NEWSLETTER

October 2023

National Critical Information Infrastructure Protection Centre

(A unit of National Technical Research Organisation)

National Critical Information Infrastructure Protection Centre
NCIIPC
सम्पूर्ण सुरक्षा
A unit of NTRO

CYBER SECURITY AWARENESS MONTH

THEME: SECURE OUR WORLD

FOCUSES ON FOUR KEY BEHAVIOURS

ENABLING MULTI-FACTOR AUTHENTICATION

USE STRONG PASSWORDS

UPDATING SOFTWARE

RECOGNISING AND REPORTING PHISHING

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

VOLUME 7 ISSUE 4

@NCIIPC

NCIIPC Newsletter

October 2023

Inside This Issue

Message from the NCIIPC Desk

Dear Readers,

Our country has recently successfully hosted the G20 Leader's Summit under the theme 'वसुधैव कुटुंबकम्'. This ancient theme of India is akin to the character of modern cyber world. In cyber world, there is no physical boundary and all of us share the same concerns. There is no boundary for the cyber criminals and rouge actors as they can target anyone from any corner of the world. It emphasizes on the basic principle that we are all one and thus need to collectively work upon to negate these evil forces in the cyber world to provide a safe digital ecosystem for public. This agenda has also been reiterated through the G20 New Delhi Leader's Declaration.

Government of India is working towards providing safe digital infrastructure for its citizens. Towards this new Digital Personal Data Protection Bill (DPDPB) has been passed in Parliament of India. This legislative framework applies to personal data collected in respect of citizen of India both in online and offline mode, inside and outside of India. It requires that personal information be processed only for a lawful purpose upon consent of an individual.

NCIIPC is constantly working with its stakeholders to create cyber security awareness within Critical Sector Entities. NCIIPC has organised cyber security awareness workshops at Vikas Soudha, Karnataka and Karnataka Power Corporation Limited. NCIIPC participated in International Cyber Security Conference Nullcon Goa 2023. NCIIPC participated in two panel discussions a) Critical Information Infrastructure (CII) Protection: Challenges and Opportunities – How can the Nullcon Community Contribute b) C4CII – Securing use of Cloud in Critical Information Infrastructure. The various concerns related to CII security were discussed and clarified during these panel discussions. NCIIPC is considering an incentive-based vulnerability disclosure program to widen the scope of NCIIPC RVDP Program.

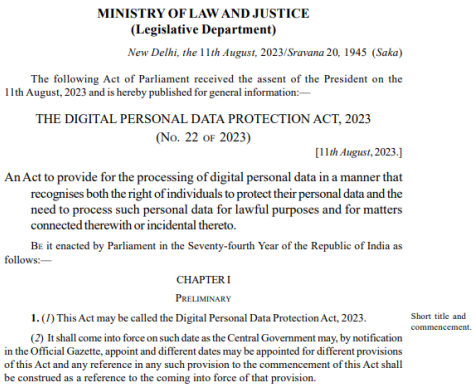
Suggestions and Feedback are welcome from our readers. Please do share your feedback on newsletter[at]nciipc[dot]gov[in]

News Snippets - National

India Passes New Digital Personal Data Protection Bill (DPDPB)

Source: https://pib.gov.in/, https://www.meity.gov.in/

The President of India has granted assent to the Digital Personal Data Protection Bill (DPDPB) marking a significant step towards securing people's information. It is unanimously passed by both houses of the parliament. According to Press Information Bureau (PIB), "The Bill provides for the processing of digital personal data in a manner that recognises both the rights of the individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto." The legislative framework, which applies to personal data collected both online and offline inside and outside of India, requires that information be processed 'only for a lawful purpose upon consent of an individual' and only store what's necessary for the purpose defined. 'Personal data' refers to "any data about an individual who is identifiable by or in relation to such data." In case of a citizen's data breach, one can simply visit to the website and provide the data protection board with details. The board will initiate an inquiry, imposing penalties on the breaching platforms.



MINISTRY OF LAW AND JUSTICE
(Legislative Department)

New Delhi, the 11th August, 2023/Sravana 20, 1945 (Saka)

The following Act of Parliament received the assent of the President on the 11th August, 2023 and is hereby published for general information:—

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
(No. 22 OF 2023)

[11*th August*, 2023.]

An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Seventy-fourth Year of the Republic of India as follows:—

CHAPTER I

PRELIMINARY

1. (*1*) This Act may be called the Digital Personal Data Protection Act, 2023. Short title and commencement.

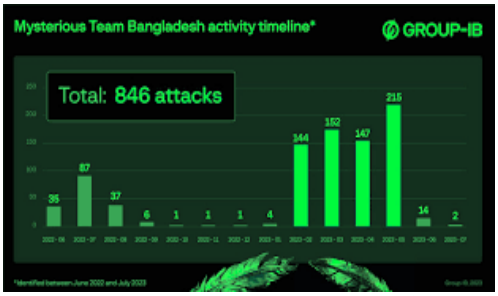
(*2*) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

The Digital Personal Data Protection Bill

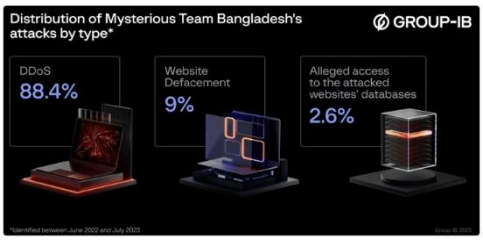
Threat Actors Targeted with DDoS and Data Breaches

Source: https://thehackernews.com/

A hacktivist group known as Mysterious Team Bangladesh has been linked to various Distributed Denial-of-Service (DDoS) attacks and website defacements most likely through the use of known security flaws or weak passwords. The group is primarily driven by religious and political motives targeting logistics, government, and financial sector organisations. Their actions are intended to disrupt critical systems, leading to potentially massive monetary and reputational losses for affected organisations. The threat actors most often exploit vulnerable versions of PHPMyAdmin and WordPress and relies on open-source utilities for conducting DDoS and defacement attacks. Group-IB anticipates that the adversaries will expand their operations in the upcoming year, intensifying its attacks across Europe, Asia-Pacific, and the Middle East. Governmental bodies and financial institutions are expected to remain focal points for the group's activities with potential ramifications for these entities' operations and reputations.



Mysterious Team Bangladesh activity timeline



Distribution of Mysterious Team Bangladesh attacks by type

News Snippets - International

U.S. Govt. Agencies' Emails Compromised in Cyber Attack

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

Microsoft has disclosed a significant cybersecurity incident involving a hacking group known as Storm-0558. This group successfully breached the email accounts of over two dozen organisations worldwide, including government agencies in the U.S. and Western Europe. Storm-0558 is suspected of being a cyber-espionage group primarily interested in gathering sensitive information through email system breaches. The attacks were first detected by Microsoft on June 16, 2023, after receiving reports from customers about unusual activity in Office 365 mail. The intrusion began on May 15, 2023, with the threat actors gaining unauthorised access to Outlook accounts of approximately 25 organisations, potentially including the U.S. State and Commerce Departments. The attackers employed stolen authentication tokens, created using a pilfered Microsoft account (MSA) consumer signing key, to access email accounts via Outlook Web Access in Exchange Online and Outlook.com. Microsoft was quick to mitigate the attack, and there is no evidence of further unauthorised access.

The attacks were first detected by Microsoft on June 16, 2023, after receiving reports from customers about unusual activity in Office 365 mail.

Israel's Largest Oil Refinery Website Offline After DDoS Attack

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

The website of BAZAN Group, Israel's largest oil refinery operator, has become inaccessible to most parts of the world due to a claimed cyber attack by threat actors. Reports indicate that incoming traffic to BAZAN Group's websites, bazan.co.il and eng.bazan.co.il, is experiencing issues such as timing out and displaying HTTP 502 errors, or being refused by the company's servers. A hacktivist group known as 'Cyber Avengers' or 'CyberAv3ngers' has claimed responsibility for breaching BAZAN's network over the weekend. They also leaked what appears to be screenshots of BAZAN's SCADA. BAZAN, however, has dismissed these leaked materials as entirely fabricated. The hacktivist group implied that they breached BAZAN via an exploit targeting a Check Point firewall at the company. While the IP address associated with the firewall device was confirmed to be linked to Oil Refineries Ltd., Check Point has refuted these claims, stating that there was no past vulnerability enabling such an attack.

