Microsoft Threat Intelligence

A year of Russian hybrid warfare in Ukraine

What we have learned about nation state tactics so far and what may be on the horizon

March 15, 2023

Microsoft

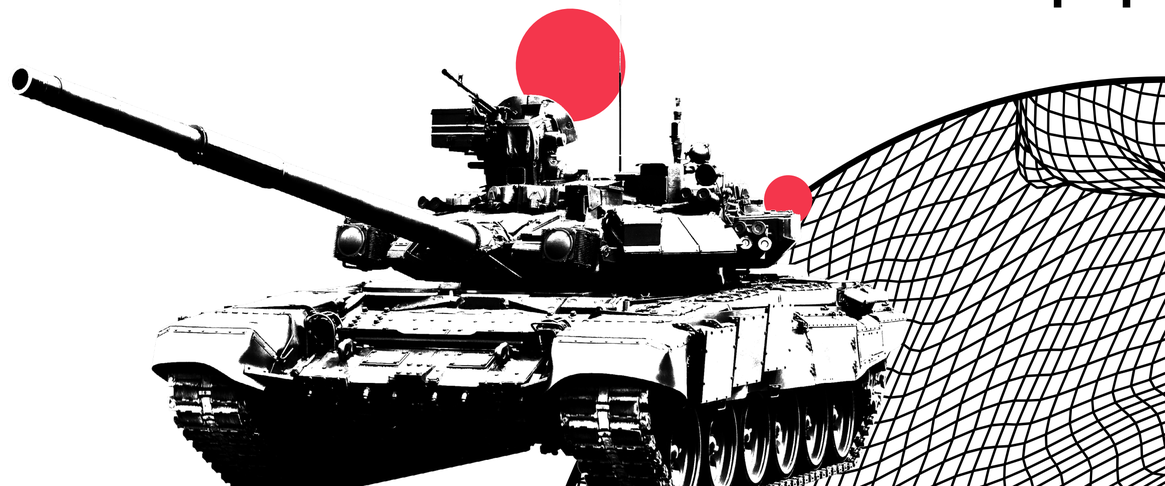


Table of contents

Introduction

Prior to Russia's full-scale invasion of Ukraine on February 24, 2022, many observers expected that a Russian-led hybrid war, like that observed when Russia invaded Donbas and illegally annexed Crimea in 2014, would involve marrying cyber weapons, influence operations, and military force to swiftly overrun Ukrainian defenses. Now, one year after its full-scale invasion, Russia's military has indeed wrought physical devastation in Ukraine but has not achieved its objectives—in part because Moscow's parallel cyber and influence operations have largely failed.

Russian destructive cyberattacks have fluctuated in intensity and been frequently repelled. Most Kremlin-backed propaganda campaigns aimed at Ukraine have had little impact, revealing the limitations of Russian influence when met by a resilient Ukrainian population. Russian state-affiliated cyber and influence actors, however, have not been deterred and continue to seek alternative strategies inside and outside Ukraine.

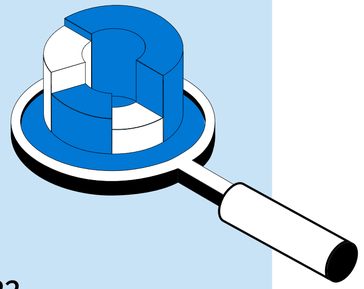
Since January 2023, Microsoft has observed Russian cyber threat activity adjusting to boost destructive and intelligence gathering capacity on Ukraine and its partners' civilian and military assets. IRIDIUM—also known as Sandworm, a threat actor attributed to Russia's military intelligence agency (GRU)—appears to be preparing for a renewed destructive campaign, like its wave of Foxblade and Caddywiper malware deployments against Ukrainian government and media organizations in the early days of the war. As of late 2022, the threat actor may also have been testing additional ransomware-style capabilities that could be used in destructive attacks on organizations outside Ukraine that serve key functions in Ukraine's supply lines. The Prestige ransomware operation against a Polish firm in late 2022 provides a precedent for such attacks.

Microsoft investigations have revealed that cyber threat actors with known or suspected ties to the GRU, Russian Foreign Intelligence (SVR), and Russian Federal Security (FSB) services have attempted to gain initial access to government and defense-related organizations in Central and Eastern Europe and the Americas. Between January and mid-February 2023, Microsoft threat intelligence analysts have found indications of Russian threat activity against organizations in at least 17 European nations, with the government sector the most targeted. While these actions are most likely intended to boost intelligence collection against organizations providing political and material support to Ukraine, they could also, if directed, inform destructive operations.

Meanwhile, Moscow's propaganda machine has taken aim at Ukrainian refugees and populations in countries aiding Ukraine and is stoking fears that Moldova is the next target for a Russian invasion. Starting in January 2023, a Russian propaganda campaign targeted Ukrainian diaspora in the European Union (EU) and United Kingdom (UK) with claims that Ukrainian refugees abroad will be extradited and forcibly conscripted into the Ukrainian Armed Forces.[1] In mid-February, Moldovan and Ukrainian authorities alleged a Russian plot to stage a coup.[2] Around that time, Moldova's pro-Russian Shor Party held protests to pressure Chișinău to pay for all citizens' winter energy bills, in line with Kremlin efforts to pressure neighbors and European states through simultaneous energy supply squeezes and messaging urging diplomatic reconciliation with Russia. Earlier in the year, pro-Russian hacktivist group KillNet claimed attacks targeting Moldovan government websites,[3] while several Moldovan political figures were the targets of a hack-and-leak campaign amplified by Russian state media called "Moldova Leaks."

1. https://web.archive.org/web/20230221212717/https://topwar.ru/210281-sbezhavshie-v-polshu-ot-mobilizacii-ukrainskie-muzhchiny-nachali-poluchat-povestki.html, https://web.archive.org/web/20230221212952/https://tass.ru/mezhdunarodnaya-panorama/16867563, https://web.archive.org/web/20230129061545/https://t.me/riafan/123713
2. https://www.bbc.com/news/world-europe-64626785
3. https://t.co/HFMX119pDd, https://twitter.com/paulaerizanu/status/1562783147397640196

Our analysis best fits into three periods of the war:



Phase 1 - January 2022 to Late March 2022
Russia's initial invasion of Ukraine

Phase 2 - Late March 2022 to September 2022
Russia's withdrawal from advance toward Kyiv to focus on the Donbas

Phase 3 - September 2022 to Present
Russia's reaction to Ukraine's counteroffensives in eastern and southern Ukraine to the present day.

We hope to provide some lessons learned from Russian state operations and Ukraine's resilience—lessons that can inform a broader playbook for defending against authoritarian aggression in the digital space.

As the war in Ukraine enters its second year, Microsoft offers insights and trends observed during Russia's first year of cyber and influence operations targeting Ukraine and its supporters.

The data and conclusions herein are drawn largely from the threat hunting and incident response work of the **Microsoft Threat Intelligence Center (MSTIC)**, the **Detection and Response Team (DART)**, **Defender for Endpoint Threat Intelligence**, other security teams across Microsoft, and Ukrainian, worldwide government, and industry partners. Our insights into malign influence activity are drawn from the **Digital Threat Analysis Center's (DTAC)** open-source investigative work and research from our **AI for Good Lab**.

