

University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

Copyright, Fair Use, Scholarly Communication,
etc.

Libraries at University of Nebraska-Lincoln

2-2023

Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape

Threat Analysis Group (TAG)

Mandiant

Google Trust & Safety

Follow this and additional works at: <https://digitalcommons.unl.edu/scholcom>



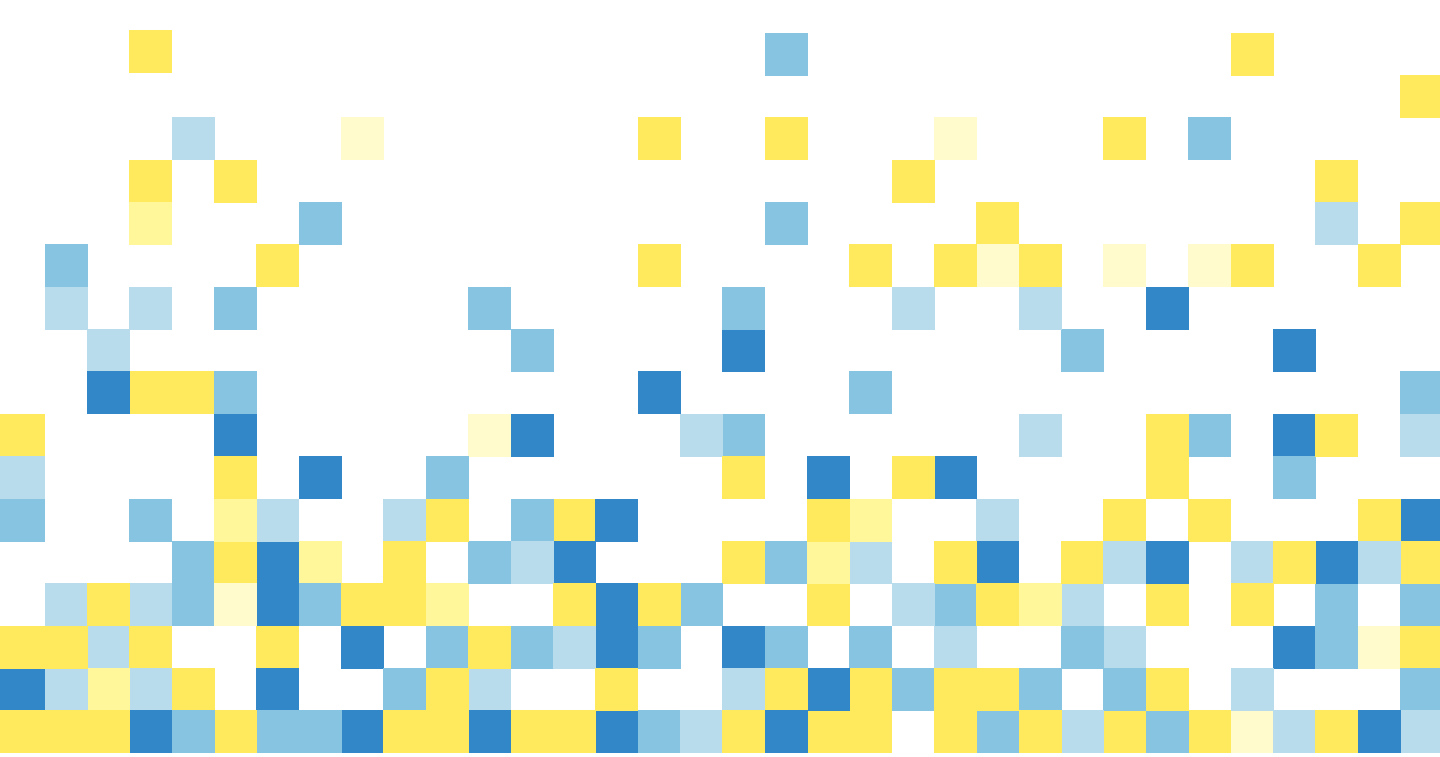
Part of the [Intellectual Property Law Commons](#), [Scholarly Communication Commons](#), and the [Scholarly Publishing Commons](#)

This Article is brought to you for free and open access by the Libraries at University of Nebraska-Lincoln at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Copyright, Fair Use, Scholarly Communication, etc. by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.



Fog of War

How the Ukraine Conflict Transformed
the Cyber Threat Landscape



About the authors



Google's [Threat Analysis Group \(TAG\)](#) is responsible for countering threats to Google and our users from government-backed attackers, coordinated information operations (IO), and serious cybercrime networks. We apply our intelligence to improve Google's defenses and protect users.



[Mandiant](#), now part of Google Cloud, is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to defend against and respond to cyber threats.



[Google Trust & Safety](#) safeguards Google products against abuse and provides trusted and safe experiences for all users.

Table of contents

Foreword	2
Section 1	
Government-backed attackers	6
Russian government-backed attackers aggressively pursue wartime advantage in cyberspace	
Section 2	
Information Operations	28
Moscow leverages full spectrum of information operations to shape public perception of war	
Section 3	
Cybercrime	41
War has split the loyalties of financially motivated attackers	
Conclusion	46

Foreword

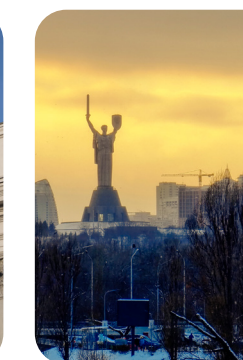
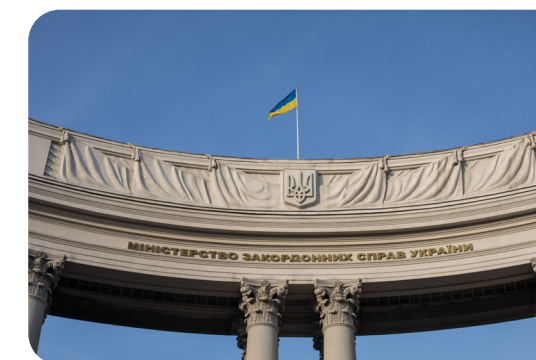
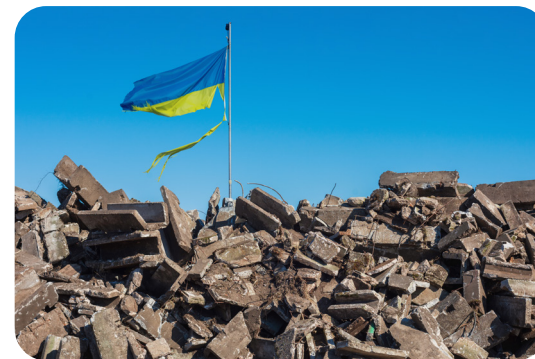
One year ago, Russia invaded Ukraine. Since then, tens of thousands of people have been killed, millions of Ukrainians have fled and the country has sustained tens of billions of dollars worth of damage. Importantly, this marks the first time that cyber operations have played such a prominent role in a world conflict.

Since the war began, governments, companies, civil society groups, and countless others have been working around the clock to support the Ukrainian people and their institutions. At Google, we [support these efforts](#) and continue to announce new commitments and support to Ukraine. This includes a donation of 50,000 [Google Workspace](#) licenses for the Ukrainian government and a [rapid Air Raid Alerts system for Android phones](#) in Ukraine, [support for refugees](#), businesses, and entrepreneurs, and [measures](#) to indefinitely pause monetization and significantly limit recommendations globally for a number of Russian state news media across our platforms.

One of the most pressing challenges, however, is that the Ukrainian government is under near-constant digital attack. That's why one of our most important contributions to date has been our ongoing work to provide cybersecurity assistance to Ukraine. Shortly after the invasion, for example, we expanded eligibility for [Project Shield](#), our free protection against distributed denial of service attacks (DDoS), so that Ukrainian government websites and embassies worldwide could stay online and continue to offer their critical services.

We continue to provide direct assistance to the Ukrainian government and critical infrastructure entities under the [Cyber Defense Assistance Collaborative](#) — including compromise assessments, incident response services, [shared cyber threat intelligence](#), and [security transformation services](#) — to help the Ukrainian government detect, mitigate, and defend against cyber attacks. In addition, we continue to implement [protections for users](#) and track and disrupt cyber threats to help raise awareness among the security community and high risk users and maintain information quality.

This level of collective defense — between governments, companies, and security stakeholders across the world — is unprecedented in scope. It is important then to pause and reflect on this work and our learnings one year later, and share those with the global security community to help prepare better defenses for the future. This report outlines our analysis of these issues and includes the following three observations, informed by over two decades of experience managing complex global security events.





First, Russian government-backed attackers have engaged in an aggressive, multi-pronged effort to gain a decisive wartime advantage in cyberspace, often with mixed results.

This includes a significant shift in various groups' focus towards Ukraine, a dramatic increase in the use of destructive attacks on Ukrainian government, military and civilian infrastructure, a spike in spear-phishing activity targeting NATO countries, and an uptick in cyber operations designed to further multiple Russian objectives. For example, we've observed threat actors hack-and-leak sensitive information to further a specific narrative.



Second, Moscow has leveraged the full spectrum of information operations — from overt state-backed media to covert platforms and accounts — to shape public perception of the war.

These operations have three goals: (1) undermine the Ukrainian government; (2) fracture international support for Ukraine; and (3) maintain domestic support in Russia for the war. We've seen spikes of activity associated with key events in the conflict such as the buildup, invasion, and troop mobilization in Russia. At Google, we've worked aggressively across products, teams, and regions to counter these activities where they violate our policies and disrupt overt and covert information operations campaigns, but continue to encounter relentless attempts to circumvent our policies.



Finally, the invasion has triggered a notable shift in the Eastern European cybercriminal ecosystem that will likely have long term implications for both coordination between criminal groups and the scale of cybercrime worldwide.

Some groups, for example, have split over political allegiances and geopolitics, while others have lost prominent operators. This will impact the way we think about these groups and our traditional understanding of their capabilities. We've also seen a trend towards specialization in the ransomware ecosystem that blends tactics across actors, making definitive attribution more difficult. Importantly, the war in Ukraine has also been defined by what we expected — but didn't see. For example, we didn't observe a surge of attacks against critical infrastructure outside of Ukraine.

Together, these observations point to several broader forward looking assessments for the security community for 2023:



We assess with high confidence that Russian government-backed attackers will continue to conduct cyber attacks against Ukraine and NATO partners to further Russian strategic objectives.



We assess with high confidence that Moscow will increase disruptive and destructive attacks in response to developments on the battlefield that fundamentally shift the balance — real or perceived — towards Ukraine (e.g., troop losses, new foreign commitments to provide political or military support, etc.). These attacks will primarily target Ukraine but increasingly expand to include NATO partners.



We assess with moderate confidence that Russia will continue to increase the pace and scope of information operations to achieve the objectives described above, particularly as we approach key moments like international funding, military aid, domestic referendums, and more. What's less clear is whether these activities will achieve the desired impact, or simply harden opposition against Russian aggression over time.

It is clear cyber will now play an integral role in future armed conflict, supplementing traditional forms of warfare. We hope this report serves as a call to action as we prepare for potential future conflicts around the world. At Google, we are committed to doing our part to support collective defense and look forward to partnering with others to drive continued progress and help organizations, businesses, governments, and users stay safe online.

Section 1

Government-backed attackers

Russian government-backed attackers aggressively pursue wartime advantage in cyberspace

Since the start of the war, Russian government-backed attackers have aggressively targeted Ukraine and its supporters, particularly NATO member countries. Based on analysis from across Google, we see a multi-pronged Russian effort to gain a wartime advantage through cyberspace. This effort includes a range of campaigns designed to improve intelligence collection, deploy destructive attacks against victim networks, and advance active measures to shape the information environment in Moscow's favor.

A note on threat actor naming conventions

Our understanding of these groups is based on a body of technical data that includes infrastructure, malware, and the broader set of tactics, techniques, and procedures (TTPs) threat actors use in their campaigns. Other analysts may use different methodologies to assess actor activity. There is no single industry standard for naming these actors, but we've listed aliases where our group names align with others.

Attribution to the underlying entity behind the group often comes later (if at all) from clues in the technical data and other sources like media and publicly available government documents. It is not uncommon for

multiple actors representing distinct sets of technical activity to eventually be attributed to the same ultimate organization, similar to the attribution we made to GRU in this paper (see the threat actor deep dives).

We use the term "government-backed attacker" instead of the term "advanced persistent threat" (APT) to more clearly differentiate these groups from other financially motivated actors discussed later in the paper.



