NEWSLETTER

July 2022

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

CYBER SECURITY GUIDELINES FOR GOVERNMENT EMPLOYEES

DO'S

1. Use Strong Password Policy
2. Keep OS & BIOS Firmware Updated, Use Authorized & Licensed Software only
3. Maintain Offline Backup of Critical Data
4. Ensure Proper Security Hardening is done on the Systems
5. Use Non-Administrator Account for Regular Work
6. Keep GPS, Bluetooth, NFC and other Sensors Disabled on Computers & Mobile Phones
7. Ensure Clean Desk Policy

DONT'S

1. Don't Use Same Password for Multiple Websites
2. Don't Open Link/Attachment from Unknown Sender
3. Don't Plug-in Unauthorized External Devices
4. Don't Allow Internet Access to the Printer & Don't Store its Print History
5. Don't Use External Mobile App Based Scanner for Scanning Internal Government Documents
6. Don't Use Any External Email Services for Official Communication
7. Don't Use External Websites for Converting/Compressing Government Documents

https://nciipc.gov.in/ | @NCIIPC | NCIIPC India | NCIIPC India | helpdesk1@nciipc.gov.in | 1800-11-4430

VOLUME 6 ISSUE 3

@NCIIPC

NCIIPC Newsletter

July 2022

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

NCIIPC Newsletter aims to bring latest news and developments in cyber security of Critical Information Infrastructure. In this regard, a number of developments have taken place during last quarter. This includes, issuing of directives and formulation of robust policy frameworks by both national and international bodies.

All service providers, intermediatory, data centre, body corporates and Government organisations in India have been asked to report cyber incidents within 6 hours of noticing such incidents or being brought to notice about such incidents. Additionally, virtual private server and virtual private network providers have been asked to store customer information for a period of 5 years or more.

In another major development, Securities and Exchange Board of India (SEBI) has introduced certain modifications in the existing cyber security and cyber resilience framework, which has tightened the rules around cyber security for Market Infrastructure Institutions.

Ransomware, Supply Chain Risks and Vulnerable application continue to remain major threats to Critical Sector organisations. NCIIPC along with other agencies have been guiding Critical Sector Organisations to maintain robust cyber hygiene practices. NCIIPC organised a number of cyber security awareness program for capacity development of officials from Critical Sector organisations during the last quarter.

Globally, the European Council and the European Parliament announced provisional agreement aimed to improve cybersecurity and resilience of both private and public sector entities in the European Union. To achieve this goal, it has set minimum rules and laid down mechanisms for effective cooperation among relevant authorities. The United States senate approved strengthening American Cybersecurity Act to increase security of critical infrastructure. This act provides additional authorities to CISA to ensure they are the lead federal agency in charge of responding to cybersecurity incidents on federal civilian networks.

NCIIPC wishes all its readers a very happy Independence Day. For any feedback/suggestions, please do write to us at newsletter@nciipc.gov.in.

News Snippets - National

SEBI Modified Existing Cyber Security Framework

Source: https://www.sebi.gov.in/, https://www.outlookindia.com/

The Securities and Exchange Board of India (SEBI) has made the cyber security framework more robust for Market Infrastructure Institutions (MIIs), which include stock exchanges, depositories, clearing corporations, among others. It has introduced certain modifications in the existing cyber security and cyber resilience framework, which has tightened the rules around cyber security for MIIs. In context of critical assets, SEBI said that MIIs should identify and classify critical assets based on their sensitivity and criticality for business services, operations and data management. Similarly, in the context of vulnerability assessment, SEBI has said that every MII should carry out periodic Vulnerability Assessment and Penetration Testing (VAPT) that includes all critical assets and infrastructure components. This vulnerability tests should be performed at least once in a financial year. MIIs whose systems have been identified as Protected Systems, should conduct VAPT at least twice in a financial year. The vulnerability tests should be conducted by CERT-In empanelled organisations. SEBI has also made it essential for all MIIs to perform a comprehensive cyber audit at least two times in a financial year.

In context of critical assets, SEBI said that MIIs should identify and classify critical assets based on their sensitivity and criticality for business services, operations and data management.

India Reaffirms New Cybersecurity Rules

Source: https://www.cert-in.org.in/

India has reaffirmed its commitment to new cybersecurity rules under a directive from the country's Computer Emergency Response Team, CERT-In. The main features of the cybersecurity directive are as follows:

- All service providers, data centres, and Government organisations are mandated to connect to the Network Time Protocol (NTP) server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks and enable logging of all their ICT systems and maintain them securely for 180 days.
- Virtual private server providers, cloud service providers, and virtual private network (VPN) service providers are mandated to store customer information for a period of 5 years or longer.
- The virtual asset service providers, virtual asset exchange providers and custodian wallet providers are to maintain all information obtained as part of KYC and records of financial

Virtual private server providers, cloud service providers, and virtual private network service (VPN) providers are mandate to store customer information for a period of 5 years or longer.

transactions for a period of 5 years to ensure cyber security in the area of payments and financial markets.

- Cyber incidents are to be reported to CERT-In within 6 hours of noticing such incidents by any service provider, data centre, body corporate and government organisation.

OIL Duliajan Ransomware Attack

Source: timesofindia.indiatimes.com, www.thehindubusinessline.com

Oil India Limited (OIL) headquarters at Duliajan (Assam) was hit by cyberattack on 10 April 2022. A multiagency quick response team including officials from NCIIPC and CERT-In were sent to investigate the incident. The anonymous hackers had demanded a ransom of $7.5 million (57 crore rupees) from OIL to restore the network. OIL spokesperson Tridiv Hazarika said that the drilling and production operations were normally functioning and the communication network was not affected due to the presence of alternate network of computers. He also added that the data was isolated from the infected servers and is safe.

Image source: https://www.oil-india.com/

Recorded Future observed network intrusions that targeted 7 Indian State Load Despatch Centres (SLDCs) responsible for carrying out real-time operations for grid control and electricity dispatch near the disputed India-China border in Ladakh

Hackers Targeted 7 Indian Electricity Grid Centres

Source: https://therecord.media/ https://go.recordedfuture.com/

Recorded Future observed network intrusions that targeted 7 Indian State Load Despatch Centres (SLDCs) responsible for carrying out real-time operations for grid control and electricity dispatch near the disputed India-China border in Ladakh. Recorded Future also reported the compromise of a national emergency response system and the Indian subsidiary of a multinational logistics company by the same threat activity group (TAG- 38). As per report, Shadowpad malware was used for these attacks. However, no conclusive evidences were found to establish any compromise.

Image source: https://en.wikipedia.org/

India, UK Cyberspace Partnership for Vision 2030

Source: https://tele.net.in/, https://www.gov.uk/

India and the United Kingdom have committed to a partnership for vision 2030 for an open, accessible and peaceful cyberspace. Vision 2030 includes revitalised and dynamic connections between people and enhanced defence and security cooperation that brings a more secure Indo-Pacific. Both countries pledged to elaborate under the United Nations

(UN) framework a comprehensive international convention to counter the use by criminals of Information and Communications Technologies (ICTs) in order to increase international cooperation on preventing, deterring, mitigating, investigating and prosecuting cybercrimes, ensuring speedy justice for the victims of cybercrime and taking into account the need for appropriate safeguards including data protection. Both countries are to work closely with industry and through international standard organisations to ensure IoTs connectable devices are secure by design. They will support efforts to increase the availability and diversity of cyber skills in the workforce and promote people-to-people and educational links to enhance awareness in the domain of cyberspace.

Both countries are to work closely with industry and through international standard organisations to ensure IoTs connectable devices are secure by design.

SpiceJet Airline Ransomware Attack

Source: https://www.bleepingcomputer.com/

On 25 May 2022, SpiceJet faced an attempted ransomware attack that impacted some of its systems and caused delays in flight departures. According to the statement posted on the airline's social media channels, its IT team was able to thwart the attack, and operations were back to normal. However, several customers reported on Twitter and Facebook, the problems they faced. Customers reported flight delays, unavailability of customer care service via phone, and the bookings system were unavailable. According to BleepingComputer, only the homepage of SpiceJet was operational while the underlying systems and webpages failed to load. The flight status tables, on the other hand, were available and showed massive delays on all destinations ranging between two to five hours.

Image source: https://twitter.com/

Microsoft Expands its Cybersecurity Training Programme

Source: https://content.techgig.com/

Microsoft has stated that it would expand its cybersecurity skills campaign to an additional 23 countries, including India, with new targeted investments, to close the skills gap in the field of cybersecurity. According to Microsoft, India, along with these countries, has a large cyberthreat risk, as well as a huge gap in their cybersecurity workforces, both in terms of the number of cybersecurity specialists employed vs. demand, and a lack of diversity. Microsoft is also building off their existing Cyber Shiksha programme, which is helping break down the gender divide in the cybersecurity sector.

Indian Data Centres Faced 51 Million Cyber Attacks

Source: https://www.business-standard.com/

The data centres in India have captured more than 51 million cyber attacks over their networks from over 40,000 unique IP addresses from April-December 2021.

The data centres in India have captured more than 51 million cyber-attacks over their networks from over 40,000 unique IP addresses during April-December 2021. A total number of 26,166 usernames and 80,282 passwords were found to be used to log into the networks by attackers. According to research conducted by the Institution of Electronics and Telecommunication Engineers (IETE) and CyberPeace Foundation (CPF) along with Autobot Infosec, attackers attempted to run several terminal commands as well as downloaded malicious payloads into the system. Researchers discovered 1,31,388 unique terminal commands that were run in the system while 1,262 unique payloads have been identified that were injected to the environment.

News Snippets - International

Europe Adopts New NIS2 Directive to Harden Cybersecurity

Source: https://www.consilium.europa.eu/, https://thehackernews.com/

The revised directive NIS2 (Network and Information Systems) aims to remove divergences in cybersecurity requirements and in implementation of cybersecurity measures in different member states.

The European Council and the European Parliament announced a provisional agreement aimed to improve cybersecurity and resilience of both private and public sector entities in the European Union. The revised directive NIS2 (Network and Information Systems) aims to remove divergences in cybersecurity requirements and in implementation of cybersecurity measures in different member states. To achieve this goal, it has set minimum rules for a regulatory framework and laid down mechanisms for effective cooperation among relevant authorities in each member state. It updates the list of sectors and activities related to cybersecurity obligations, and provides remedies and sanctions to ensure the enforcement. A peer-learning mechanism has been introduced to increase mutual trust and learning from good practices and experiences, thereby contributing to achieve a high common level of cybersecurity. The two co-legislators have streamlined the reporting obligations to avoid over-reporting that creates an excessive burden on the entities covered. All member states get a time period of 21 months from the entry into force of the directive to incorporate the provisions into their national law.

A timeline of representative intrusions from this campaign

APT41 Hackers Compromised 6 U.S. State Government Networks

Source: https://www.mandiant.com/resources/apt41-us-state-governments

Mandiant has investigated APT41's activity between May 2021 and February 2022 and has uncovered evidence of a deliberate campaign targeting U.S. state governments. During

this timeframe, APT41 successfully compromised at least six U.S. state government networks through the exploitation of vulnerable Internet facing web applications, often written in ASP.NET. APT41 is quick to adapt and use publicly disclosed vulnerabilities to gain initial access into target networks, while also maintaining existing operations. It has exploited the Log4j vulnerability to compromise at least two U.S. state governments as well as their more traditional targets in the insurance and telecommunications industries, and in late February 2022, APT41 re-compromised two previous U.S. state government victims.

APT41 is quick to adapt and use publicly disclosed vulnerabilities to gain initial access into target networks, while also maintaining existing operations.

