# War and Peace: Cyber Threat Activity Surrounding the 2022 Russian Invasion of Ukraine

Cyber Crime (CC) | Cyber Espionage (CE)
Critical Infrastructure (CI) | Fusion (FS)
Hacktivism (HK) | Strategic (ST)

May 16, 2022 05:49:14 PM, 22-00011952, Version: 1.2

## Executive Summary


- In the first four months of 2022, Mandiant identified more Russian-sponsored disruptive cyberattacks against Ukraine than it has during the past eight years.
- Several of these cyberattacks were coupled with concurrent information operations, including manipulation of a TV broadcast and dissemination of a deepfake video impersonating the Ukrainian president falsely announcing Ukraine's surrender.
- Mandiant suggests that the Russian invasion of Ukraine has caused some temporary disruption to the Russian-speaking cyber crime ecosystem, such as causing ideological divisions within threat groups and inspiring actors to use cyber capabilities in support of Russia or Ukraine.
- Mandiant observed numerous hacktivists claim to conduct threat activity in support of Russia or Ukraine. We suggest the conflict brought about a significant resurgence in global hacktivism and/or the use of hacktivist tactics, which had declined in the latter half of the last decade.


## Threat Detail

### The 2022 Ukraine Conflict

Russia began amassing troops along its border with Ukraine in fall 2021, prompting warnings and disclosures from U.S. and European officials of the threat of a Russian invasion. Mandiant identified extensive cyber espionage, disruptive and destructive cyberattacks, and information operations leading up to and since Russia's Feb. 24, 2022, invasion of Ukraine (22-00000226, 22-00003826, 21-00025520).

Vladimir Putin's obsession with returning Ukraine into the Russian sphere of influence culminated with Russia's invasion in February 2022 and created unprecedented circumstances for cyber threat activity. This likely is the first instance in which a major cyber power has conducted disruptive attacks, espionage, and information operations concurrently with widespread, kinetic military operations (Figure 1). We have never previously observed such a volume of cyberattacks, variety of threat actors, and coordination of effort within the same several months. The invasion has also caused some temporary disruption to the Russian-speaking cyber crime ecosystem, in some cases splitting criminal groups between sides, and it has seemingly triggered the biggest revival in international hacktivism since 2015. We assess with high confidence that Russian cyber espionage and attack operations, while already a serious threat to Ukrainian organizations, pose an elevated risk to Ukraine as long as Russia continues its invasion.

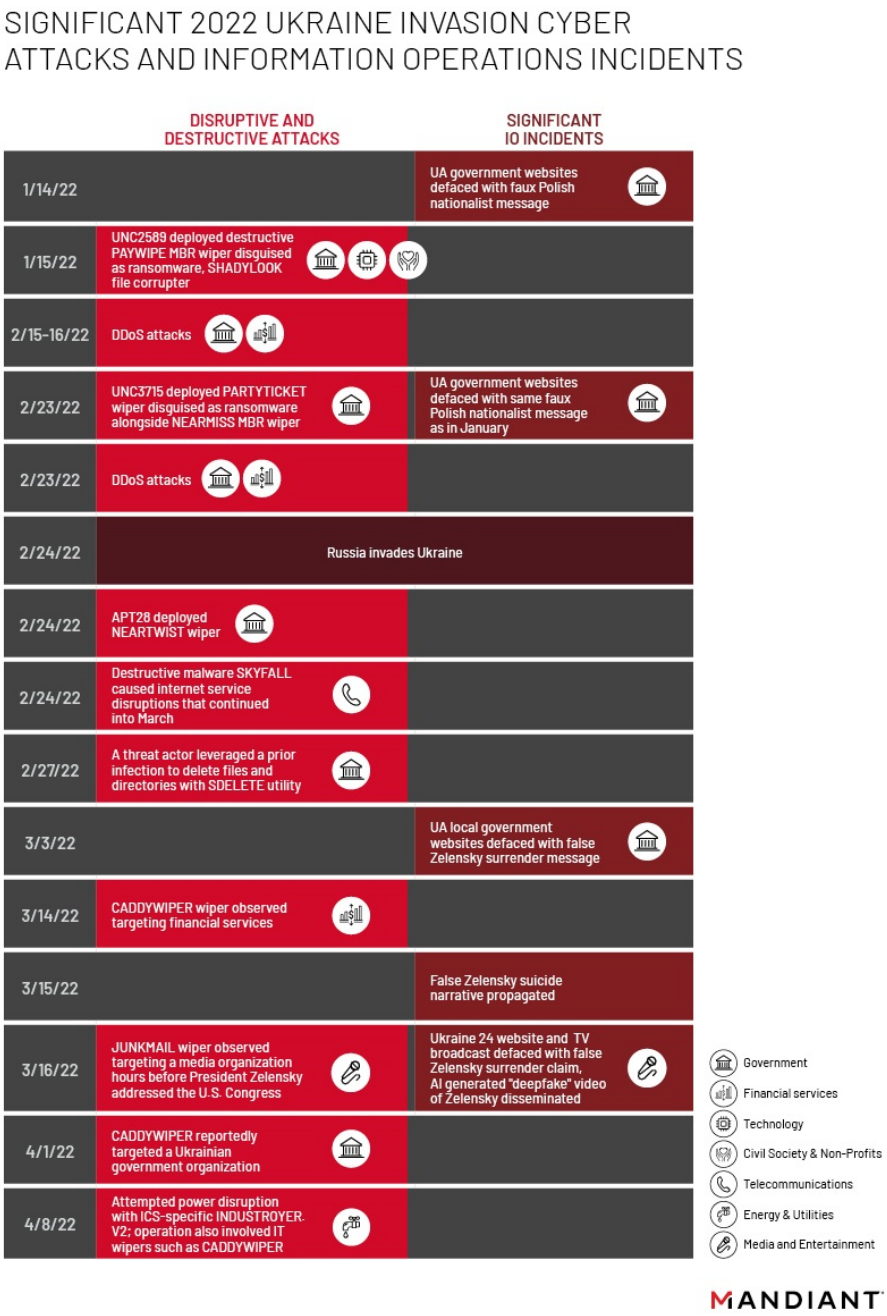


Figure 1: Timeline of significant cyber threat incidents related to the 2022 Ukraine conflict

**Cyberattack**

In the first four months of 2022, Mandiant identified more Russian-attributed disruptive cyber operations against Ukraine as it has during the past eight years (Figure 2). Despite the quantity of disruptive operations, we have observed few significant new capabilities or a notable evolution in tactics, techniques, and procedures (TTPs). We expect additional cyberattacks to occur while the war persists, particularly if Russian conventional forces are further attritted. Please see 22-00004460 and Appendix 1 for the full list and links to additional reporting.

