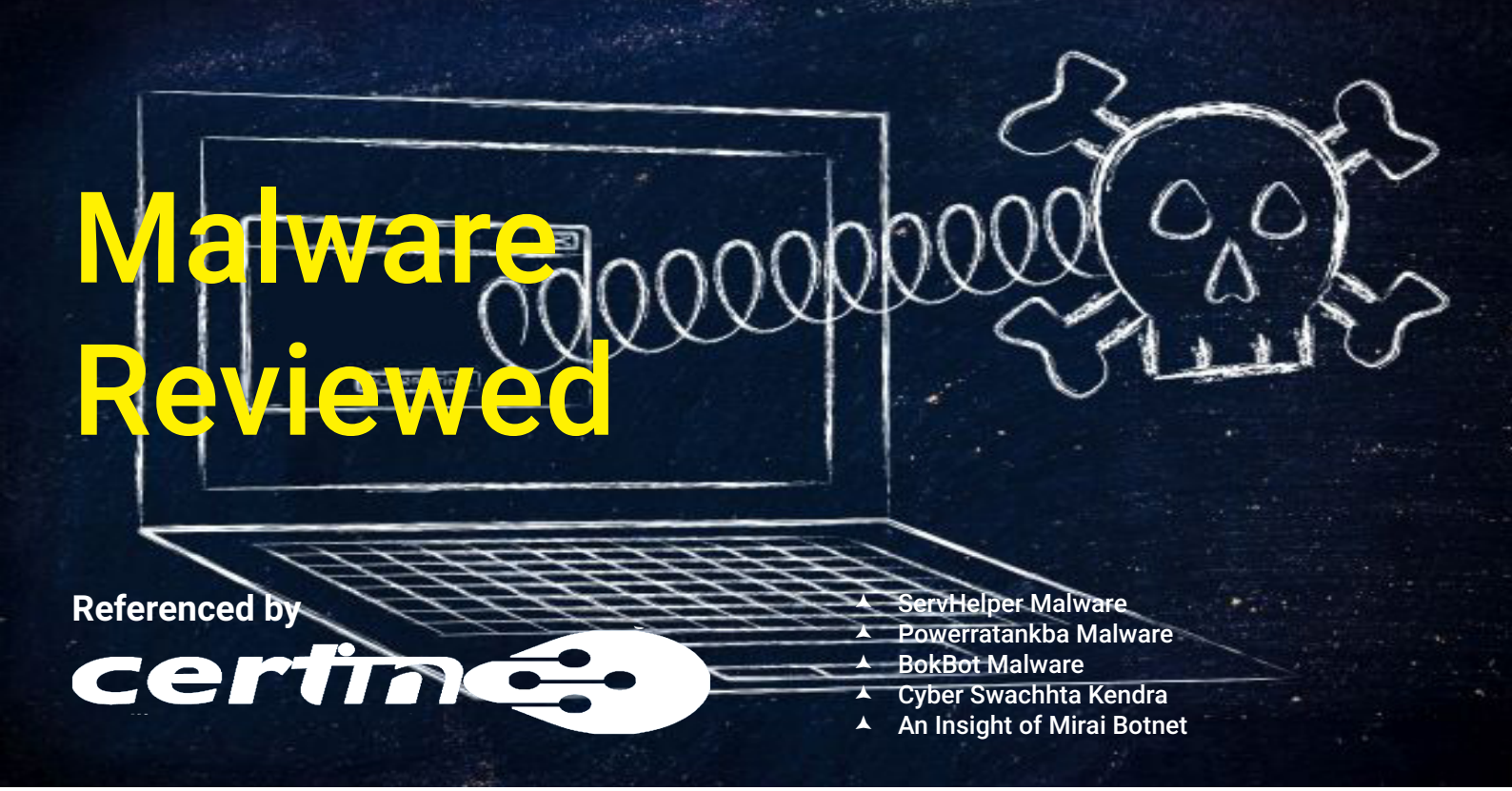


Malware Reviewed

Referenced by certin

- ServHelper Malware
- Powerratankba Malware
- BokBot Malware
- Cyber Swachhta Kendra
- An Insight of Mirai Botnet

Dr. Sanjay Bahl,
Director General, CERT-In

The Information Security Education and Awareness Program is a unique program imparting education at the Bachelors, Masters and PhD level for capacity building at a technical level in the country as well as creating awareness in multiple Indian languages for various segments of the society such as children, women, parents, teachers, etc through innovative mechanisms.

