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 (28) Russian Cyber Units

This report contains selected cyber-security information from 24th February 2022 to 14th April 2023.

Synopsis

1. This report describes Russia Cyber Forces. This includes 'government' forces, commercial companies that support the government, criminal hackers (in it for the money) and 'patriotic hackers', volunteers who want to support Russia.

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.**

The Vulcan Files

3. An employee of Russian IT Consultancy Company NTC Vulkan, disgusted by the war, released a trove of documents to German newspaper 'Süddeutsche Zeitung' shortly after the invasion of Ukraine. A consortium of eleven news organizations including 'Paper Trail Media' (Germany) and 'Der Spiegel' (Germany), 'Washington Post' (United States), The Guardian (UK), Le Monde (France), collaborated to analyze the documents. There are 1,000 secret documents that include 5,299 pages full of project plans, instructions and internal emails from Vulkan from the years 2016 to 2021. Despite being in Russian and extremely technical in nature, they provide unique insight into the depths of Russian cyberwarfare plans. Five Western intelligence agencies confirmed the authenticity of the documents.[1] These files are known collectively as 'the Vulkan Files' and provide the basis for the identification of Russia's cyber units.

Russian Cyber Order of Battle (ORBAT)

4. **Government Forces**. According to 'The Washington Post' "*Moscow's cyberwarriors are not a disparate collection of hackers launching ransomware for quick scores. Instead, they are part of a robust, state-sponsored effort using the full power of the Russian security state and private companies to identify critical targets and enemies'*

1 Source: SPIEGEL International. A Look Inside Putin's Secret Plans for Cyber-Warfare

vulnerabilities."[2] *"The Russian government regards offensive cyber capabilities as part of a holistic effort to degrade its enemies. This includes the sowing of mistrust via social media, the gathering of kompromat (compromising material), and the ability to target crucial infrastructure. That list of enemies is a long one."*[3] *"Countries on the "unfriendly countries" list include New Zealand, Australia, EU states, the UK, US, Canada, Ukraine, Singapore, Japan and Taiwan"*[4] (and NATO).

6. The cyber forces of the Russian Federation are operated by the Intelligence Agencies of Russia. Their crest is shown at right. The cyber forces include:

- Government teams, military and/or intelligence services,
- Commercial Consultants/Hackers,
- Criminal Hackers, and/or
- 'Patriotic' Hackers.

7. Military Intelligence Service of the General Staff of the Armed Forces of the Russian Federation (**GRU**). Government personnel personnel are university graduates, software developers, computer scientists etc, who are officers in their organizations.


Emblem of GRU

Also known as the 'Main Intelligence Directorate', the GRU is *very probably* the operator of the following hacking units: 'Sandworm'[5], 'Fancy Bear'[6], 'GhostWriter'[7], 'XakNet'[8], 'Infoccentr' and the 'Cyber Army of Russia_reborn.' According to a U.S. report to Congress 'Unit 54777'[9] is a GRU psychological operations team that uses cyber attacks.

The GRU cyber teams target: Infrastructure in Ukraine, including both physical infrastructure such as energy and telecommunications, as well as functional government infrastructure like Ukrainian tax software. External governments, organizations and individuals are also targeted. Analysts Comment: Target sets are not fixed. Additional targets are routinely added which may require additional malware, tactics, techniques and procedures.

8. Foreign Intelligence Service of the Russian Federation (**SVR RF**)


Emblem of SVR RF

Hacking units of the SVR RF include: 'NOBELIUM', also known as Cozy Bear, The Dukes and APT29[10]. This 'unit' *may* be multiple teams that are reconfigured in accordance with their tasks.

SVR RF hacking teams most often use information collection (espionage) malware as well as conduct disinformation operations. Espionage targets include: diplomats, embassy's, military (including supply chains), research

2 Source: The Washington Post. 7 takeaways from the Vulkan Files investigation
3 Source: The Conversation. Russia's shadow war: Vulkan files leak show how Putin's regime weaponises cyberspace
4 Source: 1News New Zealand. New Zealand joined Russia's "unfriendly countries"
5 Source: Cyber Intelligence Report. My 230202
6 Source: Cyber Intelligence Report. My 230106
7 Source: Cyber Intelligence Report. My 230106
8 Source. Cyber Intelligence Report. My 221028
9 Source: Congressional Research Service. Russian Cyber Units
10 Source: Cyber Intelligence Report. My 230331

facilities, key industries, among many others. Cyber Espionage attacks often work at remaining covert over long time periods.

9. The Federal Security Service of the Russian Federation (**FSB**)

Emblem of FSB

The FSB also includes the 18th Center for Information Security, which oversees domestic operations and security but conducts foreign operations as well. The FSB is responsible for monitoring domestic hackers meaning hackers within Russia and allied countries.[11] Similar to the SVR RF hacking organization, the FSB hacking unit appears to re-configure according to assigned tasks. Hacking groups associated with the FSB include: 'BeserkBear'[12], 'Gamaredon'[13], and 'Nodaria'[14] TA 569 also known as the Vovan & Lexus disinformation team[15] are *very probably* linked to the FSB.

