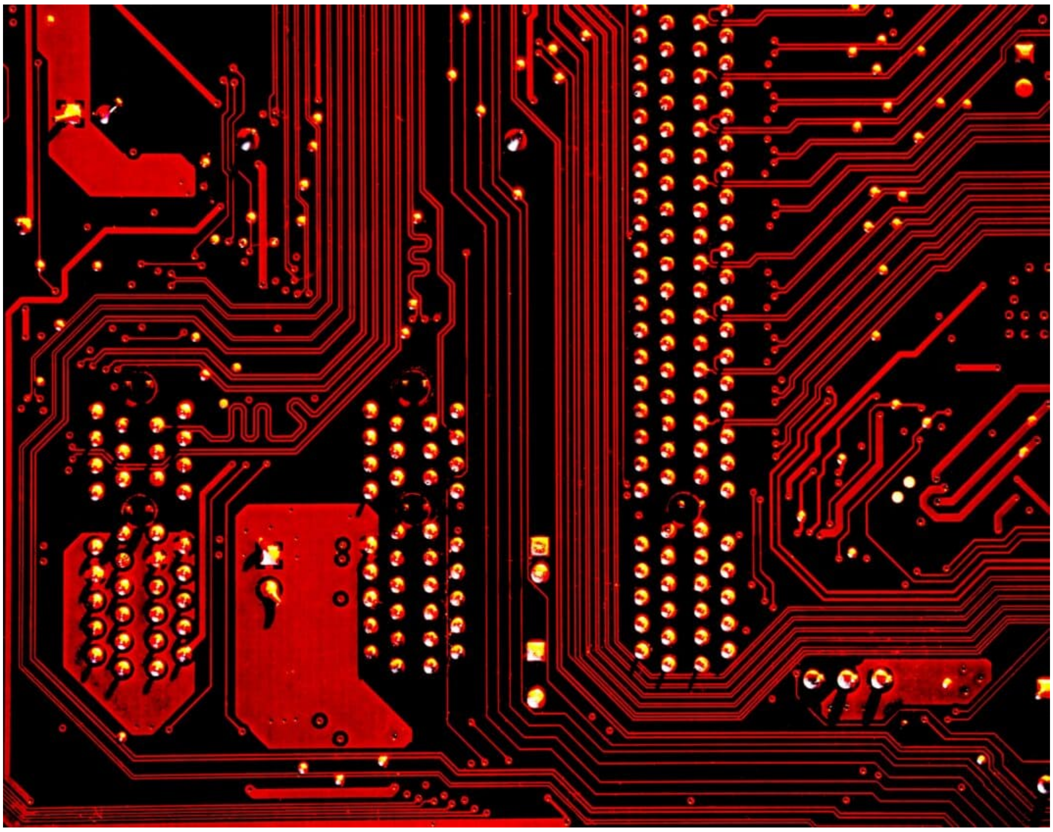
The Five Bears: Russia’s Offensive Cyber Capabilities

: 5/12/2023



1.0. Why?

The Five Bears constitute an integral part of Russia’s offensive capabilities. Russian state-sponsored Advanced Persistent Threat (APT) groups are part of a network, making Russia one of the strongest actors in cyberspace today [source]. A combination of advanced tools and solid infrastructures enable sophisticated operations of unprecedented levels targeting nations in war and peacetime.

However, even though at the forefront of war-fighting capabilities in the digital environment, the 2022 war in Ukraine suggests a limited significance of offensive cyber operations than estimated. Cyber operations alone have yet to prove sufficient to gain strategic advantages on the physical battlefield. Still, since the digital environment does not know state borders, the Russian APT actors make up an evolving threat on a global scale not only in terms of espionage but physical disturbance calling for proportionate counter- and preventive measures among nations in both peacetime and war.

2.0. Background

Since at least the 1990s, Russia has engaged in a wide range of hostile cyber operations, from espionage to sabotage. Since at least 1996, starting with the Moonlight Maze attacks [source], malicious cyber operations linked to Russia have developed into a complex network of threat actors and operations. Today, Russian state-sponsored threat actors constitute a broad network of skilful groups conducting operations ranging from espionage to sabotage on a global scale. Furthermore, offensive cyber operations are acceptable to achieve foreign policy and security objectives by deterring adversaries, controlling escalation and prosecuting conflicts [source]. Hence, Russia’s offensive cyber capabilities make up a crucial element in its global power strategy.

