ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 2/21 (October)

Overview

1. Over the last month, ACICE continued to observe significant levels of activity across cyberspace from a variety of actors, ranging from Advanced Persistent Threats (APTs) to cyber-criminals.

State-Sponsored Cyber Activity

2. Alleged state-sponsored APTs continued targeting adversaries within the NATO alliance, as well as entities of interest in Central Asia, for cyber espionage. They also pioneered new forms of malware to evade detection. In September, Talos reported that Turla APT had used the TinyTurla malware as a secondary persistence method on compromised systems in the US, Germany and Afghanistan. TinyTurla malware facilitated the exfiltration and execution of files on victims' systems. In the same month, Microsoft discovered that the Nobelium group had been using a new backdoor, called FoggyWeb, to deploy payloads and steal sensitive information from victims' Active Directory services.

Cybersecurity Trends

3. Ransomware. Ransomware operators appear to be resurfacing, after laying low several months following intense law enforcement scrutiny. In September, the REvil ransomware group reactivated their darkweb payment and data leak sites. Researchers also discovered that new samples of REvil were recently uploaded onto VirusTotal, in a possible sign that REvil campaigns have claimed new victims. Separately, the Groove ransomware group recently leaked 500,000 Fortinet Virtual Private Network credentials online, which could be used by threat actors to access networks to perform data exfiltration, install malware and perform ransomware attacks.

4. Exploitation of Windows Products. Threat actors continued to exploit Windows Products as a means to infiltrate victims. An ongoing Zloader Trojan campaign apparently disabled Windows Defender (or Microsoft Defender Antivirus) on victims' computers to evade detection. It made use of TeamViewer Google ads to redirect targets to fake download sites, which installed Zloader malware payloads on victims' computers. This campaign targeted German and Australian banking customers. Separately, Google researchers spotted malware developers creating malformed code signatures seen as valid in Windows to bypass security software. This tactic was actively used to push OpenSUpdated, a family of riskware, which injects ads into victims' browsers and installs other unwanted programs on their devices. Such campaigns were typically financially-motivated, and targeted victims in the US which download gaming hacks.

Notable Vulnerabilities

5. Several zero-day vulnerabilities and exploits were recently disclosed in Google, Windows and Internet Explorer products.

a. Google. In Sep, Google released Chrome version 93.0.4577.82 for Windows, Mac, and Linux to fix eleven security vulnerabilities, two of which were zero-day vulnerabilities exploited in the wild.

b. Windows. Threat actors have been sharing Windows MSHTML zero-day (CVE-2021-40444) tutorials and exploits on hacking forums, possibly facilitating the spread of more of such attacks.

c. Internet Explorer. In Sep, Microsoft warned of an actively exploited zero-day remote code execution flaw impacting Internet Explorer used to hijack vulnerable Windows systems by leveraging weaponized Office documents.

Global Developments

6. Actions to Curb Ransomware. The US is expected to curb the spread of ransomware by issuing sanctions against cryptocurrency exchanges, wallets and traders used by ransomware gangs.

Contact Details

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

••••

ANNEX A

News Articles

1 Russian State Hackers Use New TinyTurla Malware As Secondary Backdoor
[Link: https://www.bleepingcomputer.com/news/security/russian-state-hackers-use-new-tinyturla-malware-as-secondary-backdoor/]

2 Microsoft: Nobelium Uses Custom Malware to Backdoor Windows Domains
[Link: https://www.bleepingcomputer.com/news/security/microsoft-nobelium-uses-custom-malware-to-backdoor-windows-domains/]

3 REvil Ransomware is Back in Full Attack Mode and Leaking Data
[Link: https://www.bleepingcomputer.com/news/security/revil-ransomware-is-back-in-full-attack-mode-and-leaking-data/]

4 Hackers Leak VPN Account Passwords From 87,000 Fortinet FortiGate Devices
[Link: https://thehackernews.com/2021/09/hackers-leak-vpn-account-passwords-from.html]

5 New Zloader Attacks Disable Windows Defender To Evade Detection
[Link: https://www.bleepingcomputer.com/news/security/new-zloader-attacks-disable-windows-defender-to-evade-detection/]

6 Malware devs trick Windows validation with malformed certs
[Link: https://bleepingcomputer.com/news/security/malware-devs-trick-windows-validation-with-malformed-certs/]

7 Urgent Chrome Update Released to Patch Actively Exploited Zero-Day Vulnerability
[Link: https://thehackernews.com/2021/09/urgent-chrome-update-released-to-patch.html]

8 Google Patches 10th Chrome Zero-Day Exploited in The Wild This Year
[Link: https://www.bleepingcomputer.com/news/google/google-patches-10th-chrome-zero-day-exploited-in-the-wild-this-year/]

9 Windows MSHTML Zero-Day Exploits Shared on Hacking Forums
[Link: https://www.bleepingcomputer.com/news/microsoft/windows-mshtml-zero-day-exploits-shared-on-hacking-forums/]

10 New 0-Day Attack Targeting Windows Users With Microsoft Office Documents
[Link: https://thehackernews.com/2021/09/new-0-day-attack-targeting-windows.html]

11 U.S. to Sanction Crypto Exchanges, Wallets Used by Ransomware
[Link: https://www.bleepingcomputer.com/news/security/us-to-sanction-crypto-exchanges-wallets-used-by-ransomware/]