# Russian Cyber Attack Campaigns and Actors

ironnet.com/blog/russian-cyber-attack-campaigns-and-actors

May 29, 2020


Some of the most notorious actors in the cyber threat landscape have been traced back to sponsorship by the Russian state. As the digital revolution has accelerated, so, too, has the Russian cyber attack landscape — hold-over Cold War tactics that evolved to take advantage of new electronic methods of communication.

Strategic Russian interests are guided by the desires for Russia to be recognized as a great power, to protect the Russian identity, and to limit global United States power. These themes are evident in components commonly associated with Russian-backed cyber threat campaigns:

- The weaponization of information through disinformation campaigns and propaganda
- Attempted interference in democratic processes
- Strategic positioning within critical infrastructure, perhaps as preparation for potential escalation of hostilities with rival nations.

To summarize the threat at a more tactical level, we have scoured cybersecurity reporting in order to prepare an overview of cyber threat actors observed more recently, and to which evidence-based analysis has assigned the likelihood of Russian state-sponsorship as probable. Each actor is presented with highlights of more notable campaign activity, with notations on countries and sectors targeted, as well as a mention of behaviors or tactics, techniques, and procedures (TTPs) utilized in order to enable actions on objectives. Footnotes provide links to further, more detailed, reading.

Who are today's major Russian adversary groups and what are the main tactics and techniques of Russian cyber attack campaigns? Let's take a closer look at some of these known actors, listed here in order of threat scope and potential:

## Sandworm Team

Active since at least 2009, the Sandworm Team is responsible for the first publicly acknowledged cyber incident that resulted in power outages impacting a civilian population, occurring in Ukraine in December 2015. The malware used in this attack, BlackEnergy 3, enabled the actor to gain access to the IT network of a Ukrainian power company, from which they pivoted to the SCADA portion of the network, giving the actor the ability to manipulate the Industrial Control System (ICS) — without the need for customized malware — in order to shut down power in Kiev. This is an often mis-characterized component of the campaign, likely because the BlackEnergy 2 predecessor to BlackEnergy 3 contained ICS targeting components that are not present in BlackEnergy 3. Cybersecurity researchers also note that "Russian operators, such as Sandworm Team, have compromised Western ICS over a multi-year period *without* causing a disruption," perhaps in order to stage for future potential Russian cyber attack campaigns.

| | |
|---|---|
| **Known Targets** | NATO member countries, Ukraine, Telecommunications, Energy, Government, Education |
| **Sample TTPs** | • Spearphishing utilizing weaponized Microsoft Office documents<br>• Denial of Service attacks for the purposes of disrupting communications<br>• Remotely controlling SCADA<br>• Destruction of files by utilizing KillDisk malware |
| **Also Known As** | BlackEnergy, Voodoo Bear, TEMP.Noble, Iron Viking |

## ELECTRUM

This group is responsible for the CRASHOVERRIDE malware framework (frequently also referred to as Industroyer), which was the first malware to ever specifically target and disrupt electric grid operations. In December 2016, Russian cyber attack by these actors manipulated breakers at a substation in Kiev Ukraine, leading to power disruption and serious damage to equipment.

ELECTRUM has links to Sandworm as their development group, but it appears that the understanding of which team actually carried out the attack has evolved over time. Regardless of the specific threat actor, the behaviors demonstrated are what are important to understand.

| | |
|---|---|
| **Known Targets** | Ukrainian energy sector |

| | |
|---|---|
| **Sample TTPs** | • Maliciously impacting operations by leveraging ICS protocols<br>• Establishment of an internal proxy within a compromised network which receives connections from backdoors installed on other systems within the network, and attempts to funnel data to external command and control servers<br>• Incorporation of malware modules with data wiping capabilities |
| **Also Known As** | Sandworm Team |

## Telebots

Telebots is the group attributed to the NotPetya ransomware outbreak, which is the most destructive attack in history from a financial perspective, and is reported to be an evolution of the group or groups responsible for causing the Ukrainian blackouts described in the previous two sections. In 2018, the security firm ESET identified code linkages between NotPetya and CRASHOVERRIDE (which they refer to as the Industroyer attack). The NotPetya attack initially targeted industries in Ukraine after the threat actor was able to effect a supply-chain compromise of Ukrainian accounting software. The incorporation of the EternalBlue exploit for SMB in conjunction with the password dumping tool Mimikatz enabled NotPetya to cripple networks around the globe.

| | |
|---|---|
| **Known Targets** | Ukrainian financial sector |
| **Sample TTPs** | • Spearphishing with Microsoft Excel attachments containing malicious macros<br>• Hiding malicious network activity by abusing legitimate services to host payloads or provide communication mediums for attackers<br>• Deployingredundant backdoors within a network<br>• Disguising malware backdoors by providing them with names resembling AV-related services |
| **Also Known As** | Sandworm Team |

