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 (29) Russia's GRU Hackers

This report contains selected cyber-security information from 14th to 28th April 2023.

Synopsis

1. UK's National Cyber Security Centre is warning: Russia's Military Intelligence is indiscriminately and recklessly launching cyber attacks against the west, and that Russia's 'patriotic hackers' want to attack western critical infrastructure. Russia's cyber focus remains on Ukraine. How effective are cyber attacks on Russia? A look at some of Ukraine's volunteer hackers. Hauwei's critical components.

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.**

Russia

3. The UK's National Cyber Security Centre (NCSC) is warning that the GRU, the Russian military intelligence service is conducting "*indiscriminate and reckless cyber attacks.*" The warning says: "*a number of cyber actors widely known to have been conducting cyber attacks around the world are, in fact, the GRU. These attacks have been conducted in flagrant violation of international law, have affected citizens in a large number of countries, including Russia, and have cost national economies millions of pounds.*"[1]

4. UK Foreign Secretary, Jeremy Hunt said: *"These cyber attacks serve no legitimate national security interest, instead impacting the ability of people around the world to go about their daily lives free from interference, and even their ability to enjoy sport. … The GRU's actions are reckless and indiscriminate: they try to undermine and interfere in elections in other countries; they are even prepared to damage Russian companies and Russian citizens. This pattern of behaviour demonstrates their desire to operate without regard to international law or established norms and to do so with a feeling of impunity and without consequences."*[2]

[1] Source: UK National Cyber Security Centre. Reckless campaign of cyber attacks by Russian military intelligence service exposed

5. The NCSC *assesses* that the following hacker groups are *almost certainly (90 to 100% confidence)* GRU hacking teams:[3]

Emblem of the GRU

- APT28
- Fancy Bear
- Sofacy
- Pawnstorm
- Sednit
- CyberCaliphate
- Cyber Berkut
- Voodoo Bear
- BlackEnergy Actors
- STRONTIUM
- Tsar Team
- Sandworm

6. In a different warning, the NCSC says “*Russian hacktivists have ambitions of becoming a larger threat to Western critical infrastructure by advancing their attacks past distributed denial of service and disinformation.*“ The warning states: “*Groups could launch 'destructive and disruptive attacks' with less predictable consequences than those of traditional cyber criminals.*”[4] Analysts Comment: Given the ego-centric nature of ‘hackers’ in general, the NCSC warning is appropriate. It is *highly likely* that Russia’s ‘patriotic hackers’ want to see themselves as important players.

7. On April 15th or 16th Arseni Yeliseyeu alias “Raty”, an eighteen-year-old Belarusian citizen who was head of Anonymous Russia,was arrested by the Belarusian police because a Belarusian (Anti-Russian) operative was identified in his group. Anonymous Russia conducted distributed denial of service (DDoS) attacks against Ukraine, and later joined several Killnet campaigns. The group is considered ‘integrated’ with Killnet’s command structure. Killmilk, the Killnet founder, announced “Radis”would be the new head of Anonymous Russia. Several KillNet associate groups called for “Raty’s” release and moved to form their own, separate, groups.[5]

8. Google’s Threat Analysis Group or TAG reports that Russia’s cyber focus in 2023 remains on Ukraine. They report: “*In the first quarter of 2023, Russian government-backed phishing campaigns targeted users in Ukraine the most, with the country accounting for over 60% of observed Russian targeting.*” The GRU’s ‘Sandworm’ group is the most “*versatile GRU cyber actor with offensive capabilities including credential phishing, mobile activity, malware, external exploitation of services, and beyond. They target sectors of interest for Russian intelligence collection including government, defense, energy, transportation/logistics, education and humanitarian organizations.*”[6]

9. TAG’s observation is not a complete picture of Russian cyber activity. The UK’s National Cyber Security Centre (NCSC) warned of extensive GRU (Russian Military Intelligence hackers) activity against western critical infrastructure. This is in addition to numerous other cyber campaigns as well as an ongoing cyber espionage campaign targeting foreign ministries and diplomatic entities located in NATO member states, the

[2] Source: UK National Cyber Security Centre. Reckless campaign of cyber attacks by Russian military intelligence service exposed

[3] Source: UK National Cyber Security Centre. Reckless campaign of cyber attacks by Russian military intelligence service exposed

[4] Source: UK National Cyber Security Centre. NCSC warns of emerging threat to critical national infrastructure

[5] Source: Flashpoint. Killnet Ostracizes Leader of Anonymous Russia, Adding New Chapter to Pro-Kremlin Hacktivist Drama

[6] Source: Google Threat Analysis Group. Ukraine remains Russia’s biggest cyber focus in 2023

European Union, and Africa. According to Poland's Military Counterintelligence Service and the CERT Polska team, the observed activity maps with the activity tracked by Microsoft as Nobelium. This group is known for its high-profile attack on SolarWinds in 2020. Nobelium's operations are attributed to Russia's Foreign Intelligence Service (SVR). Polish Counterintelligence believe the campaign represents both an evolution in and a re-tooling of Nobeliums tactics.[7]

