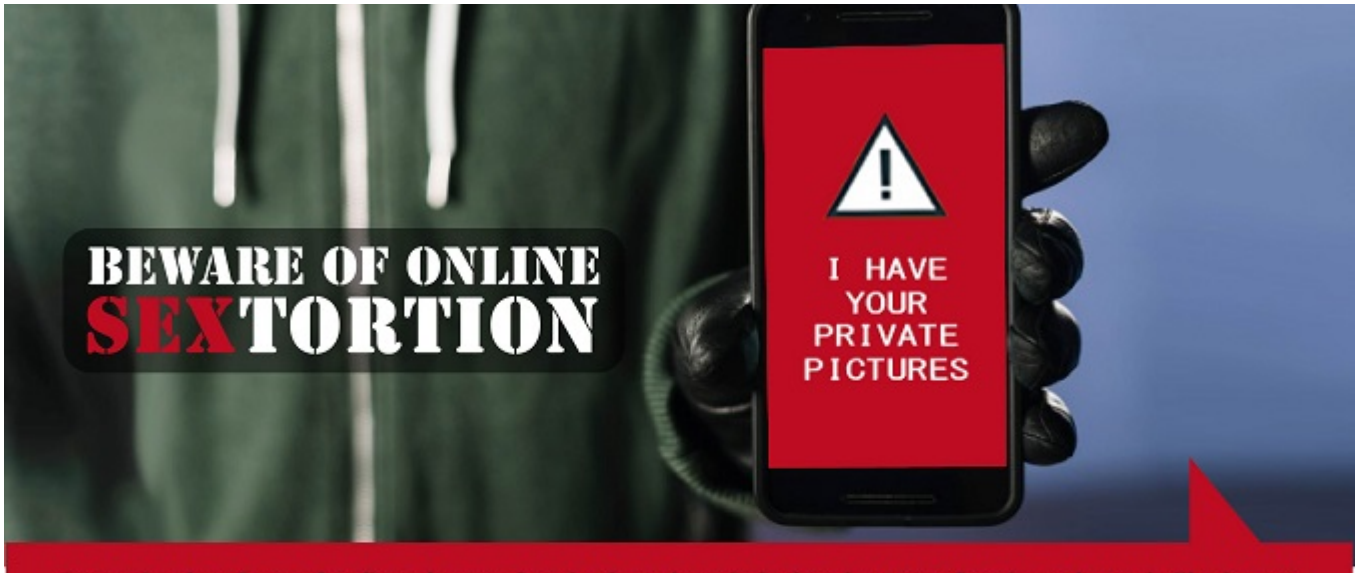
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: certin; NIC National Informatics Centre; साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in; CYBER SAFE GIRL

Implemented by: CDAC



Sextortion is a form of online abuse, wherein the cybercriminal makes use of various channels like instant messaging apps, SMS, online dating apps, social media platforms, porn sites etc., to lure the users into intimate video/audio chats and makes them pose nude or obtains revealing pictures from them. The fraudsters later make use of this material to harass, embarrass, threaten, exploit and blackmail the victims.

Online Sextortion occurs when a fraudster threatens to circulate your private and sensitive material online, if you do not provide images of a sexual nature, sexual favors, or money.

The perpetrator may also threaten to harm your friends or relatives by using information they have obtained from electronic devices unless you comply with their demands.

Dangers that victims may face

01 Blackmail

02 Abuse & Exploitation

03 Threats of public humiliation

Warning signs that may indicate victimization

Signs of fear, nervousness, anxiety, depression

Isolating self and being very reactive & emotional

Feeling desperate and frustrated

Channels used for trapping the victims

01 Messaging apps

02 Dating apps

03 Social media platforms

04 Harassment

Having suicidal thoughts and self harming behavior

04 Porn sites, etc.,

Modus Operandi:

01

The fraudsters try to lure the users into sharing intimate content in different ways:

- Posting messages for video/audio chat
- Using fake accounts/profiles
- Creating pages/ad campaigns

The users get victimized when they:

- Pay for such services and pose nude or in compromising position in video call.
- Accepts or sends friend requests to the fake account/profile and involves in intimate interaction posing nude in video chats, sends revealing pictures etc.

02

03

The fraudster records video/ takes screenshot/ takes pictures/makes use of revealing pitures/ morphs the pictures sent.

The fraudster starts blackmailing the victim leading to sextortion. The users of porn sites may also fall prey sextortion, when their chats/ video calls on the porn sites are used for blackmailing by fraudsters.

04

Advisory to safeguard yourself against online sextortion:

Never share any compromising images, posts, videos of yourself to anyone, no matter who they are.

Never pick up any calls / video calls from anonymous number.

Turn off your electronic devices and web cameras when you are not using them.

Use two factor authentication with strong passwords and different passwords for different your social media accounts.

Enable privacy and security features in all your social media accounts.

Do not suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends.

Avoid browsing the suspicious websites and websites fully which are not aware.

On social media or dating platforms, be cautious of unknown users who try to move the conversation to another interactive platform very quickly.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Stop neglect. protect before you connect"

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

USB Device Security

USB (Universal Serial Bus) storage devices are very convenient to transfer data between different computers. You can plug it into a USB port, copy your data, remove it and be on your way. Unfortunately this portability, convenience and popularity also brings different threats to your information. Data thefts and Data leakage are everyday news now! All these can be controlled or minimized with care, awareness and by using appropriate tools to secure the information. The tips and recommendations provided in this document helps you to keep your information secure while using USB storage devices.

Common Threats

- Malware Infection :Malware Spreads through USB storage devices. Somebody may intentionally sell USB storage devices with malware to track your

How to stop Data Leakage via USB storage ?

- Design and adopt a good security policy to limit the usage of USB Storage devices.
- Monitor the employees what they are copying.

activities, files, systems and networks.
- Malware may spread from one device to another device through USB Storage Devices using autorun.exe, which is by default enabled.
- Unauthorized Usage
- Somebody may steal your USB Devices for Data.

- Implement Authentication, Authoriza-tion and Accounting to secure your information.

What to do when you lose the Device?

- If you have stored any personal or sensitive information inside the USB drive like passwords etc, imediately change all passwords along with security questions and answers provided during any account creation [There may be chances that hacker can retrieve your online account logon information by using data in the stolen drive].
- Also ensure that all security measures have been taken against the data lost.

How to stop Device theft ?

- Always secure the drive physically by tagging it to a key chain.
- Never leave your drive unattended anywhere.
- Never keep sensitive information with-out encryption.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by certin NIC National Informatics Centre साइबर स्वच्छता केंद्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in CYBER SAFE GIRL

Implemented by

PIB FACT CHECK

राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022


This organisation is NOT related to the Government of India
भारतीय कौशल विकास संगठन
Indian Skill Development Organization
(Labour & Employment Department)
Head Office : Nelson Mandela Marg, Vasant Kunj, New Delhi -110067
RECRUITMENT OF SPECIALIST OFFICERS & MISLINIOUS OFFICE STAFF IN GROUP 'C' & 'D' IN VARIOUS SCALES ON REGULAR BASIS-2021
SUBMISSION OF ONLINE APPLICTION & PAYMENT OF FEES/INTIMATION CHARGES - FROM 06.08.2021 TO 25.08.2021
Indian Skill Development Organization (ISDO) invites applications from eligible candidates for appointment Of various Posts In Specialist Officers & Miscellaneous Office Staff In Group 'C' & 'D' In Various Scales.
Important Instructions:
• Candidates are advised to read all the instructions carefully and ensure to fulfil stipulated eligibility criteria as on the date of eligibility.
• The process of Registration of application is complete only when the prescribed Application Fee/Intimation Charges (wherever applicable) is deposited with the ISDO through online mode on or before the last date of fee payment.
• Candidates are provisionally admitted to shortlisting, Interview on the basis of the information furnished in the ONLINE application. Mere issue of e-Call Letter to the candidate for Interview phase will not imply that his/candidature has been finally Cleared by the Department. The Department will take up verification of eligibility criteria with reference to original documents at the time of interview (if called). If at the stage it is found the candidate is not fulfilling the eligibility criteria for post (age, caste, educational, professional qualification post-qualification, post-qualification experience etc.) his/her candidature will be cancelled and he/she will not be allowed to appear for Interview. Such Candidates are not entitled for reimbursement of any conveyance expenses.
Name of the Post: PROJECT MANAGER
No. of Posts: 72 Posts.
Vacancy : UR-32, EWS-8, SC-10, ST-6, OBC-NCL-16
SALARY: 78300-209200 & Allowances (As par 7
Position - Regular
Name of the Post: REGIONAL MANAGER
No. of Posts: 188 Posts.
Vacancy : UR-76, EWS-19, SC-29, ST-14, OBC-NCL-50
SALARY: 35400-112400 & Allowances (As par 7
Position - Regular
FAKE
FAKE
FAKE
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

ProLock Ransomware

Virus Type: Ransomware

It has been reported that a new ransomware, dubbed, "ProLock" is spreading. This is a successor of PwndLocker ransomware strain that emerged in the late 2019. The ransomware affects organizations of various sectors including government, financial, retail and heath care organizations.

Initial access and infection mechanism:

ProLock obtains the access of victim¿s network in several ways but the main vectors of initial access are: improperly configured RDP servers with weak credentials and QakBot (Qbot) Trojan. While the earlier vector is common among various malware attacks, the QakBot Trojan is one to note which is affiliated with MegaCortex ransomware and loaded via Emotet malware in erstwhile campaigns. The use of QakBot by the ProLock operators may be seen as a collaboration among threat actors to utilize the skill-set of multiple teams.

Ransom note mentions for a TOR browser downloading and use victim's user ID to pay ransom. However, as seen, the decryption key or decryptor received after paying ransom also has bug. The decryptor can potentially corrupt files that are larger than 64MB and may result in file integrity loss of approximately 1 byte per 1KB over 100MB.

QakBot also employs tactics to avoid detection. It checks for newer version of itself and replaces if found. Executables are signed with a fake or stolen signature. PowerShell downloads the initial payloads and stores it on the server with a PNG extension and it's replaced with the legitimate file calc.exe after execution. As observed, ProLock operators have not setup any website for publishing exfiltrated data in case of ransom failure.

Indicators of compromise:

Files:

- C:\ProgramData\WinMgr.bmp
- C:\ProgramData\WinMgr.xml
- C:\ProgramData\clean.bat

```
schtasks.exe /CREATE /XML C:\Programdata\WinMgr.xml /tn WinMgr
schtasks.exe /RUN /tn WinMgr
del C:\Programdata\WinMgr.xml
```

- C:\ProgramData\run.bat

```
del C:\Programdata\run.bat
```

Figure:1 Batch Script (Source: Group-IB)

Best practices for prevention:

- Users are advised to disable their RDP if not in use, if required, it should be placed behind the fire-wall and users are to bind with proper policies while using the RDP.
- Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
- All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software. Avoid applying updates / patches available in any unofficial channel.

For more details visit: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1793

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Developed in collaboration with
"**Cyber Swachhta Kendra**" under
Indian Computer Emergency Response Team
(CERT-In), Ministry of Electronics & IT.

Download Free Tool

WHAT IS A BOTNET INFECTION?

A group of computers controlled by cybercriminals to spread malware and launch other malicious attacks on their targets is called a botnet. A botnet infection is when your computer becomes a part of a botnet.

WHAT IS THE QUICK HEAL BOT REMOVAL TOOL?

This tool helps you detect and remove any botnet infection from your computer. This tool can be run with or without an antivirus program on your computer. Note that this tool only secures your computer against bots. It does not provide protection against other malware or prevent any data theft.

HOW CAN YOUR COMPUTER BE BOT-INFECTED?

Attackers can make your computer a part of their botnet by infecting it with something called a 'bot code'. They can drop this code onto your computer by sending you emails containing malicious links or attachments, fake social media posts, or exploiting existing security vulnerabilities on your system.

BENEFITS OF THE QUICK HEAL BOT REMOVAL TOOL:

- No need to install it. Simply run the tool when you need it.
- Detects and removes even the latest bot malware.
- Run it along with your existing antivirus software.
- It can be run on all Windows-based operating systems.

For more information visit
https://www.cyberswachhtakendra.gov.in/security-tools.html

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: CERT-In; NIC National Informatics Centre; साइबर स्वच्छता केंद्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in; CYBER SAFE GIRL

Implemented by: C-DAC

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Use Internet Ethically"


FAKE
The Ministry Of Education has a
distribution schedule for laptops to
be given out to families to help support
virtual learning this fall. To check
eligibility visit https://bit.ly/
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by


www.
InfoSec
awareness.in
Malware Alerts
National Cyber Security
Awareness Month
October, 2022
www.isea.gov.in
Android: BlackRock Malware
Virus Type: Android Trojan
It is reported that a new Android malware strain, dubbed "BlackRock", equipped with data stealing capabilities, is attacking a wide range of android applications. The malware is developed using the source code of Xerxes banking malware, which itself is a variant of LokiBot android Trojan.
The noteworthy feature of this malware is that the target list of applications of this malware which contains 337 applications includes not only banking and financial applications but also non-financial well

known commonly used brand name apps on android device with a focus on social, communication, networking and dating platforms. It can steal credentials and credit card information from targeted 300+ apps like email clients, e-commerce apps, virtual currency, messaging/social media apps, entertainment apps, banking, financial apps etc.

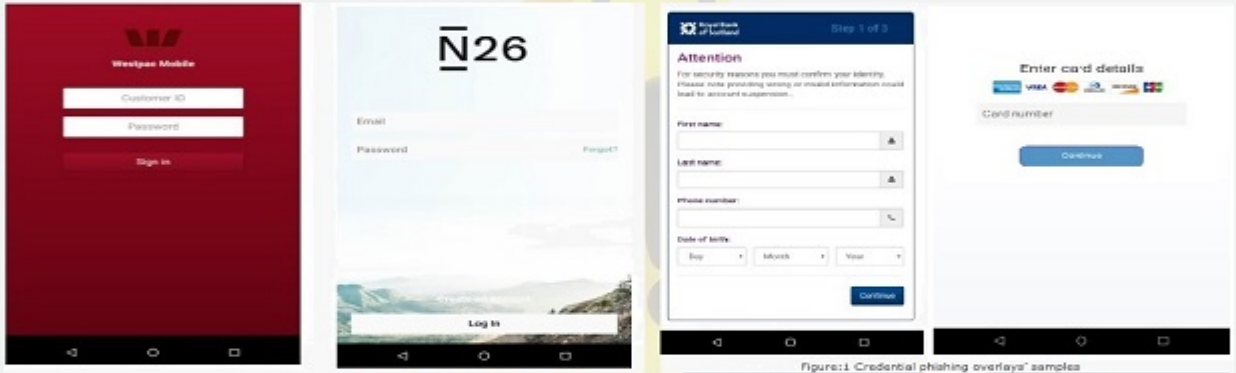


Figure:1 Credential phishing overlays' samples

Best practices for prevention:

- Do not download and install applications from untrusted sources [offered via unknown websites/ links on unscrupulous messages]. Install applications downloaded from reputed application market only.
- Install and maintain updated antivirus solution on android devices. Scan the suspected device with antivirus solutions to detect and clean infections.
- Prior to downloading / installing apps on android devices (even from Google Play Store), Always review the app details, number of downloads, user reviews, comments and "ADDITIONAL INFORMATION" section.

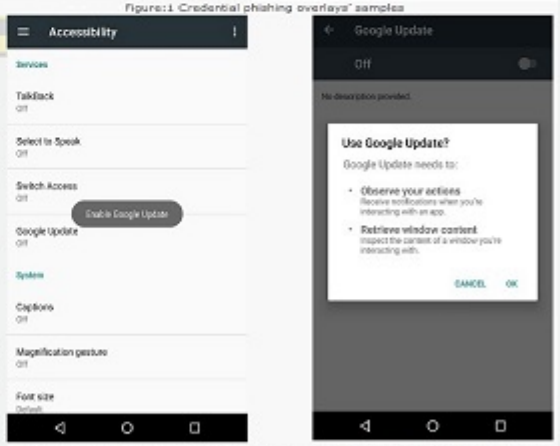


Figure:2 Trojan asking for Accessibility services privileges and posing as fake Google Update

For more details visit: https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1773

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology
Supported by: certin, Cyber Swachhta Kendra, NIC National Informatics Centre, Cyber Safe Girl, I4C
Implemented by: C-DAC, ISEA

TOOLS Awareness Month October, 2022 www.isea.gov.in

AppSamvid

Application Whitelisting Software

About AppSamvid:

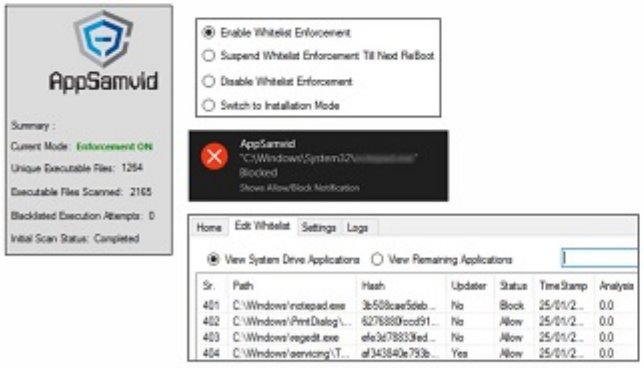
AppSamvid is application whitelisting software for Microsoft Windows based operating systems. Whitelisting allows only the pre-approved files to execute on operating system. This is in contrast to traditional signature based antivirus software approach of blacklisting the virus files. Whitelisting has the advantage over blacklisting as it does not require frequent virus definition updates. AppSamvid can work for Microsoft Windows XP SP2 and above operating systems. AppSamvid can protect operating system against computer malware (such as Viruses and Trojans).

