ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 1/22 (January)

OVERVIEW

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

State-Sponsored Cyber Activity

2. Globally, APTs continued to pose a threat to critical industries. They also exploited widely known, public vulnerabilities to gain access to their victims. Several reports noted that Earth Centaur APT had increased its tempo of attacks against transportation and government agencies worldwide. The StrongPity APT reportedly circulated malicious Notepad+ installers to victims whilst Aquatic Panda APT exploited the Log4Shell vulnerability to compromise an undisclosed large academic institution.

Cybersecurity Trends

3. Log4Shell. In early Dec 2021, a zero-day vulnerability was discovered ("Log4Shell"), affecting many versions of the ApacheLog4j library, an open-source Java package used to support activity logging in many popular Java applications. This package was believed to be widely used by global developers such as Amazon, Microsoft, VMWare, Cisco and IBM, affecting millions of applications and services that use the Log4j library. Given that most applications incorporate some form of logging function to track activities and audit purposes, logging libraries such as Log4j have extensive reach and when compromised, have significant implications. Once publicly unveiled, APTs and cyber-criminal groups (such as ransomware and cryptomining gangs) began to actively exploit this vulnerability to fulfil their objectives.

a. Threat Actors. Globally, APTs such as Phosphorous, Hafnium and Aquatic Panda are amongst nation-state threat groups exploiting the Log4shell vulnerability to conduct cyber espionage. Numerous crypto-miners, botnets, and malwares, as well as ransomware such as Khonsari, TellYouThePass and Conti have been found taking advantage of the vulnerability to target vulnerable servers.

b. Mitigating Measures. Although threat actors exploiting Log4shell have adopted a variety of attack pathways, the measures to reduce the risk of the Log4shell vulnerability remain universal. The UK National Cyber Security Centre (NCSC) has offered these suggestions: (a) to immediately install the latest patch, (b) search for unknown instances of Log4j within the organisation, and (c) deploy protective network monitoring/blocking.

4. Ransomware. Ransomware continues to threaten the finance, managed service providers (MSP) and personal consumer goods industries. These include the Cuba, Yanluowang and TellMeYourPass ransomware.

a. Cuba The FBI warned that the Russia-based Cuba ransomware gang (which appends a ".cuba" extension to its encrypted files, and had previously counted US-based payment processor Automatic Funds Transfer Services as one of its victims) earned more than US$43.9 million after compromising at least 49 critical infrastructure entities in the financial, government, healthcare, manufacturing, and information technology sectors. Furthermore, the FBI noted that Cuba ransomware infections were linked to Hancitor malware, delivered via initial access vectors such as phishing emails. The Hancitor malware is a loader known to drop or execute stealers such as Remote Access Trojans (RATs) or other types of ransomware onto victims' computers. The Cuba ransomware gang also used "living-off-the-land" techniques such as Windows Powershell, Psexec etc to obfuscate its tracks.

b. Yanluowang. Separately, reports note that the Yanluowang ransomware had been deployed against US-based finance-linked organisations, manufacturing, IT services, consultancy and engineering companies.

c. TellYouThePass. The TellYouThePass ransomware group also revived its activity of exploiting Log4shell vulnerabilities. While the group's origin is currently unknown, it was reportedly last active in 2020, and mostly targeted Chinese users.

5. Data Breach. Consumer personal data continued being leaked as a result of data breaches. First, users of password manager LastPass were warned that their master passwords had been compromised. Next, four affiliated online sports gear sites disclosed a cyber attack in which threat actors stole credit card information from more than a million customers. Last, smartphone payment provider Line Pay announced that 133,000 users' payment details had been mistakenly published on GitHub.

6. Several zero-day vulnerabilities and exploits were recently disclosed in Apache and Microsoft products. Separately, vulnerabilities continued to be discovered in IT peripherals such as Hewlett-Packard printers, the SanDisk SecureAccess software and MikroTik routers and wireless devices.

a. Apache. Apache released multiple patches to fix the critical remote code execution vulnerability in Log4j version 2.17.0, tracked as CVE-2021-44832.

b. Microsoft. Microsoft rolled out Patch Tuesday updates to address multiple security vulnerabilities in Windows, including flaws being actively exploited to deliver Emotet, Trickbot, or Bazaloader malware payloads. Separately, researchers discovered four vulnerabilities in Microsoft Teams, which enabled URL spoofing or the conduct of Denial of Service (DoS) attacks against Android users.

c. IT Peripherals. IT peripherals are potential cyber attack vectors and whose usage is not limited to any particular sector or industry. Several vulnerabilities affecting at least 150 multi-function printers made by Hewlett-Packard were discovered which could allow attackers to gain full access to the device, conduct buffer overflows, or move laterally across the victim network. Separately, Western Digital fixed a security vulnerability in the SanDisk Secure Access software, which if unpatched, would allow threat actors to brute force users' SecureAccess passwords and access protected files. Apart from that, researchers found at least 300,000 vulnerable IP addresses associated with MikroTik routers and wireless devices, which have apparently since been patched.

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

News Articles

1. China-linked APT group Aquatic Panda leverages Log4Shell in recent attack
   [Link: https://securityaffairs.co/wordpress/126148/apt/aquatic-panda-log4j.html]

2. Multiple flaws in the Log4J library are scaring organizations worldwide while threat actors are already exploiting them. 2.17 is the third fix issued in a week.
   [Link: https://securityaffairs.co/wordpress/125760/hacking/log4j-third-flaw.html?utm_source=rss&utm_medium=rss&utm_campaign=log4j-third-flaw]

3. As Log4Shell Wreaks Havoc, Payroll Service Reports Ransomware Attack
   [Link: https://arstechnica.com/information-technology/2021/12/as-log4shell-wreaks-havoc-payroll-service-reports-ransomware-attack/

4. FBI: Cuba ransomware breached 49 US critical infrastructure orgs
   [Link: https://www.bleepingcomputer.com/news/security/fbi-cuba-ransomware-breached-49-us-critical-infrastructure-orgs/]

5. Yanluowang ransomware operation matures with experienced affiliates
   [Link: https://www.bleepingcomputer.com/news/security/yanluowang-ransomware-operation-matures-with-experienced-affiliates/]

6. TellYouThePass ransomware revived in Linux, Windows Log4j attacks
   [Link: https://www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-revived-in-linux-windows-log4j-attacks/]

7. LastPass Users Warned Their Master Passwords Are Compromised
   [Link: https://www.bleepingcomputer.com/news/security/lastpass-users-warned-their-master-passwords-are-compromised/]

8. Log4j 2.17.1 Out Now, Fixes New Remote Code Execution Bug
   [Link: https://www.bleepingcomputer.com/news/security/log4j-2171-out-now-fixes-new-remote-code-execution-bug/]

9. Microsoft Issues Windows Update to Patch 0-Day Used to Spread Emotet Malware
   [Link: https://thehackernews.com/2021/12/microsoft-issues-windows-update-to.html]

10. 8-year-old HP Printer Vulnerability Affects 150 Printer Models
    [Link: https://www.bleepingcomputer.com/news/security/8-year-old-hp-printer-vulnerability-affects-150-printer-models/]

. . . .