ACICE
ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 6/22 (June)

OVERVIEW

1. In May, we observed significant levels of cyber activities from a myriad of actors. Cyber attacks continued to be conducted as part of the Russo-Ukraine conflict, whilst cyber criminals persisted in their financially-motivated campaigns. Vulnerabilities in major technological brands such as Intel and Windows also surfaced during the month.

APT Activities

2. Various reports noted the conduct of cyber attacks by APT groups. First, it was reported that the Moshen Dragon APT had been targeting telecommunication service providers in Central Asia using stolen credentials to facilitate lateral movement, before exfiltrating data from infected machines. Second, the Winnti group reportedly stole intellectual property assets such as patents, copyrights, trademarks, and other corporate data since 2019, targeting technology and manufacturing firms in East Asia, Western Europe and North America. Third, the Oilrig APT reportedly targeted Jordanian entities in the chemical, energy, financial, governmental and telecommunications industries using the Saitama backdoor. Fourth, an unknown APT targeted Russian government agencies using phishing emails with attachments that downloaded fake Windows updates to install remote access malware. Fifth, the Space Pirates APT had reportedly been targeting enterprises in the Russian aerospace industry.

Cybersecurity Trends

3. Russia-Ukraine Conflict Developments. Cyber attacks continued to be reported during the ongoing Russia-Ukraine conflict, with the majority perpetrated by hacktivists. These hacktivists persisted in their campaign of disrupting Russian institutions and webpages. Hacktivists also conducted distributed denial-of-service (DDoS) attacks against multiple Russian and Belarusian government, military and news organisation websites; and perpetrated DDoS attacks against a Russian web portal that controlled Russia’s distribution of alcoholic beverages. Separately, the Ukrainian CERT reported a string of phishing attacks against its state institutions, using the GammaLoad.PS1_v2 malware.

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

a. Conti. The Conti ransomware group breached and crippled computer networks across 27 Costa Rican government agencies. In response, the US government offered a US$15 million bounty to capture Conti members. In response, the Conti group apparently shuttered its operations, then regrouped and rebranded.

b. BlackCat/Alphv. The BlackCat ransomware group breached the computer systems of Austrian state Carinthia, demanding a US$5 million ransom. Carinthia’s government website and email services are currently offline, affecting the issuance of new passports, and processing of COVID-19 tests.

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

a. Intel. Intel reported a memory bug impacting microprocessor firmware used in hundreds of its Optane SSD and Intel Optane Data Centre products, which could result in privilege escalation, denial of service, or information disclosure.

b. Windows 11. Multiple zero-day vulnerabilities were found and successfully exploited in Windows 11 products during the 2022 Pwn2Own hacking contest.

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. Hackers Stole Data Undetected From US, European Orgs Since 2019

   [Link: https://www.bleepingcomputer.com/news/security/hackers-stole-data-undetected-from-us-european-orgs-since-2019/]

2. Hackers Target Russian Govt With Fake Windows Updates Pushing RATs

   [Link: https://www.bleepingcomputer.com/news/security/hackers-target-russian-govt-with-fake-windows-updates-pushing-rats/]

3. Iranian Hackers Exposed in a Highly Targeted Espionage Campaign

   [Link: https://www.bleepingcomputer.com/news/security/iranian-hackers-exposed-in-a-highly-targeted-espionage-campaign/]

4. Pro-Ukraine Hackers Use Docker Images to DDoS Russian Sites

   [Link: https://www.bleepingcomputer.com/news/security/pro-ukraine-hackers-use-docker-images-to-ddos-russian-sites/]

5. Ukraine's IT Army Is Disrupting Russia's Alcohol Distribution

   [Link: https://www.bleepingcomputer.com/news/security/ukraine-s-it-army-is-disrupting-russias-alcohol-distribution/]

6. Ukraine CERT-UA Warns of New Attacks Launched by Russia-Linked Armageddon APT

   [Link: https://securityaffairs.co/wordpress/131296/breaking-news/cert-ua-warns-armageddon-apt.html]

7. Fake Windows 10 Updates Infect You With Magniber Ransomware

   [Link: https://www.bleepingcomputer.com/news/security/fake-windows-10-updates-infect-you-with-magniber-ransomware/]

8. Costa Rica Declares State of Emergency Over Ransomware Attack
   [Link:https://www.nbcnews.com/tech/tech-news/costa-rica-declares-state-emergency-ransomware-attack-rcna28415]

9. US DoS Offers a Reward of Up to $15M for Info on Conti Ransomware Gang
   [Link: https://securityaffairs.co/wordpress/131050/cyber-crime/us-dos-reward-15m-info-conti-ransomware.html]

10. Conti Ransomware Shuts Down Operation, Rebrands Into Smaller Units
    [Link: https://www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/]

11. Intel Memory Bug Poses Risk for Hundreds of Products
    [Link: https://threatpost.com/intel-memory-bug-poses-risk-for-hundreds-of-products/179595/]

12. Windows 11 Hacked Again at Pwn2Own, Telsa Model 3 Also Falls
    [Link: https://www.bleepingcomputer.com/news/security/windows-11-hacked-again-at-pwn2own-telsa-model-3-also-falls/]