Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation | Mandiant

By Mandiant

Published: 2022-03-04 · Archived: 2026-04-05 20:01:37 UTC

Written by: James Sadowski, Ryan Hall

Executive Summary

- Mandiant Threat Intelligence assesses with moderate confidence that Russia will conduct additional destructive or disruptive cyber attacks connected to the crisis in Ukraine. Russian cyber attacks almost certainly will focus first on Ukraine, with Western/NATO allies also being possible targets.
- Organizations making statements condemning Russian aggression and/or supporting Ukraine and organizations taking actions to restrict Russian participation in international commerce, competitions, and events face elevated risk of future reprisal.
- We assess that Sandworm and UNC2589 are two of the most likely actors to conduct cyber attacks in retaliation, although we judge that all high-profile Russian threat actors will continue or increase cyber espionage to enhance decision advantage against Ukrainian and NATO government targets.

Retaliatory Cyber Attacks Likely

Russia invaded Ukraine again on February 24, 2022, triggering international condemnation of their actions and a series of responses from U.S., NATO, and European Union (EU) allies, including widespread sanctions from Western governments on Russian banks and elites connected to the Putin regime. Mandiant observed multiple disruptive and destructive cyber attacks targeting Ukrainian government and private sectors, including the NEARMISS (aka HermeticWiper or FoxBlade) wiper attack on February 23, 2022, and the PAYWIPE (aka WhisperGate) wiper attack on January 15, 2022.

We anticipate that Russia could conduct retaliatory actions, including additional destructive or disruptive cyber attacks, particularly against the government, financial services, and energy and utilities sectors. The nature and length of NATO and Western sanctions and responses likely will heavily influence Russia's perception of high-priority targets for retaliation. **Organizations making public statements condemning Russian aggression and/or supporting Ukraine and organizations taking actions to restrict Russian participation in international commerce, competitions, and events face elevated risk of future reprisal.**

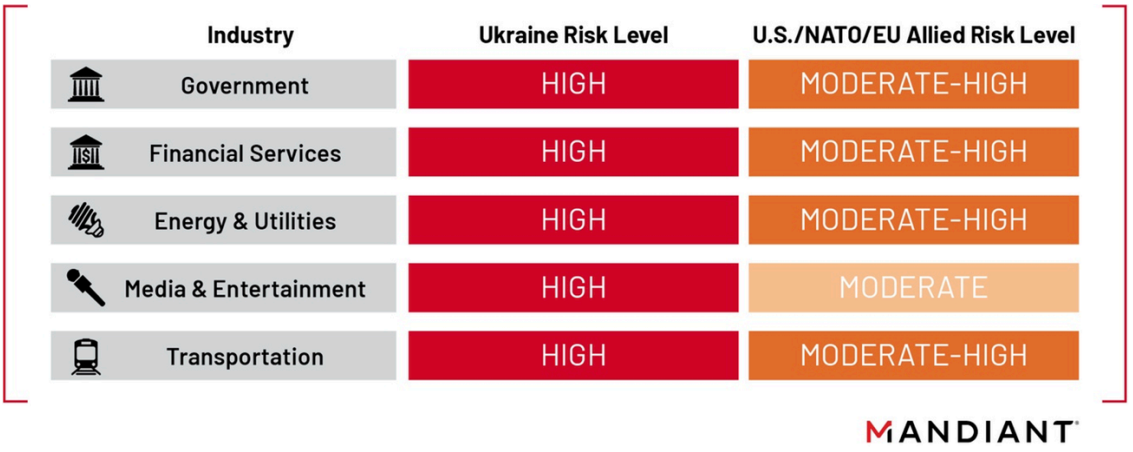

Figure 1: Sectors facing elevated risk from Russian cyber operations

For mitigation and hardening recommendations, please review our:

- Proactive Preparation and Hardening to Protect Against Destructive Attacks white paper
- Distributed Denial of Service (DDoS) Protection Recommendations white paper

