

Special Report: Ukraine

An overview of Russia's cyberattack activity in Ukraine

Cyberattacks in Ukraine

This report details the cyber activity Microsoft has observed as part of the war in Ukraine, and the work we have done in collaboration with Ukrainian cybersecurity officials and private sector enterprises to defend against cyberattacks. Microsoft's ongoing, daily engagement establishes that the cyber component of Russia's assault on Ukraine has been destructive and relentless. The purpose of this report is to provide insights into the scope, scale, and methods of Russia's use of cyber capabilities as part of the largescale "hybrid" war in Ukraine, to acknowledge the work of organizations in Ukraine defending against persistent adversaries, and to provide strategic recommendations to organizations worldwide.

Throughout this conflict, we have observed Russian nation state cyber actors conducting intrusions in concert with kinetic military action.

At least six Russian Advanced Persistent Threat (APT) actors and other unattributed threats, have conducted destructive attacks, espionage operations, or both, while Russian military forces attack the country by land, air, and sea. It is unclear whether computer network operators and physical forces are just independently pursuing a common set of priorities or actively coordinating. However, collectively, the cyber and kinetic actions work to disrupt or degrade Ukrainian government and military functions and undermine the public's trust in those same institutions.

Destructive attacks have been a prominent component of Russian cyber operations during conflict.

A day before the military invasion, operators associated with the GRU, Russia's military intelligence service, launched destructive wiper attacks on hundreds of systems in Ukrainian government, IT, energy, and financial organizations. Since then, the activity we have observed has included attempts to destroy, disrupt, or infiltrate networks of government agencies, and a wide range of critical infrastructure organizations, which Russian military forces have in some cases targeted with ground attacks and missile strikes. These network operations have at times not only degraded the functions of the targeted organizations but sought to disrupt citizens' access to reliable information and critical life services, and to shake confidence in the country's leadership.

Russian military views on information warfare

The Russian military defines information warfare as "confrontation in the information space with the goal of causing damage to critical information systems, undermining political, economic, and social systems, psychologically manipulating the public to destabilize the state and coerce the state to make decisions to benefit the adversary party", according to public Defense Ministry documents.¹ The collective comments of several former Russian military officials, including a former Chief of the General Staff, suggest a view that operations to degrade troop morale, discredit the leadership, and undermine the military and economic potential of the enemy via information means can at times be more effective than traditional weapons.²

Based on Russian military goals for information warfare, these actions are likely aimed at undermining Ukraine's political will and ability to continue the fight, while facilitating collection of intelligence that could provide tactical or strategic advantages to Russian forces. Through our engagements with customers in Ukraine, we have observed that Russia's computer-enabled efforts have had an impact in terms of technical disruption of services and causing a chaotic information environment, but Microsoft is not able to evaluate their broader strategic impact.

¹ Conceptual Views of the Armed Forces of the Russian Federation's Action in Information Space, 2011

² <https://ria.ru/20170222/1488617708.html>

Microsoft's engagement

Microsoft security teams have worked closely with Ukrainian government officials and cybersecurity staff at government organizations and private enterprises to identify and remediate threat activity against Ukrainian networks. In January, the Microsoft Threat Intelligence Center (MSTIC) discovered wiper malware in more than a dozen networks in Ukraine. We alerted the Ukrainian government and published our findings.³ Following that incident, we established a secure line of communication with key cyber officials in Ukraine to be sure that moving forward, we were working with trusted experts to help Ukrainian government agencies, enterprises, and organizations defend against attacks.

This focused engagement combined with our unique view into affected systems has offered insights into Russian cyber targets, tactics, and procedures so far, and provided new insights on how to approach network defense for customers embroiled in military conflict.

Based on our observations, known and suspected Russian nation-state actors are working to compromise organizations in regions across Ukraine. These actors use a variety of techniques to gain initial access to their targets, including phishing campaigns, exploiting unpatched vulnerabilities in on-premises Exchange servers, and compromising upstream IT service providers. This initial access allows them to conduct operations for destruction, data exfiltration, and persistence for longer-term espionage and surveillance.

Threat groups with known or suspected ties to the GRU have continuously developed and used destructive wiper malware or similarly destructive tools on targeted Ukrainian networks at a pace of two to three incidents a week since the eve of invasion. From February 23 to April 8, we saw evidence of nearly 40 discrete destructive attacks that permanently destroyed files in hundreds of systems across dozens of organizations in Ukraine.

Tracked malware families leveraged for destructive activity

- WhisperGate / WhisperKill
- FoxBlade, aka Hermetic Wiper
- SonicVote, aka HermeticRansom
- CaddyWiper
- DesertBlade
- Industroyer2
- Lasainraw, aka IssacWiper
- FiberLake, aka DoubleZero

WhisperGate, FoxBlade, DesertBlade, and CaddyWiper are all malware families that overwrite data and render machines unbootable. FiberLake is a .NET capability being used for data deletion. SonicVote is a file encryptor sometimes used together with FoxBlade. Industroyer2 specifically targets operational technology to achieve physical effects in industrial production and processes.

³ <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>;
<https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/>

Destructive attacks in Ukraine

More than 40% of the destructive attacks were aimed at organizations in critical infrastructure sectors that could have negative second-order effects on the government, military, economy, and people. Thirty-two percent of destructive incidents affected Ukrainian government organizations at the national, regional, and city levels. Microsoft has also observed that the threat actors are slightly modifying the malware to evade detection with each wave of deployment.

Acknowledging that there is ongoing activity that we cannot see, we estimate there have been at least eight destructive malware families deployed on Ukrainian networks, including one tailored to industrial control systems (ICS). If threat actors can maintain the current pace of development and deployment, we anticipate more destructive malware will be discovered as the conflict continues.

Detected destructive cyberattacks in Ukraine by week

Week 1 (February 23-March 2)	Destructive malware: FoxBlade, Lasainraw (IsaacWiper), DesertBlade, malicious use of SecureDelete utility Number of destructive incidents: 22
Week 2 (March 3-9)	Destructive malware: none Number of destructive incidents: 0
Week 3 (March 10-16)	Destructive malware: FoxBlade, malicious use of SecureDelete utility Number of destructive incidents: 4
Week 4 (March 17-23)	Destructive malware: DesertBlade, FiberLake, SonicVote, malicious use of SecureDelete utility Number of destructive incidents: 6
Week 5 (March 24-30)	Destructive malware: FoxBlade, SonicVote, malicious use of SecureDelete utility Number of destructive incidents: 3
Week 6 and beyond (March 31-April 8)	Destructive malware: CaddyWiper, Industroyer2 Number of destructive incidents: 2

