Russian influence and cyber operations adapt for long haul and exploit war fatigue

blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/

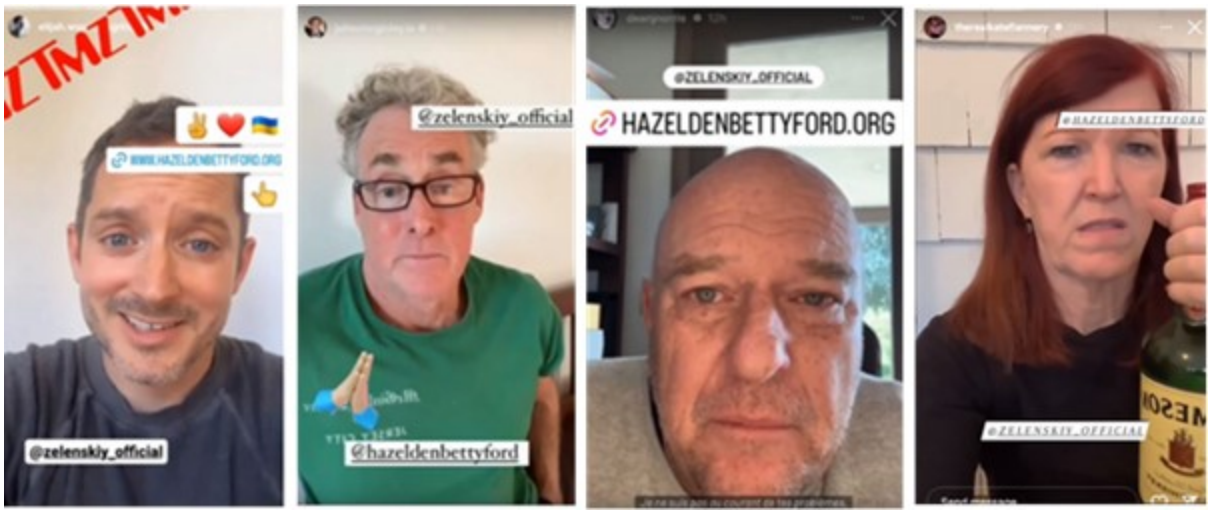
December 7, 2023

Since July 2023, Russia-aligned influence actors have tricked celebrities into providing video messages that were then used in pro-Russian propaganda. These videos were then manipulated to falsely paint Ukrainian President Volodymyr Zelensky as a drug addict. This is one of the insights in the latest biannual report on Russian digital threats from the Microsoft Threat Analysis Center: "Russian Threat Actors Dig In, Prepare to Seize on War Fatigue"

As described in more detail in the report, this campaign aligns with the Russian government's broader strategic efforts during the period from March to October 2023, across cyber and influence operations (IO), to stall Ukrainian military advances and diminish support for Kyiv.

Video messages from American celebrities are used in Russian propaganda

Unwitting American actors and others appear to have been asked, likely via video message platforms such as Cameo, to send a message to someone called "Vladimir", pleading with him to seek help for substance abuse. The videos were then modified to include emojis, links and sometimes the logos of media outlets and circulated through social media channels to advance longstanding false Russian claims that the Ukrainian leader struggles with substance abuse. The Microsoft Threat Analysis Center has observed seven such videos since late July 2023, featuring personalities such as Priscilla Presley, musician Shavo Odadjian and actors Elijah Wood, Dean Norris, Kate Flannery, and John McGinley.