Hybrid war in review

Phase 1: Cyber and influence operations parallel Russia's full-scale military invasion

January 2022 – Late March 2022

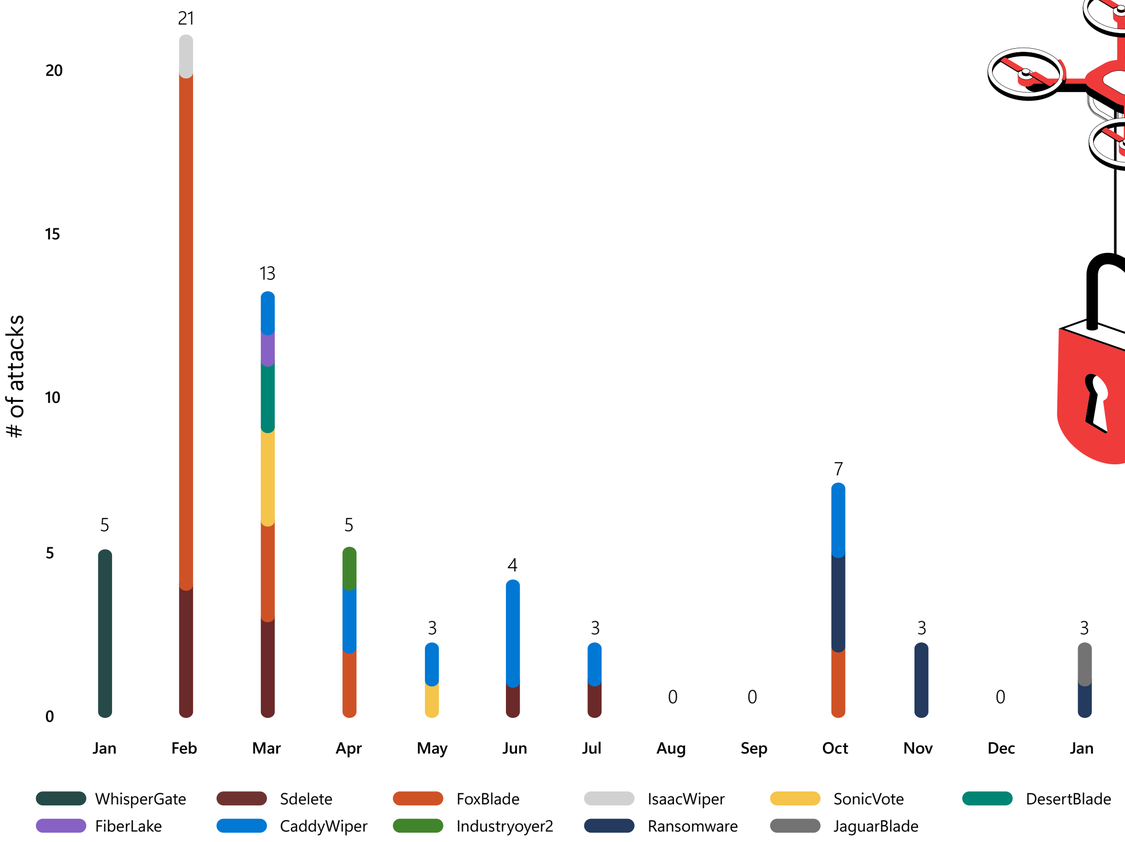
Russian cyber threat and influence actors focused much of their operational capacity on achieving an early victory in Ukraine, consistent with the value that Russian military thought places on high impact at the start of a war.[4] Perhaps anticipating a quick and decisive victory, early Russian cyberattacks did not appear to account for the rapid response by Ukrainian network defenders and the international technology community to identify and mitigate malicious activity.

In January 2022, Russian military actor DEV-0586 deployed the WhisperGate wiper against a few Ukrainian organizations.[5] Since that time, Russian threat actors have employed at least nine new wiper families and two types of ransomware against more than 100 Ukrainian organizations. Hundreds of systems across the Ukrainian government, critical infrastructure, media, and commercial sectors have been affected by wipers that permanently delete files and/or render machines inoperable, but most of these attacks coincided with Russia's initial invasion in February and March 2022.

Threat actors aligned with the Russian GRU—most prominently IRIDIUM—have not returned to the large-scale deployment of destructive wipers observed in the first 30 days of the war. Active incident response and information sharing between Ukrainian and allied network defenders has almost certainly disrupted destructive efforts and may be pressing threat actors to develop and deploy new and diverse malware families. The peaks and valleys of deployment and periodic introduction of new wipers or variants suggest continued reactive development of destructive capability rather than a deep reservoir of destructive tools.

Russian influence actors attempted to flood social media platforms in an information offensive ahead of the full-scale invasion. Russian state-affiliated messengers attempted to dehumanize Ukrainians by calling for the "denazification" of the country and shift blame to the US, alleging American biolaboratories were creating bioweapons in Ukraine.[6,7] Simultaneously, the Kremlin attempted false flag provocations—including plans to disseminate a "very graphic" fake video—to create a pretext for invasion.[8]

Destructive attacks observed since January

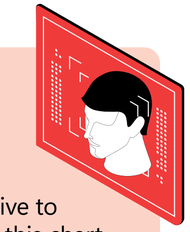


Data in the chart above is drawn from first-party sources and information shared by Ukrainian and industry partners about the different malware or native tools Russian threat actors used for destruction of data at targeted organizations. The targets were almost exclusively Ukrainian, except for a Polish transportation sector organization impacted by IRIDIUM's Prestige ransomware in October.[9]

4. Russia_Military_Power_Report_2017.pdf (dia.mil); https://www.cna.org/reports/2021/10/russian-military-strategy-core-tenets-and-concepts , pg 3.
5. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/, https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion.
6. https://www.reuters.com/world/russia-demands-us-explain-biological-programme-ukraine-2022-03-09
7. https://www.nytimes.com/2022/03/17/world/europe/ukraine-putin-nazis.html, interfax.ru/russia/824200.
8. https://www.nytimes.com/2022/01/14/us/politics/russia-ukraine-us-intelligence.html, https://www.theguardian.com/world/2022/feb/03/ukraine-russia-fake-attack-video-us-claims, https://foreignpolicy.com/2022/01/14/russia-provocation-war-pretext-false-flag-ukraine-eastern-us-intelligence
9. For additional information on the destructive tools observed see: https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/#updated-malware-details; https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland; https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded; https://blog.eset.ie/2023/01/30/swiftslicer-new-destructive-wiper-malware-strikes-ukraine.

Russia's propaganda ecosystem targeting Ukraine

Russia's propaganda ecosystem is comprised of legacy and post-invasion propaganda elements that have waxed and waned in prominence over the course of the war. The legacy ecosystem has four main categories: 1) the Kremlin's so-called "fifth column" in Ukraine, 2) media of the self-declared Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR), 3) Russian intelligence-linked media, and 4) influencers and war correspondents, mostly in Eastern Ukraine. Post-invasion, "localized" news sites, newly launched media outlets, and organized groups—some affiliated with prominent agents-of-influence—push Kremlin-aligned narratives.



Significance scored across war timeline

0 1 2 3

Each entity is scored using the above key relative to that entity's significance across the timeline in this chart (right). Some of the categories in the chart were highly influential at the start of the war but have since waned in relevance. Others have emerged since the invasion and remain prominent voices.

War in Ukraine timeline

- Phase 0 — Pre-Jan 2022
- Phase 1 — Jan 2022 to Mar 2022
- Phase 2 — Mar 2022 to Sept 2022
- Phase 3 — Sept 2022 to Present

The Kremlin's so-called "5th Column"

0 1 2 3

- Zik
- NewsOne
- Nash
- 112 Ukraina
- Golos Pravdy
- Ukraina.ru

0 1 2 3

- Mykola Azarov
- Andrii Derkach
- Viktor Medvedchuk
- Yevhen Murayev
- Anatoly Shariy
- Ilya Kiva
- Vladimir Kornilov
- Rostyslav Ishchenko

Media of self-declared Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR)

DONETSK

- DNR Ministry of Info
- Denis Pushilin
- Donbass Forces
- Oplot TV
- First Republican
- Eduard Basurin

LUHANSK

- LNR Ministry of Communications
- Lugansk Media Centre
- Lugansk 24

Russian intelligence-linked media

FSB 0 1 2 3

- NewsFront
- Politnavigator
- Southfront
- Antifashist

SVR 0 1 2 3

- Odna Rodyna

GRU
GRU-affiliated channels 0 1 2 3

- Legitimniy
- Netipichnoe Zaporozhe
- Rezident
- Odesskiy Fraer
- Spletnitsa
- Trempel Kharkov

0 1 2 3

- Donbass Tragedy

Influencers, war correspondents, and amplifiers

0 1 2 3

- Novorossia
- ANNA News
- RusVesna

RU CORRESPONDENTS 0 1 2 3

- Semyon Pegov
- Evgeniy Poddubny
- Sasha Kots

FOREIGN CORRESPONDENTS 0 1 2 3

- Graham Phillips
- Thomas Röper
- Alina Lipp

2022 invasion: New media

"LOCAL" NEWS 0 1 2 3

- ZOV
- Kherson Life

Localized Telegram

- Kherson
- Mariupol
- Zaporizhzhia
- + more

MEDIA OUTLETS 0 1 2 3

- Za! TV
- Radio Tavria
- Novoe Vremya
- Priazovsky Rabochiy
- Novaya Kakhovka
- Naddnepryanskaya Pravda
- Kharkov Z
- Radio Breeze

PR FOR OCCUPATION 0 1 2 3

- Alexander Malkevich
- Young Guard
- Volunteer Battalion
- Yunarmia
- Leaders of Revival
- Dvizheniya Pervykh
- We Are Together
- Young South
- Volunteers of Victory

Prior to Russia's 2022 invasion, Ukraine's media environment had long been heavily influenced by major pro-Russian Ukrainian figures commonly referred to as the Kremlin's "fifth column." These media figures and moguls, such as Viktor Medvedchuk and Yevhen Muraev, who collectively owned four of the largest Ukrainian channels, all with strong pro-Russian bias, played major roles in Russian influence operations in the lead-up to the invasion. In addition to spreading pro-Russian propaganda across the airwaves, the Kremlin planned to install Muraev at the head of a pro-Russian government, according to British intelligence.[10]

The self-declared Donestk People's Republic (DNR) and Luhantsk People's Republic (LNR) also used their centralized information environments—with many prominent media networks controlled by the DNR's Ministry of Information and LNR's Ministry of Communications—to spread Russian war propaganda ahead of and during the invasion. Officials of the unrecognized republics often acted as primary sources for the most egregious propaganda, a trend that continues today.