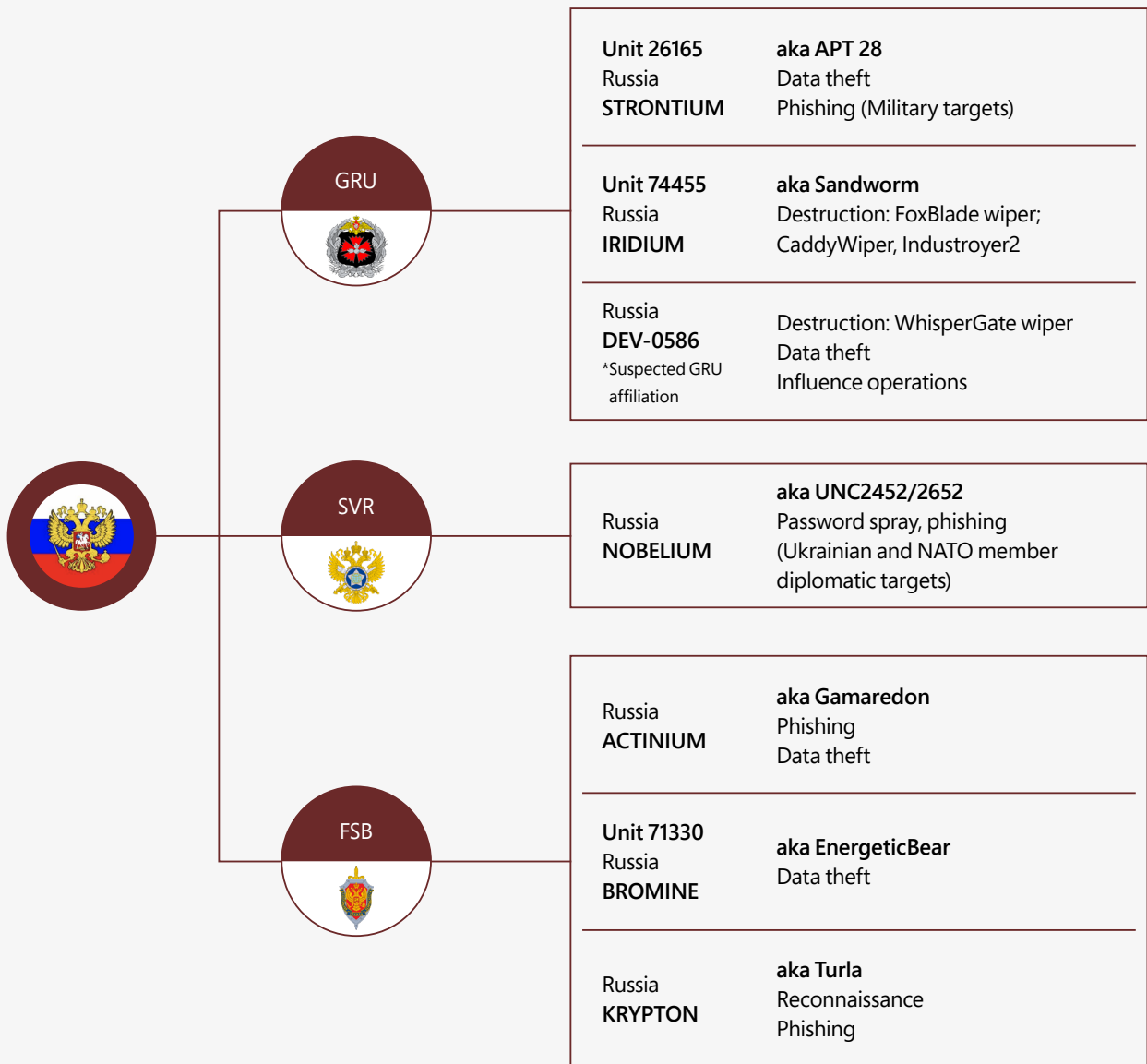
Destructive incidents are counted by organization not by impacted systems. Malware may have destroyed data across multiple systems at a single organization, but we count that as one destructive incident.

Known and suspected Russian threat actors deployed malware and abused legitimate utilities 37 times to destroy data on targeted systems. SecureDelete is a legitimate Windows utility that threat actors abused to permanently delete data from targeted devices.

Russian preparation for war

Microsoft assesses that Russia-aligned threat groups were pre-positioning for conflict as early as March 2021, when threat actors that had sporadically targeted Ukraine in the past started to conduct more actions against organizations inside or allied with Ukraine. While we cannot speak to the level of

coordination between disparate threat groups, combined, their activities appeared aimed at securing persistent access for strategic and battlefield intelligence collection or to facilitate future destructive attacks in Ukraine during military conflict.



This graphic is a snapshot of Russian cyber threat actors MSTIC observed executing operations specifically against Ukrainian targets before the invasion and examples of their activities. Ukrainian military and cyber responders have been dealing with Russian aggression since at least the first Russian invasion in 2014, making it difficult to identify an exact time when long-term espionage may have shifted to support invasion preparation.

Sought access to insights on Ukrainian defense and foreign partnerships.

In early 2021, when Russian troops first started to move *en masse* toward the border with Ukraine, we saw efforts to gain initial access to targets that could provide intelligence on Ukraine’s military and foreign partnerships. Russian actor NOBELIUM launched a large-scale phishing campaign against Ukrainian interests involved in rallying international support against Russian actions. Similarly, DEV-0257 (publicly known as Ghostwriter) began phishing campaigns attempting to gain access to Ukrainian military email accounts and networks.

Positioned themselves for third-party attacks on networks in Ukraine and partner nations.

By mid-2021, Microsoft observed known and suspected Russian threat actors separately targeting supply chain vendors in Ukraine and abroad to secure accesses and pre-position for future third-party intrusions against Ukraine and its partners in NATO. DEV-0586, a previously unknown group with suspected Russian military ties, had compromised the network of an IT firm that built resource management systems for Ukraine’s Ministry of Defense and organizations in the communications and transportation sectors.

NOBELIUM attempted to access IT firms serving government customers in predominantly NATO member states, at times successfully compromising then leveraging privileged accounts to breach and steal data from Western foreign policy organizations. Beyond broader value derived from what appear to be traditional espionage operations, persistent access to foreign policy organizations in NATO member states could provide Russian leadership continuous insights on what to expect from the West in response to Russian actions in Ukraine. Roughly 93% of all Russia-backed attack activity observed in our online services was aimed at NATO member states, particularly against the United States, the United Kingdom, Norway, Germany, and Turkey through 2021.

Sought access to insights on military and humanitarian response capabilities.

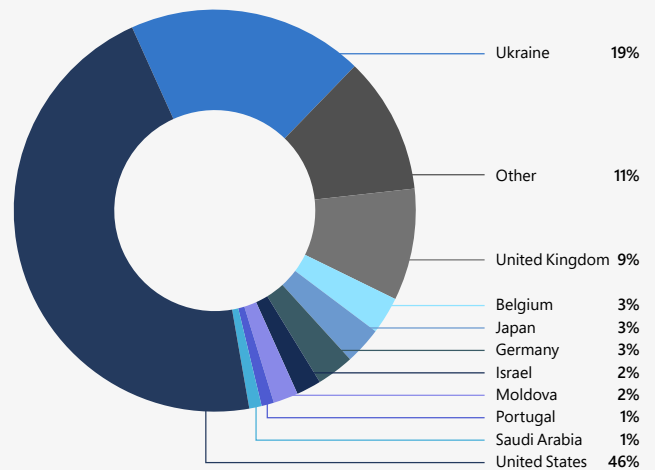
As 2021 progressed, threat actors representing multiple Russian government security services converged on Ukraine to surveil or compromise organizations that could provide valuable intelligence on a Ukrainian military, diplomatic, or humanitarian

response to Russian military action. ACTINIUM launched spear-phishing campaigns to gain access to accounts of Ukraine-based foreign military advisors and humanitarian workers, in August. Around the same time, STRONTIUM attempted to compromise defense-related organizations in Ukraine. ACTINIUM, NOBELIUM, BROMINE, SEABORGIUM, and DEV-0257 sought persistent access to their particular interests among a total target pool that included Ukrainian defense, defense industrial base, foreign policy, national and local administration, law enforcement, and humanitarian organizations.

