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 (33) Russian hackers score

This report contains selected cyber-security information from 10th to 23rd June 2023.

Synopsis

1. Russian hackers scored some major successes. Successful attacks included: Ukrainian government e-mail, European Investment Bank, and the MOVEit transfer suite. Ukrainian hackers hacked the telecommunications provider for Russia's Central Bank. Canada doesn't seem to appreciate the cyber threat.

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

> Ongoing: Russian cyber forces, including allied forces, have launched a series of cyber campaigns against both Ukrainian targets and their allies. Targeting Includes strategic and general targets as well as vulnerable governments. Russian cyber attacks are increasing against Ukrainian Allies.

Russia Cyber Attacks

3. Russian hackers had some major successes during this reporting period. There were multiple major data breaches in Australia. The United States had attacks on multiple health care systems and educational facilities (mostly universities). Microsoft had outages in its cloud services due to a Russian hacker group. Arguably the most successful attack was by the Russian ransomware gang Cl0p on Progress Software's MOVEit file transfer suite including the MOVEit Cloud. The hackers claim to have hit hundreds of organizations.[1] At least sixty-three organizations are known have been hacked, so far. Cl0p has given MOVEit victims until June 14 to pay its ransom or it will leak stolen data online.[2]

4. The MOVEit transfer system is designed to securely move large files between organizations. Cl0p hackers identified three vulnerabilities (that we know of), which enabled them to access and download data from inside the program. Stated another way, like the 'Solar Winds' hack, the attackers managed to break into network infrastructure. Some estimates place the number of potential of first order victims as high as 3,000. For example "*one of the first victims to come forward was UK-based*

1 Source: Security Week. New MOVEit Vulnerabilities Found as More Zero-Day Attack Victims Come Forward
2 Source: The Register. Hold it – another vulnerability found in MOVEit file transfer software

payroll and HR company Zellis. Several major companies using Zellis services were hit, including the airlines British Airways and Aer Lingus, the BBC, and pharmacy chain Boots." Other victims include:

- Government of Nova Scotia[3],
- University of Rochester,
- Illinois Department of Innovation & Technology (DoIT) and
- Minnesota Department of Education (MDE).

5. The files Cl0p have downloaded include a lot of personal data. For example "*the Minnesota Education Department has determined that 24 files were accessed by hackers. These files contained the information of roughly 95,000 students placed in foster care, including names, dates of birth and county of placement. Dozens of other students also had information exposed, including name, date of birth, address, parent name, high school and college transcript information, and the last four digits of their social security number.*" The Cl0p ransomware operators claim ... "*that they will not attempt to extort money from impacted government organizations, including cities and law enforcement agencies. "We erased all your data. You do not need to contact us. We have no interest to expose such information,*" the hackers wrote.[4] "A *senior CISA* (the US government's Cybersecurity and Infrastructure Security Agency) *official said there's no evidence to suggest any coordination between Clop and the Kremlin in the MOVEit attacks."*[5]

6. Analysts Comment: Like the Solar Winds hack, this attack will probably continue to get worse for some time as Cl0p managed to hack numerous service providers such as Zellis and and American networking provider, Extreme Networks. It is also possible that Cl0p will sell data, such as U.S. government data, to the Russian government.

7. On 16th June we published an 'Alert' that 3 Russian hackers groups, KillNet. Anonymous Sudan and REvil formed an "*alliance to launch a concerted cyberattack on the Western financial system, particularly targeting the SWIFT wire transfer system*" with an objective of "*cut off the pipeline of Western aid to Ukraine.*"[6] On 19th June the European Investment Bank (EIB) reported via Twitter "@EIB We are currently facing a cyber attack which affects the availability of http://eib.org and http://eif.org. We are responding to the incident. 7:21 AM · Jun 19, 2023". Reports disagree on the length of the attack with one source reporting the attack, a Distributed Denial of Service (DDoS) attack, lasted three days (until 21st of June). Reports do agree that the EIB was forced offline on the 19th and was unable to make transactions for several hours.[7]

8. Analysts Comment: There is no way to assess the 'success' of the attack. DDoS attacks can be used as cover for other types of cyber attacks, and so far there is no way of knowing if other attacks were attempted. What is chilling is the mix of

3 Source: CTV News, Atlantic Bureau. N.S. identifies thousands more victims of global data hack, including school workers

4 Source: Security Week. New MOVEit Vulnerabilities Found as More Zero-Day Attack Victims Come Forward

5 Source: The Register. US government hit by Russia's Clop in MOVEit mass attack

6 Source: Proactive Australia. Pro-Russian hackers allege "massive" cyberattack on Western financial system; led by Medibank hackers

7 Source: DIGIT News. Anonymous Sudan and Killnet Strike Again, EIB Confirms Cyber Attack

capabilities and resources in this attack:

- Anonymous Sudan: Attributed by some cyber security organizations as unformed Russian government hackers[8],
- REvil: Top Tier international ransomware group.
- KillNet: Russian 'patriotic hackers and supporters'. Potentially a force-multiplier in DDoS attacks. Can also provide distraction for a more sophisticated cyber attack.