2.1. Disclaimer

Attribution is a very complex issue. Groups often change their toolsets or exchange them with other groups. Therefore, be aware that information published here may quickly need to be updated or altered based on evolving information. Moreover, cyber security companies and antivirus vendors use different names for the same threat actors and often refer to the reports and group names of each other. However, it is difficult to keep track of the different terms and naming schemes, but below are additional lists of known alternative names for each group.

2.2. Terminology

APT: “An APT uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences” [source].

Phishing: Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers [source].

Spear-phishing: Spear phishing is an email or electronic communications scam targeting a specific individual, organisation or business [source].

Zero-day: A zero-day vulnerability is an unknown exploit that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realises something is wrong [source].

Supply chain: A digital supply chain is a set of processes that use advanced technologies and better insights into the functions of each stakeholder along the chain to let each participant make better decisions about the sources of materials they need, the demand for their products and all the relationship in between [source].

Trojan: A malicious program that is downloaded and installed on a computer that appears harmless [source].

3.0. The Russian APT Ecosystem

Russian state-sponsored APT actors use sophisticated cyber capabilities to target adversaries’ critical infrastructure in the global arena. Hostile actors have showed sophisticated tradecraft and cyber capabilities, maintaining a persistent and undetected presence in compromised environments [source]. Conducting malicious cyber activities ranging from cyber espionage attempts to suppress political and social media activity, information theft, and harming international adversaries, the Russian government is utilising its APT network to exercise power [source].

3.1. Prominent threat actors

3.1.1. Fancy Bear

Most known for its attempts to interfere with the 2016 US presidential election, Fancy Bear is a well-resourced and persistent adversary linked to Russia’s Main Intelligence Directorate (GRU) Main Special Service Center (GTsSS) Unit 26165 [source; source]. The group has been attributed to hostile operations in Europe and the US, with an increasing focus towards targets in the east, including China [source]. Fancy Bear has been active since at least 2004 [source].

Other names:

- Sofacy
- APT28
- Sednit
- Pawn Storm
- Group 74
- Tsar Team
- Strontium
- Swallowtail
- SIG40
- Grizzly Steppe
- TG-4127
- SNAKEMACKEREL

[source].

A FBI-issued Wanted List of Russian military intelligence officers linked to the GRU. Source: Federal Bureau of Investigation

3.1.2. Cozy Bear

Like Fancy Bear, Cozy Bear is a well-resourced, highly dedicated, and organised group with links to the Foreign Intelligence Service of the Russian Federation (SVR) [source]. The group mainly conducts cyber espionage, collecting intelligence worldwide to support Russian security policy objectives. Its links to the Russian government date back until at least 2008 [source]. A distinguishing feature of Cozy Bear's modus operandi is the persistence and focus on establishing access to specific targets' networks, even after losing operational control [source].

Other names:

- APT29
- Dukes
- Group 100
- Cozy Duke
- EuroAPT
- CozyCar
- Cozer
- Minidionis
- SeaDuke
- Hammer Toss

[source].

3.1.3. Venomous Bear

Venomous Bear is a highly motivated actor focusing on diplomatic intelligence. It is highly likely supported by Signals Intelligence (SIGINT) assets with links to the Russian Federal Security Service (FSB) [source]. It has been active since at least 2004 [source]. The group is characterised by its adaptability, often employing novel and sophisticated techniques to maintain operational security [source].

Other names:

- Turla Group
- Turla Team
- Snake
- Group 88
- Waterbug
- Krypton
- Uroburos
- SIG23
- MAKERSMARK
- ITG12

[source].