Samples of the videos promoting pro-Russian propaganda aiming to malign Ukrainian President Volodymyr Zelensky that feature different celebrities

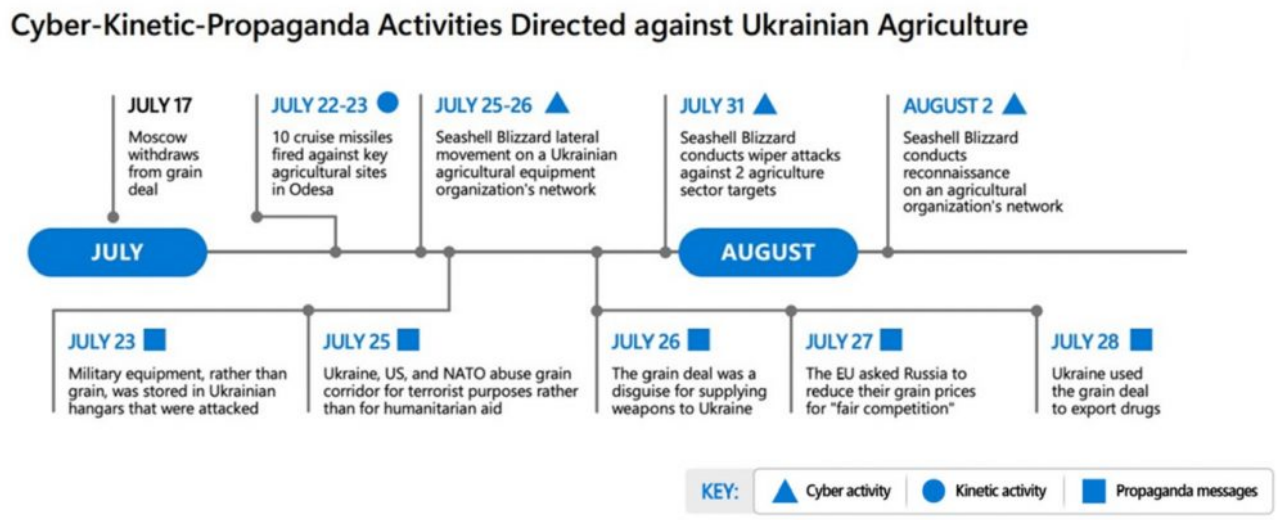
Prigozhin's death has not slowed Russia's influence operations

The August 2023 death of Russian businessman Yevgeny Prigozhin, who owned the Wagner Group and the infamous Internet Research Agency troll farm, led many to question the future of Russia's influence and propaganda capabilities. However, since then, Microsoft has observed widespread influence operations by Russian actors that are not linked to Prigozhin, indicating that Russia has the capacity to continue prolific and sophisticated malign influence operations without him.

Russia's seasonal focus switched to degrade Ukrainian agriculture

Just as the past winter saw Russia focus on creating an energy crisis and attacking Ukraine's energy sector, so this summer saw a convergence of Russian kinetic, cyber, and propaganda attacks on Ukraine's agriculture sector. During the warmer growing and harvest months, Russia penetrated agribusinesses, stole data, deployed malware, and used military strikes to destroy grain that reportedly could have fed one million people for a year.[1] Microsoft's report shows a strong alignment among its military, propaganda, and cyberattack efforts. For example, in a four-day period in late July 2023, following Moscow's withdrawal from the Black Sea Grain Initiative, Russia:

- Attacked agricultural facilities in Odessa with 10 cruise missiles
- Launched a cyberattack on a Ukrainian agricultural equipment organization
- Disseminated false narratives in pro-Russian media outlets claiming, in one example, that Ukraine, the U.S., and NATO were abusing the grain corridor for terrorist purposes not humanitarian aid



It remains to be seen if this winter will see Russia revert to its seasonal focus on the Ukrainian energy sector. However, in September 2023, the Government Computer Emergency Response Team of Ukraine (CERT-UA) announced that Ukrainian energy networks were under sustained threat and Microsoft Threat Intelligence has observed artifacts of Russian Military Intelligence (GRU) threat activity on Ukrainian energy sector networks from August through October 2023.

