Microsoft

Russian threat actors dig in, prepare to seize on war fatigue

December 8, 2023

Microsoft Threat Intelligence

Table of contents

3 Introduction

6 Kremlin launched multi-pronged assault on Ukraine's agriculture sector and targeted war crimes investigators

8 Drilling down on Ukrainian military infrastructure, and defense partners

9 Complex campaign shifts anti-Ukraine messaging to US, Israel

10 Russian propaganda exploits Israel-Hamas war to malign Ukraine

11 Spoofing mainstream media to push anti-Ukraine video content

13 Looking ahead

Introduction

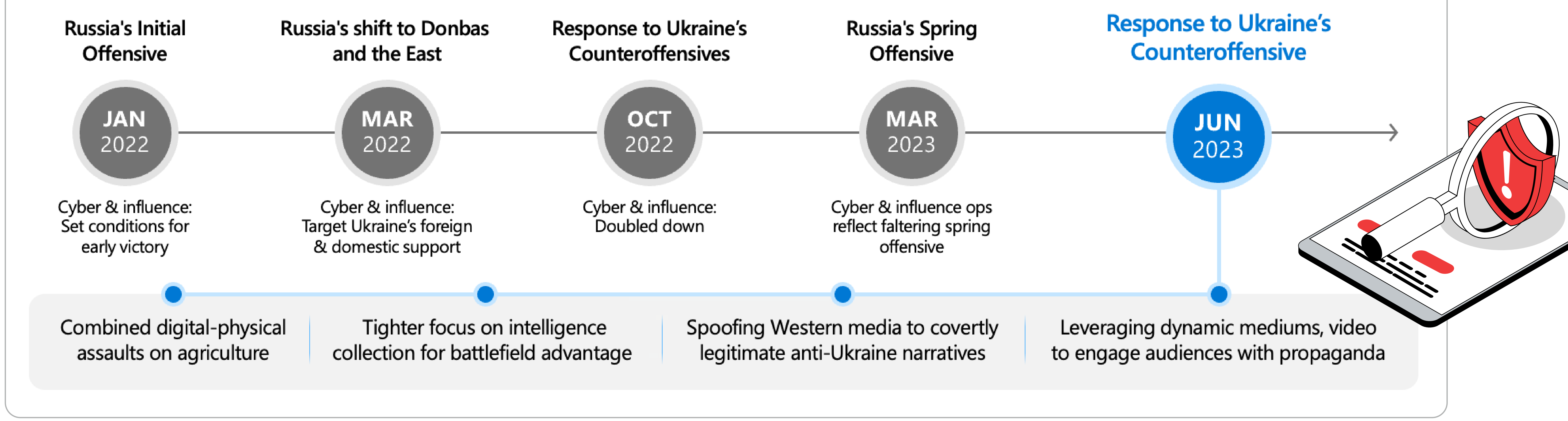
Russian cyber and influence operators have demonstrated adaptability throughout the war on Ukraine, trying new ways to gain battlefield advantage and sap Kyiv's sources of domestic and external support. This report will detail cyber threat and malign influence activity that Microsoft observed between March and October 2023. During this time, Ukrainian military and civilian populations were again in the crosshairs, while the risk of intrusion and manipulation grew to entities worldwide assisting Ukraine and seeking to hold Russian forces to account for war crimes.

Figure 1

Phases of Russia's war in Ukraine

Regaining operational footing, preparing to seize on war fatigue

Microsoft Threat Intelligence



Russia's Initial Offensive
JAN 2022
Cyber & influence: Set conditions for early victory

Russia's shift to Donbas and the East
MAR 2022
Cyber & influence: Target Ukraine's foreign & domestic support

Response to Ukraine's Counteroffensives
OCT 2022
Cyber & influence: Doubled down

Russia's Spring Offensive
MAR 2023
Cyber & influence ops reflect faltering spring offensive

Response to Ukraine's Counteroffensive
JUN 2023

Combined digital-physical assaults on agriculture

Tighter focus on intelligence collection for battlefield advantage

Spoofing Western media to covertly legitimate anti-Ukraine narratives

Leveraging dynamic mediums, video to engage audiences with propaganda

Threat actions Microsoft observed during this March to October period reflected combined operations to demoralize the Ukrainian public and an increased focus on cyber espionage. Russian military, cyber, and propaganda actors directed concerted attacks against the Ukrainian agriculture sector—a civilian infrastructure target—amid a global grain crisis. Cyber threat actors affiliated with Russian military intelligence (GRU) leaned into cyberespionage operations against the Ukrainian military and its foreign supply lines. As the international community sought to punish war crimes, groups linked to Russia's Foreign Intelligence (SVR) and Federal Security (FSB) services targeted war crimes investigators within and outside of Ukraine.

On the influence front, the brief June 2023 rebellion and later death of Yevgeny Prigozhin, owner of the Wagner Group and infamous Internet Research Agency troll farm, raised questions about the future of Russia's influence capabilities. Throughout this summer, Microsoft observed widespread operations by organizations that were not connected to Prigozhin, illustrating Russia's future of malign influence campaigns without him.

Microsoft Threat Intelligence and Incident Response teams have notified and worked with impacted customers and government partners to mitigate the threat activity described in this report.

Russian forces are relying more on conventional weapons to inflict damage in Ukraine, but cyber and influence operations remain an urgent threat to the security of computer networks and civic life within Ukraine's allies in the region, NATO, and globally. In addition to updating our security products to proactively defend our customers worldwide, we are sharing this information to encourage continued vigilance against threats to the integrity of the global information space.

Kremlin launched multi-pronged assault on Ukraine's agriculture sector...

Russian kinetic, cyber, and propaganda forces converged against Ukraine's agriculture sector this summer. Military strikes destroyed grain in amounts that could have fed over 1 million people for a year, while pro-Russia media pushed narratives to justify the targeting despite the humanitarian costs.[1]

From June through September, Microsoft Threat Intelligence observed network penetration, data exfiltration, and even destructive malware deployed against organizations tied to the Ukrainian agricultural industry and grain-related shipping infrastructure. In June and July, Aqua Blizzard (formerly ACTINIUM) stole data from a firm that assists with tracking crop yields. Seashell Blizzard (formerly IRIDIUM) used variants of rudimentary destructive malware Microsoft detects as WalnutWipe/SharpWipe against food/agriculture sector networks.[2]

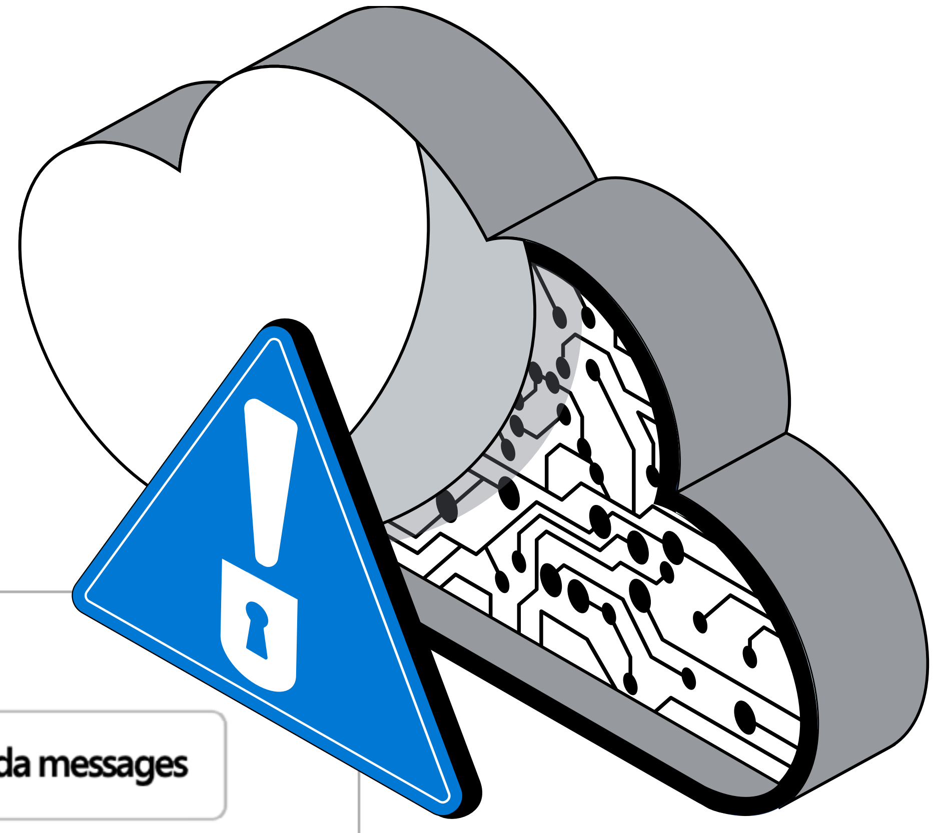
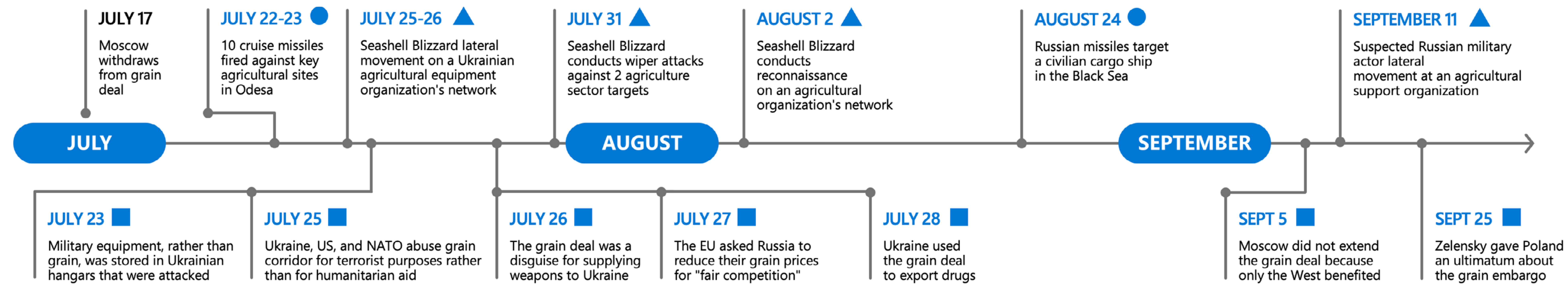