Many of the most prolific propaganda efforts in Ukraine, dating back to Russia's 2014 invasion, have been backed by Russia's Federal Security Service (FSB)—such as NewsFront—or allegedly seed-funded by Kremlin presidential grants, like PolitNavigator.[11,12] In 2022, these outlets remained among the most virulently anti-Ukrainian in their content. Separately, Ukraine's Security Service, the SBU, has outed numerous anonymous, ostensibly local news-focused Telegram accounts as managed by Russia's GRU. These channels aim to influence Ukrainian audiences in cities Russia saw as critical in its attempts to capture the country at the start of the war.[13]

Finally, dozens of pro-Russia social media influencers and war correspondents attempted to shape the perception of events on the ground, particularly in Donbas. These war correspondents form their own media brands while still contributing to Russian state-affiliated media. Figures like Semyon Pegov (known as "WarGonzo"),[14] Evgeniy Poddubny,[15] and Sasha Kots[16] are among the most prominent such correspondents, all of whom contribute to state media and have been awarded medals by the Kremlin for "courageous" and "professional" coverage.[17,18,19]

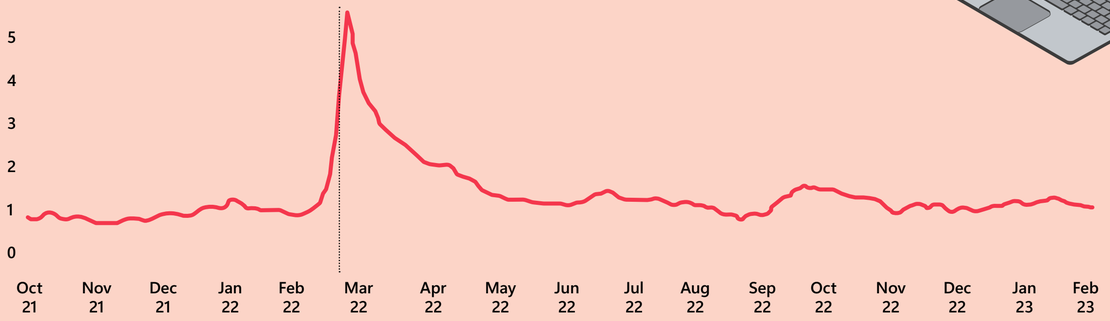
Russia's influence efforts in the weeks leading up to the invasion and the early days of the war largely fell flat among Ukrainian and western audiences, upended by the proactive release of intelligence.[20] Additional challenges limited the Kremlin's impact once tanks rolled across the border and complicated Russia's ability to reach western audiences online, with technology and social media companies removing many Kremlin-affiliated accounts.[21,22,23] RT America—which had offices in New York, Miami, Los Angeles, and Washington, DC—shut down.[24] Research groups and media outlets debunked narratives attempting to blame Ukraine for Russian attacks, like the hospital bombing in Mariupol and the massacre in Bucha in March 2022.[25,26]

In our June 2022 report "Defending Ukraine: Early Lessons from the Cyber War," we introduced the Russian Propaganda Index (RPI), a metric that measures the flow of traffic to sites known to promote pro-Kremlin narratives as a proportion of overall internet traffic.

In that report, we illustrated how Russian propaganda consumption in Ukraine spiked at the onset of the war as Russian influence operations mirrored Russia's full-scale invasion on the ground. RPI trends since the invasion illustrate the efficacy of efforts to combat the spread of Russian propaganda within Ukraine. By June 2022, RPI levels had returned to levels close to pre-war averages.

Within Russia, the Kremlin's robust domestic propaganda system largely maintained its grip, in no small part due to its wave of "fake news" laws.[27] However, small but significant acts of protest indicated some at home did not condone the horrors of the invasion.[28]

Russian propaganda consumption in Ukraine



10. https://www.reuters.com/world/who-is-yevhen-murayev-named-by-britain-kremlins-pick-lead-ukraine-2022-01-23/
11. https://home.treasury.gov/news/press-releases/jy0126,
12. https://informnapalm.org/en/frolovleaks-viii-the-orthodox-melancholy/
13. https://ssu.gov.ua/en/novyny/sbu-vykryla-ahenturnu-merezhu-spetssluzhb-rf-yaka-destabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly
14. https://t.me/wargonzo
15. https://t.me/epoddubny
16. https://t.me/sashakots
17. https://www.m24.ru/news/obshchestvo/12012023/540189, https://tass.ru/obschestvo/3213554
18. https://texty.org.ua/projects/108161/telegram-occupation-how-russia-wanted-breed-media-monster-ended-paper-tiger/
19. https://t.me/Kharkov_Z_news/10666
20. https://www.cnn.com/2022/02/11/politics/biden-administration-russia-intelligence/index.html
21. https://home.treasury.gov/news/press-releases/jy0628
22. https://www.politico.eu/article/russia-rt-sputnik-illegal-europe
23. https://www.cnn.com/2022/03/03/media/rt-america-layoffs/index.html
24. https://www.latimes.com/entertainment-arts/tv/story/2022-03-04/russia-backed-rt-america-to-cease-production
25. https://www.usatoday.com/story/news/factcheck/2022/03/15/fact-check-russian-attack-mariupol-hospital-not-staged/7041649001
26. https://www.pbs.org/newshour/world/amid-horror-in-bucha-russia-relies-on-propaganda-and-disinformation
27. https://www.politico.eu/article/russia-expand-laws-criminalize-fake-news
28. https://www.reuters.com/world/europe/more-than-64-people-detained-anti-war-protests-russia-protest-monitor-2022-03-06; https://www.nytimes.com/2022/02/24/world/europe/russia-protests-putin.html; https://apnews.com/article/russia-ukraine-europe-media-arrests-12b5b56747d611bcaea3c02e7cc56a7c

Phase 2: Cyber and influence focus turns to undermining Kyiv's foreign and domestic support

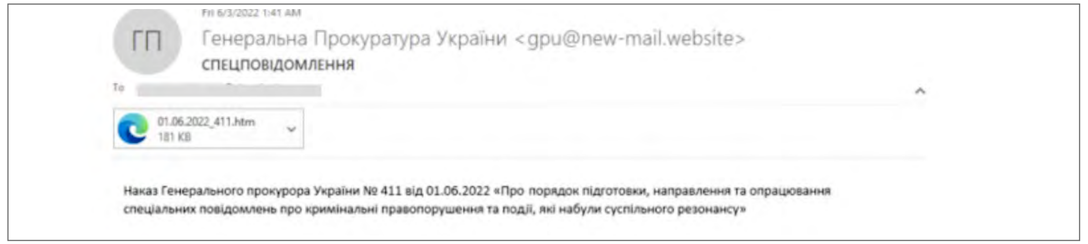
Late March 2022 – September 2022

From late March to April 2022, Russian forces withdrew from their axes of advance toward Kyiv from the north and east to focus on Donbas and other then-occupied regions.[29] At this time, Microsoft observed a cyber and influence operational pivot to target material and political support to Ukraine. Microsoft telemetry showed Russian threat actors directing their destructive cyberattacks toward the logistics and transportation sector inside Ukraine possibly to disrupt weapons or humanitarian flow to the frontlines. As reported in June, Microsoft observed GRU-affiliated threat actor IRIDIUM launch destructive wiper attacks and intelligence collection intrusions against Ukraine's transportation sector in the spring.[30] Russian forces launched numerous missile strikes against Ukrainian transportation infrastructure during this same time, suggesting a disruption of the flow of goods and people across Ukraine as a common objective.[31]

Cyber threat actors also conduced robust cyberespionage operations against organizations providing military or humanitarian assistance to Ukraine. ACTINIUM, also known as Gamaredon, conducted multiple phishing campaigns targeting humanitarian aid and resettlement organizations active in Ukraine, and entities involved in war crimes investigations from April through June 2022.[32] In April, ACTINIUM attempted to gain access to networks of entities sympathetic to Ukraine by sending phishing emails masquerading as Ukrainian military officials asking for additional humanitarian and military assistance. From late May to June, the group sent targeted phishing emails to multiple relief organizations based in Ukraine and the Baltics, as well as intergovernmental agencies assisting victims of war and documenting war crimes.

