ACICE
ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 10/22 (October)

OVERVIEW

1. In October, we observed that global cyber activities have increased, along with observed escalations in the Russia-Ukraine conflict. Cybercriminal groups continued to evolve attacks and were aggressively growing their extortion schemes. Major technology brands, WhatsApp and Microsoft, also reported new vulnerabilities.

APT ACTIVITIES

2. State-directed cyber-attacks were observed to have significantly affected some countries in this reporting window. Notable incidents include:

a. Albania. In September, the Albanian government severed diplomatic ties with the Islamic Republic of Iran, and issued an ultimatum for embassy staff to leave the country within 24 hours. This came after a series of cyber attacks from May to July targeting Albanian government sites. Microsoft assisted in the investigations and concluded with a high degree of certainty that various Iranian groups were involved. Tehran's hostility towards Tirana likely began when the Balkan State hosted members from the Iranian opposition, Mujahedeen-e-Khalq (MeK).[1] The cyber attacks were likely in response to the MEK hosting the "Free Iran World Summit" in Albania.

b. Montenegro. A coordinated cyberattack by the threat-actor named 'Cuba' affected more than 10 government institutions, crippling Montenegro's online government information platforms. Montenegrin essential infrastructure such as banking, water, and electric power systems, were also put at risk. The attacks were likely due to Montenegro's decision to sanction Russia. FBI investigators dispatched to the Balkan State to assist investigations had advised Montenegrin government officials to go offline for security reasons. The entire Montenegrin system functioned at a restrictive level for more than 20 days, before operations were restored to normalcy.

[1] MEK is a dissident group whose goal is to overthrow the government of the Islamic Republic of Iran.

CYBERSECURITY TRENDS

3. Russia-Ukraine Conflict. Reports of cyber attacks grew as hostilities increased after Ukrainian battlefield advances and Russia's partial mobilisation. However, researchers noted that Russian cyberattacks have thus far failed to shut down Ukrainian infrastructure or affect military preparations. This could be due to the Ukrainians holding backup data out-of-country. Separately, pro-Russia hacking group 'KillNet' widened their cyber-attacks to target Japan. 'KillNet' claimed that these attacks were in response to Japanese "militarism". Besides Japan's continued support for Ukraine, some analysts have noted that tensions between Russia and Japan also escalated following fresh disputes over the contested Kuril Islands. As the European Union continued sanctions against Russia, five European nations have called for a ban of Russian anti-virus software provider, Kaspersky. The countries contended that Russia had leveraged Kaspersky products for espionage. However, there was insufficient evidence to suggest that these products were being used for cyber-espionage.

4. Ransomware. The tactics and techniques used in ransomware extortions continued to evolve. In particular, ease of subscription to Ransomware-as-a-Service (RaaS) and increasing use of plug-and-play ransomware, has led to a doubling of variants observed. This model of operations is likely to continue as groups seek to expand their customer base and minimise costs. Additionally, cybercriminal groups were observed to be creating new malware, weaponising older variants, as well as retooling infrastructure to propagate different malware strains.

5. Notable Vulnerabilities. Major vulnerabilities had been reported for WhatsApp and Microsoft Teams.

a. WhatsApp. Two critical zero-day vulnerabilities (CVE-2022-36934 and CVE-2022-27492) were reported in September. CVE-2022-36934 affected WhatsApp for Android and iOS, which could result in remote code execution during a video call. Meanwhile, CVE-2022-27492 affected WhatsApp for Android, which could result in remote code execution if the targeted victim received a crafted video file. Both of these vulnerabilities were marked as "Critical", with CVE Scores of 9.8 and 7.8 respectively. The vulnerabilities were resolved from versions 2.22.16.12 onwards.

b. Microsoft Teams. A sever security vulnerability in the desktop app for Microsoft Teams allowed threat actors to access authentication tokens and accounts with multi-factor authentication turned on. This newly-discovered security issue impacted certain versions of Windows, Linux, and Mac. Till date, Microsoft had not released patches for this vulnerability.

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. Albania blames Iran for second cyberattack since July.
   [Link: https://edition.cnn.com/2022/09/10/politics/albania-cyberattack-iran/index.html]

2. Montenegro wrestles with massive cyberattack; Russia blamed.
   [Link: https://www.nbcnews.com/tech/security/montenegro-wrestles-massive-cyberattack-russia-blamed-rcna47277]

3. Ukraine is winning the Cyber War.
   [Link: https://cepa.org/article/ukraine-is-winning-the-cyber-war/]

4. Cyber Attacks Now State-Level Weapon, Disrupting Everyday Lives, with Ransomware the Number One Threat, says Check Point Software's. 2022 Cyber Attacks Trends: Mid-Year Report.
   [Link: https://pages.checkpoint.com/cyber-attack-2022-trends.html]

5. UK and allies expose Iranian state agency for exploiting cyber vulnerabilities for ransomware operations.
   [Link: https://www.channelfutures.com/from-the-industry/new-threat-spotlight-shows-ransomware-attacks-continue-to-grow]

6. Hackers attack government websites for two straight days.
   [Link: https://www.asahi.com/ajw/articles/14713185]

7. Russian War Report: Russia conducts partial mobilisation amid battlefield losses.
   [Link: https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-russia-conducts-partial-mobilization-amid-battlefield-losses/]

8. Emotet Botnet Started Distributing Quantum and BlackCat Ransomware. [Link: https://thehackernews.com/2022/09/emotet-botnet-started-distributing.html]

9. Ransomware attacks continue to become more sophisticated and aggressive: Vishak Raman, Fortinet.
[Link: https://www.dqindia.com/ransomware-attacks-continue-to-become-more-sophisticated-and-aggressive-vishak-raman-fortinet/]

10. New WhatsApp 0-Day Bug Let Hackers Execute a Code & Take Full App Control Remotely.
[Link: https://gbhackers.com/new-whatsapp-0-day-vulnerabilities/]

11. Microsoft Teams stores auth tokens as cleartext in Windows, Linux, Macs. [Link: https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/]

12. New Threat Spotlight Shows Ransomware Attacks Continue to Grow. [Link: https://www.channelfutures.com/from-the-industry/new-threat-spotlight-shows-ransomware-attacks-continue-to-grow]