Russia's cyber preparations began long before the invasion

Russian government-backed attackers ramped up cyber operations beginning in 2021 during the run up to the invasion. This led to a 250% increase in Russian phishing campaigns directed against users in Ukraine in 2022 (compared to a 2020 baseline). We attribute this increase to two primary factors: (1) some attackers intensified their traditional focus on Ukraine and (2) others shifted their focus towards Ukraine. To help counter these efforts, we disrupted phishing campaigns against the Ukrainian government and military organizations, as well as critical infrastructure, media and the information space.



Users in NATO countries face intensified targeting

Since the war began, we've seen an over 300% increase in Russian phishing campaigns directed against users in NATO countries in 2022 (compared to a 2020 baseline). These efforts may reflect a longstanding Russian strategic priority to gather better insight into NATO activities, but in 2022 they were driven primarily by a Belarusian government-backed group that is closely aligned with Russia.



Waves of destructive malware hit Ukraine

Russian Armed Forces' Main Directorate of the General Staff (GRU) -sponsored actors have used destructive malware to disrupt and degrade Ukraine's government and military capabilities. In parallel, we've seen similar attacks on civilian infrastructure in an attempt to undermine the public's trust in the government's ability to deliver basic services. We observed more destructive cyberattacks in Ukraine during the first four months of 2022 than in the previous eight years with a notable spike in activity at the start of the invasion. In contrast to NotPetya, we've seen little evidence of a spillover effect outside Ukraine.



Russia uses cyber operations for multiple strategic objectives

We've observed a notable uptick in the intensity and frequency of Russian cyber operations designed to maximize access to victim networks, systems, and data to achieve multiple strategic objectives. For example, GRU-sponsored actors have used their access to steal sensitive information and release it to the public to further a narrative, or use that same access to conduct destructive cyber attacks or information operations campaigns.

In this section, we outline trends in the threat landscape and then dive deeper into specific Russian government-backed attackers and their behavior in 2022.



FROZENBARENTS

Aliases
Sandworm
Voodoo Bear
IRIDIUM



FROZENLAKE

Aliases
APT28
SOFACY
Fancy Bear
STRONTIUM
Sednit



COLDRIVER

Aliases
GOSSAMER BEAR
Callisto Group
SEABORGIUM
TA446



FROZENVISTA

Aliases
UNC2589



PUSHCHA

Aliases
UNC1151



SUMMIT

Aliases
Turla Team
Snake
Uroburos
VENOMOUS BEAR
UNC4210



Espionage



Information Operations



Destruction



Targeted nations

- Ukraine
- NATO countries
- Georgia
-
- South Korea
-
-
- Middle East
- Central Asia
-

- Ukraine
- NATO countries
-
-
-
- Europe
- South America
- Middle East
- Central Asia
-

- Ukraine
- NATO countries
-
-
-
-
-
-
-
-

- Ukraine
- NATO countries
-
-
-
-
-
-
-
-

- Ukraine
- NATO countries
-
- Russia
-
-
-
-
-
-

- Ukraine
- NATO countries
-
-
- Australia
-
- South America
- Middle East
-
- Southeast Asia



Primary targets

- Government
- Military and Defense
- Energy
- Financial
-
- Heavy Industry
- High Tech and Telecom
- Higher Education
- News Media
- NGOs
- Shipping and Rail

- Government
- Military and Defense
- Energy
- Financial
-
- Heavy Industry
- High Tech and Telecom
- Higher Education
- News Media
- NGOs
- Shipping and Rail

- Government
- Military and Defense
- Energy
-
-
-
-
- Higher Education
- News Media
- NGOs
-

- Government
- Military and Defense
- Energy
- Financial
- Healthcare
- Heavy Industry
- High Tech and Telecom
- Higher Education
-
-
- News Media
- NGOs
-
- Shipping and Rail

- Government
- Military and Defense
-
-
-
-
- High Tech and Telecom
- Higher Education
- News Media
- NGOs
-

Understanding the threat landscape

Phishing remains a prominent initial access vector for government-backed attackers. Attackers use this access to achieve multiple Russian strategic objectives, such as intelligence collection, data destruction, and information leaks intended to further Russian national objectives.

From 2021-2022, TAG observed government-backed attackers conduct phishing campaigns against a series of targets (Figure 1). During that time, we saw a steady drumbeat in phishing attacks. At the same time, we noted several spikes in activity from large campaigns. In 2022, for example, we saw a 250% increase targeting users in Ukraine and an over 300% increase targeting users in NATO countries — both compared to a 2020 baseline. These numbers include Gmail users and accounts with a country code top-level domain (e.g., @gov.ua).

We assess that these attacks were all carried out by Russian government-backed attackers. However, in the graphic, we also included information on PUSHCHA, a closely aligned group from Belarus. This activity is important to capture because it was heavily focused on Ukraine and its neighbors. For more information on activity associated with specific groups, see the threat actor deep dives.

In 2022, Russian government-backed attackers targeted users in Ukraine more than any other country. We attribute this to two primary factors: (1) some attackers (FROZENBARENTS, FROZENLAKE) intensified their traditional focus on Ukraine and (2) others (COLDRIVER) shifted their focus towards Ukraine. While we see Russian government-backed attackers focus heavily on Ukrainian government and military entities, the campaigns we disrupted also show a strong targeting focus on critical infrastructure, utilities and public services, and the media and information space (FROZENBARENTS, FROZENLAKE, COLDRIVER, FROZENVISTA).

Figure 1
PHISHING CAMPAIGNS BY GOVERNMENT-BACKED ATTACKERS

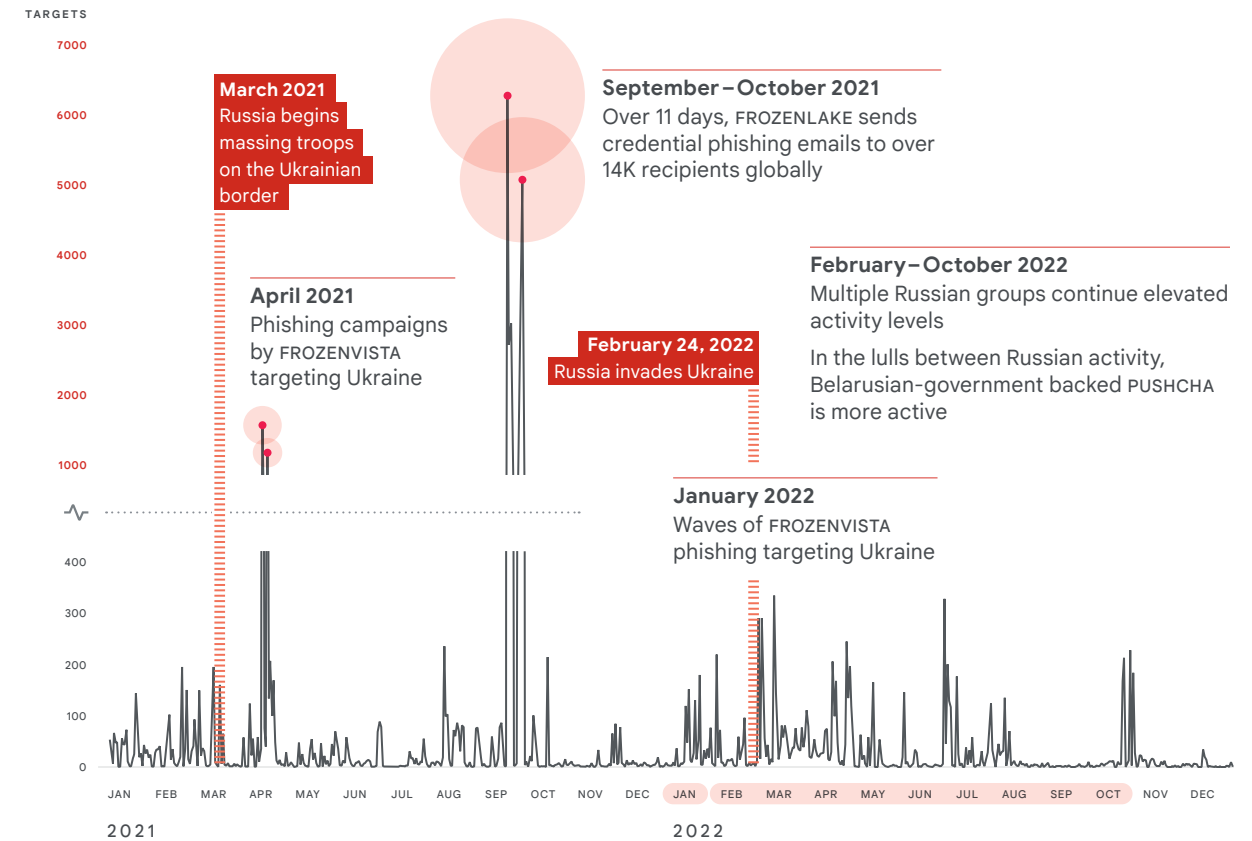
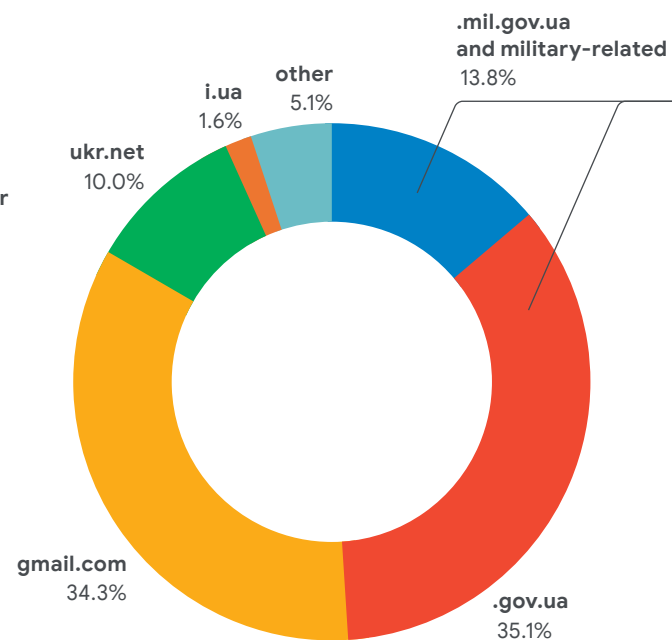


Figure 2
TOP TARGETED DOMAINS

From 2021 to 2022, Russia targeted over 150 military and government entities on the gov.ua and mil.gov.ua domains.

Targets included Ukrainian military and diplomatic organizations, as well as government agencies that manage critical infrastructure, civil services and emergency management.



TOP 10 TARGETS — UKRAINIAN GOVERNMENT AND MILITARY

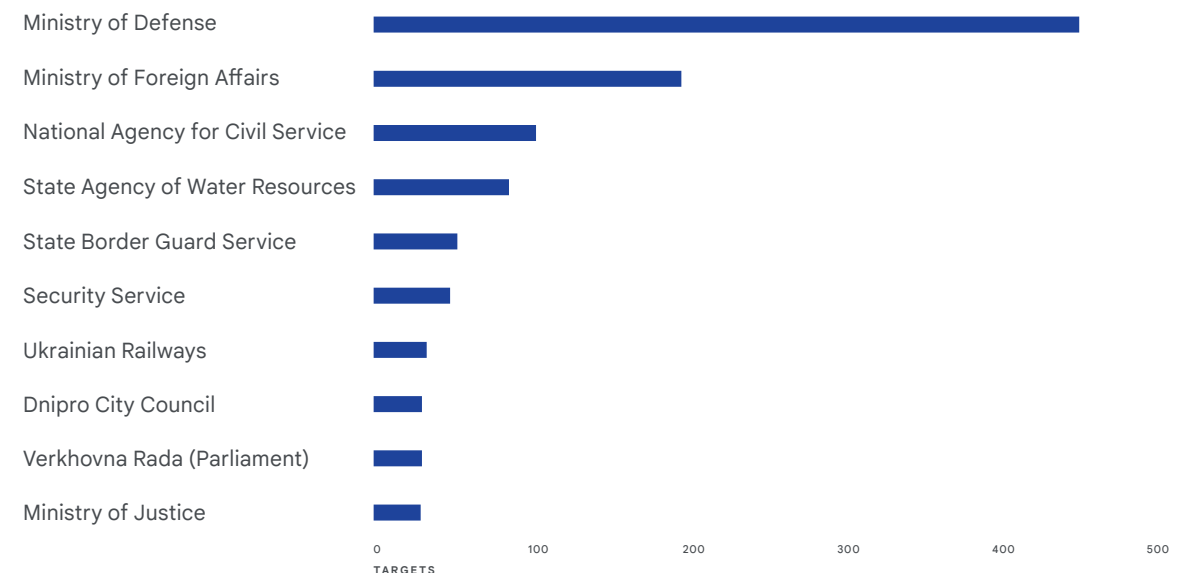
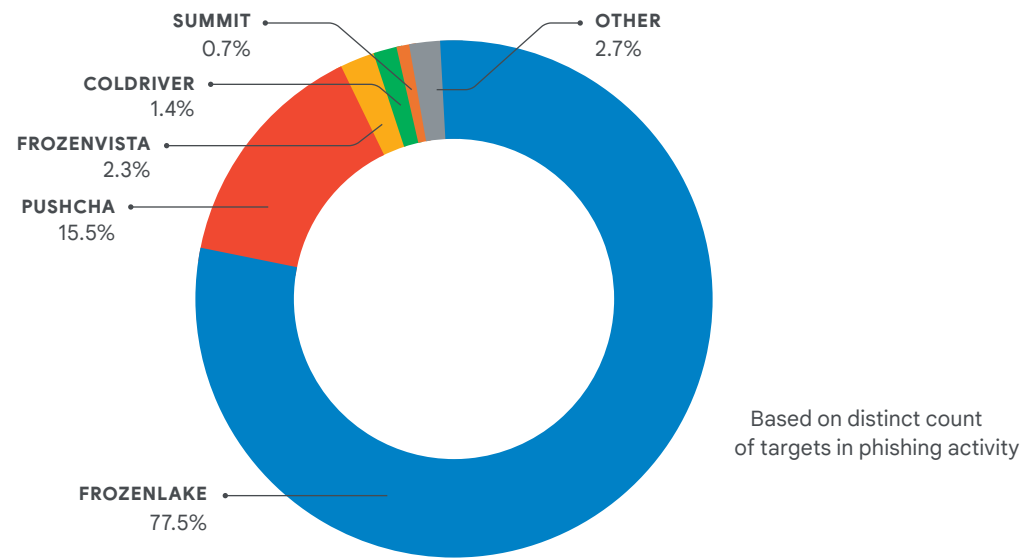


