Fog of war: how the Ukraine conflict transformed the cyber threat landscape

blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

Shane Huntley February 16, 2023

One year after the Russian invasion of Ukraine Google TAG, with additional research from Mandiant and Trust & Safety, provide insights into changes in the cyber threat landscape triggered by the war.

Nearly one year ago, Russia invaded Ukraine, and we continue to see cyber operations play a prominent role in the war. To provide more insights into the role of cyber, today, we are releasing our report Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape based on analysis from Google's Threat Analysis Group (TAG), Mandiant and Trust & Safety. The report encompasses new findings, and retrospective insights, across government-backed attackers, information operations (IO) and cybercriminal ecosystem threat actors. It also includes threat actor deep dives focused on specific campaigns from 2022.

Coming together to support Ukraine

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

government; rapid Air Raid Alerts system for Android phones in the region; support for refugees, businesses, and entrepreneurs; and measures to indefinitely pause monetization and limit the reach of Russian state news media.

One of the most pressing challenges, however, is that the Ukrainian government is under near-constant digital attack. Shortly after the invasion, 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 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 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. We wanted to share what we have learned with the global security community to help prepare better defenses for the future.

Key findings

1. 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.

 chart showing phishing activity by state sponsored actors
Russian government-backed attackers ramped up cyber operations beginning in 2021 during the run up to the invasion. 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.

 charts showing the top phishing target domains

In 2022, Russian government-backed attackers targeted users in Ukraine more than any other country. While we see these attackers focus heavily on Ukrainian government and military entities, the campaigns we disrupted also show a strong focus on critical infrastructure, utilities and public services, and the media and information space.

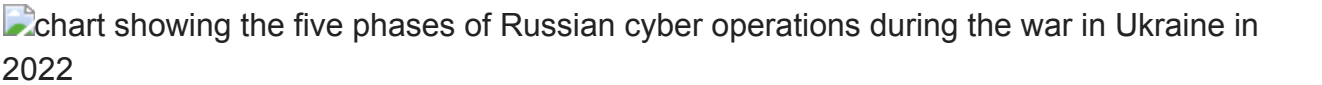
chart showing the five phases of Russian cyber operations during the war in Ukraine in 2022

From its incident response work, Mandiant observed more destructive cyber attacks 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 they saw significant activity after that period, the pace of attacks slowed and appeared less coordinated than the initial wave in February 2022. Specifically, destructive attacks often occurred more quickly after the attacker gained or regained access, often through compromised edge infrastructure. Many operations indicated an attempt by the Russian Armed Forces' Main Directorate of the General Staff (GRU) to balance competing priorities of access, collection, and disruption throughout each phase of activity.

2. Moscow has leveraged the full spectrum of IO – 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
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 IO campaigns, but continue to encounter relentless attempts to circumvent our policies.

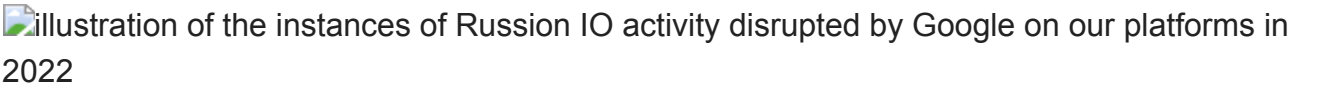
illustration of the instances of Russion IO activity disrupted by Google on our platforms in 2022

The covert Russian IO we've disrupted on Google product surfaces primarily focused on maintaining Russian domestic support for the war in Ukraine, with over 90% of the instances in the Russian language.

3. 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 have split over political allegiances and geopolitics, while others have lost prominent operators, which 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. 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.

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, 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.


chart showing UAC-0098 phishing campaigns targeting Ukraine

Looking ahead

- 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 IO 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 continue to play an integral role in future armed conflict, supplementing traditional forms of warfare, and hope this report serves as a call to action as we prepare for what lies ahead. 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.

Click here for the full report, and security practitioners interested in the webinar can sign up here.

POSTED IN:

Threat Analysis Group