ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 01/23 (January)

OVERVIEW

1. Cyber-criminal activity was the highest on record in December for the whole year. Major vulnerabilities were also reported for tele-working products and services. Additionally, this ACICE update will highlight the notable cyber trends and observations in 2022.

TARGETED INTRUSIONS

2. In 2022, the Russia-Ukraine conflict dominated headlines, with Russian-linked threat actors demonstrating a variety of destructive cyber-attacks against Ukraine. Ukrainian-linked activity was correspondingly elevated, as the country fended off and countered with their own cyber-actions. Other top-active actors included those from North Korea and Iran, undertaking campaigns in support of their political objectives. Key observations are as follows:

a. Russia-Ukraine Conflict. Upon the invasion, wiper-malware and distributed denial of service attacks were launched against Ukraine to disable infrastructure and degrade public services. An "IT Army of Ukraine" was quickly mobilised and retaliated against Russian activities. Ten months later, the online contestations persist in both intensity and frequency. Ukrainian sources claimed that more than 4,500 cyber-attacks have been thwarted thus far. Russia also continued to generate an average of 10 cyber-attacks a day. Their tactics have remained largely unchanged, with government databases and information resources being the preferred targets.

b. North Korea. Phishing was the tactic favoured by North Korean threat actors, with the focus largely on the South Korean government and media sector. State-backed criminal activities were also undertaken by North Korean groups. In particular, the Lazarus Group [1] was focused against the cryptocurrency sector. In 2022 alone, about US$626 million were stolen through ransomware and other attacks.

c. Iran. Iranian groups conducted multiple cyber operations targeting Israel, the United States, and Europe. The Balkan states were also targeted in 2022, likely in connection to Iranian dissident activities in those countries. In particular, Albania was hit by a cyber-attack, leading to widespread denial of services to websites, lasting a few days.

[1] Lazarus Group is state-sponsored and engages in cyber-crime as a means to gain funds for the North Korean regime.

CYBERCRIMES

3. In 2022, it was estimated that more than 50,000 global websites were hacked daily, and the annual cost of cybercrime have risen to approximately US$6 trillion. The top targeted industries were finance and insurance, manufacturing, and business services. Governments have also not been spared. In April, about 27 government agencies in Costa Rica were hit by ransomware, forcing officials to declare a national emergency. In August, ransomware also crippled National Health Services (NHS) in the UK. Key IT systems were shut down, leading to disruptions to medical appointments and emergency prescriptions. NHS reverted to pen-and-paper processes to ensure continuity in operations.

4. The crime wave persisted in December 2022. Cyber-criminal activity was the highest recorded thus far, having grown 9% year-on-year. Governments continued to be victims of ransomware, with the latest being the island-nation of Vanuatu. Disruptions on Vanuatu were especially prolonged, lasting almost a month. Also, World Cup-themed attacks persisted even after the conclusion of FIFA World Cup Qatar 2022. Attacks on tournament organisers persisted, and numerous fraudulent stores and apps could still be found online in December, seeking to scam unsuspecting victims.

REPORTED VULNERABILITIES

5. Notable Vulnerabilities. Major vulnerabilities were reported to have affected SharePoint, Microsoft Outlook and Google Android system.

a. SharePoint Server. Two critical vulnerabilities (CVE-2022-44690; CVE-2022-44693) were found to have affected SharePoint Server. Using a network-based attack, an authenticated attacker with ‘Manage List’ permissions could execute code remotely on vulnerable servers. Post-exploitation, attackers could acquire permissions to create-and-delete, add-or-remove columns, and add-or-remove public views. Fixes were released on 13 Dec 2022.

b. Microsoft Outlook (for Mac). CVE-2022-044713, a Microsoft Outlook for Mac spoofing vulnerability, allowed attackers to masquerade as trusted users. Attackers could then issue signed email messages that would appear legitimate. This vulnerability was resolved in upgrade 16.68.0.

c. Google Android. CVE-2022-20411 was found to have affected devices installed with Google Android System versions 10 to 13. This vulnerability allowed an attacker to perform remote code execution over Bluetooth, with no additional privileges needed. This vulnerability has since been resolved in a Google security patch.

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. Microsoft Digital Defense Report 2022 [Link: https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/]

2. 2022 Cyber Review: The Year the Ukraine War Shocked the World [Link: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2022-cyber-review-the-year-the-ukraine-war-shocked-the-world#:~:text=Yahoo%3A%20Cybersecurity%20Insurance%20Global%20Market,(CAGR)%20of%2020.7%20percent]

3. 160 Cybersecurity Statistics 2023- The Ultimate List of Stats and Trends [Link: https://www.getastra.com/blog/security-audit/cyber-security-statistics/#:~:text=strategy%20against%20hackers.-,Top%20Cyber%20Security%20Statistics%202023%2D%20Key%20Findings,malware%20at%20any%20given%20time]

4. Microsoft: Nation-state Cyber Attacks Became Increasingly Destructive in 2022 [Link: https://www.computerweekly.com/news/252526922/Microsoft-Nation-state-cyber-attacks-became-increasingly-destructive-in-2022]

5. North Korea has Hacked $1.2 billion in Crypto and Other Assets for its Economy [Link: https://www.npr.org/2022/12/22/1144996480/crypto-hacking-north-korea-billion#:~:text=SEOUL%2C%20South%20Korea%20%E2%80%94%20North%20Korean,Korea's%20spy%20agency%20said%20Thursday.]

6. Albania Blames Iran for Cyberattacks [Link: https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285]

7. NHS Ransomware Attack: what Happened and How Bad Is It? [Link: https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it]

8. How to Deal with Cyberattacks This Holiday Season.
[Link: https://www.tripwire.com/state-of-security/how-deal-cyberattacks-holiday-season]

9. The Pacific Island Nation of Vanuatu has been Knocked Offline for More Than a Month
[Link: https://www.npr.org/2022/12/06/1140752192/the-pacific-island-nation-of-vanuatu-has-been-knocked-offline-for-more-than-a-mo]

10. Cyber Threats to the FIFA World Cup Qatar 2022.
[Link: https://www.digitalshadows.com/blog-and-research/cyber-threats-to-the-fifa-world-cup-qatar-2022/]

11. Qatar World Cup Employees Targeted by Phishing Cyberattacks.
[Link: https://techmonitor.ai/technology/cybersecurity/qatar-world-cup-cyberattacks-phishing]

12. Microsoft Outlook for Mac Spoofing Vulnerability.
[Link: https://github.com/advisories/GHSA-gr7j-pg85-jvg3]

13. CVE-2022-44713: Microsoft Outlook for Mac Spoofing Vulnerability [Office for Mac]
[Link: https://www.rapid7.com/db/vulnerabilities/office-for-mac-cve-2022-44713/]

14. CVE-2022-44713: Microsoft Outlook for Mac Spoofing Vulnerability [Office for Mac]
[Link: https://www.rapid7.com/db/vulnerabilities/office-for-mac-cve-2022-44713/]