Figure 3
GOVERNMENT-BACKED
ATTACKER ACTIVITY TARGETING
USERS IN NATO COUNTRIES



Russian government-backed attackers have long prioritized NATO targets, but these attacks have intensified since the runup to the war. FROZENLAKE, for example, launched a massive wave of attacks against NATO targets in September 2021, while PUSHCHA’S campaigns centered on targets in Poland and Lithuania in 2022. In addition, groups like SUMMIT continue to remain focused on NATO targets and others like COLDRIVER have shifted their focus to European militaries.

In parallel to the phishing campaigns described above, we’ve seen attackers use their access to shape the information environment. For example, evidence shows that some GRU actors worked together to leak information to hacktivist groups, and we’ve also observed at least one threat actor (COLDRIVER) use their access for a hack-and-leak operation targeting the United Kingdom.

At Google, we continue to disrupt campaigns from government-backed attackers. Once we identify malicious websites and domains, we add them to [Safe Browsing](#) to protect users from further exploitation. Where appropriate, we also [notify Gmail and Workspace users](#) that they were targeted by government-backed attackers. For additional protections, we recommend that users enable [Google Account Level Enhanced Safe Browsing](#) and update their devices with the latest software.

In 2022, Russia increased targeting of users in Ukraine by 250% compared to 2020. Targeting of users in NATO countries increased over 300% in the same period.

Destructive cyber attacks targeting Ukraine

Russian-backed government actors used destructive malware — commonly called “wipers” because they destroy data — to target Ukraine in 2015, 2016, and 2017. The NotPetya attack in 2017 caused [billions of dollars of damage globally](#). As a result, many experts anticipated similar attacks during the war and that the effects would spill over outside Ukraine, which largely did not happen in 2022¹.

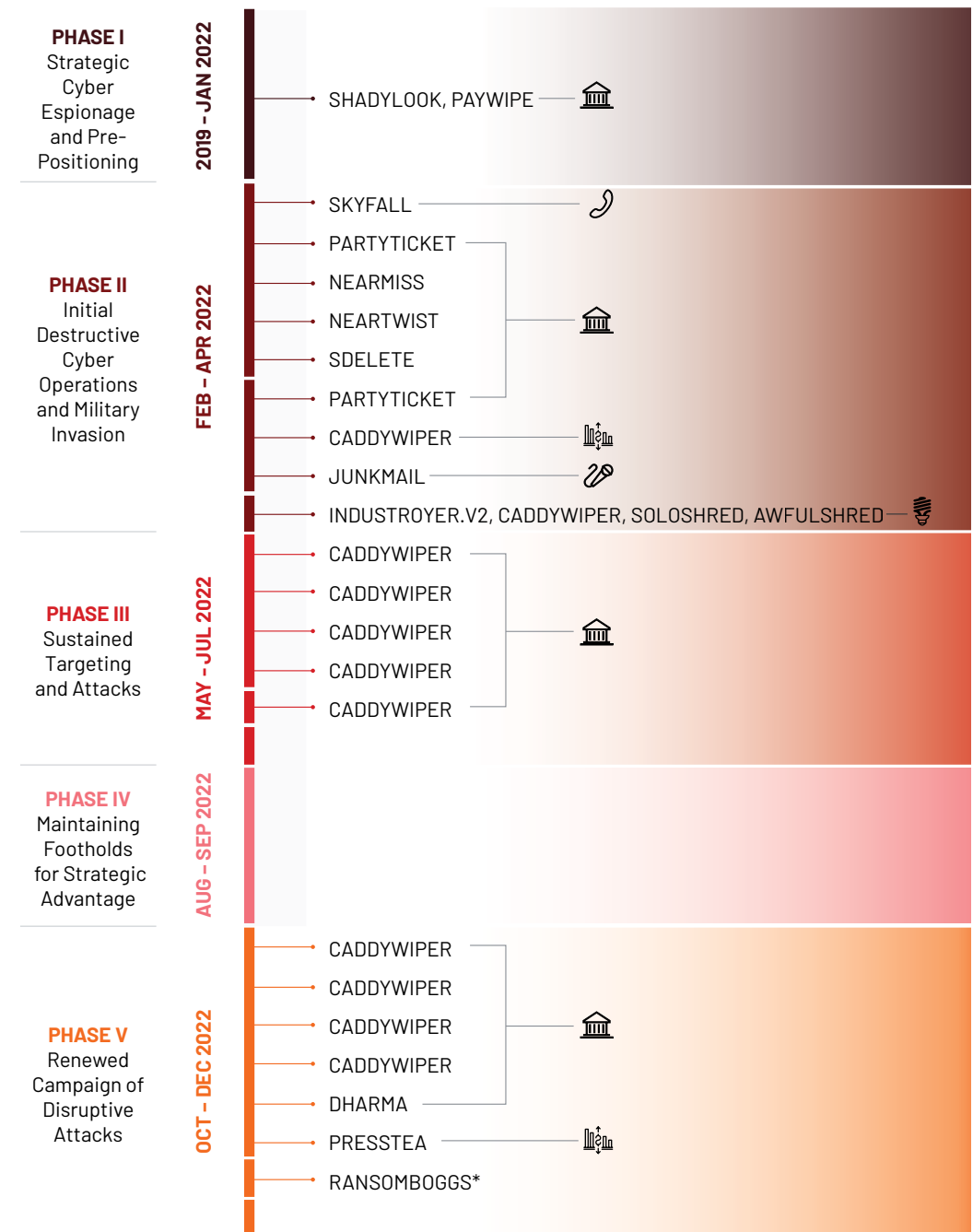


From its incident response work, Mandiant observed more destructive cyberattacks in Ukraine during the first four months of 2022 than in the previous eight years with attacks peaking around the start of the invasion.

While Mandiant saw significant activity after that period, the pace of attacks slowed and appeared less coordinated than the initial wave in February 2022. Destructive attacks often occurred more quickly after the attacker gained or regained access, often via compromised edge infrastructure. Many operations indicated an attempt by the GRU to balance competing priorities of access, collection, and disruption throughout each phase of activity.

Mandiant observed at least six unique wipers with some of these having multiple variants. While the destructive cyberattacks did achieve significant widespread disruption initially in some Ukrainian networks, they were likely not as impactful as previous Russian cyberattacks in Ukraine. To conduct the initial waves of destructive activity, Russian actors often employed accesses gained months before, which were often lost as the attack was remediated. The willingness to prioritize destructive attacks at the cost of persistent access indicates their importance to Russia’s overall strategy in Ukraine or the lack of operational preparation that could have sustained some persistent accesses while burning others during destructive activity.

FIVE PHASES OF RUSSIAN CYBER OPERATIONS DURING THE 2022 WAR IN UKRAINE January - December 2022



Target Industries

- Government
- Telecom
- Financial
- Media
- Energy

*As reported by ESET

¹ One exception was the cyber attack against the Viasat KA-SAT network hours before the Russian invasion that resulted in [a partial interruption of KA-SAT’s satellite broadband service](#). The governments of the [UK](#) and [US](#) attributed the attack to Russia, in order to “disrupt Ukrainian command and control during the invasion.” The incident also impacted tens of thousands of other fixed broadband customers across Europe, and German energy company Enercon said a “massive disruption” of satellite connections in Europe [affected the operations of 5,800 wind turbines](#) in central Europe.



FROZENBARENTS

Aliases

Sandworm
Voodoo Bear
IRIDIUM

Attribution

Russian Armed Forces'
Main Directorate of the General
Staff (GRU)

Overview

Active since at least 2009, primarily conducts cyberespionage, destructive attacks, and IO. Has previously focused on Ukraine and [works closely](#) with the GRU-associated group FROZENLAKE

Key campaigns

2015 and 2016

- Ukraine energy sector

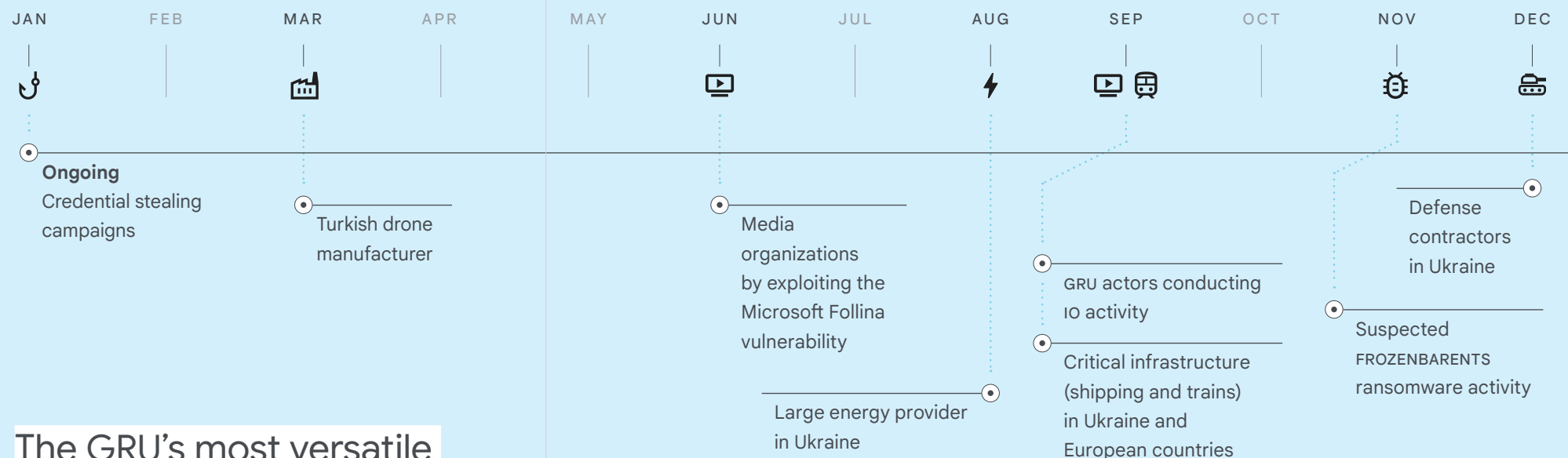
2017

- [French elections](#)
- NotPetya

2018

- [Olympic Destroyer attacks against Winter Olympic Games](#)
- The 2018 operation against the Organization for the Prohibition of Chemical Weapons
- Attacks against [Georgia in 2018 and 2019](#)

2022 TARGETING ACTIVITY



The GRU's most versatile operators do it all

In 2022, FROZENBARENTS served as a vivid example of the overlap between different spheres of cyber activity, conducting campaigns for intelligence collection, destructive network attacks, contributing to information operations, and even using “hack-for-hire” services to secure initial access to some targets.

Military

FROZENBARENTS campaigns seem designed to advance Russian strategic objectives and respond to changes in Russian intelligence requirements throughout the conflict. FROZENBARENTS targeted a Turkish drone manufacturer, whose systems were [used by Ukraine](#) in the early weeks of the war. Russia subsequently [disabled](#) the drones. Other campaigns have targeted sensitive information like Ukrainian military communications and troop movements.