Features:

- Whitelists executable and java files (.exe, class, .war, .jar)
- Has Installation Mode:
  - To allow updating of software
  - To allow installation and/or un-installation of software
- Folder Scan and File scan option to add executable files to database
- Password based access to user interface
- Supports operating system updating via Microsoft Updates
- Bundled with heuristic malware engine to gain confidence on which files to whitelist
- Allows files to be made as Trusted Updater
- Can identify potential updater files to help the user find which files can be made as trusted updater(s)

Supported Operating Systems

- Windows 7 (32 and 64-bit)
- Windows 10 version 1607 (32 and 64-bit)



Usage Flow


Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
certin
NIC
National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

tr> tr> tr> tr>

"Never share sensitive information to unknown on Internet: Share PII with care"

it, to keep it protected when not in use.

to patch up vulnerabilities.

Be wary of befriending strangers online who can lure you into sharing information that can be misused.

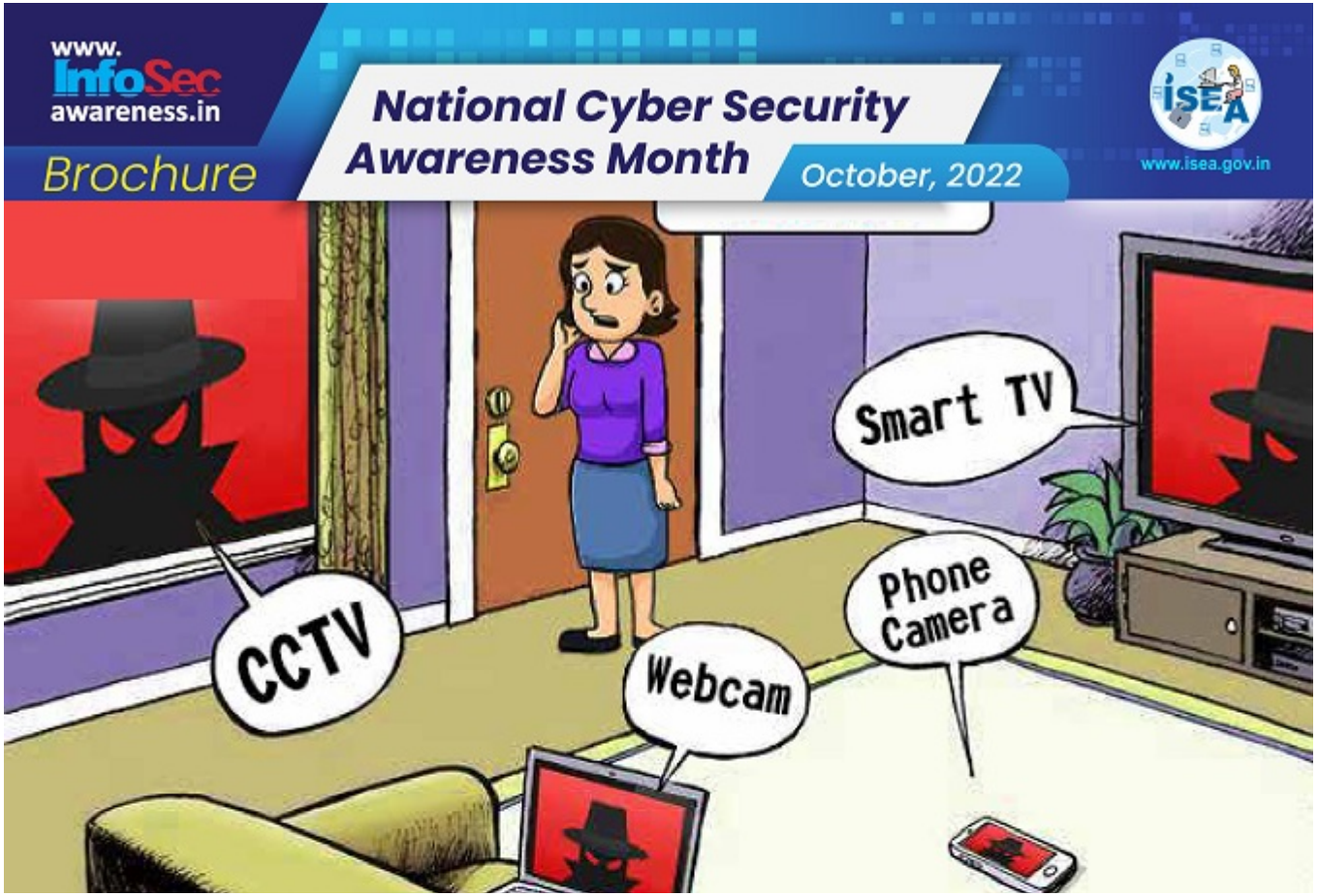
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology

Supported by: certin, CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, NIC National Informatics Centre, CYBER SAFE GIRL

Implemented by: C-DAC



CAMERA HACKING

When a fraudster hacks into a digital device and remotely takes control of the webcam, it is known as Camera hacking.

The remotely activated webcam is used by fraudster to capture pictures, record videos etc., without the knowledge of the victim. It is by infecting victim's device with a malware/virus that the fraudster gains unauthorized access and control to the webcam.

Warning Sign

- Indicator light of webcam blinking even when it is not in use

Dangers

- Capturing intimate pictures
- Unauthorized access
- Blackmail
- Uploading picture in porn sites etc.,

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology

Supported by: certin, CISO, NIC National Informatics Centre, साइबर स्वच्छता केंद्र Cyber Swachhta Kendra, www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C

Implemented by: CDAC

www.InfoSec awareness.in

Storyboard

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Be aware of Camera Hacking

Manisha is the most coolest girl in her college

She used her phone to check mails, manage social media accounts and transfer money

She used to carry her phone to washroom all the time.

She had no idea about a file downloaded by her on messenger once, which was a trojan with malware

The malware switched on front and back camera of her phone without her consent, discreetly capturing videos

Unware about the malware, Manisha kept her phone aside in the bathroom and had shower

One day her friend joel tells her that he came across her shower vedio on a porn website

Manisha is shattered, her phone did not have an antivirus installed, which protects the phone

She also regretted for not having a mobile flip cover and camera cover

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930


For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
certin
NIC
National Informatics Centre
साइबर स्वच्छता केंद्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
PIB FACT CHECK
राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022
#PIBFactCheck
केंद्र सरकार द्वारा प्रधानमंत्री रामबाण सुरक्षा नामक कोई योजना नहीं चलाई जा रही है!
Forwarded
प्रधानमंत्री रामबाण सुरक्षा योजना
जल्दी आवेदन करे
कृपया ध्यान दें
प्रधानमंत्री रामबाण सुरक्षा योजना के लिए रजिस्ट्रेशन हो रहा है, इस योजना के अंतर्गत सभी युवाओं को 4[illegible]00 रूपये की मदद राशि मिलेगी।
रजिस्ट्रेशन
करने के लिए निचे दिए गए लिंक पर क्लिक कर अपना फॉर्म भरे
ध्यान दें, आवेदन करने की अंतिम तारीख 18 अगस्त 2021 है, जल्दी करें।
फ़र्ज़ी


मुझे 4000 रूपये मिल चुके हैं, आप भी निचे दी हुई लिंक से
आवेदन प्राप्त कर लें.
आवेदन यहां से करें https://pradhanmantri
-rambaan-suraksha-yojna.blogspot.com/
संदिग्ध जानकारी यहाँ साझा करें
+918799711259
socialmedia@pib.gov.in
सोशल मीडिया पर हमें फॉलो करें
@PIBFactCheck
/PIBFactCheck
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by
www.
InfoSec
awareness.in
Malware Alerts
National Cyber Security
Awareness Month
October, 2022
www.isea.gov.in
CLOP Ransomware
Virus Type: Ransomware
It is reported that the ransomware named "CLOP" is active in attacking organizations/institutions across the globe. Post compromise this ransomware leaks information if negotiation deal of ransom fails. Recently the threat actors behind Clop have stolen and encrypted the sensitive information of various organizations and after failure of ransom payment, the stolen information was leaked on their "CLOP^_-LEAKS" data leak site, hosted on dark web. The leaked information includes data backups, financial records, thousands of emails and vouchers etc.
ClopReadMe.txt - Notepad
File Edit Format View Help
Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover
We exclusively have decryption software for your situation
No decryption software is available in the public.
DO NOT RESET OR SHUTDOWN - files may be damaged.

Figure:2 Files encrypted by Clop

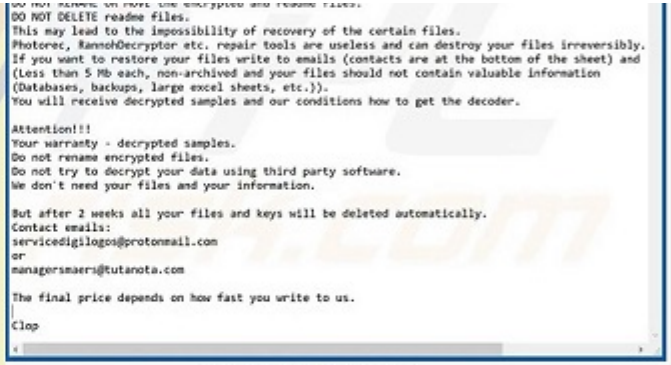


Figure:1 Clop ransomware message

Best practices for prevention:

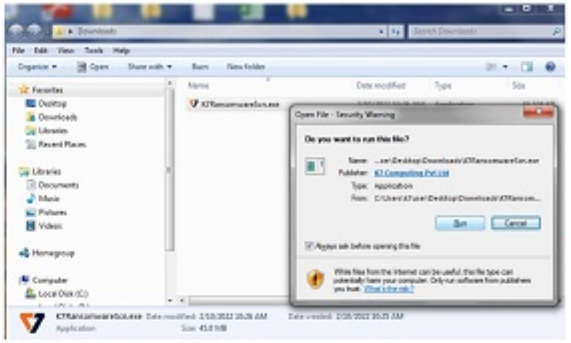
- Do not download and install applications from untrusted sources [offered via unknown websites/ links on unscrupulous messages]. Install applications downloaded from reputed application market only.
- Update software and operating systems with the latest patches. Outdated applications and operating systems are the targets of most attacks.
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
- Prohibit external FTP connections and blacklist downloads of known offensive security tools.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|-dat|hlp|hta|js|wsf
- Consider encrypting the confidential data as the ransomware generally targets common file types.

https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1753

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

The K7 Bot Removal Tool scans and removes malicious bots and prevalent ransomware variants from your computer. This is a standalone tool that can work alongside any antivirus program installed on your device. Note, this tool only targets bots and ransomware and does not defend your computer against other cyber threats. So K7 Computing recommends using a robust and certified antivirus solution that is frequently updated for comprehensive cyber safety.



What is a bot?

In general, a bot (short for robot) is a software program that performs automated, repetitive tasks without constant human intervention.

In cybersecurity parlance, individual systems that are infected by malware and controlled remotely by the attacker(s) are called a bots.

What is a botnet?

A botnet is a network of computers infected by malware. All the systems that are part of a botnet will be collectively under the control of attacker(s), who are also known as bot-master(s).
The size of a botnet can vary anywhere between hundreds to even millions of individual bots that allow the remote attacker(s) to carry out their malicious activities.

Features

Hands on learning
Practice your learning in real world environment to gain experience in working on securing digital environments and cyber assets

Industry expertise
Experience the in-depth and detailed understanding of various cyber threats, attack vectors and overall threat landscape

Real world problems
Work with scenarios and challenges faced by the real world environments in systems, servers, platforms and applications

Job aligned certifications
The course curriculum and activities are aligned to various job roles in the cybersecurity making the successful participant job ready.

Interact with professionals
Interact and learn from professionals who are working in the industry and share your queries to get role relevant clarifications

Flexible learning platforms
Available both as online and offline mode with multiple schedules to help participants choose the appropriate learning mode

For more details visit : *https://www.k7computing.com/in/*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by Supported by Implemented by


MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
cert-in
एनआईसी
National
Informatics
Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER
SAFE
GIRL

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Never connect unknown USB drives to your system"

Delete all unwanted files from device

Update your device software regularly

Always encrypt sensitive data before copying to removable devices

Monitor your active accounts regularly for any suspicious activity

Never store your personal identifiable information (PII) anywhere

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology; certin; CERT-In; NIC National Informatics Centre

Supported by: साइबर स्वच्छता केंद्र Cyber Swachhta Kendra, Botnet Cleaning and Malware Analysis Centre, www.cyberswachhtakendra.gov.in; Cyber Safe Girl; I4C

Implemented by: C-DAC

www.InfoSec awareness.in

Brochure

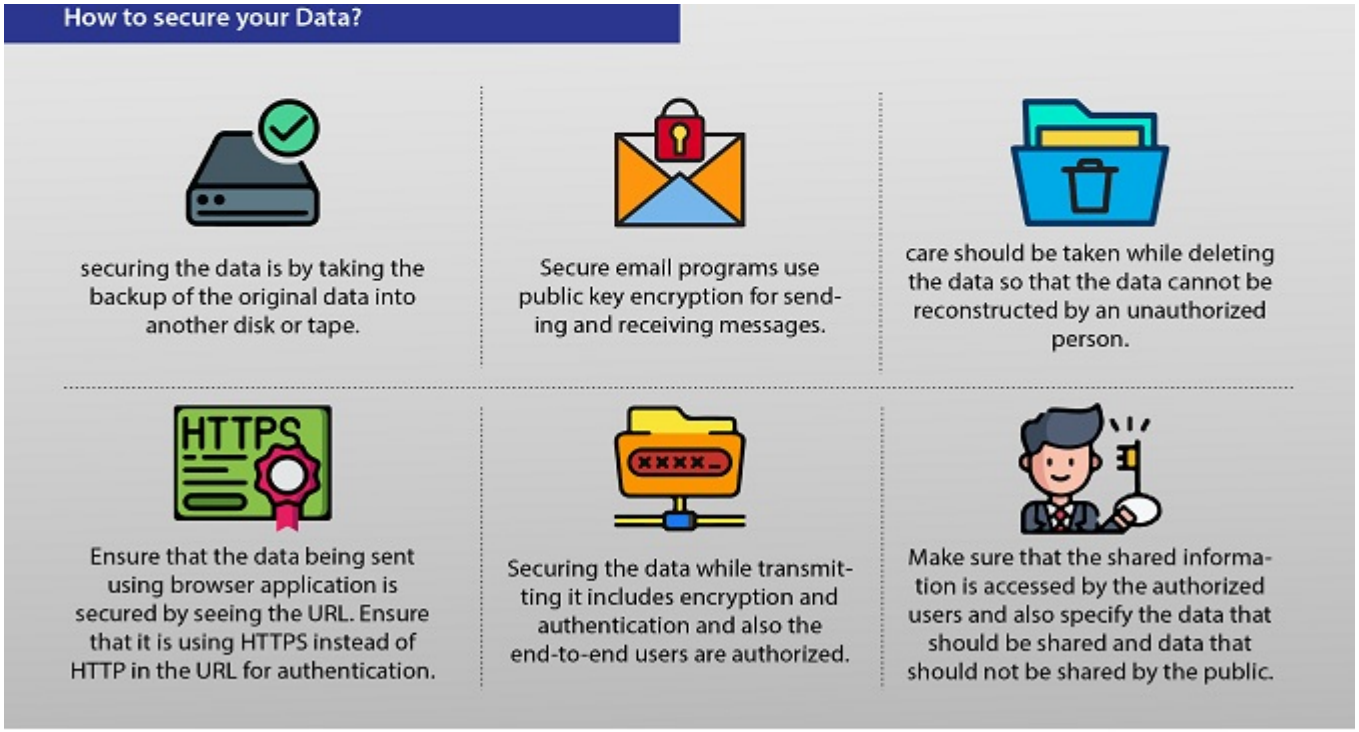
National Cyber Security Awareness Month

October, 2022

ISEA www.isea.gov.in

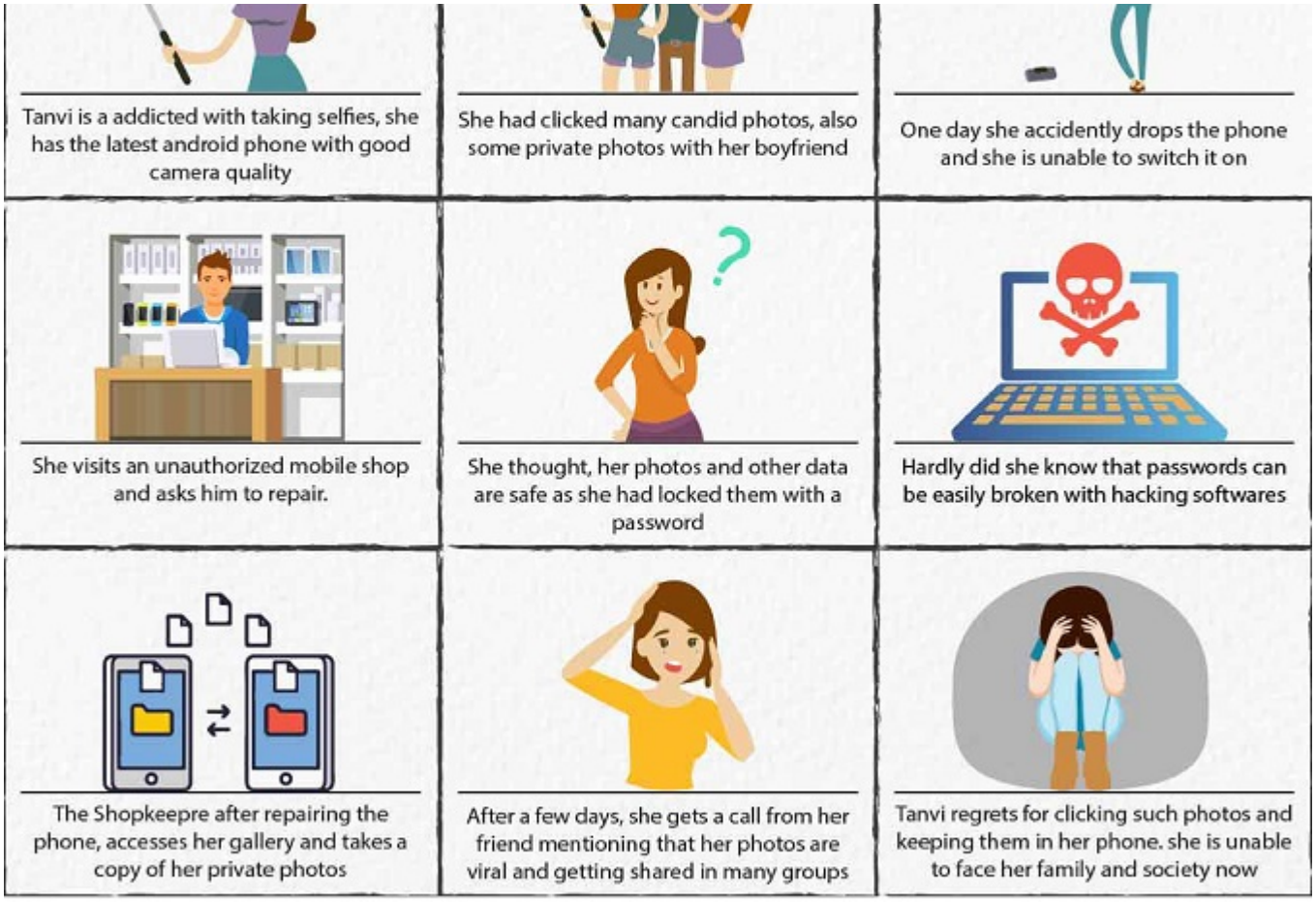
Data Security

Data Security means ensuring that the data is free from any type of fraud and the access to this data is controlled in such a way that only authorized users can access the data. Data refers to personal information regarding the individuals, bank details, etc. Data in transfer, across and between company networks, are usually the focus of extensive security efforts. However, organizations typically regard data residing on internal storage devices as secure enough. Hence, there is a need for everyone to secure the data so that it does not fall into the hands of unauthorized users.