The target set for the FSB is very broad ranging from information collection on individuals (within Russian, in Ukraine and sometimes external targets) to targeting the energy sector in the U.S. There are documented 'close connections' between the FSB and criminal hackers who *may* be used to augment operations. This suggests that 'patriotic hacker groups such as KillNet *may* take their orders from the FSB.

10. **Commercial Companies**. The Russian government has approximately forty principal consultants and contractors that support its military.

11. **NTC Vulkan**: *NTC Vulkan was founded in 2010 by Anton Markov and Alexander Irzhavsky, graduates of St Petersburg military academy and service in the Russian Army. NTC Vulkan, presents itself as a completely normal, IT consulting firm, a small company with software expertise. The company claims "Information security management" as one of its specialities.*

Vulkan works for intelligence agencies: for the military intelligence agency GRU, the domestic intelligence agency FSB and for the foreign and economic intelligence agency SVR.[16]One of the NTC Vulkan goals is to develop highly effective cyberweapons. The table (right) describes three ongoing programs developed by Vulkan. Vulkan's engineers have: developed

Tool	Description	Contract Dates
Scan	A comprehensive framework likely used to enable cyber operations. Scan consists of a variety of methods for large-scale data collection and contains comprehensive documentation on how to structure databases to store and handle such information. Based on the signatories, Scan documentation was contracted (at least in part) by GRU Unit 7445, or Sandworm Team.	~2018-2019
Amesit (Alt: Amezit)	A framework used to control the online information environment and manipulate public opinion, enhance psychological operations, and store and organize data for upstream communication of efforts. Information confrontation and psychological operations in Amesit are designed to support IO and OT-related operations.	2016-2018
Krystal-2B	A training platform for exercising coordinated IO/OT attacks against transportation and utility industries using Amesit. The exercise's program highlights particular scenarios against OT environments and Russian infrastructure. Krystal-2B may be a red teaming or defensively focused exercise, but demonstrates interest in coordinating IO/OT attacks.	2018-2020

11 Source: Congressional Research Service. Russian Cyber Units
12 Source: SPIEGEL International. A Look Inside Putin's Secret Plans for Cyber-Warfare
13 Source: Cyber Intelligence Report. My 230202
14 Source. Cyber Intelligence Report. My 230216
15 Source: Cyber Intelligence Report. My 230317
16 Source: SPIEGEL International. A Look Inside Putin's Secret Plans for Cyber-Warfare

hacking operations, worked for Russian military and intelligence agencies, trained and support operatives before attacks on national infrastructure, assisted in spreading disinformation and controlling sections of the internet. In addition Vulkan collects vulnerabilities and compromised access, enabling cyber attacks.[17] Vulkan apparently has 60 software developers plus support staff and sub-contractors.

12. Another company supporting Russian cyber operations is the "**Internet Research Agency**". *It is a private organization, funded by Kremlin-connected oligarch Yevgeniy Prighozin, which has supported Russian government disinformation and propaganda operations. Often referred to as a troll farm or troll factory, this group has focused on disinformation by impersonating domestic activists and people, primarily through various social media channels*.[18]

13. There are two other types of hackers that support Russia. Criminal Hacker Groups are typically 'ransomware groups'. Ransomware or not, the groups are in business to make money. The second group is volunteer hackers who Russia calls 'patriotic hackers'.

14. **Criminal Hacker Groups**. Prior to the invasion, the Conti Ransomware Gang was known as one of the most prolithic and successful ransomware organizations globally. It is a young group, first noticed in 2020. Based in Russia, it featured an almost corporate organization as well as its own encryption protocols and malware. Conti was the first Ransomware group to declare its support for Russia. Conti appears to have reorganized into smaller teams. It is possible that Conti is working with the FSB and Vulkan, sub-dividing in order to attack more targets. Conti's new organization is reported to have two types of groups: Fully autonomous groups which focus on stealing data, like Karakurt, BlackBasta, and BlackByte. The other groups are semi-autonomous, which acts as Conti-loyal affiliates within other collectives. This includes AlphV/BlackCat, Hive, HelloKitty/FiveHands, and AvosLocker.[19]

15. **'Patriotic Hackers'**. Recruiting of hackers to support Russia was started by the Cuba Ransomware Group[20] and continued by 'KillNet'. Recruited sub-groups include: NoName 057(16), Zarya, Phoenix, Vera, FasoninnGung, Mirai, Jacky, DDoS Gung, Sakurajima, and Sparta. KillNet and its allied groups are best known for Distributed Denial of Service (DDoS) attacks against countries that actively support Ukraine. Russia offers a bounty to these groups if they can prove they disabled a 'target' web site.[21]

---

17 Source: Security Affairs. Leaked documents from Russian firm NTC Vulkan show Sandworm cyberwarfare arsenal
18 Source: Congressional Research Service. Russian Cyber Units
19 Source: Cyber Intelligence Report. My 221118
20 Source: Cyber Intelligence Report. My 221028
21 Source: Cyber Intelligence Report: My 230120