A hacktivist group known as 'Cyber Avengers' or 'CyberAv3ngers' has claimed responsibility for breaching BAZAN's network over the weekend. They also leaked what appears to be screenshots of BAZAN's SCADA.

8 Million People Hit by Data Breach at Maximus

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

Maximus, a U.S. government services contractor, has disclosed a significant data breach in which hackers stole the personal data of approximately 8 to 11 million individuals during recent MOVEit Transfer data-theft attacks. The breach occurred due to a zero-day vulnerability (CVE-2023-34362) in the MOVEit file transfer application, which the Clop ransomware gang extensively exploited to target numerous high-profile organisations worldwide. Following an investigation, Maximus determined that the hackers did not progress beyond the MOVEit environment, which was promptly isolated from the rest of the corporate network. However, this limited access allowed the compromise of a substantial amount of personal information, including Social Security Numbers and protected health information. While the gang claims to have stolen 169GB of data, no data has been leaked yet, indicating a possibility of that the extortion process is ongoing.

The breach occurred due to a zero-day vulnerability (CVE-2023-34362) in the MOVEit file transfer application, which the Clop ransomware gang extensively exploited to target numerous high-profile organisations worldwide.

'ScarCruft' Hackers Breached Russian Missile Maker

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

ScarCruft hacking group, also known as APT37, has been linked to a cyberattack on NPO Mashinostroyeniya. In this cyberattack, ScarCruft planted a Windows backdoor named 'OpenCarrot' in NPO Mashinostroyeniya's IT systems and email server to gain remote access. The breach came to light when SentinelLabs analysed leaked emails from NPO Mashinostroyeniya, which contained highly confidential communications and a report from IT staff warning of a potential cybersecurity incident in mid-May 2022. OpenCarrot is implemented as a DLL file and supports various commands, including reconnaissance, file and process manipulation, reconfiguration, and connectivity management. It can also enter a sleep state when legitimate users are active on compromised devices and check for the insertion of new USB drives for potential lateral movement. SentinelLabs observed suspicious traffic originating from the victim's Linux email server, indicating potential involvement of ScarCruft's RokRAT backdoor.

In this cyberattack, ScarCruft planted a Windows backdoor named 'OpenCarrot' in NPO Mashinostroyeniya's IT systems and email server to gain remote access.

Interpol Takes Down 16shop Phishing-as-a-service Platform

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

The stolen data included personal information, email addresses, passwords, ID cards, credit card numbers, and phone numbers. Interestingly, the servers hosting 16shop were located in the United States, but registration information pointed to Indonesia.

In a joint operation between Interpol and cybersecurity firms, a significant blow has been dealt to the notorious phishing-as-a-service (PhaaS) platform known as 16shop. 16shop was particularly menacing, offering phishing kits targeting popular brands such as Apple, PayPal, American Express, Amazon, and Cash App. Interpol's investigation revealed that at least 70,000 users across 43 countries fell victim to phishing pages created through 16shop. The stolen data included personal information, email addresses, passwords, ID cards, credit card numbers, and phone numbers. Interestingly, the servers hosting 16shop were located in the United States, but registration information pointed to Indonesia. The Indonesian police not only arrested the operator but also seized electronic devices and luxury vehicles in his possession. The apprehension of the two facilitators followed the arrest of the administrator, indicating that he may have provided information about his associates. This operation demonstrates the effectiveness of international cooperation in combating cybercrime and dismantling significant cybercriminal infrastructure.

New HiatusRAT Malware Attacks US Defence Department

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

HiatusRAT samples have been recompiled to target various architectures and hosted on newly acquired virtual private servers (VPSs).

A new HiatusRAT malware campaign has taken an unexpected turn as threat actors targeted a server belonging to the U.S. Department of Defence, marking a shift in tactics. HiatusRAT samples have been recompiled to target various architectures and hosted on newly acquired virtual private servers (VPSs). One of these VPS nodes was involved in a data transfer operation with a U.S. military server designated for contract proposals and submissions. This suggests that the attackers may be seeking publicly accessible information related to military contracts and organisations involved in the Defence Industrial Base (DIB). HiatusRAT is known for installing additional payloads on infected devices and converting compromised systems into SOCKS5 proxies for command and control server communication. Despite prior disclosures of its capabilities, the threat actor behind HiatusRAT made minimal changes to their payload servers, continuing their operations. This shift in information collection and targeting preferences aligns with Chinese strategic interests, as highlighted in the 2023 ODNI annual threat assessment. U.S. organisations have recently faced attacks linked to other threat groups, such as Volt Typhoon and Storm-0558.

Carderbee Hacking Group Hits Hong Kong Organisations

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

A previously unidentified APT hacking group known as 'Carderbee' has been observed targeting organisations in Hong Kong and other Asian regions. Carderbee employs a supply chain attack using legitimate software, Cobra DocGuard which is used for data encryption and decryption in security applications. The group uses this software to infect target computers with the PlugX malware. Symantec observed Cobra DocGuard software installed on 2,000 computers but identified malicious activity on only 100 of them, indicating a focus on high-value targets. The updates arrive as ZIP files fetched from a suspicious domain, which, when decompressed, execute a malicious DLL acting as a downloader. Notably, the PlugX downloader is digitally signed using a Microsoft certificate, making it harder to detect. The malicious DLL pushed by Carderbee includes x64 and x86 drivers for creating Windows services and registry entries required for persistence. Eventually, PlugX is injected into the legitimate 'svchost.exe' (Service Host) Windows process to evade antivirus detection.

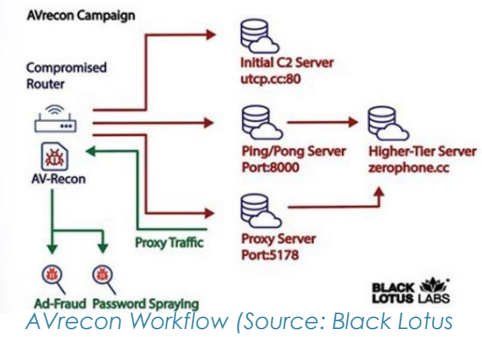
The updates arrive as ZIP files fetched from a suspicious domain, which, when decompressed, execute a malicious DLL acting as a downloader.

Malware Bytes

New AVrecon Botnet Spreads Across 20 Countries

Source: https://thehackernews.com/

Small Office/Home Office (SOHO) routers have been the target of a new malware strain that has been operating secretly for more than two years, infecting over 70,000 machines and establishing a botnet with 40,000 nodes spread across 20 nations. The malware has been named AVrecon. In this attack chain, a successful infection was followed by enumerating the victim's SOHO router and exfiltrating the information back to an embedded Command-and-Control (C2) server. By looking for active processes on port 48102 and opening a listener on that port, the malware determines whether other malware instances are already active on the host. The process linked to that port is shut down. The compromised machine will then connect to another server, referred to as the secondary C2 server, to wait for new commands.



AVrecon Workflow (Source: Black Lotus Labs)

New 'Whiffy Recon' Malware

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

Whiffy Recon works by checking for the WLAN AutoConfig service (WLANSVC) on the infected system and terminates itself if the service name does not exist.

The SmokeLoader malware is used to deliver a new Wi-Fi scanning malware variant known as 'Whiffy Recon' on compromised Windows machines. Whiffy Recon works by checking for the WLAN AutoConfig service (WLANSVC) on the infected system and terminates itself if the service name does not exist. The attack involves scanning for Wi-Fi access points via the Windows WLAN API every 60 seconds. The outcomes of the scan are sent to the Google Geolocation API, which triangulates the system's location and ultimately sends a JSON string with that information to the C2 server. Researchers of Secureworks have noted that threat actors can use the Wi-Fi scanning data to track compromised systems, and can be potentially used to intimidate victims or pressure them into complying with the demands of the threat actors.

Patchwork Hackers Target Research Organisations

Source: https://thehackernews.com/

Patchwork used a range of elaborate fake personas to manipulate people into clicking on malicious links and downloading malicious apps.

Patchwork threat actors have been spotted targeting universities and research organisations in China as part of a recently observed campaign. Patchwork used a range of elaborate fake personas to manipulate people into clicking on malicious links and downloading malicious apps. Patchwork threat actors created a fake review website for chat apps where they listed the top five communication apps, putting their own, attacker-controlled app at the top of the list. Patchwork threat actors used

a .NET-based modular backdoor called EyeShell that has the ability to connect to a remote Command-and-Control (C2) server and run commands to enumerate files and directories, download and upload files to and from the host, run a particular file, delete files, and take screenshots.

