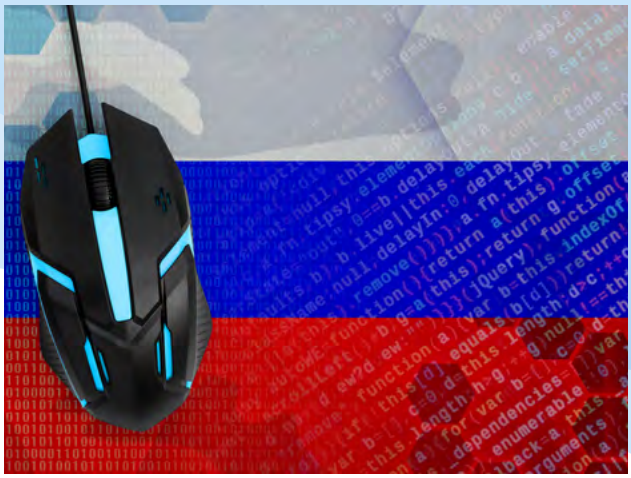
THREAT INTELLIGENCE REPORT

The Russian Threat, In Brief

By Adam Hlavek



Since the fall of the Soviet Union, the Russian state has sought to reestablish itself as a global superpower. Over the last two decades, Russian President Vladimir Putin has systemically consolidated his power within the country and wields dictatorial control over the government. A former KGB officer, Putin has fully embraced information operations and cyber espionage as tools to challenge his global adversaries, the foremost of which are the United States and its NATO allies. Within Russia, the regime engages in pervasive electronic surveillance and censorship to quell dissent to maintain political control.

Despite lacking the national wealth and technological prowess of their Western rivals, the Russian intelligence services have proven to be one of the shrewdest, most effective —and potentially most dangerous — threat actors in cyberspace. Some of the highest profile examples include:

- **Interference in the 2016 U.S. presidential elections.** These operations illustrated the reach and power of cyber-enabled influence operations.
- **Disruption of the Ukrainian power grid in 2015.** Russian cyber actors are credited with the first publicly identified attack on a live power grid, which impacted an estimated 225,000 people.
- **Intrusions into the U.S. power grid.** In 2018, the U.S. publicly accused Russia of conducting a two year long coordinated campaign of cyber intrusions into the U.S. power grid.
- **Targeting of COVID-19 research.** In July 2020, the U.S., U.K., and Canada detailed Russian-driven cyber intrusion campaigns that were directed against organizations conducting COVID-19 vaccine development.

With these instances serving as precursors, there is now widespread concern and mounting evidence within the cybersecurity community that Russian hackers are actively developing deep access into critical infrastructure networks around the globe for the purpose of executing disruptive or destructive physical attacks should they be called upon to do so by regime leadership.

Russia also harbors a large proportion of the world's active cyber criminals. Theft and fraud appear to be routinely ignored by the Russian authorities, provided the victims reside in those nations the Kremlin considers its enemies. Putin's regime offers little help in bringing these criminals to justice, and may in fact be partnering with them, placing these criminal actors beyond the reach of many Western law enforcement agencies.

Russia's Strategic Goals

1. Reestablish Status as a Great Power

The 1991 dissolution of the Soviet Union upended the Russian state and, in turn, Russian culture. Once viewing themselves as the center of a historic, global, communist movement, Moscow's political elite were forced to adapt to diminished borders, shuffled alliances, and a stagnant national economy that held few advantages over its global competitors.

The emergence of Vladimir Putin as Russia's leader at the turn of the century would prove pivotal. Putin garnered widespread public support throughout Russia, in large part thanks to the initial economic growth enjoyed by the Russian people under Putin's early years, his appeals to national pride, and his pervasive cult of personality. As the years have unfolded, Putin has sought to cement this approval by systematically limiting the free flow of information and by censoring, or even jailing, his political opponents.

While maintaining strict control over domestic Russian politics, Putin has also consistently sought to expand Russia's influence, prestige, and prosperity on the world stage. While Russia's economic power is middling (e.g., the Russian GDP represents only a fraction of that of the U.S. and China), Putin has been more than willing to use Russia's military might and intelligence services to counter Western diplomatic and military objectives in the Middle East, Eastern Europe, and elsewhere. Cyber operations represent a unique avenue for the Russian government to level the playing field with their global competitors, and they have been able to leverage these capabilities with frightening success.

Historical Cyber Examples:

- Extensive Global Information Operations
- Control of Domestic Internet

Recent Cyber Examples:

- Hacking of Olympic and Anti-Doping Organizations
- Sandworm Global Campaigns.

