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 (22) Russia's NoName hackers

This report contains selected cyber-security information from 16th to 20th January 2023.

Synopsis

1. Russia continues to grow its 'civilian hacker' force, but it remains largely ineffective. Commercial cyber support for Ukraine is in excess of $400 million USD. Sweden expects Russia to escalate the cyber conflict. Belarus authorizes internet piracy. 1,000 ships have been impacted by an attack on Ship Management Software. A skimmer attack on the Ontario Liquor Control Board attracted Canadian media attention.

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: Cyber Offense

3. Russia is not happy that its cyber efforts are being countered. Russia's top cyber diplomat has warned that "*a worsening conflict with the U.S. in cyberspace could lead to a real-world escalation between the two powers. Russian special presidential representative for cooperation in the field of information security Andrey Krutskikh accused the U.S. of having "unleashed cyber aggression against Russia and its allies." He also warned: "rest assured, Russia will not leave any aggressive actions unanswered." Krutskikh said "over 65,000 'armchair hackers' from the USA, Turkey, Georgia, and EU countries regularly took part in coordinated DDoS attacks on our country's critical information infrastructure, including Rutube video hosting." And "in total, 22 hacker groups are involved in illegal operations against Russia," Krutskikh alleged.*"[1]

1 Source: Newsweek. Russia Warns Growing Cyber Conflict With U.S. Could Spark War in Real World

4. Although the quotes in paragraph 3 are from October 2022, Russia has followed that policy, launching retaliatory cyber attacks against any NATO or EU country that supports Ukraine. Russia has continued to consolidate and organize its 'civilian' cyber forces to do some of this. One of the more visible parts of the re-organization is the creation of the 'civilian' hacker group NoName057(16). Based on its Tactics, techniques and Procedures (TTP) as well as IP addresses and other signatures, NoName was formed from 'KillNet' members. Similar to KillNet, "*NoName057(16) uses a Telegram channel to claim responsibility for disruptions, justify its actions, make threats, and mock targets. [Cyber Security company] SentinelOne says the [hacker] group, "values the recognition their attacks achieve through being referenced online".*"[2] Sentinel One assesses the targets as 'NATO-associated targets' with an objective of silencing anti-Russian activity including speech/viewpoints, news/media, and logistics.

5. Recent acttacks by NoName057(16) include:

- the Polish government in December 2022,
- attacks on Lithuanian organizations (mainly cargo and shipping firms) in January 2023,
- hits on Danish financial institutions,[3] and
- disrupt the 2023 Czech presidential elections, (January 13-14).

6. The hacker group is attempting to recruit and encourage hackers to attack targets by starting a project called "DDosia". Volunteers are encouraged to attack 'anti-Russian targets, earning as much as 80,000 rubles/1,200 USD for a successful attack, usually a Distributed Denial of Service (DDoS) attack.[4] Its estimated that the group has grown to 1,000 members, who have conducted 1,400 DDoS attacks, 190 of which were successful. That is a 13% success rate. The attacks are becoming longer and more technically aggressive. The groups capability is assessed as: *"Their DDoS attacks are basically unsophisticated, do not have large impacts, and do not aim to cause significant damage," ... "They want to draw attention to themselves in the media, similar to the Killnet group. Nonetheless, NoName057(16) activities are still more of a nuisance than dangerous."*[5]

Ukraine: Cyber Defense

7. Ukraine continues its standard operating procedure of saying nothing about its cyber operations. Countries and organizations that are supporting Ukraine are starting to release information about some of their efforts. The Telegraph is reporting that Microsoft president Brad Smith said that his company's support for Ukraine's government amounted to $400m (£333.5m) since the invasion, adding that support during 2023 would be extended "free of charge". Amazon has donated access to its 'cloud' services, another $75m (£63m) worth of services. That allowed Ukraine to move its data to the 'cloud', making it far more difficult for Russia to destroy.[6]

2 Source: Security Week. Pro-Russian Group DDoS-ing Governments, Critical Infrastructure in Ukraine, NATO Countries

3 Source: Hack Read. DDoS Attacks Hit Denmark Central Bank and 7 Private Banks

4 Source: Information Security Buzz. Pro-Russia Hacktivist Group NoName057(16) Strikes Again

5 Source: Tech Monitor. Pro-Russian hacktivist group offers citizens financial rewards to join DDoS attacks

8. Other companies supporting Ukraine include:[7]

- Mandiant (Computer Security company owned by Alphabet/Google),
- Palo Alto Network, Unit 42 (Computer Security Company),
- ESET (Cyber Security company),
- Recorded Future (Cyber Security/Threat Intelligence provider), and
- Cisco (through Talos its cyber security division)[8].

Many other companies are providing support less directly, adding their analysis and cyber security information through information sharing systems. Ukraine receives that information through their use of Recorded Future's 'Threat Intelligence' portal.

