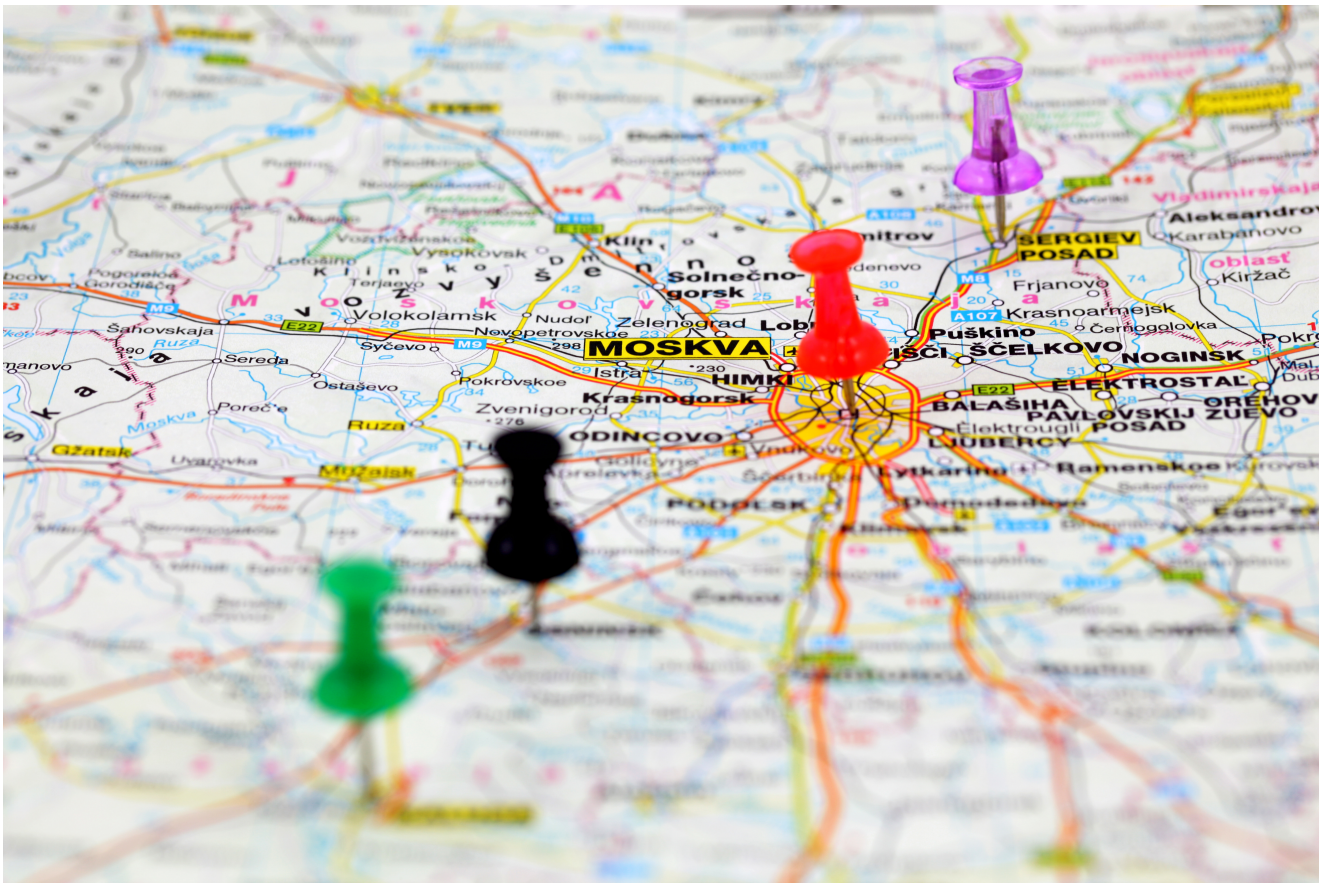
Russian cyber attack campaigns and actors

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

The latest: Microsoft reports that the Russian group behind SolarWinds attack, NOBELIUM, has struck again.