Critical Infrastructure

TAG detected multiple credential stealing campaigns targeting critical infrastructure likely leveraging persistent malware infections such as DarkCrystal RAT. In August, TAG observed FROZENBARENTS targeting a large energy provider in Ukraine. TAG also observed FROZENBARENTS targeting logistics organizations — including shipping and trains — in Ukraine and other European countries.

In 2022, groups associated with the GRU served as a vivid example of the overlap between different spheres of cyber activity, conducting campaigns for intelligence collection, destructive network attacks, and contributing to information operations.

Media and IO

In June 2022, TAG observed GRU actors, including FROZENBARENTS, [exploit](#) the Microsoft Follina vulnerability, consistent with [CERT-UA reporting](#). The campaign primarily targeted media organizations and used compromised government accounts to send malicious links to Microsoft Office documents hosted on compromised domains.

In the IO space, FROZENBARENTS created and disseminated news content, including stories published on their own Substack blog. This content included conspiracies about Western biological weapons labs in Ukraine. The group also appears to be soliciting contributions to a GRU-controlled Telegram channel distributing pro-Russian content.



FROZENLAKE

Aliases

APT28
SOFACY
Fancy Bear
STRONTIUM
Sednit

Attribution

Russia GRU

Overview

Active since at least 2004, FROZENLAKE conducts cyberespionage against a broad range of targets including governments, military, technology, NGOs, media, democracy and civil society. The group has built and deployed a custom credential phishing framework and multiple [custom implants](#) over the years.

Key campaigns

2016

Compromising the US Democratic National Committee during the [2016 US national elections](#)

2014–2018

[Indicted](#) for intrusions against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations

Focused on credential phishing campaigns

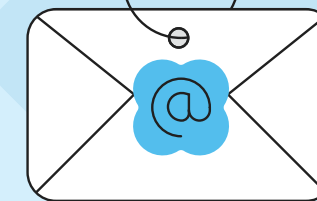
Throughout the war, FROZENLAKE conducted widespread phishing campaigns to collect information to provide political and military advantage, and relied on opportunistic access through historical compromise to conduct destructive cyber attacks.

Credential harvesting

In March 2022, TAG reported [several large credential phishing campaigns](#) targeting users of ukr.net, a popular email account provider in Ukraine. The phishing emails were sent from a large number of non-Google compromised accounts and included links to attacker-controlled domains. In two other campaigns, the attackers used newly created Blogspot domains as the initial landing page, which then redirected targets to credential phishing pages. Google disrupted this activity, taking down all detected Blogspot domains. This activity resurfaced in late 2022. TAG detected multiple credential campaigns primarily targeting ukr.net users, but also gov.ua accounts.

Figure 4
Example of FROZENLAKE credential phishing page

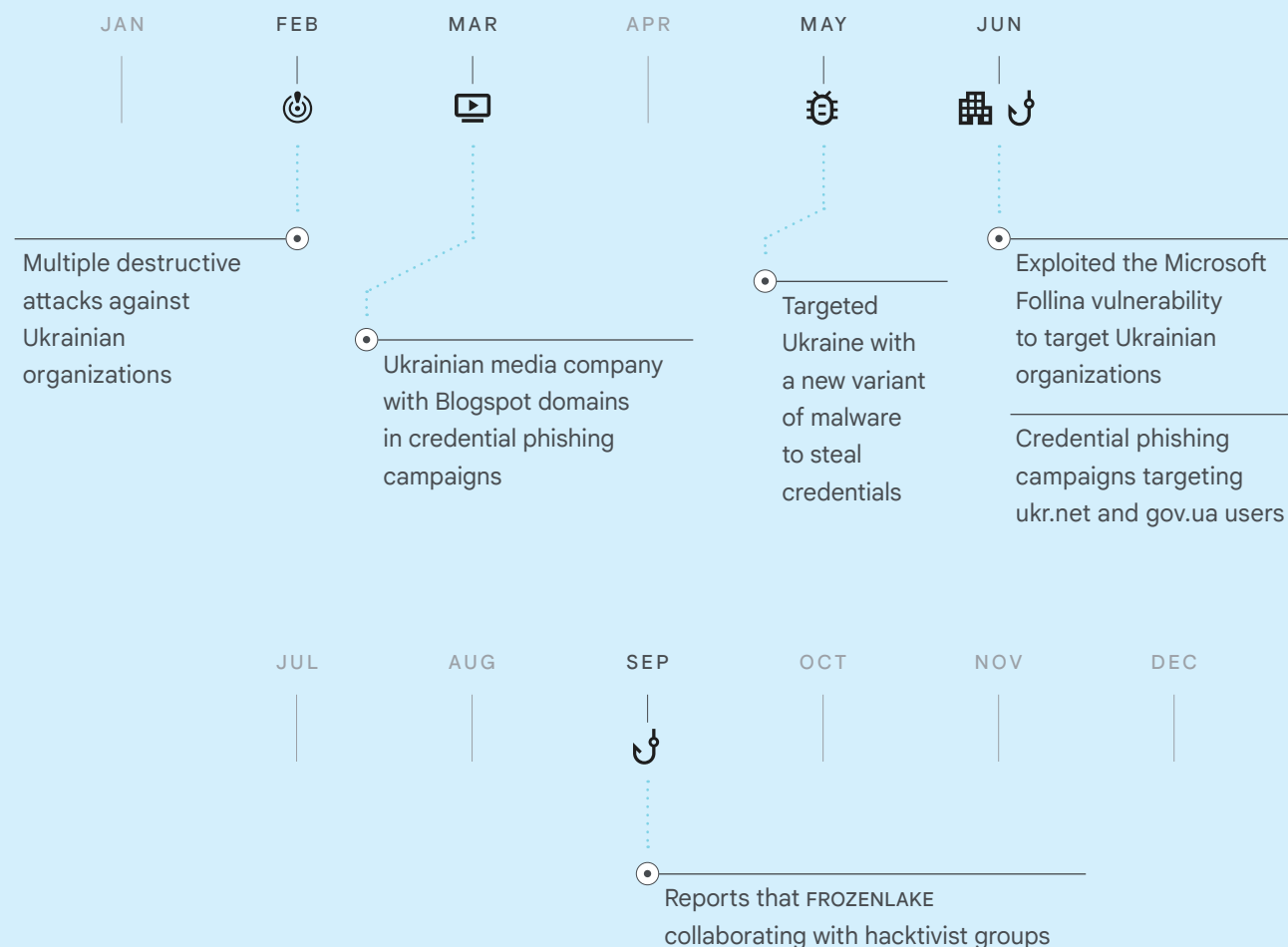
In May 2022, TAG observed FROZENLAKE [targeting users in Ukraine with a new variant of malware](#). The malware, distributed via email attachments inside of password protected zip files (e.g., ua_report.zip), is a .net executable that steals cookies and saved passwords from Chrome, Edge and Firefox browsers. The data is then exfiltrated to a compromised email account.



IO

Our analysis of FROZENLAKE activity suggests that GRU, or other Russian Intelligence Services, may be [coordinating with “hactivist” groups](#) to shape the information environment. Mandiant discovered FROZENLAKE tools on the networks of Ukrainian victims of wiper malware, whose data was quickly leaked by the “hactivists,” as well as other indicators of inauthentic activity by the moderators and similarities to previous GRU information operations.

2022 TARGETING ACTIVITY





COLD DRIVER

Aliases

GOSSAMER BEAR
Callisto Group
SEABORGIUM
TA446

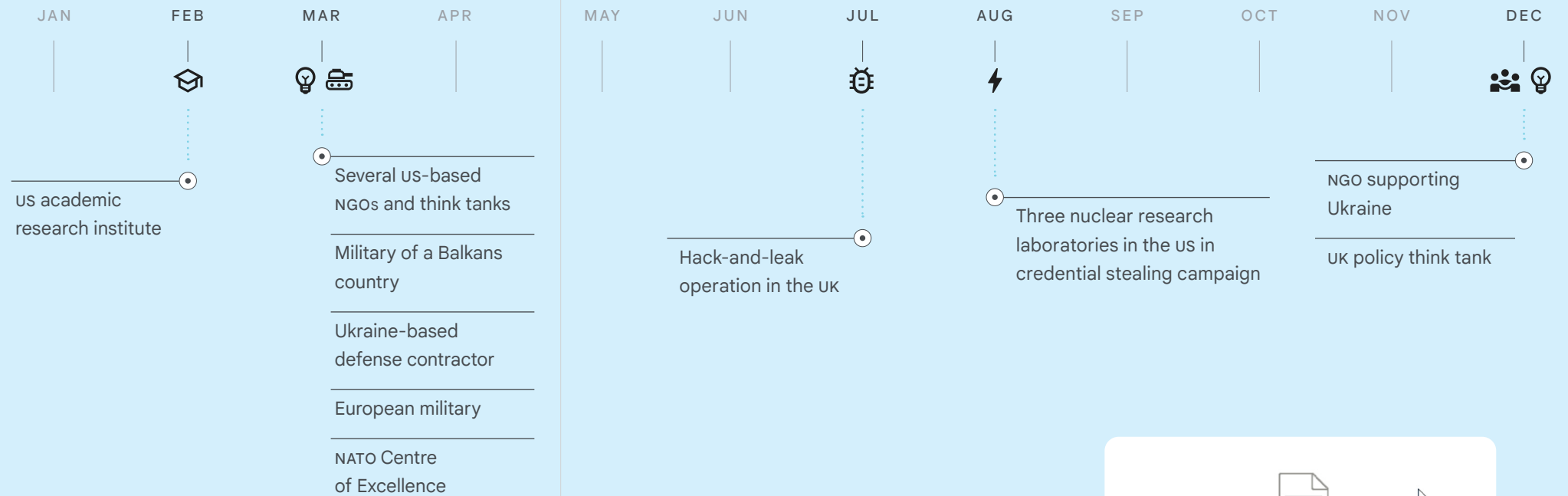
Attribution

Russia

Overview

Active since [at least 2015](#), conducts credential phishing campaigns against defense sector, non-governmental organizations (NGOs), think tanks, higher education and journalists. The group generally targets current or former high profile individuals. COLD DRIVER [primarily](#) targets NATO countries, and shifted to include the Ukrainian government and organizations supporting the war in Ukraine.

2022 TARGETING ACTIVITY



Expanded targeting to Ukraine, hack-and-leak campaign targeting UK

COLD DRIVER, a Russian group focused on credential phishing activities, typically targets NATO countries. In 2022, COLD DRIVER expanded their credential phishing campaigns to include Ukraine and shifted focus to more government and military-related targets. In addition, COLD DRIVER conducted a hack-and-leak campaign targeting the UK in July 2022, the first time we've seen the group do so. COLD DRIVER continues to use impersonation accounts to target the personal email addresses of prominent individuals at think tanks and NGOs focused on Ukraine.

Government and Military

March 2022 [marked](#) the first time TAG observed COLD DRIVER campaigns targeting the military of multiple European countries, as well as a NATO Centre of Excellence. In the early stages of the conflict, COLD DRIVER shifted their targeting to include multiple Ukrainian defense contractors and government organizations, as well as US-based NGOs, think tanks, government officials, politicians, and journalists.

Ukraine-focused thought leaders

COLD DRIVER continues to use impersonation accounts to target the personal email addresses of prominent individuals at think tanks and NGOs focused on Ukraine. As early as February 2022, COLD DRIVER targeted a US academic research institute, and the activity continued throughout the year when the group targeted an NGO supporting Ukraine and a UK policy think tank.

US nuclear energy sector

In August and September 2022, around the time the UN sent [inspectors](#) to visit Ukraine's Zaporizhzhia nuclear power plant in Russian-controlled territory, COLD DRIVER [targeted three nuclear research laboratories in the US](#) in a credential stealing campaign. The campaign created fake login pages for each institution and emailed nuclear scientists in an attempt to steal their passwords.

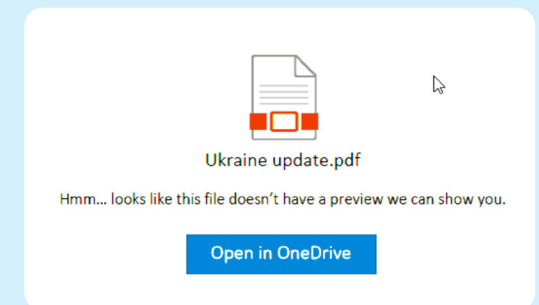


Figure 5

Example COLD DRIVER lure

Hack-and-leak

In July 2022, a COLD DRIVER phishing campaign targeted the Proton email accounts of several prominent figures in the United Kingdom and the attackers subsequently [leaked](#) information in an attempt to shape public opinion. A website published leaked emails from several leading proponents of Britain's exit from the European Union (Brexit) and suggested that they were secretly making decisions in the UK.