New SystemBC Malware Variant Targets Power Company

Source: https://thehackernews.com/, https://securelist.com/

Recently threat actors have targeted a power generation company in southern Africa with a new variant of the SystemBC malware called 'DroxiDat'. A proxy-capable backdoor was deployed alongside Cobalt Strike Beacons in this cyberattack. SystemBC is a C/C++-based commodity malware and remote administrative tool that allows multiple targets to be worked at the same time with automated tasks, allowing for hands-off deployment of ransomware using Windows built-in tools if the attackers gain the proper credentials. The DroxiDat variant used in this attack was very compact compared to previous and common SystemBC variants. The purpose of this DroxiDat malware variant was to be used as a simple system profiler. It provided no download-and-execute capabilities, but can connect with remote listeners and pass data back and forth, and modify the system registry.

The purpose of this DroxiDat malware variant was to be used as a simple system profiler. It provided no download-and-execute capabilities, but can connect with remote listeners and pass data back and forth, and modify the system registry.

Recent Phishing Attacks

Knowledge Management Team, NCIIPC

In the third quarter of 2023 various phishing attacks affected several organisations. Microsoft recently has identified a set of highly targeted social engineering attacks where threat actor Midnight Blizzard has used Microsoft Teams chats as credential theft phishing lures. Threat actor has used previously compromised Microsoft 365 tenants owned by small businesses to create new domains that appear as technical support. Using these domains from compromised tenants, threat actor leverages Teams messages to send lures that attempt to steal credentials from a targeted organisation by engaging a user and getting them to approve multi-factor authentication (MFA) prompts. To gain initial access into the targeted environments, the threat actor has used token theft tactics along with other strategies like authentication spear-phishing, password spray, and brute-force attacks.

Microsoft recently has identified a set of highly targeted social engineering attacks where threat actor Midnight Blizzard has used Microsoft Teams chats as credential theft phishing lures.

Threat actors have increasingly used a phishing-as-a-service (PhaaS) toolkit named 'EvilProxy' to pull off account takeover attacks aimed at high-ranking executives at prominent companies. The threat actors have used new advanced automation to accurately determine in real-time if a phished user

Nearly 39% of the compromised users are said to be C-level executives. The attacks have also singled out personnel with access to financial assets or sensitive information.

is a high-level profile or not, and immediately obtain access to the account if it is a high-level profile, while ignoring less lucrative phished profiles. Nearly 39% of the compromised users are said to be C-level executives. The attacks have also singled out personnel with access to financial assets or sensitive information.

A new generative AI cybercrime tool called WormGPT has been advertised on underground forums as a way for adversaries to launch sophisticated phishing and Business Email Compromise (BEC) attacks. Cybercriminals can use this tool to automate the creation of highly convincing fake emails, personalised to the recipient, thus increasing the chances of success for the attack. The fact that WormGPT operates without any ethical boundaries highlights the threat posed by generative AI. It even enables novice cybercriminals to launch attacks swiftly and at scale without having the necessary technological resources. The execution of complex BEC attacks is made more accessible through the application of generative AI. Even attackers with limited skills can use this technology, making it an accessible tool for a broader spectrum of cybercriminals.

Image source: https://wormgpt.co/

References:

[1] https://thehackernews.com/2023/08/microsoft-exposes-russian-hackers.html

[2] https://thehackernews.com/2023/08/cybercriminals-increasingly-using.html

[3] *https://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html*

Latest Ransomware Attacks

Knowledge Management Team, NCIIPC

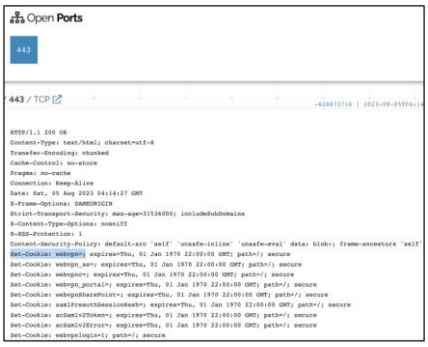
Recently many new ransomware attacks have been seen and existing ransomware threat actors have improved their attack techniques.

This new variant of Yashma executes an embedded batch file, which contains the commands to download the ransom note from the actor-controlled GitHub repository.

A threat actor has used a variant of the Yashma ransomware to target various entities in English-speaking countries, Bulgaria, China, and Vietnam since June 2023. The ransom note mentions a wallet address to which the payment is to be made but it does not specify the amount to be paid. After encryption, the Yashma ransomware variant changes the wallpaper on the victim's machine. Both the ransom note and the wallpaper set by the Yashma variant in the victim's machine mimics the WannaCry ransomware. This new variant of Yashma executes an embedded batch file, which contains the commands to download the ransom note from the actor-controlled GitHub repository. This modification evades anti-virus software and endpoint detection

solutions, which generally detect embedded ransom note strings in the binary.

Akira ransomware threat actors have targeted Cisco VPNs that were not configured for multi-factor authentication to infiltrate organisations. Akira threat actors have used compromised Cisco VPN accounts to breach corporate networks without needing to drop additional backdoors or set up persistence mechanisms that would give them away. The Akira ransomware threat actors have hacked multiple organisations in multiple industries, including finance, education, and real estate. Threat actors launched set.bat after successfully authenticating to the internal assets. Execution of set.bat resulted in the installation and execution of the remote desktop application AnyDesk. Threat actors performed further lateral movement and binary executions across other systems within target environments to broaden the scope of compromise.



Cisco VPN trait seen in eight Akira attacks

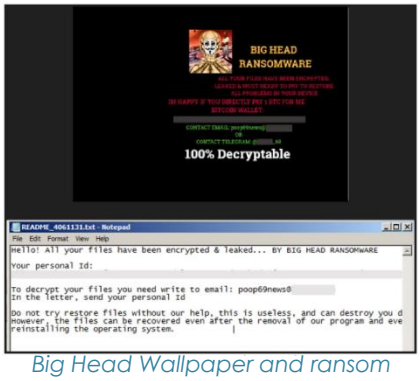
The threat actors behind BlackCat ransomware have created an improved variant that prioritises speed and stealth in an attempt to bypass security barriers and achieve their goals. This improved variant has been named Sphynx, and has the capability to strengthen the threat actor group's efforts to evade detection. The initial access to target networks was obtained through a network of actors called Initial Access Brokers (IABs). IABs employ an off-the-shelf information stealer malware to harvest legitimate credentials. The Sphynx version of BlackCat includes junk code and encrypted strings in addition to changing the command line arguments passed to the binary. Sphynx also incorporates a loader to decrypt the ransomware payload. Upon execution, this loader deletes volume shadow copies, encrypts files, drops the ransom note, and performs network discovery activities to hunt for more systems.

This improved variant has been named Sphynx, and has the capability to strengthen the theat actor group's efforts to evade detection.

Recently a malicious toolset called Spacecolon has been deployed to spread variants of the Scarab ransomware across victim organisations globally. The threat actors behind this malware called CosmicBeetle gains initial access into the victim organisation by compromising vulnerable web servers or via brute forcing RDP credentials. Spacecolon installs ScService, a backdoor with features to execute custom commands, download and execute payloads, and retrieve system information from compromised systems. The threat actor's main objective is to leverage the access provided by ScService to deliver a variant of the Scarab ransomware. It has also been discovered that the CosmicBeetle threat actor is actively developing a new ransomware variant called ScRansom, which attempts to encrypt all hard, removable, and remote drives using the AES-128 algorithm with a key generated from a hard-coded string.

The threat actor's main objective is to leverage the access provided by ScService to deliver a variant of the Scarab ransomware.

Security researchers have discovered a new ransomware strain dubbed 'Big Head' which is spreading through malvertising that



Big Head Wallpaper and ransom note (Source: Trend Micro)

promotes fake Windows updates and Microsoft Word installers. The 'Big Head' ransomware is a .NET binary that installs three AES-encrypted files on the target system. One of these files is used to disseminate the malware, another is for Telegram bot communication, and the third encrypts files and can also display a fake Windows update UI to deceive the user. On execution, the ransomware also performs actions like creation of registry autorun key, if required overwriting existing files, setting system file attributes, and disabling the Task Manager. The ransomware deletes shadow copies to prevent easy system restoration before encrypting the targeted files and appending a '.poop' extension to their filenames. After the encryption process is completed, a ransom is dropped on multiple directories, and the victim's wallpaper is also changed to alert of the infection.