## Energetic Bear

This group is assessed as the creator of the Havex RAT, which is one of five known ICS tailored malware families. Energetic Bear campaigns began in 2010 in order to collect intelligence used for espionage (as opposed to attempting destruction or disruption of systems) and have continued through at least 2017. The TTPs leveraged by this threat actor are not unique or particularly novel, but the systematic and deliberate social engineering strategies employed are. Smaller, less

defended companies and subcontractors within the energy sector have been targeted — likely as a means for the actor, in turn, to target regional and national-level energy companies and power suppliers.

| | |
|---|---|
| **Known Targets** | Energy, Aviation, Pharmaceutical, Defense, Petrochemical sectors in the United States and Europe |
| **Sample TTPs** | • Compromise legitimate industrial control systems vendor sites and plant trojanized versions of ICS-related software and applications on those sites<br>• Spearphishing emails with PDF attachments embedded with Adobe Flash exploits |
| **Also Known As** | Dragonfly, Crouching Yeti, Havex, Koala, Iron Liberty |

## DYMALLOY

Some researchers attribute the activities of this group to an evolution of Energetic Bear activity (referring to earlier activity as Dragonfly and later activity as Dragonfly 2.0); however, Dragos asserts that there are enough technical differences to justify tracking this as a separate group. This group avoids using custom malware, opting for commodity malware families that hinder attempts at applying attribution. Crowdstrike reports that this group has strong ties to Moscow, as targeting aligns closely with likely collection priorities of Russian intelligence.

| | |
|---|---|
| **Known Targets** | Industrial Control Systems in Turkey, Europe, and the United States |
| **Sample TTPs** | Use of commodity malware such as Goodor, DorShel, and Karagany |
| **Also Known As** | Dragonfly 2.0, Berserk Bear |

## APT29

This group has operated since at least 2008, collecting intelligence in support of foreign and security policy decision-making. The primary targets are Western governments and related organizations, but intrusion attempts have been witnessed across a broad spectrum of sectors. Notable compromises include the intrusion into the Democratic National Committee in 2015 and 2016, and intrusions into unclassified networks of a variety of U.S. government departments.

| | |
|---|---|
| **Known Targets** | Western governments and related organizations, as well as Western Europe, Brazil, China, Japan, Mexico, New Zealand, South Korea, Turkey, and Central Asian countries. |

| | |
|---|---|
| **Sample TTPs** | • Heavy waves of spearphishing with messages that contain either links to malicious executables hosted on legitimate but compromised websites, or Microsoft Office attachments with content making the documents appear legitimate in order to disguise embedded macros which enable malware installation<br>• System exploitation followed by downloads of steganographic PNG image files from compromised servers<br>• Use of malicious shortcut files (LNKs) to deliver payloads<br>• Use of benign decoy documents delivered intentionally to evade detection<br>• Compromising the infrastructure of various corporations in order to deliver phishing emails |
| **Also Known As** | Cozy Bear, The Dukes, CozyDuke, YTTRIUM, Hammertoss, MiniDionis |

## APT28

This espionage-focused group has also operated since at least the mid 2000s, targeting multiple sectors around the world with special focus on defensive sector organizations. Multiple governments have attributed the actions of this group to Russian military intelligence service, and notable operations have targeted organizations such as the International Olympic Committee, the Organisation for the Prohibition of Chemical Weapons, and the Democratic National Committee (similar to APT29). Cybersecurity researchers identify this actor as conducting some of the most far-reaching and sophisticated Russian cyber attack campaigns to date.

| | |
|---|---|
| **Known Targets** | Aerospace, Defense, Energy, Government and Media sectors, with victims in the United States, Western Europe, Brazil, Canada, China, Georgia, Iran, Japan, Malaysia and South Korea |
| **Sample TTPs** | • Registering domains that attempt to appear legitimately associated with victim organizations, and utilizing these domains as part of credential harvesting campaigns<br>• Abuse of OAuth access tokens in order to gain access to targeted email accounts<br>• Capturing information from air-gapped computers via infected USB devices<br>• Utilizing complex malware to target routers and IoT devices in order to enable reconnaissance within potential victim networks and potentially set the stage for wiper operations. |
| **Also Known As** | FANCY BEAR, Pawn Storm, Sednit, SNAKEMACKEREL, Sofacy, STRONTIUM, TG-4127 |

## Fxmsp

In May 2019, the hacking collective Fxmsp gained notoriety for reported breaches of three major antivirus companies.This group targeted intellectual property from each company, including code base, development documentation, and information on Artificial Intelligence (AI) modeling for the purposes of offering up this information for sale, as well as selling network access to victims.

| | |
|---|---|
| **Known Targets** | Large global organizations and government networks |
| **Sample TTPs** | • Utilization of a network of trusted proxies in order to promote and offer up network accesses for sale in underground markets<br>• Creation of a credential-stealing botnet utilized to harvest usernames and passwords |
| **Also Known As** | N/A |

