# 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 (32) Answering Your Questions

This report contains selected cyber-security information from 27th May to 9th June 2023.

### Synopsis

1. Cloudflare confirms Russia cyber attacks Ukrainian organizations when military attacks are launched. Slovakia receives most recent DDoS attack. Clop and BlackCat ransomware groups show their expertise. Is it the end of KillNet? Ukrainian hackers breach Russia's silicon valley and imitate President Putin. I'll answer some of your questions such as: 'Will I be hacked?' and 'What will *Russian hackers* do next?'

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.

3. **Russia: Cyber Offence**. Internet infrastructure company 'Cloudflare' is reporting that when "*Russia is trying to attack them physically, and then an actor is trying to prevent them from getting access to the sites that provide emergency resources on the digital side, it's a new facet in warfare.*" Cloudflare provides free web security service through an initiative called 'Project Galileo' to "*human rights and public interest organizations around the world. The main aim of Project Galileo is simply to utilize Cloudflare's products and scale for organizations that might not otherwise have any web defenses at all.*" Cloudflare protects 81 Ukrainian organizations.[1] Analysts Comments: This report matches reporting from Ukraine's Computer Emergency Response Team (CERT-UA) which has reported increased cyber attacks during Russian military attacks.

4. During the reporting period Russia launched what appeared to be a harassing cyber attack against Slovakia while Russian-allied criminal groups effected some major hacks. On May 31st while an international Global Security conference was being held in Bratislava, Slovakia, "*a massive DDoS cyber-attack disabled city hall's website in the early morning. Bratislava Mayor Matus Vallo said that no data was breached.*"[2]

1 Source: Wired. Hacks Against Ukraine's Emergency Response Services Rise During Bombings
2 Source: Euractiv. Bratislava faced massive cyber-attack during GLOBSEC conference

5. Two Russia related criminal hacker groups scored huge hacks. The Clop ransomware gang breached the 'MoveIt's' file transfer system affecting organization from the Province of Nova Scotia[3] to: 'BBC', 'British Airways', 'Aer Lingus' and 'Boots'. "*In an email to Reuters, the hackers said "it was our attack" and that victims who refused to pay a ransom would be named and shamed on the group's website."*[4] Analysts Comments: Numerous security firms are warning that many companies may not be aware that they are at risk. Essentially ANY company who is using the MoveIt software needs to patch or remove the software immediately. Previously the group has waited as long as a month before notifying victims they have been breached. This tactic ensures they have good material to blackmail the victim payment.

6. The Tech Times writes: *"The Clop ransomware group, active under the ransomware-as-a-service (RaaS) model for more than four years, primarily targets businesses with yearly revenue of $5 million or more in the United States, Canada, Latin America, Asia Pacific, and Europe, according to the Blackberry Blog. ... Mandiant wrote in a weekend blog post that there are "notable" similarities between UNC4857, a recently formed threat cluster with "unknown motivations," and FIN11, a notorious ransomware group that operates Clop ransomware."*[5]

7. In a second hack with huge implications, the BlackCat Ransomware group has hacked the 'Casepoint' legal technology platform used by US Agencies and law firms. "*Casepoint provides a leading legal discovery platform used by several US agencies, including the SEC, FBI, and US Courts."* According to BlackCat: *"We have over 2TB of very sensitive data, lawyers, SEC, DoD, FBI, Police and more. We encourage you to get in touch or we'll start posting your data on our blog soon. We mailed you the login link."* The report in Security Affairs continues: *"it is reasonable to speculate that the ransomware group might have compromised sensitive and possibly classified information."*[6]

8. BlackCat typically creates "*a victim-specific threat that takes into account elements such as encryption performance, perhaps electing to only encrypt parts of large files, as well as embedded victim credentials to allow automated propagation of the ransomware payload to other servers."*[7] BlackCat attacks typically start "*with stolen user credentials or exploiting known Microsoft Exchange vulnerabilities. ... Once they have access, they compromise user and administrator accounts. ... In addition,* ***triple extortion*** *is being used in which, in addition to the common practice of stealing sensitive data before encrypting the victim's files and threatening its public release (double extortion), the ransomware group also threatens to launch a distributed denial-of-service (DDoS) attack if their demands are not met."*[8]