Figure 2

Cyber-Kinetic-Propaganda Activities Directed against Ukrainian Agriculture

KEY: ▲ Cyber activity ● Kinetic activity ■ Propaganda messages



JULY

JULY 17
Moscow withdraws from grain deal

JULY 22-23 ●
10 cruise missiles fired against key agricultural sites in Odesa

JULY 23 ■
Military equipment, rather than grain, was stored in Ukrainian hangars that were attacked

JULY 25 ■
Ukraine, US, and NATO abuse grain corridor for terrorist purposes rather than for humanitarian aid

JULY 25-26 ▲
Seashell Blizzard lateral movement on a Ukrainian agricultural equipment organization's network

JULY 26 ■
The grain deal was a disguise for supplying weapons to Ukraine

JULY 27 ■
The EU asked Russia to reduce their grain prices for "fair competition"

JULY 28 ■
Ukraine used the grain deal to export drugs

JULY 31 ▲
Seashell Blizzard conducts wiper attacks against 2 agriculture sector targets

AUGUST

AUGUST 2 ▲
Seashell Blizzard conducts reconnaissance on an agricultural organization's network

AUGUST 24 ●
Russian missiles target a civilian cargo ship in the Black Sea

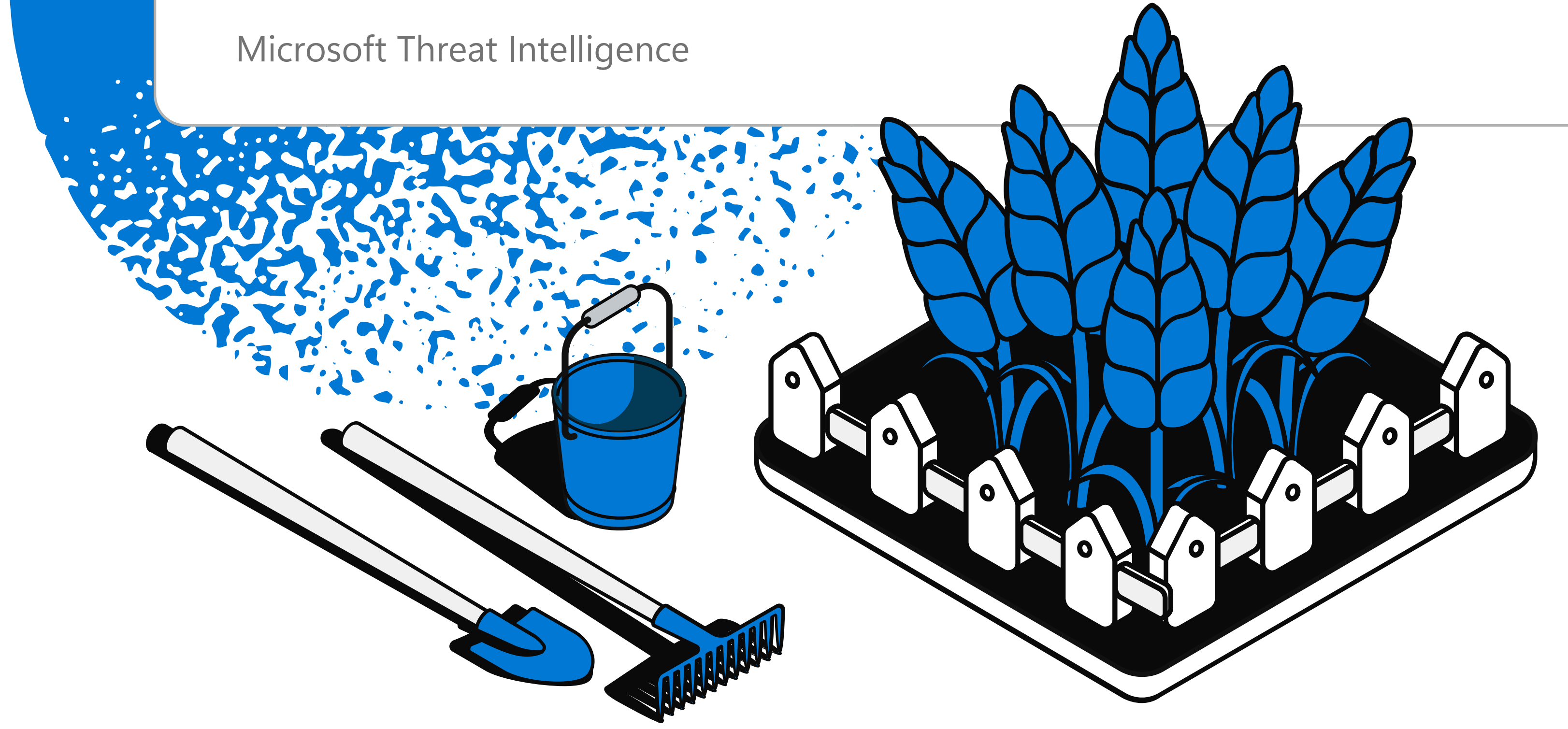
SEPTEMBER

SEPT 5 ■
Moscow did not extend the grain deal because only the West benefited

SEPTEMBER 11 ▲
Suspected Russian military actor lateral movement at an agricultural support organization

SEPT 25 ■
Zelensky gave Poland an ultimatum about the grain embargo

Microsoft Threat Intelligence



In July, Moscow withdrew from the Black Sea Grain Initiative, a humanitarian effort that helped stave off a global food crisis and allowed for the transport of more than 725,000 tons of wheat to people in Afghanistan, Ethiopia, Kenya, Somalia, and Yemen in its first year.[3] After Moscow's action, pro-Russia media outlets and Telegram channels jumped in to malign the grain initiative and provide justification for Moscow's decision. Propaganda outlets painted the grain corridor as a front for drug trafficking or cast it as a means to covertly transfer weapons, to downplay the humanitarian significance of the deal.

Deep bench of hacktivist fronts amplifying, justifying Kremlin actions

In several 2023 reports, we highlighted how legitimate or pseudo hacktivist groups with suspected connections to the GRU have worked to amplify Moscow's displeasure with adversaries and exaggerate the number of pro-Russia cyber forces.[4, 5, 6] This summer, we also observed hacktivist personas on Telegram spread messages that attempt to justify military assaults on civilian infrastructure in Ukraine and focused distributed denial-of-service (DDoS) attacks against Ukraine's allies abroad. Microsoft's continued monitoring of hacktivist groups' intersection with nation state actors offers additional insights into both entities' operational tempo and the ways their activities complement each other's goals.

To date, we have identified three groups—Solntsepek, InfoCentr, and Cyber Army of Russia—that interact with Seashell Blizzard. Seashell Blizzard's relationship with the hacktivist outlets may be one of short-term use, rather than control, based on the hacktivists' temporary spikes in cyber capability coinciding with Seashell Blizzard attacks. Periodically, Seashell Blizzard launches a destructive attack that Telegram hacktivist groups publicly claim credit for. The hacktivists then go back to the low-complexity actions they usually conduct including DDoS attacks or leaks of Ukrainian personal information. The network represents agile infrastructure that the APT can use to promote their activity.

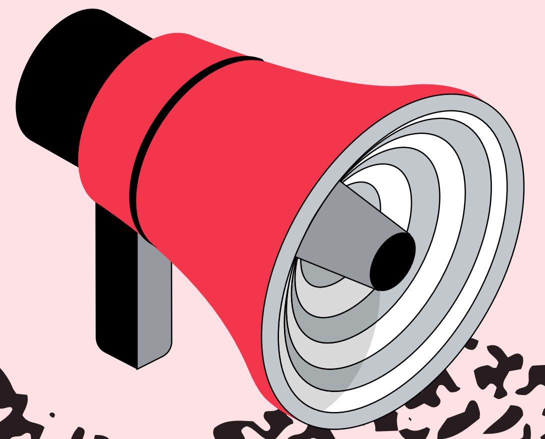
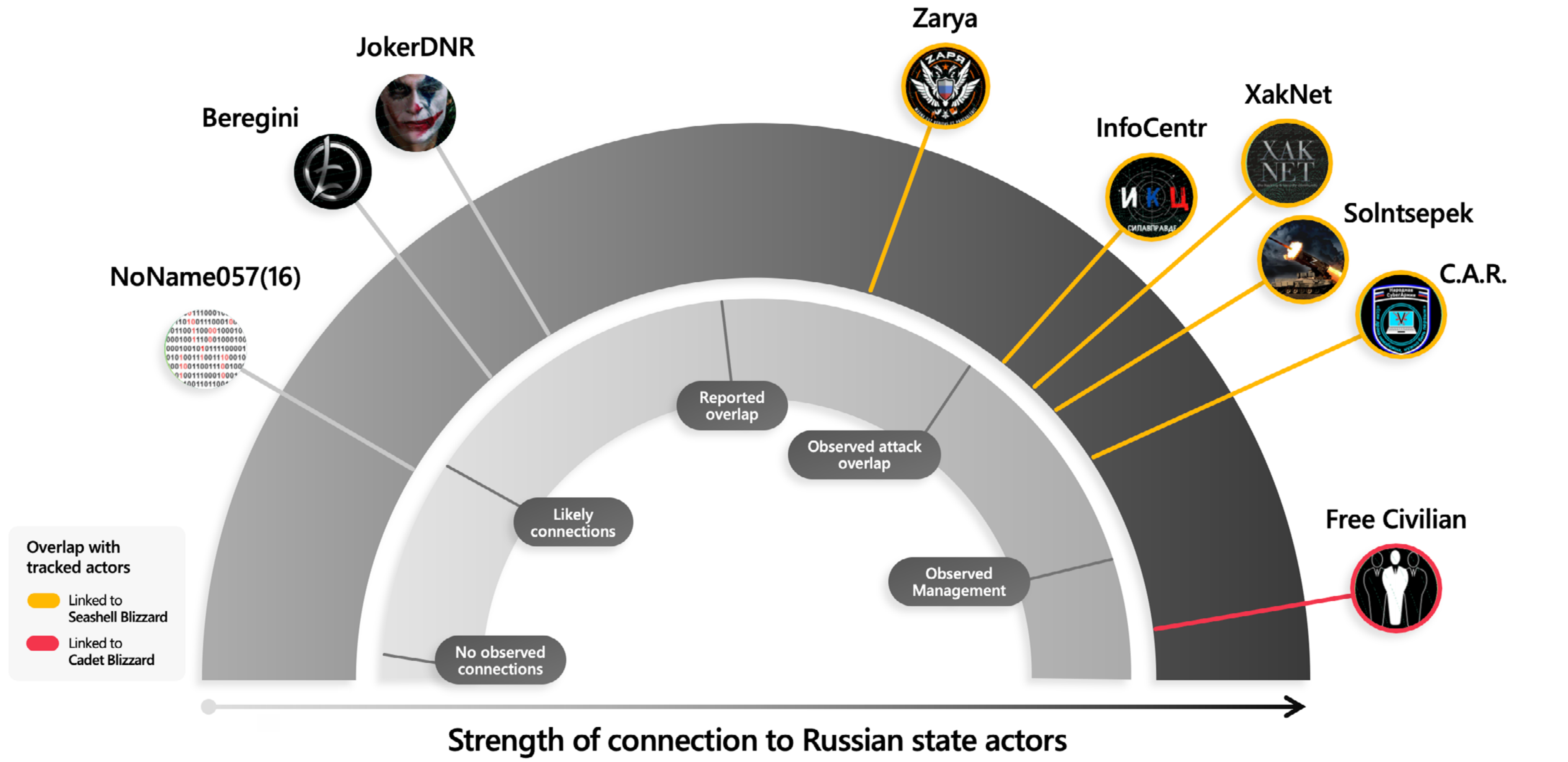