Secured access to critical infrastructure for future destruction.

Threat actors also established the access and persistence on networks for future destructive attacks. In late 2021, suspected Russian cyber actors positioned themselves in networks of Ukrainian energy and IT providers that were later targets of destructive attacks, including Kitsoft, the IT service provider that DEV-0586 compromised to facilitate destruction on the networks of several clients in January 2022.⁴

Most targeted countries (July 2020 to June 2021)



The chart above represents the geographic distribution of customers notified of all nation state threat activity, not just Russian, between July 1, 2020, and June 30, 2021. By June 2021, Ukraine was the second-most impacted country we observed, reflecting 19% of all notifications of nation-state threat activity that we provided to customers during that time, largely due to the ramp up of Russian activity.

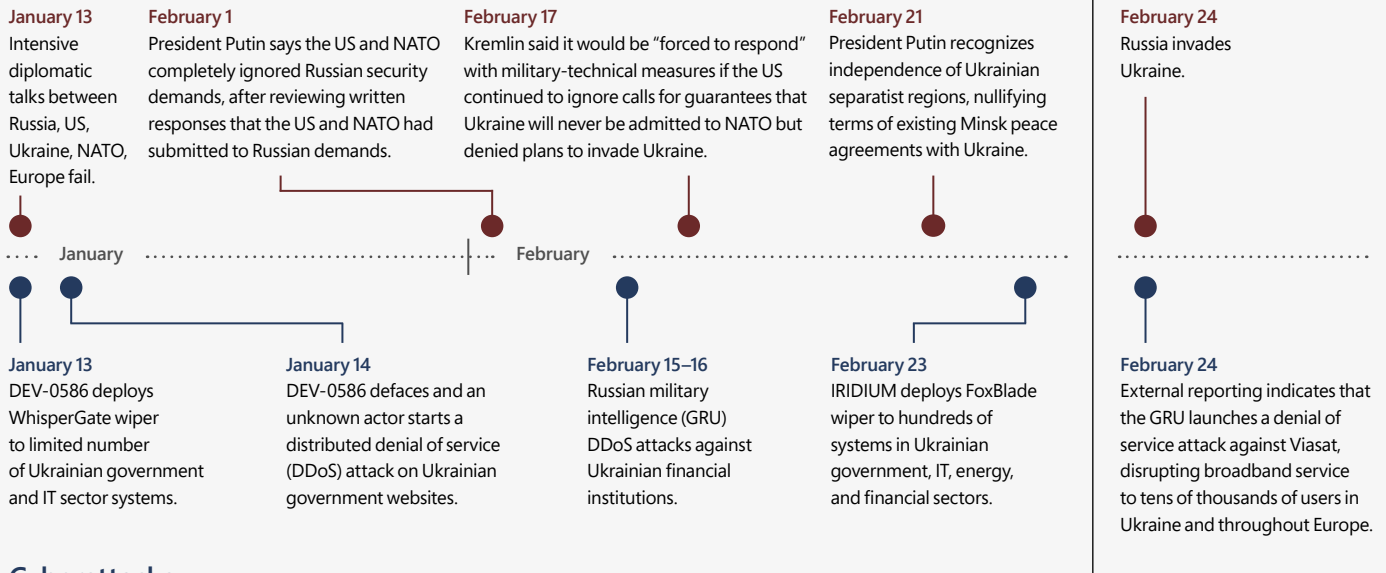
⁴ <https://www.cnn.com/2022/01/14/europe/ukraine-cyber-attack-government-intl/index.html>; <https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r>

Destructive attacks signal imminent invasion

In early 2022, when diplomatic efforts failed to de-escalate mounting tensions around Russia’s military build-up along Ukraine’s borders, Russian threat actors launched destructive wiper malware attacks against Ukrainian organizations with increasing intensity. These efforts signaled that Russian actions in Ukraine had entered a destructive phase that could escalate further. In early January, DEV-0586 launched WhisperGate⁵

malware which sought and deleted selected file extensions and then manipulated the Master Boot Record (MBR) to render targeted machines inoperable. This destructive malware impacted a limited number of government and IT sector systems, which coupled with the defacement of Ukrainian government websites in February, may have served as warnings intended to prompt Ukrainian concessions.

Political-military events



Cyberattacks

Pre-invasion timeline indicates Russian threat actors launched increasingly disruptive and visible cyberattacks against Ukraine on the heels of major diplomatic failures related to the conflict.

Cyberattacks intensified on the eve of the Russian invasion, when IRIDIUM deployed FoxBlade⁶ (aka HermeticWiper) malware to destroy roughly 300 systems across more than a dozen government, IT, energy, agricultural, and financial sector organizations in Ukraine. Unlike IRIDIUM’s NotPetya worm,

FoxBlade deployment was tailored to specific environments. Once deployed, it moves quickly to impact all domain-joined devices within a targeted organization.

⁵ <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>

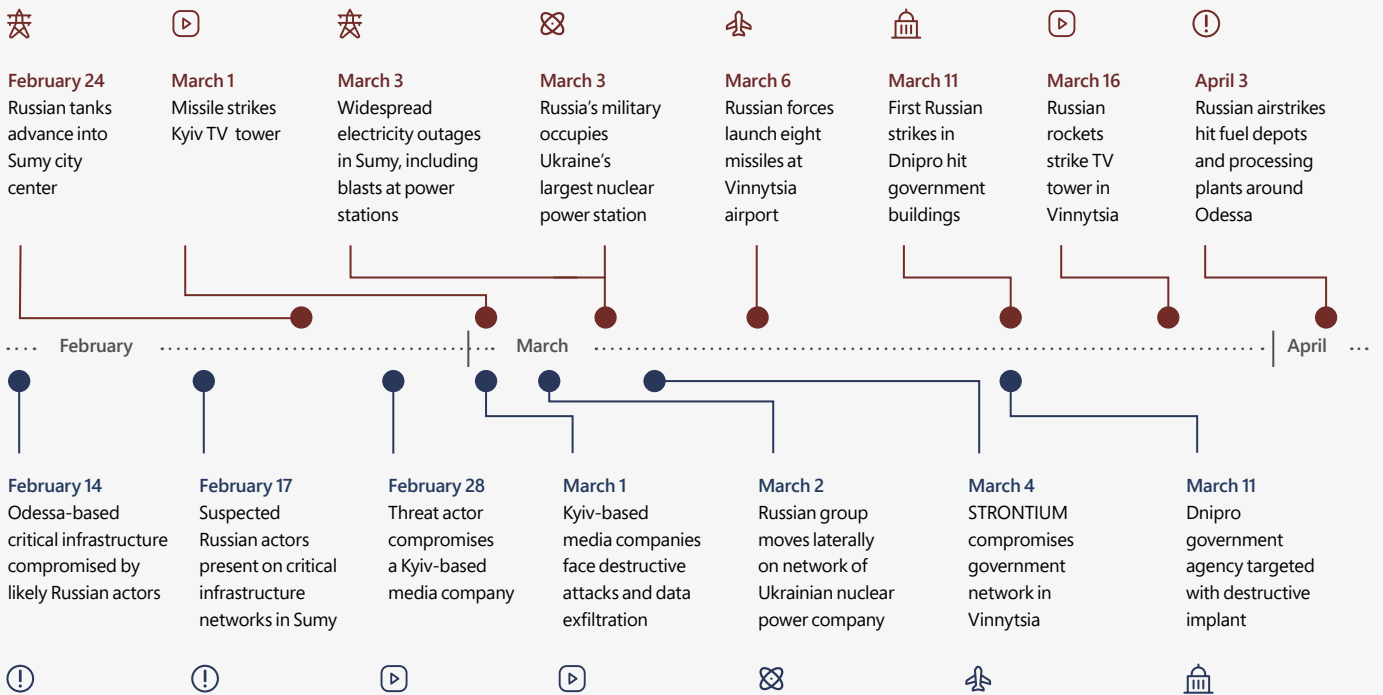
⁶ <https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/>