Since at least May, SEABORGIUM, also known as ColdRiver, has sent phishing messages to compromise organizations that produce or transport weapons, drones, protective equipment, and other military supplies for US and European military customers. Many of the targeted organizations provide services in support of Ukraine.[33]

Moscow also remobilized its propaganda efforts to target populations within occupied Ukrainian territory and abroad, pivoting to focus on fighting that hit the Zaporizhzhia Nuclear Power Plant in southern Ukraine, with Russia's propagandists fearmongering about nuclear attacks.[34] Aiming to garner Kremlin-aligned coverage in international press, the Russian government sponsored a PR tour of Donbas in the spring—with press members visiting from France, Germany, India, and Turkey, among others—as well as tours to the Zaporizhzhia Nuclear Power Plant.[35] Kremlin-affiliated occupation authorities even appeared to take control of much smaller radio stations and local print outlets in many occupied cities.[36]



Screenshot of one of the phishing messages ACTINIUM sent to accounts at Ukraine- based humanitarian organizations between April and June. The themes ranged from purported official communications on decrees and requests for additional humanitarian assistance. The lure above, masquerading as a communication from Ukraine's General Prosecutor's Office, concerns procedures for reports on high-profile criminal cases, according to machine translation.

29. https://www.reuters.com/world/europe/russia-says-first-phase-ukraine-operation-mostly-complete-focus-now-donbass-2022-03-25/; https://www.businessinsider.com/russian-forces-withdraw-kyiv-failure-capture-ukraine-capital-city-war-2022-4; https://thehill.com/policy/defense/3260613-pentagon-russian-forces-outside-kyiv-chernihiv-have-completely-withdrawn/
30. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
31. https://www.cnn.com/2022/05/04/europe/ukraine-russia-railways-intl/index.html
32. For past reporting on the technical details of ACTINIUM's phishing campaigns see https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
33. Our statement about support to Ukraine is based on information posted on the impacted organizations' public websites.
34. https://euvsdisinfo.eu/report/ukraines-attack-on-zaporizhzhia-plant-is-nuclear-terrorism
35. https://t.co/gY6zJ2TDCQ
36. https://t.me/Kharkov_Z_news/10666

Phase 3: Russia pairs kinetic operations with doubled-down cyber and influence operations

September 2022 – Present

Following Ukraine's successful southern and northeastern counteroffensive from late August through September, the Russian government deepened its claims to Ukrainian territory and intensified military operations designed to break the will of the Ukrainian people.[37] Moscow announced a partial military mobilization in late September and illegally annexed Luhansk, Donetsk, Zaporizhzhia, and Kherson regions of Ukraine by early October.[38] Almost immediately after claiming sovereignty over eastern Ukrainian territory, the Russian military launched a barrage of missile strikes on critical energy infrastructure throughout Ukraine's major cities, cutting heat and power to civilians in the impacted areas as winter set in. In December, Russian President Vladimir Putin disregarded international criticism of the missile strike, claiming attacks on energy infrastructure would continue.[39]

Russian cyber threat and influence operators took measures to augment Moscow's political and military actions during this time. As we reported in December, IRIDIUM directed wiper malware attacks against civilian power and water infrastructure in Ukraine, just as the Russian military launched missile strikes on that same infrastructure.[40]

Outside of Ukraine, IRIDIUM escalated operations to disrupt supply chains to Ukraine while other GRU-linked groups targeted Western defense-related organizations, likely for intelligence collection. MSTIC uncovered and made public the assessment that IRIDIUM expanded destructive attacks with the Prestige ransomware operation against the transportation sector in Poland, a NATO member and key logistical hub for Ukraine-bound supplies.[41] As of October, another GRU-linked group, STRONTIUM, had potentially compromised a separate Polish transportation sector firm, and later increased reconnaissance against NATO-affiliated organizations, suggesting an intent to conduct future intrusions against this target set.

Depicted in the bottom half of the chart "Russia's Propaganda Ecosystem Targeting Ukraine" on page 6 are the media and PR efforts stood up since the war began designed to push Kremlin talking points into local media environments. Established Russian agents-of-influence promoted newly launched local propaganda outlets like Radio Tavria and Za! TV to launder Kremlin-aligned narratives in occupied and annexed territory. These agents are also key to maintaining Russia's current state-sponsored PR efforts in occupied territory, promoting pro-Russia youth organizations such as the Yunarmia (Youth Army), Molodaya Gvardia (Youth Guard of United Russia), and YugMolodoy (Youth South).[42] Agents-of-influence have also spun up crowdfunding efforts to support Russia's war effort from back home. One such example is through "Readovka Helps," an organization affiliated with pro-Russian outlet Readovka and led by Alexander Ionov, who was indicted by the US Justice Department for working in conjunction with the FSB and "orchestrating a years-long foreign malign influence campaign."[43] Despite purporting to maintain a humanitarian mission, Readovka Helps has crowdfunded supplies for Russian soldiers.

Online, websites presenting as Ukrainian local news outlets pull content from Russian state-affiliated sources and prominently display Russia's "ZOV" war symbols in their digital brands. These sites and channels' operations ebb and flow: While some of the sites have gone dormant, particularly those tailored to Ukrainian cities Russia failed to occupy, others have persisted, laundering overt Russian media and pro-Kremlin messages.[44] Pro-Russian social media groups like the "Digital Army of Russia,"[45] created in January 2023, use brigading tactics—or the coordinated attack by a group of users—to spam Ukrainian social media communities online with Russian war propaganda.[46]

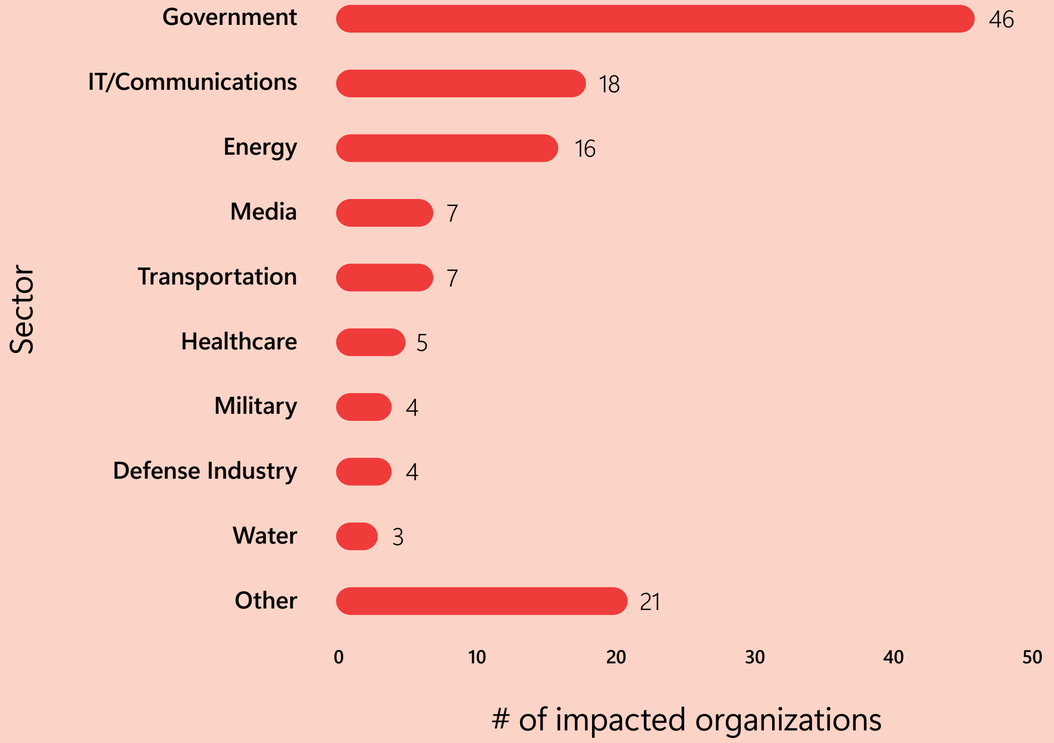
Russian agent-of-influence Alexander Ionov in a post by Readovka Helps, which requests donations for Russia's war. (Source: https://t.me/readovka_pomogaet/17.)

