ADMM Cybersecurity and Information Centre of Excellence

# UPDATE ON THE CYBER DOMAIN

## Issue 03/23 (March)

## OVERVIEW

1. In February 2023, state-linked actors and cybercriminals persisted in their targeting of government and commercial entities as well as the public. February also marked the anniversary of the Russia-Ukraine conflict, where the escalation of cyberattacks from the Russian front further increased tensions in the digital battlespace. Separately, new zero-day vulnerabilities were discovered and addressed in widely-used products from Microsoft and Apple.

## TARGETED INTRUSIONS

2. In this reporting period, state-linked threat actors continued to target government services and commercial entities. Notable incidents included:

a. Hacking of Azerbaijan State Websites. On 23 Feb 2023, the communications ministry of Azerbaijan stated that the websites of Azerbaijan's national airline AZAL and television station AzTV were attacked by hackers assessed to be linked to Iran. Both AZAL's and AzTV's websites were operating normally later during the day. The hacking incidents followed mounting tensions between the two neighbouring countries that arose over Iran's treatment of its large ethnic Azeri minority and over Azerbaijan's decision to appoint its first ever ambassador to Israel. This is not the first time Azerbaijan's websites have been hacked by actors originating from Iran. Cyber-attacks started as early as 2012, ostensibly due to Azerbaijan's friendly relations with Israel.

b. Cyberespionage against Middle Eastern Organisations. Iranian-linked threat actor Oilrig aka 'APT34' reportedly added a new backdoor to its range of tools. Since 2014, Oilrig has been known to conduct cyberespionage campaigns against countries in the Middle East, including Bahrain, Egypt Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, and United Arab Emirates. This backdoor allowed attackers to manipulate legitimate but compromised email accounts to harvest and send stolen data to external email accounts controlled by the attackers.

c. Ransomware Attacks on Healthcare and Critical Infrastructure Facilities. According to a joint advisory by the United States (US) and South Korea cybersecurity and intelligence agencies, State-backed North Korean hackers conducted ransomware attacks against healthcare and critical infrastructure facilities to fund illicit activities in support of North Korea's national level priorities and objectives. The attacks demanded a cryptocurrency ransom in exchange for recovering access to encrypted files. The attacks targeted the US and South Korea governments, including the US' Department of Defense Information Networks and Defence Industrial Base member networks. This advisory follows a new United Nations report that North Korean hackers had stolen virtual assets with an estimated worth between US$630 million and US$1 billion in 2022. The advisory comes as a new report from the United Nations found that North Korean hackers stole record-breaking virtual assets estimated to be worth between $630 million and more than $1 billion in 2022.

3. Russia-Ukraine Conflict. A year has passed since the conflict started. In view of that, various cybersecurity agencies such as the US Cybersecurity and Infrastructure Security Agency (CISA) have warned the allies of US and Ukraine to "increase their cyber vigilance" as they may experience disruptive and defacement attacks against websites to sow chaos and societal discord on 24 Feb 2023, the anniversary of Russia's 2022 invasion of Ukraine. However, there were no notable Russian attributed cyberattacks that occurred in February. Ukraine has withstood the deluge of Russian cyberattacks for the past year as it had significantly boosted its security monitoring. Technical assistance from Western allies also helped Ukraine to quickly detect and respond to the attacks before they could have a major impact. However, analysts have warned that Russia will "increase disruptive and destructive attacks" in 2023 if it perceives that the war shifts "fundamentally" in Ukraine's favour.

## CYBERCRIMES

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

a. New Ransomware Campaign Targeting Windows and VMware ESXi Systems. Cybercriminals were reported to be actively exploiting a two-year old VMware vulnerability as part of a ransomware campaign targeting thousands of organisations globally. More than 3, 200 VMware servers worldwide have been compromised thus far. France is currently the most affected country, followed by the US, Germany, Canada and the UK.

b. Fake ChatGPT Applications. Threat actors were reported to have leveraged the popularity of OpenAI's chatbot to distribute malware and lead unsuspecting users to phishing pages. For example, a fake website offered the ChatGPT windows desktop client but visitors that accessed this page were infected with the Redline info-stealing malware. In addition, there were at least 50 fake ChatGPT applications on third-party Android appstores that attempted to carry out harmful activities on user devices.

## REPORTED VULNERABILITIES

5. Major vulnerabilities were reported for Microsoft and Apple:

a. Microsoft. Microsoft's February 2023 patch fixed three actively exploited zero-day vulnerabilities. Two of those fixes involved the elevation of privilege weaknesses (CVE-2023-23376 and CVE-2023-21823) in the Windows Common Log File System Driver affecting Microsoft Window 10 and 11 systems and in the Microsoft Windows Graphic component affecting OneNote respectively. The third fix (CVE-2023-21715) addressed the security feature bypass vulnerability in Microsoft Office.

b. Apple. Apple released an emergency security update to address a new zero-day vulnerability used in attacks to hack iPhones, iPads, and Macs. The zero-day vulnerability (CVE-2023-23529) could be exploited to trigger operating system crashes and gain code execution on compromised devices. Apple has advised users to update their operating system or Safari browsers to version 16.3.1 to fix the bug.

# 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. Azerbaijan Websites Attacked by Iranian hacker
   [Link: https://www.hackread.com/azerbaijan-websites-attacked-by-iranian-hacker/]

2. Azerbaijan strongly protests Iran after fatal embassy shooting
   [Link: https://www.reuters.com/world/asia-pacific/guard-killed-shooting-azerbaijans-embassy-iran-2023-01-27/]

3. New Apt34 backdoor malware infection campaign targets Middle Eastern organizations for cyberespionage
   [Link: https://industrialcyber.co/ransomware/new-apt34-backdoor-malware-infection-campaign-targets-middle-eastern-organizations-for-cybersespionage]

4. North Korea Hackers Targeting Healthcare with Ransomware to Fund its Operations.
   [Link: https://www.thehackernews.com/2023/02/north-korean-hackers-targeting.html%3famp=1]

5. A Year of Conflict: Cybersecurity Industry Assesses Impact of Russia-Ukraine War
   [Link: https://www.securitweek.com/one-year-of-russias-ukraine-war-cybersecurity-industry-sums-up-impact/]

6. Ukraine gears for new phase of cyber war with Russia.
   [Link: https://www.politico.com/amp/news/2023/02/24/ukraine-russian-cyberattacks-00084429/]

7. Nevada Ransomware Group targets 5000 victims in US and Europe
   [Link: https://techcrunch.com/2023/02/06/hackers-vmware-esxi-ransomware/amp/]

8. Hackers Use Fake ChatGPT Applications to Push Windows, Android Malware
   [Link: https://www.bleepingcomputer.com/news/security/hackers-use-fake-chatgpt-apps-to-push-windows-android-malware/]

9. Microsoft Patch Tuesday, February 2023 Edition
   [Link: https://krebsonsecurity.com/2023/02/microsoft-patch-tuesday-february-2023-edition/]

10. Apple Fixes New WebKit Zero-day Used to Hack iPhones And Macs
    [Link: https://www.bleepingcomputer.com/news/security/apple-fixes-new-webkit-zero-day-exploited-to-hack-iphones-macs/#google_vignettee]