9. Some countries have taken note of Russia's increasing cyber capabilities. Sweden's domestic security agency is warning that it expects Russia to increase activities threatening Swedish security. Head of the agency, Charlotte von Essen, said Russia's actions were "*unpredictable,*" but stressed that "*we can expect that Russian security-threatening activities against Sweden will increase.*" She warned organizations to "*be particularly vigilant to counter espionage and sabotage*" of telecommunications, electricity supply and the transport of "*critical material.*" Russia is expected to make use, "*to a greater extent than before, of non-official platforms such as the Russian diaspora, institutions and companies in Sweden.*"[9]

10. Belarus has responded to sanctions against it by legalizing "*internet piracy of digital goods including computer software, movies, and music, if the rights holder resides in "foreign states that commit unfriendly actions against Belarusian legal entities and (or) individuals." The law authorizes the use of foreign media and IP products within Belarus from countries that have sanctioned it without the permission of rights holders. The law states that the government will still collect royalties for the use of that material, but the royalties will be held by the patent authority. If the rights holders don't collect the royalties within three years - unlikely for companies barred by law from doing business in Belarus - the funds will be absorbed by the government budget.*[10]

Shipping Industry Attacked

11. Norway is investigating a ransomware attack on DNV Ship Management Software. On January 7th the company was forced to shut down its servers due to a ransomware attacks. *ShipManager is a fleet management software that allows DNV shipping customers to monitor the operational, technical and compliance features of a shipping fleet, and is used by more than 7,000 vessels owned by 300 customers, according to the company's website. DNV said that 70 customers operating around 1,000 vessels were affected by the attack, close to 15% of its total fleet.*[11] *The Norwegian company*

6 Source: Telegraph. Amazon and Microsoft halve Russian cyber attacks on Ukraine
7 Source: Sub Stack. Security Firms Aiding Ukraine During War Could Be Considered Participants in Conflict
8 Source: Venture Beat. Russia's war in Ukraine: 3 cybersecurity takeaways for enterprises
9 Source: Federal News Network. Sweden sees bigger Russian threat to telecoms, power network
10 Source: Vice.com. Russia Ally Belarus Legalizes Pirating Media From 'Unfriendly' Nations
11 Source: Yahoo News. Maritime giant DNV says 1,000 ships affected by ransomware attack

provides services for 13,175 vessels and mobile offshore units (MOUs) amounting to 265.4 million gross tonnes, which represents a global market share of 21%.[12] DNV says: The attack has been reported to the Norwegian Police, who has informed relevant police agencies. It was also reported to the Norwegian National Security Authority, the Norwegian Data Protection Authority (DPA) and the German Cyber Security Authority. All affected customers have been notified about their responsibility to notify relevant Data Protection Authorities in their countries.[13]

Canada

12. Recent cyber attacks have captured the attention of the Canadian media. The Ontario Liquor Control Board (LCBO) website was hacked, a 'skimmer inserted' and customer data stolen. 'Skimmers' are malware or small computer programs that covertly copy data and send it to their operators.[14] In this case patrons of the LCBO Online store between January 5th and 10th almost certainly had their names, email and mailing addresses, Aeroplan numbers, LCBO.com account password, credit card information, and other identifying information sent to the hackers.[15]

13. As this attack followed hacks on: Empire Company (Sobey's), Maple Leaf Foods, Toronto Sick Kids Hospital – to name a few, Canadian media started to ask questions. Speaking to CTV a cyber security expert said: *"the ransomware industry is growing as a multi-billion dollar global criminal industry. "It's supported by sovereign countries that harbour ransomware attackers, and ransomware attacks have proven to be highly lucrative," ... noting that cyberattacks are also increasing as our reliance on technology does."* Former Deputy Prime Minister John Manley wrote a letter to Prime Minister Justin Trudeau warning the Prime Minister that Canada is not ready for cyber attacks.[16]

Are We Learning our Cyber Security lessons?

14. The short answer is no. Progress in securing our cyber environment is remarkably slow. For example the manufacturing industry was recently given a D+ cyber security grade.[17] One of the reasons that industry is struggling is that the manufacturers of Industrial Control Systems (ICS) – the interfaces between computers and manufacturing machines – have security vulnerabilities and no patches are available.[18] Only the countries that educate their citizens on cyber security, have made progress.

---

12 Source: Security Affairs. 1,000 ships impacted by a ransomware attack on maritime software supplier DNV
13 Source: DNV web site. Cyber-attack on ShipManager servers – update
14 Source: Information Security Buzz. Major Canadian Liquor Distributor's Website Infected With Skimmer
15 Source: IT Business Canada. Hackers compromised Ontario liquor board website, stole customer data
16 Source: CTV News. Cyberattacks are happening more frequently, experts explain why
17 Source: Manufacturing Net. Security Breach: Industry Gets a D+ Cybersecurity Grade
18 Source: Beta News. A third of ICS vulnerabilities have no patch available