Cyber-Intelligence Report

This cyber-intelligence product is produced by David Swan. Collection of information is in accordance with guidelines provided by clients. It contains 'observations', meaning headlines and links to information published online. It *MAY* contain comments and analysis. It is copyright ©David Swan 2023. This report MAY be circulated.

If this report does not meet your requirements, is in error or if you need additional information and/or analysis, please contact David Swan at DSC.Ops.Vulcan@gmail.com

Cyberwarfare: Russia vs Ukraine (38) Russia Focuses Attacks

This report contains selected cyber-security information from 1st to 15th Sept 2023.

Synopsis

1. Russia's cyber forces appear to have refined both their targeting and their methodology. LockBit hacks a UK Security company and a Montreal electrical infrastructure firm. Other groups that launched deliberate attacks include: NoName, Anonymous Sudan, AlphV and KillNet. Ukraine defeated another attack against its critical infrastructure while Meta dismantled Chinese and Russian information operations. The lead prosecutor for the International Criminal Court has announced he will investigate and prosecute cyber attacks that violate the Rome Statute.

2. Russia vs Ukraine cyberwar. Russia appears to be committed to the following ongoing 'Course of Action' for its cyber forces:

> Russian cyber forces, including allied and supporting hackers, continue to launch campaigns against Ukrainian targets, including perceived Ukrainian allies. Targeting Includes: critical infrastructure, industrial infrastructure, political, and media organizations as well as targets of opportunity.

Russian Cyber Activity

3. Analysts Comment: Russia's cyber activity appears to becoming more focused and deliberate. The indicators of this are the more refined targeting and more selective use of malware and attack TTP's (Tactics, Techniques and Procedures). For example, the '**Sandworm**' Russian Hacking Team, part of Russian Military Intelligence (GRU), is reusing 'Infamous Chisel' Android Malware against Ukrainian Military. This malware was previously successfully used against the U.S. government as well as Defense Industrial Base (DIB) networks.[1] The targets appear to be the Ukrainian Army's Android phones and tablets. According to 'The Hacker News': "*Russian forces captured tablets used by Ukraine on the battlefield, using them as a foothold to remotely disseminate the malware to other devices by using the Android Debug Bridge (ADB) command-line tool.*" The 'Infamous Chisel' malware is designed to "*enable unauthorized access to compromised devices, scan files, monitor traffic, and periodically steal sensitive information.*"[2]

1 Source: U.S. government, National Security Agency. Government Agencies Report New Russian Malware Targets Ukrainian Military

2 Source: The Hacker News. Russian State-Backed 'Infamous Chisel' Android Malware Targets Ukrainian Military

4. The Russian hacking group '**LockBit**' hacked "*Zaun, a UK company responsible for protecting maximum security sites. 'LockBit' released data which could help criminals breach some of Britain's most secretive sites including the HMNB Clyde nuclear submarine base, the Porton Down chemical weapon lab and a GCHQ listening post. ... The leak is also said to have included details about security equipment at RAF Waddington where Reaper drone missions have been conducted from for the last 10 years, and Cawdor Barracks, the base of the 14th Signal Regiment, which deals in electronic warfare.*"[3] Analysts Comment: Ransomware groups typically work for money. Hacking a target like this is out of character because it almost certainly will *NOT* generate a ransom and it attracts the attention of law enforcement and security forces.

5. What follows is a selection of Russian cyber attacks launched or reported during the past two weeks.

A. A 100-year-old municipal organization that manages electrical infrastructure in the city of Montreal, Commission des services electriques de Montréal (CSEM), was hacked by the **LockBit** ransomware group on August 3rd. The company refused to pay, contacting law enforcement. The hack came to light because the hackers published some of the stolen data. The company observed: "*It should be noted that all CSEM projects are the subject of public documents. Therefore, all these plans – engineering, construction and management – are already publicly available through the official process offices in Quebec.*"[4]

B. Cybernews noted that Russian 'patriotic hackers' '**NoName057(16)** "*has changed tactics and begun to specifically go after critical infrastructure – such as financial, government, and aviation sectors – to optimize the impact of its DDoS attacks.*" This observation follows 'NoNames' attack on the Warsaw Stock Exchange on August 29th. This was followed by Distributed Denial of Service (DDoS) attacks on "*several major Polish commercial banks, including Bank Pekao, Raiffeisen Bank, Plus Bank, Credit Agricole Bank, and BNP Paribas*".[5]

C. **Anonymous Sudan** flooded Elon Musk's 'Starlink' with "*huge amounts of traffic to take it offline*" for several hours causing outages in "*more than a dozen countries*. ... *Website outage-tracking site Down Detector said nearly 20,000 outage reports were logged by users in the US and the UK.*"[6] Neither Elon Musk nor any of his companies commented on the outage. Analysts Comment: Although this attack was unsuccessful, Starlink is an essential part of Ukraine's war against Russia. Further, Starlink was taken offline for several hours.