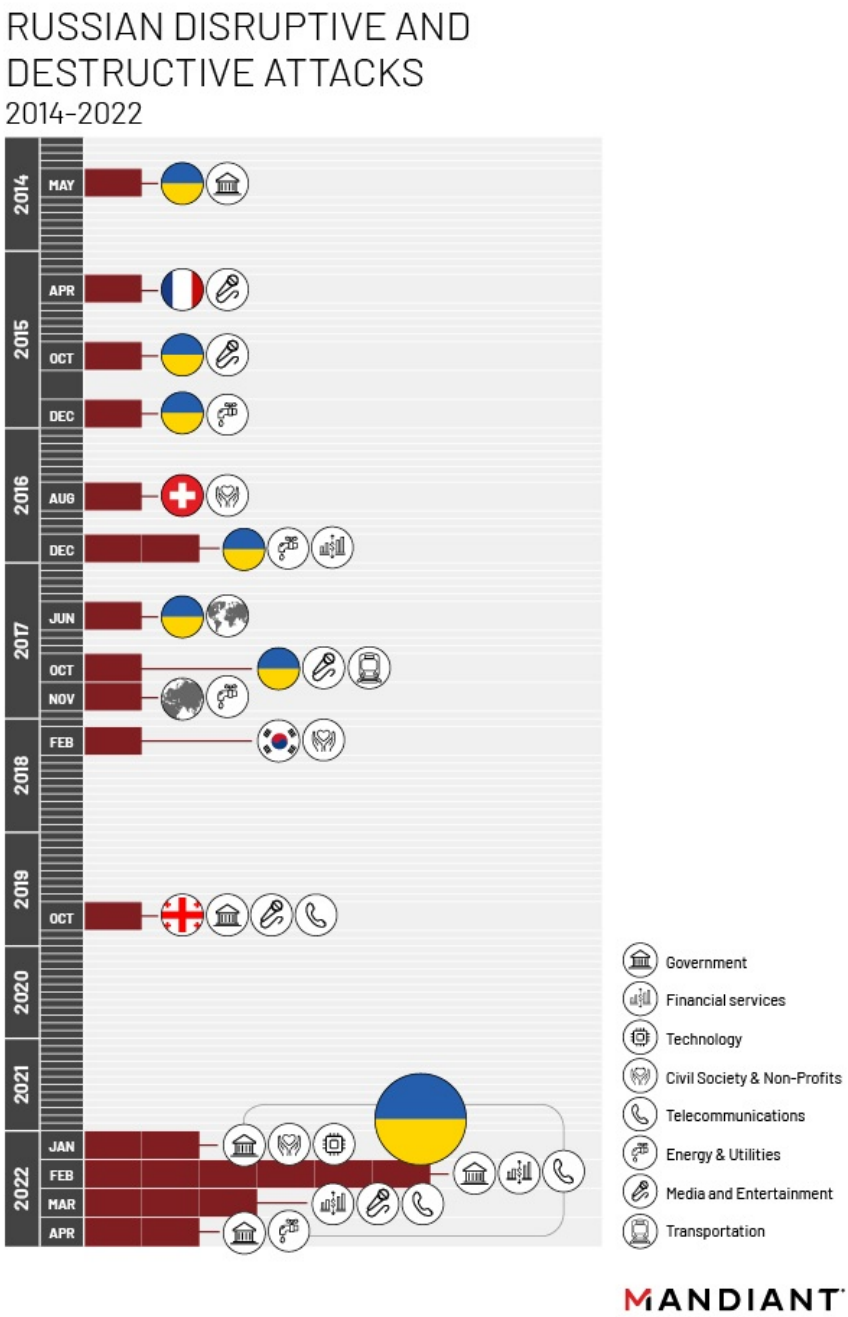


Figure 2: Timeline of Russian disruptive and destructive cyberattacks (2014–2022)

*New Dogs, Old Tricks*

We suggest that the makeup and quantity of new and established Russian threat actors conducting disruptive operations against Ukraine is unexpected and notable, including the resurgence of APT28. We have observed little confirmed activity from Sandworm, which was responsible for nearly all disruptive or destructive activity targeting Ukraine since 2015.

- Mandiant observed multiple suspected Russian groups conducting separate disruptive and destructive incidents, including APT28, UNC2589, UNC3715, and we note potential links between the INDUSTROYER.V2 incident and Sandworm.
- Some of the incidents, particularly those disabling telecommunications infrastructure or government targets, may have supported tactical objectives, restricting the Ukrainian government's ability to communicate at critical moments. Victor Zhora, the deputy chief of Ukraine's State Service of Special Communication and Information Protection, described the Feb. 24 attack on a satellite ISP as "a really huge loss in communications in the very beginning of the war."
- Other incidents, for example targeting the media and financial sector, may seek to undermine public confidence in the Ukrainian government, consistent with past Russian disruptive and destructive attacks in Ukraine and elsewhere.

*Reemergence of APT28 as a Disruptive Actor?*

Mandiant assesses with moderate confidence that the NEARTWIST wiper attack in February 2022 was conducted by APT28 based on overlaps in tactics, techniques, and procedures (TTPs), such as the use of SSH on odd ports and the unique use of wevtutil. The operation used Microsoft Exchange vulnerabilities to escalate privileges, deploy web shells, and largely rely on living-off-the-land techniques before attempting to deploy the NEARTWIST wiper. This is the first instance since 2016 that we have attributed a disruptive or destructive operation to APT28 and the first APT28 disruptive operation against Ukraine since 2014.

Three days after the NEARTWIST attack, a threat actor we also suspect is APT28 leveraged a three-year-old EMPIRE infection to regain access to a Ukrainian government organization. The threat actor moved laterally in the victim network and used the Windows SDELETE utility to delete files and directories from the infected systems. The use of a years-old infection that had seemingly lain dormant since initial compromise suggests that the actors were either tasked or felt pressure to create battlefield effects and searched for a preexisting access, rather than execute a preplanned operation.

*Scale of Cyberattacks Potentially Limited by Kinetic Operations*

Russian kinetic operations against Ukraine may have interfered with or reduced the viability of Russian cyberattacks against some Ukrainian targets, especially when Russian troops relied on existing telecommunications and/or power infrastructure for their operations and communications. We note that disruptive and destructive attacks to date peaked around the start of the invasion on Feb. 24, 2022; while we have still seen significant activity since that period, the pace of attacks seems to have slowed.

*Responses to Invasion Likely to Spur Russian Retaliation*

Mandiant assesses with moderate confidence that Russia will conduct additional destructive or disruptive cyberattacks connected to the crisis in Ukraine that almost certainly will focus first on Ukraine, with Western/NATO allies also being possible targets.

- NATO and Western sanctions and responses likely will heavily influence Russia's perception of high-priority targets for retaliation, and Russian action may be focused against the financial industry, energy and utilities sector, and media and entertainment.
- 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 cyberattacks 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.

**Information Operations**

Since January 2022, Mandiant documented several information operations that leveraged provocative narratives, such as false claims of Ukraine's surrender, and a full spectrum of tactics, including manipulation of a TV broadcast and dissemination of a deepfake video impersonating the Ukrainian president (see Table 1, Figure 3). Several of these incidents included disruptive elements and coincided with additional destructive and disruptive incidents, as noted above.

- We continued to observe long-standing information operations campaigns, such as Secondary Infektion and Ghostwriter, promote narratives supportive of Russian national interests, including content referencing the troop buildup and ensuing conflict, on social media and blog sites.
  - Mandiant previously assessed with moderate confidence that Belarus is likely at least partially responsible for the Ghostwriter influence campaign. As we have noted, some Ghostwriter activity can serve both Belarusian and Russian interests, including that targeting NATO and bilateral relations with NATO allies.
- We also reported on established pro-China and pro-Iran information operations campaigns promoting narratives critical of the United States, NATO, Europe, and Israel in their responses to the Russian invasion of Ukraine. These operations appear to be intended to undermine the U.S. and sow division between the U.S., NATO, Europe, and their allies.
- Western governments and researchers steadily reported and debunked pro-Russian false narratives associated with the conflict, including alleged Russian efforts to spread disinformation to use as casus belli to invade Ukraine. U.S., UK, and Ukrainian officials proactively exposed Russian plans to conduct disinformation campaigns before the campaigns were launched, possibly diminishing the effects of Russia's operations or forcing them to adjust.

| Date | Info Op |
|---|---|
| Jan. 14, 2022 | Multiple Ukrainian government websites, including that of the Ministry of Foreign Affairs, were defaced with a message claiming that data including Ukrainian citizens' personally identifiable information (PII) had been deleted from government servers and would be released. The defacements referenced war crimes committed by the "Ukrainian Insurgent Army" (UPA) against ethnic Poles during World War II, a narrative we have previously seen in pro-Russian information operations (22-00001084). |
| Feb. 23, 2022 | Dozens of Ukrainian government websites were defaced with the same faux Polish nationalist image displayed in January (22-00004168). |
| March 3, 2022 | Multiple local Ukrainian government websites were defaced with messages purportedly from Ukraine's President Zelensky indicating that the Ukrainian government was |

| | |
|---|---|
| | capitulating and signing a peace treaty with Russia (22-00005626). |
| March 15, 2022 | We assess with high confidence that an information operation promoted the fabricated narrative that Ukrainian President Volodymyr Zelensky committed suicide in a military bunker in Kyiv on March 13, 2022. We assess with moderate confidence that this operation is part of the Secondary Infektion campaign (22-00009572). |
| March 16, 2022 | Mandiant assesses with moderate confidence that an information operation targeting Ukraine on March 16, 2022, promoted a fabricated message alleging Ukraine's capitulation to Russia via the suspected compromise and defacement of the Ukraine 24 website and news ticker in a Ukraine 24 TV broadcast with a written message, as well as via an artificial intelligence (AI)-generated "deepfake" video impersonating Ukraine's President Zelensky delivering that same text (22-00007241). |

