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 (34)

This report contains selected cyber-security information from 24th June to 7th July 2023.

Synopsis

1. Russian hackers go after your logins. The NoName hackers group updates its DDoS software and hits Ukrainian banks. An update on the MOVEit! hack, Anonymous Sudan claims they hacked Microsoft and LockBit hacks Japan's largest port. Ukrainians countered by: downing Russia's primary Satellite Internet Provider and Russia's railroad company RZD. The Suncor hack.

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

> 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.

Russian Cyber Attacks

3. On 25th June Microsoft has disclosed that it's detected a spike in credential-stealing attacks conducted by the Russian state-affiliated hacker group known as Midnight Blizzard. Midnight Blizzard, formerly known as 'Nobelium', is also tracked under the monikers APT29, Cozy Bear, Iron Hemlock, and The Dukes. Analysts Comment: This is a Russian government hacking group that is rapidly expanding the Russian governments cyber target list. Microsoft's threat intelligence team says the campaign *"targets governments, IT service providers, NGOs, defense, and critical manufacturing sectors. ... The group, which drew worldwide attention for the SolarWinds supply chain compromise in December 2020, has continued to rely on unseen tooling in its targeted attacks aimed at foreign ministries and diplomatic entities. It's a sign of how determined they are to keep their operations up and running despite being exposed, which makes them a particularly formidable actor."*[1]

4. On 27th June Russian hacker group 'NoName(057)16' announced: *"We will start today's journey with an attack on the financial sector of Ukraine🇺🇦."* Since the threat actors edict ... *"nearly a dozen major Ukrainian banks have been hit daily by the gang's signature DDoS attack method. Targets include four of the nation's largest commercial*

[1] Source: The Hacker News. Microsoft Warns of Widescale Credential Stealing Attacks by Russian Hackers

banks, including First Ukrainian International Bank (PUMB), State Savings Bank of Ukraine (Oshchadbank), Credit Agricole Bank, and Universal Bank. The gang claims to have knocked several of the bank websites completely offline, but has specifically gone after authorization services, login portals, customer service systems, and loan processing services."[2]

5. In early June Microsoft suffered a number of 'severe outages' in a number of its premiere products including: Outlook email, OneDrive file-sharing & storage, and the cloud computing infrastructure Azure. Anonymous Sudan announced that not only were they responsible for the outages but they had stolen credentials for 30 million customer accounts. *"We announce that we have successfully hacked Microsoft and have access to a large database containing more than 30 million Microsoft accounts, email and password. Price for full database : 50,000 USD".*[3] Microsoft's response: *"We have seen no evidence that customer data has been accessed or compromised."*[4] Analysts Comment: Microsoft has been very actively supporting Ukraine's cyber security efforts. Anonymous Sudan is usually identified as a Russian government hacking team.

6. On 4th July Researchers at the cybersecurity firm Sekoia warned that the pro-Russia hacker collective 'NoName(057)16' had released an updated version of the DDoSia attack tool. The new version features an attempt to keep its targeting list secure and demonstrates the intention to make it multi-platform to Windows, Mac and Linux computers can launch attacks. NoName's objective is to flood targets with 'junk' internet requests, flooding or blocking the site, making it unable to deliver services. In general its targets have been NATO countries and Ukraine. In May and June targeted were mostly Lithuanian, Ukrainian, and Polish, accounting for 39% of the project's total activity. *"Sekoia analysts say that the DDoSia platform has grown significantly over the year, reaching 10,000 active members contributing firepower to the project's DDoS attacks and 45,000 subscribers on its main Telegram channel."*[5]

7. The updated tool was written in Golang and apparently released on 19th April. *"NoName057(16) is making efforts to make their malware compatible with multiple operating systems, almost certainly reflecting their intent to make their malware available to a large number of users, resulting in the targeting of a broader set of victims." concludes the report. "Sekoia.io analysts assess that strengthening the security of their software is part of NoName057(16)'s efforts to continuously develop their capabilities, almost certainly driven by their active community as well as the increasing scrutiny of their activities from the CTI community. It is highly likely we will observe further developments in the short term."*[6]

8. On 5th July the Pakistani government issued an advisory *"that a Russian hacker group is involved in targeting Pakistan's military and civil setups. … Kill Net is a Russian APT group that has been targeting Pakistan's military and civil setups with*

[2] Source: CyberNews. Ukrainian banks hit by pro-Russian NoName hackers

[3] Source: Security Affairs. Anonymous Sudan claims to have stolen 30 million Microsoft's customer accounts

[4] Source: Microsoft. Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks

[5] Source: Bleeping Computer. Pro-Russia DDoSia hacktivist project sees 2,400% membership increase

[6] Source: Security Affairs. NoName(057)16's DDoSia Project's gets an upgrade

numerous attack vectors including DDoS attacks. ... According to the advisory, the Kill Net uses DDoS and brute force dictionary attacks as the main weapons to cause mass service disruption of vulnerable services."[7]

9. In other Russian hacks that *may not* be related to the war with Ukraine, the MOVEit! Hack is steadily growing in scope and the 'LockBit ransomware gang shutdown Japan's largest port, Nagoya, on 5th July.

