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 (37)

This report contains selected cyber-security information from 5th to 18th August 2023.

Synopsis

1. Russia continues its cyber attacks on the Ukraine using 'MerlinAgent' against the government and attacking the 'StarLink' Internet service to access Ukraine's military. External cyber-attacks by NoName057(16) also continue. Ukraine's cybersecurity chief predicts Russia's cyber-attacks will continue long after the war is over. North Korea hacks Russian missile manufacturer? Revising some major cyber events. Canada struggles with cyber attacks.

2. 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: infrastructure, political, and media organizations as well as targets of opportunity. The number, scope and quality of Russian cyber attacks continues to increase.

Russia vs Ukraine

3. Current Russian 'government' cyber attacks continue to focus on the Ukrainian government and Ukraine's military. Ukraine's computer emergency response team (CERT-UA) is warning that an OpenSource malware named 'MerlinAgent' is a remote-access tool (RAT) that allows its users to control and access a targeted computer remotely. Attackers could gain remote access to the victim's systems, execute commands, and download or delete files.[1] MerlinAgent is being delivered as an attachment to emails. There is no indication of the campaigns effectiveness.

4. **Russia targets StarLink**: Ukraine's MI5 equivalent, the State Security Service (SBU) is reporting that Russia's GRU is again trying to hack 'StarLink' to access Ukraine's military and intelligence gathering.[2] 'StarLink' is Elon Musk's Internet Service Provider (ISP). The system has three components:

A. Ground stations that transmit Internet data;

1 Source: The Record. Ukrainian state agencies targeted with open-source malware MerlinAgent
2 Source: Reuters. Ukraine says it prevented Russian hacking of armed forces combat system

B. Several thousand satellites in 'low earth orbit'; and
C. Customers satellite dishes. [3]

"Ukrainian Army Commanders rely heavily on the infrastructure for communications. SBU experts discovered malicious software on Ukrainian tablet devices that were captured by the Russians before later being recovered from the battlefield."[4]

5. Multiple approaches have been used to attack StarLink. Electronic direction finding is used to locate, then target Ukrainian ground terminals. Russia also created a weapon called 'Tobol' designed to jam StarLink signals. "*One common method of spreading malware is to leave an infected device such as a smartphone, tablet or USB stick lying around in the hope that they are picked up and used. The malware, one of five different types of information-stealing software found on the tablets, bore the hallmarks of the Sandworm hacker gang, the Ukrainian agency added. Britain's GCHQ has previously said Sandworm is Unit 74455 of the GRU, Russia's main military intelligence division.*"[5]

6. Analysts Comment: Ukraine's use of StarLink Internet may seem like an obvious target for Russia's hackers, however there appears to be a renewed effort to hack the system. Depending on what method Russia's hackers use, there is a possibility that malware could move to the Internet outside StarLink or Ukraine.

7. Russia continues a number of other campaigns including targeting of European Diplomats. 'BlueBravo' is a Russian government hacking team attributed to Russia's Foreign Intelligence Service (SVR), who is using several malware including: 'GraphicalNeutrino' and 'GraphicalProton'. "*Based on observed trends, Insikt Group predicts that BlueBravo will continue to adapt and create new malware variants while leveraging third-party services for C2 obfuscation. Defenders are urged to invest additional time and resources to track the evolving group, particularly organizations targeted by Russian state actors in relation to the Russia-Ukraine conflict.*"[6]

8. Russia's 'patriotic hackers' NoName057(16), followed up attacks on Spain and Italy with attacks on the Netherlands and France. The impact of these effects appears to be minimal as:

- *Dutch cybersecurity agency said in a statement on Tuesday that the impact of these DDoS attacks is "limited and symbolic."* and
- The website of France's customs agency *was down due to a planned "maintenance operation."* Also, France's financial regulators website is "*currently unavailable*".[7]

9. At the Black Hat conference in Las Vegas, Ukraine's cybersecurity chief, Victor Zhora, revealed that Ukraine's defenders tackle an average of ten major cyber incidents weekly, with the country having faced 11,002 such incidents since the full-scale war began.[8] He outlined the five phases of Russia's cyber-attacks. He predicted that:

3 Source: Wired.com. The Hacking of Starlink Terminals Has Begun
4 Source: Microsoft 'Start'. Russian spy agencies targeting Starlink with custom malware, Ukraine warns
5 Source: Microsoft 'Start'. Russian spy agencies targeting Starlink with custom malware, Ukraine warns
6 Source: Recorded Future. BlueBravo Adapts to Target Diplomatic Entities with GraphicalProton Malware
7 Source: The Record. Pro-Russian hackers claim attacks on French, Dutch websites

"Russia's online attacks against his country – including cyber "war crimes" – will continue long after the physical war ends unless increased international pressure is applied. "*Russia will continue to be dangerous in cyberspace for quite a long period, at least until a complete change of the political system and change of power in Russia, converting them from an aggressor ... So definitely, even after the war ends on the battlefields and in kinetic aspects, more likely it will continue in cyberspace.*"[9]

10. A pro-Ukrainian hacker group calling itself "sudo RM-RF" said on Telegram on 7th August that "*it had hacked the website of Moscow's municipal property registration bureau (MosgorBTI).*" The group describes itself as "*IT experts working for peace in Ukraine.*"[10] The report has not been confirmed.