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by certin NIC साइबर स्वच्छता केंद्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in CYBER SAFE GIRL

Implemented by

icon

राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022


FACT CHECK
Beware of Fraudsters!
pib
Hi Dear,
You are Approved for Salary from Govt Approved AYUSH Yojana of Rs.78856/
Eligiblity monthly income Rs 50k.
Check Now : d1m.in/
FAKE
FAKE
FAKE
No such scheme has been launched by Government of India
@PIBFactCheck
/PIBFactCheck
/PIBFactCheck

www.InfoSec awareness.in

Malware Alerts

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

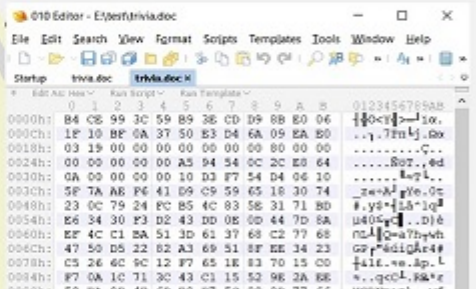
ThiefQuest Ransomware

Virus Type: Ransomware

It has been reported that a new MacOS ransomware, named "ThiefQuest ransomware" or "EvilQuest ransomware" is spreading since June 2020. This ransomware not only encrypts the files on the system but also installs a keylogger, remote shell and steals cryptocurrency wallet-related files from infected hosts. Even after ransom has been paid by the victim, the attacker continue to have access to the computer and can exfiltrate files and keystrokes. So, the attackers can carry on spying the victims.

Infection mechanism:

This ransomware is distributed via legitimate applications on torrent websites such as Little Snitch, Ableton, and Mixed in Key. After launching the installer, ThiefQuest starts encrypting files appending a BEBABEDD marker at the end. Ransomware will encrypt any files with the following file extensions of size less than 800 KB: .pdf, .doc, .jpg, .txt, .pages, .pem, .cer, .crt, .php, .py, .h, .m, .hpp, .cpp, .cs, .pl, .p, .p3, .html, .webarchive, .zip, .xsl, .xslx, .docx, .ppt, .pptx, .keynote, .js, .sqlite3, .wallet, .dat. It has been seen that it limits the number of files to be encrypted to 3000.

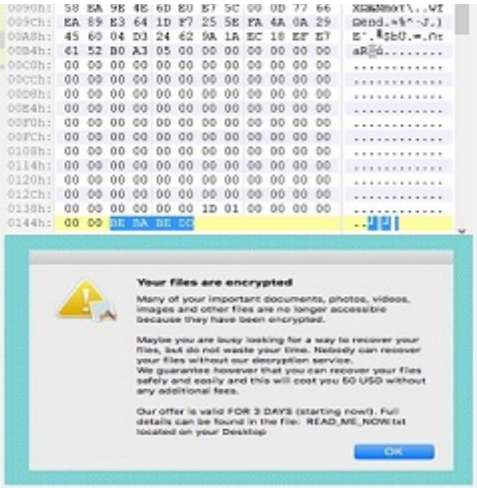


Best practices for prevention:

- Users are advised to disable their RDP if not in use, if required, it should be placed behind the firewall and users are to bind with proper policies while using the RDP.
- All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered

for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software. Avoid applying updates / patches available in any unofficial channel.

- Restrict execution of Power shell /WSCRIPT in an enterprise environment. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled. Script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis. https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html



https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1735

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: certin, CERT-In, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C | Implemented by: ISEA, C-DAC

www.InfoSecawareness.in

TOOLS

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

eScan Mobile Security for iPhones and iPads

eScan Mobile Security solution for iPhones, iPads and iPod Touch is equipped with features to activate any alarm or locate your iPhone or iPad on Map through online anti-theft portal. Using the online portal you can send alert message to the device or take photo of the user holding the device using the front camera. eScan Mobile Security for iPhone and iPad ensures safe online experience through its advanced Web Protection module that allows you to select website categories to be allowed or blocked in eScan browser. Additionally you can even take a back-up of contacts or control privacy settings for your Facebook account. It also displays the status of Location services and advises for optimizing battery usage.

Anti-theft – Find your Device after Theft/Loss

eScan Mobile Security for iPhones and iPads provides advanced anti-theft features for locating your device. If your device is lost/stolen, then you can make your device scream remotely or send any message that can be displayed on the device to improve its chance of getting back. Moreover, it allows you to take Photo of the user who is holding your device through online anti-theft portal.

Safe Surfing - Ensures Safe Online Experience

This feature helps you to select website categories to be allowed or blocked in eScan browser. For example: You can block websites categories for Porn, Child Abuse, Violence, Alcohol, Tobacco etc. and allow website categories for Education, Finance, Sports, Travel, News, Science etc.

Facebook Privacy - Protects your Privacy on Facebook

iOS Mobile Security can configure your Facebook account and control privacy settings. It detects all the privacy concerns in your account and allows you to define settings for those concerns, such as who can search you on Facebook using the phone number or email address that you have provided.

QR Code Scanner – Scans and Detects Malware URL

After the scanning process gets over, it displays the category of the scanned URL. In case it comes under Malware category, then eScan highlights it in red.
Note – eScan will not scan and Filter URL if the scanned QR code contains text along with the URL.

For more details visit : *https://www.escanav.com/en/iPhone-iPad-security/mobile-security-for-iPhones-and-iPads.asp*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: certin; NIC National Informatics Centre; साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in; CYBER SAFE GIRL

Implemented by: CDAC

www.InfoSec awareness.in

National Cyber Security Awareness Month October, 2022

ISEA www.isea.gov.in

Advisory

Advisory on Joker Malware

Infected Color Message Application

An android mobile application named Color Message infected with Joker malware is currently available for download on Google Play store and was installed by more than half a million users across the world .

The application appears to be making connections to Russian servers.

Joker is categorized as Fleeceware, as its main activity is to simulate clicks and intercept SMS to subscribe to unwanted paid premium services without the knowledge to users, Joker malware generates a very discreet footprint that can be tricky to detect.

Dangers of application

Accesses users contact list and exfiltrates it over the network.

SUBSCRIBE

The application automatically subscribes to unwanted paid premium services unknown to users.

The application has the capability to hide its icon once installed.

Stolen identity (malicious apps might abuse communication apps).

Symptoms

Device is running slowly

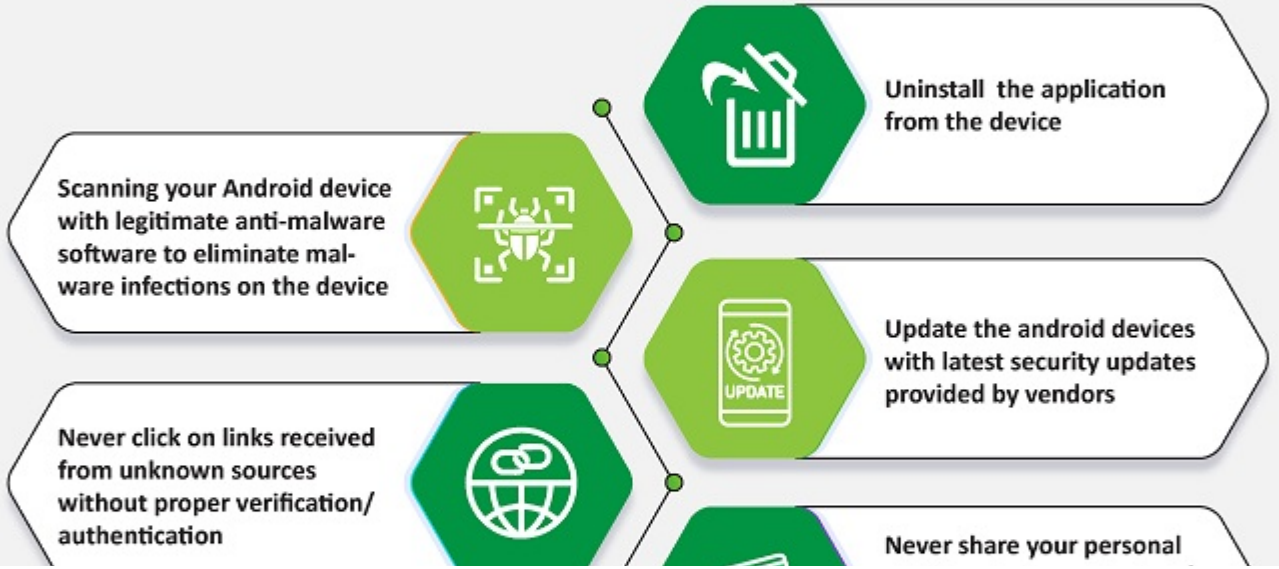
Dubious applications appear

System settings are modified without users' permission

Data and battery usage is increased significantly

Browsers redirect to rogue websites, intrusive advertisements are delivered

Advisory




details or login credentials/-passwords/credit or debit card details and other such information online .
Use a trusted anti-virus software for Mobile Security to stay safe from malware attacks.
Avoid installing mobile applications which contains advertisements


Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by


www.
InfoSec
awareness.in
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
ISEA awareness Newsletters
on IOT SECURITY

https://infosecawareness.in/newsletter/edition1-2022

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Security is not an option but a priority"

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

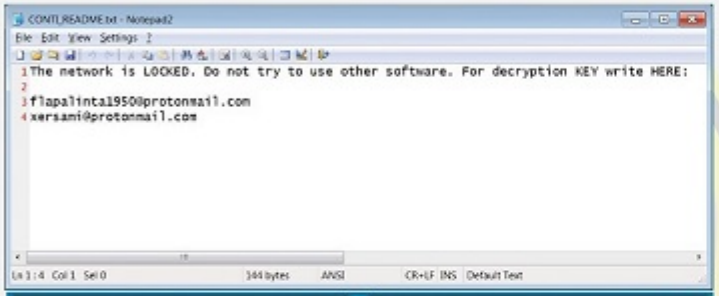
For more information visit: www.isea.gov.in and www.infosecawareness.in

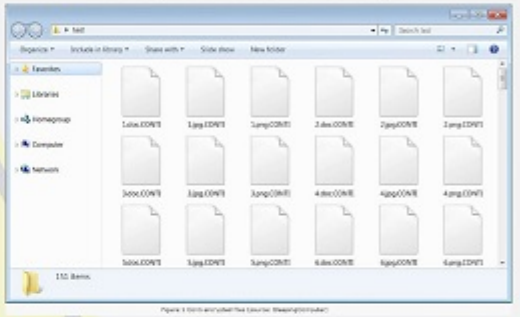
Conti Ransomware

Virus Type: Ransomware

It has been reported that a new ransomware, named "Conti ransomware" is spreading. In its infection stages, threat actors breach the corporate networks and spread laterally to acquire domain administration privilege for deploying ransomware. The coding pattern of Conti appears similar to erstwhile "Ryuk ransomware" version 2 and ransomware note used is also same as Ryuk had dropped in its earlier attacks. Moreover, the same TrickBot infrastructure is utilized by both Ryuk and Conti threat actors as part attacking mechanism. Conti is a human-operated ransomware designed to be directly controlled

by its operator rather than execute automatically by itself.





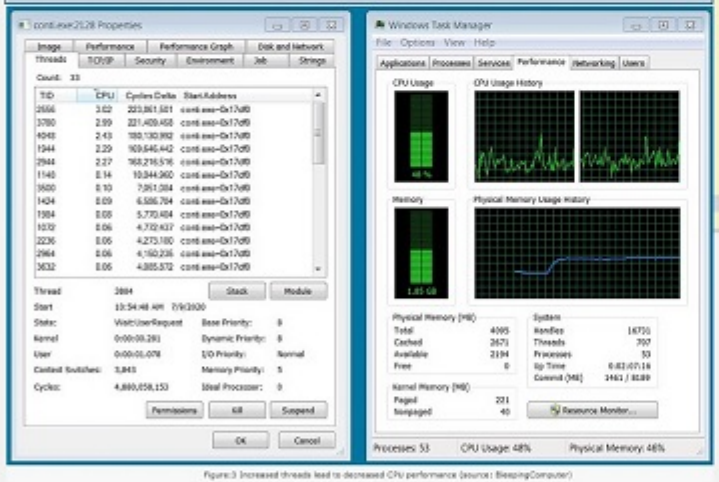


Figure:3 Increased threads lead to decreased CPU performance (source: BleepingComputer)

Best practices for prevention:

- Users are advised to disable their RDP if not in use, if required, it should be placed behind the firewall and users are to bind with proper policies while using the RDP.
- All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software. Avoid applying updates / patches available in any unofficial channel.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|-dat|hlp|hta|js|wsf.

https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1734

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

TOOLS Awareness Month October, 2022 www.isea.gov.in

Malwarebytes

Malwarebytes' Anti-Malware is a malware scanner for Windows. The authors claim to use a variety of technologies to find malware undetectable by other malware scanners. There is a free trial with limited options and a supported full version with the ability to run scheduled scan.

<u>If your computer has gotten a virus or malware infection, there are some telltale signs, including:</u>

- Slow: Your computer slows down significantly.
- Pop-ups: You have started to see a lot of unexpected pop-ups.
- System crashing: Your system unexpectedly crashes, either by freezing or by giving you a blue screen (also known as a Blue Screen of Death or BSOD).
- Loss of disk space: A lot of your device's storage has been taken up unexpectedly.
- Settings changed: Device or browser settings change without you changing them.
- Files encrypted: Ransomware has locked you out of your files or your entire computer.

You can scan and remove malware and viruses from your device with Malwarebytes Free. Download it now to detect and remove all kinds of malware like viruses, spyware, and other advanced threats. To keep your device protected after your initial malware scan and removal, we recommend Malwarebytes Premium for Windows and Mac, and our mobile security apps on Android and iOS.

Malwarebytes security software has multiple layers of malware-crushing tech, including virus protection. Traditional antivirus alone is no longer sufficient against today's sophisticated malware threats. Malwarebytes prevents threats in real-time, crushes ransomware, defends against harmful sites, and cleans and removes malware. Go beyond antivirus and stop worrying about online threats.

For more details visit : ***https://sectools.org/tool/malwarebytes/***


Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
certin
NIC
National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Always take backups of your important files"

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

- Maintain appropriate Firewall policies to block malicious traffic entering the system/network. Enable a personal firewall on workstation.
- Keep updated Antivirus/Antimalware software to detect any threat before it infects the system/network. Always scan the external drives/removable devices before use. Leverage anti-phishing solutions that help protect credentials and against malicious file downloads.
- It is also important to keep web filtering tools updated.
- Block the IP addresses of known malicious sites to prevent devices from being able to access them. Activate intelligent website blacklisting to block known bad websites.
- Use limited privilege user on the computer or allow administrative access to systems with special administrative accounts for administrators.
- Block websites hosting JavaScript miners both at the gateway and the endpoints.
- Keep software and OS up-to-date so that attackers may not take advantages of or exploit known vulnerabilities.
- Change default login credentials as they are readily available with attackers.
- Avoid downloading files from untrusted websites.
- Go beyond intrusion detection to protect servers with runtime memory protection

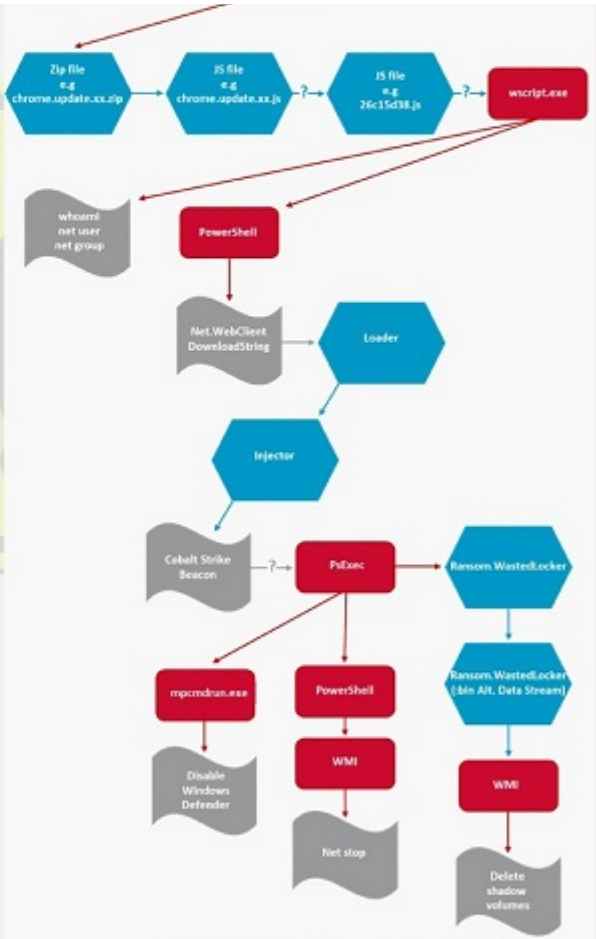


Figure:1 WastedLocker attack chain (source: Symantec)

https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1733

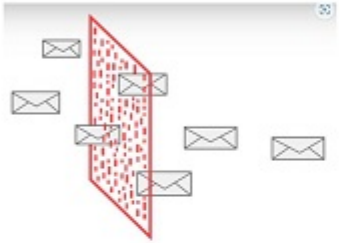
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

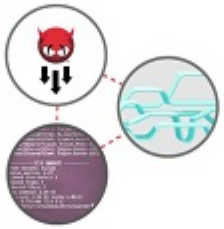
For more information visit: www.isea.gov.in and www.infosecawareness.in

TOOLS Awareness Month October, 2022 www.isea.gov.in

ClamAV

ClamAV is a powerful Antivirus scanner focused towards integration with mail servers for attachment scanning. It provides a flexible and scalable multi-threaded daemon, a command line scanner, and a tool for automatic updating via the Internet. Clam Antivirus is based on a shared library distributed with the Clam Antivirus package, which you can use with your own software. Most importantly, the virus database is kept up to date.