Israeli Government Sites Went Offline After Massive DDoS Attack

Source: https://securityaffairs.co/, https://thehackernews.com/

On 15 March, 2022 the Israeli media reported that a massive DDoS attack had taken down many Israel government websites rendering the portals inaccessible for a short period of time. Multiple Israeli ministries were impacted by this DDoS attack, including Health, Interior, Justice, and the Prime Minister's office went temporarily off-line. The Israel defence establishment and their National Cyber Directorate declared a state of emergency, it also worked to determine if the attack caused damages to Israeli critical infrastructure. Later, all of the websites were operational.

Multiple Israeli ministries were impacted by this DDoS attack, including Health, Interior, Justice, and the Prime Minister's office went temporarily off-line.

Google: Hackers are Targeting US Government Gmail Accounts

Source: https://www.binarydefense.com/, https://www.techradar.com/

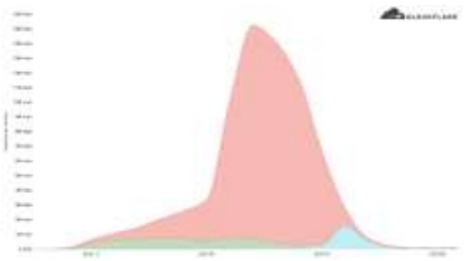
Google's Threat Analysis Group (TAG) warned several Gmail users of being targeted in phishing campaigns performed by APT31 (aka Judgment Panda and Zirconium). The warnings were issued after Gmail's defences automatically blocked the phishing emails. The attacks were launched by the notorious APT31 group and it targeted high-profile Gmail users affiliated with the U.S. government. Google notifies its alerts on government-backed attacks when they are launched via infrastructure associated with government-sponsored threat actors.

Image source: https://www.google.com/

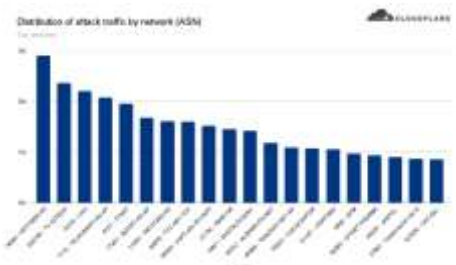
15M rps HTTPS DDoS Attack Blocked by Cloudflare

Source: https://blog.cloudflare.com/15m-rps-ddos-attack/

In the beginning of March 2022 Cloudflare's systems automatically detected and mitigated a 15.3 million request-per-second (rps) DDoS attack. This attack was one of the largest HTTPS DDoS attacks ever recorded. This attack lasted less than 15 seconds and targeted a Cloudflare customer on the Professional (Pro) plan operating a crypto launchpad. This DDoS attack was



The graphical representation of the attack



Distribution of attack traffic by client country

launched from a botnet of approximately 6000 unique bots. It originated from 112 countries around the world. Within those countries, the attack originated from over 1300 different networks. To defend organisations against DDoS attacks Cloudflare has built and operates software-defined systems that run autonomously. In this case, the DDoS attack was automatically detected and mitigated without any human intervention. Cloudflare system perform detection by sampling traffic asynchronously; it then analyses the samples and applies mitigations when needed.

Trends

US Senate Passes Major Cybersecurity Act

Source: https://www.hsgac.senate.gov/, https://www.bitdefender.com/

The United States Senate approved the Strengthening American Cybersecurity Act on 1st March 2022 to increase the security of critical infrastructure in its country. According to the new legislation, critical infrastructure organisations should report ransomware payments within 24 hours to the Cybersecurity and Infrastructure Security Agency (CISA) and cyber incidents to be reported within 72 hours. This new act consists of several measures to strengthen the federal government's cybersecurity infrastructure. It comprises pieces of three different bills:

- Cyber Incident Reporting Act (CIRA)
- Federal Secure Cloud Improvement and Jobs Act (FSCIJA)
- Federal Information Security Management Act (FISMA)

This act provides additional authorities to CISA to ensure they are the lead federal agency in charge of responding to cybersecurity incidents on federal civilian networks. Finally, the package has authorised Federal Risk and Authorisation Management Program (FedRAMP) for five years to ensure federal agencies are able to quickly and securely adopt cloud-based technologies that improve government operations and efficiency.

According to the new legislation, critical infrastructure organisations should report ransomware payments within 24 hours to the Cybersecurity and Infrastructure Security Agency (CISA) and cyber incidents to be reported within 72 hours.

NATO Completes Quantum-proof Network Tests

Source: https://www.ncia.nato.int/, https://www.oodaloop.com/

The NATO Cyber Security Centre (NCSC) has successfully completed its test run of secure communication flows that can withstand attackers using quantum computing. According to Konrad Wrona, principal scientist at the NCSC, the trial started in March 2021 and was completed in early 2022. Quantum computing has now become more affordable, scalable and practical. This means that attackers might adopt this technology to realise their attacks. This project was financed by the Allied Command Transformation's VISTA (Versatile Innovation through Science & Technology Applications) framework. The NCSC

worked with a UK-based company Post-Quantum to conduct this test. Post-Quantum is a company that provides organisations with algorithms that ensure security even if attackers are leveraging quantum computing. This project of NATO is an important milestone in the world's migration to a quantum-safe ecosystem.

This project of NATO is an important milestone in the world's migration to a quantum-safe ecosystem.

Raspberry Pi Made a Big Change to Boost Security

Source: https://www.zdnet.com/

Raspberry Pi has made a change to its operating system Raspberry Pi OS that removes the default username and password to boost security. The default username and password has been respectively "pi" and "raspberry" until now. The default username and password made setting up a new Pi device simple but also potentially made the popular internet-connected devices easier for remote attackers to hack them through techniques like password spraying. The latest release of Raspberry Pi OS removes the default "pi" username and a new wizard forces the user to create a username on the first boot of a newly-flashed Raspberry Pi OS image.

Image source: https://stimuluscheckup.com/

Supply Chain Attack Against macOS

Source: https://www.sentinelone.com/

Researchers have found a supply chain attack via a malicious python package 'pymafka' that was uploaded to the PyPI Registry. Threat actors have used typo-squatting here, victims looking for legitimate 'pykafka' package might mistype the query and download the malware instead. Another similar kind of attack is CrateDepression, a typosquatting against Rust repository that targeted macOS and Linux users. Both attacks have made use of red-teaming tools to drop payload on macOS devices. Further, attackers have used very specific packing and obfuscation method to disguise the true nature of payload. The malicious package 'pymafka' contains a python script that determines operating system of the host. If the running device is macOS then it downloads Mach-O binary called as 'MacOs' and write it to the system. The payload is packed with UPX, a technique to evade certain kind of static scanning tools. Threat hunters are looking for this particular kind of obfuscation technique to detect such attack. For organisations that think Macs as more safer in comparison to window counterparts, these kind of attacks might be a cause for concern.

The setup.py script runs different logic for different platforms, including macOS

The malicious package 'pymafka' contains a python script that determines operating system of the host. If the running device is macOS then it downloads Mach-O binary called as 'MacOs' and write it to the system.

Sample screenshot of the fake checkout form that collects user payment details

The setup.py script runs different logic for different platforms, including macOS

Web Skimmers Injecting Malicious JavaScript Code

Source: https://www.microsoft.com/, https://thehackernews.com/

Threat actors behind web skimming campaigns are using malicious JavaScript codes that mimics Google Analytics and Meta Pixel Scripts to avoid detection. Skimming attacks such as Magecart, is carried out with goal of harvesting and exporting user's payment information such as credit cards details, entered during checkout process. These kind of security vulnerabilities occur due to third-party plugins and use of other tools to inject rogue JavaScript code into online portals without owner's knowledge. In another campaign, malicious actors were observed delivering PHP-based web shells embedded within website favicons to load the skimmer code. Attackers are also inserting JavaScript code within comment blocks and concealing stolen credit card data into images and other files hosted on breached servers. To prevent such kind of attacks user should ensure their browser session are secure during checkout. Also, they can create virtual credit cards to secure their payment details.

Malware Bytes

AvosLocker Ransomware's New Trick to Disable Antivirus

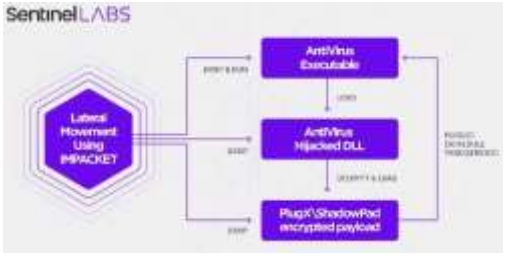
Source: https://thehackernews.com/

Cybersecurity researchers have discovered a new variant of the AvosLocker ransomware that can disable antivirus solutions to evade detection after breaching target networks by taking advantage of their unpatched security flaws. The entry point for the attack is by leveraging an exploit for a remote code execution flaw in Zoho's ManageEngine ADSelfService Plus software (CVE-2021-40539) to run an HTML application (HTA) hosted on a remote server. According to Trend Micro researchers this ransomware has capability to disable a defence solution using a legitimate Avast Anti-Rootkit Driver file (asWarPot.sys). Also, it is capable of scanning multiple endpoints for the Log4j vulnerability (Log4shell) using Nmap NSE script.

According to Trend Micro researchers this ransomware has capability to disable a defence solution using a legitimate Avast Anti-Rootkit Driver file (asWarPot.sys).

Attackers Exploiting Popular Antivirus to Target Telecom Sector

Source: https://www.sentinelone.com/, https://thehackernews.com/



Execution flow of hijacked software as carried out by Moshen Dragon

Cybersecurity firm SentinelOne has discovered a cyberespionage group called Moshen Dragon that has been striking the telecommunication sector in Central Asia with versions of malware such as ShadowPad and PlugX. Moshen Dragon's Tools, Techniques and Procedures (TTPs) involve the abuse of legitimate antivirus software belonging to BitDefender, Kaspersky, McAfee, Symantec, and Trend Micro to sideload ShadowPad and Talisman on compromised systems by using DLL search order hijacking

technique. This hijacked DLL is then used to decrypt and load the final PlugX or ShadowPad payload that reside in the same folder as that of the antivirus executable. Persistence is accomplished by either creating a scheduled task or a service. Once the threat actors have established a foothold in an organisation, they proceed with lateral movement by leveraging Impacket (collection of Python classes for working with network protocols) within the network, placing a passive backdoor into the victim environment, harvesting the credentials to ensure unlimited access, and focusing on data exfiltration.

New Sysrv Botnet Variant Uses Crypto Miners for Hijacking

Source: https://www.bleepingcomputer.com/, https://thehackernews.com/

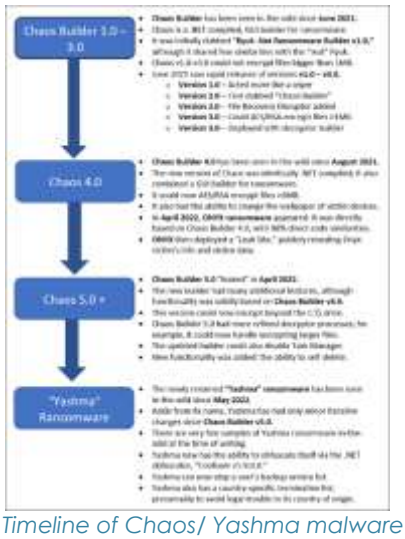
Microsoft has warned of a new variant of the srv botnet called Sysrv-K that is exploiting multiple security vulnerabilities in databases and web applications to install coin miners on both Windows and Linux systems. Sysrv-K botnet scans the Internet in search of web servers with various vulnerabilities to install itself. Once infected, it auto-spreads over the network via brute force attacks using SSH keys available on the infected machine to deploy copies of the malware to other systems and increases the botnet's size, effectively putting the entire network at risk. Sysrv-K fully compromises the Windows and Linux systems using exploits targeting remote code injection or execution vulnerabilities that allow it to execute malicious code remotely.