Table 1: Notable Ukraine conflict information operations incidents

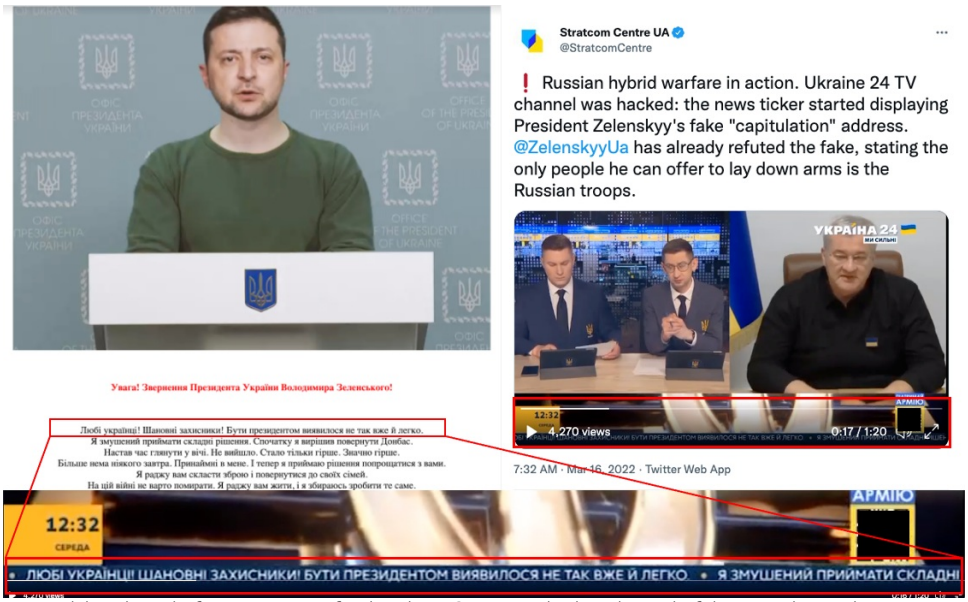


Figure 3: The text used in the defacement of Ukraine 24's website (top left) matches the text used to deface the Ukraine 24 news broadcast as shown in the video included in the Stratcom Centre UA tweet (top right). An enlarged image of the news ticker from that broadcast (bottom) shows a portion of that text and highlights the segment of the text in the website defacement with which it corresponds. Additionally, the image of Zelensky used in the defacement appears to be a screenshot from a promoted "deepfake" video of him.

Mandiant anticipates that pro-Russian information operations will continue to actively promote content supportive of Russian government interests, and critical of Ukraine, NATO, the U.S., and other nations or organizations perceived as supporting Ukraine in the conflict. We judge that Ukrainian government and media organizations face significant risk of compromise in support of information operations campaigns. We note the potential for these incidents to coincide with or support significant disruptive or destructive attacks. Elevated risk may extend to government and media targets in other nations in periods surrounding high-profile public events or announcements, such as ceasefire negotiations between Russia and Ukraine mediated or hosted in third party locations, international public speeches by Ukrainian officials, or developments regarding potential NATO membership expansion.

For more information on significant information operations targeting Ukraine in 2022, please see our Summary of Significant 2022 Ukraine Conflict Information Operations report. For a list of relevant reporting, please see Appendices 2 and 3.

### Cyber Espionage

We have observed significant cyber espionage and attacks against Ukraine in 2022 from Russian General Staff Main Intelligence Directorate (GRU)-sponsored APT28 and some activity from Foreign Intelligence Service (SVR)-sponsored APT29; we note an unusual dearth of observed Federal Security Service (FSB)-sponsored activity from Turla or TEMP.Isotope, possibly reflecting primacy for GRU operators. However, TEMP.Armageddon continues its prolific campaigns against Ukraine. We also identified significant activity, including disruptive attacks, from Russian actors we have not yet linked to a sponsor. We also observed activity from TEMP.Vermin and UNC2589 and identified several new Russian threat clusters that we have not yet attributed to other named groups, including UNC3506 (suspected Invisimole) and UNC2179.

| Espionage Actors Observed Targeting Ukraine | |
|---|---|
| APT28 | TEMP.Vermin |
| APT29 | UNC2589 |
| | UNC3506 (Suspected |

| | |
|---|---|
| TEMP.Armageddon | Invisimole) |
| UNC2179 | |

Table 2: Russian state-sponsored actors observed targeting Ukraine from late 2021 to May 2022

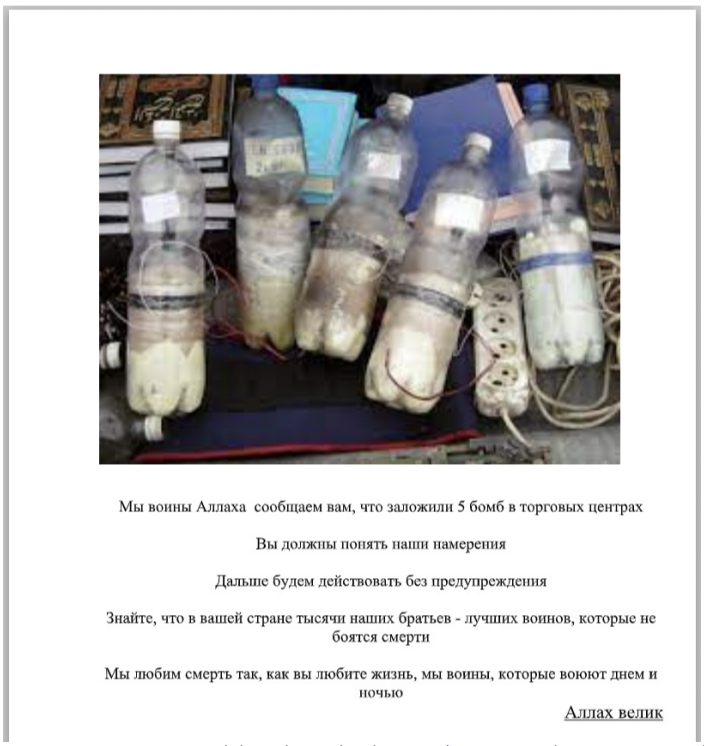


Figure 4: TEMP.Armageddon bomb threat lure used to target Ukraine

Russian operations remained focused on Ukrainian government targets, including the use of lure material directly referencing the conflict (see Figure 4). We also observed significant targeting of Ukrainian financial services, telecommunications, energy and utilities, and media organizations, likely in part to preposition access for future disruptive activity (see Figure 5). Although some operations likely were tailored to support invasion objectives, we assess that strategic intelligence on Ukrainian government and military plans and intentions almost certainly remains a top collection priority for Russian cyber espionage groups and that Russian cyber espionage will continue intensely targeting Ukraine throughout the war and after. We anticipate that Russian espionage groups will continue to adapt their operations to remain effective and attempt to obfuscate attribution.

*Russian Operational Considerations*

Russian military doctrine espouses a concept best described as "controlled escalation," in which Russian forces gradually increase pressure, either through kinetic or non-kinetic methods, while gauging adversarial reactions to each step until the adversary is willing to agree to favorable terms for Russia. Russia also views information warfare as a wide-ranging concept crucial to any armed and/or diplomatic conflict, which combines cyber operations, electronic warfare, psychological operations, and information operations. We have observed the coupling of information operations with disruptive cyberattacks, which likely are reflective of and driven by this strategic mindset. Russia may attempt to conduct disruptive cyber operations to support its kinetic military operations, particularly in areas where Russia may feel its conventional forces have bogged down.

As Russia's perception of its battlefield success and failure evolves, its cyber operations calculus—the risk tolerance for discovery, attribution, and willingness to take more aggressive action—likely has forced a shift in frequency, volume, and operational targeting. That is, what previously was a normal operational tempo can no longer be used as a baseline. Some lower priority operations will likely be sidelined to balance conflicting priorities.