The Standard
ClamAV® is the open-source standard for mail gateway-scanning software.

High Performance
ClamAV includes a multi-threaded scanner daemon, command-line utilities for on-demand file scanning and automatic signature updates.

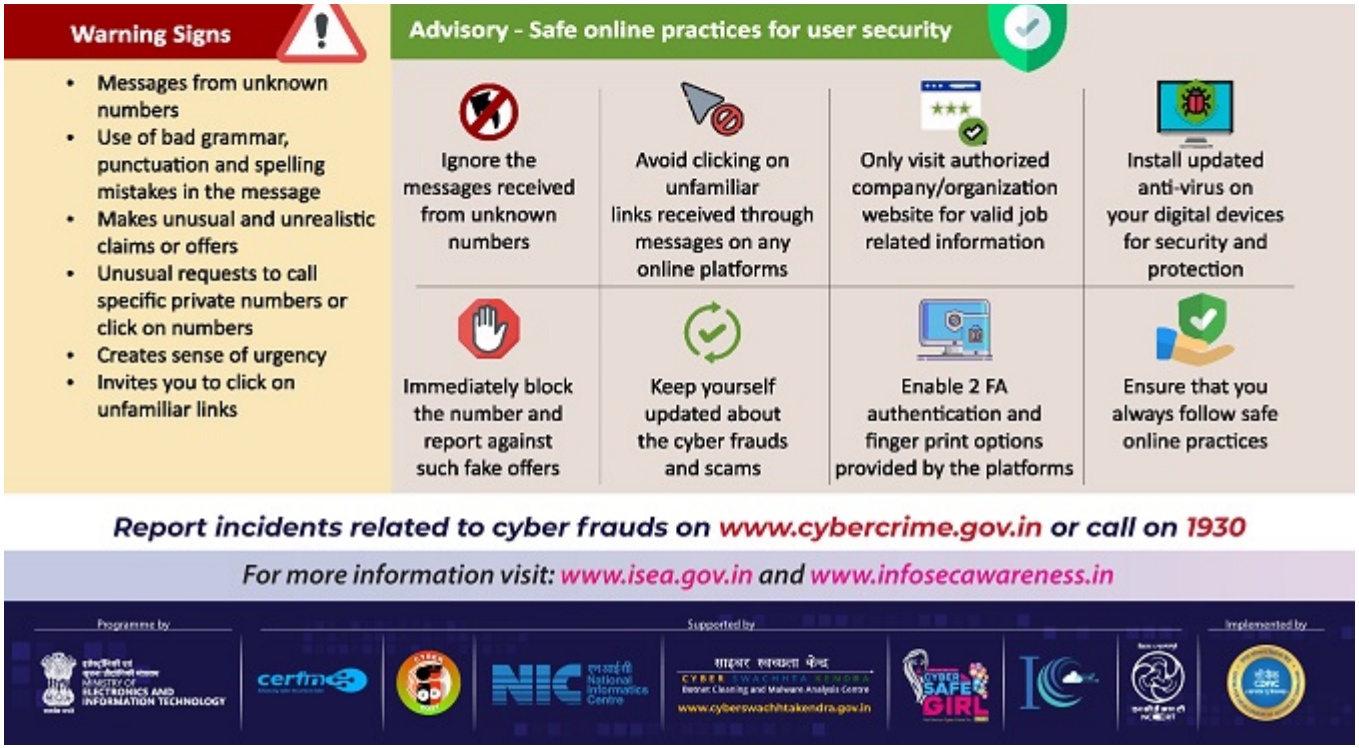
Versatile
ClamAV supports multiple file formats and signature languages, as well as file and archive unpacking.

Features

- ClamAV is designed to scan files quickly.
- Real time protection (Linux only). The ClamOnAcc client for the ClamD scanning daemon provides on-access scanning on modern versions of Linux. This includes an optional capability to block file access until a file has been scanned (on-access prevention).
- ClamAV detects millions of viruses, worms, trojans, and other malware, including Microsoft Office macro viruses, mobile malware, and other threats.
- ClamAV's bytecode signature runtime, powered by either LLVM or our custom bytecode interpreter, allows the ClamAV signature writers to create and distribute very complex detection routines and remotely enhance the scanner's functionality.

For more details visit : *https://sectools.org/tool/clamav/*


Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
certin
NIC National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by
www.InfoSec awareness.in
Advisory
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
Be Alert
Do not fall for Fake Job Offers
JOB
About free Job Scams
During these critical COVID times, cyber fraudsters are misusing people's interest in Work from Home (WFH) opportunities and sending the fake job offers related messages on WhatsApp. Through these fake messages they try to victimize the users by sending them malicious phishing links and attempt to commit financial frauds.
SCAM
Dangers
Capture user credentials
Gain access to sensitive user data (banking information, PINs, Passwords etc.,)
Redirect to false websites and false contact numbers
Commit financial fraud
the job is yours !!!
Gain unauthorized access to applications
Modus Operandi
The fraudsters send fake messages with malicious/fake links
SPAM
Clicking on the link the user may download malicious software or fake account login page/mobile numbers
The victim may lose money, access to their account, give unauthorized access to their device and sensitive data.

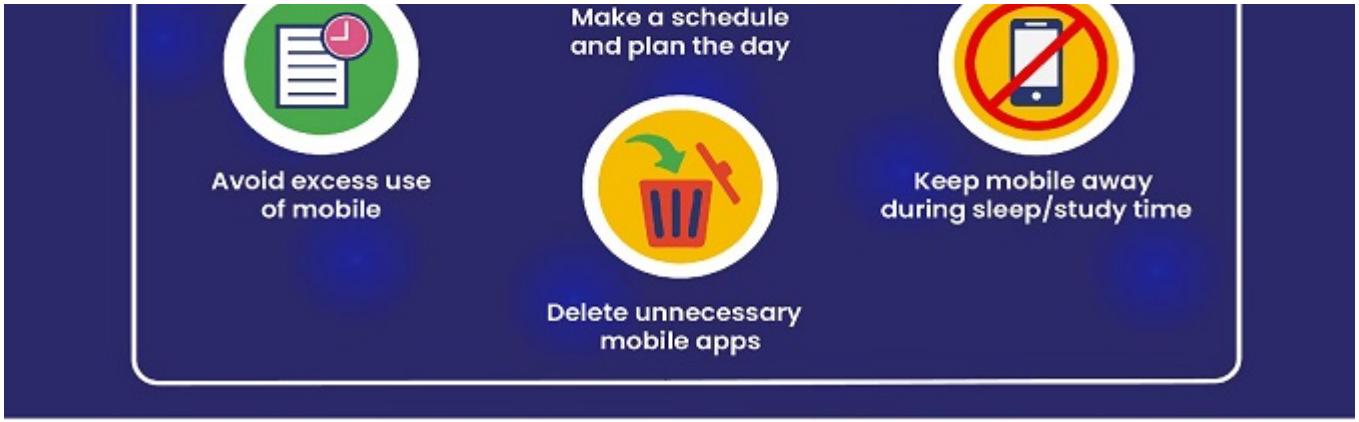

Warning Signs
Messages from unknown numbers
Use of bad grammar, punctuation and spelling mistakes in the message
Makes unusual and unrealistic claims or offers
Unusual requests to call specific private numbers or click on numbers
Creates sense of urgency
Invites you to click on unfamiliar links
Advisory - Safe online practices for user security
Ignore the messages received from unknown numbers
Avoid clicking on unfamiliar links received through messages on any online platforms
Only visit authorized company/organization website for valid job related information
Install updated anti-virus on your digital devices for security and protection
Immediately block the number and report against such fake offers
Keep yourself updated about the cyber frauds and scams
Enable 2 FA authentication and finger print options provided by the platforms
Ensure that you always follow safe online practices
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Never open email from unknown persons: Be Phish-aware"



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Warning signs or Symptoms of Digital Addiction:

As identified by mental health experts, the reasons behind internet addiction include –

Behavioral symptoms

- Spending most of the time online
- No longer interested in real time activities/ hobbies
- Skipping daily routine and negligent grooming, to keep up with online activity
- Using mobile devices during wake up and bed time
- Agitation when not accessing digital devices
- Lying about your internet use
- Inability to Prioritize or Keep Schedules
- Time drain

Mental symptoms of internet addiction:

- Poor concentration
- Attention Deficit disorders
- Anxiety and Depression
- Language issues in children
- Trouble distinguishing reality from fantasy
- Memory impairment
- Agitation and Mood swings

Physical Symptoms

- Fatigue
- Insomnia
- Bodily discomfort like backaches, headaches, muscle pain, Carpal tunnel syndrome, eye strain etc.,
- Unintended weight loss or weight gain

Social symptoms of internet addiction:

- Irritable mood
- Social isolation and lonliness
- Employment problems
- Strained interpersonal relationships
- Academic difficulty

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: cert-in, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra, www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C | Implemented by: CDAC

www.InfoSec awareness.in

Storyboard

National Cyber Security Awareness Month

October, 2022

ISEA www.isea.gov.in

Limit the time you spend on Internet

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology

Supported by: certin, Cyber Swachhta Kendra, NIC National Informatics Centre, www.cyberswachhtakendra.gov.in, Cyber Safe Girl

Implemented by

icon


PIB FACT CHECK
राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022
#PIBFactCheck
भारत सरकार का इस प्रकार की लॉटरी से कोई संबंध नहीं है!
सभी भारतीय सिम कार्ड व्हाट्सएप आईएमओ लड्डी इंडिया टेलीकम्यूनिकेशन
KBC
अनुरोध प्रिय ग्राहक तुम्हारा जीवन अच्छा है कि आप 25,00,000 / - का भुगतान कर सकते हैं, केबीसी JIO विभाग द्वारा कंपनी की राशि और विनियमों का पूरी तरह से उपयोग करके अपने भुगतान को कम करें।
भाग्यशाली दो धारक का नाम
अमिताभ बच्चन ,मुकेश अम्बानी,नरेंद्र मोदी
Namaskar Aap Ke Liye Good News Hai Aap Ke Number Par Lottery Laga Hai 25,00,000/- Lakh Rupee Ka Apko Wadhai Ho Ye Lottery KBC,Jio Department Ki Tarf Se Lagi Hai. Kripiya Kar Ke Company Ke Rule's Ko Samjhna Hoga,
Jin Logon Ne Lucky Draw Karwaya Hai Un ke
Amitabh Bachchan,Mukesh Ambani and
Only Whatsapp
975896396
Lottery No
5580
2021
फेक

Thanos Ransomware

Virus Type: Ransomware

It has been reported that a new ransomware-as-a-service (RaaS) tool, called "Thanos" which provides buyers and affiliatesa customization tool to build unique payloads, is spreading and gaining popularity among various underground forums and channels. This ransomware family employs the RIPlace tactics majorly used to bypass the anti-ransomware endpoint security.

Thanosransomware primarily delivered via phishing emails. The attack campaign attracts the user with luring financial information like tax-refund details, invoice scheme etc. Upon launch the ransomware tries to terminate various security processes and system utilities to ensure thorough encryption.

Encryption strategy:

Thanos¿ encryption technique varies with the evolution of its payloads. While encrypting, Thanos uses a random, 32-byte string generated at runtime as a passphrase for the AES file encryption. The string is then encrypted with the ransomware operator¿s public key and without the corresponding private key, recovering the encrypted files is extremely difficult / impossible.

However, the Thanos builder also provide feature to use a static password for the AES file encryption. In this optionchosen, AES password used to encrypt filesand if aThanos client is recovered after the encryption has occurred then there is a chance of files recovery without paying ransom.

Best practices for prevention:

- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization¿s website directly through browser.
- Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
- Prohibit external FTP connections and blacklist downloads of known offensive security tools.
- All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software. Avoid applying updates / patches available in any unofficial channel.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|-dat|hlp|hta|js|wsf
- Consider encrypting the confidential data as the ransomware generally targets common file types.

https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1713

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

antivirus engines from different vendors, updated regularly with new signatures. Participating antivirus vendors can get alerts when a file is not detected by their product but is by someone else's.

VT Enterprise

Get smarter, be safer, outsmart attackers. VT Enterprise provides the information your security team needs to protect your network from threats. You have the team, you have the data, you lack the context. A multi-component web platform that provides lightning fast answers to profile your adversaries and discover badness.

Search VirusTotal's dataset for malware samples, URLs, domains and IP addresses according to binary properties, antivirus detection verdicts, static features, behavior patterns such as communication with specific hosts or IP addresses, submission metadata and many other notions. Pinpoint files similar to your suspect being studied. Samples matching search criteria can be downloaded for further study.

Powerful search tools

Clustering and similarity search capabilities.
Search for similar files using several hashes/algorithms: ssdeep content similarity searches, imphash, icon visual similarity and our own in-house structural feature hash.

Content searching
Low latency searches for random binary patterns contained within files, not only strings search but any kind of binary sequence, powered by a 5 petabyte n-gram index.

Elastic searching
Over 40 search modifiers can be used to hunt down malware samples of interest based on static, dynamic and relational properties. Example: type:dmg AND signature: "T8RS3R6DT4" AND metadata:"adharma" AND behaviour:"pkill -9 -i Flash Update 13.6 Installer" AND (behaviour:"rp.wacadacaw.com" OR behaviour:"os.wacadacaw.com")

Combine any number of modifiers
Search parameters can be combined in order to identify files that match highly complex criteria, filtering noise and focusing on threats that are relevant to your investigations.

For more details visit : *https://sectools.org/tool/virustotal/*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Devices locking is as important as Premises Locking"

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Browser Security

What is Web Browser ??

Web browser is used to access the information and resources on the World Wide Web. It is a software application used to trace and display the web pages .The main purpose of a web browser is to bring the information resources to the user. An information resource is identified by a Uniform Resource Identifier/Locator (URI/URL) and may be a web page, image, video or other piece of content. Web browsers are used not only on the personal computers, laptops but are also used on mobile phones to access the information.

Tips:

- Always use the secured web browser to avoid the risks. Using secure browser we can gain access the information and resources that are available on the Internet and can have safe

browsing over Internet.

- To avoid your PC being compromised and becoming a weapon to attack other machines, web browser and the Internet users are advised to: ensure that your operating system and key system components such as the web browser is fully patched and up to date.
- Install a personal firewall along with anti-virus software with the latest virus signatures that can detect malware such as key loggers.
- Regularly change your passwords with the combinations of letters, numbers and special case characters in critical web applications if a one-time password system is not supported.
- Turn off all JavaScript or ActiveX support in your web browser before you visit any unknown websites.
- Most vendors give you the option to download their browsers directly from their websites. Make sure to verify the authenticity of the site before downloading any files.
- To additional minimize risk; follow the latest good security practices, like using a personal firewall, Updating to the latest browser with security patches installed and keeping anti-virus software up to date with regular scanning the entire system.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: certin, NIC National Informatics Centre, साइबर स्वच्छता केंद्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, CYBER SAFE GIRL

Implemented by

PIB FACT CHECK

राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022


Date: 28.07.2022
This is NOT the official account of the President of India
Follow
Draupadi Murmu
@DraupadiMurmu12
Draupadi Murmu President of India
Proud to sanatani hindu
Translate bio
Joined April 2018
1,155 Following
34.2K Followers
FAKE
FAKE
FAKE
FAKE
#PIBFactCheck
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

Lucifer Malware

Virus Type: crypto-jacking Malware

It has been reported that a new self-propagating malware, dubbed "Lucifer", targeting Windows systems with crypto-jacking and DDoS attacks is spreading. The latest variant of this malware was discovered recently related to exploitation of vulnerability in Laravel Framework (CVE-2019-9081) that can be leveraged for remote code execution (RCE) attacks. Reports indicate that this malware utilizes an exhaustive list of unpatched critical vulnerabilities. While the patches of all critical and highly severe vulnerabilities are available but the systems affected by Lucifer malware have not been applied upon with those patches.

The vulnerabilities exploited by Lucifer includes affect Rejetto HTTP File Server (CVE-2014-6287), Oracle Weblogic (CVE-2017-10271), ThinkPHP RCE (CVE-2018-20062), Apache Struts (CVE-2017-9791), Laravel framework CVE-2019-9081), and Microsoft Windows (CVE-2017-0144, CVE-2017-0145, and CVE-2017-8464) and some others depending on which version of the malware is in role.

