ACICE
ADMM Cybersecurity and
Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 8/22 (August)

OVERVIEW

1. In August, we observed cyber-attacks by numerous APTs and cyber criminals, as well as the emergence of new ransomware groups.

APT ACTIVITIES

2. APTs continued to refine their tactics, techniques and procedures (TTPs), making use of evolving phishing tactics and social engineering to target unsuspecting victims. First, the Lazarus Group reportedly hit aerospace and defence contractors in a worldwide campaign that abused social networks and messaging platforms. Lazarus operatives posed as recruiters on LinkedIn and WhatsApp to approach unsuspecting employees. They would first gain the trust of their victims, before sending them job descriptions or application forms with malicious components embedded within. Second, multiple APTs (Zirconium, APT 35 *aka* Charming Kitten, and TA482) used Twitter to target journalists by posing as other journalists or Twitter employees. The threat actors focused on phishing campaigns to harvest credentials that were subsequently used for surveillance on political journalists. Researchers assessed that the use of such tactics grew by over 20% since 2021, and is projected to increase year-on-year. Third, unknown cyber threat actors hacked the British Army's Twitter and YouTube accounts to promote online crypto-scams and spread fake Non-Fungible Tokens (NFTs). A hacked YouTube account was airing "Ark Invest" live-streams featuring old clips by Elon Musk, to mislead users into visiting cryptocurrency scam sites. While UK officials have raised concerns that this might be a state-sponsored hacking endeavour, such actions are uncommon among state-linked groups.

CYBERSECURITY TRENDS

3. Russia-Ukraine Conflict Developments. Key Ukrainian operators of public services, such as radio broadcaster (TAVR media) and government services, continued to be targeted by cyber-attacks, which disrupted and undermined their operations. According to Ukraine's State Service of Special Communications and Information (SSSCIP), the country's network suffered up to 796 cyber-attacks since 24 Feb 2022. Computer Emergency Response Team of Ukraine (CERT-UA) also observed multiple threat actors, such as APT28 and Sandworm, conducting campaigns exploiting the 'Follina' Vulnerability against Windows Office.

4. Ransomware. New ransomware groups have emerged. These new operators targeted industries by exploiting known and unpatched vulnerabilities. New tools were also used to gain initial access and conduct attacks. A novel tactic was observed to be used where the threat actors allow their victims to search through the stolen data. This tactic apparently encouraged their victims to quickly pay the ransom. Newly discovered groups include:

a. RedAlert Ransomware. RedAlert was observed to have targeted both Windows and Linux VMware ESXi servers. Unlike other ransomware operations, RedAlert only accepts ransom payments in Monero (a cryptocurrency).

b. 0mega Ransomware. 0mega was observed to have targeted enterprises since May 2022 using a 'double extortion' technique. The group would encrypt the victims' servers after stealing the data, and also threaten to sell the copied data unless their ransom demands were met.

c. Luna Ransomware. Luna displayed characteristics consistent with the latest trend in cybercrime. New malware were created, using cross-platform programming languages like Rust and GoLang, to target multiple operating systems.

d. Lilith Ransomware. Lilith was observed to specifically target 64-bit Windows systems. This threat group appeared to favour extorting large companies. However, there was nothing unique about their TTPs.

5. Notable Vulnerabilities. Major vulnerabilities continued to be exploited in software manufactured by major brands, such as Windows, Google and Android applications (apps).

a. Microsoft. Microsoft issued warnings about a known cloud threat actor group, dubbed '8220' mining group. The group targeted Linux systems and installed crypto-mining malware. In the most recent campaign, the group targeted i686 and x86_64 Linux systems using CVE-2019-2725 (Oracle WebLogic) for initial access and CVE-2022-026134 (Atlassian Confluence Server) for Remote Code Execution.

b. Google. Google released a Chrome update (103.0.5060.114) for Windows users to address a high severity zero-day vulnerability (CVE-2022-2294) exploited by attackers in the wild. This vulnerability was described as a heap buffer overflow weakness in Web Real-Time communications. Successful heap overflow exploitation could cause program crashes or arbitrary code execution, as well as to possibly bypass security solutions.

c. Android Apps. Malicious Android apps filled with adware and malware were found on Google Play Store, and installed about 10 million times on mobile devices. These apps performed malicious actions in the background, interacting with hidden elements, and burdening users with charges. Google had since removed the majority of these malicious android apps.

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. Lazarus APT hit aero, defence sector with fake job ads
   [Link: https://www.computerweekly.com/news/252522378/ESET-Lazarus-APT-hit-aero-defence-sector-with-fake-job-ads]

2. The British Army is investigating after its Twitter and YouTube accounts were hijacked
   [Link: https://www.zdnet.com/article/the-british-army-is-investigating-after-its-twitter-and-youtube-accounts-were-hijacked/]

3. British Army’s Twitter and YouTube accounts hacked to promote cryptocurrency scams
   [Link: https://www.cnbc.com/2022/07/04/uk-armys-twitter-and-youtube-accounts-hacked-to-promote-crypto-scams.html]

4. APT groups and clever Twitter schemes
   [Link: https://cyware.com/news/apt-groups-and-clever-twitter-schemes-e5ec423f]

5. APT Groups trapping targets with clever Twitter scheme
   [Link: https://www.hackread.com/apt-groups-trapping-targets-clever-twitter-scheme/]

6. Ukraine targeted by almost 800 cyberattacks since the war started
   [Link: https://www.bleepingcomputer.com/news/security/ukraine-targeted-by-almost-800-cyberattacks-since-the-war-started/]

7. Ransomware gang now lets you search their stolen data
   [Link: https://www.bleepingcomputer.com/news/security/ransomware-gang-now-lets-you-search-their-stolen-data/]

8. RedAlert, LILITH, and 0mega, 3 new ransomware in the wild
   [Link: https://securityaffairs.co/wordpress/133248/cyber-crime/lilith-redalert-0mega-ransomware.html]

9. New 0mega ransomware targets businesses in double-extortion attacks [Link: https://www.bleepingcomputer.com/news/security/new-0mega-ransomware-targets-businesses-in-double-extortion-attacks/]

10. New Luna ransomware encrypts encrypt Windows, Linux, and ESXi systems [Link: https://www.bleepingcomputer.com/news/security/new-luna-ransomware-encrypts-windows-linux-and-esxi-systems/]

11. Microsoft warns of Cryptomining Malware campaign targeting Linux servers [Link: https://thehackernews.com/2022/06/microsoft-warns-of-cryptomining-malware.html]

12. Google patches new Chrome zero-day flaw exploited in attacks [Link: https://www.bleepingcomputer.com/news/security/google-patches-new-chrome-zero-day-flaw-exploited-in-attacks/]

13. New android malware apps installed 10 million times from google play [Link: https://www.bleepingcomputer.com/news/security/new-android-malware-apps-installed-10-million-times-from-google-play/]