The risk of ransomware can be reduced by implementing a backup for sensitive data and servers, multifactor authentication, well-configured VPN, hardening of firmware, software and all operating systems periodically to reduce security risk by eliminating potential attack vectors and abridging the system's attack surface.

References:

[1] https://blog.talosintelligence.com/new-threat-actor-using-yashma-ransomware/

[2] https://thehackernews.com/2023/08/new-yashma-ransomware-variant-targets.html

[3] https://securityaffairs.com/150157/cyber-crime/cisco-asa-ransomware-attacks.html#:~:text=%E2%80%9CCisco%20is%20aware%20of%20reports,configure%20multi%2Dfactor%20authentication%20for

[4] https://www.bleepingcomputer.com/news/security/akira-ransomware-targets-cisco-vpns-to-breach-organizations/?&web_view=true

[5] https://thehackernews.com/2023/06/improved-blackcat-ransomware-strikes.html

[6] https://thehackernews.com/2023/08/spacecolon-toolset-fuels-global-surge.html

[7] https://www.bleepingcomputer.com/news/security/new-big-head-ransomware-displays-fake-windows-update-alert/

[8] https://thehackernews.com/2023/07/beware-of-big-head-ransomware-spreading.html#:~:text=In%20a%20new%20analysis%20of,display%20a%20fake%20Windows%20update.

Threat Actor Deploys New SUBMARINE Backdoor

Source: https://thehackernews.com/

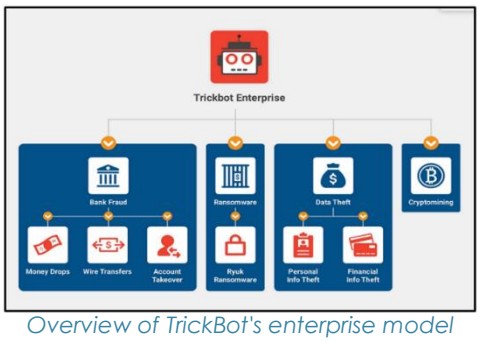
A new backdoor called SUBMARINE has been discovered that was deployed by threat actors UNC4841 to hack Barracuda Email Security Gateway (ESG) appliances. SUBMARINE comprises of shell scripts, SQL trigger, and a loaded library for a Linux daemon that together allow execution with root privileges, persistence, command and control, and cleanup. The infection chain involves sending phishing emails with booby-trapped TAR file attachments to trigger exploitation. This leads to the deployment of a reverse shell payload to establish communication with the threat actor's Command-and-Control (C2) server, from where a passive backdoor called SEASPY is downloaded to allow arbitrary commands to be executed on the target device.

SUBMARINE comprises of shell scripts, SQL trigger, and a loaded library for a Linux daemon that together allow execution with root privileges, persistence, command and control, and cleanup.

Trickbot Malware

South Zone, NCIIPC

Trickbot Malware is a type of trojan that emerged in 2005, orginally designed as a banking malware to steal confidential and sensitive information from the organisations. Since its discovery, developers prolonged the malware scope and capabilities and it has evolved into highly modular malware and toolset that provides attackers numerous options to perform malicious activities.



Overview of TrickBot's enterprise model (Source: Bleeping Computer)

How does Trickbot spread and execute?

The new form of Trickbot can allow attackers to distribute largely to users via spam mails with PDF file attachment, links or malicious files within the emails. On execution of malware, attacker can open backdoor to download further malware automatically in the machine.

Once taken control, the module is then able to affect the processing of each and every request. Attacker can perform anti-analysis check to confirm that it is not being run on a malware analysis machine, then downloads the key component and executes additional malicious payloads to gain access to other machines across a network by abusing the SMB Protocol. It has discrete payload modules for its loader, distributed denial of service (DDoS) attacks, Outlook credentials, banking fraud, credentials theft, ability to verify block listed IP on a spam list, extracting email address, ransomware and malspam and more. New version of Trickbot uses elliptic curve cryptography encryption structure for command and control communications.

Attacker can perform anti-analysis check to confirm that it is not being run on a malware analysis machine, then downloads the key component and executes additional malicious payloads to gain access to other machines across a network by abusing the SMB Protocol.

Consequences of Trickbot attack: Trickbot malware has the capability to collect local files and information about system and network for future use. It can modify registry and can capture remote desktop credentials. It can decode the modules and

configuration data. It can terminate the services of window defender. This can steal stored passwords too. Victims are then forced to send an email to the address provided by attackers to purchase decryptor software by paying hefty amount of money.

Constant monitoring is required to detect a TrickBot Trojan. Possible signs of the malware can be unauthorised login attempts through stolen credentials. Network administrator may notice changes in traffic.

Detecting and removing TrickBot Trojans: Constant monitoring is required to detect a TrickBot Trojan. Possible signs of the malware can be unauthorised login attempts through stolen credentials. Network administrator may notice changes in traffic. The malware can mask itself as an ordinary file which makes it nearly undetectable.

- It is recommended that the first step is to identify infected computer and isolate it from the network.
- Refrain from opening suspicious links and attachments in email without verifying their authenticity and identity of the sender.
- Reconfigure the Firewall rules. It is recommended to only allow access to known services or servers.
- Ensure multifactor authentication wherever possible to provide extra layer of security particularly the accounts that access critical systems.
- Hardening of firmware, software and all operating systems should be done periodically to reduce security risk by eradicating potential attack vectors and reducing the system's attack surface.
- OS and other software's should be updated regularly.
- The unnecessary open ports in the servers need to be closed

References:

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-076a
[2] https://www.kaspersky.com/resource-center/threats/trickbot
[3] https://www.cisecurity.org/insights/blog/trickbot-not-your-average-hat-trick-a-malware-with-multiple-hats
[4] https://www.wired.co.uk/article/trickbot-malware-group-internal-messages

Learning

Enhanced Monitoring to Detect APT Activity Targeting Outlook

Source: https://www.cisa.gov.in/

The US Cybersecurity & Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) has released the joint Cybersecurity Advisory to provide guidance to Critical Infrastructure Organisations (CIOs) on enhancing monitoring of Microsoft Exchange Online environments. It was found that Advanced Persistent Threat (APT) actors have accessed and exfiltrated unclassified Exchange Online Outlook data. The APT actors have used Microsoft Account (MSA) consumer key to forge tokens to impersonate consumer and enterprise users. Microsoft remediated the issue by first blocking tokens issued with the acquired key and then replacing the key to prevent continued misuse. Agencies has recommended CIOs to enable audit logging and strongly encourage organisations to:

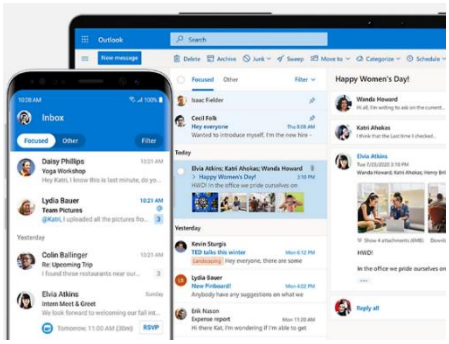


Image source: https://www.microsoft.com/

- Enable Purview Audit logging.
- Ensure logs are searchable.
- Enable Microsoft 365 Unified Audit Logging (UAL).
- Understand organisation's cloud baseline.

Agencies also recommends CIOs to implement hardening in their cloud environment-

- Apply CISA's recommended baseline security configurations.
- Separate administrator accounts from user accounts.
- Collect and store access and security logs for Secure Cloud Access (SCA) solutions, endpoint solutions, cloud applications/platforms.
- Use a telemetry hosting solution that aggregates logs and telemetry data to facilitate internal organisation monitoring, auditing, alerting, and threat detection activities.
- Review contractual relationships with all Cloud Service Providers (CSPs).

It was found that Advanced Persistent Threat (APT) actors have accessed and exfiltrated unclassified Exchange Online Outlook data. The APT actors have used Microsoft Account (MSA) consumer key to forge tokens to impersonate consumer and enterprise users.

Microsoft Shares Guidance and Resources for AI Red Teams

Source: https://www.securityweek.com/

Microsoft has shared best practices that can help security teams proactively hunt for failures in AI systems, define a defense-in-depth approach and create a plan to evolve and grow security posture as generative AI systems.

