ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 02/23 (February)

OVERVIEW

1. The start of a new year did not bring respite from the wave of cyber-attacks against countries and commercial entities. The digital battlespace of the Russia-Ukraine conflict also continued to be hotly-contested by threat actors from both sides. Additionally, new vulnerabilities have been discovered in widely-used products from Apple and Cisco.

TARGETED INTRUSIONS

2. In this reporting period, state-linked threat actors continued to target government services and commercial entities. Notable incidents included:

a. South America. APT group 'Blind Eagle', likely based in Colombia, had been spotted using a new toolset that included phishing emails disguised as coming from the Colombian government. The emails contained a link to a malicious PDF that directed victims to a malware executable hosted on the file-sharing service, MediaFire. Blind Eagle was also observed to have targeted Ecuador, in the guise of the Ecuadorian Internal Revenue Service.

b. North Korea. North Korean-linked APT group 'TA444' was identified to be behind a new phishing campaign targeting several industries in education, government, healthcare, and finance. The group had been active since 2014, and stole nearly US$1 billion worth of cryptocurrencies and digital assets in 2022. Some new lures observed included tricking victims with blockchain-related content, fake job opportunities, and salary adjustments. Additionally, the FBI investigations attributed the Jun 2022 hack of the Harmony cryptocurrency platform to North Korea's Lazarus Group. These stolen crypto-assets were then moved and laundered through the RAILFUN privacy protocol.

c. Iran and Russia. The UK's National Cyber Security Centre (NCSC) warned that Iranian and Russian hackers were targeting British politicians and journalists for sensitive data. The hackers pretended to be real contacts, in order to gain trust and lull their victims into receiving emails embedded with malicious code. Specifically, two groups – SEABORGIUM (Russia) and Charming Kitten (Iran) – were identified to have targeted the personal accounts of the former Head of MI6, Sir Richard Dearlove.

d. Russia-Ukraine Conflict. Almost a year since the conflict started, the contestations online continued unabated. It was reported that Russian companies faced the highest wave of DDoS attacks in 2022. There were a total of 21.5 million reported DDoS attacks against about 600 organisations in the country. The public sector was targeted the most, followed by the financial and education sectors. The largest attack was recorded at 760 GB/sec, while the longest attack lasted three months.

CYBERCRIMES

3. In 2022, ransomware-as-a-service continued to be a concern. Despite a growing frequency of incidents, victims were increasingly less willing to pay. This trend was likely influenced by enhanced legal consequences and cybersecurity insurance companies demanding stronger defensive measures before insuring companies. Researchers also indicated that extortion operations would likely continue throughout 2023. Notable developments over January included:

a. Takedown of Hive Ransomware. It was reported that the Hive ransomware group was taken down by law enforcement agencies from multiple countries. The group affected over 1,500 victims in 80 countries, and had earned around US$100 million since June 2021. The FBI was able to access Hive's networks to retrieve the decryption keys, which were distributed to the victims. The Hive servers and websites were then seized by the Dutch and German police.

b. ChatGPT. Cybercriminals were observed using the ChatGPT language model to create malware and ransomware. Since its launch in Nov 2022, reports indicated that ChatGPT was already used to write malware. ChatGPT was particularly popular with cyber-criminal groups, as it made hacking and writing malware more cost-efficient. The creators of ChatGPT have since started to define new ‘responsible-use’ parameters to prevent abuse or misuse by nefarious groups.

REPORTED VULNERABILITIES

4. Notable Vulnerabilities. Major vulnerabilities were reported for Cisco and Apple.

a. Cisco. Cisco Systems warned customers about two critical vulnerabilities (CVE-2023-20025 and CVE-2023-20026) affecting the web management interface of certain Cisco routers. Attackers could send crafted HTTP requests to exploit these vulnerabilities, gain access into targeted devices, and obtain root-level privileges. Cisco noted that these affected products had reached end-of-life and fixes were not available.

b. Apple. Apple warned that a security vulnerability (CVE-2022-42856) had been found in older versions of iPhones and iPads. This vulnerability allowed attackers to access sensitive information and run commands on the operating system using specially crafted web content. Apple first released patches for this vulnerability in Dec 2022, and the most recent update is iOS 12.5.7.

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. Blind Eagle Hacking Group Targets South America With New Tools [Link: https://www.infosecurity-magazine.com/news/blind-eagle-targets-south-america/]

2. TA444: The APT Startup Aimed at Acquisition (of Your Funds). [Link: https://www.proofpoint.com/us/blog/threat-insight/ta444-apt-startup-aimed-at-your-funds]

3. FBI: North Korean Hackers Behind $100M Horizon Bridge Theft. [Link: https://www.coindesk.com/policy/2023/01/23/fbi-north-korean-hackers-behind-100-million-horizon-bridge-theft/]

4. Hackers From Iran and Russia Have 'Ruthlessly' Hit British Journalists and Politicians, GCHQ's Cyber Centre Warns. [Link: https://www.cityam.com/hackers-from-iran-and-russia-have-ruthlessly-hit-british-journalists-and-politicians-gchqs-cyber-centre-warns/]

5. Russia Suffered Record Number of DDoS Attacks Last Year: Report [Link: https://therecord.media/russia-suffered-record-number-of-ddos-attacks-last-year-report/]

6. Fewer Ransomware Victims Are Paying Up. But There's a Catch. [Link:https://www.zdnet.com/article/fewer-ransomware-victims-are-paying-up-but-theres-a-catch]

7. FBI Dismantles Hive Ransomware Network From the Inside, Thwarting Over $130m in Ransom Demands [Link: https://complyadvantage.com/insights/fbi-dismantles-hive-ransomware-network-from-the-inside-thwarting-over-130m-in-ransom-demands/]

8. Cybercriminals Are Using ChatGPT to Create Malware [Link: https://www.cshub.com/malware/news/cybercriminals-are-using-chatgpt-to-create-malware]

9. Cisco Warns of Critical Vulnerability in End-of-Life Routers [Link: https://www.infosecurity-magazine.com/news/cisco-vulnerability-in-end-of-life/]

10. Flash Notice: Apple Zero Day Impacts Older Iphones and Ipads [Link: https://www.avertium.com/resources/threat-reports/apple-zero-day-impacts-older-iphones-and-ipads]