Microsoft has warned of a new variant of the srv botnet called Sysrv-K that is exploiting multiple security vulnerabilities in databases and web applications to install coin miners on both Windows and Linux systems.

Newly Discovered Chaos Ransomware Builder Variant: Yashma

Source: https://blogs.blackberry.com/, https://www.binarydefense.com/

The BlackBerry Research & Intelligence Team have discovered a new variant of the Chaos ransomware builder in the wild. This new variant is the sixth iteration of the Chaos ransomware. It includes new features like location awareness for execution and terminating various processes prior to encryption. Yashma has the ability to obfuscate itself via a .NET obfuscator known as Confuser v1.9.0.0. Yashma has also the ability to prevent itself from running based on the victim's location that is determined by the language set on the device. This feature was most likely added to avoid legal troubles if devices were encrypted in the threat actor's country of origin. This new version has the ability to stop various services like AV solutions, storage services, vault and backup services, and Remote Desktop services on the victim device.



Timeline of Chaos/ Yashma malware

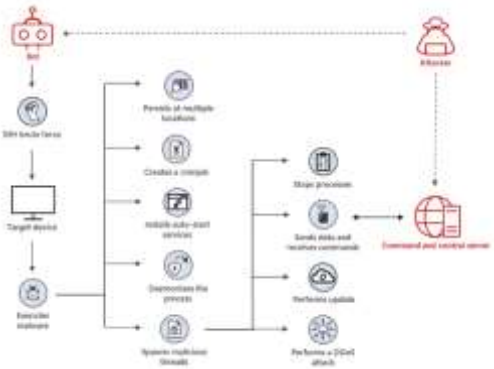
GoodWill ransom note page that explains the group's aim

CloudSEK cybersecurity researchers have dicovered a new ransomware called GoodWill that compels victims into donating for social causes and provide financial assistance to people in need.

New Ransomware Forces Victims to Donate to the Needy

Source: https://cloudsek.com/

CloudSEK cybersecurity researchers have discovered a new ransomware called GoodWill that compels victims into donating for social cause and provide financial assistance to people in need. Once infected, the GoodWill ransomware worm encrypts documents, database, photos, and other important files and renders them inaccessible without the decryption key. The threat actors suggest the victims to perform three socially driven activities in exchange for the decryption key: donate new clothes to the homeless, feed five less fortunate children in Pizza Hut, Dominos, or KFC, and provide financial assistance to anyone who needs urgent medical attention but cannot afford it. The threat actors demand that the victims record each activity and mandatorily post the images, videos, etc. on their social media accounts. On completion of these three tasks, the ransomware operators verify the media files shared by the victim and their posts on social media. The threat actors then share the complete decryption kit which includes the main decryption tool, password file and a video tutorial on how to recover all important files.



A typical attack vector for XorDdos malware

A Stealthy Linux Botnet Malware: XorDdos

Source: https://www.microsoft.com/, https://www.binarydefense.com/

The Microsoft 365 Defender Research Team has observed a 254% increase in the activity of a Distributed Denial of Service (DDoS) oriented Linux trojan known as XorDdos. XorDdos also depicts the trend of malware increasingly targeting Linux-based operating systems, which are commonly deployed on cloud infrastructures and Internet of Things (IoT) devices. XorDdos amasses botnets by compromising IoT and other Internet-connected devices to carry out Distributed Denial-of-Service (DDoS) attacks. XorDdos uses SSH brute force attacks to gain control of remote devices. XorDdos employs evasion and persistence mechanisms to keep its operations robust and stealthy. Its evasion capabilities include obfuscating the malware's activities, evading rule-based detection mechanisms and hash-based malicious file lookup, and using anti-forensic techniques to break process tree-based analysis.

BPFDoor/JustForFun implant detection

BPFDoor Malware Exploits Solaris Vulnerability

Source: https://www.bleepingcomputer.com/, https://www.crowdstrike.com/

According to CrowdStrike researchers BPFDoor or JustForFun malware was developed by threat actor DecisiveArchitect to exploit a three-year-old vulnerability, CVE-2019-3010, in the XScreenSaver component of Solaris operating system to gain root-

level permissions. DecisiveArchitect has updated its tactics, techniques, and procedures and now uses the LD_PRELOAD environmental variable to facilitate Linux system attacks, as well as it loads the BPFDoor/JustForFun implant within the /sbin/agetty process. Threat actor DecisiveArchitect have used a custom implant that is typically persisted by using SysVinit scripts. When executed, the implant overwrites the process command line within the process environment by randomly selecting a new command line from one of its ten hard-coded options. The researchers have also noted that detecting BPFDoor/JustForFun implants on a Linux system can be very difficult as the threat actor modifies existing SysVinit scripts on the host to achieve persistence. To make it even more difficult to spot the implants, the file names and paths for the implant and associated persistence-related scripts are different from one system to another.

DecisiveArchitect has updated its tactics, techniques, and procedures and now uses the LD_PRELOAD environmental variable to facilitate Linux system attacks, as well as it loads the BPFDoor/JustForFun implant within the /sbin/agetty process.

Twisted Panda: Espionage Operation Against Defence Institutes

Source: https://research.checkpoint.com/

Check Point researchers have observed multiple APT groups attempting to leverage the Russia and Ukraine war as a lure for espionage operations. It has discovered a targeted campaign against at least two research institutes in Russia, whose primary expertise is research and development of highly technological defence solutions. This campaign, named as Twisted Panda, seemed to be a continuation of what Check Point researchers believes to be a long-running espionage operation since June 2021. The operation could still be ongoing, since recent activity observed was in April 2022. The suspected threat actors behind this espionage are Stone Panda (aka APT10), and Mustang Panda. The tools used by threat actors are sophisticated multi-layered loader and a backdoor dubbed SPINNER. These tools use advanced evasion and anti-analysis techniques such as multi-layer in-memory loaders and compiler-level obfuscations.

Screenshot of the lure document sent to research institutions in Russia

RagnarLocker Ransomware Targeting Critical Infrastructure

Source: https://www.acronis.com/en-us/blog/posts/ragnar-locker/

RagnarLocker ransomware is actively targeting critical infrastructure entities. According to a report 52 entites of different critical sectors have been identified as its victim. It begins its attack by compromising organisation's network via RDP service, using brute force to guess weak passwords or with stolen credentials. To elevate privileges, attacker further exploits CVE-2017-0213 vulnerability in Windows COM Aggregate Marshaler to run arbitrary code. Attacker deploys a VirtualBox Virtual Machine (VM) with a Window XP image to evade detection. This specially-crafted VM image is mapped with all local drives as read/write into the virtual

Before Launching ransomware, attacker steals sensitive files and uploads them to one or more server to publish if victim refuses to pay ransom.

machine. This allows ransomware process running inside the VM to encrypt all files without getting detected by security products. Before Launching ransomware, attacker steals sensitive files and uploads them to one or more server to publish, if victim refuses to pay ransom. For obfuscation, attackers have included junk code as well as encryption. The payload PE files .keys section contains the crypto keys and obfuscated string. It uses hardcoded obfuscated strings which decrypts during runtime. This ransomware also deletes volume shadow copies on the compromised machine.

Attacker establishing their cover identity via email

Link to TransferNow to download the malware

BazarBackdoor Malware Spreading via Website Contact Forms

Source: https://www.bleepingcomputer.com/, https://abnormalsecurity.com/

The BazarBackdoor malware is now spreading via website contact forms in place of phishing email to evade detection by security software. It is a stealthy malware created by Trickbot group and now under development by Conti Ransomware operation. Malware provides remote access of internal device to threat actors that can be used for further lateral movement inside the network. In its latest campaigns, instead of sending phishing emails to the targets, threat actor first used corporate contact forms to initiate communication. After receiving response from the employee, attacker sends a malicious ISO file using sharing services like TransferNow or WeTransfer. The ISO archive contains a .lnk file and .log file. To evade Antivirus detection, payload is packed in the archive. The .lnk file contains a command instruction that opens a terminal window using existing windows binaries and loads the BazarBackdoor DLL. When backdoor is loaded it is injected into the svchost.exe process and then it contacts C2 server to receive commands for execution.

Korplug's loading chain (ESET)

Mustang Panda deploying New 'Hodur' Malware

Source: https://www.bleepingcomputer.com/

Mustang Panda, threat actor aka TA416, is known for phishing and espionage operations against European diplomats, ISPs and research institutes. In its latest campaign, it is using new variant of Korplug malware called Hodur and custom loaders. The targeted countries in this campaign are Russia, Greece, Cyprus, South Africa, Vietnam, Mongolia, Myanmar, and South Sudan. It uses DLL side-loading with heavier obfuscation. The malicious module and encrypted Korplug payload are downloaded along with decoy document and legitimate executable. Custom DLL loader leverages digitally-signed legitimate executable, in this case SmadAV file exploits known vulnerability for side-loading. Korplug payloads are decrypted in memory, only encrypted form is written to the disk. Persistence is achieved by creating a new registry

entry. The new created directories that contain malware components are marked as 'hidden' and 'system'.

Operation Dragon Castling Abusing CVE-2022-24934 Vulnerability

Source: https://decoded.avast.io/

Operation Dragon Castling targeted betting companies in South East Asia. Attackers have abused CVE-2022-24934 vulnerability of WPS Office updater. To exploit the vulnerability, a registry key under HKEY_CURRENT_USER needs to be modified, by doing this attacker gains persistence on the system and control over the update process. Multiple infection vectors have been used in this campaign. Multi-stage infection chain leads to the deployment of intermediate payloads allowing for privilege escalation before dropping the Proto8 module. Proto8 is a plug-in based system used to extend its functionality, enables the malware to achieve persistence, bypass user account control (UAC) mechanisms, create new backdoors and execute arbitrary commands on the infected system.

Multi-stage infection chain leads to the deployment of intermediate payloads allowing for privilege escalation before dropping the Proto8 module.

Micropsia Malware Uses Public Code from Github Libraries

Source: https://www.deepinstinct.com/

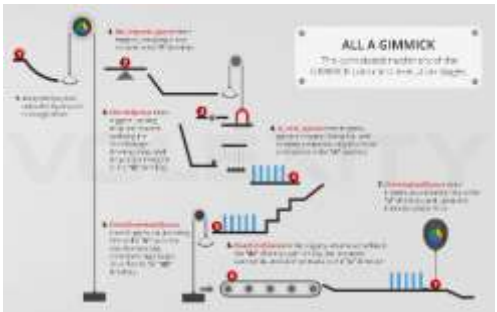
A new variant of the Micropsia malware family written in Go, known as Arid Gopher has been observed. It contains public code from libraries in Github. These libraries are not malicious, but the malware author abuses the libraries capabilities. This new variant of malware is still under development. Beside this main implant, threat actor also discovered a 'helper' malware written in Go and a second-stage malware which has been downloaded from the C2 server. To lure victims, threat actor masquerade exe using MS office document icon and with a very long filename to prevent user from seeing .exe file extension. The malware creates a LNK file and copies it to the startup folder for persistence using malware executable name. Malware is capable of taking screenshots, executing arbitrary commands, check for installed Antivirus products by running WMI query.

The malware creates a LNK file and copies it to the startup folder for persistence using malware executable name.

Gimmick macOS Implant Developed by APT Storm Cloud

Source: https://www.volexity.com/

Gimmick, a newly discovered macOS implant developed by the APT Storm Cloud is used to target organisations across Asia. Researchers have also discovered Windows versions of the same implant during the past. The macOS version of the implant is written in Objective C while the windows implant is written in .Net and Delphi. The implant uses public cloud hosting services such as



The GIMMICK workflow

Google Drive for C2 to evade detection. During analysis it was found that implant is used by rotating addition algorithm. The most important thing about GIMMICK is its adaptability. It is configured to only communicate with Google Drive-based C2 server on working days in order to mix itself within network traffic of target environment. It installs itself as a launch agent by dropping as a PLIST file with contents.