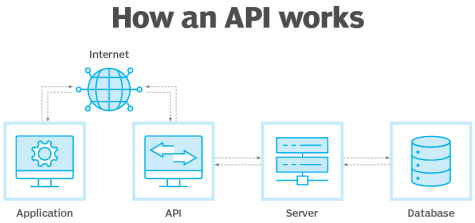
Image source: https://www.microsoft.com/

The key points that have helped shape Microsoft's AI Red Team Program: -

- AI red teaming is more expansive- AI red teaming is an umbrella term for probing security and Responsible AI (RAI) outcomes.

AI red teaming requires a defence-in-depth approach that incorporate declining harmful content, leveraging metaprompt to guide behaviour and regulating conversational drift.

- AI red teaming focuses on failures from both malicious and benign personas- AI red teaming not only focuses on how a malicious adversary can subvert the AI system via security-focused techniques & exploits, but also generate problematic and harmful content when regular users interact with the system.
- AI systems are constantly evolving- AI applications routinely change at a faster rate.
- Red teaming generative AI system require multiple attempts- Traditional red teaming is deterministic while, Generative AI systems, are probabilistic because running the same input twice may provide different outputs.
- Mitigating AI failures requires defence in depth- AI red teaming requires a defence-in-depth approach that incorporate declining harmful content, leveraging metaprompt to guide behaviour and regulating conversational drift.



Compromised APIs can allow hacker to compromise all API data, application functionality, interrupt services and thus can exfiltrate sensitive information to defame or for financial gain.

Importance of API Security

South Zone, NCIIPC

Application Programming Interface (API) security is the process of protecting APIs of software's applications by implementing security strategies. API security is important for better performance and security of APIs correspondingly the associated programs they support. API security discusses the measures and policies that protect APIs against malicious activities and vulnerabilities. APIs are the key factor of web applications are becoming target for attackers as they have access to data which is being transmitted through APIs between clients and servers connected over a network. Compromised APIs can allow hacker to compromise all API data, application functionality, interrupt services and thus can exfiltrate sensitive information to defame or for financial gain. However, by implementing controls and regular testing of APIs, can prevent their exploitation by threat actors.

How are APIs abused?

If the APIs are not coded and protected appropriately, APIs can be exploited by various techniques like Phishing attacks, bots etc. It may have vulnerabilities such as security misconfigurations, denial of service, broken authentication, malicious code injection, excessive data exposure, insufficient logging & monitoring etc.

API Security Testing:

- Tempering with Parameters: Attackers can take advantage of hidden form fields and can manipulate the data available in those fields.
- Fuzzing Testing: It is a process of Injecting random invalid data to the API; which monitors till application problem arises.
- Command Injection Testing: Attackers utilise this to find out

whether API is vulnerable to Common injection attacks. Here an attacker will try to execute an OS command by exploiting application vulnerabilities. Attackers utilise this attack to get entire access control of an application.

API security Challenges: APIs and web application work collectively but operate in totally different ways and so APIs security and its infrastructures must be unique. Most of the time Security teams do not have required information about APIs endpoints and its operations. These new structures and different file formats make it easier for attackers to attempt attacks, like Injection etc.

APIs and web application work collectively but operate in totally different ways and so APIs security and its infrastructures must be unique.

API Security Best Practices: The following best practices may help to reduce the risk of a cyber-attack by securing API misconfigurations and their vulnerabilities:

- Continuous API Monitoring: Organisations should regularly monitor the activity of API endpoints and API requests.
- Regular Log Analysis: There is a need to have a mechanism in place so that the real time analysis of logs of the APIs can be carried out regularly.
- Use API gateways
- Limit Network Traffic: Rate limiting controls the user request that an IP address is able to make to an API in a given time frame.
- Authentication: API security depends on authentication, because it verifies and allows the client to use the API. Next is authorisation which defines what data an authentic application can access while networking with the API.
- Ensure multifactor authentication wherever possible to provide extra layer of security, particularly, the accounts that access critical systems.
- Lack of Awareness: Cybersecurity awareness training, regular awareness sessions and workshops, cyber mock drills covering the social engineering attacks for the end users to stay across current threats.
- Encryption of API data: The most effective way is to use HTTPS or Hypertext Transfer Protocol Secure while using the APIs.

Ensure multifactor authentication wherever possible to provide extra layer of security particularly the accounts that access critical systems.

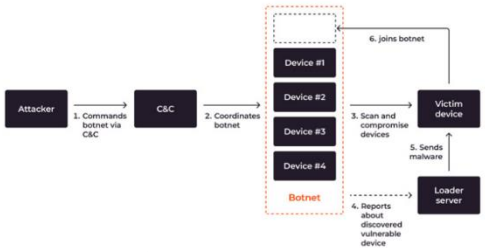
References:

[1] https://brightsec.com/blog/api-security/
[2] https://www.wallarm.com/what/api-security-tutorial
[3] https://www.techtarget.com/searchapparchitecture/definition/API-security
[4] https://threatpost.com/new-trickbot-variant-updates-anti-analysis-tricks/153616/

Trends

IoT Devices Spark New DDoS Alert

Source: https://thehackernews.com/



Process flow, demonstrating scanning, compromising, infecting and joining a new device to a botnet

The Internet of Things (IoT) has transformed efficiency across a range of industries, including healthcare and logistics, but it has also introduced new security risks like Distributed Denial-of-Service (DDoS) attacks that are IoT-driven. Due to the increasing usage of IoT devices, IoT-driven attacks are expected to grow in scale and complexity. DDoS attacks stand out among various cybersecurity risks as it is extremely difficult to mitigate. IoT devices are perfect targets for these DDoS attacks because of their distributed architecture, which makes it hard to detect and stop the malicious traffic and the mitigation is also difficult for DDoS attacks. Unpatched, unmanaged, misconfigured, IoT devices are at risk of becoming part of a botnet. To expand the botnet, an attacker hack new IoT devices. This hacking process involves two entities: the botnet itself and the loader server, a special server that infects other devices. In the first half of 2023 alone, IoT-driven DDoS attacks surged by 300%, resulting in an estimated $2.5 billion global financial loss. 90% of sophisticated, multi-vector DDoS attacks in 2023 were botnet-based. It is suggested to implement multi-layer security protocols for protection against IoT-driven botnet DDoS attacks.

Vulnerability Watch

Multiple Critical Vulnerabilities in Siemens SIMATIC CN 4100

Source: https://nvd.nist.gov, https://cert-portal.siemens.com/

https://mall.industry.siemens.com/

It has been discovered that SIMATIC CN 4100 is vulnerable to improper access control and insecure default configurations. The SIMATIC CN 4100 is a communication node that allows connecting third-party systems helping to implement system concepts for process control technology. The improper access control vulnerability leads to privilege escalation and has been assigned CVE ID CVE-2023-29130 with CVSS score 10.0. The insecure default configurations vulnerability can allow an attacker to bypass network isolation and has been assigned CVE ID CVE-2023-29131 with CVSS score 10.0. Siemens has released an update for SIMATIC CN 4100 and recommends update to the latest version.

Critical Vulnerability in vm2

Source: https://nvd.nist.gov/vuln/detail/CVE-2023-37903

The Node.js custom inspect function allows attackers to escape the sandbox and run arbitrary code.

Critical vulnerability of CVSS score 10.0 with CVE ID CVE-2023-37903 has been discovered in vm2. vm2 is an open source vm/sandbox for Node.js. The Node.js custom inspect function allows attackers to escape the sandbox and run arbitrary code. The affected versions are vm2 up to and including 3.9.19. There are no patches and no known workarounds.

Critical Vulnerability in QEMU

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-36648

A vulnerability with CVE ID CVE-2022-36648 having CVSS score 10.0 has been discovered in the hardware emulation of the of_dpa_cmd_add_l2_flood function of rocker device model in QEMU. QEMU is a machine emulator that can run operating systems and programs for one machine on a different machine. The affected versions are QEMU 7.0.0 and earlier. By exploiting this vulnerability, remote attackers can crash the host qemu and potentially execute code on the host via executing a malformed program in the guest OS.

https: http://qemu.weilnetz.de/icon/

Critical Vulnerability in GitHub Repository mlflow/mlflow

Source: https://nvd.nist.gov/vuln/detail/CVE-2023-3765

Critical vulnerability with CVE ID CVE-2023-3765 having CVSS score 10.0 has been discovered in GitHub repository mlflow/mlflow. MLflow is a platform to streamline machine learning development, including tracking experiments, packaging code into reproducible runs, and sharing and deploying models. mlflow/mlflow application has been found vulnerable to an Absolute Path Traversal vulnerability. The affected versions are GitHub repository mlflow/mlflow prior to 2.5.0.

mlflow/mlflow application has been found vulnerable to an Absolute Path Traversal vulnerability.