3 Source: CTV News. Nova Scotians' personal information stolen in global security breach: province
4 Source: Sky News (UK). BA, BBC and Boots hit by cyber security breach with contact and bank details exposed
5 Source: Tech Times. Cybersecurity Experts Confirm Clop Ransomware Gang Mass Attack on MOVEit Transfer Service
6 Sources: Security Affairs. BlackCat claims the hack of the Casepoint legal technology platform used by US agencies
7 Sources: Varonic. BlackCat Ransomware (ALPHV)

9. **KillNet**: On June 5th a group member said he was resigning from KillNet activities. A KillNet administrator said "*I do not intend to single out the rest, no one deserves an acclaim and a comment. Killnet has been completely disbanded,*" on KillNet's Telegram channel. KillMilk apparently told other followers that they could 'unsubscribe'.[9]

10. KillNet is a group of both Russian and pro-Russia hackers, who are volunteering their skills to Russia. In general terms KillNet has "*Emerged as one of the most active and ambitious pro-Kremlin hacktivist collectives*"... "*Killnet" is a financially and ideologically-motivated threat group" of mostly Russians. KillNet is noted for its "distributed denial-of-service (DDoS) and data exfiltration attacks against Western entities and Dark Web markets. ... The group constantly seeks new avenues for expansion, evolving their tactics, and capturing attention using what they proclaim as their "army of cyber partisans" and the pro-Kremlin media eager to deliver storylines that align with the narrative of the Russian government."*[10] .

11. In an interview with the Russian news site Lenta, Killmilk [self-proclaimed leader of KillNet] *claimed that the collective consists of "roughly 4,500 people" organized into various subgroups. While these subgroups operate independently, they occasionally coordinate their activities. Killnet has also claimed to have 280 members in the US, attributing an attack on Boeing to their US "colleagues." On forums such as XSS and Breach Forums, users referred to Killnet as "a group of 10th-grade schoolkids" and "a script kiddie Russian group," respectively.* Analysts Comment: Some sub-elements of KillNet are proficient while others have only basic or marginal skills. "*Although no direct operational connection between Killnet and Russian state structures has been proven, their goals align with those of the Russian government. Killnet has sought support from the Russian parliament, the State Duma, and potential links between the Kremlin and Russian cyber threat groups targeting Ukraine have been identified."*[11]

12. Analysts Comment: IF KillNet does disband [or if they leadership team has disbanded] there will be no significant change from the western perspective. Russia remains a sanctuary to dozens, perhaps hundreds of hacker groups – although their effective numerical strength is probably 20% of membership. To quote Cyber News: "*Even if Killnet disbanded, plenty of similar pro-Russian groups still perform Telegram-coordinated DDoS attacks, such as NoName, Xaknet, Legion, and others.*" More significantly, cyber command and control organization remains in place.

13. **Russia: Cyber Defence**. On May 31st 'the Record' reported "*Ukrainian hackers have breached the systems of Skolkovo Foundation, the agency which oversees the high-tech business area located on the outskirts of Moscow.*" A group of Ukrainian hacktivists took credit for the attack saying to the foundation: "*Your infrastructure has been destroyed. We have all the documents and the project source codes. Stay tuned.*" According to a Russian source, critical user data remained secure however "*the hackers were able to access presentations, photos, contracts, and lists of partners and counterparties of legal entities.*"[12] Analysts Comment: Breaching Russia's 'silicon valley'

8 Source: SOCRadar. Dark Web Profile: BlackCat (ALPHV)
9 Sources: Security Boulevard. Killnet hacktivists say they're disbanding
10 Sources: Security Boulevard. Killnet: Inside the World's Most Prominent Pro-Kremlin Hacktivist Collective
11 Sources: Security Boulevard. Killnet: Inside the World's Most Prominent Pro-Kremlin Hacktivist Collective

is a significant embarrassment for Russia however it is unlikely to have other consequences.