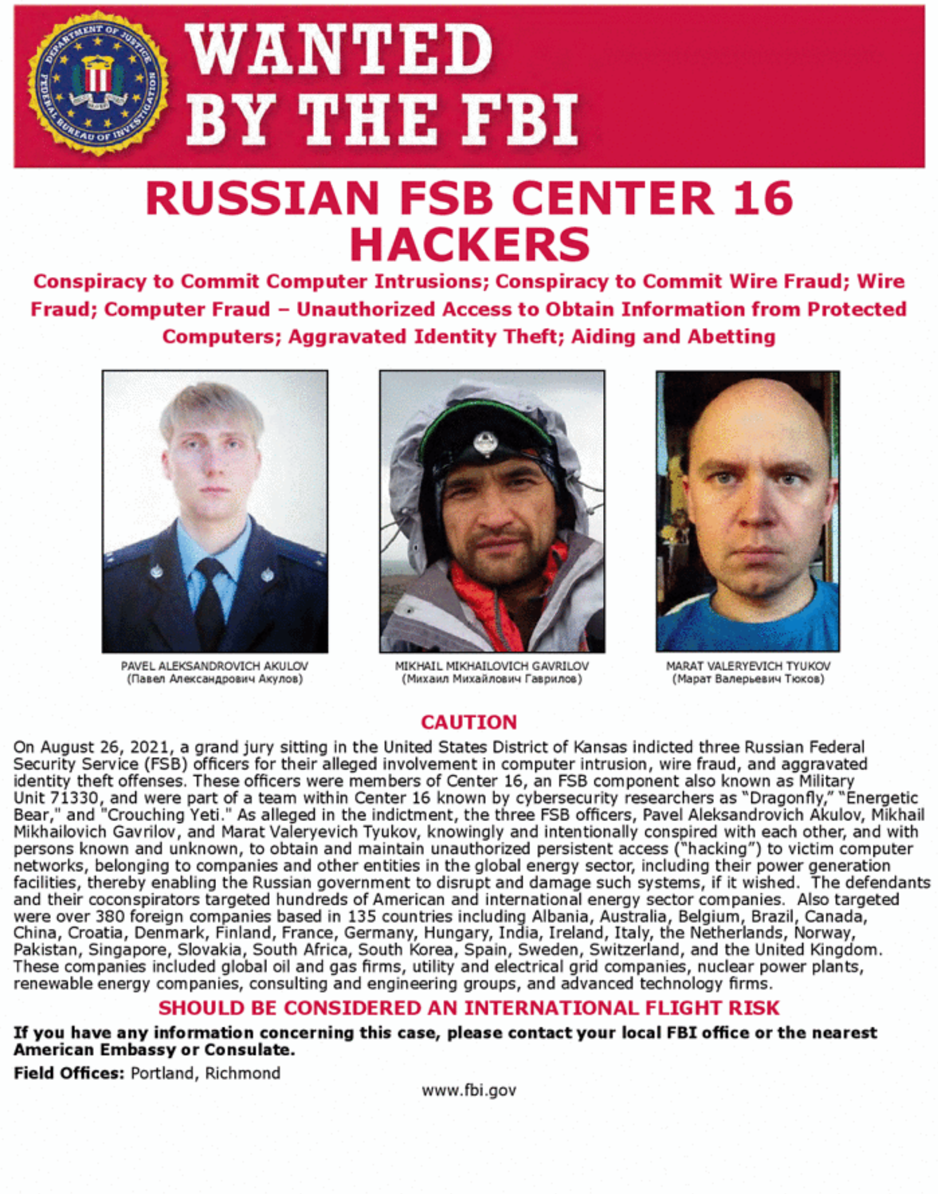
3.1.4. Energetic Bear

Energetic Bear is a highly sophisticated actor reportedly led by FSB's Centre 16 [source; source]. The group mainly targets sectors of national interest, gathering information from energy installations, Middle East oil and natural gas, and military communications equipment [source]. The group has been active since at least late 2010 [source].

Other names:

- Dragonfly
- Crouching Yeti
- Group 24
- Koala Team
- Berserk Bear
- Anger Bear
- Dymalloy
- Havex
- PEACEPIPE
- Fertger
- TEMP.Isotope
- ALLANITE

[source].