Oct 25, 2021

Editor's Note: This post, originally published on December 21, 2020, by Adam Hlavek with Kimberly Ortiz, includes updates dated March 1, April 6, 2021, May 28, 2021, and September 7, 2021.

Table of Contents

Most recent Russian cyber attack campaigns

APT29 Campaign Targeting European Diplomats with COVID-19 Lures

TLDR: ESET released a report [PDF] in early February stating that in October and November 2021, APT29 launched a spear-phishing campaign targeting European diplomatic missions and Ministries of Foreign Affairs.

More information: In the spearphishing emails, the APT29 threat actors impersonated the Iranian Ministry of Foreign Affairs and stated the Iranian embassy will be closed because of COVID-19. The goal was to target the diplomatic missions of EU countries and a Cobalt Strike Beacon on compromised systems.

Ukraine DDoS attacks

TLDR: On February 15, 2022, Ukraine's Center for Strategic Communications and Information Security reported that the Ministry of Defense and the Armed Forces of Ukraine and two of the country's state-owned banks, Privatbank (Ukraine's largest bank) and Oschadbank (the State Savings Bank), were hit by a "powerful DDoS attack on a number of information resources."

More information: The DDoS attacks consisted of three times more traffic than typically observed, 99% of which were HTTPs requests. The DDoS attacks caused interruptions in the sites of the Ukrainian Defense Ministry and the Armed Forces, and made bank customers unable to login to their online banking accounts. Privatbank's web application firewall (WAF) was also updated with a traffic geofencing rule, which automatically removed the site's contents for IP addresses outside of Ukraine and displayed a message reading: "BUSTED! PRIVATBANK WAF is watching you."

U.S. and U.K. governments recently linked the DDoS attacks to Russia's Main Intelligence Directorate, the GRU. They were able to attribute the attacks because GRU infrastructure was observed transmitting high volumes of communications to IP addresses and domains based in Ukraine. Luckily, the direct impact of these attacks are low. Though the availability of the data was temporarily compromised, the victims were able to quickly restore access within a few hours and no information was stolen or altered.

Russian Threat Actors Targeting U.S. Defense Contractors

TLDR: CISA, the NSA, and the FBI released an alert on February 16th that states from at least January 2020 through February 2022, Russian state-sponsored threat actors have regularly targeted U.S. cleared defense contractors (CDC) who support contracts for the Department of Defense (DoD) and the wider U.S. Intelligence Community.

More information: Over this two year period, the threat actors use common tactics, like spear-phishing, password spraying, and vulnerability exploitation, to gain access to CDC networks. They were able to maintain persistent access to numerous CDCs, in some cases for over six months. While having access, the threat actors were observed regularly and

repeatedly exfiltrating emails and data, through which they acquired "unclassified CDC-proprietary and export-controlled information." This gave the Russian actors insight into U.S. weapons platforms development and deployment timelines, plans for communications infrastructure, and military technologies, which can be used to inform Russian military and intelligence strategy.

APT29 Targeting of French Organizations

The French national cybersecurity agency ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) revealed that APT29 has been targeting French organizations in a number of phishing campaigns since February 2021.

The Russian threat actors compromised the email accounts of French organizations and leveraged the access to carry out spear-phishing campaigns aimed at foreign institutions. French government entities were also targeted by phishing emails sent from servers belonging to foreign entities, which were likely compromised by the same threat actor. APT29 used the spear-phishing emails to deliver a Cobalt Strike implant, and the infrastructure used in the attacks against French organizations was largely created using virtual private servers (VPS) from various providers.

Geopolitical

- In early December, President Biden and President Putin held a virtual meeting to discuss ways to defuse the growing military crisis along Ukraine's borders.

    Biden offered Putin the choice between a diplomatic solution and the severe economic and political consequences that would follow a Russian invasion of Ukraine, but there was no word of whether Putin had made any commitments.

- Twitter removes a network of 16 accounts linked to the IRA that attempted to introduce a pro-Russia viewpoint into Central African political discourse.