14. On June 5th "*the voice and likeness of Vladimir Putin appeared on radio and television stations in three regions along Russia's border with Ukraine* ... telling people *Ukraine had invaded Russian territory. He declared martial law, promised a general mobilization of the country, and urged residents to evacuate deep into Russia. ... Putin's press secretary, confirmed that the message was the result of a hack.* ." Vice news speculates that the hack "*coincided with what appears to be the beginning of Ukraine's long-awaited counteroffensive against Russia*."[13]

15. Apparently Russian officials were told recently to ditch their iPhones due to: "*data security concerns. The Russian security service FSB claims that Apple has assisted US intelligence agencies, specifically the NSA, with a spying campaign targeting thousands of iOS devices belonging to local users and foreign diplomatic missions in NATO countries, China and Israel.*[14]

**Your Questions**

16. The questions I get asked the most are: 'Will I be hacked?' And 'What are *they* going to do next?'. Asked less often are questions such as 'Who are they?' and 'How do they do this?'

17. '**Will you get hacked?**' depends on who you are and where you work. If you work in government [any level], medical / hospitals, education and media, your world is regularly scanned for vulnerabilities. Those industries are consistently at the top of the Russian 'highly desirable' hack list, possibly because they are all high visibility and possibly high impact to people affected. It is my *assessment* that Russia/Putin are attempting to send a '*see what we can do and fear us'* message. Running a close second on the list of preferred targets are energy producers. I include the entire energy spectrum from Oil and Gas producers to Solar, Wind and Electrical Grid operators. Turning off the lights is something Russia has done in previous cyber campaigns. It CAN NOT be ruled out.

18. After those top tier 'targets' remember that Russia shelters dozens of competent criminal hackers who intend to make money off the 'rich and stupid people'[15] they hack. The 'hacker' industry has developed to the point where some groups have a 'corporate organization'. Other groups have specialized functions. For example there are some hacker groups that specialize in compromising login credentials and/or breaking into networks. These hackers make money by selling those login credentials to other criminal hackers and/or the Russian government. There are millions of stolen login credentials for sale on the 'Dark Web' waiting for someone to purchase them.

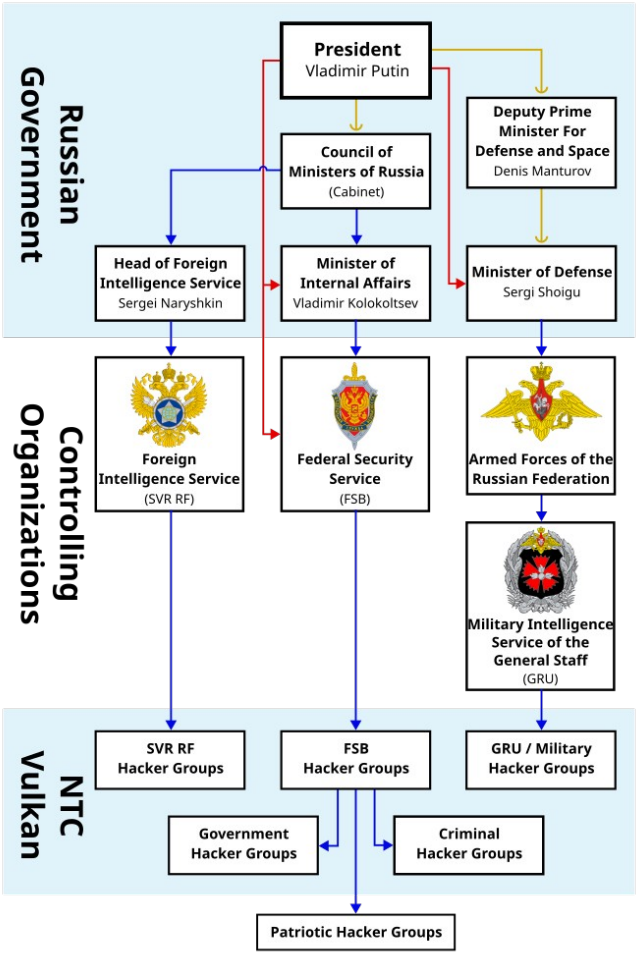
19. Who gets attacked next depends on many factors. For example, when a Canadian politician gives a pro-Ukraine speech, especially if that speech is international news, a