WANTED BY THE FBI

RUSSIAN FSB CENTER 16 HACKERS

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Wire Fraud; Computer Fraud – Unauthorized Access to Obtain Information from Protected Computers; Aggravated Identity Theft; Aiding and Abetting

PAVEL ALEKSANDROVICH AKULOV
(Павел Александрович Акулов)

MIKHAIL MIKHAILOVICH GAVRILOV
(Михаил Михайлович Гаврилов)

MARAT VALERYEVICH TYUKOV
(Марат Валерьевич Тюков)

CAUTION

On August 26, 2021, a grand jury sitting in the United States District of Kansas indicted three Russian Federal Security Service (FSB) officers for their alleged involvement in computer intrusion, wire fraud, and aggravated identity theft offenses. These officers were members of Center 16, an FSB component also known as Military Unit 71330, and were part of a team within Center 16 known by cybersecurity researchers as "Dragonfly," "Energetic Bear," and "Crouching Yeti." As alleged in the indictment, the three FSB officers, Pavel Aleksandrovich Akulov, Mikhail Mikhailovich Gavrilov, and Marat Valeryevich Tyukov, knowingly and intentionally conspired with each other, and with persons known and unknown, to obtain and maintain unauthorized persistent access ("hacking") to victim computer networks, belonging to companies and other entities in the global energy sector, including their power generation facilities, thereby enabling the Russian government to disrupt and damage such systems, if it wished. The defendants and their coconspirators targeted hundreds of American and international energy sector companies. Also targeted were over 380 foreign companies based in 135 countries including Albania, Australia, Belgium, Brazil, Canada, China, Croatia, Denmark, Finland, France, Germany, Hungary, India, Ireland, Italy, the Netherlands, Norway, Pakistan, Singapore, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, and the United Kingdom. These companies included global oil and gas firms, utility and electrical grid companies, nuclear power plants, renewable energy companies, consulting and engineering groups, and advanced technology firms.

SHOULD BE CONSIDERED AN INTERNATIONAL FLIGHT RISK

If you have any information concerning this case, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Offices: Portland, Richmond

www.fbi.gov

A FBI-issued Wanted List of Russian Hackers linked to FSB's Centre 16. *Federal Bureau of Investigation*

3.1.5. Voodoo Bear

Most known for its links to the 2015 attacks targeting the Ukrainian power grid and the NotPetya attack in 2017, Voodoo Bear is one of Russia's most infamous APT groups. The group conducts highly advanced operations ranging from espionage to kinetic attacks targeting critical infrastructure. Voodoo Bear is allegedly a cyber unit operating under GRU's Main Centre for Special Technologies (GTsST) Unit 74455 and has been active since at least 2009 [source; source].

In late March 2022, human rights investigators at the UC Berkeley School of Law requested the International Criminal Court in the Hague to consider the group's operations in Ukraine war crimes [source].

Other names:

- Sandworm Team (MITRE G0034)
- TEMP.Noble
- Electrum
- TeleBots
- BE2 APT
- Black Energy
- Iridium
- Hades
- Quedagh
- Iron Viking
- Grey Energy

[source].

4.0. Tactics, Techniques & Procedures

APT groups often change their toolsets, exchange them with other groups, or conduct false flag operations to avoid attribution [source]. Therefore, the issue of attributing attacks based on identified TTP is complex. However, the US Cybersecurity and Infrastructure Security Agency (CISA) offers some publicly known TTP employed by Russian state-sponsored APT groups [source], which are accounted for below. Note that this information is not exhaustive but may illustrate parts of the threat landscape and how some groups may gain access to adversaries' systems.

4.1. Strategic Objectives

4.1.1. Targeting and Attacks

Russian Government-affiliated APT groups are proven capable of conducting disruptive attacks targeting adversaries' critical infrastructure systems. Moreover, attacks targeting industrial control systems (ICS) with malware have been attributed to these groups. If successful, such attacks enable access to protected systems, allowing disruptive or destructive attacks.

Russian Government-affiliated APT groups have proven to possess a significant capability of maintaining a presence in compromised systems undetected over long periods. Such presence is enabled through various techniques offering initial access [source].