    Twitter also removes a network of 50 accounts that attacked the civilian Libyan government and actors that support it, while voicing significant support for Russia's geopolitical position in Libya and Syria.

- In early December, Indian Prime Minister Narendra Modi met with President Putin to discuss defense and trade relations as India has drawn closer to the U.S.

    Russia and India also signed a slew of bilateral defense agreements, including India's procurement of more than 600,000 assault rifles from Russia.

- In mid-December, Russia published draft security pacts, demanding that NATO deny membership to Ukraine and other ex-Soviet countries and roll back the deployment of troops and weapons in central and eastern Europe.

    > The documents also call for a ban on sending US and Russian warships and aircraft to areas from where they can attack each other's territory as well as a halt to NATO military drills near Russia's borders.

- In mid-December, President Putin and President Xi meet in a virtual summit, in which the two show solidarity in the face of contentions with the West.

    > Putin states a new model of cooperation has been formed between the countries, based, among other things, on such principles as non-interference in internal affairs and respect for each other's interests

- In late December, it is reported that U.S. and Russian officials will hold security talks on Jan. 10 to discuss concerns about their respective military activity and confront rising tensions over Ukraine

Renewed cyber attack on German parliament

A spokesperson for the foreign ministry in Berlin stated Russia is responsible for a renewed cyber attack on the German parliament. According to the EU, the attacks targeted "numerous members of Parliaments, government officials, etc. in the EU by accessing computer systems and personal accounts and stealing data." Germany's intelligence service warned in July that there had been "intensive attacks" by the Ghostwriter group since February, speculating that it could be preparing for "hack and leak" operations in which information is stolen to be published later on, either in its original form or doctored.

TinyTurla backdoor

TinyTurla is a "previously undiscovered" backdoor from the Turla APT group that has been used since at least 2020. This backdoor slips past malware detection systems because it's so simple. In other words, the backdoor code is extremely simple, but is efficient enough that it'll usually fly under the radar. TinyTurla was found to have been targeting the previous Afghan government as well as deployed on systems in the US and Germany. Researchers were able to spot the backdoor and attribute it to Turla because the group used the same infrastructure that it has used in previous attacks.

TinyTurla is used as a second-chance backdoor to maintain access to the system, even if the primary malware is removed. It could also be used as a second-stage dropper to infect the system with additional malware. The threat actors tried to operate under the radar by installing the backdoor as a service and naming it "Windows Time Service." Sporting the

ability to upload and execute files or exfiltrate files from the infected system, the backdoor contacted the C2 server via an HTTPS encrypted channel every 5 seconds to check if there were new commands from the operator.

Turla is pretty well-known and closely monitored by the security industry, but despite all this, they managed to use this backdoor for almost two years. This can serve as an argument for the need for network/behavior-based detection, such as IronNet's IronDefense, which would have detected the consistent beaconing used in this attack.

FoggyWeb Backdoor

Microsoft discovered a new piece of malware from APT29 - a post-exploitation backdoor called FoggyWeb. Observed in the wild as early as April 2021, this backdoor is passive, highly targeted, and capable of remotely exfiltrating sensitive information from a compromised AD FS server. It can also receive additional commands from a C2 server and execute them on the compromised server.

APT29 uses FoggyWeb to remotely exfiltrate the configuration database of compromised AD FS servers, and the backdoor configures HTTP listeners for actor-defined URIs that mimic the structure of the legitimate URIs that the target's AD FS deployment uses. The custom listeners passively monitor all incoming HTTP GET and POST requests sent to the AD FS server from the internet and intercept HTTP requests that match the custom URI patterns defined by the actor. Microsoft has notified all customers observed being targeted or compromised by FoggyWeb, as well as has recommended some mitigation tactics.