37. https://www.cnn.com/2022/08/29/politics/ukraine-shaping-counteroffensive/index.html; https://www.reuters.com/world/europe/ukrainian-counter-attack-underway-un-pushes-nuclear-plants-safety-2022-09-07/
38. https://www.bbc.com/news/live/world-62970683; https://www.bbc.com/news/world-europe-63149156
39. https://www.themoscowtimes.com/2022/12/08/ukraine-war-putin-vows-to-keep-striking-ukraine-power-grid-a79635; https://edition.cnn.com/2022/12/12/europe/melitopol-ukraine-strikes-russia-intl/index.html
40. https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/
41. https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/
42. https://www.rferl.org/a/ukraine-crimea-russia-militarization-schools/32157588.html
43. https://www.justice.gov/opa/pr/russian-national-charged-conspiring-have-us-citizens-act-illegal-agents-russian-government
44. https://texty.org.ua/projects/108161/telegram-occupation-how-russia-wanted-breed-media-monster-ended-paper-tiger/
45. https://hromadske.ua/posts/rosiyani-stvorili-internet-armiyu-shob-siyati-paniku-sered-ukrayinciv-i-lyakati-yih-nastannyam-z-bilorusi
46. https://institute.global/policy/social-media-futures-what-brigading

Digital outlook for the second year of the Russian invasion of Ukraine

Since mid-January this year, destructive actor IRIDIUM has conducted actions that could be in preparation for a renewed offensive: conducting reconnaissance, initial access operations, and wiper deployments against targets within Ukraine that are reminiscent of the early days of the invasion. Between January 12-28, 2023, IRIDIUM launched several phishing campaigns to gain access to accounts at defense industrial base and energy sector organizations in Ukraine. During this same period, the threat actor deployed a new variant of Caddywiper malware against a major Ukrainian media outlet. Of note, Ukrainian media was an early target of IRIDIUM's DesertBlade wiper. By late January, a suspected Russian threat actor deployed a new wiper MSTIC calls LeopardBlade against systems associated with a regional government organization in northern Ukraine. Cybersecurity firm ESET also spotted the attack and has attributed it to a group most equivalent to IRIDIUM.[47] MSTIC's independent attribution investigation is ongoing. An energy provider in this same region was a pre-invasion victim in early February 2022.

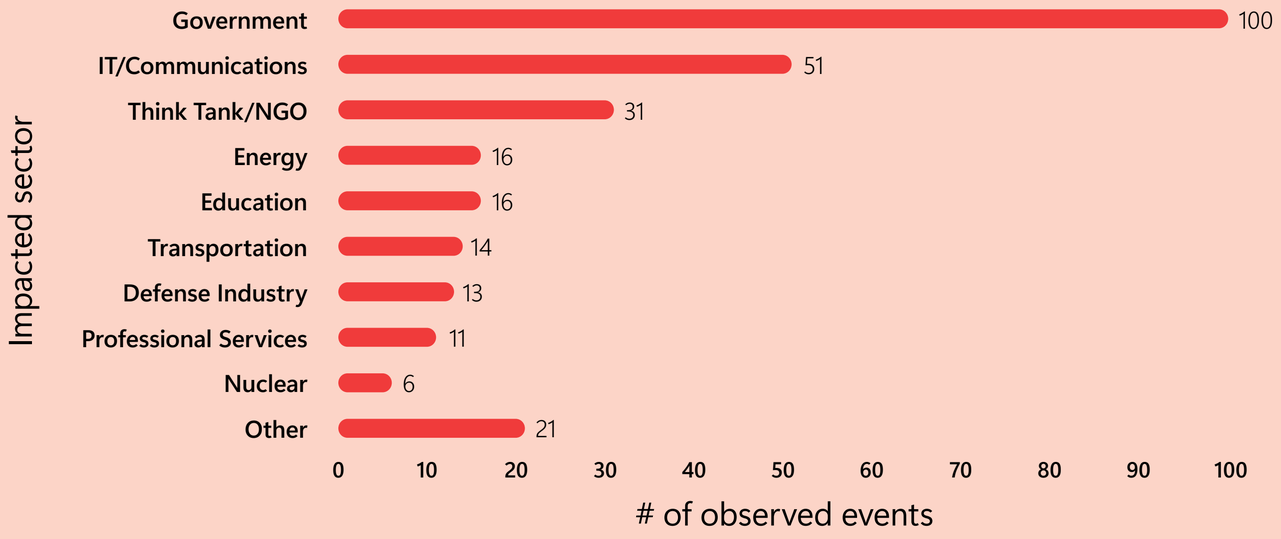
Sample of Ukraine targets since Feb 2022



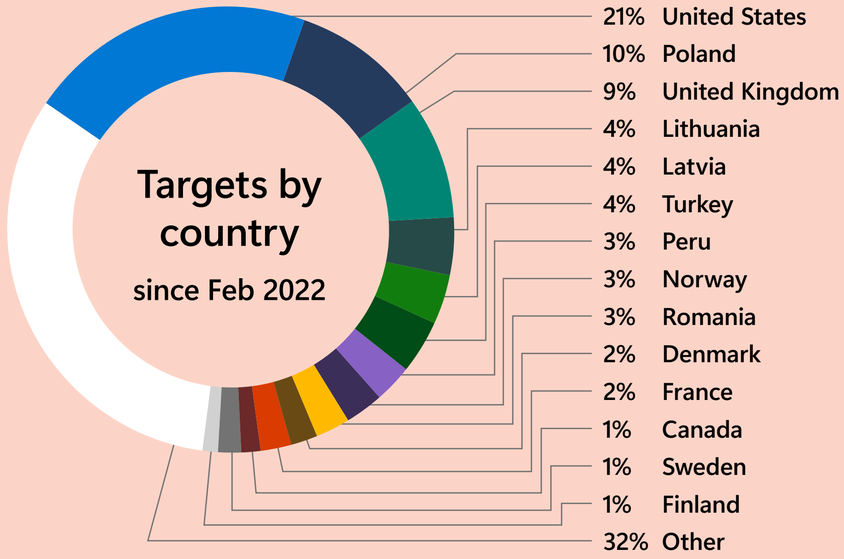
This chart provides a sample of Ukrainian sectors impacted by known or suspected Russian state-affiliated network intrusions or destructive attacks, as reflected in Microsoft data between February 2022 and January 2023.

47. https://www.welivesecurity.com/2023/01/27/swiftslicer-new-destructive-wiper-malware-ukraine/

Targeted sectors outside Ukraine since Feb 2022



Within the 74 countries targeted by Russian threat actors between February 23, 2022 and February 7 of this year, Russian threat actors were most interested in government and IT sector organizations, just as they were in Ukraine. Several actors compromise IT firms to exploit trusted technical relationships and gain access to those firms' clients in government, policy, and other sensitive organizations.



Excluding Ukraine, Microsoft has observed Russian nation state threat activity against organizations based in 74 countries, between February 23, 2022 and February 7 of this year. EU and NATO member states, especially on the eastern flank, dominate the top 10 most targeted countries by number of threat events recorded. However, Russian threat actors conducted activities that ranged from reconnaissance to data exfiltration in organizations across the globe, in Africa, Asia, Latin America, and the Middle East.

