ACICE
ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 12/22 (December)

OVERVIEW

1. In November, cyber criminals took advantage of global economic uncertainties, the year-end holiday season, and 2022 World Cup, to perpetuate various crimes online. Vulnerabilities were also reported in widely used products such as Microsoft's Azure Cloud Computing Service and OpenSSL.

TARGETED INTRUSIONS

2. In this reporting period, state-linked threat actors were observed to have targeted government services, websites, and networks. Notable incidents included:

a. Nemesis Kitten. An Iranian-linked APT used unpatched Log4Shell vulnerabilities to compromise an unnamed U.S federal network and installed crypto-currency-mining software. Deploying crypto-mining software onto government networks is not common, since such operations work better against targets with a lot of computing power. It was also possible that 'Nemesis Kitten' was trying to obfuscate other activities or mislead the incident response team.

b. Lazarus. A North Korean-linked APT used a modified variant of the DTrack backdoor against various commercial targets in Europe and Latin America. This campaign was likely intended for financial gain. A unique feature of this modified DTrack backdoor was that it was masked with filenames commonly associated with legitimate executables.

3. Russia-Ukraine Conflict. Russia appeared to have evolved their cyberwarfare tactics and tempo to not only enable quicker intrusions, but also breach the same target multiple times to disrupt and collect information. Notable incidents included attacks by a Russian-linked APT, 'Sandworm', responsible for the Prestige ransomware attacks targeting transportation and logistics targets in Ukraine this year. Many victims were also targeted with 'HermeticWiper', prior to the Russian invasion. Additionally, the European Parliament website was hit with a DDoS attack by pro-Russian hacktivist group, 'KillNet', following a vote declaring Russia to be a state sponsor of terrorism.

CYBERCRIMES

4. The upcoming Christmas and Boxing Day sales would likely continue to be exploited by cyber criminals. Some notable threats and targeted events included:

a. Phishing. Researchers tracked an increase in phishing kits offered for sale in this reporting period. ‘Robin Banks’, a phishing-as-a-service (PhaaS) platform, was observed to have relocated their infrastructure to a hosting service based in Russia, after being blocked by Cloudflare. New functions were also added onto the new ‘Robin Banks’ PhaaS-platform. Notable ones included a cookie-stealer targeting specific enterprise environments and security measures like two-factor authentication to safeguard their customers’ privacy.

b. FIFA World Cup Qatar 2022. The World Cup was a favoured theme for cyber-criminal activity this month. It was reported that 174 malicious domains were found to have impersonated official webpages. At the same time, for every legitimate application developed by the organisers, there were dozens of fraudulent applications distributed via official app stores. Cyber-awareness and accessing trusted applications and websites, remains the best defence against such topical lures and scams by criminals.

REPORTED VULNERABILITIES

5. Notable Vulnerabilities. Major software vulnerabilities were reported by major brands like Microsoft and OpenSSL.

a. Microsoft’s Azure Cloud Computing Service. On 1 Nov 2022, a “highly important” vulnerability of unknown CVE number was discovered within Azure Cosmos DB. The vulnerability allowed an unauthenticated user to obtain access to the Cosmos DB notebooks and overwrite code. Cosmos DB Notebooks are used by developers and contain highly sensitive information, such as secrets and private keys. The critical issue has since been fixed and users now require an authorisation token for each notebook session.

b. OpenSSL. On 01 Nov 2022, OpenSSL released a security advisory addressing two “critical” vulnerabilities, CVE-2022-3602 and CVE-2022-3786. The vulnerabilities affected OpenSSL versions 3.0.0 through to 3.0.6. Both CVEs potentially allowed denial of service and remote code execution. Updating OpenSSL to version 3.0.7 would rectify these issues.

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's Nemesis Kitten Hacked U.S. Merit Systems Protection Board to Implant Crypto Miner. [Link: https://metacurity.substack.com/p/irans-nemesis-kitten-hacked-us-merit]

2. Lazarus APT uses DTrack backdoor in attacks against LATAM and European orgs. [Link: securityaffairs.co/wordpress/138622/apt/dtrack-backdoor-targets-europe-latin-america.html]

3. Iranian hackers breached the agency that hears federal worker grievance. [Link: https://www.washingtonpost.com/politics/2022/11/17/iranian-hackers-breached-agency-that-hears-federal-worker-grievances/]

4. Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless. [Link: https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/]

5. Robin Banks Phishing-As-a-Service Platform Continues to Evolve. [Link: securityaffairs.co/wordpress/138199/cyber-crime/robin-banks-phaas.html]

6. Check Point Research: 14th November– Threat Intelligence Report. [Link: https://research.checkpoint.com/2022/14th-november-threat-intelligence-report/]

7. Cyber criminals have World Cup Qatar 2022 in their sights. [Link: https://www.computerweekly.com/news/252527152/Cyber-criminals-have-World-Cup-Qatar-2022-in-their-sights]

8. Cyber Threats to the FIFA World Cup Qatar 2022. [Link: https://www.makeuseof.com/why-cyberattacks-surge-during-holiday-season/]

9. Volatile Geopolitics Shake the Trends of the 2022 Cybersecurity Threat Landscape.
   [Link: https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape?utm_source=hs_email&utm_medium=email&_hsenc=p2ANqtz--xbBhBVZGMHHtb_LIEKQbcrt41qxLl9qumzm_tPE4uVrXbfjXQ7jkLhIGC-CE4_L-VvLDD]

10. Researchers: ‘CosMiss’ vulnerability affecting Microsoft Azure Cosmos DB could give attacker RCE privilege.
    [Link: https://www.scmagazine.com/analysis/cloud-security/researchers-cosmiss-vulnerability-affecting-microsoft-azure-cosmos-db-could-give-attacker-rce-privileges]

11. OpenSSL Releases Security Update.
    [Link: https://www.cisa.gov/uscert/ncas/current-activity/2022/11/01/openssl-releases-security-update]