Russia invades Ukraine

Since the beginning of Russia’s invasion of Ukraine on February 24, Microsoft has observed Russian cyber threat groups performing actions in support of their military’s strategic and tactical objectives. A timeline of military strikes and cyber intrusions shows several examples of computer network operations and military operations seeming to work in tandem against a shared target set, though it is unclear if there is coordination, centralized tasking or merely a common set of understood priorities driving the correlation. At times, computer network attacks immediately preceded a military attack, but those instances have been rare from our perspective. The cyber operations so far have been consistent with actions to degrade, disrupt, or discredit Ukrainian government, military, and economic functions, secure footholds in critical infrastructure, and to reduce the Ukrainian public’s access to information.

A note on attribution:
 MSTIC assesses with moderate confidence that IRIDIUM, an activity group that the US Government has attributed to the GRU Main Center for Special Technologies (Unit 74455), is linked to intrusion activity leading to the deployment of FoxBlade, CaddyWiper, and Industroyer2 in Ukraine.

Military strikes



Cyber intrusions or attacks

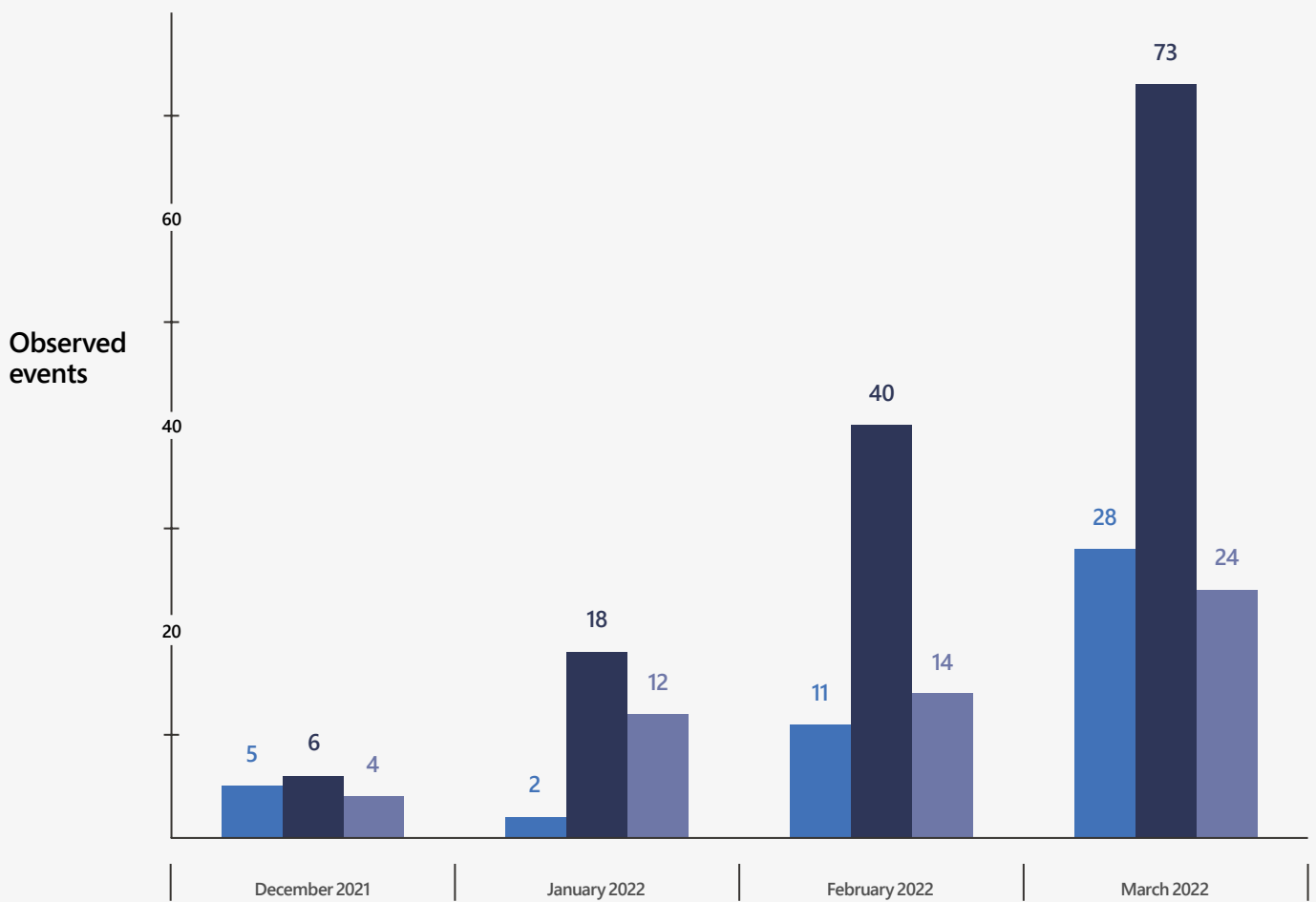
- Legend:
- ⚠ Critical Infrastructure
 - ⚡ Electrical Infrastructure
 - ☢ Nuclear Energy
 - 🚂 Transportation
 - 📺 Media
 - 🏛 Government

Multiple threat actors involved

At least six known or suspected Russian cyber threat groups in addition to other unattributed threat actors are engaged in activities that range from reconnaissance and phishing for initial access to pervasive lateral movement, data theft,

and data deletion. The multiple phases of their operations suggest these actors are positioning themselves for continued compromises and impact on Ukrainian networks for the duration of this conflict and beyond.

Stages of Russian cyber operations in Ukraine since December



Legend:

- Tooling and Reconnaissance
- Actions on Network
- Actions on Objectives (Data Exfil/Destruction)

Russian cyber operations against Ukrainian organizations grew significantly leading up to and following Moscow's invasion. That growth occurred across the full spectrum of cyber operations from research and tool preparation ("Tooling and Reconnaissance") to gaining access, establishing persistence, and lateral movement ("Actions on Network") to exfiltration and destruction of data ("Actions on Objectives"), with 237 such events in total during this period. We did not include activity in Russian-annexed Crimea in our analysis.