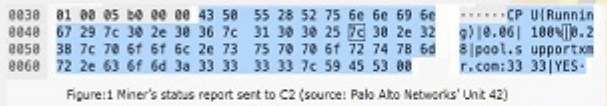


Figure:1 Miner's status report sent to C2 (source: Palo Alto Networks' Unit 42)

Figure:3 EternalBlue and DoublePulsar combo for XP targets (source: Palo Alto Networks' Unit 42)

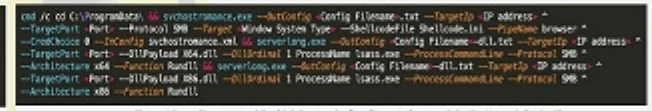


Figure:4 EternalRomance and DoublePulsar combo for all targets (source: Palo Alto Networks' Unit 42)

The malware scans open TCP ports 135(RPC) and 1433(MSSQL) and if found open, it launches brute-force attack to obtain access. In addition to this, the malware leverages exploitation for self-propagation. If SMB protocol is open, Lucifer executes several backdoors including the EternalBlue, EternalRomance, and DoublePulsar exploits to establish persistence. It also tampers registry to sched-

ule itself as a task at startup.

Best practices for prevention:

- Keep software and OS up-to-date so that attackers may not take advantages of or exploit known vulnerabilities.
- Keep updated Antivirus/Antimalware software to detect any threat before it infects the system/network. Always scan the external drives/removable devices before use. Leverage anti-phishing solutions that help protect credentials and against malicious file downloads.
- It is also important to keep web filtering tools updated.
- Change default login credentials as they are readily available with attackers.
- Use limited privilege user on the computer or allow administrative access to systems with special administrative accounts for administrators.

https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1714

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | cert-in | NIC National Informatics Centre

Supported by: साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra, Botnet Cleaning and Malware Analysis Centre, www.cyberswachhtakendra.gov.in | Cyber Safe Girl | I4C

Implemented by: C-DAC

www.InfoSec awareness.in

TOOLS

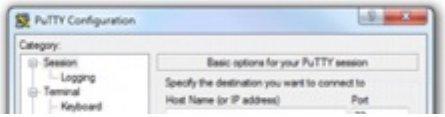
National Cyber Security Awareness Month

October, 2022

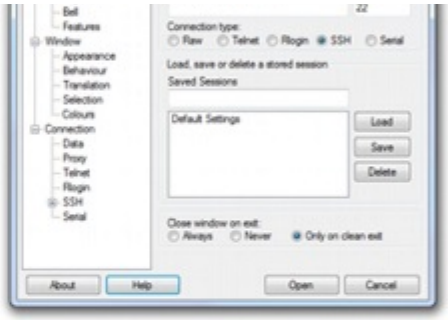
ISEA www.isea.gov.in

OpenSSH/PuTTY/SSH

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and open source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general-purpose cryptography library. Apart from being a component of many crypto programs, OpenSSL comes with a lot of command-line tools for encryption, hashing,



certificate handling, and more.



The OpenSSH suite consists of the following tools:

- Remote operations are done using ssh, scp, and sftp.
- Key management with ssh-add, ssh-keysign, ssh-keyscan, and ssh-keygen.
- The service side consists of sshd, sftp-server, and ssh-agent.

The following is a list of OpenSSH features:

- Completely open source project with free licensing
- Strong cryptography (AES, ChaCha20, RSA, ECDSA, Ed25519...)
- X11 forwarding (which also encrypts X Window System traffic)
- Port forwarding (encrypted channels for legacy protocols)
- Strong authentication (public keys, one-time passwords)
- OpenSSH extends the original SSH agent protocol to offer some path-based restrictions over the use of keys.
- Interoperability between implementations is a goal, but not a promise. As OpenSSH development progresses, older protocols, ciphers, key types and other options that have known weaknesses are routinely disabled. Some examples can be found on the legacy page.
- Complete SFTP support is included, using the sftp(1) command as a client and sftp-server(8) subsystem as a server.
- Data compression before encryption improves the performance for slow network links.

For more details visit : *https://sectools.org/tool/ssh/*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Fraud Alert

Be Aware of the KYC Scam

Targeting the Online Banking Customers

Fake SMS(s) are being circulated, to the banking customers alerting them about the account suspension/block due to pending KYC renewal/update. The fraudsters provide phishing link or fake contact numbers in the message for KYC renewal/update to commit financial scam.

In view of the COVID-19 pandemic, some banks have provided their customers, the facility of updating their KYC online or by post. Taking undue advantage of this provision, the fraudsters are sending fake SMS /text message by pretending to be a bank representative to get your personal details. The fraudsters provide the customers with the phishing link and/or 10 digit mobile number, through which they intend to get hold of customer's personal details to get unauthorized access to their banking accounts to steal money.

Dangers

Unauthorized access to account/device/data

Misuse of the personal information

Identity theft

Loss of amount

Modus Operandi

Message sent from a mobile number with a phishing link and/or 10 digit mobile number,

Upon clicking the link provided in the message, the victim is redirected to the spoofed website and prompted to enter

Or

Upon calling the number provided in the message, the victim is provoked to share personal details like account user name,

The fraudster makes use of these details to gain unauthorized access to the victim's bank account to commit fraud

for update of KYC.

the bank user name, password, OTP etc

password, account number, OTP etc.,

Warning Signs

Poor grammar, punctuation and unwanted capitalization of words in the message received.

Message sent from a mobile number instead of the authorized banking customer care / service number.

Advisory

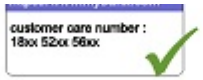
Never click on unknown links or links received from unverified sources.

Always remember that a bank never sends any links to its customers, for updating KYC.

A valid customer care number can never be a 10 digit mobile number as generally given in the fake message.

Never share your mobile number, account number, password, OTP, PIN or any other confidential details with anyone.

Any authorized bank or customer service never asks its customers to share any confidential information



Avoid contacting the customer service/contact numbers provided on Google search. Only contact the authorized numbers provided in original banking websites.

In case of any such issues immediately report to the specific bank authorities immediately.

File an online complaint regarding any such frauds on the government portal www.cybercrime.gov.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology

Supported by: CERT-In; NIC National Informatics Centre; साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) www.cyberswachhtakendra.gov.in; Cyber Safe Girl

Implemented by: I4C

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

"Be careful while using open Wi-Fi Hotspots"

Personal Information in password makes it a weak password	Regularly change and avoid repeating the password	Keep your passwords as secret even from your family members	Create personalized pass phrases as Password following password creation criteria

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: certin, CyberSwachhta Kendra, NIC, Cyber Safe Girl | Implemented by: ISEA

www.InfoSecawareness.in

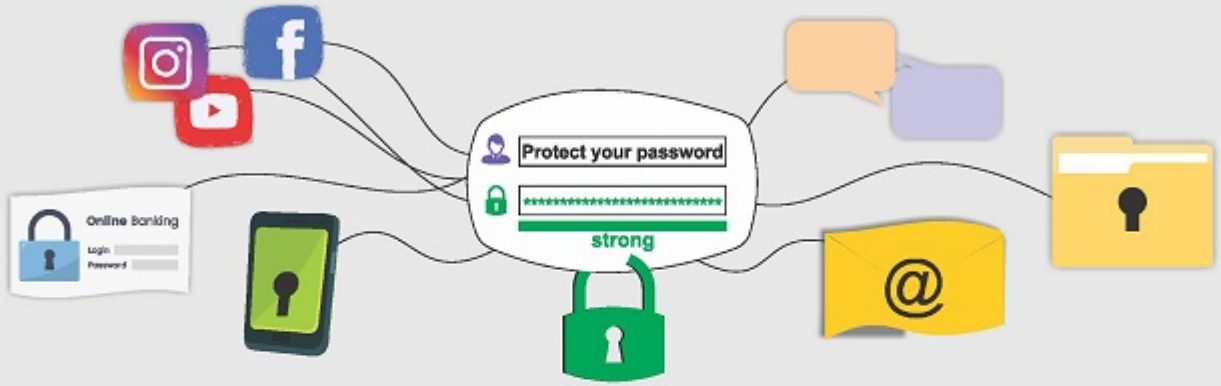
Brochure

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

PROTECT YOUR PASSWORD



Things to be remembered while creating Strong Passwords

- Use at least 8 characters or more to create a password. The more number of characters we use, the more secure is our password.
- Use various combinations of characters while creating a password. For example, create a password consisting of a combination of lowercase,
- uppercase, numbers and special characters etc..
- Avoid using the words from dictionary. They can be cracked easily.
- Create a password such that it can be remembered. This avoids the need to write passwords somewhere, which is not advisable.
- A password must be difficult to guess.
- Change the password frequently at least 2 weeks once

Guidelines for maintaining a good password

- Change the password once in two weeks or when you suspect someone knows the password.
- Do not use a password that was used earlier.
- Be careful while entering a password when someone is sitting beside you.
- Store the passwords on computer with the help of an encryption utility.
- Do not use the name of things located around you as passwords for your account.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: certin, NIC, साइबर स्वच्छता केंद्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, CYBER SAFE GIRL

Implemented by

राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022

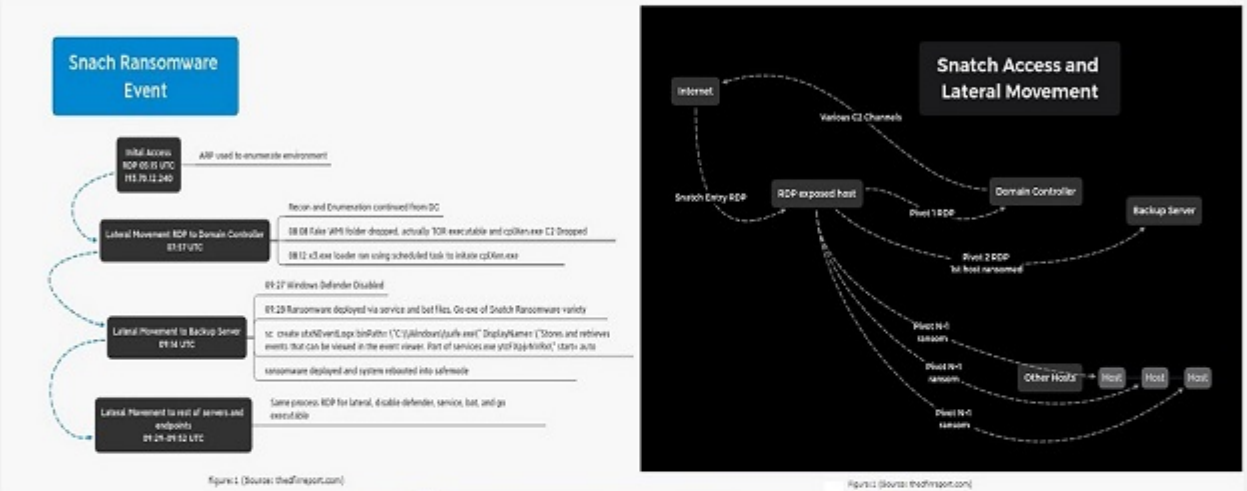
PIB FACT CHECK


#PIBFactCheck
This Letter is FAKE
Government Of India
TATA MOTORS
State Bank of India
No. 7/103/3/2022-Cab. (ii)
GOVERNMENT OF INDIA (BHARAT SARKAR)
CABINET SECRETARIAT (MANTRIMANDAL SACHIVALAYA)
New Delhi, the 14th July, 2022
Subject: Car Finance Scheme for Indian Government Employees - 2022
Ref to our previous letter No. 1/55/3/2022-Cab. (ii) dated 1st July 2022, owing to lesser number of applicants in subject scheme, Competent Authority has instructed to re-advertise to ensure all deserving employees get an equal opportunity to avail the scheme.
In subject scheme, it been decided to provide special facilities to government Employees in form of easy installment car finance Scheme (with zero interest rate) under collaboration with TATA M and above expenses will be borne by the government. Phase w opportu gh State Bank of India (SBI) has been approved nes appended below). Interested officers (ilian a milita ollow the k below to complete their registration.
FAKE
FAKE
FAKE
(Bhaskar Gupta)
(Cabinet Secretary
Finance Department
Note: Organizational Car Finance scheme / allowance will not be admissible to those employees who avail the above mentioned scheme.
Send us your queries here
+918799711259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

Snatch Ransomware

Virus Type: Ransomware

It has been reported that a ransomware dubbed as "Snatch" is on rise and intruding into target organisation's networks via brute forcing Remote Desktop Protocol (RDP) accounts. Threat actors brute forces a Domain Administrator (DA) account via exposed RDP, further leveraging this to run Meterpreter reverse shell and RDP proxy via TOR on a Domain Controller (DC) leading to encrypt all Domain joined systems. Snatch ransomware will force Windows to reboot in Safe Mode (where most of the software and system drivers will not be running) in order to perform the file encryption process.



Best practices for prevention:

- Users are advised to disable their RDP if not in use, if required, it should be placed behind the firewall and users are to bind with proper policies while using the RDP.
- Deploy Multi factor authentication (MFA) for privileged accounts.
- Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
- All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software. Avoid applying updates / patches available in any unofficial channel.
- Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.

https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1694

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, साइबर स्वच्छता केन्द्र Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C | Implemented by: C-DAC

www.InfoSecawareness.in

TOOLS

National Cyber Security Awareness Month

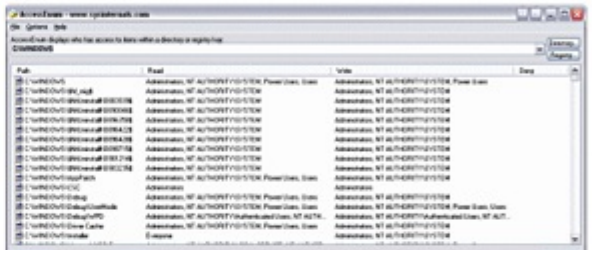
October, 2022

www.isea.gov.in

AccessEnum

AccessEnum gives you a full view of your file system and Registry security settings in seconds, making it the ideal tool for helping you find security holes and lock down permissions where necessary

Introduction



Rwhile the flexible security model employed by Windows NT-based systems allows full control over security and file permissions, managing permissions so that users have appropriate access to files, directories and Registry keys can be difficult. There's no built-in way to quickly view user accesses to a tree of directories or keys. AccessEnum gives you a

full view of your file system and Registry security settings in seconds, making it the ideal tool for helping you find security holes and lock down permissions where necessary.

AccessEnum uses standard Windows security APIs to populate its listview with read, write and deny access information.

For more details visit : ***https://learn.microsoft.com/en-us/sysinternals/downloads/accessenum***

Sysmon

System Monitor is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time.

Sysmon includes the following capabilities:

- Logs process creation with full command line for both current and parent processes.
- Records the hash of process image files using SHA1 (the default), MD5, SHA256 or IMPHASH.
- Multiple hashes can be used at the same time.
- Includes a process GUID in process create events to allow for correlation of events even when Windows reuses process Ids.

For more details visit : ***https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon***

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by certin, CERT-In, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, CYBER SAFE GIRL

Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

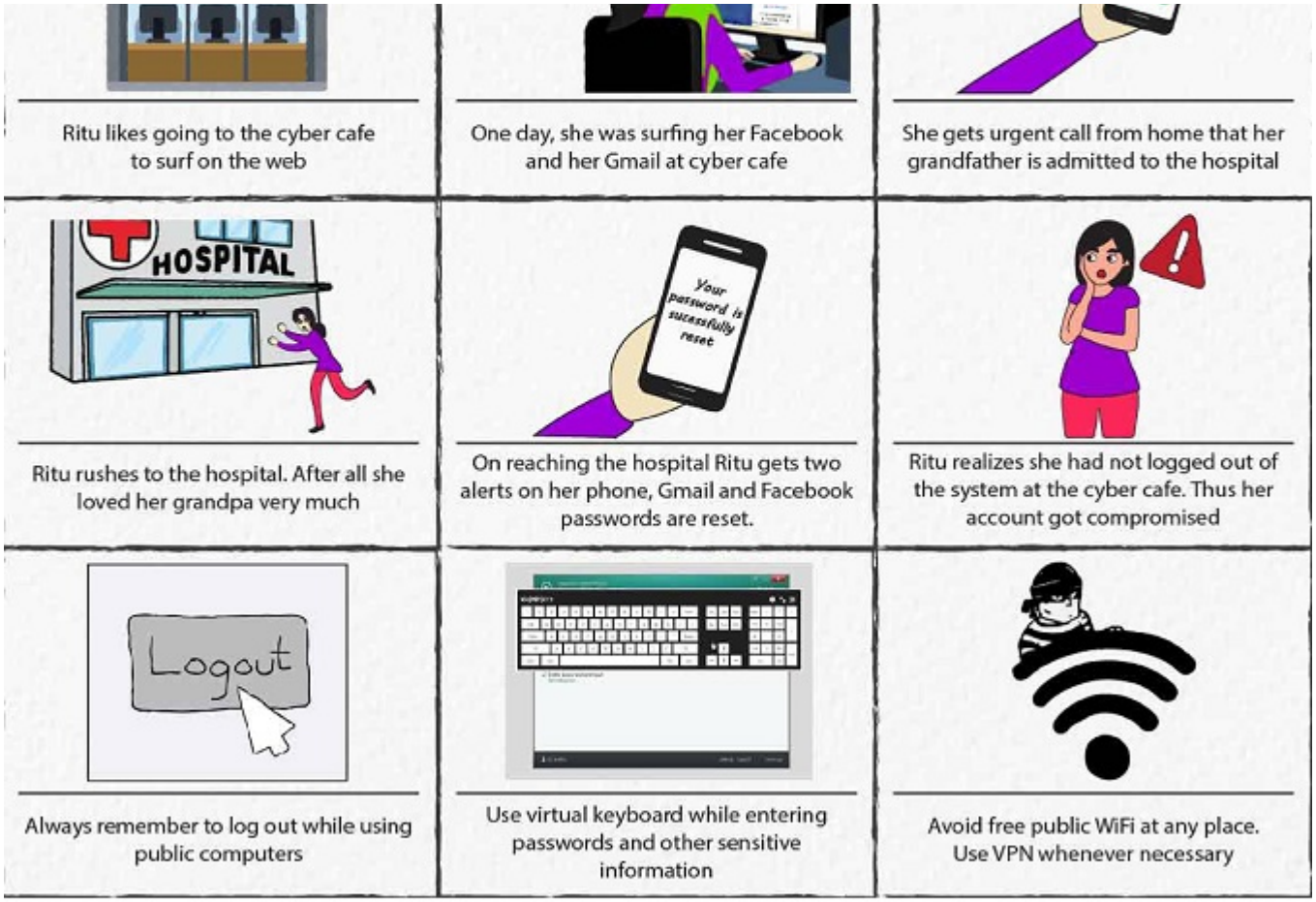
"Be wise on Phishing lies"


Don't Panic
Save the Evidence &
Report at Cyber Crime Cell
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
CYBER SWACHHTA KENDRA
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by


www.InfoSec awareness.in
Brochure
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
WHAT TO DO WHEN YOUR E-MAIL ACCOUNT IS HACKED ?
Check to see which devices have recently connected to your account
Remember the security questions with answers at the time of registration
Reset your password and make sure that it is strong and hard to guess
Scan your computer for
1
2
8
unknown device
***
Reset

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in



Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by: certin, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, CYBER SAFE GIRL
Implemented by

pib FACT CHECK

राष्ट्रीय साइबर सुरक्षा जागरूकता माह - अक्टूबर 2022


This is FAKE !
सरकार दे रही हे सभी
आधार वालो को
₹ 4,78,000
APPLY NOW
आधार कार्ड से लोन
FAKE
#PIBFactCheck
Send us your queries here
+9187997 11259
socialmedia@pib.gov.in
Follow us on social media!
@PIBFactCheck
/PIBFactCheck

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: www.isea.gov.in; www.cyberswachhtakendra.gov.in

Implemented by

www.InfoSecawareness.in

Malware Alerts

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Tycoon Ransomware

Virus Type: Ransomware

It has been reported that a new ransomware, dubbed "Tycoon" targeting Windows and Linux OS is spreading. The malware strain is involved in highly targeted attack campaign targeting small and medium sized software and educational industries. As identified, the malware was deployed in a targeted attack against an organization where system administrators had been locked out of their systems following an attack on their domain controller and file servers.