REvil ransomware gang strikes again

As mentioned in our analysis of the REvil shutdown, in July 2, 2021, the IT management software developer Kaseya Ltd. learned its VSA (Virtual System Administrator) was victim of one of the largest ransomware attacks in history. The Kaseya VSA is a common remote monitoring and management software used by MSPs (Managed Service Providers) to manage their clients' systems. Though Kaseya stated that fewer than 60 of its customers were directly breached, many of Kaseya's customers provide IT services to other businesses, leading to an estimated 800 and 1,500 downstream companies across the world being impacted.

This supply chain ransomware attack was carried out by the REvil ransomware gang, which claimed to have encrypted more than one million systems and demanded $50 million in ransom for a universal decryptor. REvil is an infamous Russia-based cybercrime syndicate responsible for several recent notable attack campaigns, including the recent ransomware attacks against Quanta Computer, Sol Oriens, Acer, and JBS. Operating under a ransomware-as-a-service (RaaS) model, REvil ranks first among most common ransomware variants with 14.2% of the total market share.

Influence campaign against the Polish government

In June 2021, the Polish government attributed a recent wave of cyberattacks to Russian Secret Services in which over 100 email and social media accounts of some of the most important Polish government officials from various political parties were targeted. Officials say this was part of a larger campaign that targeted over 4,350 accounts of various Polish public figures and citizens. The Russian hackers leaked emails and documents (some of which were reportedly altered) from the email inbox of Michał Dworczyk, the head of the Chancellery of the Polish Prime Minister's. Polish officials said the goal of this campaign was to "*hit Polish society and destabilize [the] country*." These attacks have been attributed to Russian UNC1151, which is connected to the wider Ghostwriter influence campaign, designed with the goal of destabilizing politics in Central Europe.

APT 28 / GRU Brute Force Attacks

In July 2021, the NSA, FBI, and CISA released a cybersecurity advisory [PDF] stating that since at least mid-2019 through early 2021, the GRU (aka APT28 or Fancy Bear) has carried out widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets in the US and worldwide. In this ongoing campaign, APT28 utilizes a Kubernetes cluster to conduct anonymized brute force access attempts routed through TOR and commercial VPN services. This brute force capability allows the actors to access protected data - including emails - and acquire account credentials, which can be used for many purposes, like gaining initial access, establishing persistence, escalating privileges, and evading defenses.

IronNet analysis of NOBELIUM activity

Microsoft has reported in a blog post that the same group behind the SolarWinds attack, revealed in December 2020, NOBELIUM, has struck again in the U.S., targeting about 3,000 email accounts at more than 150 different organizations.

IronNet analysis:

- The exploitation of a U.S. government email supplier by a Russian intelligence agency, allowing the agency to masquerade as a legitimate U.S. agency, appears to represent an important shift in Russian behavior.
- While the tactic of using phishing emails to obtain access and install malware on computers is hardly unique, the decision by the Russian SVR to represent itself as a legitimate U.S. government agency by exploiting an actual provider of services to the government demonstrates that Russia remains undeterred when it comes to going after the United States.

- This hack, which Microsoft reports is being conducted by the same players as the massive SolarWinds hack on U.S. government systems discussed over the past few months, could provide the Russians with sustained access to (and intelligence on) all sorts of third parties that the U.S. government works with through the U.S. Agency for International Development.
- This hack once again highlights how the exploitation of an organization in a company or government agency's supply chain entity can create risk not only for the company or agency itself but for its customers and partners as well.
- The hack therefore should also focus our attention on the importance — as highlighted in the Biden Administration's recent Executive Order — of organizations and their suppliers working closely together to share cyber threats information and collaborate in real-time on threats to provide for cyber collective defense of a supply chain.

Additional updates:

- Late-state SolarWinds / SUNBURST activity by actor dubbed NOBELIUM by the Microsoft Threat Intelligence Center.
- February 2021 exposure of new Sandworm APT attacks targeting IT companies using Centreon.
- Russian-Linked threat group "Gamaredon" conducts supply chain malware attacks against Ukraine.

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. Indeed, as the latest on the SolarWinds hack suggests, Russian cyber attacks are a real and present threat. This summary is very helpful for navigating the whirlwind of news surrounding the SolarWinds/SUNBURST attack.