Encoded Royal Road payload

TA410 Cyberespionage Umbrella Group

Source: https://www.welivesecurity.com/

TA410 is a cyberespionage umbrella group linked with APT10 known for targeting US-based organisations in the utilities sector and diplomatic organisations in the Middle East and Africa. It comprises of FlowingFrog, LookingFrog and JollyFrog each with its toolset and targets. FlowingFrog uses Royal Road RTF documents, a first-stage implant called Tendyron and a complex second-stage backdoor called FlowCloud. LookingFrog uses X4 as a first-stage backdoor and LookBack as second stage. JollyFrog uses generic malware families such as Korplug and QuasarRAT. Attackers behind these group have used Microsoft Exchange Remote Code Exceution vulnerabilities e.g., ProxyLogon and ProxyShell. FlowCloud implant used by threat actor is a complex and modular C++ RAT. It has the capability of controlling connected microphones and triggering recording when sound volume is above a specified threshold volume, monitoring clipboard events to steal clipboard content, monitoring file systems events to collect new and modified files, controlling attached camera devices etc. FlowCloud also have capability to deploy a rootkit to hide its activity on the compromised machine.

FlowingFrog uses Royal Road RTF documents, a first-stage implant called Tendyron and a complex second-stage backdoor called FlowCloud.

Indian Websites Hacked by DragonForce Hackers

Source: https://cloudsek.com/, https://www.news9live.com/

A hacker group called DragonForce has reportedly carried out cyberattacks on several Indian websites belonging to prominent government and private institutions across the country. The hacker group also leaked the hacked contents in their various social media channels, the group also posted on Pastebin, AnonFiles and Google Drive. As per reports, the group was not skilled enough to conduct sophisticated and largescale DDoS attacks. However, the DoS tools they suggest are effective when leveraged against unprotected assets. The tools like LOIC, HOIC, HULK, DDoSIM, PyLoris, OWASP HTTP Post, RUDY, Torshammer, Davoset, GoldenEye, Garuda were used by the hacker group.

Sample ransom note shared by DragonForce to substantiate their plans of converting to a ransomware group

Guest Article

VPNFilter: A Destructive Router Malware

Sajal Sarkar, Chief Manager, Power Grid Corporation of India Ltd, Gurgaon

Sajal Sarkar is working as a Chief Manager in area of information/cyber security at Power Grid Corporation of India Limited. He was a Post-Doctoral Researcher and he has worked on Cybersecurity in Power System Automation at School of Computing, National University of Singapore. He received his PhD from IIT Kharagpur. He obtained his MTech and BTech both in IT. Dr. Sarkar has in his credit a number of publications in Conferences and Journals.

A threat in the name of VPNFilter malware first appeared in May 2018. The malware targets a range of routers (such as Asus, D-Link, Huawei, Linksys, MikroTik, Netgear, TP-Link, Ubiquiti, Upvel, and ZTE) and network-attached storage (NAS) devices. It is capable of knocking out infected devices by rendering them unusable. The estimated number of infected devices were between 500,000 to 1000,000 in at least 54 countries worldwide. The malware is unlike most other malware because it is capable to maintain a persistent presence on an infected device, even after a reboot. It has capabilities of scanning and spying traffic as well as stealing data being routed through the devices as well as it attempts indiscriminately to infect other vulnerable devices across the systems. It also possesses a kill switch to destroy the infected device. It seems to have a particular target in Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS) by creating a module for intercepting Modbus protocol, an industrial communication protocol used in critical sectors.

How it Works?: The way VPNFilter malware works is admittedly remarkable in its sophistication. It is a multi-staged piece of malware and it can infect different types of routers. However, it seems that malware specifically target devices, which are specifically configured with Modbus protocol. The malware uses default credentials to infect others and install itself in the devices in multiple stages as described below:
In Stage 1, the malware in form of worm is installed inside a task scheduler and then it is used to maintain a persistent presence on the infected device. The installed worm will contact a command and control (C&C) server to download other modules of the malware. Stage 2 contains the main payload and it is capable of command execution, file collection, data exfiltration, and device management. It also has the capability to make a device unusable by destroying its firmware by executing a command from the C&C server remotely. The malware simply overwrites the device's firmware and reboots and eventually it renders the device unusable. Finally, it removes all evidence from the devices. Stage 3 has several modules, which act as plugins for Stage 2. The modules include a packet sniffer for spying on traffic that is routed through the device, including theft of website credentials and monitoring of Modbus protocol. Another special module in Stage 3 allows Stage 2 to communicate using Tor. There are few other modules of Stage 3 such as ssler, dstr, htpx, ndbr, nm, netfilter, portforwarding, socks5proxy, tcpvpn, and netfilter which are published subsequently for exploitation. The tcpvpn module allows to connect and access internal devices behind the infected and

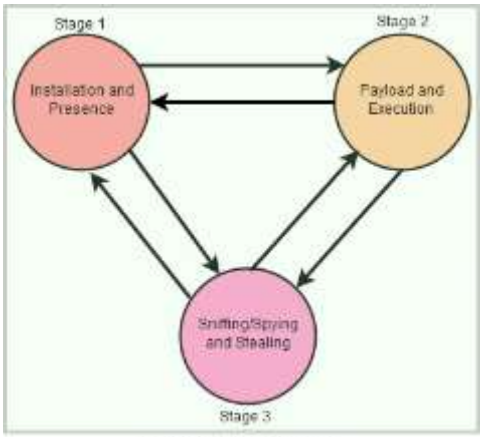


Figure 1: Stages of VPNFilter

compromised devices.

Potential Impact of Malware: The most destructive effect of the malware is that the attacker can issue the kill switch command to make the infected devices unusable and in turn disrupt network connections of the device. Thus, the potential impact is to disrupt the functionality of the device as well as the network by bricking a large number of infected devices. Finally, it uses infected devices to build a compromised network to attack others monitoring the network traffic flowing through the infected devices or using the infected devices as jumping board to reach their targets.

Persistence of the Malware: The VPNFilter malware is very persistent in nature. Rebooting of the infected device will remove Stage 2 and any Stage 3 modules of destructive component present on the device temporarily. However, if a device is infected, the Stage 1 is present in the device. So, the continuing presence of Stage 1 means that Stages 2 and 3 can be reinstalled.

How to Protect Yourself?: Restarting/rebooting of the infected devices may temporarily disrupt the effect of malware. However, in order to make the infected device malware free, a factory reset is required to be done. As a good practice, the management settings of such devices should be changed and the default credentials must be replaced with strong password after enabling encryption. The devices should be updated with latest version of firmware as and when released. The administration password should be changed periodically. To minimise the risks of VPNFilter malware infection or impact, the following practices may also be followed:

- Backup of the system and its current configurations.
- Disabling remote access to the router and administration console.
- Apply security patches immediately after release by the device vendors.
- Apply Snort rules or Indicator of Compromise (IOC) in firewall or IPS.
- Monitor network communication logs using System Information and Event Management (SIEM) tool.

The most destructive effect of the malware is that the attacker can issue the kill switch command to make the infected devices unusable and in turn disrupt network connections of the device.

References:

[1] VPNFilter state-affiliated malware pose lethal threat to routers". SlashGear. 2018-05-24. Retrieved 2018-05-31. [Accessed 22 05 2022].

[2] VPNFilter: New Router Malware with Destructive Capabilities". Retrieved 2018-05-31 [Accessed 22 05 2022].

Learning

Protecting Managed Service Providers and Customers Against Cyber Threats

Source: https://www.cisa.gov/uscert/ncas/alerts/aa22-131a

An increase in cyber threat activity targeting Managed Service Providers (MSPs) and their customers has been observed. Organisations should pursue best practices for Information and Communications Technology (ICT) services and functions, focusing on guidance that enables transparency between MSPs and their customers on securing sensitive data.

Organisations should pursue best practices for Information and Communications Technology (ICT) services and functions, focusing on guidance that enables transparency between MSPs and their customers on securing sensitive data.

Recommendations:

- Implement and maintain a logging functionality to detect threats in network.
- Network should be segregated according to internal architecture.
- Organisations should apply principle of least privilege through the network environment.
- Organisations should audit network infrastructure on regular basis to identify and disable unused system and services.
- Take backups regularly and store separately offline, isolating from network.
- Maintain up-to-date hard copies of incident response and recovery plans to ensure responders can access them incase network is inaccessible.
- It is important to understand and proactively manage ICT supply chain risk using risk assessments to identify and prioritise the allocation of resources.
- All organisations should adhere to the best practices for password and permission management.

APT Custom Tools Targets ICS/SCADA Devices

Source: https://www.mandiant.com/, https://www.cisa.gov/

In a Joint advisory released by multiple organisations have warned that certain APT actors have capability to gain full system access of multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices. APT actors have developed custom-made tools for targeting ICS/SCADA devices.

APT actors have developed custom-made tools for targeting ICS/SCADA devices.

Mitigations:

- Proper Segmentation of IT and OT networks is necessary to prevent attackers pivoting from corporate network to industrial environments.
- Implementation of industrial firewall with deep packet inspection helps in controlling access.

- Implementation of ICS-Aware Intrusion Protection Systems to monitor function codes from malicious sources.
- Monitor and block external traffic to OPC UA ports.
- Enabling and aggregating audit logs for OPC servers and clients.
- Periodic review of audit logs for inconsistent connections, security options negotiations, configuration changes and user interaction.
- Enforce Principle of least privilege.
- Enforce multifactor authentication for all remote access to ICS networks and devices.

Understanding DDoS Protection Options

Source: https://www.infosecurity-magazine.com/

Before applying DDoS security vendors it is necessary to understand the topology, advantage and disadvantage of different protection options and type of DDoS attacks that can be blocked.

A DDoS attack is a complex threat for business. Before applying DDoS security solutions it is necessary to understand the topology, advantage and disadvantage of different protection options and type of DDoS attacks that can be blocked. Five different locations for DDoS threat mitigation tools to be deployed:

On-Premises: On Premises, DDoS Protection consists of dedicated hardware appliance or an on-premise web application firewall (WAF) installed in the data centre. It allows to protect against layer3, layer4 network attacks and against application-level attacks.

ISPs: Many internet service providers (ISPs) provide DDoS protection for business. But this option covers only network layer vulnerabilities and does not protect against application-level attacks.

Cloud WAFs: With increase in the cloud-based services, DDoS protection solutions have gained popularity over on-premises alternatives. Cloud-based DDoS protection is based on companies offering CDN and cloud WAF solutions, including DDoS mitigation layer.

Scrubbing Centre: A DDoS scrubbing centre holds DDoS mitigation equipment to handle large network attacks. During an attack, traffic is diverted to the closest centre and analysed.

Mitigate Ransomware Attack on OT Devices

Source: https://www.infosecurity-magazine.com/

Security Team must have visibility across all connected devices. Having consistent visibility is the most critical foundation of industrial cybersecurity.

Ransomware has become the most concerning threat in today's attack landscape. Industrial organisations that provide essential services to society are prime target for such attackers. Key aspects to mitigate ransomware attack on OT devices:

Increase OT network visibility: Security Team must have visibility across all connected devices. Having consistent visibility is the

most critical function of industrial cybersecurity.

Patch what can be patched, segment what can't be patched: Maintaining a regular patch management strategy is necessary. Keep IT systems up to date with patches and apply patches to OT wherever possible. If mission-critical systems are too old to be patched or can't be taken offline to apply patch, segment it from other network areas.

Maintaining a regular patch management strategy is necessary. Keep IT systems up to date with patches and apply patches to OT wherever possible.

Boost Incident Response capabilities: Understanding weaknesses and minimising them through incident response training is important step in ransomware defences.

Nurture a security-conscious culture: Staff must be trained on the dangers of threats and attacker techniques. As most of the ransomware attacks are propagated through user-initiated actions such as clicking on malicious links or opening malicious attachments in email.