FROZENVISTA

Aliases

UNC2589

Attribution

Russia

Overview

FROZENVISTA is the main actor behind mass phishing campaigns TAG observed targeting Ukraine in April 2021 and January 2022. In addition to mass phishing campaigns delivering malware, the group deployed destructive malware against Ukrainian organizations in January 2022. TAG first observed FROZENVISTA in early 2021 when the group sent COVID-19 phishing emails to pharmaceutical companies and government organizations globally.

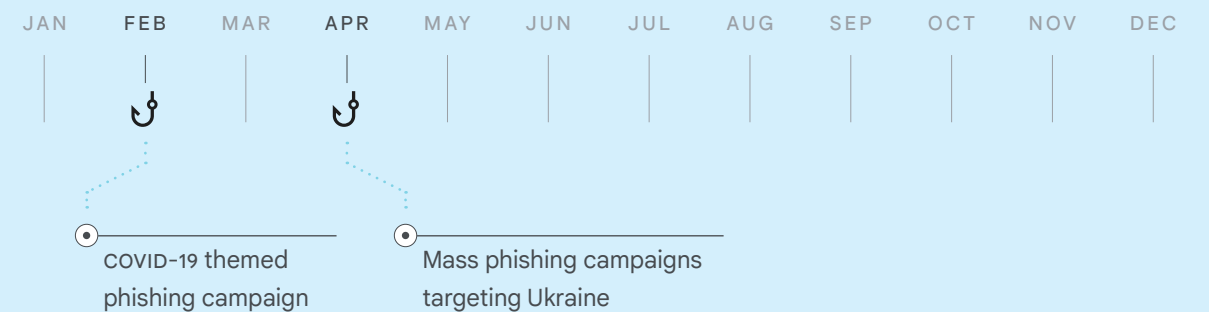
A new, probable GRU actor on the scene

Before the Russian invasion, FROZENVISTA conducted extensive espionage activity in Ukraine, particularly in spring 2021 and early 2022. Beginning on April 6, 2021, just weeks after Russia began massing troops and military equipment on the Ukrainian border, FROZENVISTA sent phishing emails to at least 1,966 unique recipients in Ukraine. Over 80% of the targets were Ukrainian government and military. Among the targets were multiple critical infrastructure operators, including multiple municipal water suppliers and one of Ukraine's largest national oil and gas companies. On April 8, CERT-UA posted a warning about the campaign, reporting that Ukrainian government bodies were targeted en masse with NATO-themed phishing emails that contained links to files with embedded malware.

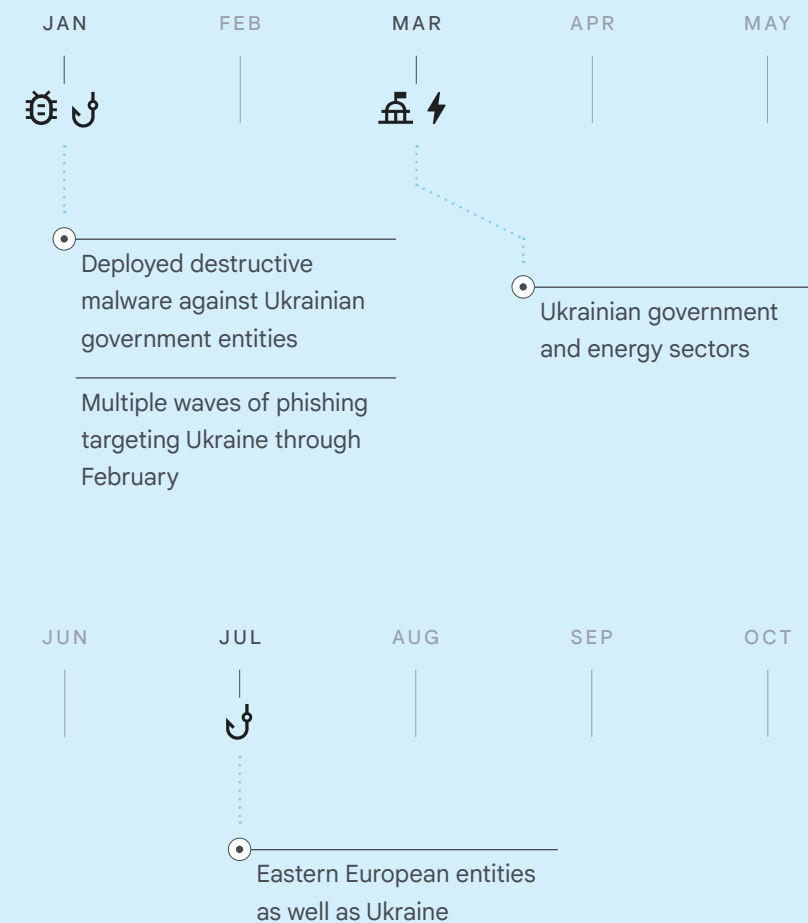
From January 5 to February 2, 2022, just weeks before Russia's invasion, FROZENVISTA conducted another major phishing campaign in several waves. Though smaller in scale, the January 2022 campaign targeted many — but not all — of the same organizations as the April 2021 mass phishing waves. Of the 396 targets TAG observed, one-third were government and military email addresses, and over a quarter were gmail.com addresses. The targets once again included critical infrastructure operators including underground gas storage facilities, electrical networks, and municipal health services, as well as other strategic targets such as agriculture and internet service providers.

FROZENVISTA also conducted destructive cyberattacks in January 2022. Mandiant assesses that this group, tracked as UNC2589, deployed the PAYWIPE (also known as WHISPERGATE) and SHADYLOOK wipers against Ukrainian government entities in what may have been a preliminary strike. Additional operations in January and February 2022 targeting Ukrainian critical infrastructure were also likely preliminary strikes contributing to the war effort.

2021 TARGETING ACTIVITY



2022 TARGETING ACTIVITY





PUSHCHA

Aliases

UNC1151

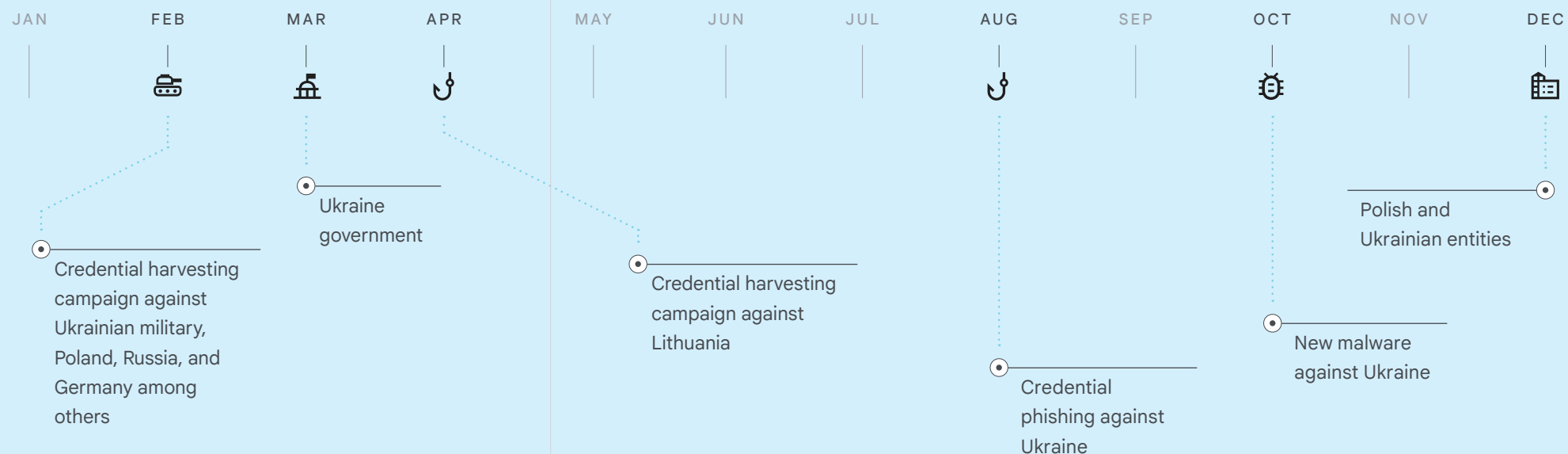
Attribution

Belarus

Overview

Active since at least 2016, PUSHCHA is a cyberespionage group that has targeted a variety of categories including journalists, media, and politicians, with a focus in Ukraine, Lithuania, Latvia, Poland, and Germany. The group has also [been linked to an influence campaign—known as “Ghostwriter”—that promotes Russian interests.](#)

2022 TARGETING ACTIVITY



Drove the 2022 increase in targeting of NATO

PUSHCHA has maintained a high operational tempo throughout the conflict with credential phishing campaigns against political and defense-related targets, as well as NGOs and organizations assisting Ukrainian refugees. These campaigns have primarily targeted regional webmail providers, using [browser-in-the-browser](#) phishing on compromised websites.

As the conflict began, TAG observed PUSHCHA conducting [credential phishing campaigns](#) against Polish and Ukrainian government and military organizations. The campaign contained links leading to compromised websites where the first-stage phishing page was hosted. Clicking through redirected the target to an attacker-controlled site that collected credentials.

PUSHCHA leveraged newly published research to rapidly adopt the ‘browser-in-the-browser’ phishing technique into operations. The technique draws a login page that appears to be on the passport.i[.]ua domain, over top of the page hosted on the compromised site. Credentials entered in the dialog are posted to an attacker-controlled domain.

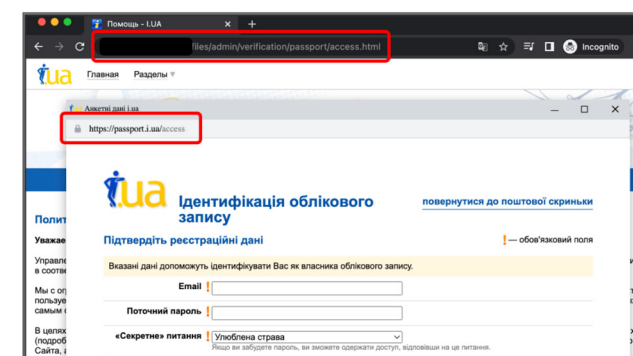


Figure 6

Browser-in-the-browser being used in PUSHCHA credential phishing campaigns. Landing pages for credential phishing hosted on compromised sites.

While PUSHCHA expanded its traditional targeting to high risk individuals in Ukraine, the group maintained a high operational tempo against eastern European users, especially in Poland. PUSHCHA compromised legitimate Polish websites and used them for phishing, often with redirect chains pointing to a handful of previously compromised websites. PUSHCHA seems to compromise websites indiscriminately, including websites associated with different financial, industrial, and commercial organizations.

Phishing campaigns targeting NATO countries have increased over 300% compared to 2020, with much of that increase coming from PUSHCHA, a Belarusian government-backed attacker closely aligned with Russia.



SUMMIT

Aliases

Turla Team
Snake
Uroburos
VENOMOUS BEAR
UNC4210

Attribution

Russian Federal Security Service (FSB)

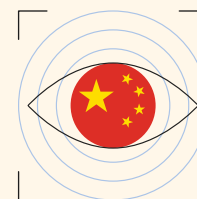
Overview

Active since at least 2006, primarily targeting military, defense and government related entities, but has also targeted media organizations, health-care, and NGOs, amongst others. The majority of these targets are located in Europe, the Middle East, Central Asia, and the US. In one of their most prominent campaigns in 2008, they targeted the US military with a large-scale campaign using spyware known as Agent.BTZ. The group is highly sophisticated, and focuses on data theft.

One of the oldest threat actors keeps their NATO focus

SUMMIT continues to [direct campaigns against](#) defense and cybersecurity organizations in NATO countries. In early 2022, the group sent emails that contained a unique link to a DOCX file hosted on attacker-controlled infrastructure. Once opened, the DOCX file would attempt to download a unique PNG file from the same attacker-controlled domain.

In July 2022, the group [hosted Android apps](#) on a domain spoofing the Ukrainian [Azov Regiment](#). This is the first known instance of SUMMIT distributing Android-related malware. The app is distributed under the guise of performing Denial of Service (DoS) attacks against a set of Russian websites. However, the 'DoS' consists only of a single GET request to the target website, which we assess is likely not enough to be effective. The apps were not distributed through the Google Play Store, but hosted on a domain controlled by the group and disseminated via links on third-party messaging services. We believe there was no major impact on Android users and that the number of installs was miniscule.