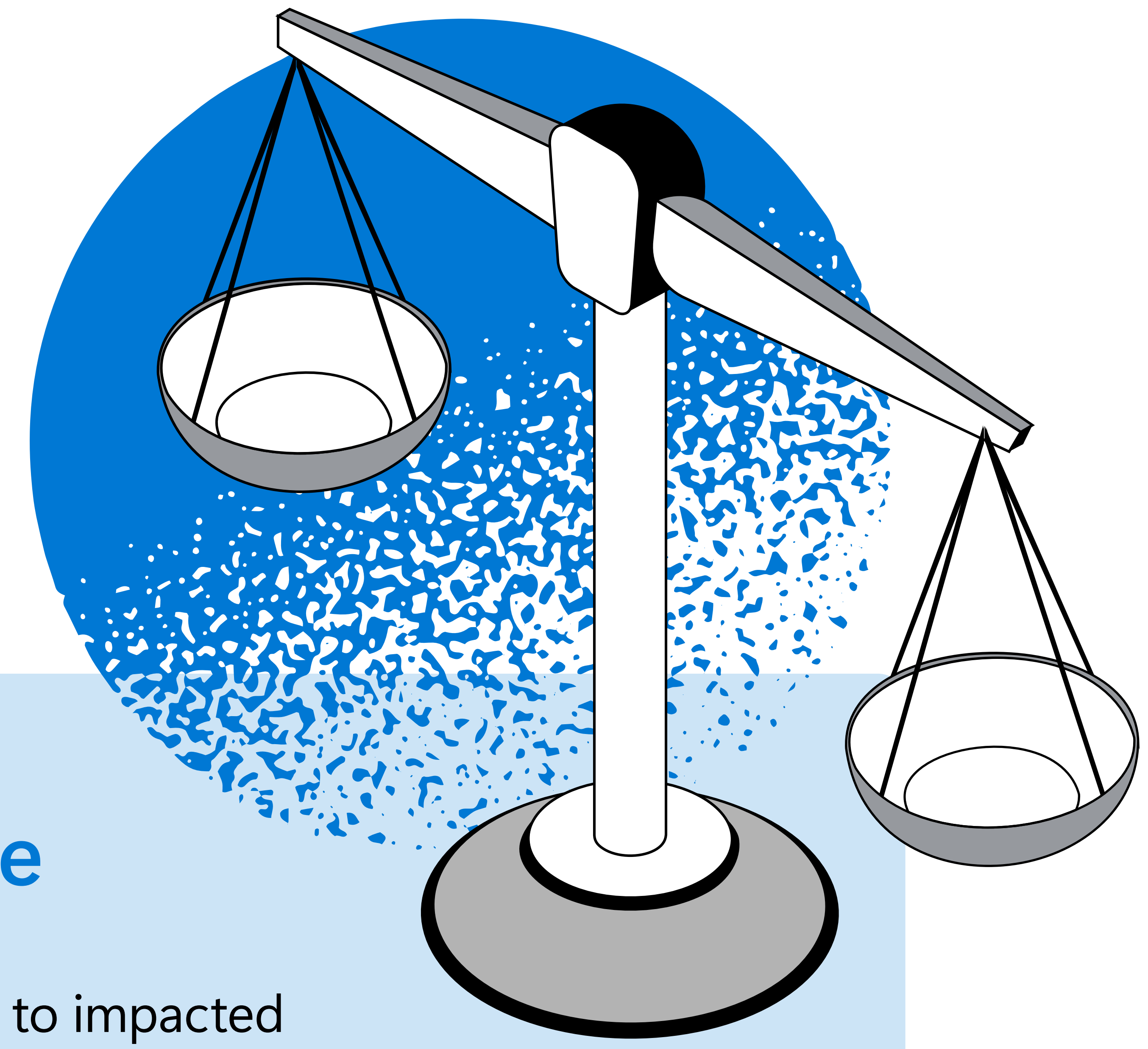
Figure 3

Microsoft Threat Intelligence

The Dial of Pro-Russia Hacktivism



From July 2022 to August 2023, Microsoft Threat Analysis Center (MTAC) identified several incidents when a pro-Russia Telegram channel targeted an organization, defaced its website, and claimed it performed a destructive attack. Our data shows some of the incidents had overlap with methods, malware, and infrastructure used by Russian military actors. Above is our current assessment of the relative proximity of many active pro-Russia hacktivist personas to the Russian state, based on first-party data, MTAC analysis of social media posts, and open-source reporting.



…and targeted war crimes investigators as the ICC pursues charges

Russian forces are not only engaging in actions that could run afoul of international law, but also targeting the criminal investigators and prosecutors building cases against them.

Microsoft telemetry revealed that actors linked to Russia's military and foreign intelligence agencies targeted and breached Ukrainian legal and investigative networks, and those of international organizations involved in war crimes investigations, throughout the spring and summer this year. These cyber operations occurred amid mounting tensions between Moscow and groups like the International Criminal Court (ICC), which issued an arrest warrant for Russian President Putin on war crimes charges in March.[7]

In April, GRU-linked Seashell Blizzard compromised the network of a law firm that focuses on war crimes cases. Aqua Blizzard, attributed to the FSB, breached the internal network of a major investigative body in Ukraine in July, then used compromised accounts there to send phishing emails to several Ukrainian telecom firms in September.

SVR actors Midnight Blizzard (formerly NOBELIUM) compromised and accessed the documents of a legal organization with global responsibilities in June and July before Microsoft Incident Response intervened to remediate the intrusion. This activity was part of a more aggressive push by this actor to breach diplomatic, defense, public policy, and IT sector organizations worldwide.

Midnight Blizzard on the Move

A review of Microsoft security notifications issued to impacted customers since March revealed that Midnight Blizzard has pursued access to **more than 240 organizations predominantly in the US, Canada, and European countries**, with varying degrees of success.[8]

Nearly 40 percent of the targeted organizations were government, inter-governmental, or policy-focused think tanks.

Mixed bag of cyber techniques favor blending in, evading detection

Russian threat actors used various techniques to gain initial access and establish persistence on targeted networks. Midnight Blizzard took a kitchen sink approach, using password spray, credentials acquired from third parties, believable social engineering campaigns via Teams, and abuse of cloud services to infiltrate cloud environments.[9] Aqua Blizzard successfully integrated HTML smuggling in initial access phishing campaigns to reduce the likelihood of detection by anti-virus signatures and email security controls.

Seashell Blizzard exploited perimeter server systems such as Exchange and Tomcat servers and simultaneously leveraged pirated Microsoft Office software harboring the DarkCrystalRAT backdoor to gain initial access. The backdoor allowed the actor to load a second stage payload we call Shadowlink, a software package masquerading as Microsoft Defender that installs the TOR service on a device and gives the threat actor surreptitious access via the TOR network.[10]