Critical Vulnerability in Kirby

Source: https://nvd.nist.gov/, https://github.com/

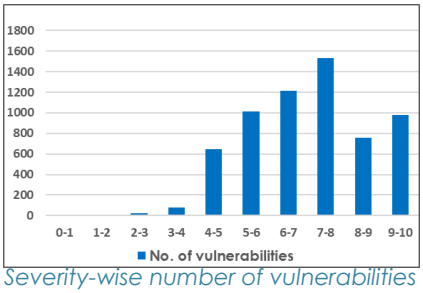
Critical XML External Entity (XXE) vulnerability having CVE ID CVE-2023-38490 and CVSS score 10.0 has been identified in Kirby, a content management system. If an attacker has control over the name of the external file, this vulnerability can be exploited for a various system impacts, such as the disclosure of internal or confidential data stored on the server (arbitrary file disclosure) or the execution of network requests on the server's behalf (server-side request forgery). This vulnerability has been patched in Kirby 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6.A

Critical XML External Entity (XXE) vulnerability having CVE ID CVE-2023-38490 and CVSS score 10.0 has been identified in Kirby, a content management system.

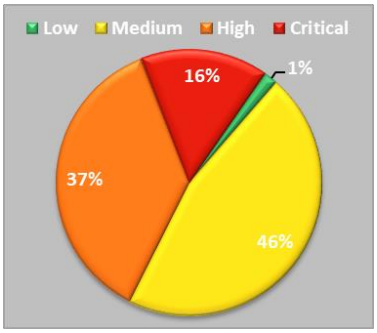
Quarterly Vulnerability Analysis Report

Knowledge Management Team, NCIIPC

During third quarter of 2023, a total of 6257 vulnerabilities have been observed, out of which majority of vulnerabilities have score ranging from 4-7. 16 percent of total vulnerabilities reported were of critical severity. Microsoft, Google, Apple, Linux and Mozilla were the top five vendors having 21% of total reported vulnerabilities.

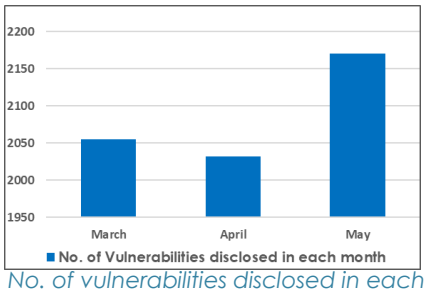


Severity-wise number of vulnerabilities

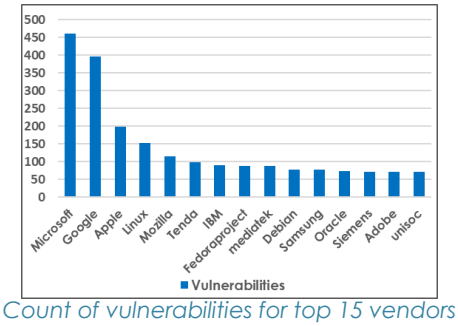


Severity-wise share of vulnerabilities

Severity	CVSSv3 Score	Number of Vulnerabilities			Total Vulnerabilities	Severity Total
		Jun'23	Jul'23	Aug'23		
Low	0-1	0	0	0	0	103
	1-2	0	0	0	0	
	2-3	9	7	5	21	
	3-4	24	34	24	82	
Medium	4-5	253	157	237	647	2880
	5-6	340	333	343	1016	
	6-7	401	404	412	1217	
High	7-8	508	530	498	1536	2294
	8-9	257	262	239	758	
Critical	9-10	263	305	412	980	980
Total		2055	2032	2170		6257



No. of vulnerabilities disclosed in each month



Count of vulnerabilities for top 15 vendors

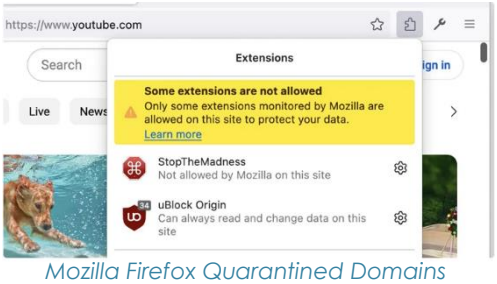
S. No.	Vendor	No. of Vulnerabilities			Total
		Jun'23	Jul'23	Aug'23	
1.	Microsoft	112	187	162	461
2.	Google	145	114	137	396
3.	Apple	76	70	53	199
4.	Linux	46	65	42	153
5.	Mozilla	85	17	14	116
6.	Tenda	13	21	65	99
7.	IBM	23	40	28	91
8.	Fedoraproject	26	29	34	89
9.	mediatek	31	23	35	89
10.	Debian	18	20	40	78
11.	Samsung	7	39	31	77
12.	Oracle	0	71	2	73
13.	Siemens	15	22	34	71
14.	Adobe	18	16	37	71
15.	unisoc	6	57	8	71

Security App

New Mozilla Feature Blocks Risky Add-Ons

Source: https://thehackernews.com/

Mozilla in its latest release 115.0 has introduced a new back-end feature to only allow some extensions monitored by Mozilla to run on specific websites due to security concerns. Some add-ons may be blocked from running on certain sites as part of new feature called Quarantined Domains. This feature allows to prevent attacks by malicious actors targeting specific domains. Users have more control over the settings for each add-on starting with Firefox version 116.0. The existing capability of Mozilla is to remotely disable individual extensions pose a risk to user privacy and security. In the current implementation, warning appears in the Extension popup rather than on the Extensions icon in the current implementation. It turns out that when an extension is pinned to the toolbar, it no longer appears in the Extensions popup. Consequently, the quarantined domains warning no longer appears in the Extension popup. Mozilla is intended to improve the user experience in future releases.



Mozilla Firefox Quarantined Domains

Users have more control over the settings for each add-on starting with Firefox version 116.0

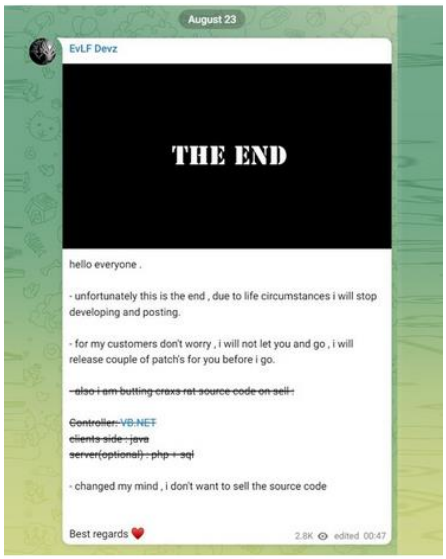
Mobile Security

Google Play Apps Load Ads Even when the Screen is Off

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

43 Android applications with over 2.5M installations have been found in the Google Play Store that displayed advertisement even when the phone's screen was off, draining device's battery. It was discovered and subsequently reported to Google by McAfee's Mobile Research Team as it violates Play Store policies. In response, Google removed those apps from its Play Store. Those apps were mostly media streaming apps or news aggregators. The target audience was mostly Korean. But the same scamming techniques could easily be used in other app categories with wider user bases as well. Although these applications are considered adware, once these adware apps are installed on the device, they wait for a few weeks before they start running their ads-fraud campaigns to trick the users and avoid detection by Google reviewers. According to McAfee, adware operators can change the adware's dormancy period and other parameters remotely through Firebase Storage and Messaging. Users get prompted to add these apps in exclusion to Android's Power Saving feature during installations which allows these apps to run in the background to fetch and load ads even when the screen is off.