4.1.2. Espionage

Espionage activities conducted by Russian-affiliated APT groups target energy, aviation, transportation, healthcare, and telecommunications sectors, to name a few. Russian intelligence services coordinate the operations to fulfil requirements ranging from developing cyber capabilities to foreign policy objectives [source].

4.1.3. Influence

Russian Government-affiliated actors strive to weaken confidence in Western democratic systems through covert online journals and media outlets. Moreover, APT groups are conducting hostile operations targeting government entities influencing national elections and leaking sensitive information such as medical records [source].

4.2. Tactics

The most common tactics employed by Russian-sponsored APTs are:

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Credential Access
- Command and Control

4.2.1. Reconnaissance

When conducting reconnaissance, Russian state-sponsored APT actors often perform large-scale scans to find vulnerable servers. Moreover, they typically conduct phishing and spear phishing operations to gain the credentials required to target specific networks.

4.2.2. Resource Development

Russian state-sponsored APT actors develop and deploy their malware, sometimes combining zero-day exploits for espionage or destructive purposes.

4.2.3. Initial Access

Gaining initial access, Russian state-sponsored APT actors use publicly known vulnerabilities and zero-days. Furthermore, they often target the software supply chain, i.e., compromising trusted third-party software to gain access to a victim organisation.

4.2.4. Execution

Russian state-sponsored APT actors use PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and execute other commands.

4.2.5. Persistence

Using credentials of the existing valid account to maintain continued and long-term access to compromised networks is a well-known procedure among Russian state-backed APT groups.

4.2.6. Credential Access

Russian state-linked APT groups use various techniques to gain credential access. Using brute force or password guessing is one of the most common. Furthermore, they often use compromised account credentials to access Group Managed Service Account passwords. Moreover, they are known to obtain private encryption keys from the Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates.

4.2.7. Command and Control

Russian state-sponsored APT actors often use proxies or virtual private servers (VPS) to route traffic to targets and to hide their activity among legitimate user traffic.

4.3. Types of malware and tools used by Russian government-affiliated APT groups

While not an exhaustive list, below is a summary of known toolkits used by Russian state-sponsored APT groups.

4.3.1. Backdoor

A backdoor is a malware enabling remote access to databases and file servers within an application. By taking advantage of flaws in the application, the backdoor is used to negate normal authentication and offer the perpetrator opportunities to remotely issue commands and further update malware in the system [source].

4.3.2. Credential Stealer

Credential Stealer attacks target an individual's login credentials to protected systems. Commonly enabled through phishing tactics, the method is usually a targeted effort as attackers search social media sites looking for specific users whose login information will provide access to critical information. Additionally, perpetrators often put a lot of effort into making phishing emails and websites look close to identical to legitimate corporations [source].

4.3.3. Downloader

A downloader is an internet-connected Trojan that downloads malign files onto a computer [source].

4.3.4. Privilege Escalation

By exploiting human behaviours, flaws in the system, or oversights in operating systems, a privilege escalation attack is conducted to gain unauthorised privileged access. The potential harm varies depending on the attack, ranging from a simple unauthorised email to large-scale ransomware attacks [source].

4.3.5. Dropper

A dropper is a malicious program functioning as a tool to transport other malware to a victim's unit. Droppers rarely perform any malicious functions but contain other malicious tools which are saved on a target's device without the victim noticing [source].

4.3.6. Wiper

The purpose of wiperware is to wipe out or destroy data. The malware is targeting crucial systems preventing recovery options as systems files required to run the system are deleted, making the system inoperable [source].

4.3.7. Web Shell

A web shell is an enabler of further attacks. The web shell is installed by first penetrating a system, allowing it to function as a backdoor to the target applications and any connected system [source].