## WIZARD SPIDER

This cyber criminal group targets large organizations by deploying Ryuk ransomware via Trickbot banking malware. Evidence suggests that the ransom demand varies depending on the size of the targeted organization, and, as of January 2019, the total amount collected by the group was $3.7 million USD. At the end of 2019, researchers identified that WIZARD SPIDER continues to add functionality to the Ryuk variants it delivers in order to maximize the number of systems within a network impacted by file encryption.

| | |
|---|---|
| **Known Targets** | United States, United Kingdom, Canada |
| **Sample TTPs** | • Trickbot is delivered via spam email or via the Emotet banking trojan<br>• Obfuscated PowerShell scripts execute and connect to remote IP addresses for additional tool downloads<br>• Lateral movement enabled through the use of Remote Desktop Protocol (RDP) |
| **Also Known As** | TEMP.MixMaster |

## Turla

Researchers have linked activity from this threat group to Moonlight Maze, a massive data breach of U.S. government classified information in the late 1990s, and one of the first widely known cyber espionage campaigns in history. Another notable campaign took place in 2008, when Agent.btz malware infected U.S. government classified networks via infected removable media. This group is still in active operation today. More recent operations of this Russian cyber attack campaign and group have been extremely targeted, going through extensive lengths to fingerprint

systems, collecting as much information as possible, before making a determination as to whether the target is of interest for further operations. One of the techniques utilized includes attempting to lure visitors of compromised websites to download fake Adobe Flash updates, an approach utilized by cyber criminals across the globe.

| | |
|---|---|
| **Known Targets** | Government, Aerospace, NGOs, Defense, Cryptology, and Education sectors in more than 45 different countries throughout the world |
| **Sample TTPs** | • Extensive use of covert exfiltration tactics such as using hijacked satellite connections and covert channel backdoors<br>• Waterholing government websites<br>• Infecting removable storage devices<br>• In-house complex malware development |
| **Also Known As** | Snake, Venomous Bear, Waterbug, Uroburos |

## XENOTIME

This group has been identified as the most dangerous threat actor publicly known, due to its association with malware known as TRITON, designed to target a specific safety instrumented system (SIS) within industrial control systems. SIS are hardware and software controls used to implement safe states in order to avoid adverse safety, health, and environmental consequences, and, as such, targeting of these systems could lead to loss of life scenarios. TRITON was discovered at a petrochemical plant in Saudi Arabia when the attacker was believed to have inadvertently shut down plant operations after gaining access to a SIS engineering workstation to deploy the attack framework. Because TRITON malware samples are now easily discoverable online, the bar has effectively been lowered for other threat actors to enter the ICS arena.

| | |
|---|---|
| **Known Targets** | Oil, gas, and electric sectors in the Middle East, North America, Europe, and APAC |
| **Sample TTPs** | • Capability to gain access to hardware and software not widely available, in order to reverse engineer proprietary protocols and identify previously unknown vulnerabilities for exploitation<br>• Perimeter VPN compromise for initial access to target network |
| **Also Known As** | TEMP.Veles |

## Gamaredon Group

This group notably conducts espionage and intelligence gathering via Russian cyber attack strategies in support of Russian national interests, and seems to primarily focus efforts on Ukrainian national security targets. Cybersecurity researchers have pointed out that this group's

current activities potentially serve as a testbed for evaluating adversarial response to TTPs, with the implication that the group could pivot to utilizing these tactics against future perceived threats beyond Ukraine.

| | |
|---|---|
| **Known Targets** | Ukrainian Government and Military, Journalists, Law Enforcement, and NGOs |
| **Sample TTPs** | • Utilization of Dynamic DNS domains for command and control servers<br>• Deployment of remote manipulation system binaries (RMS) via self-extracting archives and batch command lines<br>• Social engineering campaigns to distribute malware through macros embedded with Excel and Word documents |
| **Also Known As** | Primitive Bear |

## FIN7

The operations of this financially motivated threat group have continued well into 2020, despite the U.S. Department of Justice announcing arrests in August 2018 of individuals with ties to the group. This group is known for leveraging Carbanak malware in addition to other tools, in order to enable the theft of more than 15 million customer credit card records from victims spanning hundreds of companies in the United States and abroad. FIN7 operators have engaged in sophisticated social engineering techniques, including actively engaging targets in back and forth dialogue before sending malicious documents leading to malware implants.

| | |
|---|---|
| **Known Targets** | Predominantly U.S. Retail, Restaurant, and Hospitality sectors |
| **Sample TTPs** | • Extensive use of digital certificates to sign phishing documents, back-doors, and other tools in an effort to appear legitimate<br>• Rapid technical innovation for the purposes of detection evasion |
| **Also Known As** | Anunak, Carbon Spider, Carbanak |

## Fighting back through Collective Defense

At IronNet, we detect Russian cyber attack campaigns like these and other types of sophisticated cyber attacks through AI-based behavioral analytics and share those discoveries into our Collective Defense ecosystem. This approach allows Collective Defense members to get advanced notice on threats impacting their peers that may be headed their way. This empowers

states, sectors, supply chains, companies of all sizes — and even entire nations — to work collaboratively for stronger cyber defense against Russian and other nation-state level adversaries.