2. Counter and Weaken NATO

Since the days of the Soviet Union, Russia has seen NATO as its greatest military threat. The alliance spans the European continent, and includes both Baltic and former Yugoslavian states. These states joining NATO following the end of the Cold War has brought the NATO footprint even closer to Russia's borders. The presence of NATO troops and weapons platforms throughout Eastern Europe presents the threat of real and legitimate military action against Russia should genuine hostilities break out.
Given these circumstances, the Kremlin almost certainly seeks to avoid a physical war, yet it is still determined to find ways to undermine and weaken the NATO alliance. Cyber operations have provided an ideal platform to pursue such goals. To this end, Russian cyber operators have engaged in both espionage and disinformation campaigns aimed at governments, ministries of foreign affairs, and militaries across a number of NATO and EU states. These operations have complementary goals, namely to obtain current intelligence on rival governments, establish deep access within target networks for potential follow-on operations, and sow mistrust amongst the allies.

Historical Cyber Examples:

- Operation Secondary Infektion

Recent Cyber Examples:

- Dymalloy targeting of German companies
- Turla Targeting of Foreign Governments
- Ghostwriter and Associated Influence Campaigns

3. Counter and Weaken the United States

As the world's most capable military power and the de facto leader of NATO, Russia views the United States as its chief rival. Russia lacks the military might and economic prosperity of the United States. To overcome these disadvantages, Russia operates opportunistically, fostering alliances with U.S. adversaries and relying on espionage and disinformation operations to project power. Cyberspace provides an inexpensive and effective platform for such actions.

Those Russia cyber operations that have been publicly exposed are already some of the most notorious of the 21st century. The 2016 APT28 compromise of the Democratic National Committee and concurrent social media operations of the Internet Research Agency have served to create nationwide concern and debate within the U.S. The Russian intelligence apparatus has shown no signs of stopping, as U.S. intelligence officials have warned of renewed Russian interference in the 2020 U.S. presidential election.

Historical Cyber Examples:

- 2016 - Election Interference
- 2008 - Buckshot Yankee

Recent Cyber Examples:

- APT28 Campaign
- APT29 Targets COVID-19 Research

4. Reestablish Control over Ethno-Russian former Soviet Republics

The Putin regime often embraces narratives suggesting a return to an idealized Russian past. A key part of this narrative includes returning those ethnically Russia populations living outside the country proper to mother Russia. Thus, former Soviet Republics such as Ukraine and Georgia have become targets for military intervention and information operations. Russia has been particularly aggressive in these campaigns, perhaps believing that they hold dominion in these regions and do not fear reprisals from the West as they would in the case of NATO countries.

Russian cyber operations in these nations have notably been coupled with military action on more than one occasion. This cyber-physical form of military operations likely represents the Russian blueprint for future combat operations.

Historical Cyber Examples:

- 2019 - Georgia Cyber Attack
- Sandworm activity in Ukraine
- 2007 - Estonia attacks

Recent Cyber Examples:

- Gamaredon Group in Ukraine
- Turla Targeting of Foreign Governments

Recent Russian Threat Campaigns

Ghostwriter

Recent Activity:

Ghostwriter represents yet another recently identified cyber influence operation likely tied to the Russian intelligence apparatus. The campaign, which has been active from early 2017 through at least May 2020, has focused on disseminating falsified narratives surrounding Lithuania, Latvia, and Poland, and their relations with other NATO allies. The fake stories consistently suggest tensions between the allies or wrongdoing by NATO troops stationed within the Baltic region.

In addition to the activity attributed to Ghostwriter, the Associated Press reported that Russian intelligence services were also using several English-language websites to spread disinformation about the COVID-19 pandemic and response in the United States, providing yet another example of concerted effort by the Russian intelligence services to influence public opinion within the West.

Overview:

The actors behind this campaign have successfully compromised legitimate websites (typically news sites) which they use to post fabricated stories containing false or divisive narratives surrounding NATO with a focus on Eastern Europe. Various cyber personas are then used to amplify and further disseminate the narratives by posting to blogs, sites allowing user-generated content, or social media. In April 2020, one such fake letter was even posted to the official website of the Polish War Studies Academy.

The tactics and concepts observed during the Ghostwriter campaign are reminiscent of Operation Secondary Infektion, an online influence operation uncovered in 2019. Secondary Infektion was also designed to exacerbate tension between the NATO countries and relied upon social media to amplify and distribute fake stories. While there are no technical links between these two campaigns, the intent and tactics are strikingly similar.