The Cyber Swachhta Kendra by CERT-In takes the awareness to a different level by reaching out to the citizens with digital devices on a scale which is unprecedented globally.

This section gives you an insight on sophisticated techniques used by cybercriminals to fetch your information leading to personal and financial loss.

----------Malware: what you need to know

ServHelper Malware

Virus type: Backdoor

There are public reports about spreading of malware named as ServHelper malware. It is a backdoor malware used by attacker to steal the information from victim machine to use it in later stage for performing malicious activity. The Mode of spreading of this malware is through mail which carry either the malicious macro embedded document in the form of Doc, wiz and pub or through malicious URLs which link to the malware. Once victim enable the embedded macro, it download and execute the ServHelper malware on the victim machine. After victim is infected with ServHelper, attacker exploit the victim machine through two ways. First is "tunnel" variant in which attacker access the victim machine through Remote Desktop Protocol via SSH tunnels. After building connection to Command and control server (C2) controlled by attacker, attacker performing different malicious activity via executing commands like copying victim browser profiles data, credentials, kill process, create scheduled task and delete malware from victim machine. Second one is by deploying another Remote Access Trojan (RAT) on victim machine named as FlawedGrace. This RAT creates the configuration file at location C:\ProgramData\.dat which contains the details of C2 IP and Ports to which machine need to connect. After building connection with C2, malware perform activity via executing different commands like update, remove, download, destroy etc.

The IOC of attack is listed below for your action.

Command and Control Server

- http://officemysuppbox[.]com/staterepository
- https://checksolutions[.]pw/ghuae/huadh.php
- https://rgoianrdfa[.]pw/ghuae/huadh.php
- https://arhidsfderm[.]pw/ghuae/huadh.php
- http://offficebox[.]com/host32
- http://office365onlinehome[.]com/host32
- https://afgdhjkrm[.]pw/aggdst/Hasrt.php
- http://dedsolutions[.]bit/sav/s.php
- http://dedoshop[.]pw/sav/s.php
- http://asgaage[.]pw/sav/s.php
- http://sghee[.]pw/sav/s.php
- https://vesecase[.]com/support/form.php
- 46.161.27[.]241:443

File Location C:\ProgramData\.dat

Best Practise and Recommendations

- 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.
- 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/threatresearch/2016/02/greater_visibilityt.html
- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- 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.

Powerratankba Malware

Virus Type: Malicious Program

There are public reports about spreading of malware named as Powerratankba malware. The malware is used by attacker for stealing the victim information which they used in later stage for performing malicious activity. The Mode of spreading of this malware is through dropper which gets download on the victim machine via malicious link lurking victim to apply for a job.

- Once this dropper reach on victim machine, it decode the PowerShell script from it saved at location C:\\users\\public\\REG_TIME.ps and execute it.
- After that it will build the connection with C2 controlled by attacker to download Powerratankba malware, used by attacker for gathering the victim system information.
- Powerratankba Malware used the victim legitimate service like Windows Management Instrumentation (WMI) to obtain the IP address, Operating system information, username and registry for proxy details, files open etc. from the victim machine to remain undetected for long time.
- Finally Powerratankba malware download its final payload at location C:\windows\temp\REG_WINDEF.ps1 and register it as a service. Malware also add itself at start up location to maintain its persistence in victim machine.

Command and Control Server

- https://ecombox.store
- https://bodyshoppechiropractic.com

File Location

- C:\windows\temp\REG_WINDEF.ps1
- Autostart setting \AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ as WIN_REG.exe.
- C:\windows\temp\tmp0914.tmp
- C:\\users\\public\\REG_TIME.ps1

Best Practise and Recommendations

- 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.
- 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
- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- 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.