Russian cyberespionage prioritized war crimes investigations, governmental bodies, and think tanks

Russian authorities have not only been accused of war crimes, but have directed cyber resources to target the criminal investigators and prosecutors building cases against them. There is mounting tension between Moscow and organizations like the International Criminal Court (ICC), which issued an arrest warrant for Russian President Vladimir Putin on war crimes charges in March 2023. Actors linked to Russian military and foreign intelligence breached Ukrainian legal and investigative networks and a law firm working on war crimes investigations as part of a wider effort that targeted global diplomatic, defense, public policy, and IT organizations. One of those threat actors, aligned to the Russian Foreign Intelligence Service (SVR)and that we call Midnight Blizzard, has pursued access to more than 240 organizations since March 2023, predominantly in the U.S., Canada and European countries. Nearly 40% of the targeted organizations were governments, inter-governmental organizations, or policy-focused think tanks.

Russia shifted anti-Ukraine messaging to U.S., Israel

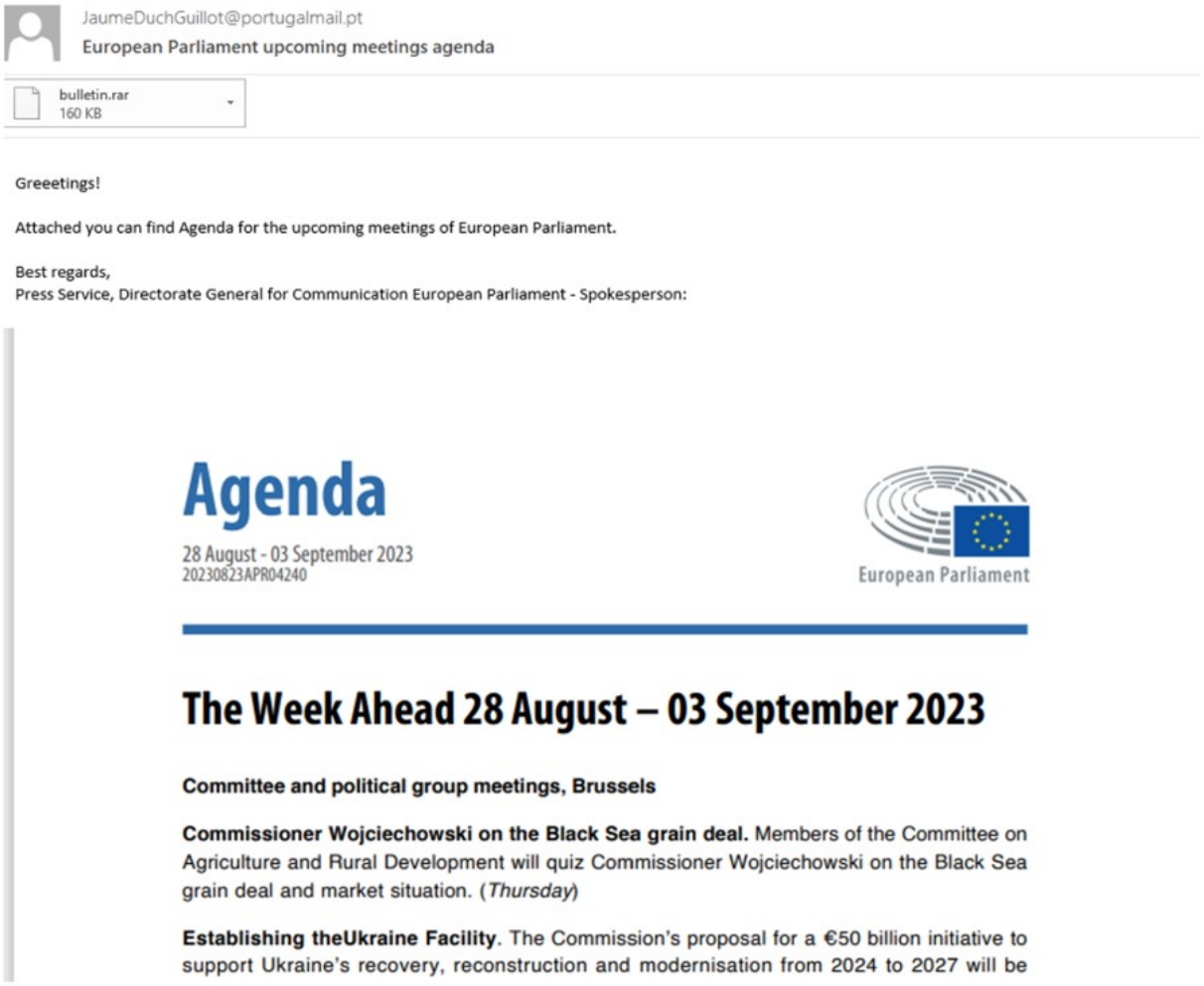
Sophisticated Russia-affiliated influence actor Storm-1099 (best known for a mass-scale website forgery operation dubbed “Doppelganger” by research group EU DisinfoLab) has been targeting international supporters of Ukraine since Spring 2022. The group creates unique, branded outlets such as the Reliable News Network (RNN) and stokes on-the-ground demonstrations, bridging the digital and physical worlds through amplification of these events. Despite efforts by technology companies and research entities to report on and mitigate its reach, Storm-1099 remains fully active. It has historically targeted Western European countries, especially Germany, but has now shifted focus to Israel and the U.S., reflecting an increased prioritization of content on the Israel-Hamas war, U.S. political themes, and the 2024 U.S. presidential election. Storm-1099 assets pushed the false claim that Hamas acquired Ukrainian weapons on the black market for its October 7 attack on Israel. Elsewhere, Russian-affiliated media pushed the false narrative that foreign recruits, including Americans, were transferred from Ukraine to join IDF forces in Gaza.