Known Targets	Poland, Latvia, and Lithuania
Sample TTPs	• Creation of fabricated narratives designed to exacerbate or create tensions between NATO allies • Compromise of news or government websites to facilitate distribution of false information • Amplification of false narratives by posting to sites allowing user-generated content, blogs, or social media
AKA	None Identified

APT28

Recent Activity:

In August 2020, the FBI and the NSA released a detailed analysis of a malware toolset known as "Drovorub," which the agencies attributed to a specific military unit within the Russian General Staff Main Intelligence Directorate's (GRU) 85th Main Special Service Center (GTsSS), and linked this activity to APT28 and previous private sector research. This reporting does not speak to the targets or intent of Drovorub's operators but appears to be part of a concerted effort by the U.S. government to publicize and counter Russian cyber threats.

Additional reporting indicates that from December 2018 until Spring 2020, APT28 conducted a wide-ranging campaign targeting a variety of U.S. institutions, including state and federal government agencies, educational institutions, and the energy sector. The victims of these breaches were apparently contacted by the FBI this past May. The group's efforts appear to have been focused on penetrating mail servers and email accounts, as well as VPN services.

Overview:

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 • Abuse of OAuth access tokens in order to gain access to targeted email accounts • Capturing information from air-gapped computers via infected USB devices • Utilizing complex malware to target routers and IoT devices to enable reconnaissance within potential victim networks and potentially set the stage for wiper operations.
AKA	FANCY BEAR, Pawn Storm, Sednit, SNAKEMACKEREL, Sofacy, STRONTIUM, TG-4127

APT29

Recent Activity:

In July 2020, cybersecurity agencies from the UK, Canada, and the US jointly attributed a campaign targeting pharmaceutical companies and academic institutions involved in COVID-19 vaccine development to APT29, a group widely believed to be operating on behalf of Russian intelligence services.

The group began its intrusions by conducting basic vulnerability scanning against external IP addresses known to belong to the target organizations. The group then deployed publicly known exploits against the vulnerable systems it found, including popular Citrix, Pulse Secure, and Fortinet devices, among others. The APT29 actors then deployed custom malware, known as WellMess or WellMail, to execute commands, upload and download files, and other operational tasks on the victimized systems. Notably, these malicious tools are designed to work on both Windows and Linux-based systems and support command and control communications over multiple networking protocols.

Overview:

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 • System exploitation followed by downloads of steganographic PNG image files from compromised servers • Use of malicious shortcut files (LNKs) to deliver payloads • Use of benign decoy documents delivered intentionally to evade detection • Compromising the infrastructure of various corporations in order to deliver phishing emails
AKA	Cozy Bear, The Dukes, CozyDuke, YTTRIUM, Hammertoss, MiniDionis

Gamaredon Group

Recent Activity:

In Spring 2020, analysts observed an increase in activity from Gamaredon (active since at least 2013) indicating that the group remains a present threat to the Ukranian organizations they appear to target. These most recent campaigns were highlighted by large waves of malicious emails directed against targets' and the group's use of new malware and tactics, techniques, and procedures(TTP).

Overview:

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 • Deployment of remote manipulation system binaries (RMS) via self-extracting archives and batch command lines • Social engineering campaigns to distribute malware through macros embedded with Excel and Word documents
AKA	Primitive Bear

Dymalloy

Recent Activity:

In Spring 2020, it came to light that German government authorities had issued an advisory to critical infrastructure operators in the country indicating that the Russia-linked Berserk Bear (aka Dymalloy) group had executed "longstanding compromises" within several German companies. Of note, there were no identified production disruptions within industrial networks, per German authorities. Instead, the goal of these campaigns appears to have been to establish persistence within the companies' IT, production and/or operational technology (OT) networks, presumably to allow for future operations.

Additionally, in October 2020, the U.S. FBI and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint advisory detailing active targeting of U.S. state and local governments and aviation networks by Berserk Bear actors. While the advisory stated that these intrusions did not appear to have disrupted any operations within the targeted networks, the group did successfully exfiltrate data from at least two victims and appeared to be hunting for information such as network configurations, passwords, and vendor purchasing data.

Overview:

Some researchers attribute the activities of Dymalloy to an evolution of Energetic Bear activity (earlier activity is referred to 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; US state, local, territorial, and tribal (SLTT) government and aviation sectors
Sample TTPs	• Use of commodity malware such as Goodor, DorShel, and Karagany • The chaining or combination of multiple legacy vulnerability exploits with exploitation of the newer Windows Zerologon vulnerability
AKA	Dragonfly 2.0, Berserk Bear

Sandworm

Recent Activity:

In May 2020, the National Security Agency issued an advisory warning of ongoing exploitation of a vulnerability in Exim mail transfer agent (MTA) software, which is popular in Unix and Linux-based systems. The advisory also specifically tied this activity to the Sandworm Team, whose actions the US government has publicly attributed to the Russian GRU's Main Center for Special Technologies.