Zero Trust Helps Organisations in Detecting, Responding and Recovering from Attacks

Source: https://threatpost.com/zero-trust-for-data/179706/

Zero trust principles help organisations in improving their security risks. There are few practical ways that can be taken to eliminate risks. The National Institute of Regulations and Technology (NIST), has released a number of cloud security standards. Federal Information Security Management Act (FISMA) is also a great reference point. The NIST's zero trust model incorporates following framework:

Zero trust principles help organisations in improving their security risks. There are few practical ways that can be taken to eliminate risks.

Visibility into Security Posture: Organisations having visibility into their data security posture are able to determine and set policies for enhanced data protection. Data Security Posture Management (DSPM) tools are a good starting point for Zero Trust.

Detection-Response: Many Critical identities and service roles needs permission to perform their job– privileged identities, applications that are fronts for databases or data lakes and Continuous Integration/Continuous Delivery (CI/CD) etc. Using detection and response protects data objects from phishing or misuse.

Protection: Organisations should create permission and entitlements, a set up to proactively prepared that respond to detected cybersecurity incidents.

Browser-in-the-browser Attack

South Zone, NCIIPC

Understanding Browser-in-the-browser Attack: Normally, the measures taken by a user to detect a phishing site include

checking to verify if the URL is legitimate, whether the website is using HTTPS, and if there is any type of homograph used in the domain, etc. In case of browser in the browser attack, everything looks fine as the domain is familiar, looks legitimate and is using HTTPS. However, as soon as it is attempted to move this prompt from the currently used window, it vanishes beyond the edge of the window because it is not a genuine browser pop-up and is formed using HTML in the present window. This being a routine thing these days, users would not contemplate much before jumping in to authenticate via one of these apps.

In case of browser in the browser attack, everything looks fine as the domain is familiar, looks legitimate and is using HTTPS.

How BITB attack works: Here the attacker completely fabricates malicious version of the pop-up window, which is essentially a snap, using basic HTML/ CSS. The popups so invented simulate a browser window within the browser and spoof domains that look like authentic domains and make it conceivable to stage substantial phishing attacks. If this window design is clubbed with an iframe pointing to the malicious server which is hosting the page intending to carry out phishing attack, it becomes indistinguishable. These slight differences are rarely noticed by users. A window can be made to appear on a link, button click or page loading screen using Javascript. The prevalent libraries like JQuery Java Script Library are capable of making the windows visually appealing or authentic.

It is very difficult to identify which is real and which is fake because the attackers easily use JavaScript to make the window appear on a link or button click, on the page loading etc.

It is very difficult to identify which is real and which is fake because the attackers easily use JavaScript to make the window appear on a link or button click, on the page loading etc. One can actually make the window appear in a visually authentic manner through various animations tools existing in libraries such as JQuery. An example is shown in the diagram.

Javascript when used effectively can fool those users who hover over the URL without clicking it to find out if it is legitimate or not, making this safety guard ineffective. When the onclick event is designed to return a false, the URL would continue to look like the website in the href attribute. However, when the link is clicked then the href attribute is ignored. This feature is exploited to make convincing or realistic fake authentication windows. In this way bitb renders both the https and hove-over-it security checks ineffective.

Javascript when used effectively can fool those users who hover over the URL without clicking it to find out if it is legitimate or not, making this safety guard ineffective.

How to identify BITB attacker's website?: If the users are careful and observe the usual pattern of sign-in options, there is one important factor to raise alarm or suspicion in the minds of the users. Usually when we sign-in the password managers would not auto fill a fake login pop-up window because the user's software may not interpret that window as a real browser window. However, if the attacker manages to get the user ignore these important indications, in no time, users will redelegate the Multi-Factor Authentication (MFA) to a single factor as they have given

away the password. Two factor authentications with username and password are much more vulnerable to these attacks. With attackers looking for sophisticated methods, going for password-less MFA is more critical now than before.

People working in cyber security profession, usually assume that the URL is typically the most reliable aspect of a domain. Even though cyberattacks like IDN Homograph and DNS Hijacking might have degraded the trustworthiness of URLs but it is not to an extent of total unreliability. The image in figure-1 shows the window that appears when someone attempts to login to Canva using their Google account. completely fabricating a malicious version of a popup window is a snap. JavaScript can make the window appear on a link, button click or page loading screen

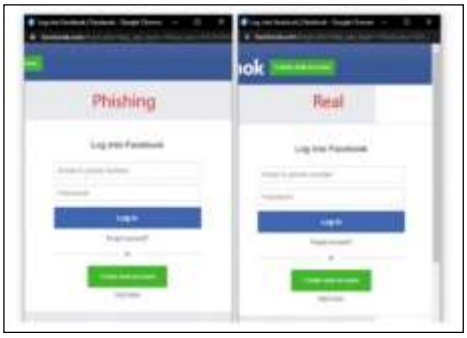


Figure-1
Image source: https://evabssi.com/

Recommendations to Prevent BITB Attack: It may not be a permanent solution to stop using the SSO feature altogether to prevent browser in the browser attack as the internet users are used to it. In most cases it has been harmless so far. The following measures could be taken to prevent BITB attack

- Multi-factor authentication (MFA) is still a better way to improve security for SSO authentication, though it has the risk of getting bypassed by attackers, with malware
- Use of password managers is the practical solutions
- Users should not click on links or attached files coming from unknown sources via email or instant messaging software. If they have doubts about an email coming from a seemingly legitimate entity or colleague, the user should call and verify they were indeed the sender and that the shared link or file is safe.
- Anti-phishing solutions should also be deployed and used.
- BITB is a plausible attack vector. The attacker usually would create an ad that has a JS payload.

It may not be a permanent solution to stop using the SSO feature altogether to prevent browser in the browser attack as the internet users are used to it.

Conclusion: The fact that just checking URL credibility doesn't guarantee security is known for a long time in context of URLs created with characters looking alike like in homograph attacks, imitating genuine URLs but malicious in nature, hijacking DNS itself to sabotage the queries. This different coding trick or technique which isn't visible to normal internet users used to extract sensitive information can be described as BITB attack. The vulnerability here is the third-party sign-in options with single-sign-in, some of the websites give with pop-up windows with Google or apple or Microsoft.

The fact that just checking URL credibility doesn't guarantee security is known for a long time in context of URLs created with characters looking alike like in homograph attacks, imitating genuine URLs but malicious in nature, hijacking DNS itself to sabotage the queries.

References:

[1] https://www.theregister.com/2022/03/18/browser_in_browser_phishing/
[2] https://cyware.com/news/browser-in-the-browser-an-almost-invisible-attack-c009e043
[3] https://cyware.com/cyber-security-news-articles

Vulnerability Watch

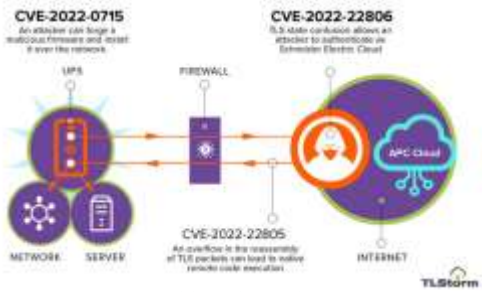
Google Cloud Armor deployment modes Image source: https://storage.googleapis.com/

Researchers found that it is possible to bypass both Google Cloud Platform (GCP) and Amazon Web Services (AWS) web app firewalls just by making a POST request more than 8 KB in size.

Google WAF Bypassed via Oversized POST Requests

Source: https://portswigger.net/

Some security flaws have been discovered in the default protection offered by Google's Web Application Firewall (WAF) which allow attackers to bypass the company's cloud-based defenses. Researchers found that it is possible to bypass both Google Cloud Platform (GCP) and Amazon Web Services (AWS) web app firewalls just by making a POST request more than 8 KB in size. WAFs are supposed to protect against web-based attacks including SQL Injection and Cross-site Scripting, even in cases where an underlying application is still vulnerable. Bypassing this protection would take a potential threat actor one step closer to attacking a web-hosted application. The default behavior of Cloud Armor can allow malicious requests to bypass Cloud Armor and directly reach an underlying application. This vulnerability can be exploited by crafting an HTTP POST request with a body size exceeding the 8KB size limitation of Cloud Armor, where the payload appears after the 8192th byte/character in the request body.



The three critical flaws in TLStorm

Critical Flaws Let Attackers Hack, Damage APC Smart-UPS Devices

Source: https://thehackernews.com/

Multiple high-impact security vulnerabilities have been discovered in APC Smart-UPS devices that could be abused by remote attackers to access and control them in an unauthorised manner. Most of the affected devices that have been identified so far are in healthcare, retail, industrial, and other government sectors. These flaws collectively dubbed as TLStorm which consists of a trio of critical flaws CVE-2022-22805 (CVSSv3 score: 9.8), CVE-2022-22806 (CVSSv3 score: 9.8) and CVE-2022-0715 (CVSS score: 9.1). These vulnerabilities can be triggered via unauthenticated network packets without requiring any user interaction, meaning it's a zero-click attack. Successful exploitation of any of the flaws could result in Remote Code Execution (RCE) attacks on vulnerable devices. Organisations are recommended to install the updates provided to reduce the risk.

Image source: https://deno.land/

Vulnerability in Deno

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-24783

It has been observed that the versions of Deno between release 1.18.0 and 1.20.2 (inclusive) are vulnerable to Improper Privilege Management vulnerability CVE-2022-24783 (CVSSv3 score: 10). Deno is a runtime for JavaScript and TypeScript. A malicious actor

controlling the code executed in a Deno runtime could bypass all permission checks and execute arbitrary shell code. Users of Deno Deploy are not affected by this vulnerability. The vulnerability has been patched in Deno 1.20.3. All users are recommended to upgrade to 1.20.3 immediately.

Vulnerability in Genian NAC

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-26622

A Remote Code Execution (RCE) vulnerability due to Server-Side Template Injection (SSTI) vulnerability and insufficient file name parameter validation was discovered in Genian NAC. Remote attackers are able to execute arbitrary malicious code with SYSTEM privileges on all connected nodes in NAC through this vulnerability.

Image source: https://www.genians.com/

Vulnerability in Parse Server

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-24760

A Remote Code Execution (RCE) vulnerability CVE-2022-24760 (CVSSv3 score: 10) has been discovered in Parse Server versions prior to 4.10.7. Parse Server is an open source http web server backend. This vulnerability affects Parse Server in the default configuration with MongoDB. The main weakness that leads to RCE is the Prototype Pollution vulnerable code in the file `DatabaseController.js`, so it is likely to affect Postgres and any other database in backend as well. This vulnerability has been confirmed on Linux (Ubuntu) and Windows. Users are advised to upgrade as soon as possible. The only known workaround is to manually patch your installation with code referenced at the source GHSA-p6h4-93qp-jhcm.

Image source: https://parseplatform.org/

This vulnerability affects Parse Server in the default configuration with MongoDB.

Vulnerability in Spring Cloud Gateway

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-22947

In spring cloud gateway versions prior to 3.1.1+ and 3.0.7+, applications are vulnerable to a code injection attack (CVE-2022-22947) when the Gateway Actuator endpoint is enabled, exposed and unsecured. A remote attacker could make a maliciously crafted request that could allow arbitrary remote execution on the remote host.

Image source: https://spring.io/

Researchers Hack Remote Keyless System of Honda Vehicles

Source: https://www.bleepingcomputer.com/

A 'replay attack' vulnerability (CVE-2022-27254 CVSSv3 score 5.3) has been discovered that can be used by nearby hackers to

Image source: https://media.wired.com/

unlock some Honda and Acura car models and start their engines wirelessly. The vulnerability is a Man-in-the-Middle (MitM) attack, in which an attacker intercepts the RF signals normally sent from a remote key fob to the car. Attackers can manipulate these signals, and re-sends these at a later time to unlock the car at will. According to the researcher, attacks can be prevented if users refrain from using their RF fobs and if Honda implements a 'rolling code' system, where a new code is generated each time the user presses the button on their fob, thus offering a more secure authentication system.

This vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management.

Vulnerability in Oracle Product

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-21431

A vulnerability has been discovered in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications. The affected component is Connection Manager. Supported versions that are affected are 12.0.0.4 and 12.0.0.5. This vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management.

Image source: https://www.swiftsensors.com/

Vulnerability in Swift Sensors Gateway SG3-1010

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-40422

An authentication bypass vulnerability (CVE-2021-40422) exists in the device password generation functionality of Swift Sensors Gateway SG3-1010. A specially-crafted network request can lead to Remote Code Execution (RCE). An attacker can send a sequence of requests to trigger this vulnerability.

Image source: https://github.com/

Vulnerability in GitHub Repository Janeczku/Calibre-web

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-0939

A Server-Side Request Forgery (SSRF) vulnerability (CVE-2022-0939) has been discovered in GitHub repository janeczku/calibre-web prior to 0.6.18.

Image source: https://community.ui.com/

Vulnerability in UniFi Door Access Reader Lite's (UA Lite) Firmware

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-22570

A buffer overflow vulnerability (CVE-2022-22570) has been found in the UniFi Door Access Reader Lite's (UA Lite) firmware. Affected versions are 3.8.28.24 and earlier. This vulnerability allows a malicious actor who has gained access to a network to control all connected UA devices. This vulnerability is fixed in Version 3.8.31.13 and later.

'Brokenwire' Hack Disrupt Charging of Electric Vehicles

Source: https://thehackernews.com/

A new attack technique has been observed against the popular Combined Charging System (CCS) that could potentially disrupt the ability to charge electric vehicles at scale. The method is dubbed as 'Brokenwire', which interferes with the control communications that transpire between the vehicle and charger to wirelessly abort the charging sessions from a distance of as far as 47m. Combined Charging System refers to a type of connector used for rapid-charging electric vehicles. Brokenwire aims at this technology by transmitting a malicious electromagnetic signal, causing the charging process to be unexpectedly stopped.

Brokenwire aims at this technology by transmitting a malicious electromagnetic signal, causing the charging process to be unexpectedly stopped.

2021's Top 15 Most Exploited Software Vulnerabilities

Source: https://www.cisa.gov/uscert/ncas/alerts/aa22-117a

Cyber security authorities from the Five Eyes nations Australia, Canada, New Zealand, the U.K., and the U.S has released a "2021 Top Routinely Exploited Vulnerabilities" report. Log4Shell, ProxyShell, ProxyLogon, ZeroLogon, and flaws in Zoho ManageEngine AD SelfService Plus, Atlassian Confluence, and VMware vSphere Client emerged as some of the top exploited security vulnerabilities in 2021. Other frequently weaponised flaws included a Remote Code Execution (RCE) bug in Microsoft Exchange Server (CVE-2020-0688), an arbitrary file read vulnerability in Pulse Secure Pulse Connect Secure (CVE-2019-11510), and a path traversal defect in Fortinet FortiOS and FortiProxy (CVE-2018-13379). Nine of the top 15 routinely exploited flaws were Remote Code Execution (RCE) vulnerabilities, followed by two privilege escalation weaknesses, and one each of security feature bypass, arbitrary code execution, arbitrary file read, and path traversal flaws. To mitigate the risk of exploitation of publicly known software vulnerabilities, It is recommended to apply patches in a timely manner and implement a centralised patch management system.

To mitigate the risk of exploitation of publicly known software vulnerabilities, It is recommended to apply patches in a timely manner and implement a centralised patch management system.

Critical Vulnerability in Jupiter Theme and JupiterX Core Plugin

Source: https://www.wordfence.com/

Authenticated Privilege Escalation and Post deletion vulnerability (CVE-2022-1654) were discovered in Jupiter Theme and JupiterX Core Plugin. This vulnerability allows any authenticated attacker, including a subscriber or customer-level attacker, to gain administrative privileges and completely take over any site running the affected versions of the plugin. Jupiter Theme 6.10.1 and below and JupiterX Core Plugin 2.0.7 and below are affected by the flaw. It is recommended to update to the latest patched version.

Image source: https://wordpress.org/

Critical Vulnerability in Argo CD

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-29165

In order for this vulnerability to be exploited, anonymous access to the Argo CD instance must have been enabled. Affected versions are version 1.4.0 and version prior to 2.1.15, 2.2.9, and 2.3.4.

Authentication Bypass by Spoofing vulnerability (CVE-2022-29165) was discovered in Argo CD. It has a CVSSv3 score of 10.0. Successful exploitation may allow an unauthenticated user to impersonate as any Argo CD user or role, including the `admin` user, by sending a specifically crafted JSON Web Token (JWT) along with the request. In order for this vulnerability to be exploited, anonymous access to the Argo CD instance must have been enabled. Affected versions are version 1.4.0 and version prior to 2.1.15, 2.2.9, and 2.3.4. It is recommended to update to the latest patched version.

Critical Vulnerability in Jenkins Pipeline: Groovy Plugin

Source:https://www.jenkins.io/security/advisory/2022-05-17/#SECURITY-359

This vulnerability allows loading any Groovy source files on the classpath of Jenkins and Jenkins plugins in sandboxed pipelines version 2689.v434009a_31b_f1 and earlier are affected by the flaw.

Sandbox bypass vulnerability (CVE-2022-30945) has been discovered in Jenkins Pipeline: Groovy Plugin. It has a CVSSv3 score of 10.0. This vulnerability allows loading any Groovy source files on the classpath of Jenkins and Jenkins plugins in sandboxed pipelines version 2689.v434009a_31b_f1 and earlier are affected by the flaw.

Critical Vulnerability in CMSimple_XH

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-42645

Image source: https://www.cmsimple-xh.org/

A Remote Code Execution (RCE) vulnerability (CVE-2021-42645) has been discovered in CMSimple_XH. It has a CVSSv3 score of 10.0. This vulnerability allows an attacker to use the "File" parameter to upload a PHP payload to get a reverse shell from the vulnerable host. Version 1.7.4 is affected by the flaw.

Multiple Vulnerabilities in Aruba ClearPass Policy Manager

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-23660, https://nvd.nist.gov/vuln/detail/CVE-2022-23658, https://nvd.nist.gov/vuln/detail/CVE-2022-23657

Image source: https://www.arubanetworks.com/

Remote Code Execution vulnerability (CVE-2022-23657, CVE-2022-23658, CVE-2022-23660) has been discovered in ClearPass Policy Manager. Successful exploitation of these vulnerabilities may allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. It is recommended to update to the latest patched version.

Critical Vulnerability in Squirrel

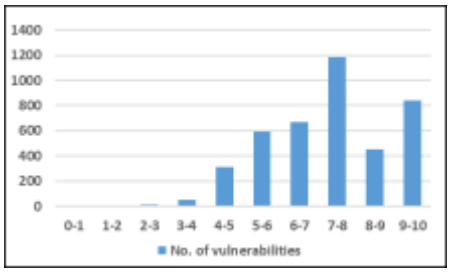
Source: https://nvd.nist.gov/vuln/detail/CVE-2022-30292

Heap-based buffer overflow vulnerability (CVE-2022-30292) has been discovered in sqbaselib.cpp in SQUIRREL due to lack of a certain sq_reservestack call. Version 3.2 is affected by the flaw. It has a CVSSv3 score of 10.0.

Quarterly Vulnerability Analysis Report

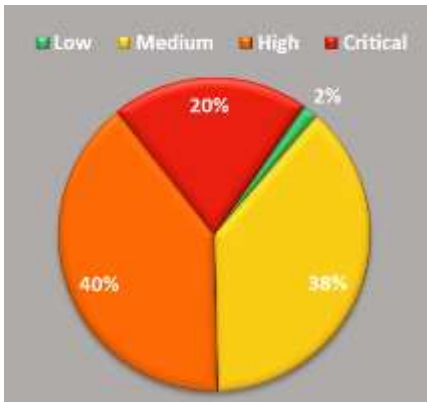
KMS Team, NCIIPC

During Second quarter of 2022, a total of 4123 vulnerabilities have been observed, out of which majority of vulnerabilities have score ranging from 7-9. 20 percent of total vulnerabilities reported were of Critical severity. Microsoft, Google, Apple, Adobe and Jenkins were the top five vendors having 24% of total reported vulnerabilities.



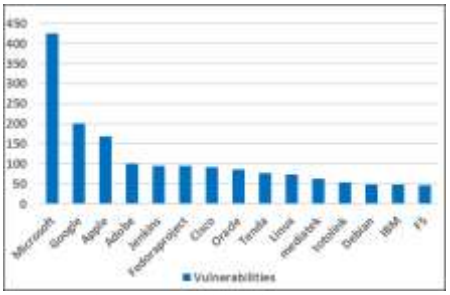
Severity-wise number of vulnerabilities

Severity	CVSSv3 Score	Number of vulnerabilities			Total Vulnerabilities	Severity Total
		Mar'22	Apr'22	May'22		
Low	0-1	0	0	0	0	67
	1-2	0	0	0	0	
	2-3	3	11	0	14	
	3-4	22	20	11	53	
Medium	4-5	89	133	92	314	1579
	5-6	201	204	191	596	
	6-7	209	277	183	669	
High	7-8	362	449	372	1183	1637
	8-9	134	193	127	454	
Critical	9-10	298	259	283	840	840
Total		1318	1546	1259		4123



Severity-wise share of vulnerabilities

S. No.	Vendor	No. of Vulnerabilities			Total
		Mar'22	Apr'22	May'22	
1.	Microsoft	103	140	182	425
2.	Google	30	108	63	201
3.	Apple	85	3	81	169
4.	Adobe	8	1	92	101
5.	Jenkins	51	17	28	96
6.	Fedoraproject	53	23	19	95
7.	Cisco	0	59	32	91
8.	Oracle	0	86	1	87
9.	Tenda	58	4	15	77
10.	Linux	30	27	17	74
11.	mediatek	13	21	28	62
12.	totolink	17	0	37	54
13.	Debian	31	11	6	48
14.	IBM	13	21	14	48
15.	F5	0	3	44	47



Count of vulnerabilities for top 15 vendors

Security App

Windows Autopatch: An Automatic Update Service

Source: https://techcommunity.microsoft.com/, www.securityweek.com/

This new feature ensures that Windows and Office products on registered endpoints are automatically updated helping admins more easily manage the security updates rolled out on the second Tuesday of every month.

Microsoft has announced Windows Autopatch, a new automatic updates service for Windows 10 and 11 Enterprise E3 customers that will manage all software, firmware, driver, and enterprise app updates. This new feature ensures that Windows and Office products on registered endpoints are automatically updated helping admins more easily manage the security updates rolled out on the second Tuesday of every month. The new service also comes with reporting and messaging capabilities, and with an Autopatch message centre, where admins can view details about schedules and update status, as well as details from the Autopatch team. All Microsoft customers with a license for Windows Enterprise E3 can enroll into Autopatch when it becomes generally available in July 2022, according to the company.

Free decryptor for HermeticRansom Ransomware

Source: https://decoded.avast.io/, https://www.bleepingcomputer.com/

Avast decryption tool for HermeticRansom

Avast has released a decryptor for the HermeticRansom ransomware strain circulating in the Ukraine. The decryptor is offered as a free-to-download tool. The ransomware strain accompanying the data wiper HermeticWiper malware was discovered which used in targeted attacks against Ukrainian systems. The ransomware contains a weakness in the crypto schema and can be decrypted using Avast decryptor. The ransomware is written in GO language. When executed, it searches local drives and network shares for potentially valuable files. Also, the tool offers the option to backup the encrypted files to avoid ending up with irreversibly corrupted files if something goes wrong with the encryption process.