12 Source: The Record. Russia's 'Silicon Valley' hit by cyberattack; Ukrainian group claims deep access
13 Source: Vice News. Russia Says 'Fake' Putin Address Declaring Martial Law Was a 'Hack'
14 Source: Security Week. Apple Denies Helping US Government Hack Russian iPhones
15 Source: 60 Minutes Australia. From a statement made by a hacker to an Australian correspondent.

# Cyber-Intelligence Report

Russian politician may decide that Canada needs to show more respect to Russia. A suggestion is made to Russia's patriotic hackers and one or more hacker groups would begin looking for Canadian targets to hack – starting with those stolen login credentials.

20. Although paragraph 19 sounds somewhat ... speculative ... it is not. If you refer to the organization chart, there is no one at the government / political level with more than casual user level knowledge of how to use computers. President Putin himself is reputed to not have any significant computer skills. He has been accused of not knowing how to use the Internet. This also means the people giving the orders do not fully understand the implications and effects those cyber attacks will have.




21. At the Controling organization level 'information operations' are a standard Russian tool. There is no evidence of planning for cyberwarfare being used in long-term warfare.

22. NTC Vulkan is a Russian consultancy that: advises, writes software (including malware), and has been accused of collecting compromised logins.

23. How are hackers assigned tasks? The blue lines at right reflect 'normal' or convential chains of command. I was reminded by a senior analyst that: "*Russia operates by cronyism; those with the ability to gain the ear of the Emperor, I mean Putin. In this regard I believe it affects the selection of targets by Russian cyber-operators.*"[16] The red lines reflect Putin's direct contact and control over those individuals and organizations. I expect a lot of direction is given

16 Source: Maj J McLearn CD Ret'd. Email dated 5 June 2023.

directly (via the red lines). The bottom line is that there is no plan so one, not even senior Russians, know what is going to happen next.

24. **Who Are the Hackers?**

- Each of the three services has its own uniformed hackers. The Foreign Intelligence Service (SVR RF), the Federal Security Service (FSB) and Military Intelligence (GRU) all have university graduates who are commissioned officers who work on one of more of the six to eight teams that each service has.
- The FSB also has criminal and mercenary hackers who work for remediation. There is a mix of 'full-time' criminals and those who do their hacking after work, as they have time. Conservatively, there are more than a dozen hacker gangs.
- Last but far from least, KillNet was the coordinating organization for the 'Patriotic Hackers' supporting Russia. There are *probably* fewer that a thousand active hackers. Its *highly likely* that fewer than one hundred and fifty have serious skills. What makes the criminal and patriotic hackers particularly problematic are their links to groups outside Russia. Hackers outside Russia can make sttributing hacks more difficult.

25. As for How Russian hackers can do what they are doing, the short answer is we (western countries including the United States and Canada) gave them the tools to learn how. We taught Russian, Chinese and Iranian students in our universities. We allowed Microsoft to sell 'source code', the heartbeat behind Microsoft Windows software, to Russia. Western countries continue to sell a large amount of technology to authoritarian regimes. NTC Vulkan continues to place its software engineers in companies across Europe, collecting even more technology, adding to Russia's tools.

26. **Summary**.

- Will I be hacked? It is becoming increasingly likely.
- What will Russia do next? There is no way to tell as the Russian's are 'off their plan's. Worse, the politicians in charge don't understand the weapons they control.
- Who are they (*the Russian hackers*)? A wide range of people from university trained professions to criminals and amateurs.
- How do they do this? We taught them.
- Why us? Russian criminal hackers see us as 'fat and stupid'. Robbing or extorting money from us is of 'no consequence'.

The only thing we know for sure is that the Russian cyber attacks are continuing to get worse.

---