Anticipating Cyber Threats as the Ukraine Crisis Escalates

mandiant.com/resources/ukraine-crisis-cyber-threats

Blog

John Hultquist

Jan 20, 2022

6 mins read

Threat Research

Threat Intelligence

Ukraine

Russia

information operations

espionage

The crisis in Ukraine has already proven to be a catalyst for additional aggressive cyber activity that will likely increase as the situation deteriorates. At Mandiant, we have been anticipating this activity, and we are concerned that, unlike the recent defacements and destructive attacks, future activity will not be restricted to Ukrainian targets or the public sector.

The Scope of Activity

Russia and its allies will conduct cyber espionage, information operations, and disruptive cyber attacks during this crisis. Though cyber espionage is already a regular facet of global activity, as the situation deteriorates, we are likely to see more aggressive information operations and disruptive cyber attacks within and outside of Ukraine.

- Russian cyber espionage actors such as UNC2452, Turla, and APT28, which are tied to the Russian intelligence services, have almost certainly already received tasking to provide intelligence around the crisis. These actors already frequently target government, military, diplomatic, and related targets worldwide for intelligence that benefits Russia’s foreign policy decision making.
- Russia leverages a multitude of additional cyber espionage operators within the region, such as TEMP.Armageddon (UNC530), actors who operate out of occupied Crimea and Eastern Ukraine.
- Information operations, such as those involving the creation and dissemination of fabricated content and social media manipulation to promote desired narratives, are already happening within the context of the crisis. We continue to see pro-Russia actors, and those promoting narratives aligned with Russian interests, regularly conduct information operations against NATO allies and partners within Eastern Europe.
- Notably, a Ukrainian official has attributed recent defacements of Ukrainian government websites to UNC1151 (an actor we have linked to Belarus), though we cannot confirm this attribution. We have previously observed similar activity conducted by GRU-related actors Sandworm Team and APT28.

- Disruptive and destructive cyber attacks are relatively infrequent when compared to cyber espionage and other forms of information operations. Sandworm Team is Russia’s preeminent cyber attack capability, having conducted complex attacks which caused electrical outages in Ukraine as well as the most expensive destructive attack in history: NotPetya. Another actor, who Mandiant calls TEMP.Isotope (UNC806/UNC2486 aka Berserk Bear, Dragonfly), has a long history of compromising critical infrastructure in the United States and Europe. While we have never seen this actor attempt to disrupt that infrastructure, we believe these breaches are preparation for a contingency when Russia is prepared to cause serious disruptions.

Information Operations

Information operations are a regular feature of Russian and Belarusian cyber activity. Such actors leverage a variety of tactics to achieve their aims, including but not limited to the use of social media campaigns involving coordinated and inauthentic activity, as well as the compromise of entities in hack-and-leak operations or for use in disseminating fabricated content to promote desired narratives.

- Broadly speaking, information operations actors have sought to advance Russian interests by exploiting existing divisions within and between adversary countries, undermining confidence in democratic institutions, and creating distrust within the NATO alliance, the European Union, and the West.
- Fabricated content, such as forged documents, doctored photographs and fake petitions, is regularly used in operations we have attributed to influence campaigns, including Ghostwriter and Secondary Infektion.
- Data obtained through intrusion activity has been leaked to great effect, causing scandals with lasting consequences. We have observed pro-Russia actors alter or falsify stolen data prior to leaking it, occasionally alongside unaltered data, to support a given operation’s intended narrative.
- Information operations actors have used third parties, such as journalists and "hacktivists,” to legitimize information and narratives and launder their content. While many such parties collaborated—wittingly or unwittingly—with those actors, we have also observed campaigns, such as Ghostwriter, supported by the cyber espionage actor UNC1151, compromise and leverage legitimate information sources. This includes news or municipal government sites or social media accounts to disseminate material.
- Russian information operations campaigns, such as those conducted by the Internet Research Agency, have also created and leveraged inauthentic personas and media outlets to publish and promote content disseminating false narratives that serve to achieve their ends.

Cyber Attacks

Disruptive and destructive cyber attacks take many forms, from distributed denial-of-service attacks to complex attacks on critical infrastructure. Like its peers, Russia leverages this capability in times of crisis.

- Successful disruptions are often a matter of scale. The most effective disruptions have broad effects. To achieve this, operators can focus on disrupting critical targets with downstream customers and dependencies (such as the Ukrainian electric grid), or directly disrupt a multitude of targets (as in the case of NotPetya).
- Attacks against critical infrastructure and operational technology networks may take more hands-on work and lead time than other methods. Actors such as TEMP.Isotope appear to take a proactive stance towards compromising these targets. As such, targets of this nature may have been compromised well in advance of this crisis for the purposes of a contingency such as this. Defenders of these networks should consider hunting for actors such as TEMP.Isotope.
- Alternatively, destructive tools and other simpler methods could be leveraged against a large cohort of targets simultaneously. Typically, Russian actors have used strategic web compromise and the software supply chain to gain access at this scale. Mass propagation through these methods may be early warning of impending cyber attack.
- The perpetrators of attacks often fabricate evidence of culpability or make false statements of responsibility designed to suggest that some other party is responsible for the incident. They plant evidence in code and make public statements that suggest incidents were carried out by previously unknown nationalist elements, criminals, or government hackers. On multiple occasions, wipers have masqueraded as ransomware, as in the case of the most recent incident in Ukraine. Though these “false flags” are often paper-thin, they complicate efforts to convince the public of attribution and make these operations more deniable.
- Ransomware is a form of cyber attack that is being used by state affiliated actors as part of “lock and leak” campaigns that have dubious financial motivations. Because of its mature criminal underground, Russia has unmatched access to this capability. The security services have previously leveraged criminal operations for national security purposes and could bring them to bear in any number of ways to carry out their mission.
- Though destructive attacks observed thus far in this crisis appear to have focused on government systems, civilian systems are usually targeted to greatest effect. These actors have had particular success targeting utilities, but also by targeting transportation and logistics, finance, and media.
- Cyber attacks are most often leveraged as a form of information operation, meaning they are meant to manipulate perception rather than have lasting disruptive effects. Defenders often overestimate the technical capability necessary for these actors to achieve their goals and underestimate the value of technically simple operations.

Outlook

Cyber capabilities are a means for states to compete for political, economic, and military advantage without the violence and irreversible damage that is likely to escalate to open conflict. While information operations and cyber attacks such as the 2016 US election operations and the NotPetya incident can have serious political and economic consequences, Russia may favor them because they can reasonably expect that these operations will not lead to a major escalation in conflict.

Mandiant recommends that defenders take proactive steps to harden their networks against and has provided a guide to this process, *Proactive Preparation and Hardening to Protect Against Destructive Attacks*, for free to the public.

Free access to Mandiant Advantage is also available for qualifying organizations. With access to this platform, users can obtain additional detailed information from Mandiant’s intelligence operations that have not yet been publicly released.