Some of the affected Android apps
Source: McAfee

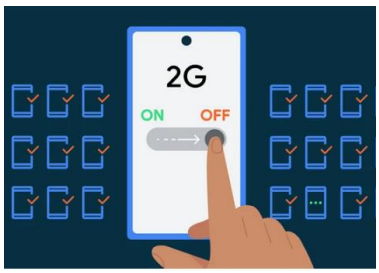


EVLF's Telegram Page (Source: Telegram)

EVLF: Creator of Android Malware CypherRAT and CraxsRAT

Source: https://thehackernews.com/

As per the publication of Cybersecurity firm Cyfirma, CypherRAT and CraxsRAT Remote Access Tools allow an attacker to control the camera, location and microphone of the victim device remotely and perform real-time actions. The CypherRAT and CraxsRAT malwares are also provided to others as part of MaaS (Malware-as-a-Service). It is estimated that 100 threat actors have purchased these tools with lifetime license within last three years. As per Cyfirma, CraxsRAT is one of the most harmful RATs on the Android market today. This RAT has powerful features like google play protect bypass, Live screen view, and command execution shell as well. The app's 'Super Mod' feature makes the app even more dangerous, making it difficult for victims to uninstall it. In addition, the Android malware asks victims to give it access to Android's accessibility services, which allows it to collect a large amount of data that would be useful to cybercriminals, for example call records, contacts, remote storage, location and SMS messages. On August 23, 2023, EVLF announced that they were ceasing work on the project, most likely in reaction to the disclosure of their activities.



By disabling 2G support, IT administrators can ensure that devices under their management exclusively connect to more secure and faster 3G, 4G, or 5G networks.

IT Admins Can Now Disable 2G Networks in Android 14

Source: https://thehackernews.com/

Android is widely used mobile operating system. Android 14, the latest iteration of the platform, introduces several key features designed to bolster security across the board. One standout feature of Android 14 is the newfound control that IT administrators have over network connectivity. While 2G networks were revolutionary in their time, they are now considered outdated and insecure for modern data transmission. The slow data speeds and lack of encryption make 2G networks susceptible to various security threats, including eavesdropping and data interception. By disabling 2G support, IT administrators can ensure that devices under their management exclusively connect to more secure and faster 3G, 4G, or 5G networks. This shift not only enhances data security but also improves the performance and reliability of mobile connections. Enabling this security feature is straightforward for IT administrators. They can access it through the device management console, where they have the option to toggle 2G network support on or off for each device within their organisation.

How Android Malware Slips onto Google Play Store: Explained

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

Google Play Store is the primary source for Android users to discover, download, and update their apps. Google employs a

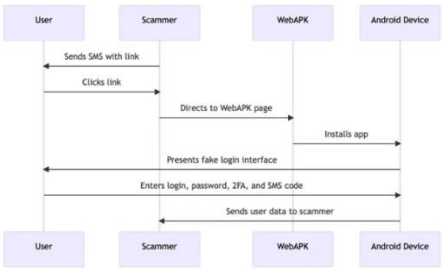
multi-layered approach to app security, which includes automated scans, human reviews, and Play Protect, a built-in security feature on Android devices. However, no system is foolproof, and malware occasionally finds its way in. To explain this Google highlighted a malware named SharkBot, spotted by Cleafy's Threat Intelligence Team in Oct-2021 and known for utilising this technique. SharkBot is banking malware that will make unauthorised money transfers via the ATS protocol (Automated Transfer Service) after compromising an Android device. To evade detection by Play Store systems, SharkBot have adopted the technique of releasing versions with limited functionality on Google Play, hide their apps' suspicious nature. However, once a user downloads the limited functionality trojanised app, it downloads the full version of the Trojan App. It's important to note that Google is continuously improving its security measures to counter these threats. Additionally, they provide regular updates to Play Protect to enhance device-level security.

SharkBot is banking malware that will make unauthorised money transfers via the ATS protocol (Automated Transfer Service) after compromising an Android device.

Hackers Abuses WebAPK to Exploit Android Users

Source: https://thehackernews.com/

Hackers are using WebAPK technology to trick Android users into mistakenly installing malicious apps. WebAPK allows Android users to install Progressive Web Apps (PWAs) on their home screen without using the Play Store. According to the researchers from CSIRT KNF, the threat actors send text messages to banking customers claiming that they need to update their mobile banking app. Google's documentation explains that when a user installs a PWA using WebAPK, the minting server 'mints' (packages) and signs an APK for the PWA. The browser automatically installs the app on the user device without any notification. As the apk is signed by trusted party, it gets installed without compromising security like any app from an official store and the sideloading of app is not required. Once the malicious app is installed it urges user for login credentials and two factor authentication tokens which ultimately resulting to theft. To counter such activity, it is recommended to block the websites which uses WebAPK mechanism to carry out phishing attacks.



Workflow of Hacker Exploitation of WebAPK

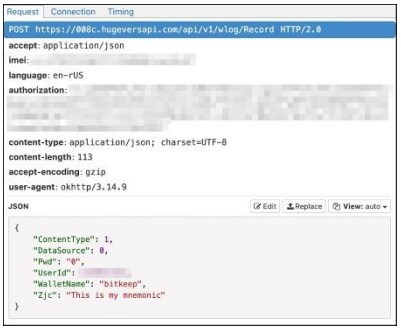
Google's documentation explains that when a user installs a PWA using WebAPK, the minting server 'mints' (packages) and signs an APK for the PWA.

Cherryblos Malware Uses OCR Technique to Steal Passwords

Source: https://thehackernews.com/

Trend Micro has recently discovered two new malwares namely Cherryblos and Fake Trade on Google Playstore which steal the cryptocurrency credentials and funds. CherryBlos abuses the Optical Character Recognition (OCR) techniques to gather sensitive data stored in pictures. It was observed that the both malwares use the same network infrastructure and certificates

CherryBlos abuses the Optical Character Recognition (OCR) techniques to gather sensitive data stored in pictures.



which indicates that the same threat actors have created them. Upon installation, CherryBlos uses the Accessibility service permissions to fetch configuration files from the command-and-control server and prevent user from stopping the malicious app. Trend Micro discovered connections to a campaign, where 31 scam apps called 'FakeTrade' collectively were using the same Command and Control network infrastructure and certificates as the CherryBlos malware.

NCIIPC Initiatives

Workshop on Cyber Security Awareness by NCIIPC

A Cyber Security Awareness Session was organised by NCIIPC South zone on 14 June 2023 at Vikas Soudha, State Government of Karnataka. The following topics were discussed in the awareness session:

- NCIIPC and Information Technology Act
- Cyber security related major issues and their preventive measures
- Different threat vectors
- Ransomware Attacks and Prevention
- Incident Reporting & Management
- Cyber Crisis Management Plan (CCMP)

A Cyber Security Awareness workshop was also organised by NCIIPC South zone on 29 August 2023 at Karnataka Power Corporation Limited (KPCL). The following topics were discussed in the workshop:

- Information Technology Act and NCIIPC
- Threat Vectors, Ransomware and Prevention
- Cyber Crisis Management Plan (CCMP)
- Dos and Don'ts

NCIIPC at Nullcon Goa 2023

DG NCIIPC at Nullcon 2023

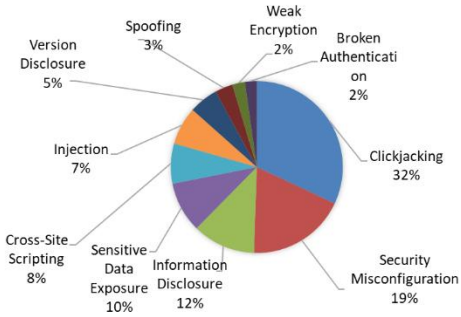
NCIIPC participated in NULLCON Goa 2023 conference. Sh. Navin Kumar Singh, DG NCIIPC hosted a discussion on NCIIPC's key role, role of the community, emerging technologies in CII. The other speakers were Sh. M V Shashadri (CISO, NSE), Sh. Mathan Babu Kasilingam (CISO, Vodafone), and Ms. Madhavi Purandare (CISO, ICICI bank). NCIIPC partcipated in two panel discussions. The first was Critical Information Infrastructure(CII) Protection: Challenges and Opportunities- How can the Nullcon Community Contribute held on 23 September 2023 and second was C4CII - Securing Use of Cloud in Critical Information Infrastructure held on 24th September 2023.