The ransomware, written in Java, is deployed in the form of Trojanized Java Runtime Environment (JRE) build after intruding victim's network by abusing vulnerable and internet exposed RDP servers. Some peculiar and noteworthy features of this ransomware are:

1. "Image File Execution Options (IFEO) injection" technique is used to gain persistence and execute a backdoor alongside the Microsoft Windows On-Screen Keyboard (OSK) feature of the OS.
2. Anti-malware solutions are disabled using ProcessHacker utility and password of Active Directory servers are changed to deny the access of infected servers.
3. In the final stage, attacker executes Java ransomware module encrypting all file servers including backup systems that are

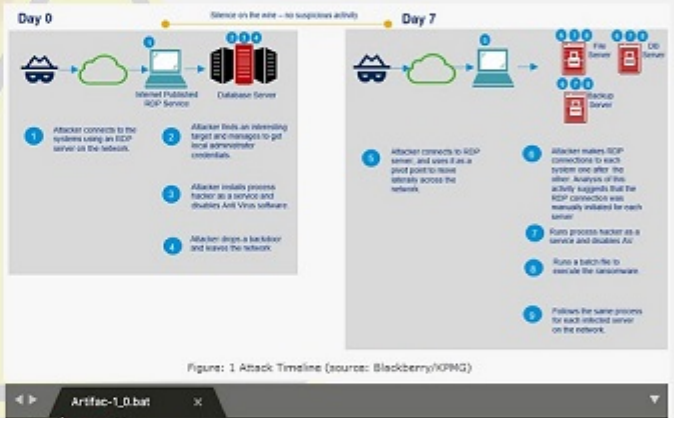


Figure: 1 Attack Timeline (source: Blackberry/KPMG)

connected to the network.

Best practices for prevention:

- Users are advised to disable their RDP if not in use, if required, it should be placed behind the firewall and users are to bind with proper policies while using the RDP.
- Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.

Figure:1 Shell scripts used to execute ransomware, and Java "release" file (source: Blackberry/KPMG)

https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1693

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | cert-in | NIC National Informatics Centre

Supported by: साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra, Botnet Cleaning and Malware Analysis Centre, www.cyberswachhtakendra.gov.in | Cyber Safe Girl | I4C

Implemented by: CDAC

www.InfoSecawareness.in

TOOLS

National Cyber Security Awareness Month

October, 2022

ISEA www.isea.gov.in

AccessChk

As a part of ensuring that they've created a secure environment Windows administrators often need to know what kind of accesses specific users or groups have to resources including files, directories, Registry keys, global objects and Windows services. AccessChk quickly answers these questions with an intuitive interface and output.

Installation

AccessChk is a console program. Copy AccessChk onto your executable path. Typing "accesschk" displays its usage syntax.

Examples

The following command reports the accesses that the Power Users account has to files and directories in `\Windows\System32`:

Using AccessChk

If you specify a user or group name and path, AccessChk will report the effective permissions for that account; otherwise it will show the effective access for accounts referenced in the security descriptor. By default, the path name is interpreted as a file system path (use the "\pipe\" prefix to specify a named pipe path). For each object, AccessChk prints R if the account has read access, W for write access, and nothing if it has neither. The -v switch has AccessChk dump the specific accesses granted to an account.

cmd Copy

```
accesschk "power users" c:\windows\system32
```

This command shows which Windows services members of the Users group have write access to:

cmd Copy

```
accesschk users -cw *
```

To see what Registry keys under `HKLM\CurrentUser` a specific account has no access to:

cmd Copy

```
accesschk -kns austin\mruss hklm\software
```

To see the security on the HKLM\Software key:

Parameter	Description
-a	Name is a Windows account right. Specify `*` as the name to show all rights assigned to a user. Note that when you specify a specific right, only groups and accounts directly assigned to the right are displayed.
-c	Name is a Windows Service. e.g. `ssdpsrv`. Specify `*` as the name to show all services and `scmanager` to check the security of the Service Control Manager.
-d	Only process directories or top-level keys
-e	Only show explicitly set Integrity Levels (Windows Vista and higher only)
-f	If following `-p`, shows full process token information including groups and privileges. Otherwise is a list of comma-separated accounts to filter from the output.
-h	Name is a file or printer share. Specify `*` as the name to show all shares.
-i	Ignore objects with only inherited ACEs when dumping full access control lists.
-k	Name is a Registry key, e.g. `hklm\software`
-l	Show full security descriptor. Add `-i` to ignore inherited ACEs.
-m	Show only objects that have no access
-o	Name is an object in the Object Manager namespace (default is root). To view the contents of a directory, specify the name with a trailing backslash or add `-s`. Add `-t` and an object type (e.g. section) to see only objects of a specific type.
-p	Name is a process name or PID, e.g. `cmd.exe` (specify `*` as the name to show all processes). Add `-f` to show full process token information, including groups and privileges. Add `-t` to show threads.
-q	Omit Banner
-r	Show only objects that have read access
-s	Recurse
-t	Object type filter, e.g. `"section"`
-u	Suppress errors
-v	Verbose (includes Windows Vista Integrity Level)
-w	Show only objects that have write access

For more details visit : *https://learn.microsoft.com/en-us/sysinternals/downloads/accesschk*

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by: certin; CERT-In; NIC National Informatics Centre; साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in; CYBER SAFE GIRL; I4C

Implemented by: ISEA

Visiting Frauds

Fake customer care numbers and calls related frauds

In recent times there have been increasing number of cases where the calls are being received by fraudsters posing to be a service provider or customer care executive and cheat the unsuspecting customers. May it be the case of the man from Lucknow wanting to cancel the food order ordered through food delivery app and ending up paying Rs. 4 lakhs or a Mumbaite loosing Rs.1.25 lakhs upon trying to place a online order for a bottle of wine or student who ended up loosing Rs.27,000/- upon trying to call a customer care of online food service for refund of amount for bad quality of pizza delivered, they have all been robbed off their money by the fraudsters.

Search for wine bottle goes wrong

A deputy manager with a mobile service provider lost Rs.1.25 lakhs when he placed a home delivery order for a wine bottle on October 12. The money was gone within seconds after he called the contact number of Ujwal Wines in Mumbai, which he found through an online search. The police later informed the victim that the owner of Ujwal Wines had filed a complaint that someone had misused the shop name to draw customers keen on home delivery.

Rs 27,000/- for 'bad pizza'

Seecha Vajpayee, a 25-year-old IIT student, became a victim of a UPI fraud when three transactions for a total Rs 27,000 were done through her account. This happened when Vajpayee tries to get in touch with customer care of an online food service for a refund for a 'bad quality pizza' delivered to her on October 27. Police found that the customer care number had been replaced by dupe callers.

Mayur Shetty and V Narayanan - TOI
February 12th, 2020

Man loses Rs 4L while cancelling food order

A man wanting to cancel an order made through a food delivery app was duped of Rs 4 lakhs on Nov. 13 in Lucknow. Not satisfied with the delivery, the man called a 'customer care' number he got on the internet. The call was received by a man who said he was a company representative and asked him to install a app and log in to his savings bank account. " I entered my bank details on the app and received an OTP. The caller asked me to enter the OTP to get the refund. Within minutes Rs 4 lakh was debited from my bank account," he said. Police said the app allowed the fraudster to get remote access of the victim's mobile phone.

Mayur Shetty and V Narayanan - TOI
February 12th, 2020

In the current scenario it becomes essential for every consumer to be aware of modus operandi or meathod of operation of these kind of frauds and the ways and measures to be adopted to safeguard from such frauds.

It is generally seen that we try to contact the service providers for issues /services/queries concerning Credit/Debit card, banking services, mobile phone service , online payment services like paytm/UPI, gas service, Household appliance service (fridge/TV/Washing machine) provider, cable service provider, online purchase or sale etc., The fraudsters come in contact of the users through various means faking to be from one of these institutions that provide the related services and swindle the money of gullible and unsuspecting consumers.

Modus Operandi

- The fraudsters use this common need of people for customer care service providers and upload fake numbers on google search or they get hold of the numbers of customers and call them up on some or the other pretext.
- The fraudsters can create or claim a Google My Business Account using the service providers number or suggest their own number using edit feature/option, and that is how gullible customers land up calling these fake numbers
- Credit card number, PIN Number, download third party apps or share desktop etc., and cheat them with their hard earned money.
- The fraudster may also manipulate people into divulging their personal information by hacking social media accounts and through social engineering techniques wherein they convince people using various techniques to share their personal information, UPI PIN, OTP etc., or click on a link sent by them (Phishing), scan a bar code

customers land up calling these fake numbers updated by fraudsters.

- They trick the people into providing their personal details or financial details like OTP,

on a link sent by them (Phishing), scan a bar code to receive amount, pay small amounts to receive some large amounts as prize etc.,

www.infosecwareness.in | www.isea.gov.in

Security measures or tips to safeguard yourself against fake calls, messages from fraudsters :

Sharing of the sensitive information can give access to strangers and fraudsters to operate with your financial accounts.

Never share your OTP, PIN number, Credit/Debit card details with anyone

The fraudsters can create or claim a Google My Business Account using the service providers number or suggest their own number using edit feature/option and misdirect the gullible callers wrongly to cheat them

Never call the numbers that you find on random google search for a service provider/ customer care centre. Always go to the specific website of the institution or organization for a reliable customer care or service number

The fraudster can try to cheat you by calling you by pretending to be from some company/govt. Agency/LIC etc., for paying you some amount and you have to enter a pin or scan QR code, or send your financial details to receive the amount or get the benefit

Never proceed to either enter your pin number or give your financial details or scan a QR code , that the caller sends you saying that you will receive some amount from someone/some organization if you do so. Always remember that the pin number or QR code scanning is done only for payment of the amount from your end not receiving the amount

The fraudsters may try to install malware into your mobile or system by sending fake links or ask you to download Anydesk app that gives them complete access to your system to commit fraud. This is done by convincing consumers of some free prize amount/service, resolving some issue, providing some beneficial service etc.,

Never download unreliable apps or click on links sent by callers in the disguise of customer care. An authentic customer care person will not send you links or ask you to download apps on your mobile.

The fraudster may try to do SIM Swap by calling consumers pretending to be from service providers like airtel, idea, jio etc.,and on the pretext to give you better service, will try all means to get your unique 20-digit SIM number, that every SIM card has behind it. Once it is done he will ask you to press 1 to swap the SIM, which gives him access to your mobile phone and all OTPs n other details.

Never share SMS with your SIM card number in it to anyone, even if the caller insists that it is required for providing better services etc.,

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

ISEA awareness Newsletters on WHATSAPP SECURITY


SECURITY OVER
WHATSAPP
Scan and Download
https://infosecawareness.in/newsletter/edition1-2022
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
CYBER SWACHHTA KENDRA
www.cyberswachhtakendra.gov.in
Implemented by

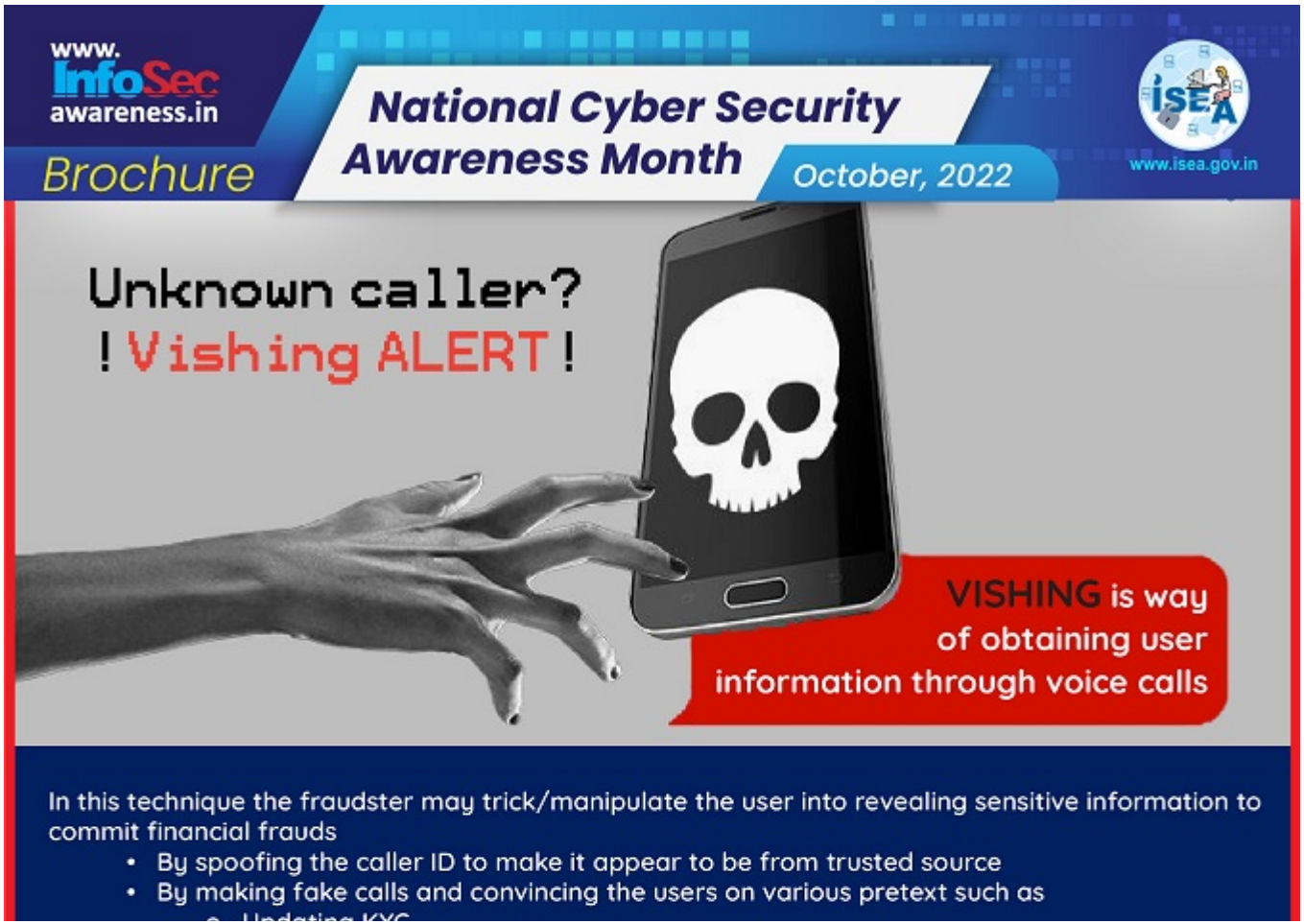
Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

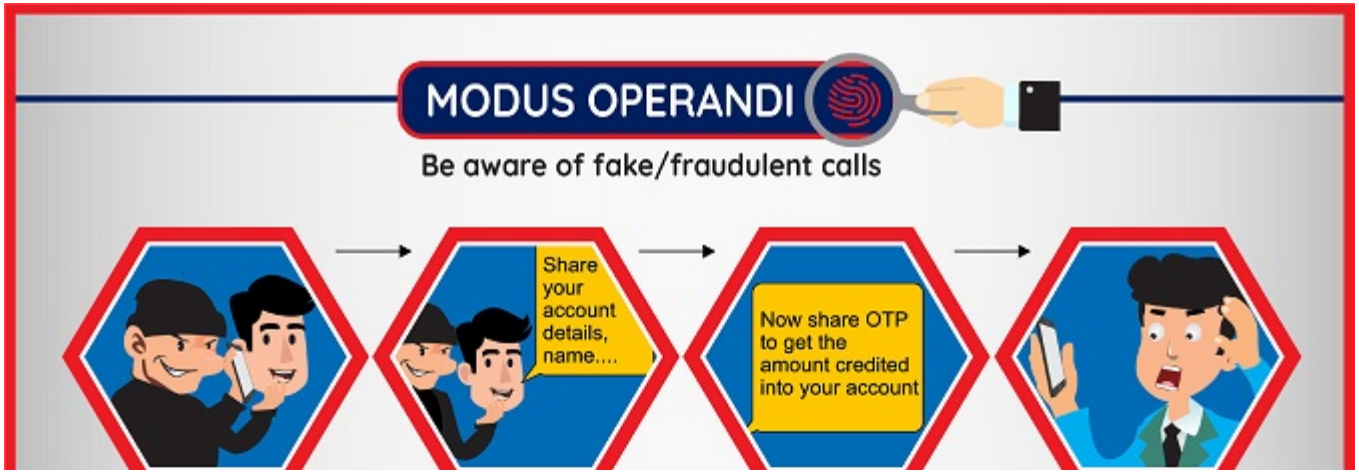
"Keep an eye on children when they use Internet"