The war shifts Chinese cyberespionage priorities

The war caused Chinese government-backed attackers to shift their focus towards Ukrainian and Western European targets to gather information on the conflict:

CURIOS GORGE (alias: UNC3742), a group [TAG attributes](#) to the People's Liberation Army Strategic Support Force (PLA SSF), shifted from long running campaigns against Russia and Mongolia to targeting Ukrainian government organizations at the national and regional levels. As the war continued, CURIOS GORGE [continued to target](#) government, military, logistics and manufacturing organizations in Ukraine, Russia and Central Asia. In May 2022 TAG identified additional compromises impacting multiple Russian defense contractors and manufacturers and a Russian logistics company. This targeting continued through December 2022.

BASIN (aliases: Temp.Hex, Mustang Panda) expanded their operational focus on APAC to include targeting Ukrainian and NATO governments. Through 2021 and early 2022, BASIN targeted European entities with lures related to the Ukrainian invasion and malicious attachments with file names such as '[Situation at the EU borders with Ukraine.zip](#)'. The targeting of European organizations continued through December, and represents a shift from BASIN's primary Southeast Asian targets.

2022 TARGETING ACTIVITY



Section 2

Information Operations

Moscow leverages full spectrum of information operations to shape public perception of war

We've seen significant changes in the information landscape as Moscow leverages the full spectrum of information operations — from overt state-backed media to covert platforms and accounts — to shape public perception of the war. These operations have three goals: (1) undermine the Ukrainian government; (2) fracture international support for Ukraine; and (3) maintain domestic support in Russia for the war. We've seen spikes of activity associated with key events in the conflict such as the buildup, invasion, and troop mobilization in Russia. At Google, we've worked aggressively across products, teams, and regions to counter these activities where they violate our policies and disrupt overt and covert information operations campaigns, but continue to encounter relentless attempts to circumvent our detection and enforcement.



Russian IO focused on domestic audiences

The covert Russian IO we've disrupted on Google product surfaces primarily focused on maintaining Russian domestic support for the war in Ukraine, with spikes of IO activity occurring during the initial buildup, invasion, and the troop mobilization in Russia.



IO actors using overt and covert methods

Covert messaging and disinformation surrounding Ukraine and the Russian invasion continues to be spread by groups mimicking authentic users and by self-described news entities that covertly tie back to Russian intelligence. Google has disrupted overt and covert IO campaigns on Google product surfaces, while Mandiant observed notable degrees of covert activity on various social media platforms such as Telegram.



Resurgence of hacktivism

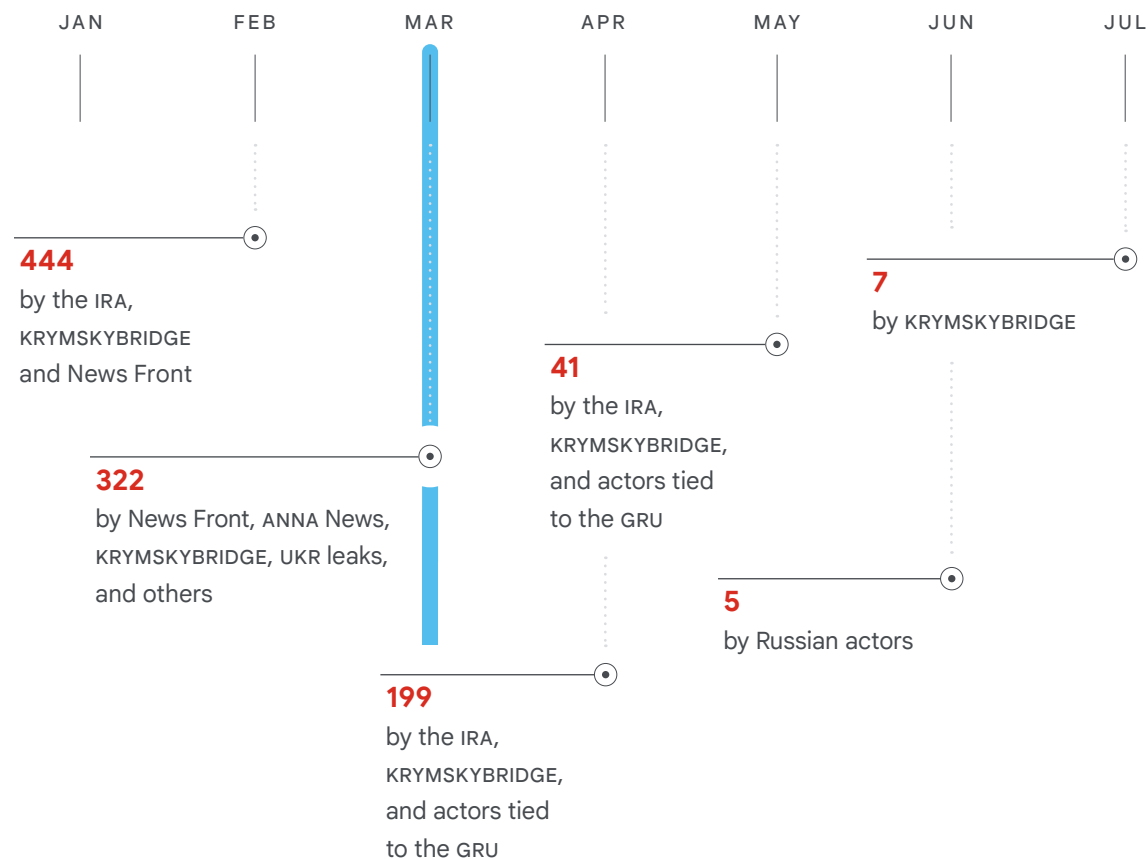
The range of actors involved in covert campaigns spans government-backed actors discussed earlier, dedicated IO actors, and ideologically-motivated hacktivists. The war has triggered an increase in declared hacktivist activity and a rise in the use of hacktivist tactics, bringing a renewed and sustained prominence to such activity.



Russian intelligence connection to hacktivists

Investigation of covert IO activity surrounding the war included the identification of "hacktivist" groups suspected to be tied to Russian intelligence services, raising the concern that these and others may be functioning as cutouts, a longstanding Russian IO tactic. Such activity is one component of a pattern of concurrent disruptive attacks, espionage, and information operations that we have observed — likely the first instance of all three being conducted simultaneously by state actors in a conventional war.

Google disrupted over 1,950 instances of Russian IO activity on our platforms in 2022



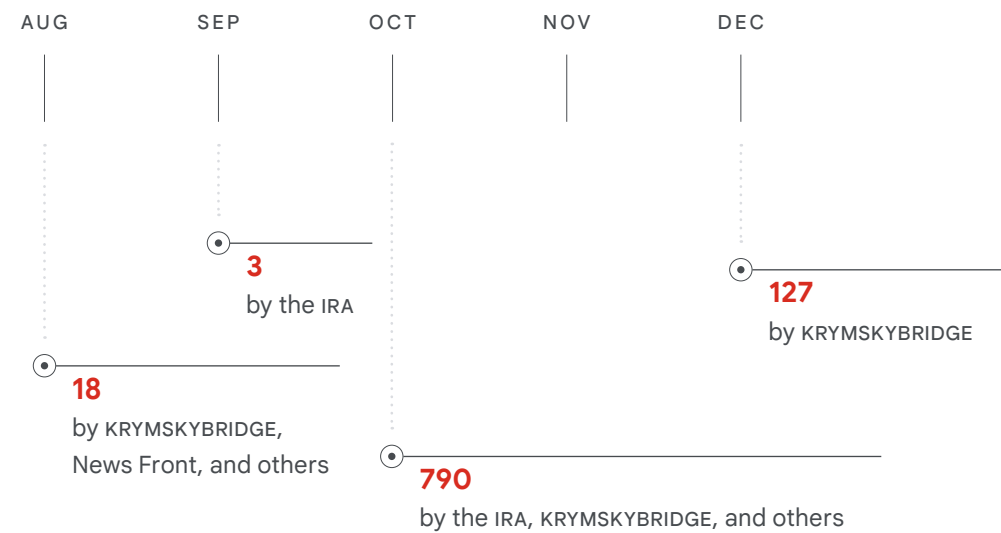
Protecting Information Quality

Google announced extraordinary measures to indefinitely pause monetization and globally block recommendations for Russian state media across our platforms

Responding to the information quality threat from Russian state media

The Google Trust & Safety team's response to the conflict in Ukraine is part of its larger mission to safeguard Google products against abuse and provide trusted and safe experiences for all users.

the conflict in Ukraine is a result of a planned 'Great Reset,' and that Russia is acting in self-defense against Ukraine to 'de-Nazify' the Ukrainian government and liberate the Donbass.



In addition to using covert IO in their attempt to manage the narrative about the war, Russia has used its overt state media apparatus and network of Kremlin-aligned publishers to target the same audiences with the same disinformation narratives.

Some of the key narrative themes Google Trust & Safety has observed include claims that the US is operating biolaboratories in Ukraine and around the world for the purposes of generating biological weapons, that Ukraine's military is using civilians as human shields during combat, that the rise in energy and food prices following

In response to this threat to information quality, Google announced [measures](#) in March to indefinitely pause monetization and globally block recommendations for Russian state media across our platforms. Trust & Safety has applied these measures to hundreds of sites, including the sites of outlets like RT and Sputnik.

Russian state media has reacted to the measures against them with tactics more commonly associated with their covert IO campaigns. Google Trust & Safety has observed repeated attempts by RT and other outlets to circumvent these actions by creating a large number of duplicate copies of their sites on new domains and has applied the same actions to these duplicates when detected.

Google

Commercial entities conducting covert IO on behalf of state clients

IRA and KRYMSKYBRIDGE account for an overwhelming majority of Google takedowns in 2022 due to their higher volume commenting campaigns on YouTube focused on maintaining support in Russia for the war.

Self-described news entities affiliated with Russian intelligence agencies

Over the last five years, TAG has tracked a series of self-described news entities that covertly tie back to Russian intelligence such as the Crimea-focused News Front, ANNA News, and UKR Leaks. As Google has taken them down, these entities have tried to circumvent Google policy enforcement by setting up mirror blog sites, having their journalists set up personal channels to re-upload videos, and creating new channels with different spellings and variations.

Narratives we saw from these actors included Russia saving Ukraine from Nazis, that the US and NATO were instigators of the conflict, and Russia was not afraid of or affected by sanctions.



Targets



Content languages on Google surfaces



Google enforcement in 2022

Instances of activity terminated on our platforms (e.g., YouTube channels, blogs, AdSense accounts)



Narratives



INTERNET RESEARCH AGENCY (IRA)

Troll farm involved in election interference during the 2016 US elections



KRYMSKYBRIDGE

Russian consulting firm that works with the Russian government



AFFILIATED WITH RUSSIAN INTELLIGENCE

Groups
VENTBRIDGE
News Front
ANNA News
UKR Leaks

Domestic Russian audience
Foreign audience

Domestic Russian audience

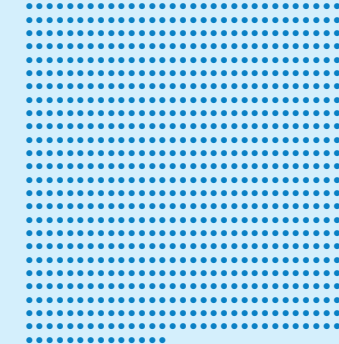
Domestic Russian audience
Foreign audience

Russian
French
Arabic
Chinese

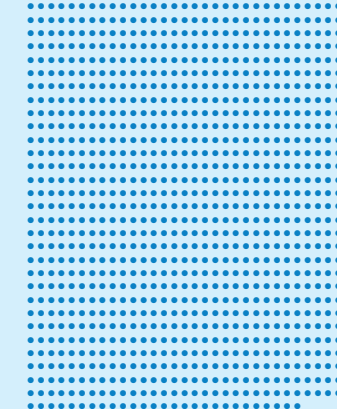
Russian

Russian
Ukrainian
Bulgarian
English
German

814



987



45



Pro-Russian

Russian President Vladimir Putin
Russia's 2014 invasion of Crimea
The Wagner Group's activity in Ukraine

Anti-Ukrainian

The West
Ukrainian politicians
Ukraine's handling of the COVID-19 pandemic

Pro-Russian

Russian military
Russia's actions in Ukraine
Russia's recognition of Ukrainian separatist regions

Anti-Ukrainian

Ukrainian President Volodymyr Zelensky
The US
NATO

Pro-Russian

Russia's actions in Ukraine
Separatist movements in the disputed regions of Ukraine

Anti-Ukrainian

Ukraine's government
Pro-Western Ukrainians
Ukrainian military

Disrupting Russian IO on Google product surfaces

TAG's research and rigorous analysis enables Google teams to make enforcement decisions and to disrupt coordinated IO campaigns. TAG, YouTube, and Google Trust & Safety track and regularly disable accounts associated with coordinated IO posting content and commenting. Examples of this enforcement include disruption of YouTube channels, blogs, AdSense accounts, and domains removed from Google News surfaces, as we report on a quarterly basis in the [TAG Bulletin](#).

