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 (23) Russia Deploys 'Wipers'

This report contains selected cyber-security information from 20th January to 3rd February 2023.

Synopsis

1. Russia increased its cyber attacks, both at Ukraine and against external 'enemies' using KillNet. More countries are warning of potential cyber attacks from 'pro-Russian groups' – as demonstrated by an attack on the London Stock Exchange. Ukraine's cyber forces have hacked Russia's Gazprom. The latest hacks in Canada. Lastly, many Canadians remain unaware that hacking is a 'thing'.

2. Russian 'Courses of Action' for cyber forces, including allies such as 'patriotic', mercenary, and domestic criminal hackers are *assessed* as:

> **Ongoing**: Russian cyber forces, including allied forces, have launched a series of cyber ***campaigns*** against **both strategic targets and general targets** as well as vulnerable governments.
>
> **Worst Case Scenario**: President Putin decides to focus Russia's cyber attacks on one country (such as Canada) or a small group of vulnerable countries. *Assessed as UNLIKELY.*
>
> **Best Case Scenario:** Russia agrees to cease or is forced to cease offensive cyber operations. *Assessed as VERY UNLIKELY.*

Russia

3. **Cyber Offence**: Russia increased the number and the severity of its cyber attacks during the past two weeks. Multiple groups from Russian security services launched new attacks or increased their attacks. The 'Gamaredon Group' has been attacking Ukrainian 'Telegram' channels, targeting military and law enforcement users. The technique is new. According to the he BlackBerry Research and Intelligence Team: "the Gamaredon group's network infrastructure relies on multi-stage Telegram accounts for victim profiling and confirmation of geographic location, and then finally leads the victim to the next stage server for the final payload." Ukrainian Security associates the Gamarendon Group with the FSB (formerly the KGB).[1]

4. The Sandworm APT (Advanced Persistent Threat) hackers group of Russian Military

1 Source: The Hacker News. Gamaredon Group Launches Cyberattacks Against Ukraine Using Telegram

Intelligence (GRU) launched two cyber attacks during the past two weeks. A brand new 'wiper' called SwiftSlicer was targeted attack against an unidentified Ukrainian organization. The attack was notable in that its characteristics suggested that the attackers already had internal access to the target network.[2] A second attack has been described as a 'swarm' of 'wiper attacks'. Wiper attacks destroy all information on the computer, rendering the computer useless. Five wipers were identified in the one attack. 'CaddyWiper', 'ZeroWipe' and 'Sdelete' targeted Windows computers. "*AwfulShred and BidSwipe took aim at Linux and FreeBSD systems at Ukrinform*", a Ukrainian News agency.[3] Most analysts assess the attacks as 'low impact' or 'generally ineffective'.

5. Russia's 'patriotic hacker group', KillNet has been active against external 'enemies'.

   A. The first attack was a Distributed Denial of Service (DDoS) attack against web sites of German airports, 'administrative bodies' and financial sector organizations (ie. Banks). The German Federal Cyber Security Authority (BSI) reported the attacks made "*some websites unavailable*", without there being "*any indication of direct impacts on (the organisations') services*".[4]

   B. The next DDoS attack successfully crashed the website of a Dutch hospital. KillNet had also called for supporters to attack hospitals in Utrecht, Rotterdam and Nijmegen. '*It's very simple,' the founder of Killnet wrote in the group chat. 'We are destroying the medical facilities in these countries for their support for the Nazis in Ukraine.*'[5] According to the hospital only the web side was crashed. "*The medical records of UMCG patients has not been compromised. Patients can still view their medical history, operations, medicines, and appointments.*"[6]

   C. The third attack was against the "*websites of 14 top US hospitals and universities. ... Targets included Stanford Healthcare, Duke University Hospital and Cedars-Sinai. DailyMail.com found seven hospital websites were back in service by 12pm EST.*[7] The University of Michigan and Atrium Health's web sites took longer to resume service, however operational services remained secure.[8] [9] Los Angeles-based UCLA Health and Colorado-based UCHealth did not fare as well. Data analytics tools integrated into the health system's public website and mobile app compromised some patient information. "*UCHealth had data from 48,879 individuals compromised by a breach at its hosted services provider Diligent.*"[10]

6. Analyst's Comment: When KillNet attacks an organization that is prepared (that has

2 Source: Security Affairs. Sandworm APT targets Ukraine with new SwiftSlicer wiper
3 Source: DarkReading. Russia's Sandworm APT Launches Swarm of Wiper Attacks in Ukraine
4 Source: Security Week. Cyberattacks Target Websites of German Airports, Admin
5 Source: Dutch News. Pro-Russian hackers bring down website of Dutch hospital
6 Source: NL Times. Pro-Russian hackers Killnet behind Groningen hospital cyberattack
7 Source: Daily Mail (UK). Russian cyber gang Killnet brings down websites of 14 top US hospitals and universities - including Stanford and Duke
8 Source: Detroit Free Press. University of Michigan Health public websites hit by pro-Russian cyberattack
9 Source: WSOC-TV. Atrium Health's website offline after being targeted by Russian hacking group
10 Source: SCMagazine. Data breaches hit UCLA Health, UCHealth

good cyber defences), impact is minimal. When organizations are **not** prepared, KillNet is able to cause significant issues, such as at UCHealth. In all cases listed above, national authorities warned of the potential of cyber attacks for many months.

