ACICE
ADMM Cybersecurity and Information Centre of Excellence

# UPDATE ON THE CYBER DOMAIN

Issue 9/22 (September)

## OVERVIEW

1. In September, we observed significant cyber activities that targeted healthcare services, possibly for geopolitical signalling and financial theft. Cyber-attacks continued in the Russia-Ukraine conflict, and ransomware operators persisted in conducting 'big-game hunting' campaigns. Vulnerabilities in major technology brands, Realtek and Google, were also reported.

## APT ACTIVITIES

2. Financial and healthcare institutions have been targeted by cyber actors in support of national strategic goals. Specifically on financial crime, reports have noted APTs conducting crypto-hacks, with stolen proceeds surging by 60% to $1.9b from January to July 2022. State-linked threat actors were also noted to have targeted essential healthcare services, likely because the healthcare sector remained very sensitive to service disruptions. Notable incidents include:

a. National Health Services (NHS). A cyber-attack on NHS in August 2022, had caused key IT systems to shut down, disrupting medical appointments and emergency prescriptions. NHS had to rely on pen and paper processes to continue operations. The attackers demanded money in return for not leaking personal data, while leaving the NHS without access to key services for over three weeks. Some analysts observed that the attack seemingly coincided with the visit by then-UK Prime Minister Boris Johnson to Ukraine in the same month. There were reports attributing this attack to Conti/Black Basta, a criminal group that provides ransomeware-as-a-service.

b. Tornado Cash. A virtual currency platform, 'Tornado Cash', was sanctioned by U.S. Treasury Department's Office of Foreign Assets Control for their role in laundering more than US$7b in crypto-currencies derived from cyber-criminal activities. At least US$455m was moved for the Lazarus Group, which analysts suspected was to fund a foreign missile program. Lazarus Group also laundered over US$100m stolen from their attacks on various blockchain-bridge[1] providers between June and August. State-linked groups were observed engaging in criminal-like activities in the crypto-space, possibly as a means to fund operations or as a form of retaliation against sanctions.

[1] Blockchain-bridges are infrastructure that connect different blockchains for users to transfer crypto-assets.

## CYBERSECURITY TRENDS

3. Russia-Ukraine Conflict Developments. Distributed denial of service (DDoS) attacks nearly trebled during the first six months of 2022. ‘IT Army of Ukraine’ claimed a successful attack against TrueConf, a popular video-conferencing service in Russia. Separately, ‘KillMilk’ claimed responsibility for DDoS attacks conducted against Lockheed Martin in retaliation for their supply of long-range rocket artillery to Ukraine. Estonia’s public institutions and the private sector were also hit by DDoS attacks in an apparent response to a decision to remove all Soviet-era monuments.

4. Ransomware. Ransomware remained the most common threat vector in the commercial space. ‘Hive’, ‘LockBit’, and ‘BlackCat’ ransomware gangs were observed targeting the same victim within weeks. The first two attacks occurred within hours of each other, while the third took place two weeks later. This was unusual, as multiple attacks by different gangs on the same victim, were months or years apart previously. Such victims also likely had unresolved vulnerabilities, which made them susceptible to repeated attacks. The ransomware gangs might have targeted one victim within a short time, presumably so that it had no time to recover and patch vulnerabilities. In addition, BlackCat, the last group that attacked the victim, not only deleted logs of their activities, but also deleted the activity-logs of the Hive and LockBit gangs. It was unknown if the ransomware gangs were collaboratively targeting the same victim, or if the attacks were opportunistic, based on vulnerabilities detected in the victim.

5. Notable Vulnerabilities. Major vulnerabilities were reported in the software by major brands like Realtek and Google.

a. Realtek. A critical vulnerability was detected that could affect network devices with Realtek’s RTL819x system. Affected components have been estimated to be in the millions. The flaw (CVE-2022-28255) could potentially allow a remote attacker to compromise devices such as routers, access points, and signal repeaters.

b. Google. Google released Chrome 104.0.5112.101 for Mac and Linux, and Chrome 104.0.5112.102/101 for Windows, to address multiple vulnerabilities. These patches addressed a high severity security issue linked to “Intents” – a feature that enabled applications and web services to be launched directly from a webpage.

c. Electron. A series of vulnerabilities was found in Electron, a software that underpins popular messaging and work-space apps like Discord, Microsoft Teams, and Slack, which are used by millions of people globally. The vulnerability could be exploited by simply inviting a victim to a meeting. Hackers would then be able to remotely control the victim’s computers after they clicked on the malicious invitation links.

# 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. 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]

2. Virtual Currency Platform ‘Tornado Cash’ Accused of Aiding APTs
   [Link: https://techcrunch.com/2022/06/24/harmony-blockchain-crypto-hack/]

3. US Treasury Department Blacklists Crypto-Mixing Service Tornado Cash Over North Korea Ties
   [Link: https://www.outlookindia.com/business/us-treasury-department-blacklists-crypto-mixing-service-tornado-cash-over-north-korea-ties-news-215231]

4. A look at Tornado Cash, the coin mixer which allegedly laundered $7B worth virtual currency
   [Link: https://www.cnbctv18.com/cryptocurrency/tornado-cash-the-coin-mixer-sanctioned-by-us-treasury-for-allegedly-laundering-7b-worth-virtual-currency-14430572.htm]

5. Ukraine war drives DDoS attack volumes ever higher
   [Link: https://www.computerweekly.com/news/252523959/Ukraine-war-drives-DDoS-attack-volumes-ever-higher]

6. Hackers attacked Russian electronic document management services
   [Link: https://24happenings.com/top-world/50221.html]

7. Killnet Releases 'Proof' of Its Attack Against Lockheed Martin
   [Link: https://www.securityweek.com/killnet-releases-proof-its-attack-against-lockheed-martin]

8. Russian hacker group Killnet claims to have launched a DDoS attack on the aerospace and defense giant Lockheed Martin.

   [Link: https://securityaffairs.co/wordpress/134341/hacking/killnet-lockheed-martin.html/]

9. Estonia Repels Cyber Attacks as Pro-Kremlin Group Takes Credit

   [Link: https://www.bloomberg.com/news/articles/2022-08-18/estonia-repels-cyber-attacks-as-pro-kremlin-group-takes-credit#xj4y7vzkg]

10. A third of organizations experience a ransomware attack once a week

    [Link: https://www.helpnetsecurity.com/2022/08/04/organizations-experience-ransomware-attack/]

11. Three ransomware gangs consecutively attacked the same network

    [Link: https://www.helpnetsecurity.com/2022/08/09/ransomware-gangs-attacks/]

12. Exploit Out for Critical Realtek Flaw Affecting many Networking Devices

    [Link: https://www.privacy.com.sg/cybersecurity/exploit-out-for-critical-realtek-flaw-affecting-many-networking-devices/]

13. 'High-severity vulnerability' found in Google Chrome browser, SingCERT advises users to install updates

    [Link: https://www.channelnewsasia.com/singapore/google-chrome-high-severity-vulnerability-hackers-singcert-2888976]

14. Researchers found one-click exploits in Discord and Teams

    [Link: https://www.malwarebytes.com/blog/news/2022/08/researchers-found-one-click-exploits-in-discord-and-teams]