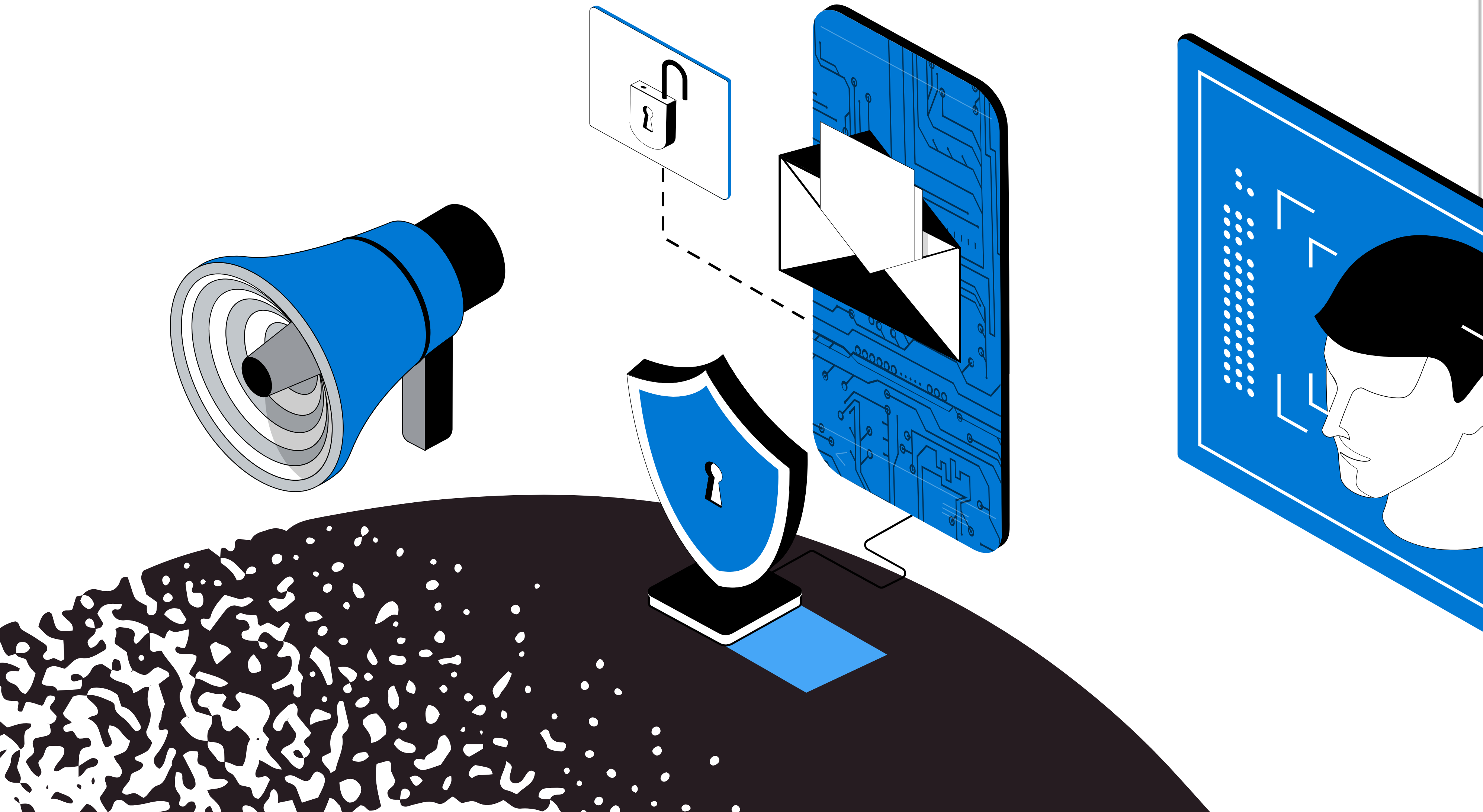
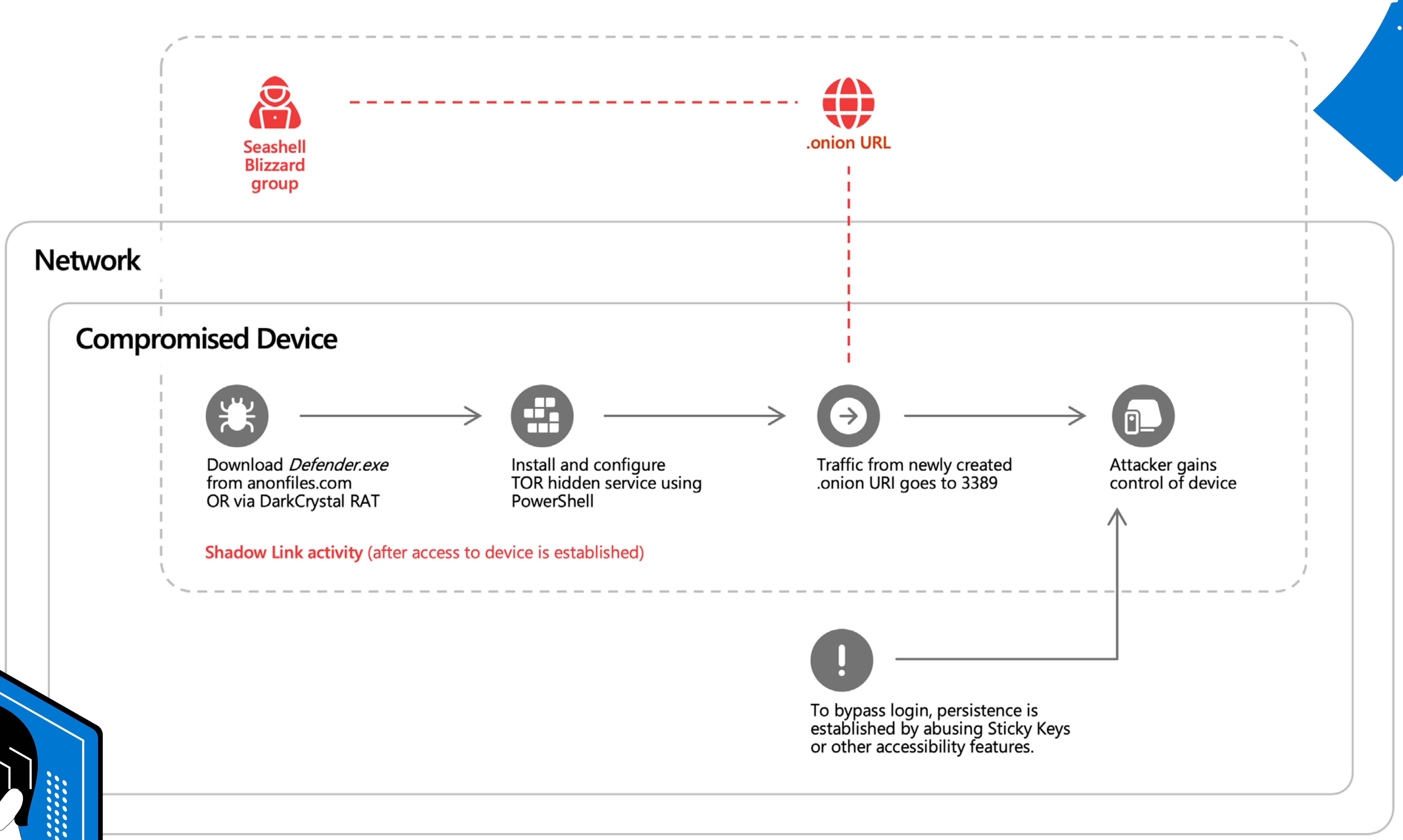


Figure 4

ShadowLink attack diagram

Microsoft Threat Intelligence


Seashell Blizzard group
.onion URL
Network
Compromised Device
Download *Defender.exe* from anonfiles.com OR via DarkCrystal RAT
Install and configure TOR hidden service using PowerShell
Traffic from newly created .onion URI goes to 3389
Attacker gains control of device
Shadow Link activity (after access to device is established)
To bypass login, persistence is established by abusing Sticky Keys or other accessibility features.

Drilling down on Ukrainian military infrastructure, and defense partners

Since Russian forces launched their spring 2023 offensive, GRU- and FSB-affiliated cyber actors have concentrated their efforts on intelligence collection from Ukrainian communications and military infrastructure in combat zones.

As of March, Microsoft Threat Intelligence connected Seashell Blizzard to potential phishing lures and packages that appeared tailored to target a major component of Ukrainian military communications infrastructure. We had no visibility on follow-on action. According to the Ukrainian Security Service (SBU), Seashell Blizzard's other attempts to access Ukrainian military networks included malware that would allow them to collect information about the configurations of connected Starlink satellite terminals and glean the location of Ukrainian military units.[11, 12, 13]

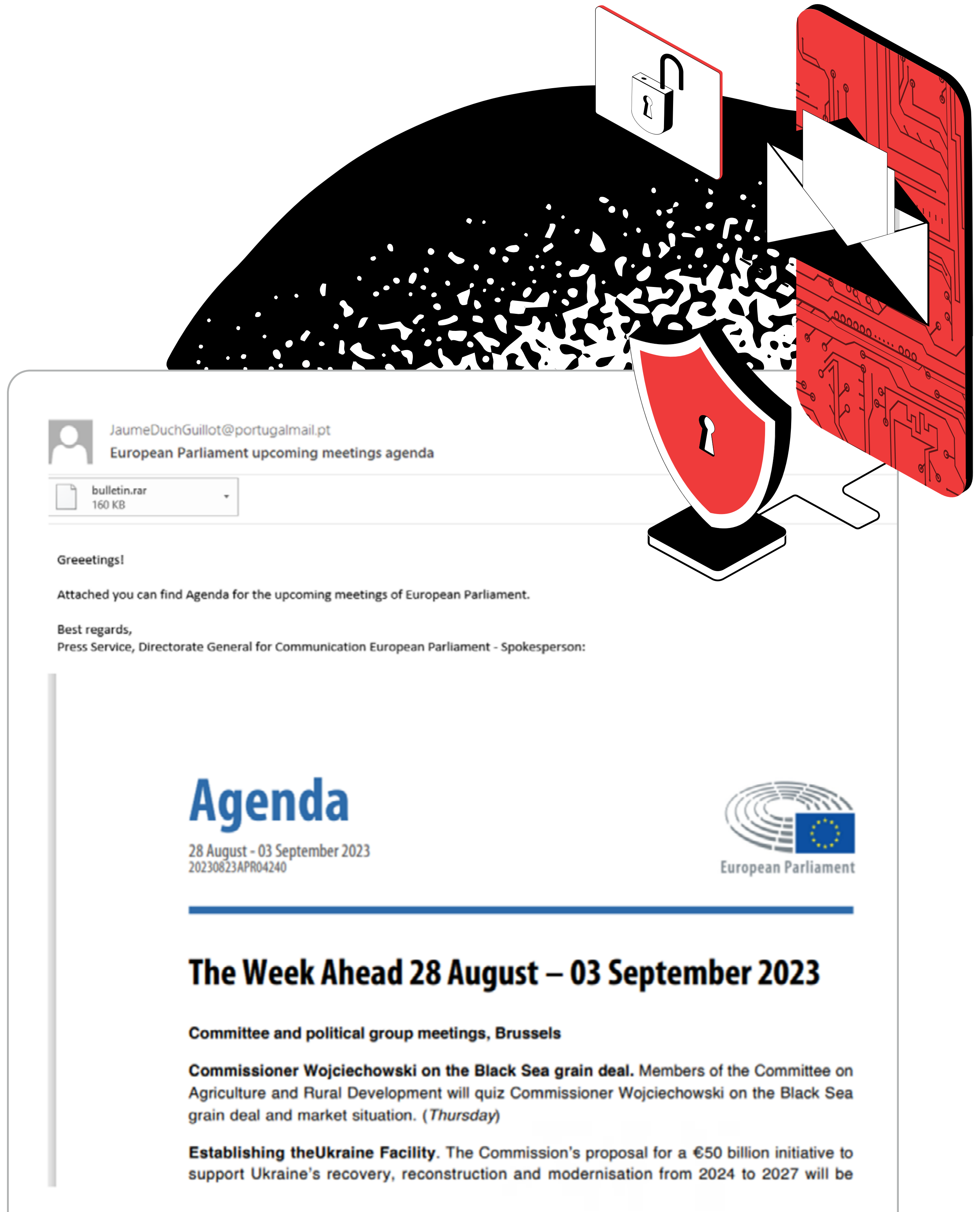
Secret Blizzard (formerly KRYPTON) also moved to secure intelligence collection footholds in Ukrainian defense-related networks. In partnership with the Government Computer Emergency Response Team of Ukraine (CERT-UA), Microsoft Threat Intelligence identified the presence of Secret Blizzard's DeliveryCheck and Kazuar backdoor malware on Ukrainian defense forces' systems.[14] Kazuar allows more than 40 functions including stealing credentials from a variety of applications, authentication data, proxies, and cookies, and data retrieval from operating system logs.[15] Secret Blizzard was particularly interested in stealing files with messages from the Signal Desktop messaging application, which would allow them to read private Signal chats.[16]

Forest Blizzard using novel techniques to collect intelligence on Ukrainian partners

Forest Blizzard (formerly STRONTIUM) renewed focus on its traditional espionage targets, defense-related organizations in the United States, Canada, and Europe, whose military support and training are keeping Ukrainian forces equipped to continue the fight.