Russia has demonstrated a willingness to burn existing accesses to support broader mission objectives, and establishing new accesses is not instantaneous. Reconnaissance, such as network scanning, email address discovery, and phishing, will still be required for new targets. Alternative tradecraft and tools may be used to obscure links to past operations.

*State-Sponsored Activity from Other Nations*

Although Russian-sponsored cyber espionage remains the highest threat to Ukraine, we have observed some activity from other state actors targeting Ukraine in the lead-up to and since the Russian invasion. Given China's close relations and support for Russia during the last decade, the war in Ukraine likely will become a sustained priority for Chinese threat groups.

- We identified at least two unique Chinese state-sponsored actors targeting Ukraine before and after Russia's invasion, and we observed a third Chinese group targeting European organizations with a Ukraine-related lure.
- UNC3367, a cluster we assess with low confidence to be part of Belarusian-sponsored UNC1151, conducted several operations targeting Ukraine in the period around the invasion, consistent with this actor's focus on countries bordering Belarus. We have previously assessed that UNC1151 provides technical support to the

Ghostwriter campaign.

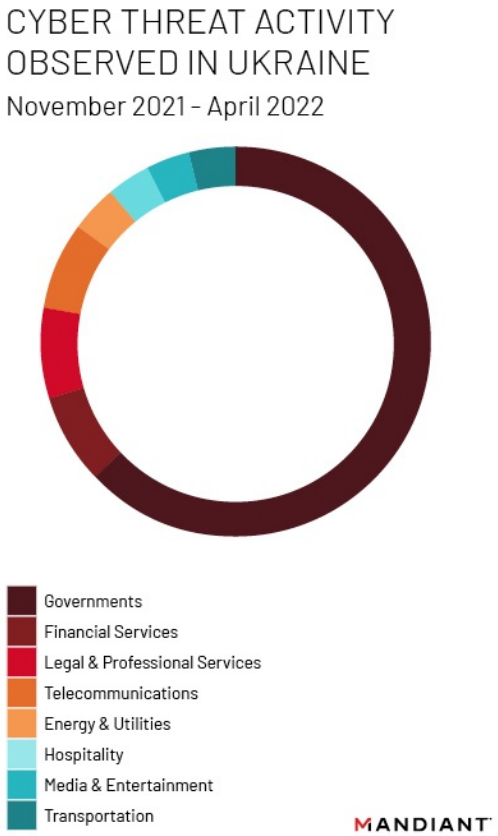


Figure 5: Cyber threat activity observed in Ukraine (November 2021 – April 2022)

For a summary of our reporting on Russian and other nations' cyber espionage operations targeting Ukraine in the lead-up to and since the invasion of Ukraine, please see Appendices 4 and 5. Some of this activity includes lure content related to the war in Ukraine, but Appendix 4 focuses on cyber espionage activity targeting Ukraine directly.

**Cyber Crime**

Mandiant suggests that the Russian invasion of Ukraine has caused some temporary disruptions to the Russian-speaking cyber crime ecosystem, causing ideological divisions within a few established groups, inspiring some typically financially motivated actors to use their tools and capabilities in support of Russia or Ukraine, complicating cashout operations for Russia-based actors, and potentially changing the relationship between criminal actors and their governments.

*Ukraine Conflict Increases Some Targeting of Russia*

Historically, the vast majority of Russian-speaking, financially motivated threat groups that we track strictly avoided targeting Russia or other Commonwealth of Independent States (CIS) countries. Russia's war against Ukraine appears to have changed the calculus of at least some of these groups, and we have observed a small, but notable, uptick in Russian-language cyber crime targeting Russian or CIS organizations.

- For instance, in late March 2022, Mandiant identified a Russian-language lure document delivering the POWERPLANT backdoor that we attribute to a FIN7-associated threat cluster. This campaign uses a ROSCOMNADZOR press watchdog theme and delivers a Russian-language lure document, indicating that this activity is targeting Russia-based individuals. This FIN7 threat cluster has previously only targeted organizations based in the U.S. Indictments have linked several Ukrainian nationals to FIN7.

*Some Financially Motivated Actors Announce Political Affiliations*

In response to Russia's invasion of Ukraine, several financially motivated threat actors have announced support for one side of the conflict and threated action against various parties.

- Notably, this includes the CONTI ransomware team, one of the most prolific ransomware groups during the last few years that almost certainly has some affiliates and operators based in Russia. CONTI declared their "full support of [the] Russian government" and implied they may take action against Western organizations accordingly (Figure 6). However, in response, a Twitter account with the handle "ContiLeaks" leaked internal chats from the group, exposing previous collaboration with likely the Russian intelligence services and reinforcing our assessments that these groups sometimes work on behalf of the Russian state.
  - Based on a series of leaked conversations from mid-July 2020, we have high confidence that at least some CONTI operations were specifically aimed at obtaining access or information that would fulfill Russian intelligence requirements. We have low confidence that, in at least some cases, this targeting was directed by a third party rather than opportunistically obtained.

    - Some CONTI operations, or activity by other Russia-based criminal groups, may also be undertaken as a perceived "patriotic" duty, without specific direction from the Russian state. In a series of April 2021 discussions, threat actors identified in the leaked chats implied that targeting a journalist critical of the Russian Federation would be an act of patriotism.
- The LOCKBIT Ransomware-as-a-Service (RaaS), which almost certainly has at least some Russia-based affiliates, posted that they successfully breached and encrypted files on the network of the Bulgarian government agency responsible for refugee management, including those from Ukraine. However, we lack evidence that this attack was politically motivated, rather than a "typical" extortion attempt.

Figure 6: Updated announcement posted on CONTI DLS on Feb. 25, 2022

*Russian State May Lean on Domestic Criminals*

Mandiant previously assessed with moderate confidence that the Russian state approaches cyber criminal operations based in Russia from a position of strategic tolerance; the Kremlin infrequently co-opts or directs Russian cyber criminal operations when their skills suit state interests but typically overlooks criminal operations as long as they refrain from targeting Russian domestic entities. However, since Russia invaded Ukraine, the Putin regime may be more willing to compel or request assistance from cyber criminal groups with at least some operators in Russia. Recently, the U.S., UK, Canadian, Australian, and New Zealand governments warned that some Russian cyber criminal groups and alleged hacktivist organizations pose a threat to Western critical infrastructure networks, even those not directly connected to the Russo-Ukrainian war.

**Ukraine Conflict Sparks Hacktivism Renaissance?**

Mandiant observed numerous hacktivist actors and groups declare support for Russia or Ukraine in the conflict and threaten or claim to conduct threat activity against organizations in either country or perceived allies of each side. We suggest the conflict brought about a significant resurgence in global hacktivism and/or the use of hacktivist tactics, which had declined globally in the latter half of the last decade.

- Observed threat activity has included defacements, data leaks, and distributed denial-of-service (DDoS) attacks, as well as disruptive and destructive incidents. For example, on May 9, 2022, Russian satellite television stations were reportedly modified to display the message "You have blood on your hands" to viewers in Moscow (Figure 7).
- We identified some activity with implications for critical infrastructure and operational technology (OT).
- Open sources indicate that the amount of data stolen from Russian organizations may be enormous, and some sources claim that Russia suffered more data breaches than any other country from January – March 2022.
- While we are unable to corroborate the high number of hacking claims related to this conflict, some of the activity is plausible and consistent with our expectations of the threat actors' capabilities and motivations.
- For a summary of our reporting on hacktivism related to the conflict, please see Appendix 6.

