ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 11/22 (November)

OVERVIEW

1. In October, cyberattacks continued to be observed in the Russia-Ukraine Conflict. Global economic uncertainties have spurred growth in cybercrime. Vulnerabilities were also reported in widely used products such as Microsoft Exchange and WordPress.

TARGETED INTRUSIONS

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

a. Iran. The state broadcaster of Iran appeared to have been hacked during live broadcast. The news segment was interrupted for a few seconds, and defaced by an image of a mask, followed by a depiction of Supreme Leader Ali Khamenei aflame, with a target on his head. This hack followed weeks of mass protests in Iran, which were triggered by the death of 22-year-old, Mahsa Amini. She had died under suspicious circumstances while in police custody, after being arrested for allegedly wearing her hijab improperly.

b. North Korea. North Korea threat actors reportedly "weaponised" a range of open source software and targeted personnel in numerous media, defence and aerospace, and IT organisations. Affected personnel and organisations in this campaign spanned across different countries. It was reported that threat actors had posed as job recruiters on LinkedIn. Under the guise of job-offers, individuals were instructed to download or install seemingly common applications. These applications contained malicious payloads, which subsequently infected the individuals' IT work environment. The high rates of success observed in this campaign was likely due to the attackers' effective social engineering. The use of seemingly innocuous applications to hide malicious payloads was also a contributing factor in lowering the defences of their victims.

c. Russia-Ukraine Conflict. Pro-Russia hacktivist groups appeared to have intensified their levels of distributed denial of service (DDoS) attacks in October. Notable incidents included attacks by 'KillNet' and 'Anonymous Russia' against the websites of at least 12 US State Governments and 48 airports. Separately, KillNet claimed responsibility for an attack on the Polish stock exchange website on 24 Oct. On the other hand, several Russian-based actors were also observed to have targeted Kremlin-linked entities in Russia. These attacks were likely in protest for what the actors viewed as an "unnecessary war" in Ukraine.

CYBERCRIMES

3. The global economic uncertainty continued to spur growth in cybercrime. Notable incidents over this reporting period included:

a. Typo-Squatting. A new typo-squatting [1] campaign was discovered, with over 200 domains created to impersonate 27 well-known brands from areas like mobile applications and services, software, cryptocurrency, and stock trading. Visitors would mistakenly visit these fake sites, which would then download malware and key stealers onto the victims' systems.

b. Ransomware. 'LockBit' ransomware syndicate overtook 'Conti' group as the most prolific extortion gang during this period. The growth of 'LockBit' was partly due to its successful transition into ransomware-as-a-service (RaaS), as well as a global crackdown on 'Conti'. This crackdown also resulted in the proliferation of smaller ransomware groups, such as 'Black Basta' and 'Hive Leaks', which gained market share at the expense of 'Conti'.

c. Online Scams. Cyber-criminal activity is expected to peak as the year-end festive period approaches. Online shopping, especially over Black Friday, Cyber Monday, Christmas, and Boxing Day sales, is likely to be exploited by cyber-criminals using various phishing scams.

REPORTED VULNERABILITIES

4. Notable Vulnerabilities. Major vulnerabilities were reported in the software by major brands like Microsoft and WordPress.

a. Microsoft Exchange. Two new zero-day vulnerabilities (CVE-2022-41040 and CVE-2022-41082) allowed hackers to remotely access internal services in Microsoft Exchange servers. Fixes for these vulnerabilities have yet to be released. Microsoft recommended for customers to disable remote PowerShell access for non-admin users.

b. WordPress. Two high-severity vulnerabilities (CVE-2022-3394 and CVE-2022-3395) affecting All Export Pro WordPress plugin versions prior to 1.7.9 were reported. CVE-2022-3394 could allow any logged-in user privileges to execute arbitrary code on the site, while CVE-2022-3395 could allow users previously given permissions to conduct SQL injection.

[1] A method of tricking people into mistakenly visiting a fake website by registering a domain name similar to that used by genuine brands.

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. Iran State TV Hacked With Image of Supreme Leader in Crosshairs. [Link: https://cyware.com/news/iran-state-tv-channel-hacked-to-show-supreme-leader-in-crosshairs-18d972da]

2. North Korean Hackers Weaponising Open-Source Software in Latest Cyber Attacks.
   [Link: https://thehackernews.com/2022/09/north-korean-hackers-weaponizing-open.html]

3. South Korea's KakaoTalk Outage Shows Need for Regulation Amid 'Entanglement' of Public, Private Sectors. [Link: https://www.scmp.com/week-asia/politics/article/3196255/south-koreas-kakaotalk-outage-shows-need-regulation-amid]

4. Ransomware Tracker: the latest figures [October 2022]. [Link: https://therecord.media/ransomware-tracker-the-latest-figures/]

5. Russian Hackers Take Aim at Kremlin Targets. [Link: https://www.oodaloop.com/briefs/2022/10/04/russian-hackers-take-aim-at-kremlin-targets/]

6. We breached Russian Satellite Network, say pro-Ukraine Partisans. [Link: https://cybernews.com/cyber-war/we-breached-russian-satellite-network-say-pro-ukraine-partisans/]

7. Several state websites disrupted by Killnet DDoS attacks. [Link: https://www.scmagazine.com/brief/malware/several-state-websites-disrupted-by-killnet-ddos-attacks]

8. Typosquat campaign mimics 27 brands to push Windows, Android malware.
[Link: https://www.malwarebytes.com/blog/threat-intelligence/large-typosquatting-campaign-delivers-tech-support-scams]

9. Ransomware In Q3 2022.
[Link: https://www.digitalshadows.com/blog-and-research/ransomware-in-q3-2022/]

10. LockBit 3.0 Ransomware Unlocked.
[Link: https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html]

11. Leaked LockBit 3.0 builder used by 'Bl00dy' ransomware gang in attacks.
[Link: https://www.bleepingcomputer.com/news/security/leaked-lockbit-30-builder-used-by-bl00dy-ransomware-gang-in-attacks/]

12. Microsoft Exchange servers hacked to deploy LockBit ransomware
[Link: https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-lockbit-ransomware/]

13. CVE-2022-3394 Detail
[Link: https://nvd.nist.gov/vuln/detail/CVE-2022-3394]