In late October 2023, French authorities suspected four Moldovan nationals of painting graffiti of the Star of David in public spaces in Paris, images of which were then amplified by Storm-1099 assets. Two of the Moldovans reportedly claimed that they were directed by a Russian-speaking individual, suggesting possible Russian responsibility for the incident,

which strongly aligns with Russia's Active Measures playbook. Russia likely assesses that the ongoing Israel-Hamas conflict is to its geopolitical advantage, as it believes the conflict distracts the West from the war in Ukraine.

Ukrainian military infrastructure and defense partners remain key targets

Since Russian forces launched their spring 2023 offensive in Ukraine, Russian intelligence-affiliated cyber actors have concentrated their efforts on intelligence collection from Ukrainian communications and military infrastructure in combat zones, and from Ukraine's partners. One actor, that we call Forest Blizzard, 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 to accountholders at a European defense organization.



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

Looking forward

Ukraine's military chief has suggested the war with Russia is moving to a new stage of static trench warfare, protracting the conflict further. Russian cyber and influence operators will aim to demoralize the Ukrainian population and degrade Kyiv's external sources of military and financial assistance, along with possible winter attacks on Ukraine's energy sector.

Elsewhere, the 2024 U.S. presidential election and other major political contests give malign influence actors an opportunity to degrade support for Ukraine-supporting political candidates. To date, Russian threat actors and propagandists have not demonstrated sophisticated capabilities leveraging or integrating artificial intelligence (AI) tools into influence operations. However, Microsoft continues to monitor this area closely.

Microsoft is working across multiple fronts to protect our customers in Ukraine and worldwide from these multifaceted threats. With our Secure Future Initiative, we are integrating advances in AI-driven cyberdefense and secure software engineering, with efforts to fortify international norms to protect civilians from cyber threats. In the elections space, we are deploying resources across a core set of principles to safeguard voters, candidates, campaigns, and election authorities worldwide, as more than two billion people prepare to engage in the democratic process over the coming year.

---

[1] https://www.gov.uk/government/news/new-intelligence-shows-russias-targeting-of-a-cargo-ship

Tags: cyberattacks, cybersecurity, cyberwar, digital threats, MTAC, Russia, threat, Ukraine