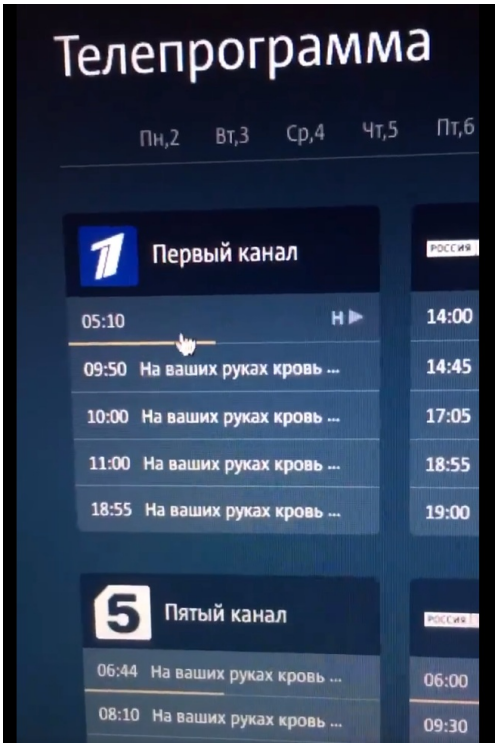

Figure 7: Russian satellite television stations were reportedly modified on May 9, 2022, to display the message "You have blood on your hands" to viewers in Moscow

*IT Army of Ukraine*

Shortly after the start of the Russian invasion, Ukraine's Deputy Prime Minister and Minister for Digital Transformation, Mykhailo Fedorov, called for "developers, cyber specialists, designers, copyrighters, marketers" to join a volunteer cyber force. Interested parties can join a dedicated, government-run, public Telegram channel to receive instructions for coordinated DDoS attacks against Russian and Belarusian websites and other activities, including defacements, crowdsourced reporting of Russian troop movements, reporting disinformation on social media platforms, and cyber defense.

- On April 6, the IT Army of Ukraine claimed to deface websites belonging to a subsidiary of Russian oil and gas company Gazprom with images from the Bucha massacre.
- Operations organized by the Ukrainian government reportedly had briefly interrupted rail ticket sales in western Russia around Rostov and Voronezh and knocked out telephone service in parts of Ukraine occupied by Russian-backed separatists since 2014.
- On May 2, the IT Army claimed credit for a DDoS attack that temporarily disrupted a Russian state information system that was responsible for tracking the production and distribution of alcoholic beverages in the country. The disruption reportedly interrupted the Russian alcohol supply chain for up to two days.

*Network Battalion 65 (NB65)*

NB65 is an English-speaking reportedly hacktivist persona that has targeted systems belonging to Russian organizations, stolen data, and then leaked that data online. The group asserts that its attacks are in response to Russia's invasion of Ukraine.

- Russian entities already targeted by NB65 hack-and-leaks include document management operator "Tensor," the Roscosmos space agency, and Russian state-owned VGTRK, or All-Russia State Television and Radio Broadcasting Co., Russian bank JSC Bank PSCB, and Russian-owned payments and financial services company Qiwi.
- NB65 has also reportedly deployed a modified version of the leaked CONTI ransomware, but it modified each version for each new victim to prevent victims from sharing a decryptor.

*Cyber Partisans*

Mandiant has tracked activity from the group CyberPartisans since at least September 2020, when the actor claimed to compromise resources associated with Belarusian government agencies. The actor appears to have organized its earliest operations in response to the government detaining protestors during the anti-Lukashenka protests that began after the fraudulent 2020 Belarusian presidential election in which Lukashenka declared himself victor. We have observed consistent CyberPartisans operations against the Belarusian government since late 2020, and as Russia began staging troops in Belarus for the invasion of Ukraine, the group announced its operations would also seek to cripple Russia's ability to use Belarus as a staging ground to attack Ukraine.

- On Feb. 27, CyberPartisans and other threat actors claimed that they had attacked Belarusian Railways, causing the company to enter manual control mode (Figure 8).
  - CyberPartisans previously claimed in January 2022 to compromise the company after it learned that Russia was using the rail transport network to move military personnel and equipment into Belarus.

- As proof of the February incident, CyberPartisans shared a screenshot ostensibly displaying internal computer network information from Belarusian Railway. It is possible that this artifact was taken during the February 2022 incident, but Belarusian Railway also announced that ticketing services were unavailable—a similar impact as the January 2022 incident.


Figure 8: CyberPartisans claim of continuing attacks against railways

*Pro-Russia Groups XakNet and KILLNET Likely Connected*

Two explicitly pro-Russian government groups calling themselves "XakNet" and "KILLNET" conducted multiple operations against Ukraine and countries allied with Ukraine, including KILLNET's defacement and/or disruption of multiple websites in the U.S. and Europe. Mandiant uncovered evidence that indicates that XakNet Team is working with or directly linked to Russian actors "KILLNET."

- KILLNET conducted several disruptive operations against European governments, banks, and railways, and both XakNet and KILLNET claim to have been created in response to Anonymous actions against Russian targets. Both groups have extremely limited verifiable history before recent actions taken against Ukraine, potentially suggesting that both groups were only recently stood up. Social media assets for both actors were set up recently and in the same month (March 2022).
- XakNet published a post to their Telegram channel on March 4 stating that XakNet and KILLNET would be working together to launch a "full-scale offensive against the fascists from Ukraine" (Figure 9).


Figure 9: A March 4, 2022, post from the @XakNet_team Telegram channel indicating cooperation between XakNet and KILLNET, machine translated from Russian to English

*Hacktivist Threats to Operational Technology*

Mandiant observed some reportedly hacktivist activity with implications for critical infrastructure and operational technology (OT), including reports of activity impacting embedded assets in Russia, such as human-machine interface

(HMI) display panels and an electric car charging station display board. While we are unable to corroborate the high number of hacking claims related to this conflict, some of the activity is plausible and consistent with our expectations of the threat actors' capabilities and motivations. We suggest critical infrastructure and OT will remain targets of interest for the various parties participating in the conflict.

**Mandiant Resources for Network Defenders**

We continue to closely monitor developments in Ukraine and regularly update the data model supporting Mandiant Advantage with new indicators of compromise (IOCs), malware families, actors, attributes, capabilities, and relationships upon discovery. New reporting and analysis related to relevant incidents and discoveries will be released as it becomes available.

For mitigation and hardening recommendations, please review:

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

The Ukraine Crisis Resource Center lists additional recommendations. Subscribers can access updated MITRE ATT&CK tactics and IOCs for relevant actors on Mandiant Advantage and access recent reporting for descriptions of observed activity.

**Appendices**

*Appendix 1: Observed Disruptive and Destructive Attacks*

| Date | Target Industry | Actor | Malware | Type of Activity | Related Reporting |
|---|---|---|---|---|---|
| 1/14/22 | Government | Ukraine attributes defacements to UNC1151 | | Disruptive: defacements of Ukrainian government websites | 22-00001084 |
| 1/15/22 | Government, Technology, Civil Society & Non-Profits | Mandiant and Ukraine attribute to UNC2589 | PAYWIPE (aka WhisperGate), SHADYLOOK (aka WhisperKill) | Destructive: PAYWIPE MBR wiper disguised as ransomware | 22-00001136 |
| 2/15–16/22 | Government, Financial Services | U.S. and UK attribute to GRU | | Disruptive: DDoS | source, source, source |
| 2/23/22 | Government, Financial Services | | | Disruptive: DDoS, defacements | 22-00004164, 22-00004168, source |
| 2/23/22 | | UNC3715 | NEARMISS (aka HermeticWiper, FoxBlade), PARTYTICKET (aka HermeticRansom) | Destructive: PARTYTICKET wiper disguised as ransomware allegedly deployed alongside MBR wiper NEARMISS | 22-00004168, 22-00004497 |
| 2/24/22 | Government | APT28 | NEARTWIST (aka IsaacWiper) | Destructive: wiper | 22-00004605, 22-00004674, source |
| 2/24/22 | Telecommunications | U.S. reportedly attributes to GRU | SKYFALL | Destructive malware caused Internet service disruptions | 22-00004499, 22-00007054, 22-00008615, source, source |
| 2/27/22 | Government | Possibly APT28 | SDELETE | Destructive | 22-00007625 |
| 3/14/22 | Financial Services | | CADDYWIPER | Destructive: wiper | 22-00006393, source |
| 3/16/22 | Media & Entertainment | | JUNKMAIL (aka DoubleZero) | Destructive: wiper | 22-00007112 |

| | | | | | |
|---|---|---|---|---|---|
| 3/28/22 | Telecommunications | | | Cyber incident disrupts Internet access | source, source |
| 4/1/22 | Government | | CADDYWIPER | Destructive: wiper | 22-00009571, source |
| 4/8/22 | Energy & Utilities | | CADDYWIPER, INDUSTROYER2 | Destructive and Disruptive: attempted power disruption with ICS-specific INDUSTROYER2; operation also involved IT wipers | 22-00009571, 22-00009760, source, source |

