ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 7/22 (Jul)

OVERVIEW

1. In Jun, we continued to observe cyber attacks conducted by both APTs and cyber-criminals. Vulnerabilities in major technological brands such as Microsoft and Windows had also surfaced during the month.

APT Activities

2. APTs continued to refine their tactics, techniques and procedures (TTPs), and toolsets to mask their intent, obfuscate their tracks, evade detection, and conduct cyber espionage. First, Bronze Starlight APT reportedly deployed post-intrusion ransomware to cover up its attempts at cyber espionage and theft of intellectual property against Japanese organisations. Second, Gallium APT reportedly deployed a previously undocumented PingPull Remote Access Trojan (RAT) against financial institutions and government entities in Europe, Southeast Asia, and Africa. Third, the Luo Yu APT reportedly employed man-on-the-side attacks against companies from the defence, logistics and telecommunications sectors, as part of a sophisticated cyber espionage campaign. This involved modifying in-transit network traffic to insert malicious payloads, making it difficult to detect such an attack. Fourth, unknown APTs conducted spear-phishing campaigns targeting former Israeli officials, high-ranking Israeli military personnel, and US public sector executives to gain access to their email accounts. Fifth, a new APT called ToddyCat compromised Microsoft Exchange servers of government and military installations in Iran, India, Taiwan, Vietnam, Malaysia, Indonesia, Slovakia, Russia, and the UK, to steal information for geopolitical advantage.

Cybersecurity Trends

3. Russia-Ukraine Conflict Developments. Key Ukrainian public operators continued to be targeted by cyber attacks, possibly in attempts to disrupt and undermine their operations. The Governmental Computer Emergency Response Team of Ukraine (CERT-UA) has warned of a phishing campaign that deploys the DarkCrystal Remote Access Trojan to target Ukrainian telecommunications operators.

4. Ransomware. Ransomware operators continued to target industries which were sensitive to business downtimes, by exploiting known and unpatched vulnerabilities. We also observed the launch of the first Dark Web bug bounty program, as part of the continued trend of professionalisation of the cyber-crime eco-system.

a. Vice Society. The Vice Society ransomware group breached the municipal network infrastructure of Italy’s Palermo city. This cyber attack caused widespread operational disruptions, affecting video surveillance management, police operations, online bookings, digital communications channels, and partially corrupting some of the city’s network back-up resources. While it has not been disclosed how the attack was carried out, Vice Society has a track record of exploiting known operating system and application vulnerabilities.

b. Alphv/BlackCat. According to Microsoft, Alphv/BlackCat ransomware affiliates are now breaching Microsoft Exchange servers via unpatched vulnerabilities to steal user credentials and harvest sensitive data before dropping their ransomware payload. Notably, reports highlight that Alphv/BlackCat is the first ransomware written in the Rust programming language, exemplifying how threat actors are switching to uncommon programming languages to evade detection.

c. LockBit. The LockBit ransomware group recently released an upgraded version of its ransomware-as-a-service program (LockBit 3.0), and launched the Dark Web’s first bug bounty program. The program offers rewards for personal identifiable information (PII) on high value targets, security exploits, information to fuel doxing campaigns and also fresh cyber-crime ideas. Bounty pay-outs reportedly start at US$1,000.

5. Notable Vulnerabilities. Major vulnerabilities continued to be discovered in software manufactured by major brands, such as Intel and Windows.

a. Microsoft. Researchers discovered a Microsoft Office zero-day vulnerability, dubbed “Follina” (CVE-2022-30190), which threat actors have been actively exploiting via the native Microsoft Support Diagnostic Tool (MSDT). The flaw allows an attacker to remotely execute malicious code without requiring authentication, and is typically delivered via malicious Microsoft Office documents. Microsoft has released a patch for this vulnerability as part of its June 2022 security update.

b. Windows. A newly discovered Windows search zero-day vulnerability could be abused to launch remotely hosted malware. This flaw allows an attacker to exploit the Windows URI protocol handler, “search-ms”, to get applications to launch customised searches on a device. This function could be abused to force the Windows search function to query file shares (such as pulling in the malware executable) from remote hosts. They could then set up a remote Windows share to host malware disguised as security updates and then include the search URI in the phishing attachment.

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. China-Linked APT Bronze Starlight Deploys Ransomware as a Smokescreen
   [Link: https://securityaffairs.co/wordpress/132624/apt/bronze-starlight-deploy-ransomware.html]

2. GALLIUM APT Used a New PingPull RAT in Recent Campaigns [Link: https://securityaffairs.co/wordpress/132217/apt/gallium-apt-pingpull-trojan.html

3. Chinese LuoYu Hackers Using Man-on-the-Side Attacks to Deploy WinDealer Backdoor
   [Link: https://thehackernews.com/2022/06/chinese-luoyu-hackers-using-man-on-side.html?&web_view=true

4. State-Sponsored Phishing Attack Targeted Israeli Military Officials
   [Link: https://threatpost.com/phishing-attack-israeli-officials/179987/]

5. New ToddyCat APT Group Targets Exchange Servers in Asia, Europe
   [Link: https://www.bleepingcomputer.com/news/security/new-toddycat-apt-group-targets-exchange-servers-in-asia-europe/]

6. Ukrainian Telecommunications Operators Hit by DarkCrystal RAT Malware
   [Link: https://securityaffairs.co/wordpress/132651/malware/cert-ua-darkcrystal-rat-attacks.html]

7. Italian City of Palermo Shuts Down All Systems to Fend off Cyberattack
   [Link: https://www.bleepingcomputer.com/news/security/italian-city-of-palermo-shuts-down-all-systems-to-fend-off-cyberattack/]

8. Vice Society Ransomware Claims Attack on Italian City of Palermo

   [Link: https://www.bleepingcomputer.com/news/security/vice-society-ransomware-claims-attack-on-italian-city-of-palermo/]

9. BlackCat Ransomware Gang Targeting Unpatched Microsoft Exchange Servers

   [Link: https://thehackernews.com/2022/06/blackcat-ransomware-gang-targeting.html]

10. Atlassian Confluence Server Bug Under Active Attack to Distribute Ransomware

    [Link: https://www.darkreading.com/attacks-breaches/atlassian-confluence-server-vulnerability-active-attack-ransomware]

11. Microsoft Exchange Servers Are Being Hacked to Deploy Ransomware

    [Link: https://www.techradar.com/news/microsoft-exchange-servers-are-being-hacked-to-deploy-ransomware]

12. LockBit 3.0 Debuts With Ransomware Bug Bounty Program

    [Link: https://www.darkreading.com/threat-intelligence/lockbit-3-debut-bug-bounty-program]

13. Follina. Unpatched Microsoft Office Zero-Day Vulnerability Exploited in the Wild

    [Link: https://grahamcluley.com/follina-unpatched-microsoft-office-zero-day-vulnerability-exploited-in-the-wild/]

14. New Windows Search Zero-Day Added to Microsoft Protocol Nightmare

    [Link: https://www.bleepingcomputer.com/news/security/new-windows-search-zero-day-added-to-microsoft-protocol-nightmare/]