Cyber operations complement kinetic action

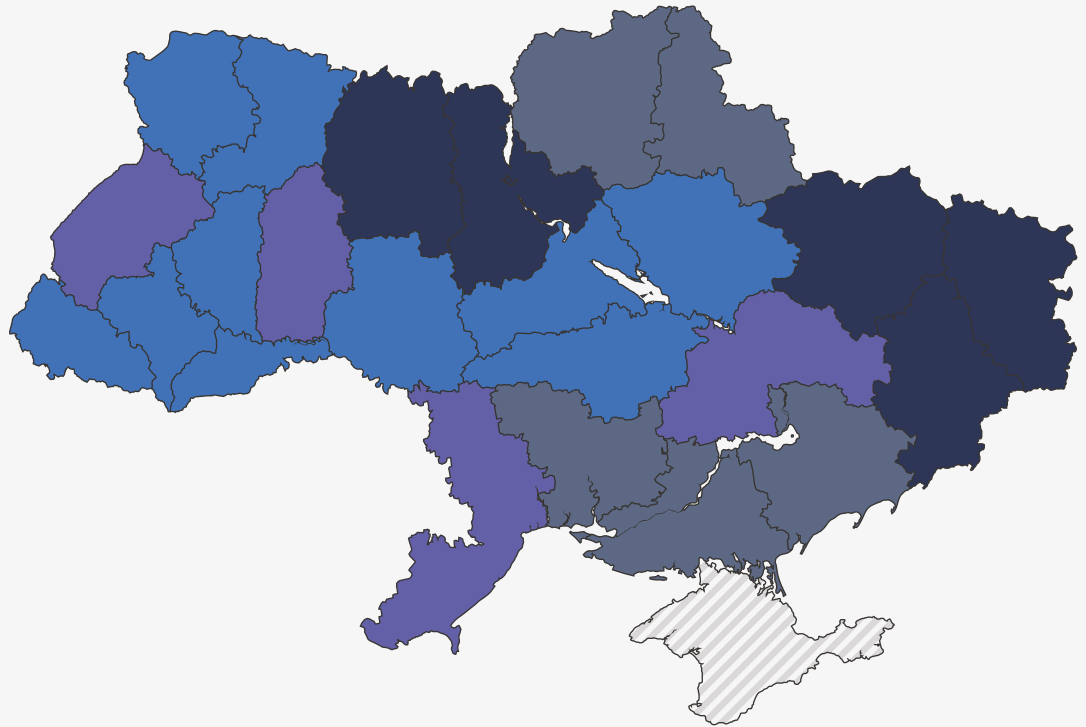
Based on our direct engagement with impacted entities in Ukraine, we observed that cyber and kinetic military operations appeared to be directed toward similar military objectives. Threat activity groups often targeted the same sectors or geographic locations around the same time as

kinetic military events. Analysis of Microsoft signals with open-source kinetic attack data shows high concentrations of malicious network activity frequently overlapped with high-intensity fighting during the first six plus weeks of the invasion. (see map of Kinetic and cyber activity).

Kinetic and cyber activity

Legend:

-  High kinetic/high cyber
-  High kinetic/low cyber
-  Low kinetic/high cyber
-  Low kinetic/low cyber



High kinetic:

Regions which reflect more than 90% of daily reported Russian physical attacks in the data sources.

High cyber:

Regions which reflect more than 80% of daily detected and blocked actor indicators in Microsoft Defender Antivirus.

Time frame:

February 23 through April 6.

Data sources:

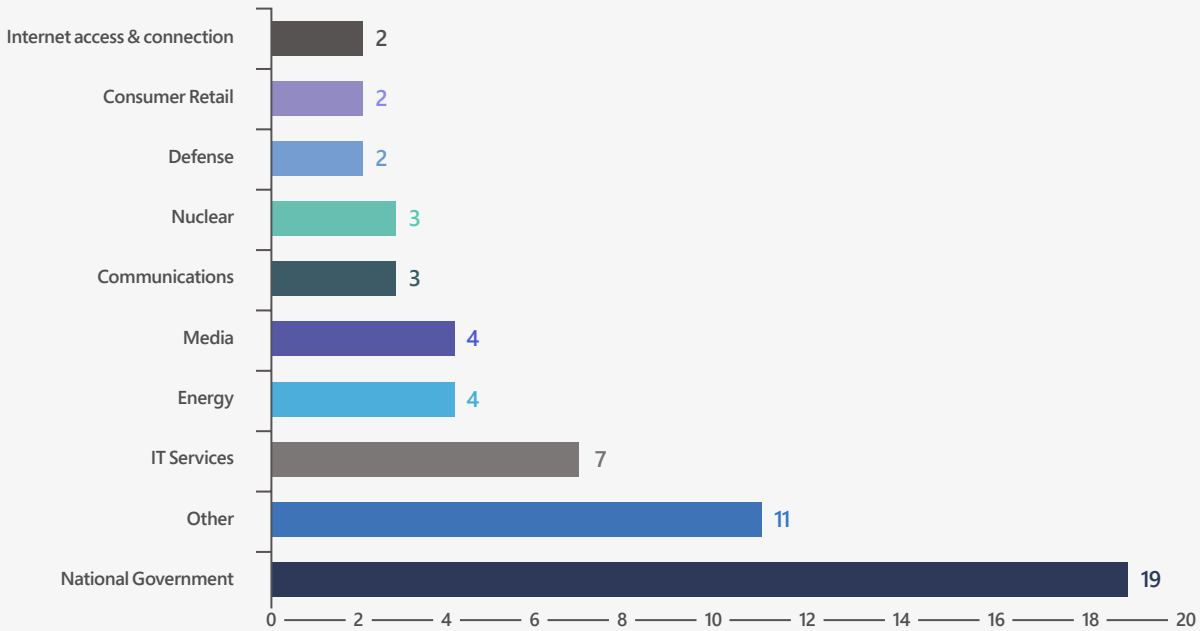
Detected and blocked activity by Microsoft Defender Antivirus based on known actor indicators; open source data on kinetic attacks from the Armed Conflict Location and Event Data Project and the Centre for Information Resilience. Russian-occupied Crimea was excluded from this analysis.

The war by week

The following week-by-week analysis provides a more granular view of the threat activity we observed in the context of Russian military operations to highlight consistent cyber-kinetic congruence in the conflict. The insights are derived

from a limited dataset, and our understanding of the threat actors and their objectives is likely to change as the conflict and our investigations continue. This initial view should serve as a starting reference for continued analytic work.

Sample set of targets by industry



This chart provides a sample of Ukrainian industries impacted by known or suspected Russia-aligned network intrusions or destructive attacks during the Russian invasion of Ukraine. National government organizations and critical infrastructure sectors were top targets. The "Other" percentage represents 11 other categories of impacted organizations including regional and city-level government, agriculture, defense industrial base, healthcare, transportation, and finance, among others.

WEEK 1 (Feb 23 - Mar 2):

Suspected Russian threat actors and Russian troops have attempted to control the information environment in Ukraine since the beginning of the conflict. During the first week of the invasion, suspected Russian threat actors launched DesertBlade against a major broadcasting company on March 1, the same day that the Russian military announced its intention to destroy “disinformation” targets in Ukraine and directed a missile strike against a TV tower in Kyiv.⁷ DesertBlade actions and the missile strike demonstrated cyber and kinetic impact to a key source of information to the Ukrainian public.