Table 3: Observed disruptive and destructive attacks

*Appendix 2: Mandiant Reporting About Pro-Russian Information Operations*

| Publish Date | Title | Report ID |
|---|---|---|
| 12/10/21 | Suspected Ghostwriter Operation Promoted Narrative Alleging That Ukrainian Government Forces Shot Migrants Trying to Enter the Country from Belarusian Border | 21-00026128 |
| 12/17/21 | Suspected Ghostwriter Operation Alleged that Polish Government Enlisted Volunteers from Far-Right Ukrainian Political Party to Help Secure Polish-Belarusian Border | 21-00026692 |
| 1/12/22 | Hacktivist Persona 'JokerDNR' Publishes Post Alleging Ukrainian Military Involvement in Orchestrating Kazakhstan Protests | 22-00000929 |
| 1/26/22 | Chronic Infektion: Years-Long, Pro-Russian 'Secondary Infektion' Influence Campaign Remains Highly Active | 22-00002024 |
| 2/16/22 | Pro-Russian 'Secondary Infektion' Operations Promote Narratives Targeting Ukraine Amid Russian Military Escalation | 22-00003826 |
| 2/16/22 | Coordinated and Inauthentic Russian-Language Twitter Network Promotes Pro-Russia Narratives, Including Those Related to Ukraine Tensions and Relations with China | 22-00003796 |
| 3/9/22 | Multiple Ukrainian Regional and Local Websites Reported to Be Defaced with Messages Suggesting Ukraine Capitulated to Russia | 22-00005626 |
| 3/18/22 | The Moment Makes the...GAN? Information Operation Leverages "Deepfake" Video of Ukrainian President Zelensky and Defacements to Promote Fake Message Alleging Ukraine's Capitulation in Fight to Repel Russian Invasion | 22-00007241 |
| 3/21/22 | Telegram Channels Promoting Content Related to Russia's Invasion of Ukraine Attributed to the Russian GRU by Ukraine's SBU | 22-00007001 |
| 3/28/22 | Russian TrollZ: Telegram Channel 'Cyber Front Z' Coordinating Promotion of Pro-Russia Messaging About Russia's Invasion of Ukraine Potentially Linked to Paid Russian Trolling Operation | 22-00008104 |
| 4/11/22 | Suspected Inauthentic Personas from Ghostwriter Influence Campaign Continue Promotion of Opinion Articles with Increased Mentions of Ukraine | 22-00009538 |
| 4/12/22 | Suspected 'Secondary Infektion' Information Operation Falsely Claims Ukrainian President Zelensky Committed Suicide in Military Bunker | 22-00009572 |
| 4/15/22 | Coordinated and Inauthentic Russian-Language Twitter Network Promotes Disinformation Pertaining to Russia's Invasion of Ukraine and the West's Response | 22-00010092 |
| 5/2/22 | Suspected 'Secondary Infektion' Information Operation Alleges That Azov 'Gang' Threatened Ukrainian President Zelenskyy for Abandoning Forces in Mariupol | 22-00011419 |
| 5/2/22 | Suspected 'Secondary Infektion' Information Operation Alleges That Poland Used Fabricated Ukrainian 'Provocation' in Bucha to Attempt to Station Polish Troops in Ukraine | 21-00026128 |
| 5/4/22 | Suspected Ghostwriter Operation Alleges Illegal Polish Human Organ Trade Targeting Ukrainian Refugees | 21-00026692 |

Table 4: Mandiant reporting about pro-Russian information operations

*Appendix 3: Mandiant Reporting About Additional Information Operations Referencing the Ukraine Conflict*

| Publish Date | Title | Report ID |
|---|---|---|
| 2/22/22 | Impersonator of Russian Journalist Comprises Part of Pro-Iran Influence Campaign, Promotes Narrative that Israel Supports Ukraine Against Russia in Current Tensions | 22-00004014 |
| 2/23/22 | Threat Activity Report: DRAGONBRIDGE Campaign Promotes Content Critical of U.S. Surrounding Russia-Ukraine Conflict | 22-00004158 |
| 3/7/22 | TAR: Arabic-Language Twitter Accounts Comprising Part of Iranian Liberty Front Press Campaign Promote Content Pertaining to Russian Invasion of Ukraine (3/8) | 22-00004849 |
| 3/21/22 | Threat Activity Report: DRAGONBRIDGE Social Media Account Impersonates Belarusian Vlogger, Promotes Content Pertaining to Russia's Invasion of Ukraine | 22-00007663 |
| 3/23/22 | Threat Activity Report: DRAGONBRIDGE Information Operations Campaign Amplifies Conspiracy Theory About U.S. Bioweapons Program in Ukraine and Portrays U.S. as Instigator of Global Conflict | 22-00007884 |
| 4/13/22 | Threat Activity Report: DRAGONBRIDGE Campaign Promotes Content Casting Doubt on U.S.-Europe Alignment on Sanctions Against Russia, Alleging U.S. Coercion of Europe | 22-00009927 |
| 4/13/22 | Impersonators in Pro-Iran Influence Campaign, Including Those of Ukrainian Journalist and Former NATO Official, Promote Narratives on Russian Invasion of Ukraine | 22-00009889 |
| 4/28/22 | DRAGONBRIDGE Information Operations Campaign Alleges Discovery of Chronic Malicious Cyber Activities Involving U.S. Government Actors | 22-00010969 |
| 5/13/22 | Pro-Cuban 'DeZurdaTeam' Network Promotes Spanish-Language Content Related to Russia's Invasion of Ukraine in Support of Russia's Interests | 22-00012130 |

Table 5: Mandiant reporting about additional information operations referencing the Ukraine conflict

*Appendix 4: Mandiant Reporting on Russian Cyber Espionage and Attack Operations*

| Publish Date | Title | Report ID |
|---|---|---|
| 12/7/21 | UNC2589 Uses Fake Website of President of Ukraine to Distribute SPRINGBEE Malware | 21-00025919 |
| 12/14/21 | TEMP.Armageddon Returns to Its Activity After Being Indicted by Ukrainian Law Enforcement | 21-00026317 |
| 12/14/21 | Suspected UNC2179 Activity Targeting Government Entities in Ukraine and Belarus with LOUDSTEP | 21-00026319 |
| 12/16/21 | Suspected UNC3506 Targets Ukrainian Government Entities and Private Enterprises to Deploy Malware from INVISIMOLE Ecosystem | 21-00026612 |
| 1/14/22 | Ukrainian Government Websites Defaced with Threatening Messages, No Claimed Attribution | 22-00001084 |
| 1/19/22 | TEMP.Armageddon Uses Bomb Threat Lure to Target Ukraine | 22-00001511 |
| 1/20/22 | Wiper Identified Targeting Ukrainian Government Entities | 22-00001136 |
| 1/28/22 | APT29 Targeting European/Ukrainian Government Entities Using LINKSHELL Backdoor | 22-00002137 |
| 1/31/22 | UNC2589 Leverages GOOSECHASE and FINETIDE in Recent Activity | 22-00002186 |
| 2/1/22 | APT29 Targets European Diplomatic Entities with New Downloaders BEATDROP and BOOMMIC to Deploy BEACON | 22-00001942 |
| 2/3/22 | UNC2589 Activity Targets Ukrainian Government Entities with MOUNTSTEEL and SPRINGBEE Malware | 22-00002730 |
| 2/16/22 | Ukrainian State-Owned Banks and Ministry of Defense Targeted by DDoS Attacks | 22-00003730 |
| 2/24/22 | UNC3691 Targets British Journalist Working in Ukraine with Credential-Stealing XFILES Malware | 22-00004245 |
| 2/25/22 | APT29 Targets MFAs with ROOTSAW, BEATDROP, BEACON | 22-00004314 |
| 2/25/22 | TEMP.Armageddon Likely Targets Ukrainian Government Officials with Russia-Ukraine Conflict-Themed Lure Content | 22-00004238 |
| 3/2/22 | Viasat Believes a 'Cyber Event' Is Disrupting Its | 22- |

