ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 3/22 (March)

OVERVIEW

1. Over the past month, even as cyber attacks against Ukraine continued to proliferate, ransomware operators have persisted in their global targeting campaigns against CIIs. In cyber defence developments, Google observed that vendors were fixing zero-day vulnerabilities faster than before.

Recent APT Activities

2. Globally, APTs continued to conduct cyber espionage against a range of victims, update their toolsets to avoid detection, as well as conduct disruptive cyber attacks against their traditional adversaries. As part of the ongoing Russia-Ukraine conflict, APT Gamaredon reportedly conducted spear-phishing campaigns to harvest credentials. Separately, APT Charming Kitten was reported to be deploying a new backdoor called PowerLess in its cyber campaigns, whilst APT TunnelVision continued to exploit the Log4j vulnerability to infect unpatched VMware users with ransomware in disruptive attacks.

Cybersecurity Trends

3. Cyber Attacks targeting Ukraine. Multiple Ukrainian financial, government and defence entities had recently fell victim to waves of Distributed-Denial-of-Service (DDoS) attacks, webpage defacements, data leaks, and destructive wiper malware attacks.

   a. DDoS Attacks. Reportedly conducted between 15 to 18 Feb and on 23 Feb, the DDoS attacks rendered the websites of several Ukrainian government and financial institutions inaccessible. Victims included the websites for the defence and foreign affairs ministries, as well as Ukraine's two national banks, PrivatBank and Oschadbank. Many other Ukrainian entities apparently took their websites offline to avoid becoming victims of DDoS attacks.

b. Webpage Defacements and Data Leaks. Launched against multiple Ukrainian government and media entities, some of the defaced websites had their data leaked, purportedly by the "Free Civilian" and "Cyber Partisans" hacktivist groups.

c. Wiper Malware. A new destructive wiper malware called HermeticWiper was launched against Ukrainian banks and government contractors. Whilst similar to January's WhisperGate wiper malware that could wipe the Master Boot Records, HermeticWiper was purportedly more systematic and thorough in erasing data from victims' systems.

4. Ransomware. Ransomware operators continued to compromise critical information infrastructure (CII) in the oil, government, financial, food and agricultural sectors. Large companies continued to be targeted, possibly due to their ability to pay and fear of further losses when their business systems are down. Separately, affiliates of the defunct DarkSide Ransomware-as-a-Service (RaaS) have purportedly re-emerged as the Alphv/BlackCat RaaS.

a. European Port Oil Companies Breached. The IT systems of major port oil companies in Belgium (Sea-Invest) and Netherlands (Evos) were reportedly compromised by Alphv/BlackCat RaaS and Conti RaaS respectively, leading to significant service disruptions.

b. Compromise of US CIIs. US CISA released an advisory warning that the BlackByte RaaS had compromised multiple US-based businesses, including those in the government, financial and food and agricultural sectors.

c. Alphv/BlackCat RaaS Possibly Rebranded from DarkSide. In a continued trend of ransomware operators regrouping and rebranding to lay low and evade law enforcement scrutiny, Alpv/BlackCat RaaS was found to have links to the former DarkSide/BlackMatter RaaS. *[DarkSide was responsible for the 2021 breach of Colonial Pipeline, which massively disrupted the supply of oil in the US East Coast. Thrust into the spotlight, DarkSide faced significant pressure from international law enforcement, who seized their cryptocurrency wallet and offered financial rewards to capture its members. This pressure continued even after rebranding as BlackMatter, with law enforcement seizing its servers and forcing it to shut down again.]*

Global Developments

5. The Google Project Zero team recently published findings which showed that vendors had improved in reaction times to fix zero-day vulnerabilities. In 2021, vendors took an average of 52 days to fix zero-day vulnerabilities, as compared to an average of 80 days in 2018.

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. Russian Gamaredon APT Targeting Ukraine Since October
   [Link: https://securityaffairs.co/wordpress/127729/apt/actinium-gamaredon-ukraine.html?utm_source=rss&utm_medium=rss&utm_campaign=actinium-gamaredon-ukraine]

2. Cyberspies Linked to Memento Ransomware Use New PowerShell Malware
   [Link: https://www.bleepingcomputer.com/news/security/cyberspies-linked-to-memento-ransomware-use-new-powershell-malware]

3. VMware Horizon Servers Are Under Active Exploit by Iranian State Hackers
   [Link: https://arstechnica.com/information-technology/2022/02/iranian-state-hackers-are-using-log4shell-to-infect-unpatched-vmware-servers/]

4. Ukrainian military agencies, state-owned banks hit by DDoS attacks
   [Link: https://www.bleepingcomputer.com/news/security/ukrainian-military-agencies-state-owned-banks-hit-by-ddos-attacks/]

5. Ukraine Says It's Targeted by 'Massive Wave of Hybrid Warfare'
   [Link: https://www.bleepingcomputer.com/news/security/ukraine-says-it-s-targeted-by-massive-wave-of-hybrid-warfare-/]

6. European Oil Port Terminals Hit by Cyberattack
   [Link: https://www.securityweek.com/european-oil-port-terminals-hit-cyberattack]

7. BlackByte Ransomware Attacks Target U.S. Critical Infrastructure, FBI Warns
   [Link: https://cyware.com/news/blackbyte-ransomware-attacks-target-us-critical-infrastructure-fbi-warns-c639cd32/?web_view=true]

8. BlackCat (ALPHV) Ransomware Linked to BlackMatter, DarkSide Gangs
   [Link: https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-linked-to-blackmatter-darkside-gangs/]

9. FBI Shares Lockbit Ransomware Technical Details, Defense Tips
   [Link: https://www.bleepingcomputer.com/news/security/fbi-shares-lockbit-ransomware-technical-details-defense-tips/]

10. Google Project Zero: Vendors Are Now Quicker at Fixing Zero-Days
    [Link: https://www.bleepingcomputer.com/news/security/google-project-zero-vendors- are-now-quicker-at-fixing-zero-days/]