Late-stage SolarWinds / SUNBURST activity

Three new pieces of malware being used in late-stage activity have been identified, with activity seen as early as June 2020. These are tailor-made for specific networks introduced after the actor has gained access. The threat actor has been observed using stolen creds to access cloud services like email and storage, as well as, VPNs and remote access tools. The Microsoft Threat Intelligence Center (MSTIC) has named the actor behind the attacks against SolarWinds, the SUNBURST backdoor, TEARDROP malware, and related components as NOBELIUM.

GoldMax

This malware was discovered persisting on networks as a scheduled task impersonating systems management software. The scheduled task was named after the software and pointed to a subfolder in ProgramData named after that software with a similar executable name.

- Malware is written in Go and acts as a C2 backdoor
- The C2 domains are high-reputation and are acquired from domain resellers or previously compromised domains. This tactic is used for OPSEC purposes because the purchased domains maintain their original creation date.

Sibot

This dual-purpose malware was implemented in VBScript designed to achieve persistence on the machine and then download and execute a payload from the C2 server. It reaches out to a legitimate but compromised website and places itself in system32/drivers.

GoldFinder

This malware acts as a custom HTTP tracer tool that logs the route that a packet traverses to reach the C2 server.

- This malware was written in Go - used a a custom HTTP tracer tool that logs the route that a packet traverses to reach the C2 server.
- When it attempts to reach the hardcoded C2 server, it will continue trying up to 99 times or until the redirects stop and GoldFinder receives a 200 request - whichever comes first.

SUNBURST tactics, techniques, and procedures

The threat actor used several sophisticated techniques to hide command and control traffic, such as mimicking SolarWinds' Orion traffic and leveraging infrastructure providers to masquerade as trusted geolocated environments.

While one of the distinctive network behaviors associated with SUNBURST that has been discussed by the cybersecurity community is command and control (C2) using Domain Generation Algorithm (DGA), it is our perspective at IronNet that this behavior more closely aligns with DNS tunneling. In fact, our initial detections of the SUNBURST C2 domain in early Summer 2020 were based upon our DNS tunneling analytic.

More than 18,000 SolarWinds customers downloaded the update that had the SUNBURST backdoor and were exposed. The actor then chose a much smaller set of companies and government agencies they wanted to exploit and downloaded a second set of tools and compromised those networks.

You can learn more about what we know, including analysis observations about SUNBURST TTPs from IronNet's SOC and threat researchers here.

Additional high-profile Russian cyber attack examples

Prior to the SolarWinds/SUNBURST attack, Russian cyber attacks have included the following:

- 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. grid.
- Targeting of COVID-19 research: In July 2020, the U.S., U.K., and Canada detailed Russian-driven cyber intrusion campaigns 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). In the case of the SolarWinds/SUNBURST attack, the gravity of this incident has yet to be determined.

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.

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.

Across cybersecurity communities, a deep dive into SUNBURST is ongoing and will yield additional insights over time. In historical instances, though, strategic Russian interests are guided by Russia's desire 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.

What does the Russian cyber attack threatscape look like?

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:

Ghostwriter

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 coronavirus 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.

The actors behind this campaign have successfully compromised legitimate websites (typically news sites) which they in turn use to post fabricated stories containing false or divisive narratives surrounding the alliance 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

Sandworm Team

In February 2021, an ANSSI report exposed new Sandworm APT attacks targeting IT companies using Centreon.

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.

In May 2020, the National Security Agency had 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 (known as the GTsST).

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 • 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

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 • 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 • 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 • Hiding malicious network activity by abusing legitimate services to host payloads or provide communication mediums for attackers • Deployingredundant backdoors within a network • 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 • Spearphishing emails with PDF attachments embedded with Adobe Flash exploits

Also Known As	Dragonfly, Crouching Yeti, Havex, Koala, Iron Liberty

DYMALLOY

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 intrusion 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.

In Spring 2020, it had come 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 and/or production / operational technology (OT) networks, presumably to allow for future operations.