BokBot Malware

Virus Type: Trojan

There are public reports about spreading of malware named as BokBot malware. This banking Trojan is modular in nature for performing different malicious activity on the victim machine. The Mode of spreading of this malware is through spear phishing attachment or link or via Emotet malware distribution.

- Once this malware reach on victim machine, it will decode the shell code from it, create its directory (at C:\ProgramData location) and executes from there.
- After malware got installed on victim machine, it will generate the system ID and Collect System information like (Windows version information, User name, user SID, Member of a domain, LAN group).
- After that malware try to build connection with C2 controlled by attacker. Once it successfully build the connection with C2, it register the victim on C2 with information it gather from previous step and start performing malicious activity based upon the command it received from C2 controlled by attacker like Credential theft , Intercepting proxy, Remote control via VNC, updating of malicious module of malware etc.
- Attacker used Process injection (i.e. svchost.exe) technique through which they used legitimate process of system for performing their malicious activity and window API so that they remain

undetected for long time. The IOC of attack strategy is listed for your action.
- Attacker created the task at system logon on victim machine, so that malware execute automatically whenever victim logon the system.

File Location
- C:\ProgramData\{P6A23L1G-A21G-2389-90A1 95812L5X9AB8}\ruizlfjkex.exe
- C:\ProgramData\yyyyyyyyiu\kthbnvx-madh.dat -- CredTheft Module
- C:\ProgramData\yyyyyyyyiu\qitradn-bmxh.dat -- C2 Config
- C:\ProgramData\yyyyyyyyiu\thrfacx-vby.dat -- Webinject Config
- C:\ProgramData\yyyyyyyyiu\etfakdexa-li.dat -- Reporting Config
- C:\ProgramData\yyyyyyyyiu\poqwhg-chat.dat -- VNC Module
- C:\ProgramData\yyyyyyyyiu\ltoefa-caky.dat -- Proxy Module
- Task Name: {Q6B23L1U-A32L-2389-90A1-95812L5X9AB8} is created at system logon

Best Practise and Recommendations
- 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.
- 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
- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- 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.

Cyber Swachhta Kendra

Botnet Cleaning and Malware Analysis Centre

A citizen centric initiative of Government of India for Detecting, notifying, cleaning and securing end user systems infected by malware/botnets

S.S.Sarma
Scientist 'F', ICERT-In, MeitY

Bhupendra Singh Awasya
Scientist 'D', ICERT-In, MeitY

For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India has ushered an increased usage of mobiles/computers in the country, which in turn has translated to a substantial growth in digital transactions in India. Due to the increased presence of users online the threat of online credential stealing from malware infected mobiles/computers has also increased, increasing the instances of cybercrime. It is estimated that a new malware appears every 10 seconds. The consequences of cybercrime inflict a huge burden on society and can potentially be disruptive. This has a direct impact on security thereby having the potential to erode users trust in ICT.

Cyber Security is a key component of Digital India. Cyber Swachhta Kendra (CSK) is an important pillar for creating a secure cyber ecosystem.

The "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. The " Cyber Swachhta Kendra " (Botnet Cleaning and Malware Analysis Centre) is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber eco system in the country.
The centre operates the website https://www.cyberswachhtakendra.gov.in/ which provides information and tools to users to secure their systems/devices. This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.

The "Cyber Swachhta Kendra (CSK)" is a citizen centric cost effective cyber security project implemented in a public private partnership model operated by the Indian Computer Emergency Response Team (CERT-In) as part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY). Its goal is to enhance trust among users in ICT by creating a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. This centre is a multi-stakeholder, collaborative, public private partnership model.

Cyber Swachhta Kendra operates in close coordination and collaboration with Internet Service Providers (ISPs), Product/Antivirus companies and academia thereby facilitating a smooth and productive interaction in terms of guidance, communication and persuasion between the Government and the general public. Currently, 202 organizations from multiple sectors like Telecom (ISPs), Finance,

Transport, Power, Academia, Datacenters and Government are also collaborating and being benefited by using CSK services. Through 123 Internet Service Providers (ISPs) it covers a 90% subscriber base. The Centre provides free bot removal tool, various security tools, security best practices, and information to users to secure their systems/devices while creating cyber security awareness amongst them.

