**Cyber Security Advisories**

**Date: 28 June 2024**

1. **Adv/2024/Jun/024**

It has been observed that the Underground Team ransomware group is using new tactics, techniques and procedures (TTPs) which lead to the deployment of ransomware variants and exfiltration of sensitive information.  Threat actor uses API functions to identify system drives and file systems, which allows them to encrypt files efficiently on the targeted system. After encryption, the adversary conducts defense evasion tactics via a CMD file named “temp.cmd” to delete specified files, clear event logs and remove traces of tool execution. Adversary  conducts post-exploitation activities such as establishing persistence, disrupting system recovery mechanisms and staging activities. The “vssadmin.exe delete shadows /all /quiet” command is used to delete all volume shadow copies on the system, which is used by Windows for restoring previous versions of files. The Microsoft SQL server service is forcefully disabled via the “net stop MSSQLSERVER /f /m” command to disrupt critical database operations. Threat actor locks out all other users to gain exclusive access to the database by restarting SQL server in single-user mode.

**IOCs: IOC\_Adv2024Jun024.txt attached**

1. **Adv/2024/Jun/025**

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\_Adv2024Jun025.txt attached**

1. **Adv/2024/Jun/026**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages. The Spear-phishing email contains an archive file named “Application Form brouchers.zip” which contains three files, two of them “Application For.pdf” & “Housing Project Brouchers.docx” are non-malicious files while “Password.elf” is a malware. Upon click, PDF and DOCX file asks for password. Victim is misguided to open the “Password.elf” to get password. Once the file is executed, it gets decompressed and malware is executed in the background.

The malware performs following functions:-

a) Defense Evasion(obfuscated files or information, Indicator file Removal, Hidden Files and  Directories)

b) Discovery(Security Software Discovery)

c) Command and Control(Application Layer Protocol)

1. **Adv/2024/Jun/027**

It has been observed that ShrinkLocker is a new ransomware variant, written in Visual Basic Script (VBScript). It uses BitLocker (a legitimate encryption technology) to target vulnerable systems. After intrusion into the victim machine, the variant first checks if the target machine's operating system is running Windows versions later than Vista before initiating encryption with BitLocker. With the use of Bitlocker, the script changes the operating system’s boot parameters and encrypts the hard disk partitions. It has the capability to infect both older and newer versions of the Windows operating system upto Windows Server 2008.

I**OCs: IOC\_Adv2024Jun027.txt attached**

1. **Adv/2024/Jun/028**

Reference is made to earlier advisories on the above subject.

It has been observed that group is engage in cyber espionage operations against government entities .The group used spear phishing emails to access the victim’s systems. The email contains attachments in the form of documents embedded with obfuscated Visual Basic Script (VBScript) and JavaScript files.

The group have been observed using various tools such as SunSeed LUA script, WasabiSeed VBS and NODEBOT (JavaScript malware designed to bypass anti-virus software detections). Asylum Ambuscade  perform the following actions:

1. Deliver Cobalt Strike for post-compromise activities and an undisclosed remote access Trojan (RAT).

2. Take screenshots and log keystrokes, Gather the victim host and Active Directory information via Windows Management Instrumentation (WMI) queries.

3. Download and install hidden virtual network computing (hVNC). HVNC allowed Asylum Ambuscade to open a hidden instance in the form of a virtual desktop and control it covertly instead of taking over the victim's desktop.

**IOCs: IOC\_Adv2024Jun028.txt attached**

1. **Adv/2024/Jun/029**

t has been observed that threat group dubbed as  "Velvet Ant" is active in the cyber threat landscape. The threat actor tried to exploit the vulnerable F5 BIG-IP which is a network device widely used for load balancing and application delivery to gain control over system.  Threat group utilizes the backdoor PlugX (also known as Korplug) in espionage operations.

**Toolset Used by Velvet Ant:**

VELVETSTING: This tool is used for connecting to the threat actor's Command and Control (C&C) server and executing commands. It likely facilitates remote control and data exfiltration.

VELVETTAP: Designed for capturing network packets, this tool enables the threat actors to monitor and intercept network communications, potentially extracting sensitive information.

SAMRID: Identified as an open-source SOCKS proxy tunneller available on GitHub. This tool could be used by Velvet Ant to anonymize their network traffic or evade detection while maintaining communication with their infrastructure.

ESRDE: Similar to VELVETSTING but uses bash instead of csh (C shell). This tool likely serves a similar purpose in terms of command execution and control.

**IOCs: IOC\_Adv2024Jun029.txt attached**

1. **Adv/2024/Jun/030**

It has been observed that a critical-severity vulnerability, tracked as CVE-2024-30103 is affecting Microsoft Outlook. The vulnerability has been assigned with CVSS Score - 8.8. This zero-click remote code execution (RCE) flaw arises from Outlook's mishandling of specific email content. Whenever a recipient opens a specially designed email containing malicious code, the exploit is triggered which allows attackers to run arbitrary code potentially leading to unauthorized access, data theft, and system compromise.

**Recommendation:-**

* It is recommended to prioritize patching this vulnerability promptly to mitigate the risk of potential cyberattacks.

**Reference**: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-30103

1. **Adv/2024/Jun/031**

Reference is made to earlier advisories on QuasarRAT  Malware.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jun031.txt attached**

1. **Adv/2024/Jun/032**

Reference is made to earlier advisories on RedLine Stealer.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jun032.txt attached**

1. **Adv/2024/Jun/033**

Reference is made to earlier advisories on Racoon Malware.

PFA additional IOCs in this regard.

**IOCs: IOC\_Adv2024Jun033.txt attached**

1. **Adv/2024/Jun/036**

It has been observed that a file-encrypting ransomware variant dubbed as Lucky Ransomware is targeting both Linux and Windows Platforms. Adversary uses asymmetric cryptography (RSA-2048) to encrypt files with file extension ".lucky"

PFA IOCs in this regard.

**IOCs: IOC\_Adv2024Jun036.txt attached**

1. **Adv/2024/Jun/037**

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\_Adv2024Jun037.txt attached**

1. **Adv/2024/Jun/038**

It has been observed that FIN7 cybercrime group aka GOLD NIAGARA, ITG14, Carbon Spider, ELBRUS, and Sangria Tempest is using Ransomware as a Service (RaaS) platforms for their campaigns, such as REvil, CL0P, DarkSide, and BlackMatter. Recently, a malicious campaign adversary has been delivering CL0P ransomware variants with updated functionalities. The ransomware variant integrates three segmented encryption functions into a single unified function, which increases the ransomware’s efficiency. The other variant directly employs Windows Management Instrumentation (WMI) to delete shadowcopy files and to prevent victims from using shadow volume copies to restore data.

The attack chain involves multiple stages. After gaining initial access, FIN7 uses powershell script to load their post-exploitation tools and establish a foothold within victim networks. The attack chain also involves lateral movement and deployment of the ransomware using the Impacket tool “wmiexec.py” and SSH reverse shell.

**IOCs: IOC\_Adv2024Jun038.txt attached**

1. **Adv/2024/Jun/039**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains and phishing web pages. The spear-phishing email contains a malicious link. Upon clicking, it opens the cloned phishing page of NIA with the title “PRESS RELEASE”. Inside the page, there is a “Download” with the headline “Hacked account being operated by Dark/Web OSINT Accounts and List of Involved persons and ID's”. On clicking the download button, it gives a pop-up which asks for the username and password of the NIC email account.

**IOCs: IOC\_Adv2024Jun039.txt attached**