In October 2020, the US Justice Department announced the indictment of six Russian men who are members of the Sandworm Team. The indictment also lists numerous intrusion campaigns executed by these actors, to include the infamous NotPetya attacks, targeting of French politicians and government entities during the 2017 elections, and efforts to interfere in media and government networks in Georgia in 2018 and 2019. These charges also included the first official acknowledgement by the US government that Sandworm was responsible for the Olympic Destroyer malware used to disrupt the 2018 Winter Olympic Games in PyeongChang, South Korea.

Overview:

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 there 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 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 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 • Denial of Service attacks for the purposes of disrupting communications • Remotely controlling SCADA • Destruction of files by utilizing KillDisk malware
AKA	BlackEnergy, Voodoo Bear, TEMP.Noble, Iron Viking

Turla

Recent Activity:

Throughout the first half of 2020, the Turla group was linked to multiple cyber espionage operations targeting government entities in Europe and the Caucasus. Researchers at ESET detailed updates to Turla's ComRAT malware, the heir to the infamous Agent.BTZ malware, which was used to target two Ministries of Foreign Affairs and a national parliament. Turla actors were also linked to a narrowly focused waterhole campaign targeting Aremenian government officials and politicians and may have been behind an intrusion into the network of the Austrian foreign ministry.

Overview:

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 and 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 • Waterholing government websites • Infecting removable storage devices • In-house complex malware development
AKA	Snake, Venomous Bear, Waterbug, Uroburos

XENOTIME

Recent Activity:

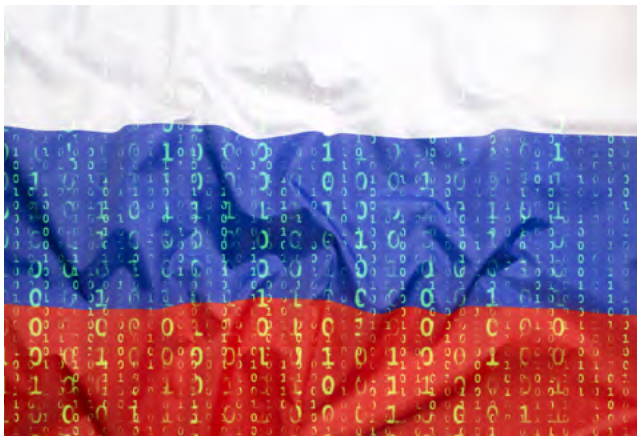
In October 2020, the US Treasury Department imposed sanctions on the Russian Central Scientific Research Institute of Chemistry and Mechanics, effectively cutting off any US business or engagement with the research institute and opening the prospect of sanctions against third-party nations that continue to do business with them. The sanctions represent the first public acknowledgement by the US government of the institute's connection to the Triton malware designed to target industrial safety systems, which had been previously alleged by private sector cybersecurity researchers.

Overview:

This group has been identified as the most dangerous threat actor publicly known due to its association with malware known as TRITON, as it is designed to target a specific safety instrumented system (SIS) within industrial control systems. SISs are hardware and software controls used to implement safe states to avoid adverse safety, health, and environmental consequences. 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. Since 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 • Perimeter VPN compromise for initial access to target network
AKA	TEMP.Veles

In Summary



Russian cyber operations represent a very real and sophisticated threat to a wide range of sectors in numerous countries and regions. As the campaigns outlined here illustrate, Russian intelligence services view corporations, governments, and civil society as viable targets for espionage and disinformation operations. In many cases, this simply isn't a fair fight. The Russia state brings resources to bear that many of the organizations, even many nations, they victimize cannot match.

Nearly all of the campaigns discussed here have been active within just the past several months. Just since May 2020, the US government has publicly attributed multiple distinct campaigns and toolsets to specific Russia state sponsored groups. While this is not the first time the US and its allies have "named and shamed" malicious foreign actors, the pace with which this has occurred is indeed unprecedented. This is not a coincidence. These threats are not hypothetical and are not projected to arrive at some distant date—they are here now.

IronNet technology is designed to level the playing field. Collective Defense presents a unique opportunity to identify and correlate sophisticated cyber threats as detected by Network Detection and Response behavioral analytics, allowing an organization to rely not only on what they can see within their own networks, but to leverage the accumulated knowledge of the IronDome community to rapidly discover malicious behavior across enterprises or sectors.