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; 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

APT29

In late July 2021, RiskIQ identified nearly three dozen command-and-control (C2) servers under the control of APT29 actively serving WellMess and WellMail malware. APT29 uses WellMess in a highly targeted manner, making signs of the malware and its C2 servers relatively rare. RiskIQ began their investigation with a tweet mentioning possible IOCs associated with APT29 and WellMess. RiskIQ found several additional IP addresses and Certificates that closely matched the pattern found on the original IP address mentioned in the Tweet. Building on that, RiskIQ was able to link SSL Certificates you can see in the table on the slide and IP addresses to APT29 C2 infrastructure with high confidence.RiskIQ assesses with high confidence that these IP addresses and certificates are in active use by APT29, though they do not have enough information to say how it is being used or who the targets are.

On July 6th, 2021, it was reported that Synnex — a technology provider for the Republic National Committee (RNC) — was attacked by Russia's Foreign Intelligence Service (SVR). The SVR, also known as APT29 and Nobelium, used Synnex to gain access to high-value customer applications in the Microsoft cloud environment. However, the threat actors reportedly did not succeed in accessing sensitive RNC data through the breach.

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.

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

APT28

In August 2020, the FBI and the NSA released 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 US government to publicize and counter Russian cyber threats.

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 in order 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

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 • 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 • Obfuscated PowerShell scripts execute and connect to remote IP addresses for additional tool downloads • Lateral movement enabled through the use of Remote Desktop Protocol (RDP)
Also Known As	TEMP.MixMaster

Turla

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, 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.

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 • Waterholing government websites • Infecting removable storage devices • In-house complex malware development
AKA	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.

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.

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
Also Known As	TEMP.Veles

Gamaredon Group

The Russian-linked threat group "Gamaredon" has conducted a supply chain malware attacks against Ukraine. Gamaredon, also known as Primitive Bear, has been active since 2013 and has targeted Ukraine in many of its cyber operations before.

Firstly linking the attack to "one of the hacker spy groups from the Russian Federation," Ukraine's National Security and Defense Council (NSDC) later confirmed that the supply chain attack was the action of Gamaredon, sharing IoCs related to the attack, including an IP address and a domain. Ukraine accuses Gamaredon of attempting to deliver malicious documents containing macro code designed to install malware on target systems that would allow the attackers to control the compromised system remotely. The supply chain attack was targeted at the System of Electronic Interaction of Executive Bodies (SEI EB), which is used by government organizations to distribute documents to officials.

Of note:

- New evidence also suggests the Gamaredon is a hack-for-hire group that provides services to other APTs in addition to conducting its own separate activity as well. Gamaredon's modus operandi takes after that of second-tier APTs that delivers important information to top-tier, more advanced actors.
- What is interesting about this is that Gamaredon lives in a grey middle area between APTs and crimeware gangs. This brings up debate over whether Gamaredon is an APT or a crimeware gang. Using TTPs commonly employed in the crimeware world, like spam emails with malicious payloads and trojanized installers, along with having a diverse level of targeting, Gamaredon mimics the characteristics of crimeware gangs. However, its specific interest in Ukraine and lack of efforts to monetize stolen data has led it to be long considered as an APT.

An increase in activity from this group was observed in Spring 2020, indicating that Gamaredon, which has been active since at least 2013, is a ongoing threat to the Ukranian organizations they so brazenly appear to target. The Spring 2020 campaigns were highlighted by large waves of malicious emails directed against targets' and the group's use of new malware and TTPs.

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

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, backdoors, and other tools in an effort to appear legitimate • Rapid technical innovation for the purposes of detection evasion
Also Known As	Anunak, Carbon Spider, Carbanak

Russian cyber attack landscape: 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 they victimize, even many nations, cannot match.

Nearly all of the campaigns discussed here have been active within just the past several months. Just since May 2020, the U.S. government has publicly attributed multiple distinct campaigns and toolsets to specific Russia state-sponsored groups. While this is not the first time the U.S 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, 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, 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.

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.

.