During the year 2018-19, 385 types of botnet/malware were tracked and reported to collaborating ISPs/organizations. Malware/Botnet infections include Bots affecting desktop systems, IoT bots, Ransomware, cryptocurrency miners, information stealing Trojans, banking trojans etc.

Tools and information provided on website:

- Cyber Swachhta Kendra provides various kinds of cyber security information and alerts related to the latest threats and malware targeting desktop, mobiles and devices including WiFi routers, IP camera, home routers, android platform and other Internet of things (IoT) devices, etc.
- The centre provides Security Best Practices for secure digital payments, securing personal computers, broadband routers, mobile phones, etc.
- The website provides Free Bot Removal Tool (FBRT) to enable cleaning of infected computer systems. Free Bot Removal Tool (FBRT) is being regularly updated with signatures/detections for recent botnet/malware observed to enable cleaning of infected systems. Notifications to users are being sent on regular basis with the help of Internet Service Providers (ISPs). Over 8.9 Lakh citizens have benefited from this service so far by downloading the free tools, along with remedial measures so as to clean infections.
- Security tools developed by CDAC are available free of cost for the users namely 'M-Kavach', which is a comprehensive mobile device security solution for Android devices thereby protecting users data and information; 'USB Pratirodh', which securely stores data on USB devices and allows authenticated users to access the data thereby restricting unauthorized access; 'AppSamvid', which allows only approved applications to run on user's computer thus avoiding malicious applications and 'Browser JSGuard' which detects and defends malicious HTML & JavaScript attacks made through the web browser.

Enhancing citizen awareness about information security:

Cyber Swachhta Kendra is helping in raising awareness of citizens about information security through unique way of sending communication to them at individual level through their respective Internet Service Providers. After receiving the message the user appreciates the malware threat is indeed impacting his personal data (including identity theft) and action need to be taken to thwart the same. The Cyber Swachhta Kendra portal helps user in cleaning their systems/devices and also provides best practices to secure their systems while informing the users of the latest malwares in the cyber space and their adverse impacts. In this way the initiative is introducing information about cyber threats and resources to protect user's information there by raising awareness among common users about information security in an innovative manner.

This Centre is also providing free of cost services to organizations from multiple sectors such as Banking and Financial Services, Transport, Power, Government, Academia and Datacenters. The Centre is in continuous contact with respective organisations for sharing automated reports on daily basis comprising of information about systems infected with malware/botnet and systems running with vulnerable services within their organizational network. The information provided by this Centre is found useful by a majority of the organizations and has helped them take necessary remedial actions to strengthen their respective cyber security posture.

Achievements:

- "Cyber Swachhta Kendra" was awarded as one of 51 "Gems of Digital India 2018" in June 2018.
- "Cyber Swachhta Kendra" also awarded "SKOCH Order-of-Merit and Gold Award" for Cost Effective Cyber Security Model in the month of December 2018.
- Users are encouraged to visit the website https://www.cyberswachhtakendra.gov.in/ and explore the information and use the security best practices and free tools to secure their computers and devices.

An Insight of Mirai Botnet

T Sai Gopal
Centre for development of Advanced Computing (C-DAC), Hyderabad

The recent drift of malware targeting IoT devices have increased drastically, with billions of IoT devices such as home appliances, sensors, actuators, and wearable are increasingly connected to the Internet, making them vulnerable targets for the attackers. Gartner estimates IoT devices will reach 20.4 Billion IoT devices by the year 2020. Technology companies are embracing the IoT to seize opportunities in the global market while cybercriminals are exploiting the IoT devices for financial gains and as a result, multiplying and differentiating their tactics. According to the Kaspersky Lab IoT report, IoT malware raised three folds in 2018, and more than 1,20,000 modification of malware attacks were reported. Vulnerabilities in many IoT devices, the ability to connect to other devices and lack of defensive mechanisms lure cybercriminals to exploit and turn them into a bot for illegal activities. All these bots form a network called botnet.