- The Institute for War and Peace Reporting reported that the first thing that Russian troops did when they captured the southern city of Berdyansk on 27 February was to occupy the TV tower⁸ and turn off all broadcasts, underscoring broadcast and information control as a key kinetic and cyber military objective. Attempts to compromise and or stage destructive malware on media companies is a trend that has continued throughout this conflict.

IRIDIUM conducted operations against Ukrainian economic targets, in line with Russian military objectives to degrade an adversary’s economy.

- IRIDIUM staged a file encryptor on the network of an agricultural firm, holding this entity at risk for future destruction. Microsoft assesses that this was likely targeting grain production, a major export commodity in Ukraine’s economy. As of early April, the World Bank predicted the war would shrink Ukraine’s economy by 45.1% this year in part by destroying infrastructure and choking of imports and exports.⁹

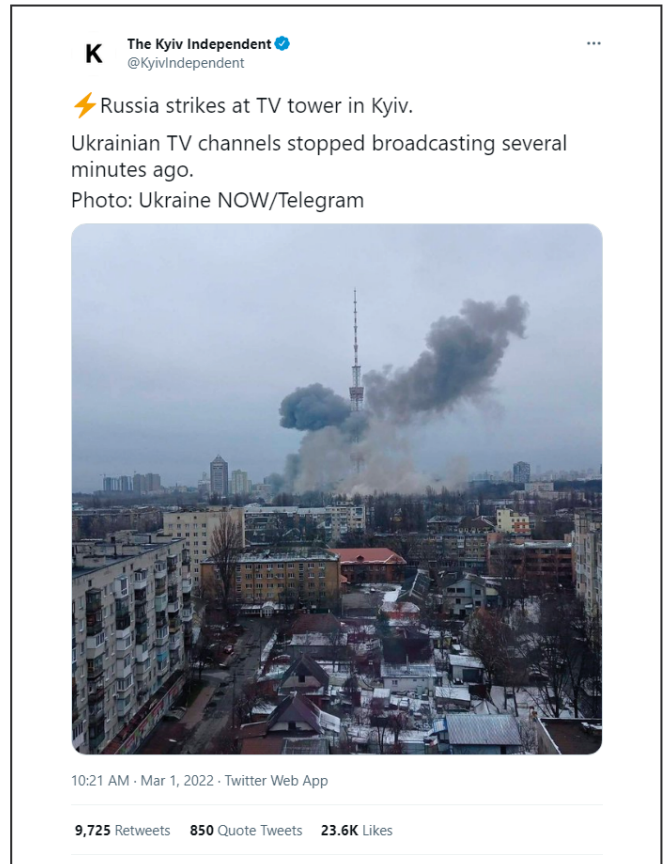


Photo of tv tower after missile strike.

⁷ <https://web.archive.org/web/20220301133913/https://tass.com/defense/1414199>

⁸ <https://iwpr.net/global-voices/berdyansk-life-under-russian-occupation>

⁹ <https://abcnews.go.com/Business/wireStory/russias-war-shrink-ukraine-economy-45-world-bank-84008993>

WEEK 2 (Mar 3 - 9):

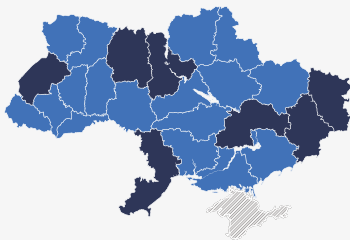
During this time, Russian military forces prepared for a major offensive on Kyiv, while known and suspected Russia-aligned threat actors attempted to compromise public information sources and communications infrastructure and increase insights into Ukrainian military operations.

- Another suspected Russian threat actor conducted lateral movement on a communications sector system and expanded focused targeting of media organizations from broadcast organizations to compromise systems belonging to a digital media firm.

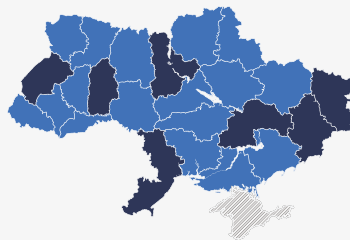
- DEV-0257 and STRONTIUM sought access to military and regional government accounts by directing phishing campaigns against the Ukrainian military and government employees in central Ukraine, respectively. The regional government campaign was a shift toward tactical targeting by STRONTIUM, which has typically pursued national-level organizations.

Weekly view of malicious cyber activity by region

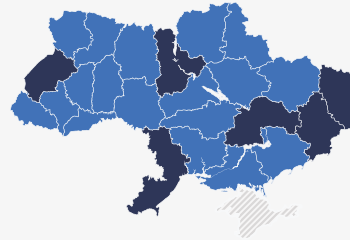
Week of February 23



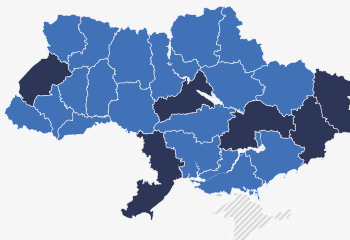
Week of March 2



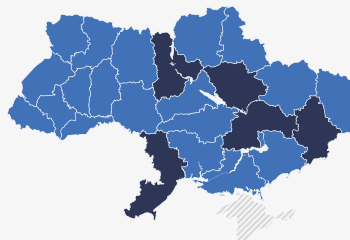
Week of March 9



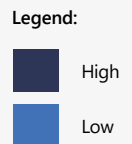
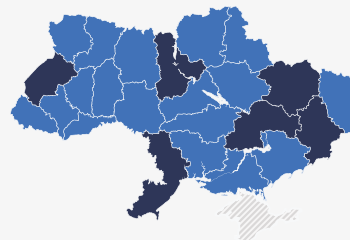
Week of March 16



Week of March 23



Week of March 30



High:

Regions which reflect more than 50% of detected and blocked actor indicators in the given week.

Data source:

Detected and blocked activity by Microsoft Defender Antivirus based on known actor indicators. Russian-occupied Crimea was excluded from this analysis.

WEEK 3 (Mar 10 - 16):

As military units captured nuclear power plants, and Russian military and state-run media pushed disinformation that Ukraine was working to create chemical and biological weapons, threat actors conducted operations to steal data from nuclear sector organizations that could assist those efforts.¹⁰

- A suspected Russian threat actor compromised an institution in Ukraine that was featured in false Russian weapons conspiracies in the past. IRIDIUM, an actor with a history of leaking documents to support disinformation narratives, conducted an intrusion into the same research institution later in March.
- On March 13, a suspected Russian nation state actor stole data from a nuclear safety organization that FSB-affiliated actor BROMINE had compromised in December 2021. BROMINE stole data from this entity from December through mid-March. In the first two weeks of the invasion, Russian troops seized the defunct Chernobyl nuclear power plant and the Zaporizhzhia Nuclear Power plant, the largest in Europe, indicating a clear military interest in nuclear energy targets.¹¹



Ukrainian Foreign Minister Kuleba tweet highlights a potential danger of Russian government narratives around chemical and biological weapons in Ukraine.