7. One effect of the attacks is that national Intelligence and Security organizations in several countries are warning their citizen to expect more and worse attacks, coming from more than KillNet.

> A. In the UK the National Cyber Security Centre (NCSC), part of Britain's GCHQ, is warning that "*a Russia-based hacking group named Cold River is behind an expansive and ongoing information-gathering campaign that has struck various targets in government, politics, academia, defence, journalism, and activism. A second, Iran-based, group known as Charming Kitten has deployed the same "spear-phishing" techniques to gather information. Since Russia's invasion of Ukraine, Cold River has escalated its hacking campaign against Kyiv's allies, cybersecurity researchers and western government officials.*"[11]
>
> B. Canada's Communications Security Establishment (CSE) said the agency "*is aware of reporting regarding an increase in Russian state-aligned hacktivist groups seeking to compromise or disrupt Ukrainian-aligned allies, in response to their continued support of the government of Ukraine.* and called for a "*heightened state of vigilance" against the threat of retaliatory cyber attacks from Russia-aligned hackers.*"[12]
>
> C. Denmark *"raised its cybersecurity alert level from "medium" to "high" after several attacks by pro-Russian hacker groups in recent weeks, the country's Center for Cyber Security said. ... "The risk level is being raised on the back of high activity among pro-Russian cyber activists, who are carrying out many attacks against targets within a wide range of NATO countries," the center said in a statement. ... Hackers have become better at planning and executing their attacks, giving them more "striking power."*[13]

8. On February 2nd trading on the London Stock Exchange was halted due to a ransomware attack. The hacker group 'Lockbit' hacked Ion Markets, a financial data group crucial to the financial plumbing underlying the derivatives trading industry. The attack affected 42 clients. Ion says: "*The incident is contained to a specific environment, all the affected servers are disconnected, and remediation of services is ongoing.*"[14] [15] Lockbits previous target was the Royal Mail.

Ukraine

9. "*In April 2022, cybersecurity expert Jeff Carr told CyberNews that cyber operators at the Main Directorate of Intelligence at the Ministry of Defense of Ukraine (GURMO) have been conducting computer network operations (CNO) against Gazprom* (Russia's

11 Source: Reuters. Britain sounds alarm on Russia-based hacking group
12 Source: CBC. Intelligence agency calls for a 'heightened state of vigilance' against Russian-aligned hacks
13 Source: Business Insurance. Denmark raises cyber risk alert level after Russian attacks
14 Source: IT Security Guru. Ransomware attack halts London trading
15 Source: Telegraph (UK). City Trading in chaos as Russian cyber gang strikes software giant

principal energy corporation). *According to Carr, GURMO was able to exfiltrate almost 1.5 TB of sensitive data from the company. The data includes administrative files for Gazprom management, communication requirements for the plants, maps, a massive 3,600 page .pdf on all of the requirements for construction of a new pipeline facility, a work order for an overhaul of the relay protection and automation devices, information on the assignment of the primary communications network of the pipeline as well as the digital radio-relay communication line (CRRL), and much, much more."*[16] Analyst's Comment: Gazprom has been a target for Ukraine's IT Cyber Army since the beginning of the conflict.

Canada

10. There continue to be significant hacks being reported across Canada. In B.C. Maple Ridge-Pitt Meadows School District is warning its school community about a data breach involving more than 19,000 records – without providing any details of what got breached. files containing first names, last names, schools/departments, district email addresses and student grades were released, but the school district says this is low sensitivity information.[17]

11. Nunavut's Qulliq Energy Corporation (QEC) was targeted and network breached in a cyberattack. The utility delivers electricity to approximately 15,000 electrical customers across 2 million sq. km. of Canada's far north through stand-alone diesel power plants in 25 communities. Power generation wasn't disrupted, but customers are being warned to watch their bank and credit card accounts for unusual activity.[18]

12. A Toronto-headquartered Canadian manufacturer of die cast tools and car parts that three production facilities within its Large Mould Group are recovering from a cyber attack. "*Although fuller details are yet to be disclosed about the attack on three of Exco Corp's production facilities, current indicators point to this not being ransomware related," said Dave Masson, director of enterprise security for Darktrace Canada"*.[19]

13. Analyst's Comment: This week I was asked by a Canadian media organization to answer the question: "Is ransomware a thing?". Neither the producer nor the on-air personality was aware that malware from the Russia – Ukraine conflict could affect them or Canadians in general.[20]

---

16 Source: Security Affairs. IT Army of Ukraine gained access to a 1.5GB archive from Gazprom
17 Source: Microsoft. B.C. school district investigating data breach affecting up to 19,000 people
18 Source: IT World Canada. Nunavut power utility's servers hit by cyber attack
19 Source: IT World Canada. Canadian tool manufacturer hit by cyber attack
20 'Is ransomware a thing?' was intended as a serious question. That media organization is apparently unaware of the impact of hacking/malware.