Russian Decision Doctrine

Russian doctrine broadly follows a concept best described as "controlled escalation" or "escalation management/dominance," in which Russian forces gradually increase pressure, either through kinetic or non-kinetic methods, while gauging the adversarial reaction to each step until the adversary is willing to agree to favorable terms for Russia. In theory, Russia then is able to continue to escalate its operations only as far as necessary to achieve its desired outcome, relying on adversarial forces to back down first. This doctrine has sometimes been less accurately described as "escalate to de-escalate," suggesting that Russia will act in a significantly escalatory manner in order to achieve its goal, beyond the threshold an adversary would be willing to cross, in an attempt to prevent adversarial escalation or response.

Russian Information Warfare Doctrine

Russian doctrine also views information warfare as a wide-ranging concept crucial to any armed and/or diplomatic conflict. Russian information warfare combines cyber operations, electronic warfare, psychological operations, and information operations, with the ultimate goal of controlling the "information sphere"—a vital component of Russian strategy. In addition to using destructive and disruptive cyber attacks in advance of kinetic ones (such as those seen with PAYWIPE and NEARMISS), Russian doctrine calls for sustained information warfare throughout the conflict, both as a supplement to military action and as a component of the aforementioned controlled escalation.

Russia Likely to Respond to Western Sanctions

As one tool in its response, we assess that Russia will almost certainly engage its offensive cyber programs to at least increase cyber espionage against primarily government targets to enhance decision advantage, and likely also conduct additional destructive or disruptive cyber attacks.

- Russia will likely task at least APT28 and Sandworm to engage Ukraine in multiple ways, such as information operations, intelligence collection, and additional disruptive or destructive cyber attacks to degrade Ukraine's capabilities and supplement kinetic action.
- Other Russian state sponsored cyber espionage groups will—at a minimum—continue espionage activities against Ukraine and NATO-aligned nations. It is possible that Russian state sponsored operators will need to shift resources to focus on Ukraine and NATO-aligned nations during this conflict.
- Currently, we assess that APT29 does not have a destructive mandate, whereas at least Sandworm and TEMP.Isotope likely do. Although we have no evidence of this happening in any previous operations, it is possible, however, that even actors without a destructive mandate could be ordered to turn over their accesses to groups with a destructive mandate in a time of war.

Likely Threat Actors

Sandworm

Sandworm likely poses the greatest threat for destructive and disruptive attacks based on the group's historical targeting of and destructive operations against Ukraine, which included the use of BLACKENERGYv2, BLACKENERGYv3, and INDUSTROYER as well as the NotPetya fake ransomware. Now that Russia has invaded Ukraine, Sandworm, or another entity sponsored by the Russian General Staff Main Intelligence Directorate’s (GRU) Main Center for Special Technologies (GTsST), almost certainly is involved.

- Recently, the U.S. and UK governments attributed a sophisticated supply chain operation to Sandworm, although Sandworm had not used this network for destructive activity. Sandworm's disruptive operations have historically shown disregard or ignorance of potential secondary and tertiary affects. This, for example, led to NotPetya spreading well beyond Ukraine and causing billions of dollars of damage worldwide.

UNC2589

UNC2589 is a cyber espionage cluster active since at least early 2021 that has employed a consistent set of tactics, techniques, and procedures (TTPs). Its focus has been primarily in Ukraine and Georgia, but spearphishes have also been detected targeting Western European and North American foreign ministries, pharmaceutical companies, and financial sector entities. We assess UNC2589 also has a destructive mandate, based on UNC2589’s possession of the WARYLOOK (aka WhiteBlackCrypt) file corruptor.

UNC2589 has used a variety of publicly available and what appear to be proprietary malware. This group likely is at least partially a government-sponsored entity that we have observed conducting cyber espionage, but we have also observed UNC2589 using tools associated with criminal activity. In mid-January 2022, a disruptive attack wiped multiple Ukrainian government computers and defaced Ukrainian government websites. Malware used to launch the corruption tool has been used by UNC2589. The overlaps in malware and targeting means it is plausible that UNC2589 conducted these attacks, although we have not attributed that activity to UNC2589 at this time.