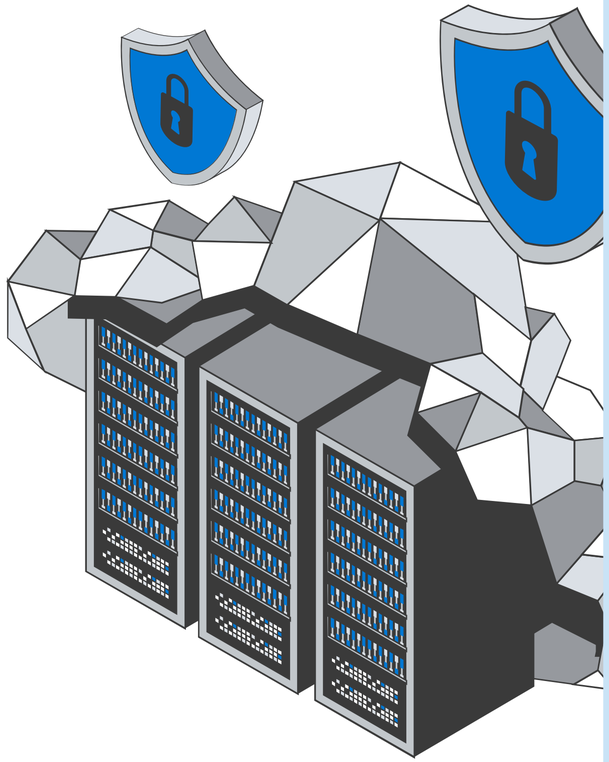
Cyberespionage operations against Ukraine's allies that pre-date and have persisted throughout the war are likely to intensify and focus on diplomatic and military-related organizations in NATO member states, Ukraine's neighbors, and against private sector firms directly or indirectly involved in Ukraine's military supply chain. For the past year, threat actors with known or suspected ties to the GRU, FSB, and SVR have targeted and potentially gained footholds in government, policy, or critical infrastructure sectors throughout the Americas, Europe, and elsewhere. Although most of the operations are probably espionage-focused, the GRU actors have already shown a willingness to use destructive tools outside Ukraine if instructed.

A quickly evolving digital landscape lends itself to renewed momentum for Russian information warfare as well. Despite limited success over the course of the war's first year, Russia's propaganda efforts will likely surge if the rumored military offensive in the spring of 2023 commences.[48]

48. https://www.politico.eu/article/manpower-will-be-crucial-for-russia-to-mount-a-spring-offensive, https://twitter.com/DefenceHQ/status/1622843727298404353

Trends in cyber threats since Russia's invasion

Russian cyber actors have time and again been stymied by a hypervigilant and engaged community of cybersecurity professionals within Ukraine and worldwide. As noted earlier, this community of defenders has likely blunted the impact of Russian state-affiliated network operations but has not stopped Moscow's efforts to gain access to and conduct attacks on desired targets.



Aside from the numerous destructive wiper attacks, Microsoft has observed three trends in Russian threat activity emerge as the war progresses that are likely to shape Russian cyber operations going forward:

1. **Using ransomware as deniable destructive weapon**
2. **Gaining initial access through diverse means**
3. **Integration of real and pseudo hacktivists for power projection**

In the following section we describe how each of these serve to complicate attribution, evade defenses, improve network persistence, or amplify effects of influence operations.

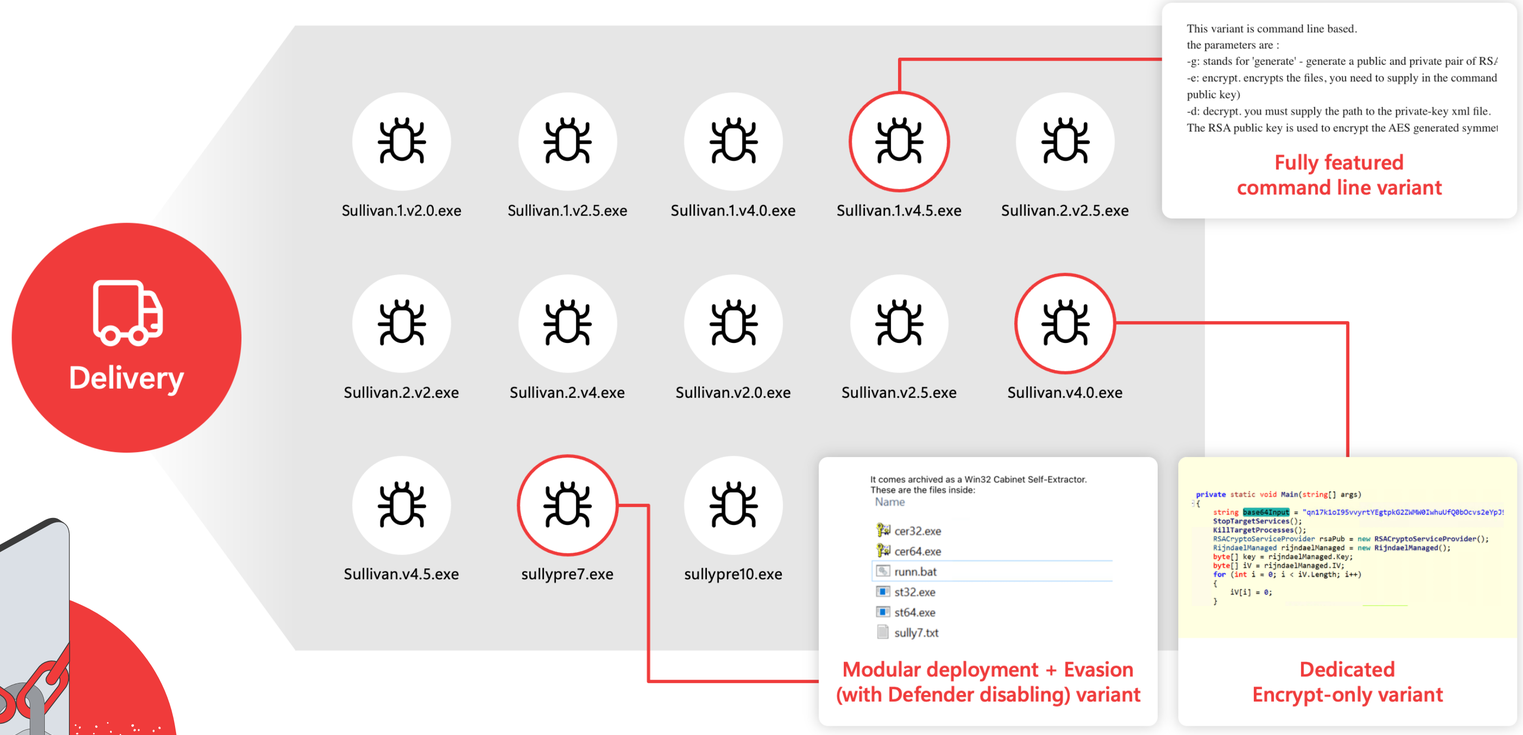
1

Using ransomware as deniable destructive weapon

IRIDIUM's development and deployment of Prestige ransomware against Ukrainian and Polish transportation sector organizations in October may have been a trial balloon, testing the international community's ability to attribute espionage operations to Moscow or testing the reaction of Ukraine's allies to a targeted destructive attack outside Ukraine. Since then, an actor that another cybersecurity firm suggests is likely to be IRIDIUM, deployed a new "Sullivan" ransomware (RansomBoggs).[49]

MSTIC observed at least three variants of this ransomware deployed against one Ukrainian organization over the course of three to four days, reflecting iterative development and refinement for modular functionality and improved detection evasion. As of December, MSTIC had only observed Sullivan at two Ukrainian organizations with no obvious military or political significance. IRIDIUM's use of ransomware in Poland and the testing and refinement of Sullivan on networks that seem more like cyber test ranges than actual targets suggest the actor is preparing Sullivan, or related malware, for use outside of Ukraine.

Sullivan variants with multiple modified wrappers deployed at 2 victims



MSTIC observed that between November 21 and 25, suspected Russian threat actors deployed at least three variants of the Sullivan ransomware, as well as two variants of the wrapper code, engineered to tamper with anti-malware products and make Sullivan more difficult to detect. The multiple files pictured above include the variants as well as additional files with names that suggest some relation to Sullivan, but whose functionality MSTIC could not determine. Overall, the actor made rapid adaptations over eight distinct attempts to evade detections and mitigations and destroy network systems over this four-day period.

49. https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/

2

Gaining initial access through diverse means

Throughout the conflict, Russian threat actors have gained initial access to their targets within and outside of Ukraine using a diverse toolkit. On a technical level, common tactics and techniques have included the exploitation of internet-facing applications, backdoored pirated software, and ubiquitous spearphishing. IRIDIUM has backdoored pirated versions of Microsoft Office to gain access to targeted organizations in Ukraine. Microsoft also assesses that the actor is responsible for uploading a weaponized version of Windows 10 to Ukrainian forums, exploiting demand for low-cost versions of the software to gain access to government and other sensitive organizations in Ukraine.

