ACICE
ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 2/22 (February)

OVERVIEW

1. Over the past month, ACICE continued to discover 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 engage in various types of activities including disruptive and destructive attacks against states, as well as non-government entities and individuals. This highlights the ever-present threat to cybersecurity posed by APTs which impacts not just government agencies, but also commercial companies and individuals.

a. Cyberattacks on Ukraine. On 14 Jan 2022, about 70 Ukrainian government websites, including those belonging to the Defence and Foreign Affairs ministries, were defaced before being taken offline. Distributed denial of service attacks were reportedly also launched against a number of Ukrainian state organisations. Additionally, destructive data-wiping malware was discovered within the systems of "multiple Ukrainian government, non-profit, and IT organisations".

b. Targeting of Individuals. Lazarus APT reportedly targeted job seekers of US defence company Lockheed Martin, using employment-themed spear phishing emails. Separately, MolesRats APT also targeted prominent Palestinians as well as activists and journalists in Turkey, by conducting spear phishing attacks in the form of sending malicious files made to look like legitimate content related to the Israeli-Palestine conflict.

Cybersecurity Trends

3. Ransomware. Ransomware continued to impact business operations and disrupt the provision of services. Operators are increasingly targeting large organisations sensitive to business downtimes, and continue to evolve techniques and tools to evade detection.

a. <u>FIN7</u>. The US FBI warned that the FIN7 criminal group targeted several US companies through packages containing malicious USB devices. The packages, masqueraded as being issued from the US Department of Health & Human Services, were sent to businesses in the US defence, transportation, and insurance industries. Users were tricked into opening the packages and connecting the USB drives to their systems, which then led to the deployment of ransomware.

b. <u>Lapsus$ Ransomware Gang</u>. Reports noted that the Lapsus$ ransomware gang hacked Impresa, Portugal's largest media conglomerate. The attacks compromised Impresa's online IT server infrastructure, rendering its news websites and TV channels offline.

c. <u>TellYouPass</u>. The TellYouPass ransomware, which first surfaced in early 2019 has reportedly re-emerged as a Golang-compiled malware, making it easier to be used against both Windows and Linux platforms. The new malware variant is also able to minimise detection by reducing the signature of its command and control server communications.

4. <u>Critical Information Infrastructure (CII) Targeting</u>. Sectors such as oil and gas, telecommunications and finance continued to be popular targets of exploitation for disruptive and espionage attacks.

a. <u>Energy</u>. Two German fuel supply subsidiaries of Mabanaft group were reportedly forced to operate at limited capacity following an attack in end Jan. The automated systems responsible for filling and emptying storage tanks were apparently rendered offline and impacted 13 distribution terminals across Germany. Affected customers, including Shell, were forced to divert to alternative supply depots. This attack echoed the May 2021 attack on US oil supplier Colonial Pipeline, highlighting the impact of supply chain disruptions.

b. <u>Telecommunications</u>. Two subsidiaries of OTE group, Greece's largest technology company offering fixed and mobile telephony, broadband, and network communication services, were reported to have sensitive data stolen following a cyberattack. The perpetrator used social engineering and brute-forcing to obtain employee credentials via LinkedIn, and then proceeded to use those credentials to extract data from the victim server. The compromised server contained information such as call data and subscriber details including rough positional data, age, gender, and International Mobile Subscriber Identity (IMSI) numbers.

c. <u>Finance</u>. Singapore-based cryptocurrency exchange Crypto.com suffered a cybersecurity breach which resulted in the compromise of about 400 customer accounts. The perpetrators, who managed to bypass the two-factor authentication (2FA) of the affected users while conducting transactions, made unauthorised withdrawals totalling about USD31 million.

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 North Korea's Lazarus APT leverages Windows Update client, GitHub in latest campaign [Link: https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/]

2 MoleRats APT Launches Spy Campaign on Bankers, Politicians, Journalists [Link: https://threatpost.com/molerats-apt-spy-bankers-politicians-journalists/177907/]

3 'Massive cyber attack' shuts down Ukraine government websites [Link: https://www.msn.com/en-gb/news/world/massive-cyber-attack-shuts-down-ukraine-government-websites/ar-AASLoVb]

4 TellYouThePass ransomware returns as a cross-platform Golang threat [Link: https://www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-returns-as-a-cross-platform-golang-threat/]

5 FBI: Hackers use BadUSB to target defense firms with ransomware [Link:https://www.bleepingcomputer.com/news/security/fbi-hackers-use-badusb-to-target-defense-firms-with-ransomware/]

6 Lapsus$ ransomware gang hits SIC, Portugal's largest TV channel [Link: https://securityaffairs.co/wordpress/126236/cyber-crime/impresa-lapsus-ransomware.html?utm_source=rss&utm_medium=rss&utm_campaign=impresa-lapsus-ransomware

7 Cyber-attack strikes German fuel supplies [Link: https://www.bbc.com/news/technology-60215252]

8 Telco fined €9 million for hiding cyberattack impact from customers [Link:https://www.bleepingcomputer.com/news/security/telco-fined-9-million-for-hiding-cyberattack-impact-from-customers/]

9 Singapore-based Crypto.com CEO confirms 400 accounts hacked, says affected customers reimbursed [Link: https://www.straitstimes.com/business/banking/singapore-based-cryptocom-ceo-says-regulators-havent-reached-out-after-hack]