| | | |
|---|---|---|
| | Satellite Internet Service in Ukraine | 00004499 |
| 3/2/22 | UNC2589 Leverages Security Service of Ukraine Evacuation-Themed Lure to Potentially Target Chemical Factory in Lviv, Ukraine | 22-00004590 |
| 3/3/22 | NEARMISS, New Master Boot Record Wiper Targets Ukraine, Defacements of Ukrainian Government Websites | 22-00004168 |
| 3/8/22 | GOOSECHASE, FINETIDE, and MARSSTEALER Leveraged Against Transportation and Government Industries in Europe; Possible Link to UNC2589 | 22-00005119 |
| 3/9/22 | Multiple Ukrainian Regional and Local Websites Reported to Be Defaced with Messages Suggesting Ukraine Capitulated to Russia | 22-00005626 |
| 3/10/22 | UNC2589 Targets Ukrainian Energy Infrastructure and Government Agencies | 22-00005898 |
| 3/13/22 | INDUSTROYER.V2 Used in Attacks Against Ukrainian Power Grid | 22-00009760 |
| 3/14/22 | Suspected APT28 Activity Targets Ukrainian Citizen Using Fake Security Alert | 22-00006225 |
| 3/14/22 | New CADDYWIPER Malware Targets Ukraine | 22-00006393 |
| 3/18/22 | NEARTWIST Wiper Used Against Ukraine Linked to APT28 with Moderate Confidence | 22-00007232 |
| 3/18/22 | JUNKMAIL Wiper Targets Ukrainian Media Company Ahead of Zelenskyy's Speech to Congress | 22-00007112 |
| 3/21/22 | Dormant EMPIRE Infection Reactivated to Trigger Wiping with SDELETE at Ukrainian Government Organization; Suspected Ties to APT28 | 22-00007625 |
| 3/21/22 | Suspected APT28 Activity Continues Targeting Ukrainian Citizen | 22-00007656 |
| 3/24/22 | Temp.Vermin Targets Ukrainian Government with SPECTRUM Malware | 22-00007886 |
| 3/25/22 | LOADEDGE Malware Used to Target Ukrainian Government, Links to 'Invisimole' Group | 22-00007810 |
| 3/29/22 | ProxyShell Exploitation Leads to THRESHGO Email Data Miner in Suspected Russia-Nexus Activity Targeting Ukrainian Government Entities | 22-00008243 |
| 3/29/22 | Suspected UNC2589 Targets Ukraine with GRIMPLANT and GRAPHSTEEL Malware | 22-00008201 |
| 4/4/22 | Temp.Armageddon Targets Ukraine with Russian War Criminals Theme | 22-00008755 |
| 4/12/22 | CADDYWIPER Deployed via ARGUEPATCH Loader Targeting Ukrainian Energy Sector | 22-00009571 |
| 4/13/22 | FREETOW Dropper Targets Ukrainian Entities; Suspected Ties to APT28 | 22-00008827 |
| 4/21/22 | Proxy Tunneling Malware GOGETTER Likely Linked to Recent Disruptive Activity at Ukrainian Government Organizations | 22-00010407 |
| 4/21/22 | MONSTERMAIL Credential Stealer Targets Ukrainian Individuals' Browser Logon Credentials and Cookies | 22-00010493 |
| 5/6/22 | UNC3846 Targets Ukrainian ISP with FACEFISH Linux Backdoor | 22-00011571 |
| 5/11/22 | APT29 Targets European Diplomatic Entities with ROOTSAW Dropper and New BEATDROP Variants Using Dropbox and Slack for C&C | 22-00011950 |
| 5/11/22 | Ukraine Warns of "Chemical Attack" Phishing Pushing Stealer Malware | 22-00011944 |
| 5/11/22 | File Stealer MAYOGRAB Observed in Historic Targeting of Ukrainian Government Organizations in October 2019 | 22-00011747 |

Table 6: Mandiant reporting on Russian cyber espionage and attack operations

*Appendix 5: Mandiant Reporting on Non-Russian Cyber Espionage Operations*

| Publish Date | Title | Report ID |
|---|---|---|
| 11/3/21 | Suspected UNC3367 Activity Targeting Ukrainian Government Entities Using MICROBACKDOOR C&C Tool | 21-00023858 |
| 2/14/22 | Massive Credential Harvesting Phishing Campaign by UNC1151 Against Ukrainian Military (Possible Connection with the Military Exercises of Russia and Belarus) | 22-00003578 |

| | | |
|---|---|---|
| 3/7/22 | Suspected UNC1151 Activity Targeting Ukrainian Government Using MICROBACKDOOR and Bombardment Sheltering Guideline Lure | 22-00004821 |
| 3/16/22 | Suspected Chinese APT Targeting Ukraine Pre-Invasion | 22-00006903 |
| 3/22/22 | Suspected APT Campaign Leverages Ukraine- and Kremlin-Themed Lures Against Ukraine, Czech Republic, and Poland | 22-00007226 |
| 3/24/22 | UNC1151 Targets Ukrainian Entities with BEACON Backdoor | 22-00007918 |
| 3/24/22 | GONEAWAY Downloader Suspected of Targeting Russian-Backed Separatists in Ukraine Pre-Invasion | 22-00006684 |
| 3/24/22 | UNC532 Leverages Russian War Crimes Lure Against Entities in Ukraine | 22-00007807 |
| 4/14/22 | Suspected TEMP.Hex Likely Targeted European Security Organizations with Russia-Ukraine Conflict-Themed Lures | 22-00009884 |
| 4/20/22 | Mail Collection Campaign Targets Ukraine; Exploitation of XSS Vulnerability in Zimbra Observed | 22-00010216 |

Table 7: Mandiant reporting on non-Russian cyber espionage operations

*Appendix 6: Mandiant Reporting About Hacktivist Activity*

| Publish Date | Title | Report ID |
|---|---|---|
| 1/26/22 | Hackers Say They Encrypted Belarusian Railway Servers in Protest | 22-00001926 |
| 1/26/22 | Threat Activity Alert: Hacktivist Actor 'CyberPartisans' Hacks Belarusian Railway | 22-00001979 |
| 2/24/22 | Threat Activity Report: Hacktivist Personas 'Beregini' and 'JokerDNR' Call for Ukrainian Surrender and Allege That a Ukrainian Military Unit Ignored Such a Call and Suffered Missile Strike | 22-00004244 |
| 2/25/22 | Threat Activity Alert: English-Speaking Actor GhostSec Leaks Russian Military and Governmental Credentials on Telegram | 22-00004310 |
| 2/27/22 | Threat Activity Alert: Hacktivist Actor 'CyberPartisans' Hacks Belarusian Railway | 22-00004435 |
| 2/28/22 | Anonymous Hacking Group Declares "Cyber War" Against Russia | 22-00004265 |
| 2/28/22 | Threat Activity Alert: Georgian Hacktivist Actor 'GNG' Leaks Data from Russian Bank 'Sberbank' on Discord | 22-00004451 |
| 3/1/22 | Threat Activity Alert: English-Speaking Actor 'NB65' Claims Hack-and-Leak Attack Against Nuclear Safety Institute of Moscow, Hacking of Severnaya Kompaniya, and Other Russian OT Devices on Twitter | 22-00004487 |
| 3/1/22 | Threat Activity Alert: 'Intel Repository' Leaks Internal Documents Allegedly from Russian Defence Manufacturer | 22-00004466 |
| 3/2/22 | Ukrainian Cyber Resistance Group Targets Russian Power Grid, Railways | 22-00004602 |
| 3/7/22 | Multiple Actors Seek Accesses to Media Screens; Could be Leveraged to Promote Narratives Related to the Ukraine War (3/8) | 22-00004925 |
| 3/9/22 | Threat Activity Alert: English-Speaking Group 'GhostSec' Shares Data from the International Research Center for Nuclear Sciences in Russia on Telegram Under #OpRussia | 22-00005567 |
| 3/14/22 | Anonymous Sent a Message to Russians: 'Remove Putin' | 22-00006321 |
| 3/14/22 | Rosneft's German Unit Reports Cyber Attack- Media Reports | 22-00006317 |
| 3/18/22 | Russian Government Website Experiences Massive Cyber Attack, Up To 1 Terabyte | 22-00007228 |
| 3/18/22 | Cyber Threat Actors Announce Threats and Attacks Against Critical Infrastructure in Response to Russia/Ukraine Conflict | 22-00004492 |
| 4/4/22 | Updated: Hacktivists Conduct DDoS Attacks, Defacements, and Data Leaks Against Russian, Crimean, Belarusian, and Chechen Targets in Protest of the Russian Invasion of Ukraine | 22-00005875 |
| | Threat Activity Alert: Anonymous Affiliated Actor | 22- |