Just before and early in the war, Microsoft observed that DEV-0586 exploited Confluence servers to gain access to Ukrainian organizations later impacted by Whispergate wiper malware or other operations. STRONTIUM has used public exploits to compromise on-premises Microsoft Exchange servers and abuse Exchange Online to gain access to government and transportation sector organizations in Central Europe, among other targets. In late 2022, IRIDIUM sent spearphishing emails to dozens of organizations in Ukraine, as well as Romania, Lithuania, Italy, the United Kingdom, and Brazil, which included malicious payloads targeting CVE-2022-41352 in on-premises Zimbra servers. The targeted sectors included, among others, IT, energy, disaster response, finance, media, and refugee assistance.

Russian threat actors are also actively abusing technical trust relationships, targeting IT providers to reach more sensitive targets downstream without immediately triggering alerts. STRONTIUM and KRYPTON both attempted to access an IT provider in Poland that counts sensitive sectors among its client base. NOBELIUM, the same actor behind the SolarWinds intrusion, regularly attempts to compromise diplomatic organizations worldwide and foreign policy think tanks by first compromising cloud solutions and managed services providers that serve those organizations, a trend Microsoft first highlighted in 2021.[50]

50. https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium/

3

Use of hacktivists for power projection

An evolving landscape of real or pseudo hacktivist groups have played active roles in expanding the reach of Moscow's cyber presence since the outset of the war. Overall, these groups have served to amplify Moscow's displeasure with adversaries and exaggerate the number of pro-Russian cyber forces.

Microsoft and others in the US cybersecurity community have uncovered artifacts to indicate links between Russian military intelligence threat actors and hacktivist influence campaigns on Telegram.[51] In January 2023, DTAC observed overlap between IRIDIUM and pro-Russian hacktivist Telegram channel Cyber Army of Russia, which claims to be a grassroots movement of patriotic Russians. On January 17, IRIDIUM used a modified CaddyWiper payload in a destructive attack against a Ukrainian media organization that CERT-UA identified as Ukrinform.[52] The same day, Cyber Army of Russia claimed responsibility for the attack, asserting it was a response to the outlet's war reporting. The link between the IRIDIUM wiper attack and Cyber Army of Russia social media posts suggests coordination between the two entities but the exact nature of the relationship remains unclear.

51. https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

52. https://www.bleepingcomputer.com/news/security/ukraine-links-data-wiping-attack-on-news-agency-to-russian-hackers/; https://cip.gov.ua/ua/news/ukrinform-mogli-atakuvati-khakeri-z-ugrupuvannya-sandworm-pov-yazanogo-z-rosiiskim-gru-poperedni-dani-doslidzhennya-cert-ua

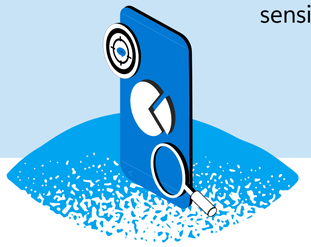
Trends in influence operations since Russia's invasion

Several additional trends have emerged in Russian influence operations as the war has progressed. Links between cyber actors and hacktivist groups in the information space represent one of the novel influence tactics used by Russia since the start of the war.

First,

Russian influence actors seek to weaponize fact-checking to spread Kremlin-aligned narratives.

Playing off information integrity efforts that emerged following the Kremlin's interference in the 2016 US presidential election, Russian messengers manipulate the language and credibility of fact-checking to spread false claims. Social media accounts purporting to be fact-checking entities, like the Telegram channel War on Fakes,[53] spread claims of "Ukrainian fakes" and "debunked" reports of Russian attacks on civilian and critical infrastructure.



Second,

pro-Russian actors online consistently spread purportedly leaked information to target political figures and governments supportive of Kyiv.

Russia's use of allegedly leaked materials—such as sensitive documents or communications—to wield influence is not a new tactic.[54] However, the regularity with which allegedly leaked materials have been promoted on pro-Russian social media channels throughout the war highlights the importance of hack-and-leak operations for the Kremlin. Leaks are often difficult to authenticate, making them an effective tool to amplify existing divisions and tensions by allegedly exposing sensitive information.

Third,

Russian government and affiliated entities regularly coordinate foreign press tours throughout occupied Ukraine to garner international media coverage from sympathetic voices and achieve wider messaging goals.

These tours often result in favorable coverage of Russia's war by the visiting reporters in their respective media outlets and websites, acting as a pathway for pro-Russian propaganda to reach audiences otherwise unlikely to engage with Russian media. Ostensibly independent reporters who publish content aligned with Kremlin propaganda narratives are frequently given honors by the government, including the Russian agency Rossotrudnichestvo's recent "Honest View" media awards.[55]

Finally,

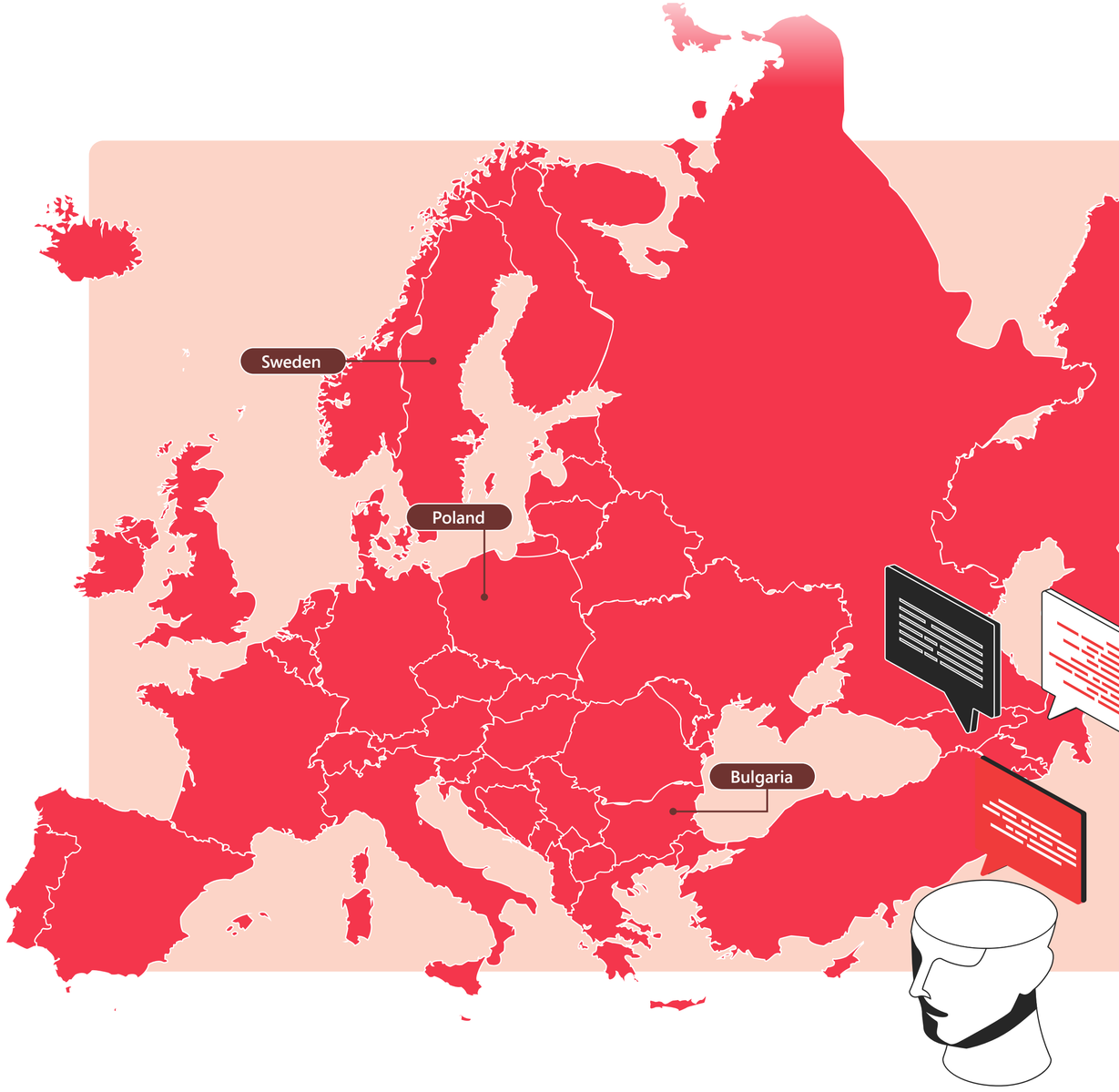
in addition to operations targeting Moldova, Russia continues to conduct multi-faceted influence operations in Ukraine's periphery and across Europe to widen societal divisions, discredit leadership supportive of Ukraine, and promote pro-Russian networks in those countries.

