ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 3/21 (November)

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. [*Note: Please see Annex A for the news articles.*]

State-Sponsored Cyber Activity

2. Alleged state-sponsored APTs continued targeting victims within Southeast Asia, the NATO alliance and Russia for cyber espionage. In particular, the supply chains of telecommunications companies, and Managed Service Providers (MSPs) such as IT or technology providers were prime targets. APTs targeted Asia-based governments, telecommunication and IT services entities using newly discovered rootkits on systems running the latest Windows 10 versions. Separately, Google and Microsoft respectively warned of spear-phishing campaigns against Gmail users by APT 28, and supply chain attacks against technology service providers by Nobelium. Microsoft also warned that US and Israeli defence technology companies were targeted in password spraying attacks. Apart from that, the ChamelGang had reportedly been targeting targeting fuel, energy and aviation industries in Russia.

Cybersecurity Trends

3. Ransomware. Ransomware gangs are rebranding, recruiting new affiliates, and adopting innovative techniques to evade detection and expand their operations. Reports note that the current Karma ransomware had possibly been rebranded from the Nefilim, Nemty and original JSWorm groups, in a possible effort to fly under law enforcement radar. Separately, several reports note that the Trickbot cyber-criminal gang had recruited additional affiliates, leading to an uptick in ransomware compromise cases. Reports also note that the FIN7 cyber-criminal group had set up fake cybersecurity company profiles to recruit and lure technical professionals into conducting ransomware attacks under the guise of pen-testing jobs. Separately, reports note that Russian entities are regularly compromised by Dharma, Phobos, CryLock and Thanos groups ransomware, amongst others.

4. Data Breach. There have been several recent high profile data breaches, affecting governments and private sector retailers. It was reported that an unknown hacker had breached the Argentinian government's IT network to steal personal identifiable information (PII) for the entire population. The intrusion point was said to be an employee's compromised VPN account. Separately, luxury retailer, Neiman Marcus disclosed a data breach impacting approximately 4.6 million customers. The intrusion vector is currently unknown.

Critical Information Infrastructure (CII) Targeting

5. Critical Information Infrastructure (CII) Targeting. This month, sectors such as finance, water, telecommunications and energy continued to be popular targets of exploitation by threat actors, for both disruptive and espionage attacks.

a. Finance. Banking and investment platform MoneyLion's customer accounts were recently compromised in credential stuffing attacks. Threat actors reportedly gained access to customers' accounts using leaked credentials to steal sensitive information and money. MoneyLion's systems were not breached.

b. Water. The U.S. Cybersecurity Infrastructure and Security Agency (CISA) issued an advisory that warned of ransomware attacks disrupting water and wastewater treatment facilities.

c. Telecommunications. Vice reported that Syniverse, which stores call data records for global telecommunications providers such as AT&T, T-Mobile and China Mobile, had been breached by threat actors. This potentially revealed the metadata of billions of subscribers worldwide, including phone numbers, geolocations and SMS message content.

d. Energy. Reports note that gas stations operated by the National Iranian Oil Products Distribution Company (NIOPDC) had suffered an outage, after being hacked by unknown threat actors, affecting Iran's supply of gas.

Notable Vulnerabilities

6. Several emergency patches have been rolled out for Google and Apache products.

a. Google. In Oct, Google released Chrome 94.0.4606.71 for Windows, Mac, and Linux, to fix two zero-day vulnerabilities. Both zero-day vulnerabilities had been exploited in the wild.

b. Apache. Apache released HTTP Web Server 2.4.51 after being informed that a previous security update had not fixed an actively exploited vulnerability.

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 GhostEmperor Hackers Use New Windows Rootkit in Attacks
[Link: https://www.bleepingcomputer.com/news/security/ghostemporer-hackers-use-new-windows-10-rootkit-in-attacks/]

2 Hackers State-Backed Hackers Breach Telcos With Custom Malware
[Link: https://www.bleepingcomputer.com/news/security/state-backed-hackers-breach-telcos-with-custom-malware/]

3 Google warns 14,000 Gmail users targeted by Russian hackers
[Link: https://www.bleepingcomputer.com/news/security/google-warns-14-000-gmail-users-targeted-by-russian-hackers/]

4 SolarWinds hackers, Nobelium, once again strike global IT supply chains, Microsoft warns
[Link: https://www.zdnet.com/article/solarwinds-hacking-group-nobelium-is-now-targeting-the-global-it-supply-chain-microsoft-warns/]

5 ChamelGang APT Group Found Targeting Russian Industries
[Link: https://cyware.com/news/chamelgang-apt-group-found-targeting-russian-industries-0ca0a773/]

6 Microsoft: Iran-linked hackers target US defense tech companies
[Link: https://www.bleepingcomputer.com/news/security/microsoft-iran-linked-hackers-target-us-defense-tech-companies/]

7 New Karma ransomware group likely a Nemty rebrand
[Link: https://www.bleepingcomputer.com/news/security/new-karma-ransomware-group-likely-a-nemty-rebrand/?&web_view=true]

8 TrickBot Gang Enters Cybercrime Elite with Fresh Affiliates
[Link: https://threatpost.com/trickbot-cybercrime-elite-affiliates/175510/]

9 Hacking Gang Creates Fake Firm to Hire Pentesters For Ransomware Attacks
[Link: https://www.bleepingcomputer.com/news/security/hacking-gang-creates-fake-firm-to-hire-pentesters-for-ransomware-attacks/]

10 Russian orgs heavily targeted by smaller tier ransomware gangs
[Link: https://www.bleepingcomputer.com/news/security/russian-orgs-heavily-targeted-by-smaller-tier-ransomware-gangs/]

11 Hacker steals government ID database for Argentina's entire population
[Link: https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population/]

12 Neiman Marcus sends notices of breach to 4.3 million customers
[Link: https://www.bleepingcomputer.com/news/security/neiman-marcus-sends-notices-of-breach-to-43-million-customers/]

13 MoneyLion locks customer accounts after credential stuffing attacks
[Link: https://www.bleepingcomputer.com/news/security/moneylion-locks-customer-accounts-after-credential-stuffing-attacks/]

14 CISA Issues Warning On Cyber Threats Targeting Water and Wastewater Systems
[Link: https://thehackernews.com/2021/10/cisa-issues-warning-on-cyber-threats.html]

15 Company That Routes Billions of Text Messages Quietly Says It Was Hacked
[Link: https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked]

16 Iranian gas stations out of service after distribution network hacked
[Link: https://www.bleepingcomputer.com/news/security/iranian-gas-stations-out-of-service-after-distribution-network-hacked/]

17 Google pushes emergency Chrome update to fix two zero-days
[Link: https://www.bleepingcomputer.com/news/security/google-pushes-emergency-chrome-update-to-fix-two-zero-days/]

18 Apache emergency update fixes incomplete patch for exploited bug
[Link: https://www.bleepingcomputer.com/news/security/apache-emergency-update-fixes-incomplete-patch-for-exploited-bug/]