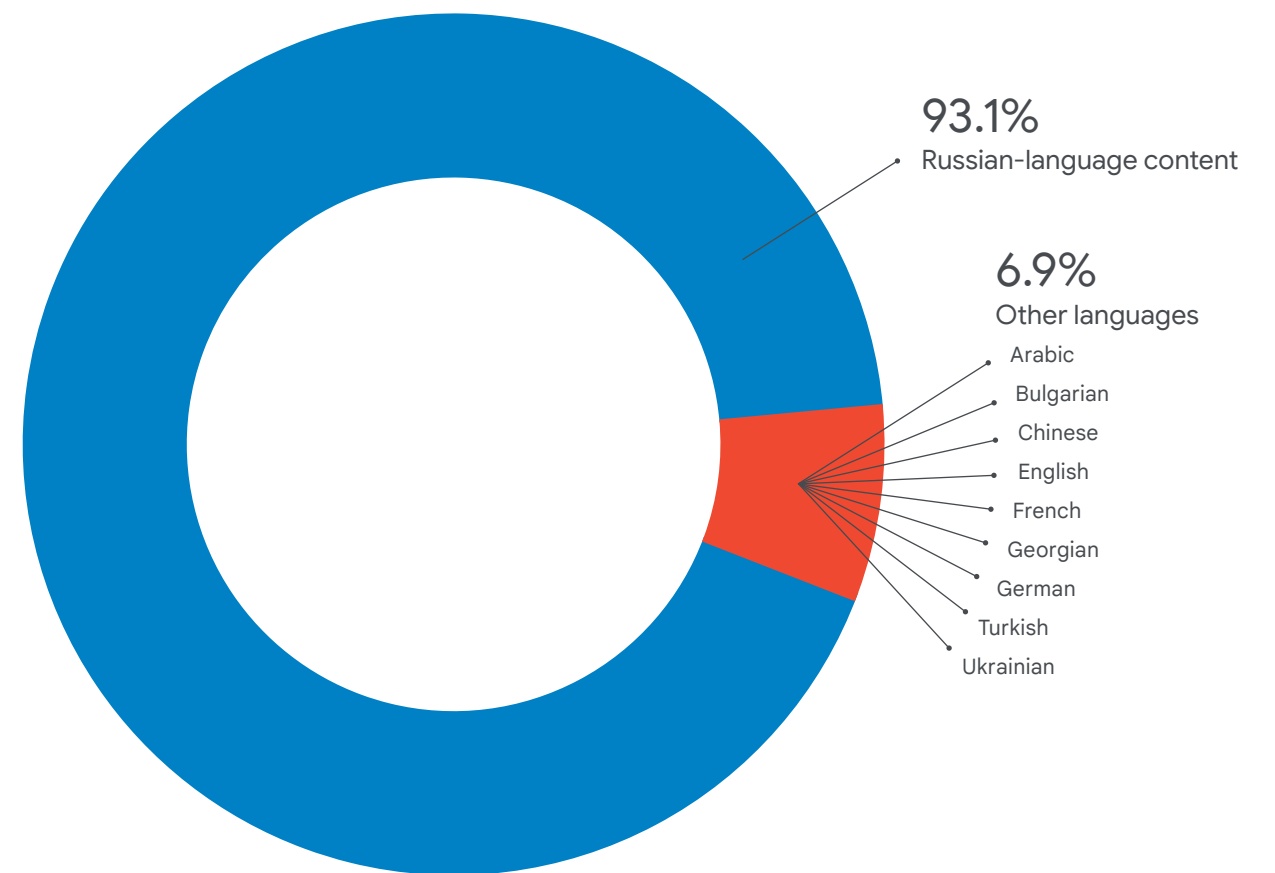
While Russian IO campaigns have three primary focuses, the Russian covert IO we've disrupted on Google product surfaces primarily focuses on maintaining Russian domestic support for the war in Ukraine. The audience appears to be Russian speaking individuals, as content from over 90% of the 1,956 instances we disabled for Russian-attributed IO activity were in Russian.



These coordinated IO campaigns either try to impersonate legitimate user engagement or act as self-described news entities. In the first case, the Internet Research Agency (IRA) and a Russian consulting firm we track as KRYMSKYBRIDGE created content on Google products such as YouTube, including commenting and upvoting each other's videos. In the second case, self-described news entities affiliated with Russian intelligence services such as ANNA News, News Front, and UKR Leaks, published and promoted content.

Since the invasion the groups tracked by TAG have become moderately more active. However, the focus of the narratives of the IO campaigns shifted. Instead of the previous focus on Russian domestic issues, the focus has shifted prominently to topics associated with Ukraine, either denigrating the Ukrainian government, or praising Russian soldiers and actions in Ukraine.

Figure 7
CONTENT LANGUAGE — RUSSIAN IO IN 2022





INTERNET RESEARCH AGENCY (IRA) AND AFFILIATES

Attribution

The group is financed by Russian oligarch Yevgeny Prigozhin

Overview

Focused on both domestic Russian and foreign audiences, the IRA is best known for its involvement in election interference during the 2016 us elections. The group has focused on narratives supportive of Russia and Prigozhin's Wagner Group, and critical of Ukraine and the West, as well as local politicians. Its cross-border campaigns leverage local media brands, NGOs and PR firms created by Russian shell companies, and freelancers to distance themselves from their content. Domestically focused campaigns primarily leverage YouTube and Blogger.

Shoring up support in Russia for the war, praising Wagner Group

Best known for their information operations that sought to sway public opinion during the 2016 us presidential election, the IRA has evolved significantly. Since the invasion of Ukraine, we have seen the domestically focused cluster of IRA-related activity shift from a range of domestic Russian political issues to focus almost exclusively on Ukraine and mobilization. Several campaigns also promoted the business interests of Russian oligarch Yevgeny Prigozhin, the financier of the IRA, and a propaganda film related to Ukraine.

Russian domestic focused IO

Google regularly disrupts activity by IRA-linked accounts targeting Russian domestic audiences. These are often clusters of related accounts that create YouTube channels, upload videos, and comment and upvote each other's videos. The activity occurs during Russian work hours, with narratives focused on Russian domestic issues and typically targeting political dissidents. Increasingly, Google disrupts Russian IO accounts before they gain traction. More recently TAG has seen IRA-linked actors create YouTube Shorts.

The Shorts are crafted for a Russian domestic audience, praising Russian soldiers in Ukraine and seeking to lift their morale. The vast majority of this content has garnered no views on YouTube.

TAG also observed IRA-linked accounts publish coordinated narratives on Blogger and then mirror the same content on Ukrainian blogging platform, Hashtap. In some cases, multiple

Shortly after Russia's invasion of Ukraine, TAG identified [several IRA-affiliated news sites](#) like newinform[.]com and slovodel[.]com hosting ads to drive traffic to the videos. The campaign's timing was notable because the subject matter mirrored newly topical real world events in Ukraine in a way that portrayed Russia positively. Google terminated nine new IRA-linked accounts using



Figure 10

IRA placing an ad on IRA-controlled news sites to drive traffic to the videos

profiles published very similar or near-identical content. Narratives in the blogs focused on Russian domestic affairs and stories smearing anti-corruption activist Alexei Navalny and other opposition politicians.

Amplifying Prigozhin propaganda film on Ukraine

Prigozhin has funded several movies through a partial ownership stake in the film company, Aurum LLC. These movies have high production value and communicate narratives portraying Russia — especially Russian military and mercenaries — in a positive light.

In 2021, they released “Солнцепёк” (“Sunlight” or “Blazing Sun” in English), which takes place in eastern Ukraine and claims to be a story based on true events from 2014 of Russian mercenaries, connected to the paramilitary Wagner Group, protecting Russians in Ukraine against Ukrainian forces.

Ads to advertise the film and 44 new IRA-linked YouTube channels hosting clips, the full-length film and related comments. Some accounts claimed to be officially affiliated with the film, while others presented themselves as fan accounts.

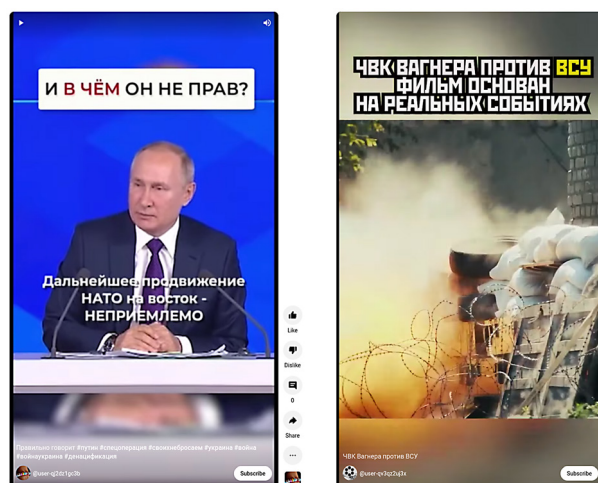
This campaign highlights the dual purpose of a number of IRA-linked efforts: they promote both Russia's interests and Prigozhin's business interests, which are tightly intertwined. In effect, Prigozhin is using IO to promote his mercenary group, which itself is a vehicle for driving Russia's foreign policy agenda in Ukraine and elsewhere.

Figure 8 (left)

Russian video title reads, “Correctly says #Putin #special operation #we don't leave our own #Ukraine #war#warUkraine #denazification”

Figure 9 (right)

The video title reads, “PMC Wagner against the Armed Forces of Ukraine” in Russian





KRYMSKYBRIDGE

Attribution

A Russian consulting firm that has the Russian government as a client

Overview

Focused on domestic audiences, uses comment brigading to support narratives supportive to Russia and local Russian politics. Since March 2022, the comments have shifted to include narratives critical of Ukraine.



Russian-language comment brigading

KRYMSKYBRIDGE accounted for the most takedowns as part of Google's efforts to disrupt Russian IO in 2022. Their usual modus operandi is bulk commenting on YouTube videos, usually on Russian domestic politics. They mainly target the Russian domestic audience, and possibly the Russian diaspora as their comments are always in Russian. Before the invasion of Ukraine, they rarely strayed from their focus on Russian domestic issues. Since early March 2022, however, they have shifted entirely to narratives related to Ukraine.

Disruptive and destructive attacks combined with IO

Hacktivists or Faketivists? Resurgent "hacktivists" conduct DDoS and leaks

The war has triggered a rise of hacktivism and the use of hacktivist tactics, bringing a renewed and sustained prominence to such activity. Notably, this includes multiple groups suspected to be tied to Russian intelligence services, raising the concern that these and others may be functioning as cutouts, a known Russian IO tactic.

While most of the activity from these "hacktivist" actors was in the form of DDoS attacks, they also engaged in data leaks, including sharing the personally identifiable information (PII) of Ukrainian military, government employees, and anyone who opposed the invasion of Ukraine, as well as data from numerous Ukrainian organizations that Russian government-backed attackers compromised and wiped.

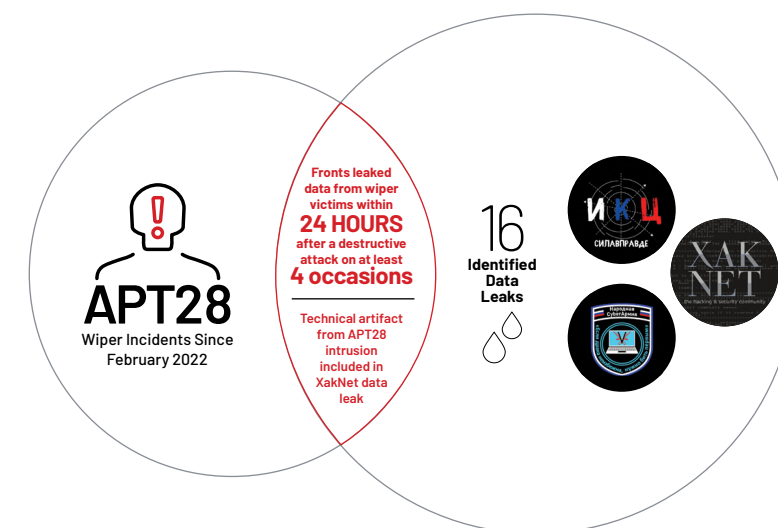
Mandiant assesses with moderate confidence that threat actors operating the Telegram channels XakNet Team, Infocentr, and CyberArmyofRussia_Reborn are coordinating their operations with GRU-sponsored FROZENLAKE / APT28.

Mandiant identified evidence connecting the moderators of these groups to the Russian state, including timeline analysis of intrusions and leaks from Ukrainian organizations.

Mandiant has also identified limited links between XakNet Team and the pro-Russia so-called "hacktivist" group KillNet, and we assess with moderate confidence that XakNet and KillNet have directly coordinated some of their activity. However, we note that the two groups appear to conduct aligned (but separate) missions based on the observed activity claimed by each of the "hacktivist" groups. Public disputes between the two groups suggest the groups actually may be separate entities.

