ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 04/23 (April)

OVERVIEW

1. In March 2023, state-linked actors and cybercriminals persisted in their targeting of academia, government and commercial entities. Government agencies also rolled out new initiatives to strengthen cybersecurity awareness and resilience of organisations and public systems. Separately, zero-day vulnerabilities previously discovered in widely-used products from Microsoft and Fortinet were addressed.

TARGETED INTRUSIONS

2. In the reporting period of March 2023, state-linked threat actors targeted researchers and geopolitical experts focusing on Iran and Korean Peninsula issues. Notable incidents included:

a. Iran-linked Hackers Target Human Rights Researchers. On 9 March, cybersecurity firm Secureworks® reported that Iran-linked hackers, APT42 (also known as 'Charming Kitten'), had manufactured a fake Atlantic Council-affiliated persona to reach out to legitimate researchers asking if they were interested in contributing to an upcoming Atlantic Council report. APT42 is known to have targeted individuals, academics, journalists, activists, military and government sectors from the US, European and Middle Eastern countries since 2014. The group has also exhibited a pattern of using fake personas to establish contact with individuals who are of strategic interest to the Iranian government. Apart from identifying individuals sympathetic to the anti-government movement in Iran, APT42 also undertakes intelligence gathering, often human focused intelligence like extracting the contents of mailboxes, contact lists, travel plans, relationships, physical locations, and integrates with other sources to be used to inform military and security operations conducted within and outside of Iran. The Computer Emergency Response Team in Farsi – a group of researchers focused on cybersecurity threats related to Iran – has also reported the discovery of an assortment of fake social media accounts manufactured by APT42 actors for cyber espionage.

b. North Korea APT Targets Geopolitical Experts on Korean Peninsula Issues. On 23 March, German and South Korean government agencies reported a fresh spearphishing

campaign by North Korea APT 'Kimsuky' (also known as TA406) that targeted experts on Korean Peninsula issues. Operational since 2012, 'Kimsuky' had previously mounted similar campaigns largely targeting diplomats, non-governmental organisations, think tanks and is known to collect strategic intelligence on geopolitical events and negotiations affecting DPRK's interests. In the latest campaign, the group had sought to gain access to victims' Google accounts through the malicious use of an Android application and a Chromium web browser extension. As the technology exploited by 'Kimsuky' is used universally, the attack methods could be replicated and used to target other foreign affairs and security think tanks around the world.

3. Russia-Ukraine Conflict. Microsoft revealed that Russia-linked threat actors targeted at least 17 European nations between January and mid-February 2023. Microsoft reported that while the threat actors mostly intended to boost intelligence collection against organisations providing political and material support to Ukraine, they could also, if directed, inform destructive operations. Microsoft also stated that the Russia-linked APT group IRIDIUM appeared to be preparing for a renewed destructive campaign that could target Ukraine and organisations outside the country that serve key functions in Ukraine's supply lines. Microsoft has assessed that Russian actors might seek to disrupt military and humanitarian supply chains beyond Ukraine and Poland by incorporating newer destructive malware variants should Russia suffer more setbacks on the battlefield.

CYBERCRIMES

4. Cybercriminals continued to evolve and refine their tactics in this reporting period. Notable developments included:

a. GoAnywhere Zero-Day Attacks Hit Major Organisations. A Russian-speaking ransomware group named 'Silence' was linked to the zero-day exploits hitting Forta's GoAnywhere Managed File Transfer (MTF) application. Since March, 'Silence' has also been posting the names of organisations allegedly impacted by the attacks, notably the luxury brand retailer Sak's Fifth Avenue, consumer goods giant Proctor and Gamble, and United Kingdom's Pension Protection Fund on its Tor-based leak site. These organisations had also acknowledged the attacks on the MTF application in their systems. Thus far, no ransom was reported to have been made to the threat actor.

b. Potential Criminal Abuse of ChatGPT. Europe's policing agency Europol warned that cybercriminals could take advantage of artificial intelligence such as ChatGPT to commit fraud and other cybercrimes. For instance, cybercriminals could leverage ChatGPT to research and learn about areas they are not proficient in, automate malware code generation, or produce authentic sounding text for propaganda and disinformation purposes. Europol stressed the importance of raising awareness to such scenarios, and emphasised that any potential content moderation loopholes discovered should be closed as quickly as possible.