Mirai is a latest botnet that exploits vulnerabilities IP cameras and home routers and turns them into a bot. Mirai malware has carried out a most massive distributed denial of service (DDoS) attacks which has generated 1.2Tbps and infected millions of devices. Many new variants have come up after Mirai source code published on the GitHub. An isolated network was set up and have carried out experiments to get an insight of the Mirai botnet.

Bot

A bot is a malicious/compromised node (IP Camera or any IoT device) in the network. It is a slave node that acts on behalf of the attacker. All bots receive commands from the master (CNC server). Each bot scan for the nearby vulnerable device and report to the report server

Command and Control Center (CNC)
The attacker is one who controls the botnet. Attacker issues command to the bot to perform various types of attack like DDoS attack and flooding the network.

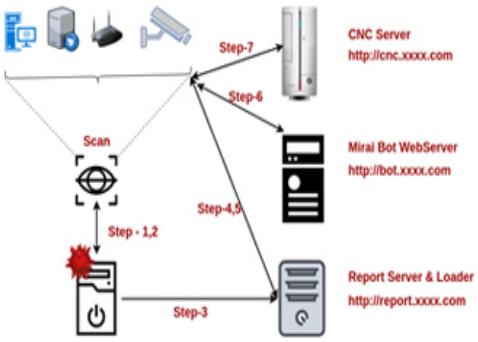
Report Server
It contains information about vulnerable nodes and their stolen login credentials. The bot reports this information if it finds a vulnerable device

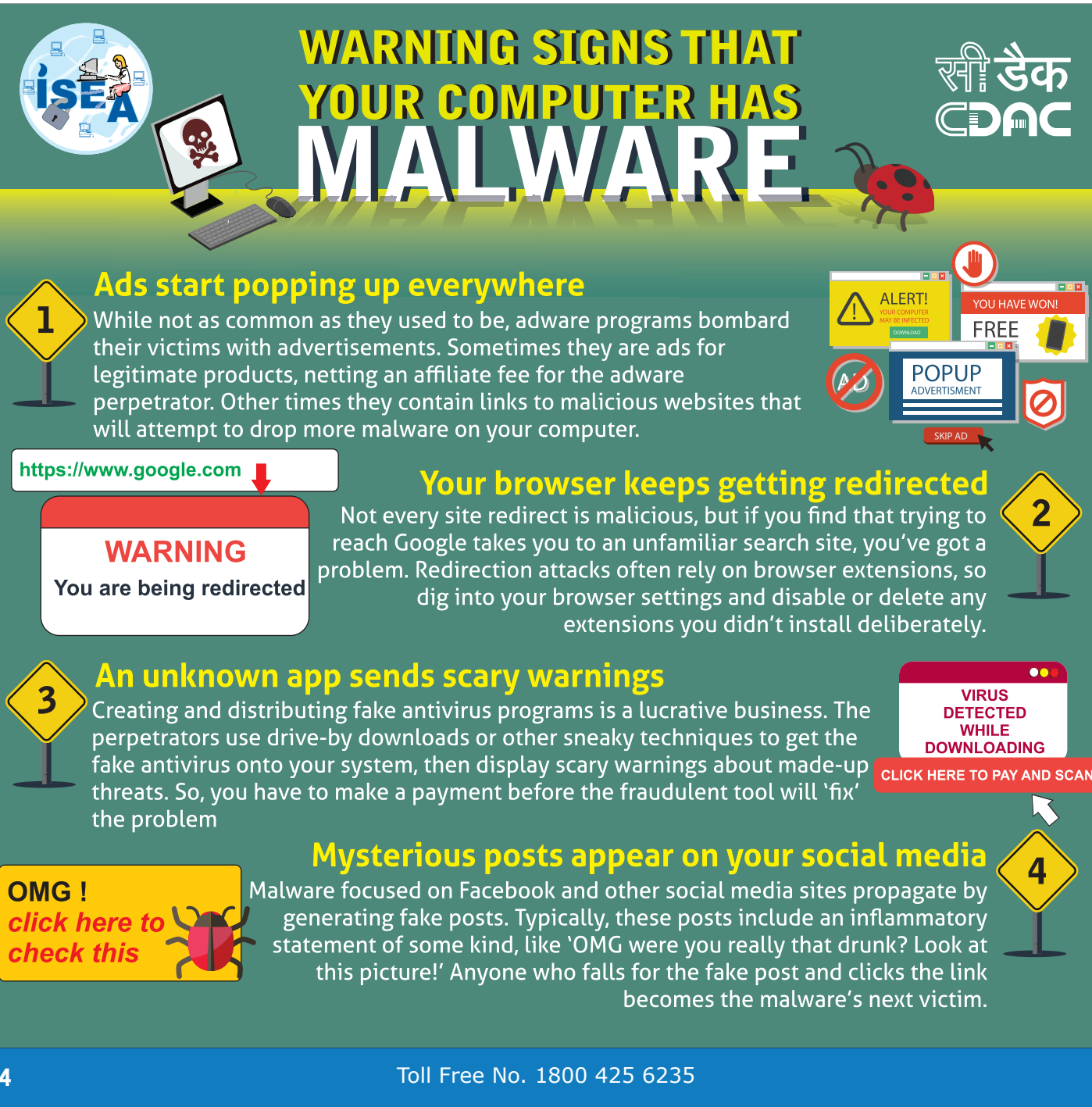
Loader
Loader seeks vulnerable device information from the report server and exploits the node to transform it into a bot.