10. MOVEit! One source estimates that more than 200 organizations have been compromised by the MOVEit! Hack conducted by the Cl0p hacker gang. The issue with the MOVEit! hack is that it is all about large quantities of sensitive data that the company was supposed to move securely. Newly announced victims include:

- Insurance giant Genworth Financial with 2.5 million to 2.7 million of its customers and agents compromised.[8]
- Largest public pension fund in US affected by MOVEit breach. $477 billion in assets for over 1.5 million public employees, retirees, and their families in California.[9]
- Wilton Re, a US-based insurer, exposed the details of nearly 1.5 million people.[10]
- Barrick Gold Corp. of Toronto, ON[11]
- Vancouver, BC Metro Transit Police Department[12]
- Schneider Electric and Siemens Energy[13]
- Shell Confirms MOVEit-Related Breach, employee personal information has been stolen[14]

This is **NOT** a comprehensive list of victimized companies. A large number of the breaches are coming from third party service providers who were compromised. There is potential for many more victims to be compromised. By extension, many more people have had personal data compromised. I *assess* this as still early days in the MOVEit! hack.

11. LockBit is a ransomware-as-a-service operator that works with affiliates that conduct attacks. Nagoya the primary shipping port for Toyota as well as moving 2.68 million shipping containers and 164 million tons of cargo in 2022. This makes it an ideal ransomware target. Port announcements suggested the port would be back in operation the afternoon of 6th July.[15] Analysts Comment: The rapid recovery of port operations suggests that either the attack was detected 'early' and rapidly mitigated (*most likely*) and/or recovered from backups.

Ukrainian & Allied Cyber Attacks

[7] Source: Pakistan Today. Russian hacker involved in targeting Pakistan's military and civil setups
[8] Source: Bank Info Security. MOVEit Hacks: Data Breach Victim Count Grows by Millions
[9] Source: The Record. Largest public pension fund in US affected by MOVEit breach
[10] Source: Cyber News. 1.5M people exposed in biggest MOVEit bug breach so far
[11] Source: IT World Canada. Canadian-based gold miner among the latest MOVEit data breach victims
[12] Source: TransitPolice.ca . Cyberattack on third-party software impacts Transit Police
[13] Source: Security Affairs. Schneider Electric and Siemens Energy are two more victims of a MOVEit attack
[14] Source: Security Week. Shell Confirms MOVEit-Related Breach After Ransomware Group Leaks Data
[15] Source: The Register. LockBit louts unload ransomware at Japan's most prolific cargo port

12. On 30th June a group claiming affiliation to the PMC Wagner, the private military company run by Victor Prigozhin, “infiltrated” and “compromised” Dozor-Teleport CJSC, a Russian satellite telecom company. The satellite company provides internet and other communication services that support state agencies such as Moscow’s main intelligence agency. In addition the hackers leaked nearly 700 files, defaced several websites and put up Wagner-related messages and a video. Russian reports say full recovery of Dozor-Teleport could take up to two weeks. “*Early investigations show the company was breached through a third-party cloud provider.”*[16]

13. “*Oleg Shakirov, a cyber policy expert and consultant at the Moscow-based PIR Center think tank, tweeted Thursday that “Wagner’s involvement is very unlikely,” and that it looked “like Ukrainian false flag trolling.”*[17]

14. On 5th July “*Russian state-owned railway company RZD said Wednesday that its website and mobile app were down for several hours due to a “massive” cyberattack, forcing passengers to only buy tickets at railway stations. ... RZD’s system was down for at least six hours, but the company said later on Wednesday that it had restored its operation despite ongoing attacks. Some of the company's online services are still unavailable due to the increased load, RZD said. ... The Ukrainian hacktivist group IT Army claimed responsibility.” “The group’s claims could not be immediately verified.”*[18]

Suncor

15. This morning on the ‘EyeOpener’ the CBC Calgary morning show I heard the question, “but why would they hack Suncor?” Suncor Energy produces approximately 20% of Canada’s energy, and *“is one of Canada's largest synthetic crude producers, having an annual revenue of $31 billion”*[19] *“as well as owning a network of more than 1,800 Petro-Canada retail and wholesale locations.”* This means the Suncor has the cash to pay a ransom. More significantly, hacking Suncor messes with Canada’s energy supplies and by extension, North American (read American) energy supplies. Russia has been actively probing networks of energy providers for over a year – since the start of the ‘Special Military Operation’. An attack ***should*** have been anticipated. Suncor’s response: *Suncor acknowledged it had experienced a "cybersecurity incident" and stressed that while it was confident that no customer or employee data had been stolen, "some transactions with customers and suppliers may be impacted."*[20]

To unsubscribe from this service send an email to DSC.Ops.Vulcan@gmail.com

[16] Source: Dark Reading. Russian Satellite Internet Downed via Attackers Claiming Ties to Wagner Group

[17] Source: Cyberscoop. Russian telecom confirms hack after group backing Wagner boasted about an attack

[18] Source: The Record. Russian railway site allegedly taken down by Ukrainian hackers

[19] Source: Bleeping Computer. Suncor Energy cyberattack impacts Petro-Canada gas stations

[20] Source: CBC News. Petro-Canada payment problems continue, but company says it's 'making progress' on fix