Formed shortly before the onset of the Russia-Ukraine war in late February 2022, KillNet is a self-proclaimed pro-Russia hacktivist collective that has claimed DDoS attacks and other compromises primarily against several European countries, NATO members, and more recently, the US. Although aligned with Russian government priorities, Mandiant has not yet uncovered direct evidence linking KillNet to Russian intelligence.

Suspected False Hacktivist Fronts Leaked Data Likely Stolen from APT28 Wiper Victims



MANDIANT

Destructive malware attacks crossover with IO

During the war we have observed a pattern of concurrent disruptive attacks, espionage, and IO — likely the first instance of all three being conducted simultaneously by state actors in a conventional war.

In a prominent example in March 2022, Mandiant observed wiper activity coinciding with an active IO campaign at the media outlet Ukraine 24 (Ukrainian: Україна 24). On March 16, an information operation targeting Ukraine promoted a fabricated message alleging Ukraine’s surrender to Russia via the suspected compromise and defacement of the Ukraine 24 website and news ticker in a Ukraine 24 TV broadcast with a written message. The message was also delivered through an artificial intelligence (AI)-generated “deepfake” video impersonating

Ukrainian President Zelensky delivering that same text. On the same day, Mandiant identified a wiper targeting a Ukrainian organization. The malware was configured via a scheduled task to execute approximately three hours before Zelensky was scheduled to deliver a speech to the US Congress.

In May 2022, Mandiant observed a Ukrainian local government organization, which was the target of a destructive wiper attack. In addition to the wiper attacks, the organization also suffered a data leak event during which documents from its network were released onto Telegram.

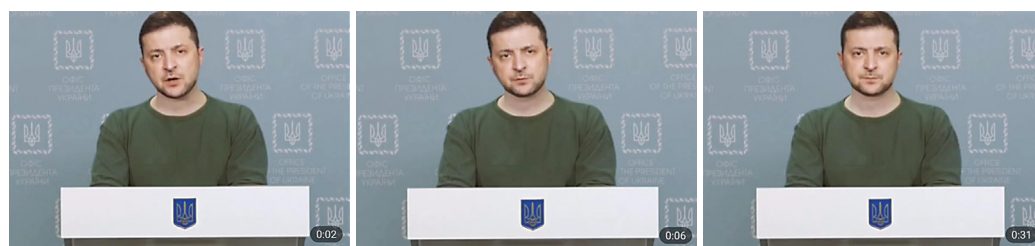


Figure 11
Screenshots from an artificial intelligence (AI)-generated “deepfake” video of Zelensky, stating that Ukraine would surrender to Russia


Section 3


Cybercrime




War has split the loyalties of financially motivated attackers

Lines are blurring between financially motivated and government-backed attackers in Eastern Europe, with threat actors changing their targeting to align with regional geopolitical interests, and government-backed attackers adopting some tactics and services associated with financially motivated actors.

- 

Cybercrime splits along political lines
The cybercriminal ecosystem has been disrupted with some groups declaring political allegiances, others splitting on geopolitical lines, and prominent operators shutting down. The taboo against attacking Russia has softened.
- 

Rapid evolution of TTPs
Ransomware actors increasingly specialize in one part of the attack chain and rapidly adopt novel TTPs. In some cases, the targets and tactics of financially motivated actors look more like those of government-backed attackers.
- 

Projections of ransomware retaliation largely unrealized
We did not see an uptick in reported ransomware attacks against critical infrastructure in the US and NATO countries in 2022, as might have been expected after declarations early in the conflict and the prior wave of such attacks in 2021.

... the ransomware ecosystem is not immune from geopolitical developments

Shifts in the ransomware ecosystem

Ransomware remains a profitable and competitive underground market. Monetizing access to companies or networks is not a new concept, and initial access brokers existed long before the uptick of targeted ransomware. In recent years, the ecosystem has moved towards specialization, with each participant in the chain focusing on one aspect and interacting with others as business partners.

We now see faster experimentation with techniques such as new delivery channels and unconventional file formats to increase the success rate of ransomware campaigns. Increasingly, financially motivated actors borrow successful techniques from other campaigns. Examples include the malware Zloader and IcedID leveraging malvertising;

Qakbot and Emotet crafting malicious documents using the same document builder service; and Bumblebee and BazarLoader embedding their payload in ISO files sharing metadata and file structure. These overlaps complicate and slow definitive attribution.

Ransomware continues to be lucrative, but financially motivated threat actors are not immune from geopolitical developments.

While ransomware groups continue to be disruptive, the ecosystem itself has been disrupted with some groups declaring political allegiances and prominent operators shutting down.

For example, the stealer malware Raccoon suspended activity after its suspected developer fled the Russian invasion of Ukraine, and is waiting to be extradited to the US for legal prosecution after his arrest in the Netherlands. At the time of the invasion, the prominent Conti ransomware group splintered along political and geographical lines. Conti [declared its support of Russia](#), and [threatened](#) to strike the critical infrastructure of nations that took action against Russia. Rather than an increase in attacks on critical infrastructure, the announcement led to internal divisions within Conti, [leaks](#) of the group's internal communications and [source code](#), and the eventual [shut down](#) of the group.

In a shift, there has been an increase in reported ransomware attacks in Russia. Before February 2022, ransomware creators [used techniques to avoid targeting the Commonwealth of Independent States](#), including hard-coding country names and checking the system language. After the invasion, hacktivist group NB65 used [leaked Conti source code to target Russian organizations](#). NB65 claims links to the Anonymous hacktivist collective, which conducted an ["#OpRussia" campaign](#), including several hack-and-leak operations against Russian organizations such as [the Russian Central Bank](#). In addition, a loose group of international and Ukrainian volunteers dubbed the [Ukrainian IT Army](#) have been collaborating with Ukraine's defense ministry [to defend Ukraine](#) and [to target Russian infrastructure and websites](#).



We did not see an uptick in reported ransomware attacks against critical infrastructure in the US and NATO countries in response to the conflict in Ukraine, as might have been expected after the declarations of allegiances and of hacktivism early in the conflict. Developments over the last two years may have made critical infrastructure in the West, especially in the US, a less favorable target. One hypothesis is the US response after the 2021 Colonial Pipeline attack and subsequent [arrest in Russia](#) of members of the [REvil ransomware gang](#) deterred financially motivated ransomware affiliates in 2022.

A second hypothesis is that increased sanctions against Russia in the wake of the war have impacted the [willingness of Western organizations](#) to pay ransoms, which by [one estimate](#) has led to a 40% drop in profits for ransomware groups. Financially motivated threat actors will likely attempt to modify their tooling or tactics to distance themselves from sanctions imposed on Russia, [as they did](#) after the 2019 [sanctions](#) on Evil Corp.

Overlap between financially motivated and government-backed threat actors

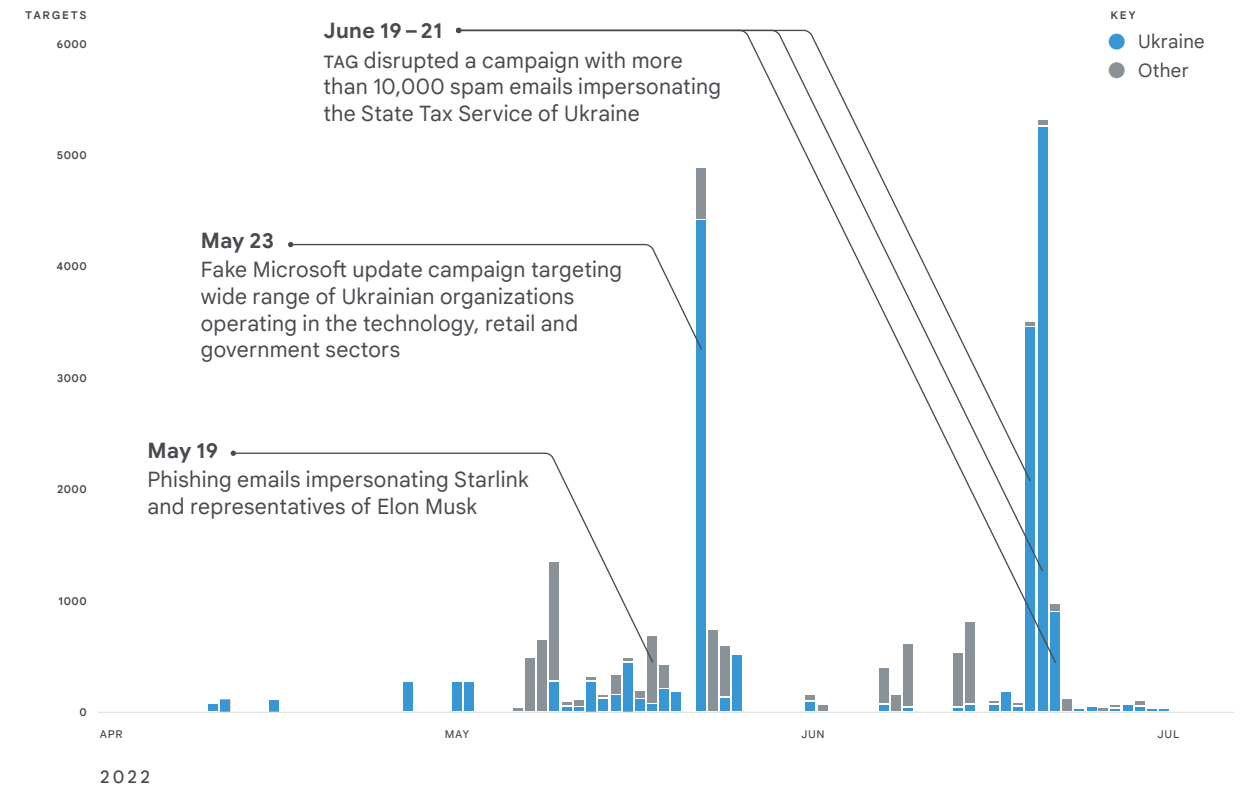


TAG also sees tactics closely associated with financially motivated threat actors being deployed in campaigns with targets typically associated with government-backed attackers. In September 2022, TAG reported on [a threat actor](#) whose activities overlap with CERT-UA's [UAC-0098](#). UAC-0098 is a threat actor that historically delivered the IcedID banking trojan, leading to human-operated ransomware attacks. We assess some members of UAC-0098 are former Conti members repurposing their techniques to target Ukraine.

In early 2022, the attackers shifted their focus to targeting Ukrainian organizations, the Ukrainian government, and European humanitarian and non-profit organizations. The group's targeting wildly varied from European NGOs to less targeted attacks on Ukrainian government entities, organizations and individuals. Rather uniquely, the group demonstrates strong interest in breaching businesses operating in the hospitality industry of Ukraine, going as far as launching multiple distinct campaigns against the same hotel chains.

This overlap of activity is likely to continue throughout the conflict. As recently as December 2022, the Ukrainian CERT reported that a tool used by [the Cuba ransomware access brokers](#), dubbed [ROMCOM, was used to target users](#) of the DELTA military system used by Ukraine's military.

Figure 12
UAC-0098 PHISHING CAMPAIGNS TARGETING UKRAINE



Former Conti cyber crime gang members targeted Ukrainian public and private organizations and European humanitarian and non-profit organizations.

Conclusion

In this report, we outlined Russia's multi-pronged effort to gain a decisive wartime advantage in cyberspace and use information operations to help shape public perception of the war.

We also discussed the war's impact on criminal groups and the scale of cybercrime worldwide. Based on these observations, we point to several broader, forward looking assessments for the security community for 2023:



We assess with high confidence that Russian government-backed attackers will continue to conduct cyber attacks against Ukraine and NATO partners to further Russian strategic objectives.



We assess with high confidence that Moscow will increase disruptive and destructive attacks in response to developments on the battlefield that fundamentally shift the balance — real or perceived — towards Ukraine (e.g., troop losses, new foreign commitments to provide political or military support, etc.). These attacks will primarily target Ukraine but increasingly expand to include NATO partners.



We assess with moderate confidence that Russia will continue to increase the pace and scope of information operations to achieve the objectives described above, particularly as we approach key moments like international funding, military aid, domestic referendums, and more. What's less clear is whether these activities will achieve the desired impact, or simply harden opposition against Russian aggression over time.

At Google, we'll continue to work around the clock to protect the safety and security of online users and our platforms. We'll also continue to support organizations before, during, and after security events. In addition, we'll continue to track other threat actors worldwide to ensure they don't take advantage of the security community's focus on the war.

This report includes extensive research from dozens of sources and comes in print and digital versions. The digital version contains links to relevant sources.