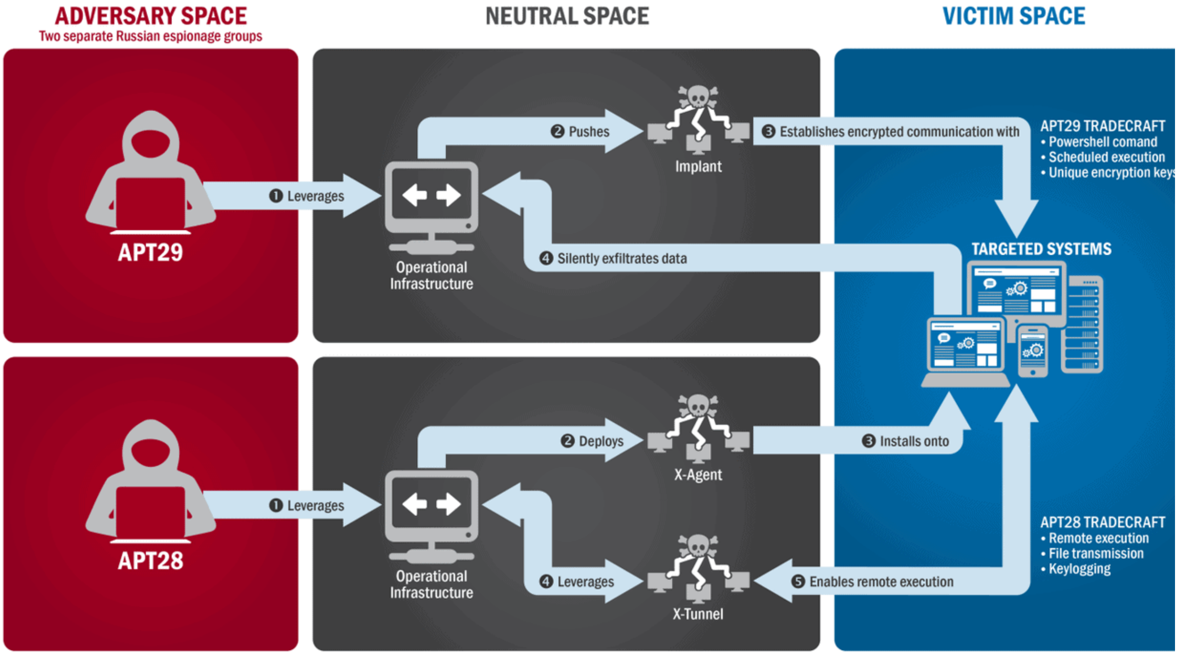


Diagram from US-CERT’s report on APT28 and APT29 (aka GRIZZLY STEPPE) – Image: Wikicommons

5.0. Target Sectors

Russian state-sponsored APT actors use highly advanced cyber capabilities to target a broad range of international critical infrastructure organisations. Targets are mainly organisations within Government and the private sector providing essential infrastructure services and the internet service providers supporting these sectors [source].

According to the US Office of the Director of National Intelligence 2021 Annual Threat Assessment, “Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and allied and partner countries, as compromising such infrastructure improves – and in some cases can demonstrate – its ability to damage infrastructure during a crisis.” [source].

5.1. Common Target Sectors

- COVID-19 research
- Governments
- Election organisations
- Healthcare and pharmaceutical companies
- Defence
- Energy
- Video gaming
- Nuclear
- Commercial facilities
- Water
- Aviation
- Critical manufacturing

[source].

5.2. Target Sectors by Group

5.2.1 Fancy Bear

- Government entities
- Political parties
- Anti-chemical weapons organisations
- Anti-doping organisations
- Energy
- Education

5.2.2. Cozy Bear

- Governments
- Research institutes
- Think tanks

- Political organisations

5.2.3. Venomous Bear

- Governments
- Military
- Education
- Research
- Aerospace
- Telecommunications
- Pharmaceutical companies

5.2.4. Energetic Bear

- Governments
- Aviation
- Energy
- Industrial Control Systems
- Critical Infrastructure

5.2.5. Voodoo Bear

- Ukrainian energy sector
- Governments
- Anti-chemical weapons organisations
- Political parties and campaigns
- Critical infrastructure

[source; source].

6.0. Prominent attacks attributed to Russian state-sponsored APT groups

6.1. 2011-2018 – Global Energy Sector Intrusion Campaign

Between 2011 and 2018, Russian state-sponsored cyber actors conducted a large-scale intrusion campaign targeting international energy sector networks. The perpetrators primarily conducted reconnaissance and launched malware targeting Industrial Control Systems [source].