WEEK 4 (Mar 17 - 23):

Threat actors targeted logistics providers and regional government organizations in advance of the Russian military's announcement of a strategic refocus¹² on eastern Ukraine.

- IRIDIUM conducted a destructive attack on the network of a transportation/logistics provider, the type of organization that could be involved in moving Ukrainian supplies to conflict hotspots. The firm is headquartered in Western Ukraine, where much of the foreign military and humanitarian assistance is entering the country.
- The week prior, a suspected Russian actor deleted data from a regional government network in eastern Ukraine, disrupting government services there.

WEEK 5 (Mar 24 - 30):

Suspected Russia-aligned threat actors targeted Ukrainian civilian support and communications sector organizations, as Russian and Ukrainian peace negotiators¹³ met in Turkey to discuss a resolution to the conflict.

- Unknown actors compromised and potentially destroyed data at a portal that connects citizens to government services and compromised the network of another major media organization. Separately, Ukrainian authorities reported¹⁴ that they brought down five "enemy" bot farms that had been spreading disinformation about the Russian invasion to the Ukrainian public since February 24.
- Microsoft observed suspected Russia-aligned threat actors attempt to escalate privileges in the network of a communications provider network and broaden targeting efforts to compromise a mobile communications provider. Separately, Forbes reported that Ukraine's largest fixed line telecommunications provider, Ukrtelecom, had suffered a severe cyberattack, which NetBlocks claims brought the service down to 13% of its pre-war levels.¹⁵ This provides another data point on communications sector targeting.

¹⁰ <https://abcnews.go.com/Politics/russia-escalates-false-chemical-weapons-claims-us-ukraine/story?id=83366504>

¹¹ https://en.as.com/en/2022/03/07/latest_news/1646686014_463478.html

¹² <https://www.npr.org/2022/03/25/1088885299/russias-assault-on-kyiv-slows-as-it-shifts-focus-to-eastern-ukraines-donbas-regi?msclkid=8b22cc7fba6a11ecac00492d4da8e1c3>

¹³ <https://www.reuters.com/world/europe/ukraine-sets-ceasefire-goal-new-russia-talks-breakthrough-looks-distant-2022-03-29/>

¹⁴ <https://www.zdnet.com/article/ukraine-takes-out-five-bot-farms-spreading-panic-among-citizens/>

¹⁵ <https://www.forbes.com/sites/thomasbrewster/2022/03/28/huge-cyberattack-on-ukrtelecom-biggest-since-russian-invasion-crashes-ukraine-telecom/?sh=2174fe777dc2>

WEEK 6 and beyond (Mar 31 - Apr 8):

This period saw an escalation of attacks on energy infrastructure and targeted efforts to influence Ukrainians' support for their government.

- IRIDIUM and suspected Russian actors have been conducting intrusions into Ukrainian energy company networks since before the invasion started. During this period, IRIDIUM took the next steps to launch a destructive attack against the network of a regional energy provider.

Meanwhile, DEV-0586 launched a cyber-enabled influence operation to try to turn Ukrainian citizens against their government.

- DEV-0586 sent emails masquerading as a resident in besieged Mariupol that blamed the Ukrainian government for abandoning them and suggested resisting the government. There were no malicious links or attachments in the message further suggesting the intended objective was influence operations. This was the first instance we had observed such intense anti-government messaging in email.

Наше урядове капітал-шоу у сфері останніх подій остаточно наплювало на совість та мораль. Марно балакаючих лицемірних пик, як Арестович, слухати вже не можливо. Та в цих блядських російських свинях більше порядності, ніж в наших придворних блазнях. Вони думають, що ми тут у Маріуполі красуємося перед камерами, підбираючи охуєнні ракурси? Покидьки, блять! Ці "патріоти" нас просто залишили в цьому пеклі щоб ми здохли! Я пишаюсь, що ми с побратимами готові віддати свої життя за ради нашої мети. Нас таких не одна сотня, і ми готові змішати з гівном солодкуватих покидьків цієї клоунської зграї, поки самі не станемо двоохсотими, бо їх зрада може змити тільки їх загибель. І нехай хоч хтось наважиться нам перешкодити, влаштуємо їм зустріч з чортами.

Зараз, я звертаюся особисто до Вас, [REDACTED]. Якщо у вашій душі є хоч крапля українського патріотизму, Ви зобов'язані не дозволити нашій спільній мрії розчинитися у брехні та пропаганді цих лицемірних блазнів. Я закликаю Вас виконати національний обов'язок, відстояти право називатися українським народом і покінчити з цією зграєю безхребетних тварин. Разом Ми-Сила! Слава Нації! Смерть ворогам! Слава Україні! Україна по над усе!

This is a screenshot of the DEV-0586 email message to targeted Ukrainian citizens. A machine translation of the message says:

"In the light of recent events, our government capital has finally spat on conscience and morality. . . If there is even a drop of Ukrainian patriotism in your soul, you are obliged not to allow our common dream to dissolve into lies and propaganda of these hypocritical clowns. I urge you to fulfill your national duty, to defend the right to be called the Ukrainian people and to put an end to this pack of invertebrates."

The messages were addressed to people by name (redaction above), raising the prospect that DEV-0586 stole this personal information from at least one of their government victims.

Microsoft assistance to defend Ukraine

Microsoft has consistently acted to notify organizations and enterprises that we observed being threatened or attacked as described in this report. As the war commenced, we used the secure communication channels we had established with Ukrainian government cybersecurity officials to provide real-time threat intelligence and guidance to assist Ukrainian organizations' efforts to find and defeat cyberattacks. Leveraging RiskIQ's outside-in approach to illuminating attack surfaces, we provided our liaisons with actionable information about Ukrainian government systems that remained unpatched against known vulnerabilities that would likely be targeted by attackers. Microsoft respects and acknowledges the tireless efforts of Ukrainian network defenders and the unwavering support provided by CERT UA to protect their networks and maintain service to their customers during this extraordinary and challenging time.

With the consent and cooperation of the Ukrainian government, we have helped to proactively update systems with cyber countermeasures against the types of attacks we have observed. Specifically, we recommended that Ukrainian

organizations enable controlled folder access,¹⁶ an existing Microsoft Defender feature that is disabled by default. This feature meaningfully mitigated some of the damage done by destructive wiper malware. We have continuously integrated intelligence gained by tracking threat activity into new product detections to block malicious use of certain tools against Ukraine-based infrastructure.

We observed firsthand how customers running endpoint detection and response (EDR) solutions were able to respond to alerts and remediate intrusions before a destructive attack was launched. As Microsoft customers, our Ukrainian partners were using Microsoft Defender for Endpoint, but alternate EDR solutions could also provide much needed observability and detection capabilities.

We have kept the US Government advised of relevant information and have established communications with NATO and EU cyber officials to communicate any evidence of threat actor activity spreading beyond Ukraine.

¹⁶ <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders>

Outlook: Continued destructive attacks in Ukraine may increase in severity

Implications of wartime operations for global cybersecurity

The dynamic nature of the armed conflict will introduce a level of uncertainty not seen since the annexation of Crimea in 2014. As the war progresses, actors with a vested interest in the conflict will operate under increasingly urgent requirements to fill critical intelligence gaps and achieve specific tactical objectives. How cyber operators choose to meet these requirements may pose significant risk to the global cybersecurity landscape.