Web server
Web server hosts precompiled binaries of bots for different architectures.

The diagram depicts the steps in compromising a vulnerable device. Initially, a bot scans for nearby vulnerable devices as shown in step 1. This bot performs login brute force attack with the default factory list of username and passwords of different vendors. If the login attempt is a success, it transmits the information to report server as indicated in step 2 & 3. Loader component exploits the vulnerability and gets the remote shell as shown in step 4 & 5. Subsequently, in step 6, Loader identifies appropriate architecture and downloads the corresponding bot binary from the web server. Upon download, it turns the device into the bot and waits for an instruction from the CNC server as pointed in step 7.

Unfortunately, lack of standardization, public disclosures, comprehensive studies on IoT malware is likely to remain a potential threat.





INFORMATION SECURITY AWARENESS FOR CHILDREN

There is an urgent need to educate the children about the need to be cautious in cyber space. Most of the children only know how to use Internet and are not aware of the dangers associated with it. Children being innocent and ignorant of many dangers of cyber world are a major target for the cyber criminals. This has paved way to the urge in educating the younger generation about cyber hygiene. Keeping this in View Information Security Education & Awareness has made Children as one of the stake holder and has taken many initiatives educating the younger generation in India. Cyber aware kids will help in creating a better India in all aspects fostering the development of the country to a higher level.

Let's have a look at the different initiatives taken under the purview of ISEA programme to create a cyber aware younger generation in India.

1. CBSE has recommended and placed the ISEA weblink in the website of all schools in India for creating awareness among students, teachers and parents.
2. NCERT /CIET have accepted the syllabus suggested by CDAC for adoption/ inclusion into existing ICT curriculum of schools from 3rd standard to 12th standard with an aim to inculcate cyber ethics at an earlier stage.
3. Central institute NCERT provided ISEA and CDAC logo @ www.ictcurriculam.in. Also multimedia awareness content created under ISEA phase II is being uploaded into MHRD's National Repository of Open Educational Resources website www.nroer.gov.in.
4. In view of delivering awareness in direct mode on information security, ISEA has conducted Awareness workshops for children at schools across the country and distributed posters/brochures on cyber security related topics to create awareness among the children.
5. A dedicated portal infosecawareness.in covers the various topics related to cyber security of children. Encourage children to engage themselves in promoting cyber safety.
6. Created a cartoon based handbook 'Cartoon story book for children' based on the issues and dangers generally faced by children.