ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 4/22 (Apr)

OVERVIEW

1. In March, we observed significant levels of cyber activities from a variety of actors. Cyber attacks continued to be conducted as part of the Russia-Ukraine conflict, ransomware operators persisted in their illicit lucrative campaigns, and supply chain risks remained an ongoing threat. Vulnerabilities in major technological brands such as Windows, Google, and Hewlett-Packard have also surfaced.

Cybersecurity Trends

2. Russia-Ukraine Conflict Developments. Cyber attacks continued to be reported during the ongoing Russia-Ukraine conflict. Cyber-related tactics and techniques were employed to disrupt essential services and spread psychological fear, impede troop progress and undermine populace morale. These included disruptive wiper malware attacks, webpage defacements, Distributed Denial of Service (DDoS) attacks, cyber attacks against satellite communication (SATCOM), and cyber-enabled information operations.

a. Wiper Malware Attacks. New destructive wiper malware such as IsaacWiper and CaddyWiper were deployed against Ukrainian government networks and other unnamed organisations. These targeted the victim systems' logical drives, wiped disk files and destroyed user data from attached drives.

b. Webpage Defacements. Russian government agency websites were reportedly defaced after the stats widget used to track visitor numbers was hacked. The affected websites were apparently restored within a day.

c. DDoS Attacks. Russian state-linked aerospace and defence conglomerate Rostec was reportedly targeted in DDoS attacks by the Ukrainian IT Army hacking group. The Russian government also shared a list of more than 17,000 IP addresses allegedly used in DDoS attacks against Russian networks.

d. SATCOM attacks. Global cybersecurity agencies have warned of possible threats to international SATCOM networks. This comes amid investigations into a major outage affecting US telecommunications company Viasat's internet service for broadband customers on the European KA-SAT satellite network. The outage first started in February, coinciding with the invasion of Ukraine. As of 29 Mar, according to Viasat, hacking attempts at disabling Viasat satellite modems have not ceased.

e. Cyber-enabled Information Operations. The Security Service of Ukraine revealed that unknown hackers had compromised local government websites to release fake news that Ukraine had surrendered and signed a peace treaty with Russia.

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

a. AvosLocker. The FBI reported that AvosLocker ransomware had been observed in ransomware campaigns against multiple US critical infrastructure sectors, including financial services, manufacturing companies and government facilities.

b. Lapsus$. Microsoft confirmed that they had been breached by the Lapsus$ group, with the threat actors accessing and stealing some of their source code.

c. LockBit. The LockBit gang revealed that they had successfully compromised major tyre manufacturer Bridgestone America. However, it is not known if there was any leak of information.

4. Notable Vulnerabilities. Major vulnerabilities continued to be discovered in software and equipment manufactured by major brands, such as Windows, Google, and Hewlett-Packard.

a. Windows. Researchers have highlighted a local privilege escalation zero-day vulnerability in Windows systems which researchers have failed to address for months. Exploitation of this vulnerability would enable users to gain administrative privileges in Windows 10, 11 and Windows Server.

b. Google. Google released Chrome updates for Windows, Mac, and Linux users to address a high-severity zero-day vulnerability exploited in the wild. The impact of this vulnerability is currently not known.

c. Hewlett-Packard. Hewlett-Packard published security advisories for critical-severity vulnerabilities affecting hundreds of its printer models. If not addressed, these could facilitate buffer overflows that could lead to remote code execution, as well as data leaks, remote code execution and denial of service.

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. Ukraine Says Local Govt Sites Hacked to Push Fake Capitulation News
   [Link: https://www.bleepingcomputer.com/news/security/ukraine-says-local-govt-sites-hacked-to-push-fake-capitulation-news/]

2. Ukrainian CERT Warns Citizens of Phishing Attacks Using Compromised Accounts
   [Link: https://thehackernews.com/2022/03/ukrainian-cert-warns-citizens-of.html]

3. Russian Defense Firm Rostec Shuts Down Website After DDoS Attack
   [Link: https://www.bleepingcomputer.com/news/security/russian-defense-firm-rostec-shuts-down-website-after-ddos-attack/]

4. CaddyWiper: Yet Another Data Wiping Malware Targeting Ukrainian Networks
   [Link: https://thehackernews.com/2022/03/caddywiper-yet-another-data-wiping.html]

5. FBI: Avoslocker Ransomware Targets US Critical Infrastructure
   [Link: https://www.bleepingcomputer.com/news/security/fbi-avoslocker-ransomware-targets-us-critical-infrastructure/]

6. Microsoft Confirms They Were Hacked by Lapsus$ Extortion Group
   [Link: https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/?&web_view=true]

7. Bridgestone Americas Confirms Ransomware Attack, LockBit Leaks Data
   [Link: https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware-attack-lockbit-leaks-data/]

8. EU & US Agencies Warn That Russia Could Attack Satellite communications
[Link: https://securityaffairs.co/wordpress/129243/cyber-warfare-2/russia-could-attack-satellite-communications.html?utm_source=rss&utm_medium=rss&utm_campaign=russia-could-attack-satellite-communications]

9. Windows Zero-Day Flaw Giving Admin Rights Gets Unofficial Patch, Again
[Link: https://www.bleepingcomputer.com/news/microsoft/windows-zero-day-flaw-giving-admin-rights-gets-unofficial-patch-again/]

10. Emergency Google Chrome Update Fixes Zero-Day Used in Attacks
[Link: https://www.bleepingcomputer.com/news/security/emergency-google-chrome-update-fixes-zero-day-used-in-attacks/]

11. Hundreds of HP Printer Models Vulnerable to Remote Code Execution
[Link: https://www.bleepingcomputer.com/news/security/hundreds-of-hp-printer-models-vulnerable-to-remote-code-execution/?&web_view=true]