- The Ukrainian Government assesses this cluster is responsible for destructive activity undertaken against it, and they track this cluster as UAC0056.
- We identified UNC2589 infrastructure that hosted the WARYLOOK file corruptor in June 2021, which also indicates this actor has a destructive mandate. WARYLOOK (aka WhiteBlackCrypt) is a fake ransomware that has code overlap with SHADYLOOK (aka WhisperKill), the file corruptor used in the January 15 destructive attack on Ukrainian networks. SHADYLOOK was not fake ransomware but was deployed with PAYWIPE (aka WhisperGate), which was posing as ransomware.
- The attack on January 15 involved the use of GOOSECHASE (a subcomponent of WhisperGate) and FINETIDE (aka WhisperPack), both tools which we have observed UNC2589 also deploy. However, both GOOSECHASE and FINETIDE appear to have been used by multiple actors.

UNC3715

We currently track the actor responsible for the February 23 NEARMISS (aka HermeticWiper) wiper attack as UNC3715. Although we have not yet connected this group to other named actors that we track, this group may carry a broad destructive mandate as well, based on its deployment of NEARMISS. NEARMISS was notably more sophisticated and capable than PAYWIPE, which could indicate this group has more resources available to it or is a component of another actor we track.

TEMP.Isotope

Mandiant assesses that TEMP.Isotope also has a destructive mandate, although we have not observed this group use a tool capable of destruction. However, this group's choice of targets and data collection indicates an intent to conduct disruptive or destructive activities in the event they are tasked to do so. They have historically targeted primarily western Europe and North America, with a focus on energy, local governments, and transportation, but also have targeted water and other critical infrastructure facilities.

Criminal Actors

The Russian intelligence services almost certainly have the ability to coopt criminals residing within Russia in order to achieve their desired ends, although we assess the Kremlin primarily overlooks criminal operations as long as they refrain from targeting Russian domestic entities. In addition to financially motivated groups, hacktivist groups have also been conducting cyber operations in support of both Russia and Ukraine.

- We consider it plausible that Russia could seek to use criminal actors against NATO nations as a means of reprisal. Criminal actors that reside in Russia often target entities within NATO nations and we surmise that Russia could task them to conduct destructive or disruptive operations against financial entities, relying heavily on ransomware or wipers as the method of disruption. However, it is similarly possible they could use other disruptive or destructive methods.
- The CONTI ransomware group announced at the end of February that it would offer its "full support of Russian government" against the West, supposedly to help counteract Western aggression against Russia. Conti has reportedly also conducted targeting of journalists on behalf of the FSB.

Sandworm has historically used customized or generic versions of criminal tools and techniques in their operations, including their well-known employment of a modified BlackEnergy variant to disrupt the Ukrainian

power grid in 2015. In June 2017, Sandworm unleashed on Ukraine NotPetya, which was a destructive tool built off and masquerading as the Petya ransomware. The campaign appeared designed to closely mimic a financially motivated operation, likely in an attempt to obfuscate its true purpose serving Russian strategic interests in Ukraine. Both BlackEnergy and Petya source code had been leaked or was publicly accessible before Sandworm deployed their modified variants, although we cannot rule out that Sandworm might have engaged with the malware developers.

Russian Disruptive or Destructive Operations Against Financial Sector

Mandiant anticipates that Russian action against the financial sector outside of the conflict zone will include cyber espionage to gather information about implementation of Western and international sanctions. We expect that Russian cyber threat actors will continue to conduct disruptive operations and spread disinformation regarding the Ukrainian financial sector during the conflict. This activity may spill over to neighboring countries—like NotPetya did in 2017, resulting in billions of dollars in damage worldwide—or banking networks closely connected to Ukraine's, and in extreme cases, Russia could choose to conduct disruptive or destructive activity against financial sector organizations outside of Ukraine.