Since March, Forest Blizzard has attempted to gain initial access to defense organizations via phishing messages that incorporated novel and evasive techniques. For example, in August, Forest Blizzard sent a phishing email that incorporated an exploit for CVE-2023-38831 to accountholders at a European defense organization. CVE-2023-38831 is a security vulnerability in WinRAR software that allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive.

The actor is also leveraging legitimate developer tools such as Mockbin and Mocky for command and control. As of late September, the actor conducted a phishing campaign abusing GitHub and Mockbin services. CERT-UA and other cybersecurity firms publicized the activity in September, noting the actor used adult entertainment pages to entice victims to click a link or open a file that would redirect them to malicious Mockbin infrastructure.[17, 18] Microsoft observed a pivot to using a technology-themed page in late September. In each case, the actors sent a phishing email containing a malicious link that would redirect the victim to a Mockbin URL and download a zip file bundled with a malicious LNK (shortcut) file masquerading as a Windows update. The LNK file would then download and execute another PowerShell script to establish persistence and conduct follow-on actions like data theft.



JaumeDuchGuillot@portugalmail.pt
European Parliament upcoming meetings agenda

bulletin.rar
160 KB

Greeetings!

Attached you can find Agenda for the upcoming meetings of European Parliament.

Best regards,
Press Service, Directorate General for Communication European Parliament - Spokesperson:

Agenda
28 August - 03 September 2023
20230823APR04240

European Parliament

The Week Ahead 28 August – 03 September 2023

Committee and political group meetings, Brussels

Commissioner Wojciechowski on the Black Sea grain deal. Members of the Committee on Agriculture and Rural Development will quiz Commissioner Wojciechowski on the Black Sea grain deal and market situation. (*Thursday*)

Establishing theUkraine Facility. The Commission's proposal for a €50 billion initiative to support Ukraine's recovery, reconstruction and modernisation from 2024 to 2027 will be

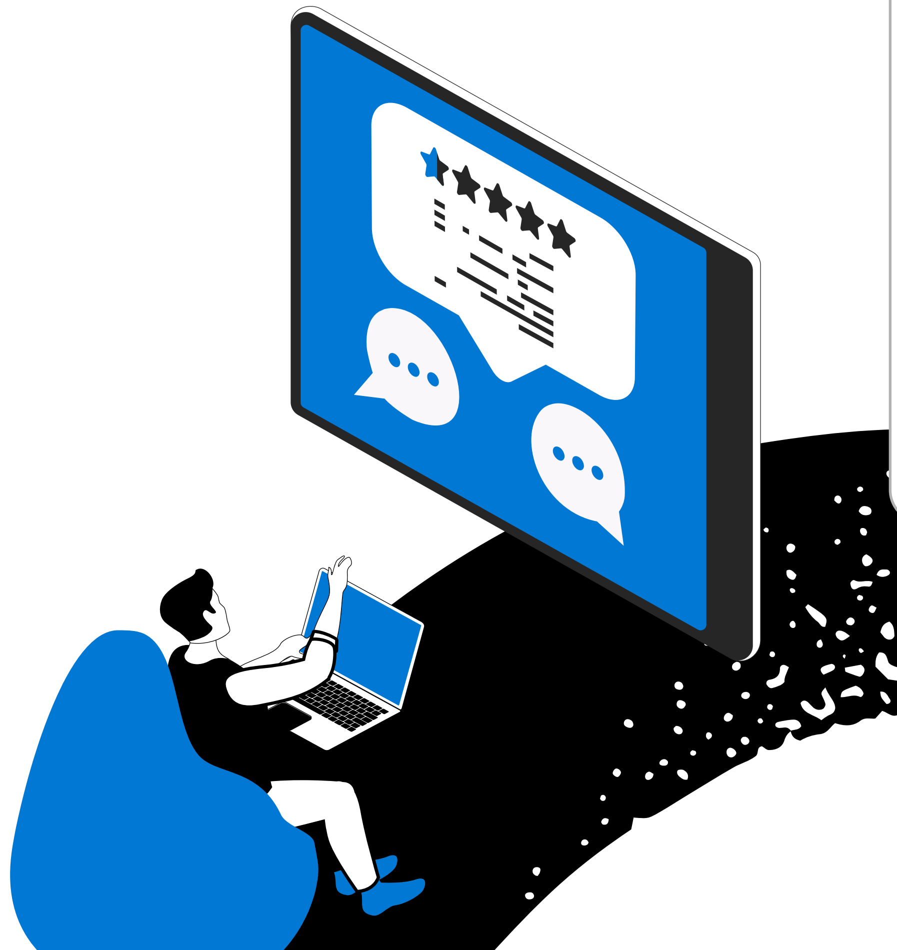
Figure 5: Screenshot of a sample PDF lure associated with Forest Blizzard phish of defense organizations. Actor masquerades as European Parliament staff.

Complex influence campaign shifts anti-Ukraine messaging to US, Israel

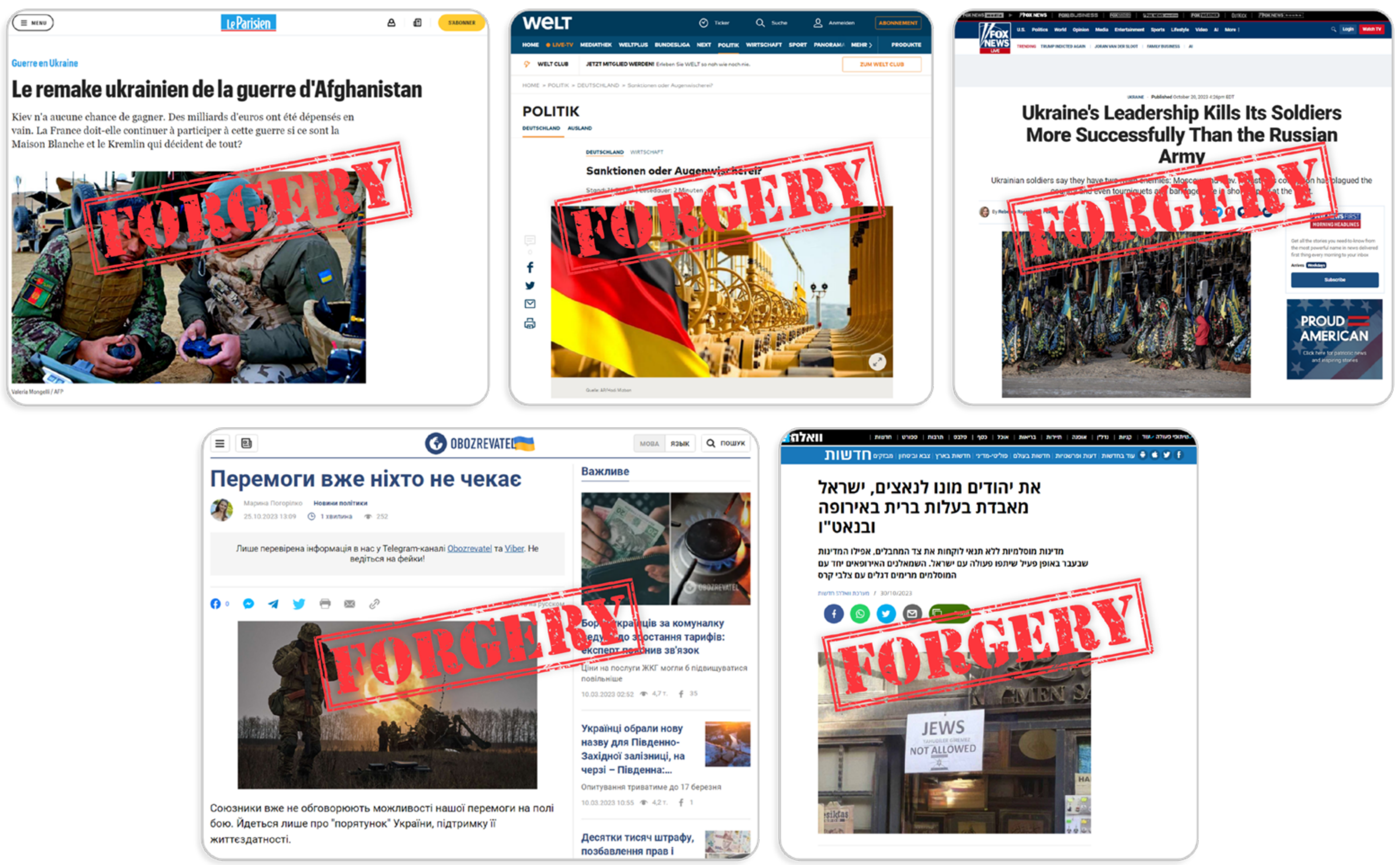
Throughout 2023, the Microsoft Threat Analysis Center (MTAC), continued observation of Storm-1099, a Russia-affiliated influence actor responsible for a sophisticated pro-Russia influence operation targeting international supporters of Ukraine since the spring of 2022. Perhaps best known for the mass-scale website forgery operation dubbed "Doppelganger" by research group EU DisinfoLab,[19] Storm-1099's activities also include unique branded outlets such as Reliable Recent News (RRN), multimedia projects such as anti-Ukrainian cartoon series "Ukraine Inc.," and on-the-ground demonstrations bridging the digital and physical worlds. Although attribution is incomplete, well-funded Russian political technologists, propagandists, and PR specialists with demonstrable ties back to the Russian state have conducted and supported several Storm-1099 campaigns.[20]

Storm-1099's Doppelganger operation remains in full force as of the time of this report, despite persistent attempts by technology companies and research entities to report on and mitigate its reach.[21] While this actor has historically targeted western Europe—overwhelmingly Germany—it has also targeted France, Italy, and Ukraine. In recent months Storm-1099 has shifted its locational focus towards the United States and Israel. This transition began as far back as January 2023, amid large-scale protests in Israel against proposed judicial overhaul and intensified after the onset of the Israel-Hamas war in early October. Newly created branded outlets reflect an increasing prioritization of US politics and the upcoming 2024 US presidential elections, while existing Storm-1099 assets have forcefully pushed the false claim that Hamas acquired Ukrainian weapons on the black market for its October 7 attacks in Israel.