D. **AlphV** also known as 'BlackCat', a Russian ransomware gang has been vigorously attacking Australian targets. They claim to hold 4.95 terbytes of data on a number of Victorian companies. Access to these companies may have

3 Source: DailyMail (UK). 'Russia-linked hackers' target MoD and leak thousands of documents online relating to some of Britain's most sensitive sites in 'potentially very damaging' security breach

4 Source: The Record. Montreal electricity organization latest victim in LockBit ransomware spree

5 Source: Cybernews. Polish stock exchange, banks knocked offline by pro-Russian hackers

6 Source: Lastly.com . X Down: Sudan-Based Hackers Shut Down Elon Musk-Run X for More Than Two Hours To Put Pressure Into Launching Internet Starlink Service in Country

come from the hack of an IT provider, Core Desktop, a company based in South Melbourne.[7]

E. On 4th Sept "*the German Federal Financial Supervisory Authority (BaFin) announced today that an ongoing distributed denial-of-service (DDoS) attack has been impacting its website since Friday. BaFin is Germany's financial regulatory authority, part of the Federal Ministry of Finance, responsible for supervising 2,700 banks, 800 financial, and 700 insurance service providers.*"[8] Media speculation is that a Russian hacker group is behind the attack as Russian hacker group '**KillNet**' listed the BaFin website on its target list, published on its Telegram channel in January.[9]

F. The Canadian/U.S. Joint Commission (IJC) that oversees the shared lake and river systems along the border between the two countries has been hacked by the '**NoEscape**' ransomware gang.[10] According to Bleeping Computers this group is probably a rebranding of a defunct Russian hacking group Avaddon. Their assessment is based on the groups code, as well as its TTP (Tactics, Techniques and Procedures).[11]

6. Although there is improved TTP and targeting being demonstrated by Russia's cyber forces, defenders continue to do well. On 6th September the Computer Emergency Response Team of Ukraine (CERT-UA) on Tuesday said it "*thwarted a cyber attack against an unnamed critical energy infrastructure facility in the country*."[12] The attacker was identified as a Russian government hacking group identified as ATP28.

7. This was not the only unsuccessful attack. 'Meta', parent company of 'Facebook' and 'Instagram' announced that they 'took down' influence campaigns from China and Russia. The disrupted Russian campaign was known as Doppelganger. First disrupted by Meta in 2022, the campaign involved dozens of websites spreading Russian propaganda related to the war in Ukraine. *"This operation was focused on mimicking websites of mainstream news outlets and government entities to post fake articles aimed at weakening support for Ukraine. It has now expanded beyond initially targeting France, Germany and Ukraine to also include the US and Israel."*[13]

8. The Chinese campaign was a massive effort, compromising more than "*50 apps, including Facebook, Instagram, X (formerly Twitter), YouTube, TikTok, Reddit, Pinterest, Medium, Blogspot, LiveJournal, VKontakte, Vimeo, and dozens of smaller platforms and forums ... The network, which included 7,704 Facebook accounts, 954 Pages, 15 Groups and 15 Instagram accounts, is said to have been run by "geographically dispersed operators" across China, posting content about China and its province Xinjiang, criticism of the U.S, Western foreign policies, and critics of the Chinese*

7 Source: ABC.net. Russian ransomware gang AlphV targets pathology company, law firms in latest string of attacks
8 Source: Bleeping Computer. German financial agency site disrupted by DDoS attack since Friday
9 Source: Security Affairs. A massive DDoS attack took down the site of the German financial agency BaFin
10 Source: ITWorldCanada. Ransomware gang says it has hit International Joint Commission
11 Source: Bleeping Computer. Meet NoEscape: Avaddon ransomware gang's likely successor
12 Source: The Hacker News. Ukraine's CERT Thwarts APT28's Cyberattack on Critical Energy Infrastructure
13 Source: Security Affairs. Meta disrupted two influence campaigns from China and Russia

government."[14]

9. **ICC May Prosecute Some Cyber Crimes**: From Wired magazine: *Last month in the quarterly publication Foreign Policy Analytics, the International Criminal Court's lead prosecutor, Karim Khan, spelled out that new commitment: His office will investigate cybercrimes that potentially violate the Rome Statute, the treaty that defines the court's authority to prosecute illegal acts, including war crimes, crimes against humanity, and genocide.*

> *"Cyber warfare does not play out in the abstract. Rather, it can have a profound impact on people's lives," Khan writes. "Attempts to impact critical infrastructure such as medical facilities or control systems for power generation may result in immediate consequences for many, particularly the most vulnerable. Consequently, as part of its investigations, my Office will collect and review evidence of such conduct."*[15]

10. In 1998 the International Criminal Court (ICC) adopted the Rome Statute which addresses four core international crimes including: genocide, crimes against humanity, war crimes and 'the crime of aggression'. Karim Khan has observed that the lines between physical and digital battlefronts in warfare have long been blurred. The digital realm can generate "damage and suffering comparable to what the founders of the ICC sought to prevent." The ICC has officially announced that it will pursue prosecutions in cases of rogue cyber operations that contravene the Rome Statute under "*appropriate circumstances*" and when "*the gravity is sufficiently grave.*"[16]

11. A secondary effect of young Russians fleeing Russia is that many Russian hackers have settled in Turkey. According to the 'Financial Times' this is giving Turkish cyber crime a '*new lease on life*'.[17] By this the article means there are new groups of cyber criminals forming as well as significantly improved cyber/hacking capability.

12. **The Weather Network is Down**. On the morning of 12th Sept, the Canadian weather provider, 'The Weather Network' warned its customers of a 'system outage'. 24 hours later, Pelmorex Corp., which owns The Weather Network, said they had "*called in the RCMP to investigate a cybersecurity incident that took down its website and mobile application.*"[18] No further details have been released.

---

14 Source: The Hacker News. Meta Takes Down Thousands of Accounts Involved in Disinformation Ops from China and Russia
15 Source: Wired magazine. The International Criminal Court Will Now Prosecute Cyberwar Crimes
16 Source: Techspot online magazine. The International Criminal Court will start prosecuting cyber war crimes
17 Source: Financial Times. Influx of Russian fraudsters gives Turkish cyber crime hub new lease of life
18 Source: Globe and Mail. The Weather Network calls in RCMP to probe cyber hack