We assess that a destructive mandate has likely been assigned to at least Sandworm, TEMP.Isotope, and possibly UNC2589. We judge that although APT29 likely has the technical proficiency to create their own disruptive malware or the potential to purchase this malware from contract development teams such as those included in the SolarWinds sanctions, they likely do not have a disruptive or destructive mandate as they have not been observed conducting these operations or targeting critical infrastructure in preparation for disruptive or destructive activity.

Historically, Russia-sponsored targeting of financial entities has been relatively limited, though Mandiant has observed likely Russian malware called QUIETCANARY at a European financial entity in the last six months. However, some older activity and significant recent Russian-sponsored disinformation and disruptive operations targeted Ukrainian financial institutions, likely in an attempt to reduce the Ukrainian public's trust in its financial system.

If NATO elects to remove additional Russian entities from SWIFT or sanctions Russian entities that cross a Russian-perceived red line, Russia will likely respond, and could take action against NATO-aligned financial entities in a tit-for-tat response.

Energy Sector Also Likely Under Threat

We currently judge that if the NATO/Western response to Russia's invasion of Ukraine was perceived by Russian leadership as escalatory, Russia will likely seek to escalate in a manner that it deems proportional, without drawing NATO further into conflict.

- The decision to sanction Russian financial institutions as well as the cancellation of Nord Stream 2 is likely to lead to a Russian response. Russia likely has multiple options they could utilize as a part of their decision calculus, which could include energy cost hikes, destructive cyber operations, or other economic measures designed to hurt Europe more than Russia.

Possible Russian Responses

We judge there are two linked, viable measures Russia may choose to impose cost on NATO-affiliated countries that would be less likely to draw NATO further info conflict: directly raising the cost of Russian gas supplies to Europe and disruptive or destructive cyber operations against non-Russian organizations that supply gas to Europe.

- Due to Europe's reliance on Russian energy supplies, raising the cost of gas as a part of an incremental escalatory measure likely would cause NATO nations and their citizens distress, without offering NATO sufficient justification to draw them into the war. Higher gas prices concurrently could cause backlash against the elected government officials of NATO nations, potentially damaging their reputation and reducing their political leverage both abroad and at home.
- Russian cyber attacks on energy-related facilities outside of NATO nations—which would likely include Middle Eastern entities—could reduce the likelihood of a NATO response while simultaneously reducing NATO's leverage to respond to increased prices.
    - For example, Russian natural gas currently accounts for 40% of all of Europe's gas supplies. If Russia judges that raising prices is not an appropriate escalatory measure, Russia could undertake cyber attack operations against non-European suppliers as a means to raise gas prices and disrupt supply chains.

These two options could limit the likelihood of disruptive or destructive cyber attacks against NATO energy entities, as such operations are more likely to cause a significant escalatory response from NATO and the U.S. However, it increases the possibility that Russia could seek to conduct operations outside of NATO's purview.

Media and Entertainment Industry a Possible Target

Russia's ban from the Eurovision song contest, or the multiple sports organizations' decisions to cancel sporting events with Russian teams or move competitions to new locations that were formerly scheduled to take place in Russia, could also spur Russian retaliatory action against the media and entertainment sector. Russia has historically placed a premium on its competition in high-profile international sports and entertainment events and has previously used cyber operations to retaliate for perceived grievances.

As noted, Russian information warfare doctrine calls for control of the information sphere and, as a result, Ukrainian media organizations will likely also be targeted in both physical and cyber space to help disseminate fabricated pro-Russia content, such as allegations of the surrender of Ukrainian government or military forces, as well as to interrupt Ukrainian command and control and pro-Ukraine messaging.