Most recently, in late October, MTAC observed accounts Microsoft assesses to be Storm-1099 assets promoting a new kind of forgery in addition to fake articles and websites on social media. These are a series of short fake news clips, ostensibly created by reputable outlets, which spread pro-Russia propaganda to undermine support for both Ukraine and Israel. While this tactic—using video spoofs to push propaganda lines—is a tactic observed in recent months by pro-Russia actors more broadly, Storm-1099's promotion of such video content only highlights the actor's varied influence techniques and messaging goals.



Microsoft Threat Intelligence



Guerre en Ukraine

Le remake ukrainien de la guerre d'Afghanistan

Kiev n'a aucune chance de gagner. Des milliards d'euros ont été dépensés en vain. La France doit-elle continuer à participer à cette guerre si ce sont la Maison Blanche et le Kremlin qui décident de tout?

POLITIK

Sanktionen oder Augenwischerei?

Ukraine's Leadership Kills Its Soldiers More Successfully Than the Russian Army

Перемоги вже ніхто не чекає

Лише перевірена інформація в нас у Telegram-каналі Obozrevatel та Viber. Не ведіться на фейки!

Союзники вже не обговорюють можливості нашої перемоги на полі бою. Йдеться лише про "порятунок" України, підтримку її життєздатності.

את יהודים מונו לנאצים, ישראל
מאבדת בעלות ברית באירופה
ובנאט"ו

מדינות מוסלמיות ללא תנאי לוקחות את צד המחבלים, אפילו המדינות
שבעבר באופן פעיל שיתפו פעולה עם ישראל. השמאלנים האירופאים יחד עם
המוסלמים מרימים דגלים עם צלבי קרס

Figure 6: Fake articles published on forged Doppelganger sites, the campaign conducted by the Russia-affiliated influence actor Microsoft tracks as Storm-1099, observed October 31, 2023.

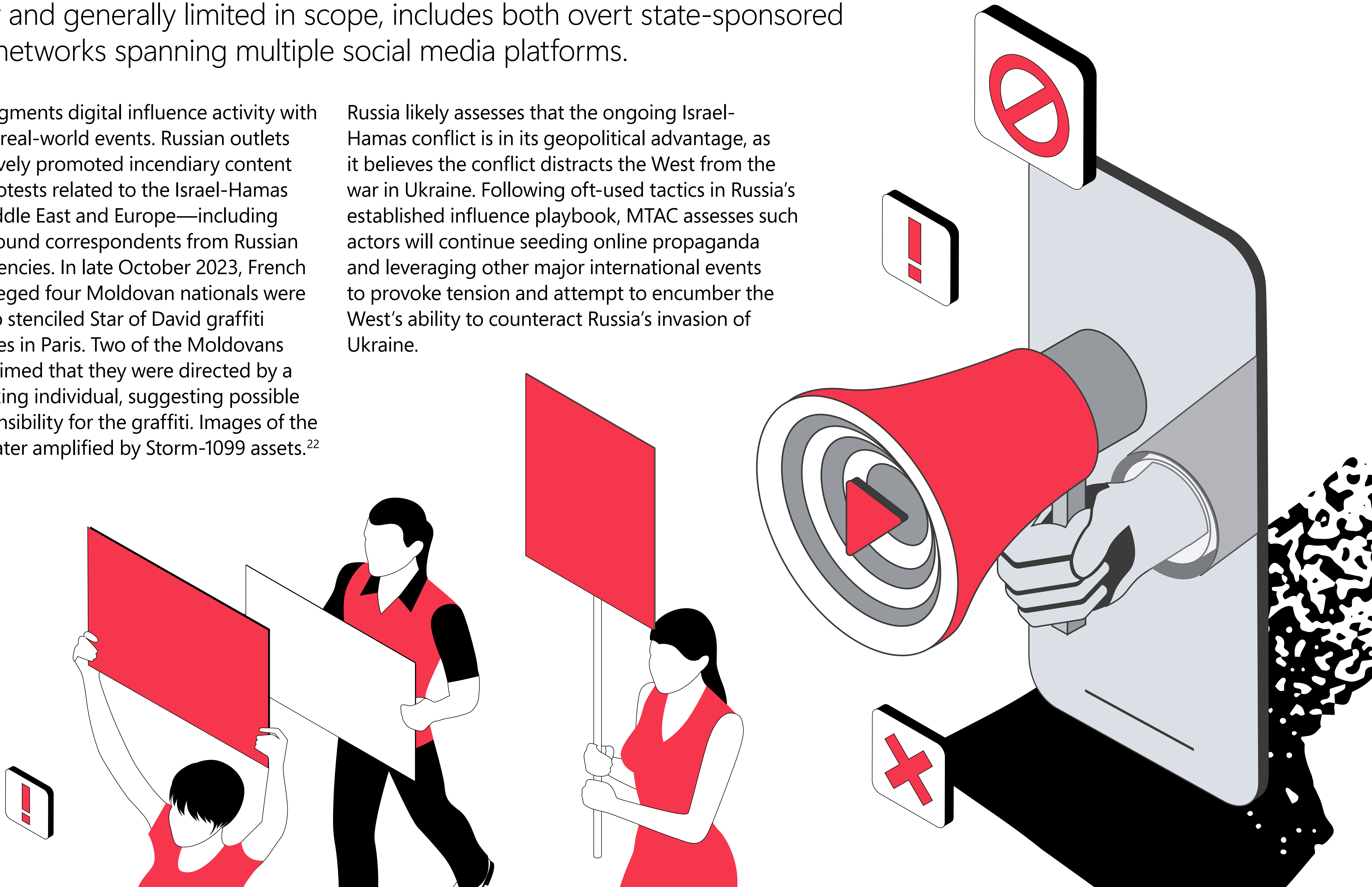
Russian propaganda exploits Israel-Hamas war to malign Ukraine

Since Hamas's attacks in Israel on October 7, Russian state media and state-aligned influence actors have sought to exploit the Israel-Hamas war to promote anti-Ukraine narratives, anti-US sentiment, and exacerbate tension among all parties. This activity, while reactive to the war and generally limited in scope, includes both overt state-sponsored media and covert Russia-affiliated social media networks spanning multiple social media platforms.

Narratives promoted by Russian propagandists and pro-Russian social media networks seek to pit Israel against Ukraine and diminish Western support for Kyiv by falsely claiming that Ukraine armed Hamas militants in spoofs of reputable media outlets and manipulated videos. An inauthentic video that claimed foreign recruits, including Americans, were transferred from Ukraine to join Israeli Defense Forces (IDF) operations on the Gaza Strip, which garnered hundreds of thousands of views across social media platforms, offers just one example of such content. This strategy both propels anti-Ukrainian narratives to a wide audience and drives engagement by shaping false narratives to align with major developing news stories.

Russia also augments digital influence activity with promotion of real-world events. Russian outlets have aggressively promoted incendiary content amplifying protests related to the Israel-Hamas war in the Middle East and Europe—including via on-the-ground correspondents from Russian state news agencies. In late October 2023, French authorities alleged four Moldovan nationals were likely linked to stenciled Star of David graffiti in public spaces in Paris. Two of the Moldovans reportedly claimed that they were directed by a Russian-speaking individual, suggesting possible Russian responsibility for the graffiti. Images of the graffiti were later amplified by Storm-1099 assets.[22]

Russia likely assesses that the ongoing Israel-Hamas conflict is in its geopolitical advantage, as it believes the conflict distracts the West from the war in Ukraine. Following oft-used tactics in Russia's established influence playbook, MTAC assesses such actors will continue seeding online propaganda and leveraging other major international events to provoke tension and attempt to encumber the West's ability to counteract Russia's invasion of Ukraine.