North Korea hacks Russia?

11. Cyber security firm SentinelOne reports that Russian missile and satellite developer NPO Mashinostoyeniya was hacked by Two North Korean hacker groups. State-backed hacker group 'ScarCruft' was identified as the group behind the email server compromise, while the Windows backdoor was attributed to Lazarus Group. The two groups had access to 'sensitive internal IT infrastructure' for five to six months. NPO Mashinostoyeniya is known for:

- developing rockets for the Soviet military;
- designing missiles;
- designing and building the hypersonic cruise missile known as Zircon;
- IP for ampulization of rocket fuel.[11]

Revisiting Major Cyber Events

12. This report has covered a number of 'standalone' major cyber events outside. We forecast major impacts from: the 'Solar Winds' hack, Apache Log4j vulnerability, and the ongoing MOVEit! Hack.

- '**Solar Winds**'. Solar Winds is an American company that develops and sells software, the 'Orion Platform', to manage computer networks and associated information technology infrastructure. In 2020 Russian Foreign Intelligence Service hackers hacked the companies production processes and inserted a 'backdoor' in a software library. When the software was updated, the backdoor was installed.
- In a Securities and Exchange Commission (SEC) filing Securities and Exchange Commission fewer than 18,000 of its 33,000 Orion customers were affected.[12] Organizations hacked included a 'who's who' of U.S. government departments, defence contractors and major organizations. A few of the

8 Source: Euromaidanpress. Ukraine tackles ten major Russia's cyber attacks weekly – Ukraine's cybersecurity chief
9 Source: The register. Ukraine's Victor Zhora: Russia's cyber 'war crimes' will continue after ground invasion ends
10 Source: rferi.org. Ukraine-Linked Group Claims It Hacked Website Of Moscow Property Registration Bureau
11 Source: The Register. North Korean hackers had access to Russian missile maker for months, say researchers
12 Source: New York Times. Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit

organizations impacted include: NATO, the EU (government and industry), the UK (GCHQ, MoD, and the National Health Service).

- The 'Solar Winds' company, is still in operation. The corporation hired former CISA director Chris Krebs to help recover from the cyber attack. The hack *appears* to have been remediated by both Solar Winds and its clients.

- **Apache Log4j**. Hackers trying to manipulate the computer game 'Minecraft' discovered they could enter commands directly into a game process, and subsequently take over the server running the game. They discovered the Apache Log4j vulnerability, an OpenSource slice of computer code used in computer programs, industrial systems, arguably billions of devices. The effort to patch the vulnerability was massive. No matter how determined the effort to patch the vulnerability, some software and devices are too old, or not designed to accept patches. The vulnerability should still be considered 'active'.
- For more information I highly recommend the following YouTube video as a summary of the issues: Apache Log4j: The Exploit that Almost Killed the Internet

- **MOVEit!** Ipswitch Inc, a subsidiary of Progress Software, created a means of securely moving very large data files. The Cl0p ransomware group got into the software and planted a backdoor. According to 'Kon Briefing' the number of known primary victims is 689 organizations and 43 to 48 million individuals (effective 17th August). The Cl0p ransomware group has commenced hiring other criminal hackers in order to affect as many victims as possible. One estimate has the ransomware group collecting 100 million dollars (USD) from this hack. This hack remains 'in progress' with fourteen newly named organizations joining the victim list on August 17th.[13]

Canada

13. Canada is far from immune to increasing cyber threats. The LexisNexis® Digital Identity Network found 183% Increase in Bot Attacks for Canadian E-commerce Industry, from January to December 2022, year over year.[14] Another recent Canadian hack outlines the scale of the threat. Nearly 1.5 million Albertan's are affected by a data breach at the Alberta Dental Service Corporation. This include 7,300 Albertan's whose banking information was exposed. A relatively new ransomware group, 8Base, was the attacker. The ransom was paid.[15] Most Canadian cyber attacks, including ransomware attacks, go unreported, including in security filings.

---

13 Source: Kon Briefing. MOVEit hack victim list

14 Source: Yahoo Finance. Canadian Cybercrime and Fraud Trends Report Notes a Drastic Increase in Bot and Human Initiated Attacks

15 Source: Channel Daily News. Alberta dental plan administrator paid ransomware gang after attack