- If Russian state media channels continue to be blocked widely, Russia likely will respond with symmetric action to close Western news sites in Russia. It is possible that Russia may take further action in cyberspace if they feel Western outlets can still successfully reach Russian audiences.

Notably, some of this type of activity likely will not be immediate; Russian cyber threat operators may begin planning and establishing access to targeted environments, but any public-facing leaks, disruptions, or influence campaigns are more likely to coincide with future sport or entertainment events to maximize the impact of the activity.

Olympic Athlete Doping Scandal

After the International Olympic Committee (IOC)-confirmed allegations of a widespread Russian state-sponsored doping program, many Russian athletes were banned from the 2016 Summer Games, initiating a series of "hack-and-leak" and information operations that Russia almost certainly intended as retaliation.

- Most notably under the guise of the "Fancy Bears' Hack Team," APT28 began a hack-and-leak campaign targeting the World Anti-Doping Agency (WADA) through major social media platforms and purpose-made websites. WADA had sponsored the original inquiry into Russian doping violations, which led to the 2016 ban. APT28 compromised WADA and other Olympic or sporting organizations networks during multiple operations from at least 2016–2018. In one instance, the Russian cutouts leaked the data of Western athletes who had been approved for medical exemptions for certain drug prescriptions, likely to portray these athletes as no better than the banned Russian athletes.

Russia was subsequently fully banned from the 2018 Winter Games, with a small number of Russian athletes allowed to compete under a neutral flag.

- In February 2018, Sandworm likely conducted the cyber attack on the Opening Ceremony at the Winter Olympics in Pyeongchang, South Korea. This attack was likely again in retribution for Russia's ban from the Games.

Transportation and Logistics Sector Also Faces Elevated Risk, Particularly Aviation

Multiple global transportation sector organizations have begun to withdraw services and support to Russian organizations and this drawback could spur Russian retaliation both in an effort to punish the organizations responsible as well as attempt to stop more organizations from isolating Russia further.

- Transportation and logistics giants like FedEx, UPS, and Maersk announced they would stop servicing Russian clients, cutting off major sources of global shipping and delivering to and from Russia.
- Aviation organizations may face particularly elevated risk, given the extensive impact these actions will have on both domestic and international Russian travel. Global reservations provider Sabre will no longer serve Russian carriers and both Boeing and Airbus announced they would cease providing support to Russian clients.
- Concurrently, destructive operations undertaken by Russian threat actors against other sectors may have secondary and tertiary effects against entities within the transportation sector similar to when NotPetya disrupted Maersk in 2017.

Russia likely lacks other forms of leverage against these organizations, so disruptive cyber operations are likely if Russia selects to retaliate against organizations in this sector. Russia has previously targeted the aviation industry, including a Russian cyber attack on Boryspil airport outside Kyiv and a compromise of a U.S.-based airport's systems.

Outlook and Implications

Russia will almost certainly continue to use cyber operations for a variety of reasons to include espionage, information operations, and disruptive or destructive measures. In the event a disruptive or destructive action is

selected, Russia is likely to task actors including Sandworm, UNC2589, UNC3715, and possibly TEMP.Isotope. Government, financial sector, energy and utility, and transportation and logistics organizations face elevated risk. Sandworm and UNC2589 are likely the most significant threats to NATO-aligned entities in the event Russia seeks retribution for perceived NATO escalation beyond Russian red lines, such as more Russian banks' removal from SWIFT, or continued lethal aid NATO partners are sharing with Ukrainian forces. Russia could also task criminal groups to conduct destructive or disruptive operations thereby muddying attribution while still responding to perceived NATO escalation.

Currently, it is difficult to predict how Russia's invasion of Ukraine might unfold and the consequences NATO will continue to seek to impose on Russia. However, sanctions like those against Russia's largest bank, Sberbank, and the potential for Russia's full removal from SWIFT may be red lines that will cause Russia to lash out at NATO-aligned organizations.

Posted in

- Threat Intelligence
- Security & Identity