CYBERCRIMES

5. CISA's New Initiative on Pre-Ransomware Alerts. In March 2023, the US Cybersecurity and Infrastructure Security Agency (CISA) announced a new initiative to alert more than 60 organisations in the energy, education, healthcare, water/wastewater of early-stage ransomware attacks. As a proactive cyber defence capability, these pre-ransomware notifications would warn organisations that they had been breached, so that they could evict threat actors from their networks before any file-encrypting ransomware was deployed. By taking immediate action in receipt of such early warning, organisations could reduce potential data loss, minimise impact on operations, and mitigate financial impact.

6. EPA Takes Action to Improve Cybersecurity Resilience for Public Water Systems. In March 2023, the US Environmental Protective Agency (EPA) released a memorandum stressing the need for the federal states to assess cybersecurity risks and audit practices at public water systems (PWSs). Currently, many PWSs do not implement cybersecurity practices. Given the relative ease of access to critical water treatment systems from the internet, there have been incidents of malicious cyber activity against PWSs. For example, critical treatment processes are shutdown or suspended; control system networks are held for ransom and communications used to monitor and control distribution system infrastructure like pumping stations are being disabled. The inclusion of cybersecurity in PWS sanitary surveys or equivalent alternate programs, is an essential tool to address vulnerabilities and mitigate consequences of attacks on critical infrastructure, which could reduce the risk of a successful cyberattack and improve recovery in the case of a cyber-incident.

REPORTED VULNERABILITIES

7. Major vulnerabilities were reported for Microsoft and Fortinet:

a. Microsoft. Microsoft's March 2023 patch fixed two actively exploited zero-day vulnerabilities. One of the vulnerabilities fixed (CVE-2023-23397) was a Microsoft Outlook privilege elevation bug that could allow threat actors to breach victims' network and steal emails from specific accounts. The other vulnerability fixed (CVE-2023-24880) was a Window SmartScreen Security Feature Bypass vulnerability that would allow threat actors to bypass the Windows Mark of the web defences, resulting in a limited loss of integrity and availability of security features.

b. Fortinet. In March 2023, Fortinet released security updates to address a high-severity vulnerability (CVE-2022-41328) that had allowed threat actors to execute unauthorised code or commands. Fortinet concluded from past incidences that the unidentified threat actors had demonstrated advanced capabilities in their attacks, with evidence showing that government networks were among those targeted. Fortinet customers were advised to upgrade to a patched version of FortiOS immediately, to block potential attack attempts.

.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

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. Iran-linked hackers used fake Atlantic Council-affiliated persona to target human rights researchers.
   [Link: https://cyberscoop.com/iran-linked-hackers-used-fake-atlantic-council-persona-to-target-human-rights-researchers/]

2. Iranian Hackers Target Women Involved in Human Rights and Middle East Politics.
   [Link: https://thehackernews.com/2023/03/iranian-hackers-target-women-involved.html

3. DPRK-linked 'Kimsuky' Targeting Korean Experts With New Spearphishing Campaign
   [Link: https://therecord.media/north-korea-apt-kimsuky-attacks]

4. German and South Korean Agencies Warn of Kimsuky's Expanding Cyber Attack Tactics
   [Link: https://thehackernews.com/2023/03/german-and-south-korean-agencies-warn.html]

5. Microsoft Sheds Light on a Year of Russian Hybrid Warfare in Ukraine
   [Link: https://securityaffairs.com/143570/cyber-warfare-2/russian-hybrid-warfare-ukraine.html]

6. CISA Gets Proactive With New Pre-Ransomware Alerts
   [Link: https://www.securityweek.com/cisa-gets-proactive-with-new-pre-ransomware-alerts/]

7. EPA Takes Action to Improve Cybersecurity Resilience for Public Water Systems
   [Link: https://www.epa.gov/newsreleases/epa-takes-action-improve-cybersecurity-resilience-public-water-systems]

8. GoAnywhere Zero-Day Attack Hits Major Orgs
   [Link: https://www.securityweek.com/goanywhere-zero-day-attack-hits-major-orgs/]

9. 'Grim' Criminal Abuse of ChatGPT is Coming, Europol Warns
   [Link: https://www.securityweek.com/grim-criminal-abuse-of-chatgpt-is-coming-europol-warns/]

10. Microsoft March 2023 Patch Tuesday fixes 2 zero-days, 83 flaws
    [Link: https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2023-patch-tuesday-fixes-2-zero-days-83-flaws/]

11. Fortinet: New FortiOS bug used as zero-day to attack govt networks
    [Link: https://www.bleepingcomputer.com/news/security/fortinet-new-fortios-bug-used-as-zero-day-to-attack-govt-networks/]