6.2. 2015 & 2016 – The Ukrainian Power Grid Attacks

In 2015 and 2016, Russian state-sponsored APT actors conducted attacks targeting Ukrainian energy distribution companies in 2015 and an electrical transmission company in 2016. Consequently, the attacks caused power outages and made infected computers inoperable [source].

6.3. 2016 – US Presidential Election Hack

In 2016, multiple networks of US Democratic National Committee organisations were targeted by spear phishing attacks, giving the perpetrators access to election-related documents [source; source].

6.4. 2017 – The NotPetya Attack

In 2017, Ukraine's financial and governmental institutions were targeted by Russian state-sponsored actors in what is described as the fastest-propagating piece of malware. By utilising a combination of the EternalBlue and Mimikatz tools, the launched malware circumvented patched flaws, taking advantage of a specific Windows protocol. Once a unit was infected, the malware spread rapidly, wiping out critical data on users' machines and making them inoperable. In essence, what distinguishes NotPetya is that it is not designed to be decrypted, making it a purely destructive tool or weapon [source; source; source].

7.0. Russian APTs in Ukraine: some sightings

Russian cyber operations during the war in Ukraine have inflicted negligible damage regarding strategic objectives. Initially, traditional jamming enabled a tactical advantage during the invasion. Still, the strategic value of sophisticated cyber operations has remained absent. The cyber capabilities of Russian operations have largely been overshadowed by their kinetic physical counterparts. The absence of any significant value in cyber operations may be due to the infeasibility of burning presence and capabilities in cyberspace when the same goals can be accomplished through regular artillery.

Furthermore, an inability to integrate cyber operations in a coherent all-domain strategy will inevitably result in shortcomings, of which logic is the same in any domain. Successful warfare is rarely conducted exclusively at sea, in the air, or on land. Another explanation may be Ukraine's defensive capabilities. As Ukraine has been a target of Russian aggression in cyberspace long before the invasion, there are prospects for lessons learned and efforts to increase resilience.

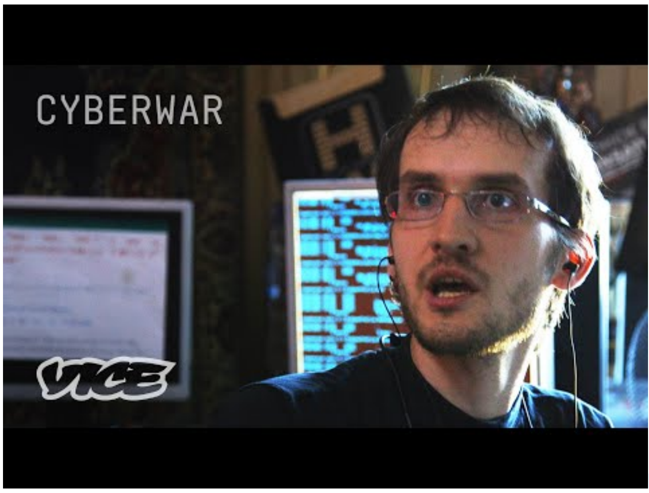
However, even though the strategic value of Russian offensive cyber operations has remained absent, the capabilities are known, and the potential for unintentional spillover effects. Hence, Russian cyber operations constitute a real threat to any digitalised society.

8.0. What's Next?

Russia will likely continue to pose a severe threat to Western nations regarding sensitive information, influence campaigns, and attacks targeting critical infrastructure. Moreover, as Western governments are reacting to Russia's invasion of Ukraine, there are prospects for future attacks.

9.0. Summary

Previous attacks attributed to Russian state-sponsored APT groups highlight their capabilities and the risk of unintentional spillover to other nations. As Russia will most likely utilise its offensive cyber capabilities, Western countries face a severe threat requiring joint counter efforts. Moreover, cyberspace does not recognise any state borders, highlighting Russia's reach and efficiency in targeting its opponents. Looking at the past and the future, the Five Bears constitute an integral part of Russia's offensive capabilities.



https://youtu.be/cdfZsJd4D28