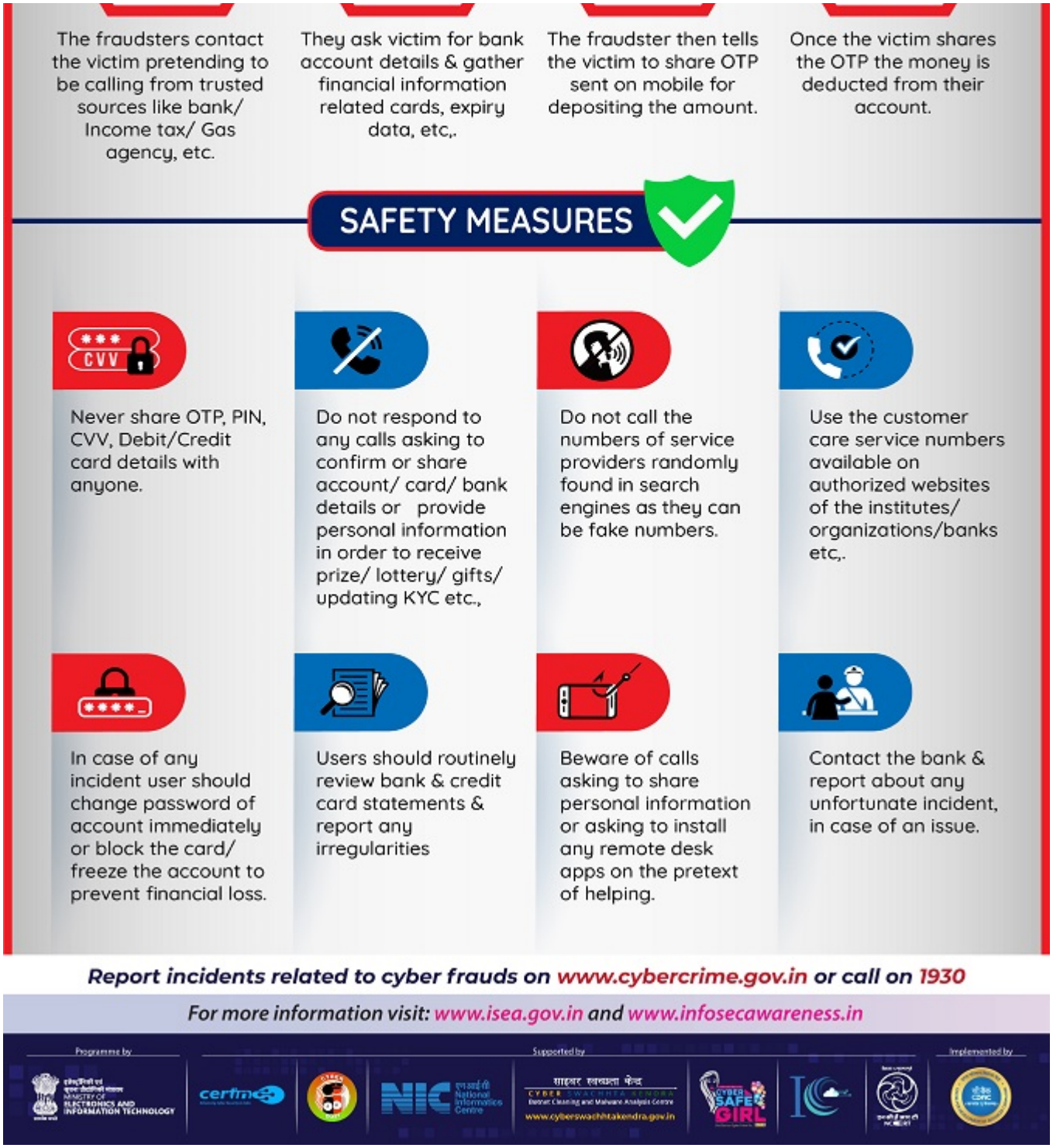

/sbibank
Official Bank Customer care or communication number never be a 10 digit mobile number
RBI never sends any bank link for updating your KYC
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
Supported by
Implemented by


www.InfoSec awareness.in
Brochure
National Cyber Security Awareness Month
October, 2022
www.isea.gov.in
Unknown caller?
!Vishing ALERT!
VISHING is way of obtaining user information through voice calls
In this technique the fraudster may trick/manipulate the user into revealing sensitive information to commit financial frauds
• By spoofing the caller ID to make it appear to be from trusted source
• By making fake calls and convincing the users on various pretext such as

- Updating KYC
- Linking Aadhar
- Offering free gifts/lottery/prizes
- Customer service executive from bank/gas agency etc.,

- By asking the user to scan the bar code to receive money
- By getting the users to call the fake customer care numbers updated by them on google.




The fraudsters contact the victim pretending to be calling from trusted sources like bank/ Income tax/ Gas agency, etc.
They ask victim for bank account details & gather financial information related cards, expiry data, etc,.
The fraudster then tells the victim to share OTP sent on mobile for depositing the amount.
Once the victim shares the OTP the money is deducted from their account.
SAFETY MEASURES
CVV
Never share OTP, PIN, CVV, Debit/Credit card details with anyone.
Do not respond to any calls asking to confirm or share account/ card/ bank details or provide personal information in order to receive prize/ lottery/ gifts/ updating KYC etc.,
Do not call the numbers of service providers randomly found in search engines as they can be fake numbers.
Use the customer care service numbers available on authorized websites of the institutes/ organizations/banks etc,.
In case of any incident user should change password of account immediately or block the card/ freeze the account to prevent financial loss.
Users should routinely review bank & credit card statements & report any irregularities
Beware of calls asking to share personal information or asking to install any remote desk apps on the pretext of helping.
Contact the bank & report about any unfortunate incident, in case of an issue.
Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930
For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
साहार स्वच्छता केंद्र
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by

www.InfoSec awareness.in

Storyboard

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Phishing Attacks

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930


For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by


pib
FACT CHECK
राष्ट्रीय साइबर सुरक्षा
जागरूकता माह - अक्टूबर 2022


Dear All,
Listen to world wide radio From Indian Space Research Organisation (ISRO) when u click the link u can see the globe rotating. There are green dot on which you simply touch you can start listening to live radio from that place
Simply Amazing
FAKE
FAKE
This claim is Fake!
Radio garden has
NOT been developed
by ISRO

Necurs Botnet

Virus Type: Banking Trojan

It has been reported that the variants of the malware named as Necurs are spreading. The malware mainly targets the windows operating systems and is well known for its spamming and malware distribution functionalities. The malware mainly spread by means of spear phishing emails containing phishing URLs or malicious attachments and also through dating sites.

It has the following functionalities:

- Anti-detection capabilities to hide itself by disabling Antivirus driver components or other security features.

- Spread banking Trojans, ransomwares, RATs, infostealers or cryptocurrency miners
- Stop its activities for a period of time and then reinitiate with new commands for the infected hosts.
- Machines infected with necurs botnet make network connections to remote command and control server to receive commands and operate accordingly.
- Make use of victims email IDs to send spam mails.
- Spreads malware that are capable of launching DDoS attacks.

Best practices for prevention:

- Make use of "Microsoft Safety Scanner", this scan tool is designed to find and remove identified threats & malware from Windows computers.
- Delete the system changes made by the malware such as files created/ registry entries /services etc.
- Monitor traffic generated from client machines to the domains and IP address mentioned in Installation section.
- Avoid downloading pirated software.
- Protect yourself from social engineering attacks.
- Scan infected system with updated versions of Antivirus solution
- Disable Autorun and Autoplay policies.
- Use limited privilege user on the computer or allow administrative access to systems with special administrative accounts for administrators.
- Do not visit untrusted websites.
- Do not download or open attachment in emails received from untrusted sources or unexpectedly received from trusted users.
- Enforce a strong password policy and implement regular password changes.
- Enable a personal firewall on workstation.
- Disable unnecessary services on agency workstations and servers.

https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2019-1658

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

slingshot linux distribution

Slingshot is an Ubuntu-based Linux distribution with the MATE Desktop Environment built for use in the SANS penetration testing curriculum and beyond. Designed to be stable, reliable and lean, Slingshot is built with Vagrant and Ansible. It includes many standard pen testing tools, as well as the PenTesters Framework (PTF). Course-specific builds include all of the tools, files and documentation needed for class labs. The initial release of Slingshot is for the general community with course-specific builds deploying throughout 2020.

Key Features of Slingshot

- Provides a consistent experience for SANS students
- Extensive use of virtual environments (e.g., pyenv, rbenv) to prevent version conflicts
- Repeatable and testable build process using Vagrant and Ansible
- Automated testing during the build process verifies that updates do not break tools
- Streamlines courseware creation by course authors for students

Minimum System Requirements:

- VMware Player or similar
- 2 GHz dual-core processor
- 4 GB of system memory
- 15 GB of disk space

Tools Included

- Aircrack-ng
- Asleap
- BeEF
- Burp Suite
- checksec.sh
- Covenant
- coWPAtty
- Docker
- Empire 3 (latest BC Security fork)
- EQL
- Ettercap
- ExploitDB
- EyeWitness
- Golang
- hashcat
- hping3
- John the Ripper
- Kismet
- LogonTracer
- Masscan
- Metasploit Framework
- Mimikittenz
- Nikto
- Nmap
- OpenVAS
- Powershell Empire
- Recon-ng
- Responder
- RITA
- Social Engineer Toolkit
- sqlmap
- tcpdump
- THC-Hydra
- Unicornscan
- Veil Evasion
- Wapiti
- weirdAAL
- Wireshark
- WPScan
- ZAProxy

For more details visit
https://www.sans.org/slingshot-vmware-linux#:~:text=What%20is%20Slingshot%3F,built%20with%20Vagrant%20and%20Ansible.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930


For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
cert-in
NIC National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by
CDAC

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

"Beware of Skimmers and Social Engineering"

Online shopping — the glorious invention which allows people to buy things from the comfort of their homes. No more travelling to multiple stores to find the right product; no more having to deal with over-enthusiastic sales persons; no more standing in long lines at the checkout counter. The e-commerce boom has certainly changed the way we shop for the better. But, like everything else, the world of online shopping is not all roses. Despite all the efforts of e-commerce companies to alleviate them, there are a few problems that customers still have to face while shopping online

How to safe during online shopping

Keep track of your digital payments

Shop only through trusted sites

Check the security aspects of the website

Don't save the card details or bank details on websites

Never respond to email which asks about your purchases

Don't clink on links offering discounts/ prizes

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Let's look into few ways that cyber criminals may target women

Expensive branded products at low cost:
In social networking sites very often we get advertisements showing expensive branded products at unbelievable prices. This catches attention of customer's most likely women and they may end up paying money for those products which are not genuine. For example branded bags, clothes, costly phone and beauty products.

Natural remedies for weight loss:
Most often in our social networking and Instant messaging Applications we get messages giving tips on weight loss and for further inputs they request for payment to purchase their product. Women who are desperate to weight loss get trapped by these messages. They end up paying money for fake products.

Expensive Jewelry:
Cyber-criminals may spoof certain online jewelry websites and give exciting discounted offers for jewelry products targeting women customer. They purchase products online with certain value but end up receiving some other products of lesser value. And they feel cheated and when they raise complaint to the original website they just deny that purchase happened through their website. This may lead to loss of your money?

Risks in online shopping

A few questions you need to check before you start online shopping

Brand
is the e commerce site genuine?

Security
Is your credit card safe?

Privacy
Is your information being sold?

Shipping
Are you getting the correct product at the requested time?

Tips for safe online shopping

- **Keep computer OS updated:**
  Make sure your PC is secured with an antivirus, anti spyware, firewall, system updated with all patches and web browser security with the trusted sites and security level at high.

- **Shop only through trusted sites:**
  Research about the web site that you want to connected to the internet and try to send spam emails and try to install the malicious software that may collect your personal information.

- **Never respond to email which asks about your purchases:**
  Beware of the emails like "please confirm of your payment, purchase and account detail for

buy things from, since attackers try to trap with websites that appear to be legitimate, but they are not. So make a note of the telephone number's physical address of the vendor and confirm that the website is a trusted site. Search for different web sites and compare the prices. Check the reviews of consumers and media of that particular web site or merchants.

- **Check the security aspects of the website:**
  If you are ready to buy something online check whether the site is secure with https or padlock on the browser address bar or at the status bar and then proceed with financial transactions.

- **Keep track of your digital payments:**
  Immediately check the credit card statements as soon as you finish and get them to know about the charges you paid were same; and if you find any changes immediately report to concerned authorities.

- **Don't save the card details or bank details on websites:**
  Do not store the card no either debit or credit on the shopping websites.After finishing your online shopping clear all the web browser cookies and turn off your PC since spammers and phishers will be looking for the system

the product." Remember legitimate business people never send such emails. If you receive such emails immediately call the merchant and inform the same.

- **Change passwords frequently:**
  Don't use a single password for a long time, change your Email id, bank account, credit-debit card passwords frequently.

- **Different passwords for different websites:**
  If hackers crack your one password they may crack all others if you are using same or similar password for all. So use different t password for all websites. However it is more complex to remember all passwords but it will add the Safety layer too.

- **Use Secured Networks:**
  Always use secured internet connection. Public Wi-Fi spots are Vulnerable to cyber attacks.

- **Don't click on links offering discounts/ prizes:**
  Cyber criminals sent messages in featuring great discounts in popular e commerce websites. It is always better to check in the original website for offers rather than clicking on links received in WhatsApp groups or from unknown numbers.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

www.InfoSec awareness.in

Storyboard

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Be aware of online shopping

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930


For more information visit: www.isea.gov.in and www.infosecawareness.in
Programme by
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Supported by
NIC National Informatics Centre
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in
CYBER SAFE GIRL
Implemented by


PIB FACT CHECK
राष्ट्रीय साइबर सुरक्षा
जागरूकता माह - अक्टूबर 2022


#PIBFACTCHECK
NO such scheme is being run by the Govt of India


11:02 AM
Government giving free Laptop to all the students of India. Register your Number on Gov-Laptop app to get free laptop.
Link: http://tiny.cc/Be
FAKE
FAKE

Clipsa Malware

Virus Type: Multipurpose Password Stealer

It has been reported that a malware named as "Clipsa" is spreading. The malware mainly spreads in the form of executable files masquerading as installer for media players.The malware is capable of performing the following functions:

- Steals administrative credentials from unsecured wordpress sites.
- Mine and steal crypto currencies by replacing crypto addresses present in a clipboard via clipboard hijacking.
- Scans internet and launches brute-force attacks on Wordpress sites.
- Leads to degradation of system performances due to excessive use of resources in crypto cur-

rency mining.
- May use the compromised websites as secondary command and control servers to host malicious files or upload stolen data.

Best practices for prevention:

- Monitor and block network traffic and systems making connections to the above mentioned domain/IPs at firewall, IDS, web gateways, routers or other perimeter based devices.
- Delete the file system and registry changes made by the malware.
- Disable the Autorun functionality in Windows
- http://support.microsoft.com/kb/967715
- Keep up-to-date patches and fixes on the operating system and application software.
- Keep up-to-date Antivirus and Antispyware signatures at desktop and gateway level.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations.
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf.
- Consider encrypting the confidential data as the ransomware generally targets common file types.
- Exercise caution while visiting links to Web pages.
- Do not visit untrusted websites.
- Use strong passwords and also enable password policies.
- Enable firewall at desktop and gateway level.

https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2019-1657

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

KAPE

KROLL ARTIFACT
PARSER AND EXTRACTOR

Kow KAPE works

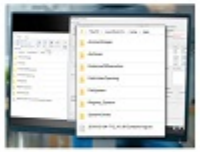
Over 60 Predefined Targets and 90 Modules

- KAPE has two primary phases – target collection and module execution:
- Targets are essentially collections of file and directory specifications.
- Modules are used to run programs, which can target anything, including files collected via targets as well as any other kinds of programs you may want to run on a system from a live response perspective.

KAPE gives you access to targets and modules for the most common operations required in forensic exams, helping investigators gather a wider range of artifacts in a fraction of the time, enriching evidentiary libraries.

Grouping Artifacts Expedites Triage

KAPE focuses on collecting and processing relevant data quickly, grouping artifacts in categorized directories such as EvidenceOfExecution, BrowserHistory and AccountUsage. Grouping things by category means an examiner no longer needs to know how to process prefetch, shimcache, amcache, userassist, etc., as they relate to evidence of execution artifacts.



Standardize Forensic Processes

When handling an incident, forensic examiners are tasked with knowing which artifacts to collect, where they may reside, and how to collect the data without damaging the evidence or chain of custody. With KAPE, forensic examiners have a solution to find, collect and process forensic artifacts in a way that standardizes forensic engagements by leveraging a wider range of extracted artifacts. KAPE can also help facilitate the onboarding and training of new investigators by standardizing and scaling artifact pulls.