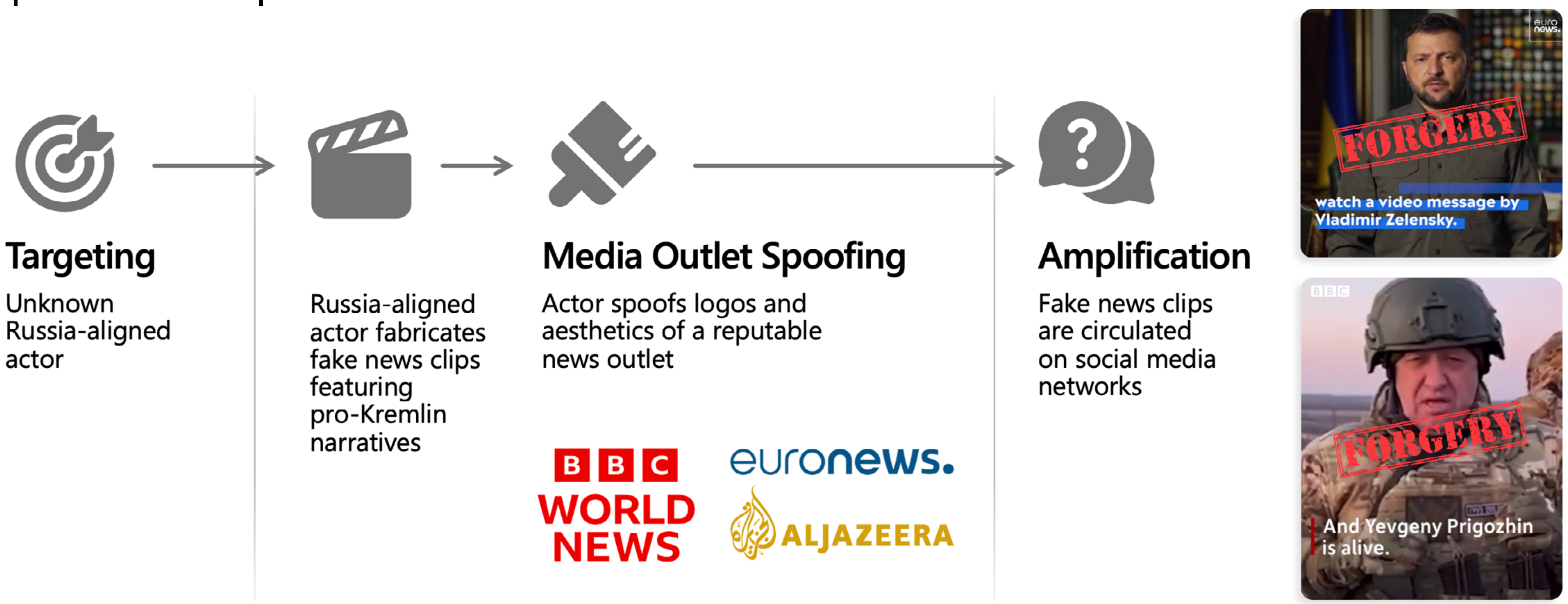
Spoofing mainstream media to push anti-Ukraine video content

Anti-Ukraine propaganda has broadly permeated Russian influence activity since before the 2022 full-scale invasion. In recent months, however, pro-Russia and Russia-affiliated influence networks have focused on using video as a more dynamic medium to spread these messages coupled with spoofing authoritative media outlets to leverage their credibility. MTAC has observed two ongoing campaigns conducted by unknown, pro-Russia actors that involve spoofing mainstream news and entertainment media brands to push manipulated video content. Like previous Russian propaganda campaigns, this activity focuses on painting Ukrainian President Volodymyr Zelensky as a corrupt drug addict and Western support for Kyiv as detrimental to those countries' domestic populations. The content in both campaigns consistently seeks to diminish support for Ukraine but adapts narratives to align with emerging news events—like the June 2023 Titan submersible implosion or the Israel-Hamas war to reach wider audiences.

Figure 7

Spoofed News Clips Overview

Microsoft Threat Intelligence



Targeting

Unknown Russia-aligned actor

Russia-aligned actor fabricates fake news clips featuring pro-Kremlin narratives

Media Outlet Spoofing

Actor spoofs logos and aesthetics of a reputable news outlet

Amplification

Fake news clips are circulated on social media networks

BBC WORLD NEWS
euronews.
ALJAZEERA
FORGERY
watch a video message by Vladimir Zelensky.
FORGERY
And Yevgeny Prigozhin is alive.

One of these video-centric campaigns involves a series of fabricated videos that spread false, anti-Ukrainian, Kremlin-affiliated themes, and narratives under the guise of short news reports from mainstream media outlets. MTAC first observed this activity in April 2022 when pro-Russia Telegram channels posted a fake BBC News video, which claimed that the Ukrainian military was responsible for a missile strike that killed dozens of civilians. The video uses BBC's logo, color scheme and aesthetics, and features English-language captions containing errors commonly made when translating from Slavic languages to English.

This campaign continued throughout 2022 and accelerated in the summer of 2023. At the time of compiling this report, MTAC has observed more than a dozen spoofed media videos in the campaign, with the most frequently spoofed outlets being BBC News, Al Jazeera, and EuroNews. Russian-language Telegram channels first amplified the videos before they spread to mainstream social media platforms.

Although this content has had limited reach, it could pose a credible threat to future targets if refined or improved with

Microsoft Threat Intelligence

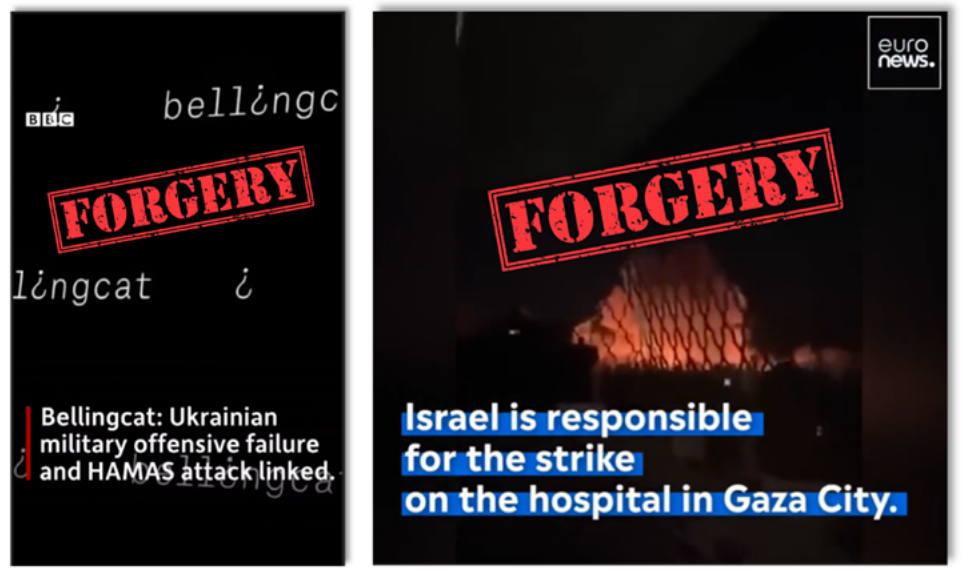

bellingc
BBC
FORGERY
lingcat
Bellingcat: Ukrainian military offensive failure and HAMAS attack linked.
euro news.
FORGERY
Israel is responsible for the strike on the hospital in Gaza City.

Figure 8: Fabricated news clips containing Russia-aligned disinformation. The videos imitate BBC News (left) and EuroNews (right) by spoofing their logos and aesthetics.

the power of AI or amplified by a more credible messenger. The pro-Russia actor responsible for the spoofed news clips is sensitive to current world events and nimble. For example, a spoofed BBC News video falsely claimed that investigative journalism organization Bellingcat uncovered that weapons used by the Hamas militants were sold to the group by Ukrainian military officials through the black market. This video content closely mirrored public statements made by former Russian President Dmitry Medvedev just one day before the video was released, demonstrating the campaign's strong alignment with overt Russian government messaging.[23]

Celebrity videos manipulated to malign President Zelensky

Starting in July 2023, pro-Russia social media channels began circulating videos of celebrities, deceptively edited to push anti-Ukraine propaganda. The videos—the work of an unknown Russia-aligned influence actor—appear to leverage Cameo, a popular website where celebrities and other public figures can record and send personalized video messages to users who pay a fee. The short video messages, which often feature celebrities pleading with "Vladimir" to seek help for substance abuse, are edited by the unknown actor to include emojis and links. Videos circulate through pro-Russian social media communities and are amplified by Russian state-affiliated and state-run media outlets, falsely portrayed as messages to Ukrainian President Volodymyr Zelensky. In some cases, the actor added media outlet logos and social media handles of celebrities to make the video look like news clips from reporting on the celebrities' supposed public appeals to Zelensky or the celebrities' own social media posts. Kremlin officials and Russian state-sponsored propaganda have long promoted the false claim that President Zelensky struggles with substance abuse; however, this campaign marks a novel approach by pro-Russia actors seeking to further the narrative in the online information space.

The first video in the campaign, observed in late July, features Ukrainian flag emojis, watermarks from American media outlet TMZ, and links to both a substance abuse recovery center and one of President Zelensky's official social media pages. As of late October 2023, pro-Russia social media channels have circulated six more videos. Notably, on August 17, Russian state-owned news outlet RIA Novosti published an article covering a video featuring American actor John McGinley, as if it were an authentic appeal from McGinley to Zelensky.[24] Beyond McGinley, celebrities whose content appears in the campaign include actors Elijah Wood, Dean Norris, Kate Flannery and Priscilla Presley; musician Shavo Odadjian; and boxer Mike Tyson. Other state-affiliated Russian media outlets, including US-sanctioned media outlet Tsargrad, have also amplified the campaign's content.[25]