If the Russian government or even the Federal Security Service, perceived the attack as successful, there is potential for much worse.

9. A known hacker team of Russian Military Intelligence (GRU) manged to penetrate some Ukrainian government email servers. The attack used a technique called 'spearphishing' (fake emails) designed to get users to click on links or attachments. Once inside the email program 'Roundcube', the attackers ran "*reconnaissance and exfiltration scripts, redirecting incoming emails and gathering session cookies, user information, and address books. The attachment contained JavaScript code that executed additional JavaScript payloads* ….". The attack *may* have been running since November 2021. A Ukrainian prosecutors office, an 'executive authority' and some 'air force logistics' have been compromised. Recorded Future, a western cyber security company working with Ukraine's Computer Emergency Response Team (CERT-UA) assessed: "*that BlueDelta* (the GRU hacking team) *activity is likely intended to enable military intelligence-gathering to support Russia's invasion of Ukraine and believe that BlueDelta will almost certainly continue to prioritize targeting Ukrainian government and private sector organizations to support wider Russian military efforts.*"[9]

Ukraine Cyber Attacks

10. During the first week of June, as the Ukrainian Army started the 'counter-offensive, cyber attacks were launched on "multiple Russian websites". Most of the attacks were 'defacements' designed to show support for the Ukrainian military.[10] At least one attack was more significant. On 9th June A group of Ukrainian hackers known as the 'Cyber.Anarchy.Squad' claimed responsibility for a cyber attack that crashed Russian telecom provider Infotel JSC on 8th June. Moscow-based Infotel is the Internet Service Provider (ISP) for connectivity services between the Russian Central Bank and other Russian banks, online stores, and credit institutions. Multiple major banks across Russia had their access cut off from the country's banking systems so that they could no longer make online payments.[11]

11. The 'Cyber.Anarchy.Squad' claims, made on Telegram, were somewhat extreme. "*Acidify the soil, fill the ground with concrete*," the group wrote in a message posted to

8 Source: CyberCX. A bear in wolf's clothing: Insights into the infrastructure used by Anonymous Sudan to attack Australian organisations

9 Source: Recorded Future. BlueDelta Exploits Ukrainian Government Roundcube Mail Servers to Support Espionage Activities

10 Source: Cyberscoop. Ukrainian hackers target telecom firm connected to Russian central bank

11 Source: Bleeping Computer. Ukrainian hackers take down service provider for Russian banks

Telegram, according to a Google translation. "*All their infrastructure is destroyed, nothing alive is left there.*[12] [13]*Let them try to restore it now, but their chances are as slim as finding an easy life in Russia.*" The Russian ISP appeared to confirm some of the attackers claims saying: "*We inform you that as a result of a massive hacker attack on the Infotel network, part of the network equipment was damaged. ... Restoration work is currently underway. Additional deadlines for completing the work will be announced.*" Some core Infotel services appeared to be down for at least thirty-three hours. 'The Record' also reported that the hackers downloaded Infotel documentation including customer lists and email.[14]

Canada

12. Informal discussions among the Canadian cyber security personnel I know suggest that if Canadian cyber security is improving, progress is spotty and very slow. One of the reasons for the slow progress is the apparent lack of appreciation of the threat by any level of government. For example, the CBC published a look at why Newfoundland's health system was hacked. When investigating the hack, the Canadian Centre for Cyber Security reported there were **three** IT security staff for the entire provincial health system. The cost of this lack of security:

- *More than a half million people ... had their privacy breached.*
- *More than 200,000 files on an Eastern Health network drive, accessed and taken.*
- *More than 200 gigabytes of data exfiltrated, or stolen, by cyberthieves affiliated with the Hive ransomware gang.*[15]

13. The federal response to cyber threats is at best 'tepid'. Canadian Defense Minister Anita Anand said in an interview on the sidelines of an Asian security summit in Singapore, "*We have seen attacks on critical infrastructure in our country and we are very conscious to advise Canadian organisations and Canadian companies to take mitigation measures.*"[16] Closer to home, the Canadian Centre for Cyber Security, part of CSE, issued a warning that there is a cyber threat to Canada's oil and gas sector. Buried deep within is the assessment: "*that state-sponsored cyber threat actors are almost certainly continually improving their capability to conduct destructive or debilitating cyber activity against critical infrastructure.*"[17]

---

12 Source: Cyberscoop. Ukrainian hackers target telecom firm connected to Russian central bank
13 Source: The Record. Pro-Ukraine hackers claim to take down Russian internet provider
14 Source: Twitter @igorsushko . After being down for 33 hours, the Infotel network shows a pulse. BGP (Border Gateway Protocol) connectivity is back. Note: Other Twitter users reported that only some Russian banks were back online.
15 Source: CBC News. The inside story of how N.L. health officials failed to act before a ransomware gang struck
16 Source: Alarabuya News. Canada facing rising threat from cyberattacks: Minister
17 Source: CSE / Canadian Centre for Cyber Security. The cyber threat to Canada's oil and gas sector

Cyber-Intelligence Report