For more details visit
https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology

Supported by: CERT-In, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C

Implemented by: C-DAC

www.InfoSecawareness.in

Advisory

National Cyber Security Awareness Month

October, 2022

ISEA www.isea.gov.in

COVID-19

Large Scale Phishing Attack Campaign against Indian Citizens

Problem Statement

It is expected that cyber criminals are targeting Indian citizens through COVID-19 Phishing Malware attacks through emails disguised as **free COVID-19 test**. The fraudsters claim to have 2 million email addresses of Indian citizens which they would be using for sending fake emails claiming to be from government authorities. As per the reports, the fraudsters will be sending fake emails to Indian citizens impersonating various government officials which are expected to be from an spoofed email address **ncov2019@gov.in**

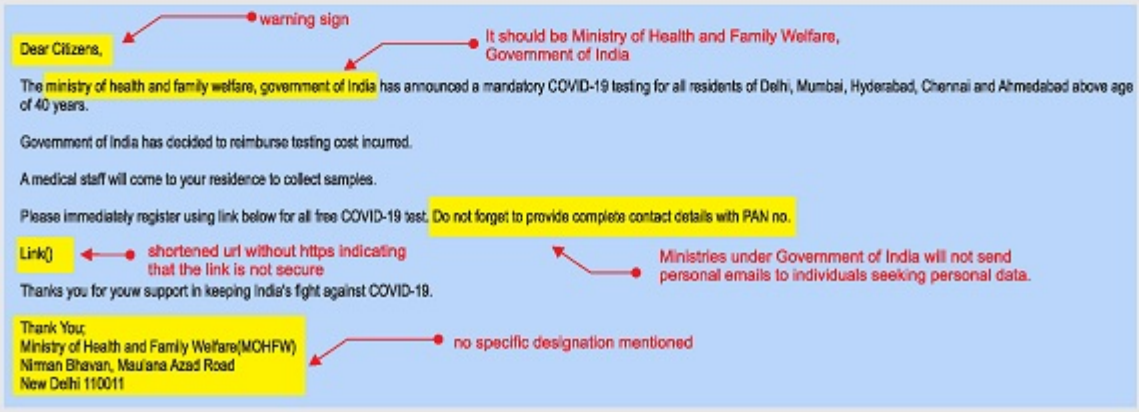
Motivation : Financial Gains

As Indian government has announced Rs 20 lakh crore (US$307B) of credit, finance and collateral-free loans to micro, small and medium enterprises, as well as welfare packages for citizens of India; a Phishing campaign is expected to impersonate government agencies, departments and trade associations who have been tasked to oversee disbursement of the government fiscal aid.

Method: The hacking campaign involves phishing emails under the guise of local authorities in charge of dispensing government-funded Covid-19 testing and support initiatives. These phishing emails are designed to drive recipients to malacious websites where they will be deceived into divulging personal and financial information.

Watch out for warning signs of Malicious Phishing Scams

A Sample email highlighting the warning signs are shown below.



www.infosecwareness.in | www.isea.gov.in

- The subject of the fraud email would be: free COVID-19 testing for all the residents of Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad inciting them to provide personal information.
- The mail is commonly addressed as 'Dear Citizen', which is a warning sign
- The mail referred the ministry as' ministry of health and family wellfare, government of india' where the it should have been 'Ministry of Health and Family Wellfare, Government of India'
- The mail is addressed from 'Ministry of Health and family welfare' with no specific designation mentioned
- Ministries under Government of India will only give notification through trusted government sources regarding wellfare packages announced for citizens and will not send personal emails to individuals seeking personal data.
- When a user clicks on the link mentioned in the email, they will be redirected to malicious websites which asks them enter their personal information.
  - The link mentioned in the email is shortened url without https indicating that the link is not secure.

---------- Preventive Measures ----------

Beware of e-mails, links providing special offers like Covid-19 testing, Aid, Winning *a prize, Rewards, Cashback offers. Check the integrity of URLs before providing login credentials or clicking a link*

Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) *in your antivirus, firewall, and filtering services. Update spam filters with latest spam mail contents*

Always send confidential information using Pretty Good Encryption (PGP) only wherein only sender and receiver can see the information

Exercise extra caution in opening attachments, even if the sender appears to be known

Delete email from unknown sources without opening attachments

Do not submit your personal information on any websites you are not familiar with

Ensure the website/link starts with https which means it is secure

Beware of fraudulent emails that have spelling mistakes. Do not open those

Any unusual activity or attack should be reported immediately at **incident@certin.org.in**. with the relevant logs, email headers for the analysis of the attacks and taking appropriate actions further

To check the integrity of e-mail, Log on to **https://www.cyberforensics.in/** click on e-mail Tracer

Do not fall prey to cyber criminals. Beware of online frauds and be responsible to save yourself!

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology

Supported by: CERT-In, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra, Botnet Cleaning and Malware Analysis Centre, www.cyberswachhtakendra.gov.in, Cyber Safe Girl

Implemented by

Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

"Never share your password to anyone"

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: certin, CSK, NIC National Informatics Centre, साइबर स्वच्छता केंद्र Cyber Swachhta Kendra www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C | Implemented by: ISEA, CDAC

www.InfoSec awareness.in

Brochure

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

SECURE USAGE OF CREDIT & DEBIT CARD/ATM

Security Threats

Identity theft

The fraudulent acquisition and use of person's private identifying information, usually for financial gain. It can be divided into two broad categories :

- **Application fraud**
  Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information.

- **Account takeover**
  Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for the mail to be redirected to a new address. The criminal then reports the card loss and asks for a replacement to be sent.

Do's

- Before you use an ATM, please ensure that there are no strange objects in the insertion panel of the ATM. (to avoid skimming)
- Shield the ATM pin number during transaction. Don't claims to represent the Bank.
- Don't get carried away by strangers who try to help you use the ATM machine.
- Don't use the ATM machines if the device is not in good conditions.

carry the transaction receipts along.
- Please change your ATM PIN once in every 3 months. As advised by banks.
- Keep your credit card receipts to guard against transaction frauds, check your receipts against your monthly statement.
- Only carry around credit cards that you absolutely need.
- Shred anything that contain your credit card number written on it. (bills)
- Notify your credit card issuers in advance of your change of address, then you change home address.
- If you lose your credit card, please report the loss immediately.
- When you dispose a card at the time of renewal/ upgradation, please make sure to cut it diagonally before disposal.

Don'ts

- Don't accept the card received directly from bank in case if it is damaged or seal is open.
- Don't write your PIN number on your credit card.
- Don't carry around extra credit cards that you rarely use.
- Don't disclose your Credit Card Number/ATM PIN to anyone.
- Don't hand over the card to anyone, even if he/she
- Don't transfer or share your account details with unknown/non validated source.
- Don't access Netbanking or make payment using your Credit/Debit card from shared or unprotected computers in public places.
- Don't open unexpected e-mail attachments from unexpected sources or instant message download links. Delete suspicious e-mail immediately.
- Don't give out your account number over the phone unless you initiate the call and you know the company is reputable. Never give your credit card info out when you receive a phone call. (This is called Vishing)
- Don't provide your credit card information on a website that is not a secure site.
- Don't share any confidential information such as password, customer id, Debit card number, Pin, CVV, DOB to any email requests, even if the request is from government authorities like Income Tax department, RBI or any card association company like VISA or Master card.
- Don't address or refer to your bank account problems or your account details and password on social networking site or blogs.
- Don't store critical information like your ATM PIN number on your mobile phone.

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: CERT-In, NIC, साइबर स्वच्छता केन्द्र, Botnet Cleaning and Malware Analysis Centre, www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C | Implemented by: CDAC

www.InfoSecawareness.in

Storyboard

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

Beware of in-game purchases for online games

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

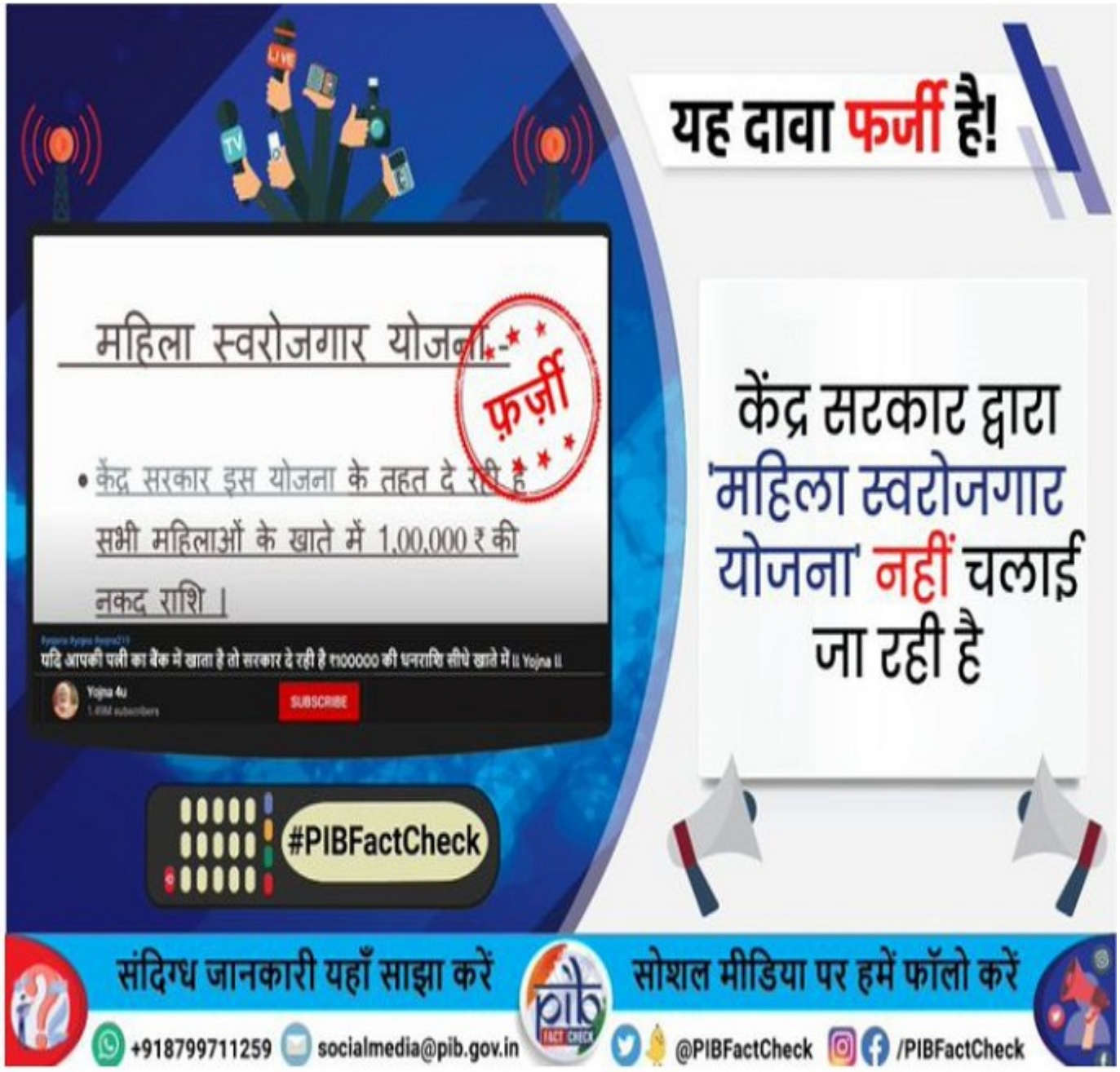
For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by | Supported by | Implemented by

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

National Informatics Centre

साइबर स्वच्छता केंद्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
www.cyberswachhtakendra.gov.in

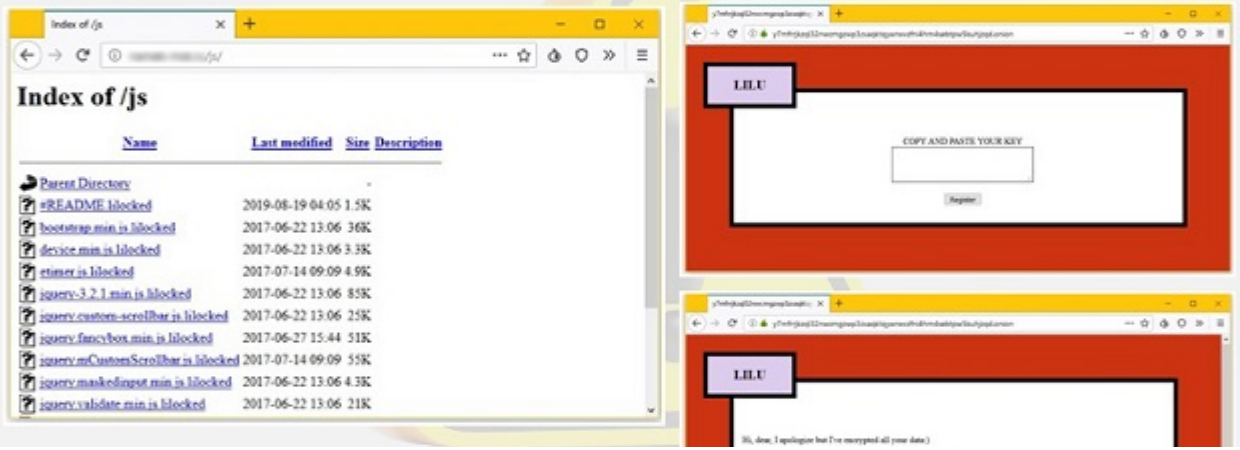

यह दावा फर्जी है!
महिला स्वरोजगार योजना -
फ़र्ज़ी
• केंद्र सरकार इस योजना के तहत दे रही है
सभी महिलाओं के खाते में 1,00,000 ₹ की
नकद राशि ।
यदि आपकी पत्नी का बैंक में खाता है तो सरकार दे रही है ₹100000 की धनराशि सीधे खाते में || Yojna ||
Yojna 4u
SUBSCRIBE
केंद्र सरकार द्वारा
'महिला स्वरोजगार
योजना' नहीं चलाई
जा रही है
#PIBFactCheck
संदिग्ध जानकारी यहाँ साझा करें
+918799711259
socialmedia@pib.gov.in
सोशल मीडिया पर हमें फॉलो करें
@PIBFactCheck
/PIBFactCheck

Linux: Lilu/Lilocked Ransomware

Virus Type: Ransomware

It has been reported that the malware named as lilu/Lilocked having ransomware capabalities targeting linux machines is spreading. The infection vector used by the ransomware is currently unknown. However some of the functionalities of the malware is as follows:

- Target linux servers and gain their root access.
- Locked files after encryption with ".lilocked" extension.
- Shows ransomware note ot the victim and demands 0.03 bitcoin or $325 in the Electrum Wallet for decryption key.
- It encrypts or targets only specific file types such as HTML, SHTML, JS, CSS, PHP, INI and other image file formats and does not encrypts or effect system files.



Best practices for prevention:

- Users are advised to disable their RDP if not in use, if required it should be placed behind the firewall and users are to bind with proper policies while using the RDP.
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Consider encrypting the confidential data as the ransomware generally targets common file types.

https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2019-1656

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology | Supported by: cert-in, NIC National Informatics Centre, साइबर स्वच्छता केन्द्र Cyber Swachhta Kendra Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in, Cyber Safe Girl, I4C | Implemented by: C-DAC, ISEA

www.InfoSec awareness.in

TOOLS

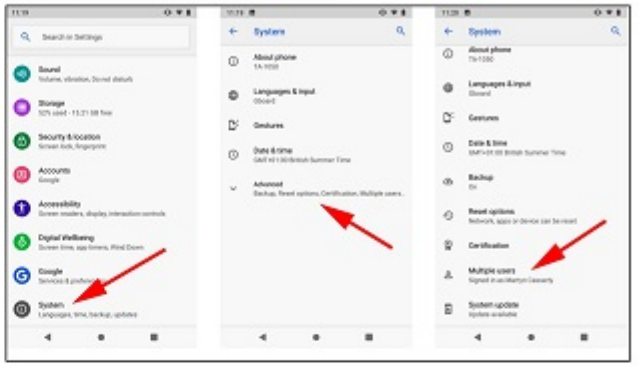
National Cyber Security Awareness Month

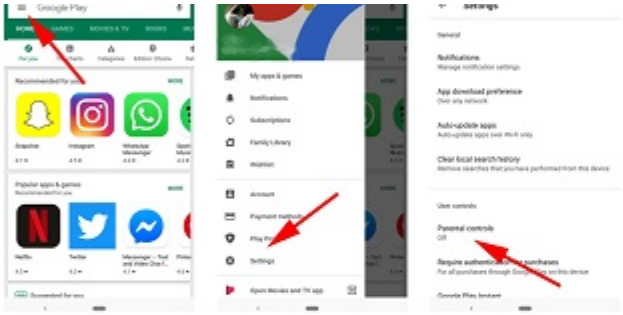
October, 2022

www.isea.gov.in

How to add a user account in Android

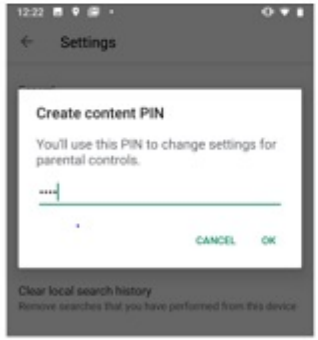
Launch the device's Settings menu then scroll down and select System > Advanced > Multiple Users.

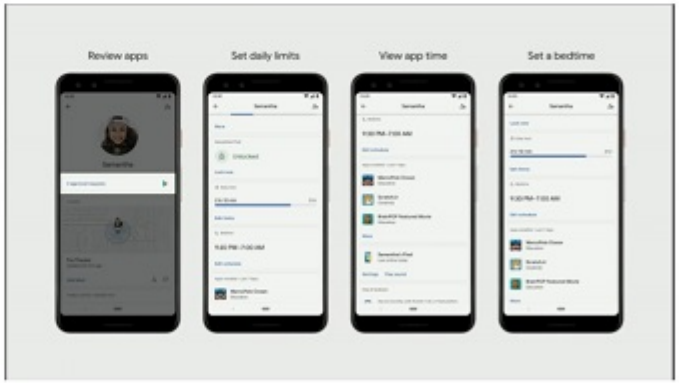




- Set up various elements of the account, including updating the software, adding security features (fingerprints, passcodes, etc.)
- Launch the Play Store app and tap the three horizontal lines at the top left. Scroll down and tap Settings, then scroll until you see Parental controls.

- The different sections are Apps & games, Films, TV, Books, and Music. Tap on one and you'll see the various age categories available. Simply tap the highest age you want the child to have access to and then tap Save
- Now, your child won't be able to download any content that is rated above the setting you have e put in place.
-
- Adjust the following settings as per your child's age and requirements.





Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Supported by

Implemented by