NCIIPC Responsible Vulnerability Disclosure Program

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

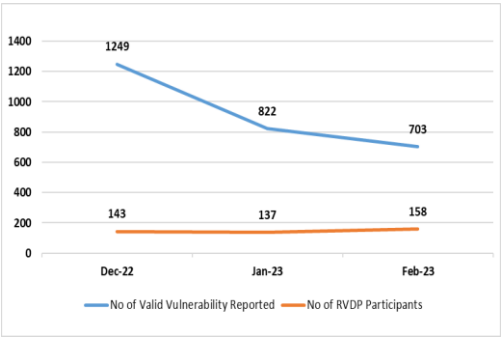
The NCIIPC Responsible Vulnerability Disclosure Program provides opportunity for researchers to disclose vulnerability observed in Nation's Critical Information Infrastructure. There are 1860 vulnerabilities reported during the third quarter of 2023. The top 10 vulnerabilities are:

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



Around 426 researchers participated in RVDP programme during the third quarter of 2023. NCIIPC acknowledges following top 15 researchers for their contributions (names are in alphabetical order):

- Abhijith Jd
- Affan Ahmed
- Akanksha Verma
- Anant Deoashish Beck
- Ashesh Chakraborty
- Devansh
- Dhabaleshwar Das
- Hrishikesh Patra
- Jagat Singh
- Michael Gomes
- Nijith Wilson
- No Name (Name of researcher is not available)
- Sharanabasappa Kalyan
- Shubhranshu Gorai
- Uddesh Vaidya



Last three months' timeline chart for vulnerabilities and RVDP participants

Sh. Navin Kumar Singh,DG NCIIPC at cOcOn@16 Conference

NCIIPC at Cocon 2023

The 16th edition of the Cocon conference, organised by Kerala Police, in association with the Information Security Research Association (ISRA) was held at Grand Hyatt, Kochi from 6th to 7th October 2023. Around 1,300 delegates from 32 countries took part in the conference. Sh. Arun Kumar Sinha, Chairman National Technical Research Organisation (NTRO), and Sh. S. Somanath, Chairman Indian Space Research Organisation (ISRO), were among the keynote speakers. Sh. Navin Kumar Singh Director General, NCIIPC was also panelist at Cocon@16 conference.

Sh. Lokesh Garg, DDG NCIIPC at International Conference on Cyber Security in Power Sector

Sh. Neeraj Saini at International Conference on Cyber Security in Power Sector

NCIIPC at International Conference on Cyber Security in Power Sector

The CIGRE India & Central Board of Irrigation & Power, India jointly with Grid Controller of India Limited (GRID-INDIA) organised an one-day International Conference on 'Cyber Security in Power Sector – Collaboration is the Key to Success' on 12th October 2023 at New Delhi. The event was organised under the aegis of CIGRE Study Committee D2 on Information Systems and Telecommunications. Sh. Lokesh Garg, Dy. Director General, NCIIPC was in the panel discussion on the 'Regulatory Framework for Cyber Security in Power Sector-needs & Expectation', moderated by CISO GRID-India. Apart from this, Sh. Neeraj Saini, Director NCIIPC also delivered talk on 'Cyber Security & Incident Management' where he covered the important aspects Incident Management and Response Plan, Modern Incident Response Life Cycle, Key areas of concerns in Power Sector etc.

Upcoming Events - Global

October 2023

- Hacks & Hops 2023, Minneapolis 5 Oct
- IAPP Privacy Security Risk 2023, San Diego 5-6 Oct
- California Cybersecurity Education Summit, Sacramento 12 Oct
- SecureWorld St. Louis, St. Louis 19 Oct
- CISOs, OT/ICS & IoT Cyber Security Professionals Meetup, Houston 19 Oct
- SGF-IEC Week 2023, Amsterdam 16-20 Oct
- Columbus Cyber Security Summit, Columbus 27 Oct
- OWASP 2023 Global AppSec, Washington DC 30 Oct-3 Nov

November 2023

- Scottsdale Cyber Security Summit, Scottsdale 1 Nov
- INTERFACE Omaha 2023, Omaha 2 Nov
- Ransomware Resilience Conference 2023, Kuala Lumpur 6-7 Nov
- SecureWorld Seattle, Washington 8-9 Nov
- CODE BLUE 2023, Tokyo 8-9 Nov
- Black Hat Middle East and Africa, Malham 14-16 Nov
- Corinium: CISO Indonesia 2023, Jakarta 29 Nov
- The Norfolk Cyber Conference 2023, Norwich 30 Nov

December 2023

- Bsides Cape Town 2023, Cape Town 2 Dec
- NICE K12 Cybersecurity Education Conference 2023, Arizona 4-5 Dec
- INTERFACE Seattle 2023, Seattle 7 Dec
- IT-Tage 2023, Frankfurt 11-14 Dec
- SecureWorld Pacific, Virtual 13 Dec
- Houston Cybersecurity Conference, Houston 13 Dec
- International Conference on Information Theory and Machine Learning, Virtual 30-31 Dec

OCTOBER 2023

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				

NOVEMBER 2023

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		

DECEMBER 2023

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

JANUARY 2024

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			

January 2024

- Bsides Cape Town 2023, Cape Town 2 Dec
- INTERSEC Dubai 2024, Dubai 16-18 Jan
- Cybertech Global Tel Aviv 2024, Tel Aviv 29-31 Jan
- IT Security Insights 2024, Stockholm 31 Jan
- IT-Defense 2024, Stuttgart 31 Jan-2 Feb

Upcoming Events - India

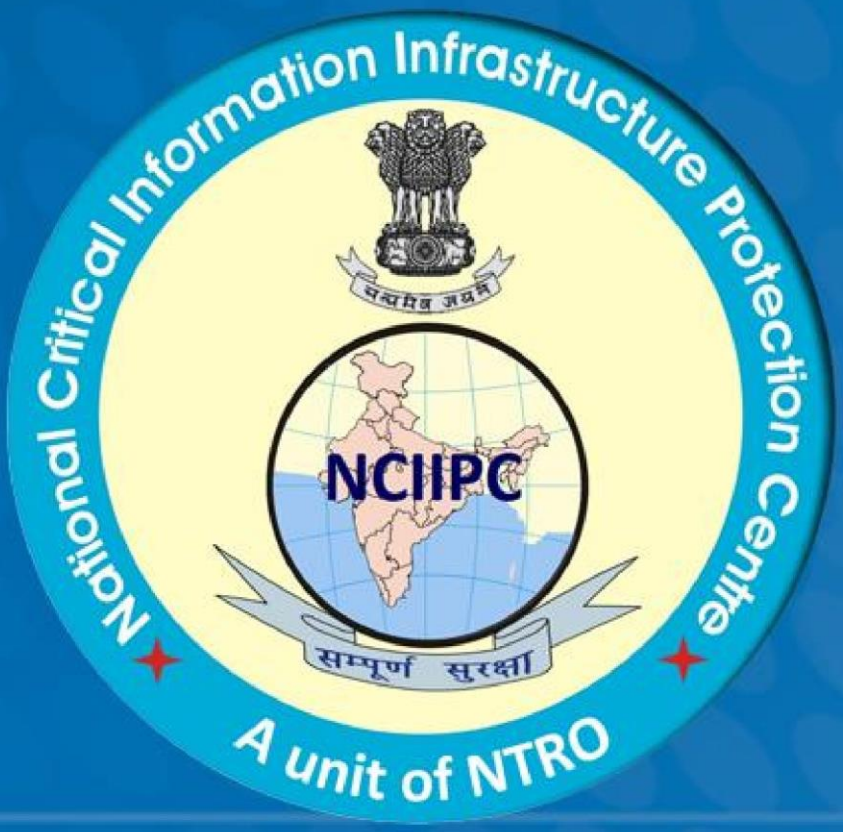
- TECHSPO Delhi NCR 2023, New Delhi 4-5 Oct
- BSides Ahmedabad 2023, Ahmedabad 6 Oct
- Cypher India 2023, Bengaluru 11-13 Oct
- Cybersecurity Summit: Mumbai, Mumbai 1 Nov
- BSides Odisha, Bhubaneswar 2 Dec

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

- API: Application Programming Interface
- APT: Advanced Persistent Threat
- BEC: Business Email Compromise
- C2: Command-and-Control
- CCMP: Cyber Crisis Management Plan
- CIO: Critical Infrastructure Organisation
- CISA: Cybersecurity & Infrastructure Security Agency
- CSP: Cloud Service Provider
- DDoS: Distributed Denial-of-Service
- DIB: Defence Industrial Base
- DPDPB: Digital Personal Data Protection Bill
- ESG: Email Security Gateway
- FBI: Federal Bureau of Investigation
- IABs: Initial Access Brokers
- IoT: Internet of Thing
- KPCL: Karnataka Power Corporation Limited
- MFA: Multi-Factor Authentication
- MSA: Microsoft Account
- OCR: Optical Character Recognition
- Phaas: Phishing-as-a-service
- PWA: Progressive Web App
- RAI: Responsible AI
- SCA: Secure Cloud Access
- SOHO: Small Office/Home Office
- UAL: Unified Audit Logging
- XXE: XML External Entity

Notes



Feedback/Contribution

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