ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 5/22 (May)

OVERVIEW

1. In April, we observed significant levels of cyber activities from a variety of actors. APTs maintained their cyber espionage and financial theft campaigns to fulfil national strategic goals. Cyber attacks continued to be conducted as part of the Russia-Ukraine conflict. Cyber-criminals persisted in their financially motivated campaigns. Vulnerabilities in major technological brands such as Trend Micro, VMware, and Palo Alto and Lenovo also surfaced during the month.

APT Activities

2. Reports observed the conduct of cyber espionage and financial theft campaigns by APTs in support of national strategic goals. First, reports noted that the PinkPanther APT exploited the Log4Shell vulnerability in VMware Horizon servers to deploy backdoors against an unnamed victim's systems to steal sensitive data. In general, PinkPanther typically targeted the global finance, education, beauty and tourism sectors. Second, the APT-C-23 APT targeted high-profile Israeli individuals employed in defence, law enforcement and emergency services-related organisations, as part of phishing campaigns for cyber espionage. Last, the US revealed that the Lazarus group had been breaching cryptocurrency and blockchain industries using compromised cryptocurrency applications. One such cryptocurrency heist against the Ronin Network netted Lazarus US$625 million. Separately, Lazarus had been linked to cyber espionage campaigns against South Korea's chemical sector, and South Korean journalists whose area of work centred around the DPRK.

Cybersecurity Trends

3. Russia-Ukraine Conflict Developments. Cyber attacks continued to be reported during the ongoing Russia-Ukraine conflict, with data leaks being perpetuated by, and occurring on both sides. The Ukrainian CERT also reported that it had thwarted an attack against an unnamed Ukrainian electricity provider.

1.

a. Data Leaks. The *Anonymous* hacktivist group has launched multiple campaigns against Russian government agencies and organisations since the onset of the conflict. To date, it has published approximately 5.8 TB of Russian data on the public blog Distributed Denial of Secrets. Separately, the Ukrainian defence ministry reportedly hacked and leaked the personal data of 620 Russian domestic intelligence agency officers. Such campaigns presumably have the intended effect of embarrassing and undermining the legitimacy of the respective victim governments.

b. Cyber Attack Against Ukrainian Electrical Grid Provider. The Ukrainian CERT reportedly thwarted an attempt by a threat actor to disconnect an unnamed Ukrainian provider's electrical substations using the Industroyer2 malware. If successful, this attack would have disrupted the flow of electricity to multiple Ukrainian households.

4. Ransomware. Ransomware operators continued to target major firms which were sensitive to business downtimes, for more lucrative pay-outs.

a. NB65. A new hacking group called NB65 had repurposed the Conti ransomware group's source code for its own use, typically against Russian organisations. Alleged Russian victims include the document management operator Tensor, space agency Roscosmos and VGTRK, the state-owned Russian Television and Radio broadcaster. These cyber attacks were apparently conducted in response to the Russo-Ukraine conflict.

b. Lapsus$. Reports revealed that the Lapsus$ ransomware group had breached US telecommunications operator T-mobile using stolen employee credentials, and had also stolen its source code.

5. Notable Vulnerabilities. Major vulnerabilities continued to be discovered in software and hardware manufactured by major brands, such as Trend Micro, VMWare, Palo Alto and Lenovo.

a. Software Vulnerabilities. Trend Micro, VMware and Palo Alto recently patched high severity security flaws in their products. These respectively (1) facilitated arbitrary code execution, (2) launched remote code execution, (3) left it vulnerable to an OpenSSL infinite loop bug.

b. Hardware Vulnerabilities. It was revealed that a variety of Lenovo laptops contained firmware-level vulnerabilities that would enable threat actors to deploy malware that could maintain persistence even after reboots or OS re-installations.

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. Hamas-Linked Threat Actors Target High-Profile Israeli Individuals
   [Link: https://securityaffairs.co/wordpress/129973/apt/hamas-linked-apt-targets-israeli-individuals.html]

2. U.S. Gov Believes Lazarus APT Is Behind Ronin Validator Cyber heist
   [Link: https://securityaffairs.co/wordpress/130260/apt/lazarus-ronin-validator-cyber-heist.html]

3. Lazarus Eyes Chemical Sector in South Korea
   [Link: https://cyware.com/news/lazarus-eyes-chemical-sector-in-south-korea-f26c757a/]

4. North Korea-Linked APT37 Targets Journalists With GOLDBACKDOOR
   [Link: https://securityaffairs.co/wordpress/130606/apt/apt37-targets-journalists-goldbackdoor.html]

5. Since Declaring War on Russia Anonymous Leaked 5.8 TB of Russian data
   [Link: https://securityaffairs.co/wordpress/130554/hacktivism/anonymous-leaked-5-8-tb-russian-data.html]

6. Ukraine Intelligence Leaks Names of 620 Alleged Russian FSB Agents
   [Link: https://securityaffairs.co/wordpress/129736/cyber-warfare-2/ukraine-intelligence-leaks-names-of-620-alleged-russian-fsb-agents.html]

7. The Unceasing Action of Anonymous Against Russia
   [Link: https://securityaffairs.co/wordpress/130262/hacktivism/anonymous-targets-russian-entities.html]

8. Sandworm Hackers Fail to Take Down Ukrainian Energy Provider
   [Link: https://www.bleepingcomputer.com/news/security/sandworm-hackers-fail-to-take-down-ukrainian-energy-provider/]

9. T-Mobile Confirms Lapsus$ Hackers Breached Internal Systems
   [Link: https://www.bleepingcomputer.com/news/security/t-mobile-confirms-lapsus-hackers-breached-internal-systems/]

10. Trend Micro Fixes Actively Exploited Remote Code Execution Bug
    [Link: https://www.bleepingcomputer.com/news/security/trend-micro-fixes-actively-exploited-remote-code-execution-bug/]

11. VMware Releases Critical Patches for New Vulnerabilities Affecting Multiple Products
    [Link: https://thehackernews.com/2022/04/vmware-releases-critical-patches-for.html]

12. Palo Alto Networks Firewalls, VPNs Vulnerable to OpenSSL Bug
    [Link: https://www.bleepingcomputer.com/news/security/palo-alto-networks-firewalls-vpns-vulnerable-to-openssl-bug/]

13. Millions of Lenovo Laptops Contain Firmware-Level Vulnerabilities
    [Link: https://www.darkreading.com/threat-intelligence/millions-of-lenovo-laptops-contain-firmware-level-vulnerabilities]