Google to Add IT Security Integrations to Chrome

Source: https://www.zdnet.com/

This new Chrome Enterprise Connectors Framework currently comprise of integrations for identity and user access, integrations for endpoint management and integrations for security insights and reporting.

Google has announced, it is adding collection of plug-and-play integrations into Chrome with popular IT security tools. This makes easier for IT Teams to keep workers safer on the chrome browsers. This new Chrome Enterprise Connectors Framework currently comprise of integrations for identity and user access, integrations for endpoint management and integrations for security insights and reporting. This framework is a part of Google's larger effort to promote a zero trust security model:

- For identity and user access: The Netskope Security Cloud Integration optimizes user access to critical data based on

verifying the user, the device and action requested by the user.

- For Endpoint management across mobile and desktop: In addition to BlackBerry UEM and Samsung Knox Manage integrations, VMware Workspace ONE will update its existing integration to the new Chrome Policy API and will be available through Google's Trusted Tester Program.
- For Security insights and reporting: There is a new Splunk Cloud Platform integration. Palo Alto Networks and CrowdStrike integrations will be available through Trusted Tester Program.

Image source: https://chromereleases.googleblog.com/

CISCO launched CyberSecurity Preparedness Tool for SMBs

Source: https://ciso.economictimes.indiatimes.com/

Cisco has launched a Cybersecurity Assessment Tool to enable small and medium-sized businesses (SMBs) to understand the overall security posture. The new assessment tool assesses the 'cybersecurity readiness' of organisation through the lens of "Zero Trust". Zero trust concept is about all attempts to access organisation's network architecture that are not granted until trust can be verified for e.g., when user accesses an application using a device, both user and device are to be verified, with that trust continuously monitored. It helps in securing organisation's applications and environments from any user, device and location. This tool assesses the organisation's level of maturity in six areas of zero trust, e.g., user and identity, device, networks, workload (applications), data, and security operations.

Image source: https://tools.cisco.com/

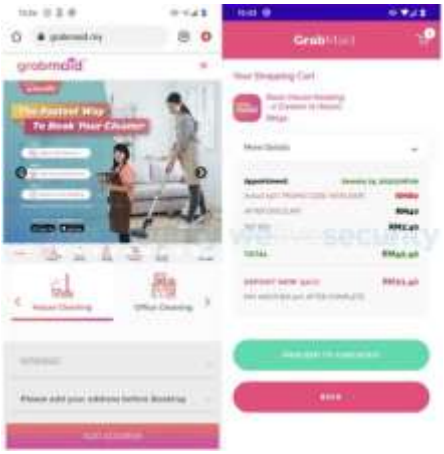
Mobile Security

Octo Banking Trojan Prowl via Fake Apps on Google Play store

Source: https://thehackernews.com/

Security researchers at ThreatFabric have discovered a new Android banking trojan named Octo being spread via Fake Apps on Google Play Store and it is the revised version of another Android malware called ExobotCompact. The Octo trojan is equipped to perform fraud by gaining remote control over devices by having the accessibility permissions as well as Android's MediaProjection API to capture the screen content. Moreover, its has the capability of logging keystrokes, carrying out overlay attacks on banking apps to seize credentials, harvesting speak to information, and persistence actions to avoid uninstallation and evade antivirus engines. As per the ThreatFabric report, the ultimate goal of this trojan is to trigger the automatic initiation of fraudulent transactions and its authorisation without manual efforts from the operator, thus allowing fraud on a significantly larger scale.

The Octo trojan is equipped to perform fraud by gaining remote control over devices by having the accessibility permissions as well as Android's MediaProjection API to capture the screen content.



Fake E-shop Campaign targets Malaysian Banks

Source: https://thehackernews.com/

At least eight Malaysian banks have been targeted by malicious applications since November 2021. The targeted banks include Maybank, Affin Bank, Public Bank Berhad, CIMB bank, BSN, RHB, Bank Islam Malaysia, and Hong Leong Bank. As per the report shared by the Slovak cybersecurity firm ESET the attacks involved setting up legitimate looking fraud websites to trick users into downloading the apps. The copycat websites impersonated cleaning services such as Maid4u, Grabmaid, Maria's Cleaning, Maid4u, YourMaid, Maideasy and MaidACall and a pet store named PetsMore, all of which are aimed at users in Malaysia. The ultimate goal of the campaign is to steal the banking credentials entered by the users and exfiltrate it to the attacker-controlled server, while displaying an error message that the entered user ID or password is invalid. Through Facebook Ads visitors are urged to download the Fake Apps available on Google Playstore, however it redirect them to the rouge servers under their control.

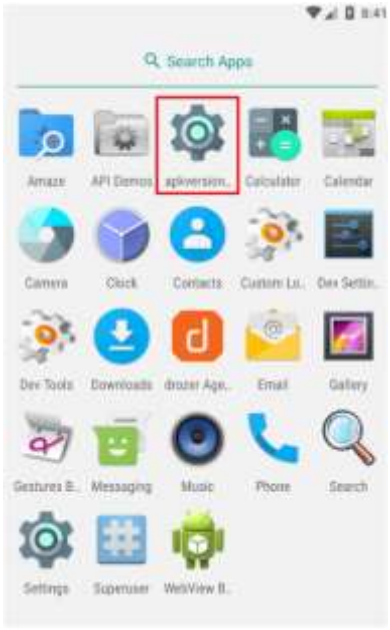


Figure: Application Name and Icon as displayed on Android Devices

Android Malware Targeting Banking Users Across Europe

Source: https://blog.cyble.com/

Cyble Research Labs came across an Android bankbot named 'GodFather' with the name 'apkversion1.1.5.43', an icon similar to the default Settings app and similarities with Cereberus and Medusa banking trojans. GodFather malware acts on the commands from Threat Actor's Command & Control (C&C) server to steal sensitive information from the victim's device. Upon successful execution, the malware can perform malicious activities such as transferring money by making USSD (Unstructured Supplementary Service Data) calls without using the dialer user interface, getting device information such as phone number, installed app list, battery info, etc. By further abusing the permissions on the affected device, the malware can also steal SMSs, control device screen using VNC, forward calls, and open URLs without the user's knowledge. The malware initially requests the victims to enable Accessibility, and then it hides its icon from the Android device's screen. The malware fetches the C&C URL from the Telegram channel hxxps://t[.]me/dobrynyanikitichsobre.

Android Malware Coper Posing as Google Play Store Installer

Source: https://blog.cyble.com/2022/03/24/coper-banking-trojan/

Cyble Research Labs came across various malware samples of Coper malware. Coper is linked to ExoBotCompat, a revised version of Exobot Android malware. Coper malware was initially discovered targeting Colombian users around July 2021. Coper

malware has modular design and multi-stage attack method. It can also survive various removal attempts. New versions of Coper Banking trojans are impersonating Utility apps, targeting Android users in different countries across Europe. Infection using Coper is done using two distinct phases – first step is to install the fake app which is nothing but the dropper app which hides the primary harmful module within it. The current version of Coper malware is able to send USSD requests, send SMS, lock/unlock device screen, start/stop intercepting SMS, display push notification, run a keylogger, uninstall itself along with the dropper app etc. The malware also receives commands from the threat actors through the C&C URL hard coded within the app in encrypted text.

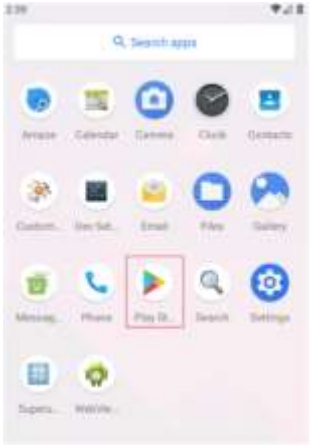


Figure: App Name and Icon

Newly Found Android Spyware Related to Turla APT Group

Source: https://www.bleepingcomputer.com/

A previously unknown Android malware uses the same shared-hosting infrastructure previously seen used by APT group known as Turla, though attribution to the hacking group not possible. Researchers from Lab52 identified a malicious APK named 'Process Manager' that acts as Android spyware, uploading information to the threat actors. While it is not clear how the spyware is distributed, once installed, Process Manager attempts to hide on an Android device using a gear-shaped icon, pretending to be a system component. After receiving the permissions, the spyware removes its icon and runs in the background with only a permanent notification indicating its presence. The information collected by the device, including lists, logs, SMS, recordings, and event notifications, are sent in JSON format to the command-and-control server at 82[.]146[.]35[.]240, which is located in Russia. While researching the app, the Lab52 team also found that it downloads additional payloads to the device and found a case of an app fetched directly from the Play Store named 'Roz Dhan: Earn Wallet cash' and it is a popular app featuring a money-generating referral system.

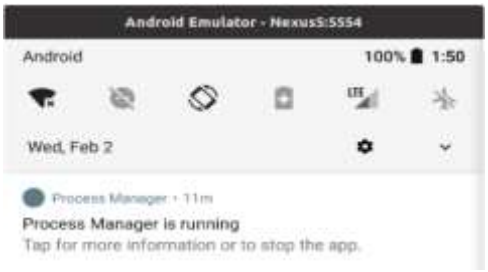


Figure: Notification Shown by the Spyware

Three Types of Android Malware Most Harmful in Nature

Source: https://www.welivesecurity.com/

Today's smartphones are capable of doing a lot of things rather than just calling or sending text messages. Smartphones can be used to store various types of sensitive data like personal documents, photos, videos, notes, schedules, remainders, login credentials etc. More than 70% of these smartphones are powered by Android which has an open ecosystem. A number of privacy and security enhancing features have been introduced by

Google. Other than that, in order to crack down malicious app from Google Play Store, Google announced that, last year it had stopped 1.2 million malicious apps from using its app store. However, users should be very careful, especially when installing apps from third-party app stores. Devices can be infected by malware in various ways. The three most harmful types of android malwares are:

However, users should be very careful, especially when installing apps from third-party app stores. Devices can be infected by malware in various ways.

- Ransomware: This type of malwares encrypts all the personal data in the device and some form of ransom is demanded for the decryption key.
- Banking Trojan: This type of malwares steals login details of the financial apps and send it back to the attacker. Sometimes, they are able to bypass the 2 Factor Authentication (2FA) system.
- Remote Access Trojan (RAT): This type of malware is very dangerous in nature and can be used to get full control of the device remotely.

#ALHACK: A Single Codec Capable of Hacking the Entire World

Source: https://research.checkpoint.com/

Malformed ALAC frame

In 2004, Apple Inc. developed the Apple Lossless Audio Codec (ALAC) which is used for lossless digital music compression. Initially this codec was proprietary. This ALAC format has been used extensively in many non-Apple based audio playback devices when Apple made this codec open-source in 2011. Although Apple continues to update and fix security issues of its proprietary version, the open-source version has never been updated. This open-source version is used by many third-party vendors for implementing their own ALAC. MediaTek and Qualcomm, the two largest mobile chipset makers, have included this vulnerable ALAC code into their audio decoders. These ALAC issues could be exploited by an attacker for Remote Code Execution (RCE) using a malformed audio file. These vulnerabilities can be used by an unprivileged Android app to escalate its privilege and gain access to the stored media and user conversations. Two thirds of all smartphones which are manufactured by MediaTek or Qualcomm and sold in 2021 suffers from this vulnerability. CVE-2021-0674 and CVE-2021-0675 have been assigned by MediaTek for this ALAC issues. These vulnerabilities are already fixed. Qualcomm released patch for CVE-2021-30351 in December 2021.

However, users should be very careful, especially when installing apps from third-party app stores. Devices can be infected by malware in various ways.

TeaBot Spreads via Google play

Source: https://thehackernews.com/

'TeaBot' it is an Android banking trojan that first emerged at the beginning of 2021 designed for stealing victim's text messages.