| | | |
|---|---|---|
| 4/4/22 | "DepaixPorteur" Leaks 65 GB of Data from Russian Law Firm | 00008775 |
| 4/6/22 | Threat Activity Alert: Hacktivist Group 'IT Army of Ukraine' Claims Defacement of Websites of Oil Producer in Russia | 22-00008981 |
| 4/6/22 | Threat Activity Alert: Anonymous Affiliated Actor 'DepaixPorteur' Claims Compromise and Leak Against Ration Supplier of the Russian Army | 22-00008977 |
| 4/7/22 | Threat Activity Alert: Hacktivist Group 'IT Army of Ukraine' Claims DDoS Against the Operator of Russian National System for the Digital Labelling of Products | 22-00009205 |
| 4/8/22 | Hacktivist Persona JokerDNR Launches New Telegram Channel and Claims Defacement of Website Linked to Ukrainian Military | 22-00009091 |
| 4/11/22 | Hackers Use Conti's Leaked Ransomware to Attack Russian Companies | 22-00009482 |
| 4/18/22 | BIG Sabotage: Famous npm Package Deletes Files to Protest Ukraine War | 22-00007242 |
| 4/19/22 | Threat Activity Alert: Pro-Russian Hacktivist Group 'KillNet' Claims to Have Compromised Eight Polish Airports | 22-00010280 |
| 4/19/22 | Threat Activity Alert: English-Speaking Actor 'Network Battalion 65'' Claims to Have Breached Russian Commercial Bank | 22-00010279 |
| 4/19/22 | Threat Activity Alert: Ukrainian Hacktivist Group 'Bandera Hackers' Claims to Compromise Communication Systems Supplier for Russian Government Agencies and Corporations | 22-00010278 |
| 4/20/22 | Threat Activity Alert: Pro-Russian Hacktivist Group 'KillNet' Claims to Perform DDoS Attack Against Websites of Airports, Government Entities, Bank, Telecommunication and Hosting Providers in Czech Republic | 22-00010504 |
| 4/22/22 | Threat Activity Alert: Hacktivist Group 'IT Army of Ukraine' Claims DDoS Against The Most Popular Accounting Service in Russia | 22-00010608 |
| 4/22/22 | Anonymous Leaked Data Stolen from Russian Pipeline Company Transneft | 22-00007535 |
| 4/22/22 | Threat Activity Alert: Pro-Russian Hacktivist Group 'KillNet' Claims to Perform DDoS Attack Against Websites of Airports, Major Train Operator, Hosting Provider and NATO Cyber Centre in Estonia | 22-00010607 |
| 4/25/22 | Anonymous Claims to Have Hacked the Central Bank of Russia | 22-00007974 |
| 4/28/22 | Threat Activity Alert: Hacktivist Group 'IT Army of Ukraine' Claims DDoS Attacks Against Russian E-Trading Platforms on Telegram Channel | 22-00011046 |
| 4/28/22 | While Twitter Suspends Anonymous Accounts, the Group Hacked VGTRK Russian Television and Radio | 22-00008117 |
| 4/29/22 | Threat Activity Alert: Pro-Russian Hacktivist Group 'KillNet' DDoSed Government Entities, Defence Ministry, Border Police, Train Operator and Bank in Romania | 22-00011102 |
| 4/29/22 | Ukraine Targeted by DDoS Attacks from Compromised WordPress Sites | 22-00011074 |
| 5/2/22 | Pro-Russia Hacktivist Group 'KillNet' and 'Legion' Claim DDoS Attacks Against Moldovan, Latvian, and Lithuanian Government, Railways, and Bank Websites | 22-00011258 |
| 5/2/22 | Threat Activity Alert: Pro-Russia Hacktivist Group 'KillNet' and 'Legion' Claim DDoS Attacks Against German Government, Automotive and Payment System Websites | 22-00011374 |
| 5/2/22 | Threat Activity Alert: Hacktivist Actor 'Network Battalion 65' Claims Hack-and-Leak Attack Against Russian Payment and Financial Services Company on Twitter | 22-00011241 |
| 5/6/22 | Threat Activity Alert: Hacktivist Group 'IT Army' Claims DDoS Attacks Against Russian State Automated Information System Causing Liquor Supply Chain Disruptions | 22-00011569 |
| 5/9/22 | Russian Satellite TV Shows a Ukraine Message: 'Blood on Your Hands' | 22-00011706 |
| | Threat Activity Alert: Hacktivist Actor 'Network | |

| | | |
|---|---|---|
| 5/10/22 | Battalion 65' Claims Hack-and-Leak Attack Against Russian Payment and Financial Services Company on Twitter | 22-00011241 |
| 5/10/22 | Threat Activity Alert: English-Speaking Group 'CaucasNet' Claims Hack Against Patrol Robots of Russian Robotics Company on Telegram | 22-00011775 |
| 5/11/22 | Threat Activity Alert: Anonymous-Affiliated Actors 'DepaixPorteur' and 'B00daMooda' Claim Hack-and-Leak Attack Against Polar Branch of Russian Federal Research Institute of Fisheries and Oceanography on Twitter | 22-00012034 |
| 5/12/22 | Threat Activity Alert: Pro-Russia Hacktivist Group 'Legion' Claims DDoS Attacks Against Ukrainian ISPs and Italian Government Sites on Telegram | 22-00012033 |
| 5/13/22 | Threat Activity Alert: Pro-Russia Hacktivist Group 'Legion' Announces DDoS Attacks on 100 Latvian Sites in Protest Against Removal of Soviet Monument in Riga | 22-00012129 |
| 5/13/22 | Threat Activity Alert: English-Speaking Actor 'Kelvin Security' Shares Data from Russian Telecom Construction Company 'TRON' Under #OpRussia | 22-00012105 |

Table 8: Mandiant reporting about hacktivist activity

**Please rate this product by taking a short four question survey**

## First Version Publish Date

May 16, 2022 05:49:14 PM

### Threat Intelligence Tags

Actors

- UNC1151
  Aliases
  - UNC 1151
  - UNC-1151
  - UNC1151
- APT29
  Aliases
  - APT 29
  - APT-29
  - APT29
- UNC2589
  Aliases
  - UNC 2589
  - UNC-2589
  - UNC2589
- FIN7
  Aliases
  - FIN 7
  - FIN-7
  - FIN7
- APT28
  Aliases
  - APT 28
  - APT-28
  - APT28
- TEMP.Vermin
  Aliases
  - TEMP.Vermin
- Sandworm Team
  Aliases
  - Sandworm Team
- TEMP.Armageddon
  Aliases
  - TEMP.Armageddon

Affected Industries

- Energy & Utilities
- Financial Services
- Governments

- Media & Entertainment
- Telecommunications

Affected Systems

- Users/Application and Software

Intended Effects

- Military Advantage
- Political Advantage
- Financial Theft
- Disruption
- Destruction
- Interference with ICS

Motivations

- Military/Security/Diplomatic
- Ideological/Religious
- Financial or Economic
- Ethnic/nationalist

Malware Families

- NEARTWIST
  Aliases
  - NEARTWIST
- CONTI
  Aliases
  - CONTI
- LOCKBIT
  Aliases
  - LOCKBIT
- SDELETE
  Aliases
  - SDELETE
- EMPIRE
  Aliases
  - EMPIRE
- V2
  Aliases
  - V 2, V-2, V2

Source Geographies

- Belarus
- China
- Iran
- Russia

Tactics, Techniques And Procedures (TTPs)

- Defacement
- Distributed Denial-of-Service (DDoS) Attack
- Malware Propagation and Deployment
- Doxing
- Social Engineering

Target Geographies

- Ukraine

Targeted Information

- Financial Data
- Government Information

## Version Information

Version:1.0, May 16, 2022 05:49:14 PM