10. Current Russian cyber campaigns include:

- ‘Decoy Dog’: Scans enterprise networks for vulnerabilities,[8]
- Cisco Routers: ATP28 is scanning for unpatched Cisco routers which will permit attacks on network infrastructure,[9]
- ‘Silence’ / ‘Truebot’: Cybersecurity company Huntress, found about 1,800 publicly exposed PaperCut servers subject to ransomware deployment,[10]
- ‘Black Basta’: Attacked and released information from Canadian Yellow Pages,[11]
- ‘KillNet’: Used a Distributed Denial of Service attack to block and force off-line the web site of Europe’s air-traffic agency.[12]

Ukraine

11. The Moscow Times reported that “The number of data breaches in Russia surged last year and is on course to increase further in 2023. ... According to Group-IB, 1.4 billion pieces of data such as names, phones, addresses and birthdays appeared online in 2022. That marks a 42-fold increase from the 33 million pieces of data leaked the previous year.” The report noted that the “*vast majority*” of the leaks appeared online for free. Valery Baulin, the head of Group-IB’s digital forensics lab, said “*This means that the cyber-criminals’ motive wasn’t to make money but to cause reputational or economic damage to Russian businesses and their customers.*” The most attacked sectors of Russia’s business were retail, industrial, transportation and energy.[13]

12. The BBC published an interview with some of Ukraine’s most prominent hackers.[14] Oleksandr is a member of the IT Army of Ukraine, a volunteer hacking network. He and his team forced Russia’s barcode based product authentication system, certifying food quality, off-line using a a targeted DDoS (Distributed Denial-of-Service) attack. Around the first anniversary of the invasion, Oleksandr joined a team of hackers, called ‘One Fist’, to hijack Russian radio stations and broadcast the sound of fake air raid sirens and an alert message telling citizens to take shelter. "*We feel ourselves like military,*" says

[7] Source: The Hacker News. Russia-Linked Hackers Launches Espionage Attacks on Foreign Diplomatic Entities

[8] Source: Beta News. Decoy Dog sniffs out enterprise networks to target

[9] Source: Security Week. US, UK: Russia Exploiting Old Vulnerability to Hack Cisco Routers

[10] Source: The Hacker News. Russian Hackers Suspected in Ongoing Exploitation of Unpatched PaperCut Servers

[11] Source: Mobile Syrup. Canadian directory publisher Yellow Pages hit by cyber attack

[12] Source: QZ. Pro-Russian hackers have attacked Europe's air-traffic agency

[13] Source: Moscow Times. Russia’s Data Breaches Increase 42-Fold in 2022 – Report

[14] Source: BBC News. Meet the hacker armies on Ukraine's cyber front line

Oleksandr. "*When my country calls me to pick up a rifle I am ready, but hacking Russia now, I feel that I am helpful.*"[15]

13. Unofficial links are emerging on the Ukrainian side between vigilante groups and military officials. Another Ukrainian hacker, Roman is the co-founder of a volunteer group called ‘IT Stand for Ukraine’. He has officially been recruited by his country's cyber military. Roman confirms his hacking team worked directly with Ukrainian authorities before he was recruited. "*We started to communicate with state forces doing the same as us and we began kind of synchronizing our operations. They basically started to give us some targets and say what to do, when to do,*"[16] he says. Part of his military job is finding ways to comb through piles of data and leaked information from the cyber war.

14. Ukrainian hacks are being organized to cause as much disruption as possible to the Russian people. A co-ordinators of the IT Army of Ukraine was asked whether his group could be "gamifying" criminal hacking - and whether this created a danger of escalation. "*Talking from the standpoint of Western laws, I think, yes, there is a danger of gamification of illegal hacking. But what we need to realise is that when war is coming to your country, there are no good ways or bad ways to fight.*"[17]

15. Analysts Comment: A recent report from the ‘European Cyber Conflict Research Initiative’ prov ided a secondary source and confirmation for for the BBC report.[18] Typically academic reports remove first person data making them unusable as sources. In this case the academic report reflected the attitudes and general details of the BBC report allowing me to use a single source, the BBC report.

Huawei

16. Like Canada, Germany has been slow to criticize or ban telecommunication components from Chinese firms Huawei and ZTE. Following a probe by multiple German ministries, the German Interior Ministry is auditing components made by Chinese suppliers that are used by national telecommunications network operators. There is speculation that the government will order “*rip and replace*” the risky component, an energy management component from Huawei, because the component “*could be used to disrupt telecoms operations and or to bring down a network.”*[19]

---

[15] Source: BBC News. Meet the hacker armies on Ukraine's cyber front line

[16] Source: BBC News. Meet the hacker armies on Ukraine's cyber front line

[17] Source: BBC News. Meet the hacker armies on Ukraine's cyber front line

[18] Source: European Cyber Conflict Research Initiative. The Cyber Dimensions of the Russia-Ukraine War

[19] Source: Security Affairs. A component in Huawei network appliances could be used to take down Germany’s telecoms networks