TeaBot is an only piece of malware to be spread through Google's official play store. Since its emergence, the malware has undergone various upgrades to infiltrate more targets and expand its attack surface. As per research published by Swiss cyber threat intelligence company PORDAFT in July 2021 established that the banking malware had already "infected more than 7632 devices and stolen over 1023 banking credentials". Bitdefender researcher earlier this year identified TeaBot hiding in the official Android app as a 'QR Code Reader – Scanner App'. These apps, also known as dropper application, act as a conduit to deliver a second-stage payload that retrieves the malware strain to take control of the infected devices. However, once downloaded, the dropper will request immediately an update through a popup message. Unlike legitimate apps that perform the updates through the official Google Play Store, the dropper application will request to download and install a second application, as displayed in Figure 2. This application has been detected to be a TeaBot.

Figure 1: TeaBot dropper published on Google pay store

Figure 2: TeaBot installation via a fake update

Escobar AbereBot Malware Targets Banking and Financial Apps

Source: https://www.bleepingcomputer.com/

Escobar mobile malware is becoming increasingly powerful against banking and financial applications. Escobar masquerades itself as a mcAfee antivirus app. This variant of Escobar widens its information-stealing capabilities by accessing features built-in to smartphones to get as much information as it can, to take complete control of victim's accounts and perform unauthorised transactions. Escobar can steal two-factor authentication (2FA) codes, SMS, call logs and location of a device. Escobar also uses VNC Viewer remote-desktop function to completely take over a phone.

Figure: Escobar uses McAfee's logo and brand name

Bogus Valorant Cheats Infects Users with RedLine Stealer

Source: https://www.bleepingcomputer.com/

South Korean security researchers have discovered a malware distribution operation on YouTube that uses fake valorant cheats to fool gamers into download RedLine, Malware that can steal information and infect operating systems with malware. Valorant cheats are allegedly add-ons installed in the game to help the players to winning matches without demonstrating any skill. Users download valorant cheat from video's description links. That link leads to RAR archive that contains an executable named "Cheat installer.exe". This file is, in reality a RedLine stealer that steals Computers basic information (such as computer name, username, IP address and OS information), Web Browsers information (Passwords, credit card info, AutoFill forms, etc.).

Figure: YouTube video promoting fake auto-aiming bot

NCIIPC Initiatives

DG, NCIIPC in panel session at Cyber Resiliency and Incidence Response Management 2022

NCIIPC in ASSOCHAM Webinar

A one-day webinar was conducted on 'Cyber Resiliency and Incidence Response Management 2022' by ASSOCHAM in collaboration with NCIIPC and Microsoft on 28th June 2022. Sh. Navin Kumar Singh, DG NCIIPC was one of the panel members. The webinar was about how the number and severity of attacks are rising, impact of incident response, need of Enterprises to develop & operationalise appropriate cyber incident response plan, etc.

C3i Hub Seminar on 'Modernising Security Operations for Power Sector'

C3i Hub IIT Kanpur R&D team collaborated with Microsoft R&D team to host an event on 'Modernising Security Operations for Power Sector'. This event was organised under the guidance of NCIIPC and Ministry of Power to address issues of Cyber Security in Grid Operation.

NCIIPC Cybersecurity Awareness Program in FCI

NCIIPC organised a Cyber Security Awareness program at Food Corporation of India (FCI) on 02 June 2022. This Cyber Security Awareness program was attended by midlevel management personnel of FCI.

NCIIPC Training Session on 'Onboarding Organisation on NCIIPC Threat Dissemination Platform'

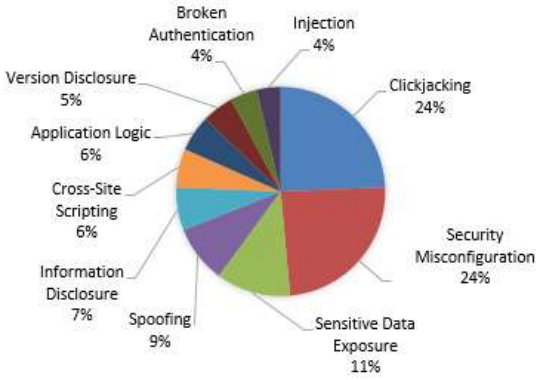
NCIIPC organised a training and demo session on 'Onboarding Organisation on NCIIPC Threat Dissemination Platform' for its various stakeholders through virtual mode on 27th May 2022. More than 300 critical sector organisation personnel joined the session.

NCIIPC Responsible Vulnerability Disclosure Program

Source: https://nciipc.gov.in/RVDP.html

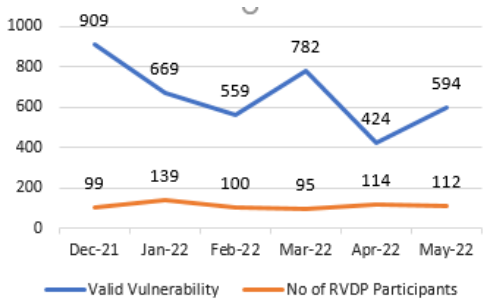
The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Nation's Critical Information Infrastructure. There are 1792 vulnerabilities reported during the second quarter of 2022. The top 10 vulnerabilities are:

- Clickjacking
- Security Misconfiguration
- Sensitive Data Exposure
- Spoofing
- Information Disclosure
- Cross-Site Scripting
- Application Logic
- Version Disclosure
- Broken Authentication
- Injection



Around 269 researchers participated in RVDP programme during the second quarter of 2022. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Abhilal S
- Aditya A Patel
- Aditya Kumar
- Ashish Kumar
- Cappricio Securities
- Darshan K Kulkarni
- Dnyanesh Gawande
- Harsh
- Joshua Arulsamy
- Khushi Agrawal
- Orsu Prasad
- Rakesh Sharma
- Rhishinathvarma M
- Sachhit Anasane
- Souvik Biswas



Last six months' timeline chart for vulnerabilities and RVDP participants

In last six months the total number of vulnerabilities reported were 3937 and number of RVDP participants were 659.

Upcoming Events - Global

July 2022

- Electrosuisse ExpertTalk Cyber Threats, Virtual — 4 Jul
- 2022 Cyber Stability Conference Geneva & Virtual — 5 Jul
- SECRYPT 2022, Lisbon — 11-13 Jul
- SANS London July 2022, London & Virtual — 11-16 Jul
- CRESTCon UK 2022, London — 13 Jul
- Philadelphia Cyber Security Summit, Philadelphia & Virtual — 19 Jul
- Blockchain Economy Istanbul Summit, Istanbul — 27-28 Jul
- INTERFACE Albuquerque 2022, Albuquerque — 28 Jul

August 2022

- BSides Dundee, Dundee — 6 Aug
- Black Hat USA, Las Vegas & Virtual — 6-11 Aug
- SANS Melbourne 2022, Melbourne & Virtual — 8-13 Aug
- FutureCon Cybersecurity Event: Kansas City, Kansas City & Virtual — 10 Aug
- INTERFACE Montana 2022, Montana — 11 Aug
- Vulnerability and Patch Management: Every day is a zero day, Virtual — 16-17 Aug
- OFFZONE 2022 International Conference on Practical Cybersecurity, Moscow — 25-26 Aug
- Chicago Cyber Security Summit, Chicago & Virtual — 26 Aug

September 2022

- SANS London September 2022, London & Virtual — 5-10 Sep
- Critical Infrastructure Cyber Security Summit, Virtual — 8 Sep
- BSides Montreal 2022, Montreal — 10 Sep
- 6th Annual African Cyber Security Conference, Gaborone — 14-15 Sep
- CRITIS 2022, Munich — 14-16 Sep
- SANS Amsterdam September 2022, Amsterdam & Virtual Deep — 19-24 Sep
- Learning Summit, Singapore — 20 Sep
- Cyber Security for Critical Assets Europe, London — 20-21 Sep
- InfoSec World 2022, Lake Buena Vista — 26-28 Sep

CREST CON

black hat USA 2022

SECRYPT 2022
19th International Conference on Security and Cryptography
11 - 13 July, 2022 Lisbon - Portugal

JULY 2022

S	M	T	W	T	F	S
31					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

AUGUST 2022

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

African Cyber Security

BSIDES MONTREAL

October 2022

- COSAC 2022: Information Security Conference, Naas — 2-6 Oct
- National Information Security Conference 2022, Chester — 5-7 Oct
- AISA Australian Cyber Conference, Melbourne — 11-13 Oct
- SecureWorld New York, New York — 13 Oct
- Scottsdale Cyber Security Summit, Scottsdale & Virtual — 14 Oct
- Cyber Security Conference UK: ALLOWLIST 2022, Yorkshire — 20 Oct
- Los Angeles Cyber Security Summit, Los Angeles & Virtual — 27 Oct
- Cyberdefensecon 2022, Orlando — 28 Oct

Upcoming Events - India

- DevOps India Summit 2022, Virtual — 26 Aug
- SANS Cyber Defence India August 2022, Virtual — 29 Aug - 3 Sep
- Nullcon, Goa — 6-10 Sep
- SANS South by South East Asia Offensive Operations 2022, Virtual — 19-24 Sep
- c0c0n Hacking and Cyber Security Briefing Conference, Kochi — 21-24 Sep
- SANS India Cloud Security 2022, Virtual — 17-22 Oct

SEPTEMBER 2022

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

OCTOBER 2022

S	M	T	W	T	F	S
30	31					1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

General Help		helpdesk1@nciipc.gov.in helpdesk2@nciipc.gov.in
Incident Reporting	:	ir@nciipc.gov.in
Vulnerability Disclosure	:	rvdp@nciipc.gov.in
Malware Upload	:	mal.repository@nciipc.gov.in

Abbreviations

- ALAC: Apple Lossless Audio Codec
- AWS: Amazon Web Services
- C&C: Command & Control
- CCS: Combined Charging System
- CI/CD: Continuous Integration/Continuous Delivery
- CIRA: Cyber Incident Reporting Act
- CISA: Cybersecurity and Infrastructure Security Agency
- CPF: CyberPeace Foundation
- DDoS: Distributed Denial of Service
- FCI: Food Corporation of India
- FedRAMP: Federal Risk and Authorisation Management Program
- FISMA: Federal Information Security Management Act
- FSCIJA: Federal Secure Cloud Improvement and Jobs Act
- GCP: Google Cloud Platform
- HTA: HTML Application
- ICT: Information and Communications Technology
- IETE: Institution of Electronics and Telecommunication Engineers
- IOC: Indicator of Compromise
- IoT: Internet of Things
- ISP: Internet Service Provider
- MII: Market Infrastructure Institution
- MitM: Man-in-the-Middle
- MSP: Managed Service Provider
- NCSC: NATO Cyber Security Centre
- NIC: National Informatics Centre
- NIS2: Network and Information Systems
- NPL: National Physical Laboratory
- NTP: Network Time Protocol
- OIL: Oil India Limited
- RCE: Remote Code Execution
- rps: request-per-second
- SCADA/ICS: Supervisory Control and Data Acquisition/Industrial Control Systems
- SEBI: Securities and Exchange Board of India
- SIEM: System Information and Event Management
- SLDC: State Load Despatch Centre
- SSTI: Server-Side Template Injection
- TAG: Threat Analysis Group
- TTPs: Tools, Techniques and Procedures
- UAC: User Account Control
- USSD: Unstructured Supplementary Service Data
- VAPT: Vulnerability Assessment and Penetration Testing
- VISTA: Versatile Innovation through Science & Technology Applications
- VPN: Virtual Private Network

Feedback/Contribution

Suggestions, feedback and contributions are welcome at newsletter@nciipc.gov.in

Disclaimer

NCIIPC does not endorse any vendor, product or service. The content of the newsletter is for informational purpose only. Readers may validate the information on their own.