We assess that such an environment of urgency may incentivize the use of sensitive capabilities that will allow threat actors to gain assured access to networks or manipulate aspects of information systems to achieve strategic objectives. Highly reserved capabilities such as zero-days, critical infrastructure attacks, supply-chain attacks, and other novel techniques will almost-certainly be showcased in the medium-term.

As Microsoft and the greater security community increases outreach in Ukraine, the community will inevitably identify and mitigate previously unknown vulnerabilities and attack chains, forcing an already diverse ecosystem of well-resourced actors to reverse patches and carry out “N-day attacks” tailored to underlying vulnerabilities. This cat and mouse cycle almost guarantees that discovered capabilities will proliferate across multiple categories of threat actors, creating a long tail of incidents stemming from or modeled on the conflict in Ukraine. Organizations worldwide must acknowledge and prepare for the reality that such events will not occur in a vacuum and are unlikely to stay limited to a specific domain.

As of this report’s drafting, Microsoft and cybersecurity firm ESET worked with Ukrainian authorities to identify and mitigate the impact of an IRIDIUM wiper attack against the industrial control system infrastructure of a Ukrainian energy company.¹⁷ The targeting of ICS was an escalation beyond what we had observed up to early April in that it was intended to produce physical effects on critical infrastructure. On April 12, Russian President Vladimir Putin said that peace talks with Ukraine were dead and that his “military operation” would continue until objectives were achieved,¹⁸ setting expectations for protracted military engagement.

Given cyber operators’ demonstrated conduct of actions that mirror and augment military actions and the gradual expansion of targets of destructive attacks, cyberattacks will probably continue to escalate as conflict rages. In addition to the energy sector, the communications sector in Ukraine may suffer future destructive attacks, based on several known and suspected actors’ continued pursuit of compromises in that sector. Microsoft observed IRIDIUM, STRONTIUM, and unknown but suspected Russian nation state threat actors pursue compromises or expand on existing access in the communications sector in April, targeting IT infrastructure that supports the sector and a major ISP.

¹⁷ <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/>

¹⁸ <https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-04-12/card/putin-says-peace-talks-have-reached-dead-end-vows-war-will-go-on-pstQwRdkQV1WjLl9kwAH>

Outlook: Expansion of cyberattacks outside of Ukraine

As the conflict persists and countries provide more military assistance to Ukraine or take more punitive measures against the Russian government, Russian nation state threat actors may be tasked to expand their destructive actions in retaliation against targets outside of Ukraine in retaliation. Russia-aligned actors active in Ukraine are also showing interest in or conducting operations against organizations in the Baltics and Turkey, all member states on NATO's eastern flank that are actively providing political, humanitarian, or military support Ukraine. In addition to typical intelligence-gathering operations, this activity may represent pre-positioning for future destructive attacks if tasked.

Microsoft has notified these customers of the malicious activity and provided information that may aid in identifying and mitigating the threat on their networks. While much of what

Microsoft has observed to date suggests threat actors DEV-0586 and IRIDIUM are operating with restraint in the execution of destructive attacks by limiting malware deployments to specific target networks. However, Russia-aligned nation state actors are actively pursuing initial access to government and critical infrastructure organizations worldwide suggesting possible future targeting.

Microsoft encourages all organizations that are directly or indirectly associated with the conflict in Ukraine to proactively protect themselves from the threats described in this report and actively monitor for similar actions in their environment. Any organization that may be faced with defending their systems in future conflicts can follow the same general guidance to improve their defense against malicious cyber activity during conflicts.

Recommendations

Microsoft has observed throughout our engagement that Russia-aligned cyber operations use several common tactics, techniques, and procedures to execute their intrusions. We have been able to turn these observations into actionable guidance for network defenders and security teams. Some of the most common intrusion techniques include:

- Exploitation of public facing applications or spear-phishing with attachments/links for initial access.
- Credential theft and use of valid accounts throughout the attack lifecycle, making "identities" a key intrusion vector. This includes within Active Directory Domain and through VPNs or other remote access solutions.
- Use of valid administration protocols, tools, and methods for lateral movement, relying on compromised identities with administrative capability.
- Use of known publicly available offensive capabilities, sometimes obfuscated using actor specific methods to defeat static signatures.
- "Living off the land" during system and network discovery, often utilizing native utilities or commands that are non-standard for the environments.
- Use of destructive capabilities that access raw file systems for overwrites or deletions.

Based upon these observations, we recommend taking the following actions:

Minimize credential theft and account abuse:

Protecting the identities of your users is a key requirement to secure your network and resources from attackers. Microsoft recommends enabling multi-factor authentication and identity detection tools. Additionally, customers are urged to apply least privilege access and secure the most sensitive and privileged accounts and systems.

Secure internet-facing systems and remote access solutions:

Internet facing systems should be secured against external attacks by ensuring they are updated to the most secure levels, regularly evaluated for vulnerability, and audited for changes to the integrity of the system. Anti-malware solutions and endpoint protection should be enabled for detection and prevention of attackers. Legacy systems should be isolated to prevent them from being an entry point for persistent threat actors. Remote access solutions should require two-factor authentication and be patched to the most secure configuration.

Leverage anti-malware, endpoint detection, and identity protection solutions:

A combination of defense-in-depth security solutions, paired with trained and capable personnel, can empower your organization to identify, detect, and prevent intrusions impacting your business. Enabling cloud-protections¹⁹ allows identification and mitigation of known and novel threats to your network at scale.

Enable investigations and recovery:

In the case you detect or are notified of a threat to your environment, it is critical to have auditing of key resources to enable investigations. Customers are urged to have and exercise an incident response plan to prevent any delays or decrease dwell time for destructive threat actors. Customers are urged to have a backup strategy that accounts for the risk of destructive actions and prepare to exercise recovery plans.

Defend against destructive attacks:

Destructive attacks observed in Ukraine have similar characteristics and mitigations to Ransomware scenarios that Microsoft has identified worldwide in recent years. We have comprehensive guidance to help safeguard your organization against destructive attacks by leveraging features within Defender such as Attack Surface Reduction (ASR) and Controlled Folder Access (CFA). These features have been successful in defeating destructive attacks in Ukraine and elsewhere.²⁰

Review and implement “best practices” for defense in depth:

We have developed extensive resources and best practices for customers of Microsoft solutions that provide clear actionable guidance for security-related decisions. These are designed to help improve your security posture and reduce risk whether your environment is cloud-only, or a hybrid enterprise spanning cloud(s) and on-premises data centers. Microsoft's Security Best Practices covers topics such as governance, risk, compliance, security operations, identity and access management, network security and containment, information protection and storage, applications, and services.²¹

¹⁹ <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-cloud-protection-microsoft-defender-antivirus?view=o365-worldwide>

²⁰ <https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware>

²¹ All the materials, including videos and downloadable presentations, can be found here: <https://docs.microsoft.com/en-us/security/compass/compass>

Contributors

This report is prepared by Microsoft's Digital Security Unit, leveraging the intelligence and findings of the Microsoft Threat Intelligence Center and data analysis of Microsoft's AI for Good Research Lab. Together with security teams across Microsoft, we continue our work to protect customers in Ukraine and share insights and protection recommendations with the world.