Microsoft Threat Intelligence

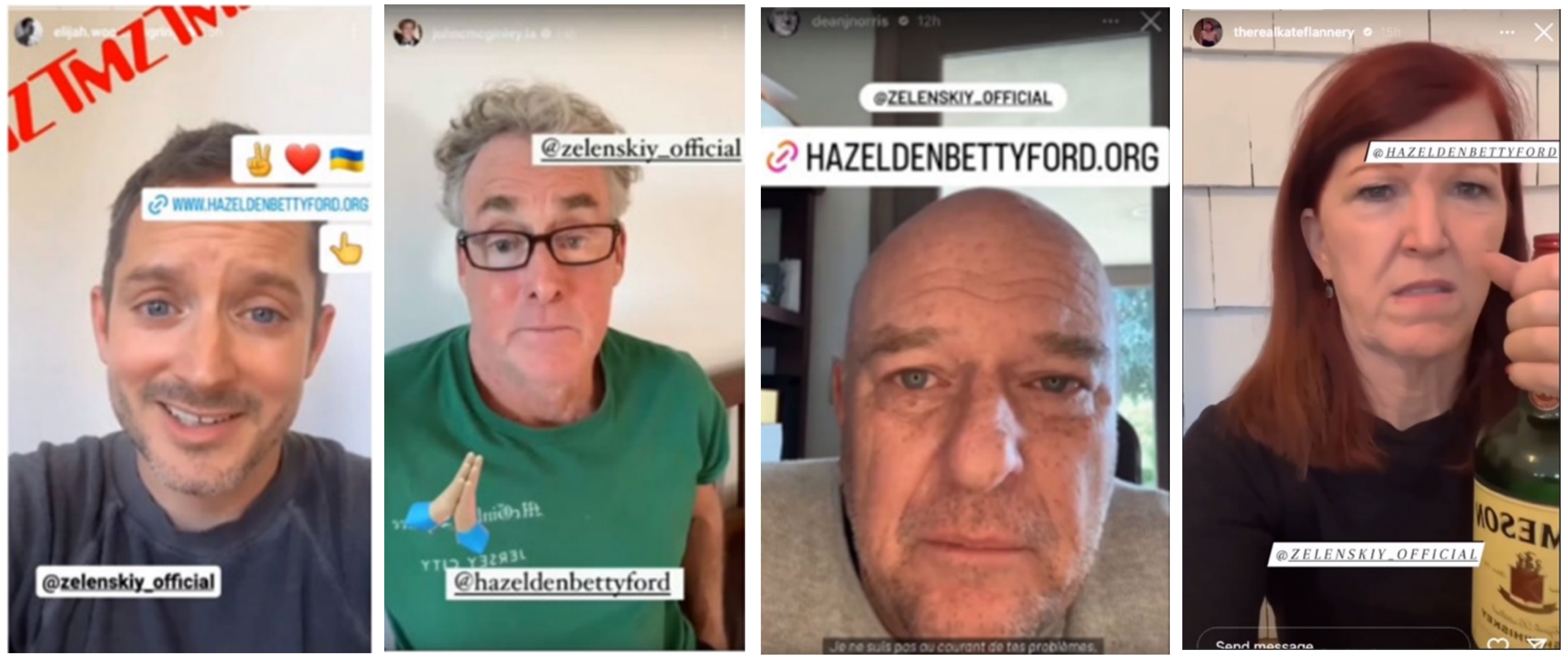
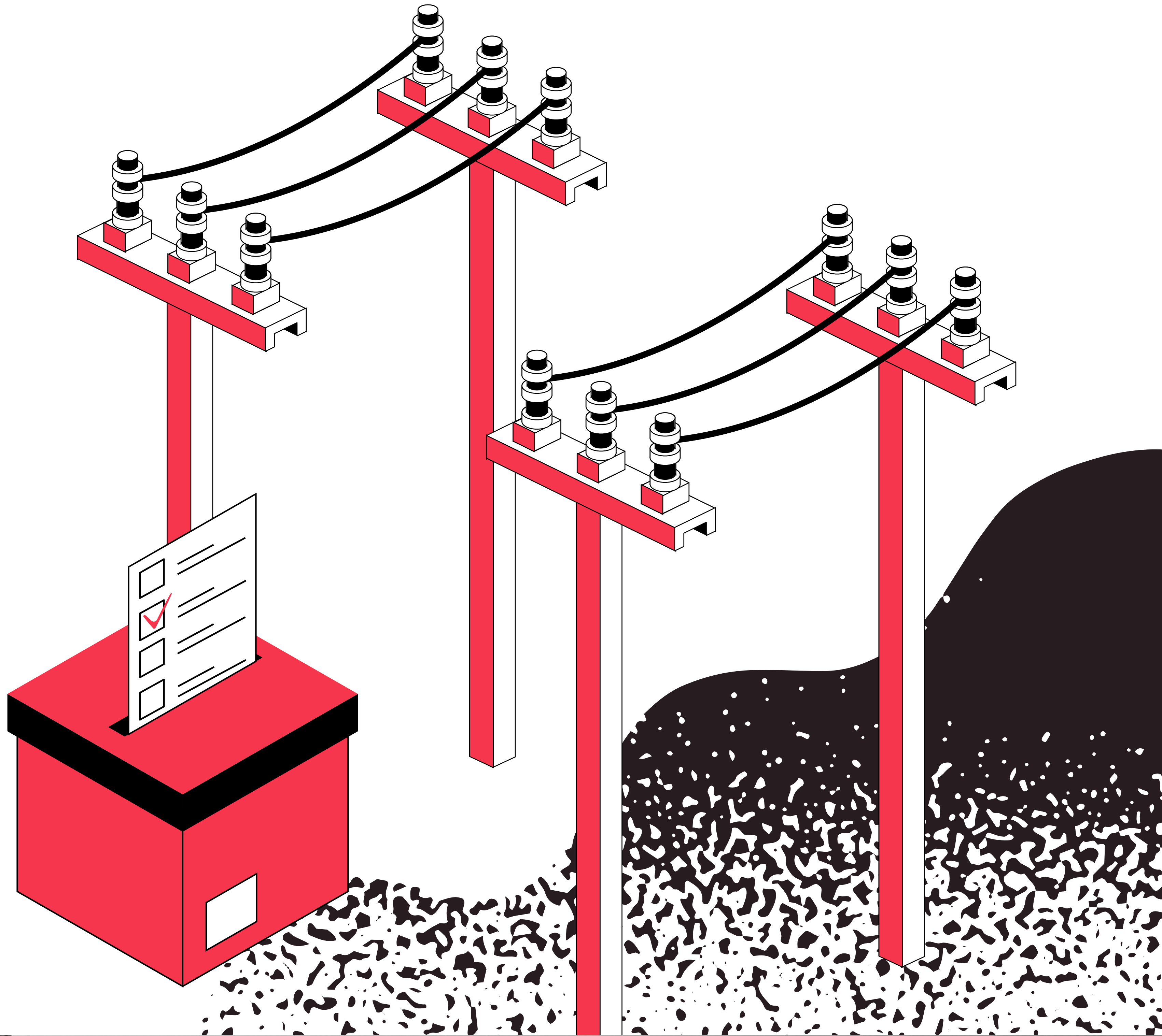


Figure 9: Still images from videos featuring celebrities seemingly promoting pro-Russian propaganda.

Looking ahead

Russian fighters are moving to a new stage of static, trench warfare, according to Ukraine's military chief, suggesting an even more protracted conflict.[26] Kyiv will require a steady supply of weapons and popular support to continue resistance, and we are likely to see Russian cyber and influence operators intensify efforts to demoralize the Ukrainian population and degrade Kyiv's external sources of military and financial assistance.



As winter approaches, we may again see military strikes aimed at power and water utilities in Ukraine, combined with destructive wiper attacks on those networks.[27] CERT-UA Ukrainian cybersecurity authorities announced in September that Ukrainian energy networks were under sustained threat, and Microsoft Threat Intelligence observed artifacts of GRU threat activity on Ukrainian energy sector networks from August through October.[28] Microsoft observed at least one destructive use of the Sdelete utility against a Ukrainian power company network in August.[29]

Outside of Ukraine, the US presidential election, and other major political contests in 2024 may afford malign influence actors an opportunity to put their video media skills to use to turn the political tide away from elected officials who champion support to Ukraine.[30]

Microsoft is working across multiple fronts to protect our customers in Ukraine and worldwide from these multi-faceted threats. Under our Secure Future Initiative, we are integrating advances in AI-driven cyber defense and secure software engineering, with efforts to fortify international norms to protect civilians from cyber threats.[31] We are also deploying resources along with a core set of principles to safeguard voters, candidates, campaigns, and election authorities worldwide, as more than 2 billion people prepare to engage in the democratic process over the next year.[32]

1. https://www.gov.uk/government/news/new-intelligence-shows-russias-targeting-of-a-cargo-ship; https://www.reuters.com/world/europe/russia-destroyed-300000-tons-grain-since-july-port-ship-attacks-kyiv-2023-10-13/; https://x.com/DefenceHQ/status/1713570513883213916?s=20
2. For technical information on the latest destructive attack methods in Ukraine see https://ti.defender.microsoft.com/articles/6dd6a218
3. https://news.un.org/en/story/2023/07/1138532
4. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW10mGC
5. https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023-nation-state-threats, pg 57
6. https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/
7. https://news.un.org/en/story/2023/03/1134732
8. Based on notifications issued between March 15, 2023, and October 23, 2023.
9. https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
10. For more technical detail on ShadowLink visit the Microsoft Defender Threat Intelligence portal: https://ti.defender.microsoft.com/articles/fbbd8e0c
11. https://ssu.gov.ua/en/novyny/sbu-exposes-russian-intelligence-attempts-to-penetrate-armed-forces-planning-operations-system
12. https://ssu.gov.ua/uploads/files/DKIB/technical-report.pdf, p. 14.
13. https://www.npr.org/2023/08/10/1193167328/russia-hack-ukraine-military
14. https://cert.gov.ua/article/5213167; https://twitter.com/_cert_ua/status/1681544571472293888?s=46&t=2ofTkFXBlGBwAfFmxezNLDdcws200nAZcu8MzQjPWG8
15. https://cert.gov.ua/article/5213167
16. https://x.com/MsftSecIntel/status/1681695399084539908?s=20
17. hxxps://cert[.gov[.]ua/article/5702579
18. https://www.darkreading.com/application-security/steal-it-campaign-onlyfans-models-lures
19. disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf
20. https://www.sgdsn.gouv.fr/files/files/20230619_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_VF.pdf;
21. https://about.fb.com/wp-content/uploads/2022/11/CIB-Report_-China-Russia-Sept-2022.pdf;
22. https://www.lemonde.fr/en/france/article/2023/11/07/stars-of-david-graffiti-in-paris-russian-interference-suspected_6235378_7.html
23. https://www.kyivpost.com/videos/22580
24. ria[.]ru/20230817/zelenskiy-1890522044.html
25. tsargrad[.]tv/news/jelajdzha-vud-poprosil-zelenskogo-vylechitsja_829613; iz[.]ru/1574689/2023-09-15/aktrisa-iz-seriala-ofis-posovetovala-zelenskomu-otpravitsia-v-rekhab
26. https://www.economist.com/by-invitation/2023/11/01/the-commander-in-chief-of-ukraines-armed-forces-on-how-to-win-the-war; https://www.svoboda.org/a/zaluzhnyy-voyna-v-ukraine-stala-pozitsionnoy-chto-vygodno-rossii/32666890.html
27. https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/
28. https://cip.gov.ua/services/cm/api/attachment/download?id=60068
29. For technical details https://ti.defender.microsoft.com/articles/6dd6a218
30. https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2023/11/MTAC-Report-2024-Election-Threat-Assessment-11082023-2-1.pdf
31. https://blogs.microsoft.com/on-the-issues/2023/11/02/secure-future-initiative-sfi-cybersecurity-cyberattacks/
32. https://blogs.microsoft.com/on-the-issues/2023/11/07/microsoft-elections-2024-ai-voting-mtac/

Microsoft