53. https://www.poynter.org/fact-checking/2022/how-war-on-fakes-uses-fact-checking-to-spread-pro-russia-propaganda/
54. https://www.wired.com/2017/05/russian-hackers-using-tainted-leaks-sow-disinformation, https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html
55. https://honestview.ru/tpost/e8zo9pxad1-the-honest-view-awards-were-announced-fo

Alongside Russia's destructive cyberattacks reaching into Poland, influence operations—at times supported by influence actors in Belarus—target Polish political bodies and everyday citizens alike with propaganda on energy and western militarism. The Kremlin continues to dedicate particular attention in Poland to stoking ethnic conflict between Poles and Ukrainians, attempting to foment nationalistic intolerance in Polish far-right circles. Political initiatives such as "Stop the Ukrainization of Poland"[56] and on-the-ground demonstrations such as those sponsored by "This Is Not Our War"[57] are promoted, amplified, and supported by Russian influence actors. Meanwhile, a recent campaign targeting the Ukrainian diaspora primarily in Poland and the Baltic states has been promoting fake or manipulated government documents indicating that Ukrainian men of military age will be forcibly conscripted to fight in Ukraine.[58]

Bulgaria, despite its own historical vulnerabilities to Russian influence operations, has emerged as a key partner to Ukraine in the face of Russia's full-scale invasion.[59,60] Bulgarian political leaders supplied military aid to Ukraine, despite the Kremlin's efforts to infiltrate Bulgarian politics through its diplomatic presence.[61] Bulgaria's support to Ukraine earned the ire of the Kremlin—cyberattacks blamed on Russian actors have targeted government websites while Gazprom, Russia's gas monopoly, chose to cut exports to Bulgaria and Poland early in the war.[62,63] Russian digital influence operations targeting Bulgaria leverage pro-Russian social media communities to direct local audiences to sites known to promote pro-Kremlin narratives. Russian propaganda consumption in Bulgaria spiked at the time of the invasion of Ukraine and has remained elevated, with current levels of consumption roughly 65% higher than pre-war averages.

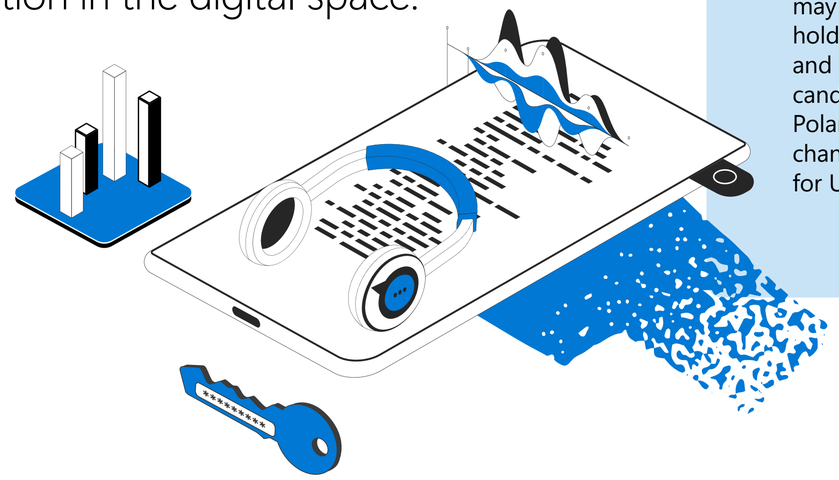
In Sweden, a provocation in late January in which a far-right political figure burned a Quran outside of the Turkish embassy in Stockholm sparked a strong response from Turkey, including statements from the Turkish government indicating Turkey would consider blocking Swedish accession into NATO.[64] While at the time of this writing it remains unknown if Russian actors contributed to the coordination of the provocation, the alleged organizers and sponsors of the provocation have ties to Russian state media and influence networks.[65] The incident highlights Sweden's NATO bid as a strategic issue for Russia, as well as Sweden and Turkey's relationship as a major wedge that Russia could exploit in future influence operations.



56. https://echodnia.eu/radomskie/marsz-stop-ukrainizacji-polski-w-warszawie-z-udzialem-radnego-z-szydlowca-arkadiusz-sokolowski-pokazany-w-rosyjskiej-telewizji/ar/c1-16928313, https://oko.press/posel-braun-wykorzystuje-sejm-by-nakrecac-antyukrainskie-nastroje-to-spodoba-sie-w-rosji, https://www.politnavigator.net/zdes-polsha-a-ne-ukropol-v-varshave-mitingovali-protiv-ukrainizacii.html, https://www.fondsk.ru/news/2022/09/26/ob-ukrainizatorskom-pomrachenii-varshavy-57279.html
57. https://news-front.info/2023/01/13/poljaki-provedut-miting-protiv-vstuplenija-polshi-v-konflikt-na-ukraine/, https://ria.ru/20230121/miting-1846466688.html
58. https://twitter.com/Cen4infoRes/status/1618592711442927617, https://www.gov.pl/web/baza-wiedzy/uwaga-csirt-nask-ostrzega-przed-kampania-e-mailowa-podszywajaca-sie-pod-ministerstwo-spraw-wewnetrznych-i-administracji, https://www.gov.pl/web/baza-wiedzy/uwaga-csirt-nask-ostrzega-przed-kampania-e-mailowa-podszywajaca-sie-pod-ministerstwo-spraw-wewnetrznych-i-administracji
59. https://www.politico.eu/article/ukraine-war-kremlin-reach-bulgaria-kiril-petkov
60. https://www.reuters.com/world/europe/bulgaria-send-its-first-military-aid-ukraine-2022-12-09, https://www.bloomberg.com/news/articles/2022-11-03/bulgaria-breaks-taboo-and-backs-first-military-aid-for-ukraine
61. https://www.reuters.com/world/europe/bulgaria-expels-70-russian-diplomatic-staff-over-espionage-concerns-2022-06-28/
62. https://www.rferl.org/a/bulgaria-cyberattack-russia/32084869.html
63. https://www.reuters.com/business/energy/gazprom-says-it-halts-gas-supplies-poland-bulgaria-payments-row-2022-04-27/
64. https://www.bbc.com/news/world-europe-64380066
65. https://www.theguardian.com/world/2023/jan/27/burning-of-quran-in-stockholm-funded-by-journalist-with-kremlin-ties-sweden-nato-russia

Looking ahead to a second year of Russian cyberattacks and influence operations

Russia's destructive cyberattacks and influence operations increased headed into their new military offensive in eastern Ukraine. Recent Kremlin-backed efforts have not been any more successful than any of their previous campaigns in the past year, but there are many indicators we might look for to detect Russian escalation in the digital space.



Should Russia suffer more setbacks on the battlefield, Russian actors may seek to expand their targeting of military and humanitarian supply chains by pursuing destructive attacks beyond Ukraine and Poland. These possible cyberattacks, should the last year's pattern continue, may incorporate newer destructive malware variants as well.

Separately, cyber intrusions may be key for Russia for:

1. **Espionage purposes to understand military support and political deliberations of different nations in their commitment to the Ukrainian resistance.**
2. **Potential hack-and-leak operations targeting key figures essential for support to Ukraine.**

The convergence of Russian cyber hacks and information leaks may soon rise given that several countries supporting Ukraine hold elections. Russia, since at least 2015, has employed cyber and influence campaigns across western elections to elevate candidates favorable for the Kremlin's foreign policy objectives. Poland, Estonia, Finland—all have elections in 2023 where a change in leadership and political governance could alter support for Ukraine. Add to this to Finland and Sweden's bids for NATO membership and Russia likely has strong incentive to use cyber-enabled influence operations to interfere in European politics in attempts to undermine NATO and EU support for Ukraine.

Microsoft is proud to have supported Ukraine's digital defense since the start of the Russian invasion and the company's entire threat intelligence community remains committed to detecting, assessing, and protecting against Russian cyberattacks and online provocations as the war enters its second year.