Ukraine remains Russia’s biggest cyber focus in 2023

blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023

Billy Leonard

April 19, 2023

Threat Analysis Group

Google’s Threat Analysis Group (TAG) continues to disrupt campaigns from multiple sets of Russian government-backed attackers focused on the war in Ukraine. This blog provides insights on attacker trends from primarily January - March 2023, continuing our analysis from Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape.

In the first quarter of 2023, Russian government-backed phishing campaigns targeted users in Ukraine the most, with the country accounting for over 60% of observed Russian targeting. Looking at information operations (IO), our takedowns reflect a steady pattern of Russian attempts to circumvent our policies, details of which are reported in our quarterly TAG Bulletin.

Here is a deeper look at notable campaigns TAG has observed since our last update:

FROZENBARENTS targets energy sector, continues hack and leak operations

FROZENBARENTS (aka Sandworm), a group attributed to Russian Armed Forces’ Main Directorate of the General Staff (GRU) Unit 74455, continues to focus heavily on the war in Ukraine with campaigns spanning intelligence collection, IO, and leaking hacked data through Telegram.

As we described in the Fog of War report, FROZENBARENTS remains the most versatile GRU cyber actor with offensive capabilities including credential phishing, mobile activity, malware, external exploitation of services, and beyond. They target sectors of interest for Russian intelligence collection including government, defense, energy, transportation/logistics, education and humanitarian organizations.

FROZENBARENTS continues to exploit EXIM mail servers globally and use these compromised hosts as part of their operational network, a trend going back to at least August 2019. These compromised hosts have been observed accessing victim networks, interacting with victim accounts, sending malicious emails and engaged in information operations (IO) activity.

Energy sector targeting

The Caspian Pipeline Consortium (CPC) controls one of the world's largest oil pipelines that transports oil from Kazakhstan to the Black Sea. Since November 2022, FROZENBARENTS has engaged in a sustained effort to target organizations associated with the CPC and other energy sector organizations in Europe. The first campaign targeted CPC employees, specifically the Moscow office, with phishing links delivered via SMS.

image of a phishing site spoofing CPC, an energy sector organization
Phishing site spoofing CPC, an energy sector organization

Throughout Q1 2023, FROZENBARENTS conducted multiple campaigns against energy sector organizations in Eastern Europe, delivering links to fake Windows update packages hosted on a domain spoofing CPC. If executed, the fake update would run a variant of the Rhadamanthys stealer to exfiltrate stored credentials, including browser cookies.

Defense targeting

Beginning in early December 2022, FROZENBARENTS launched multiple waves of credential phishing campaigns targeting the Ukrainian defense industry, military and Ukr.net webmail users. These phishing emails spoofed security and other system administrator type notifications and in some cases were sent through third-party email campaign management services.

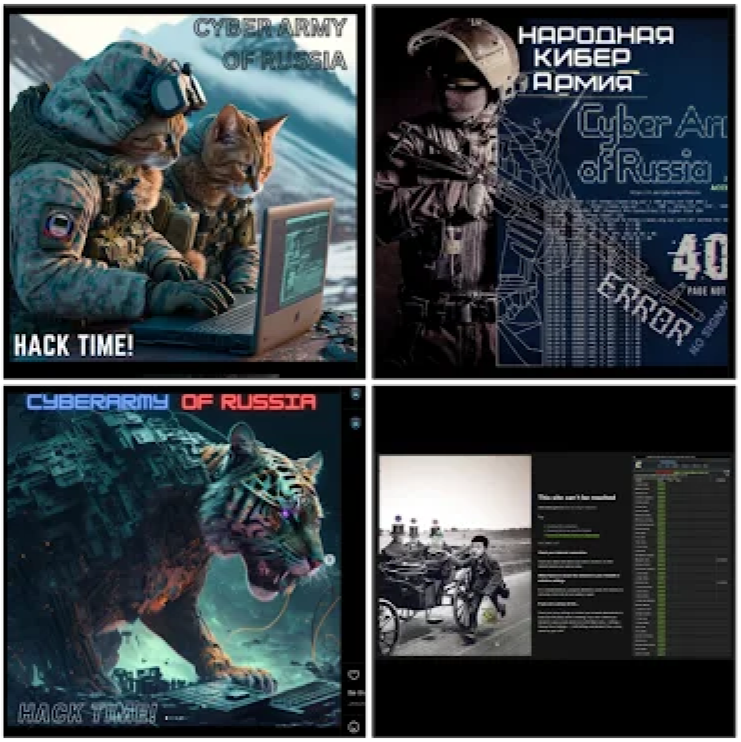
image of a phishing site spoofing Ukroboronprom, a Ukrainian defense company
Phishing site spoofing Ukroboronprom, a Ukrainian defense company

IO, hack and leak campaigns

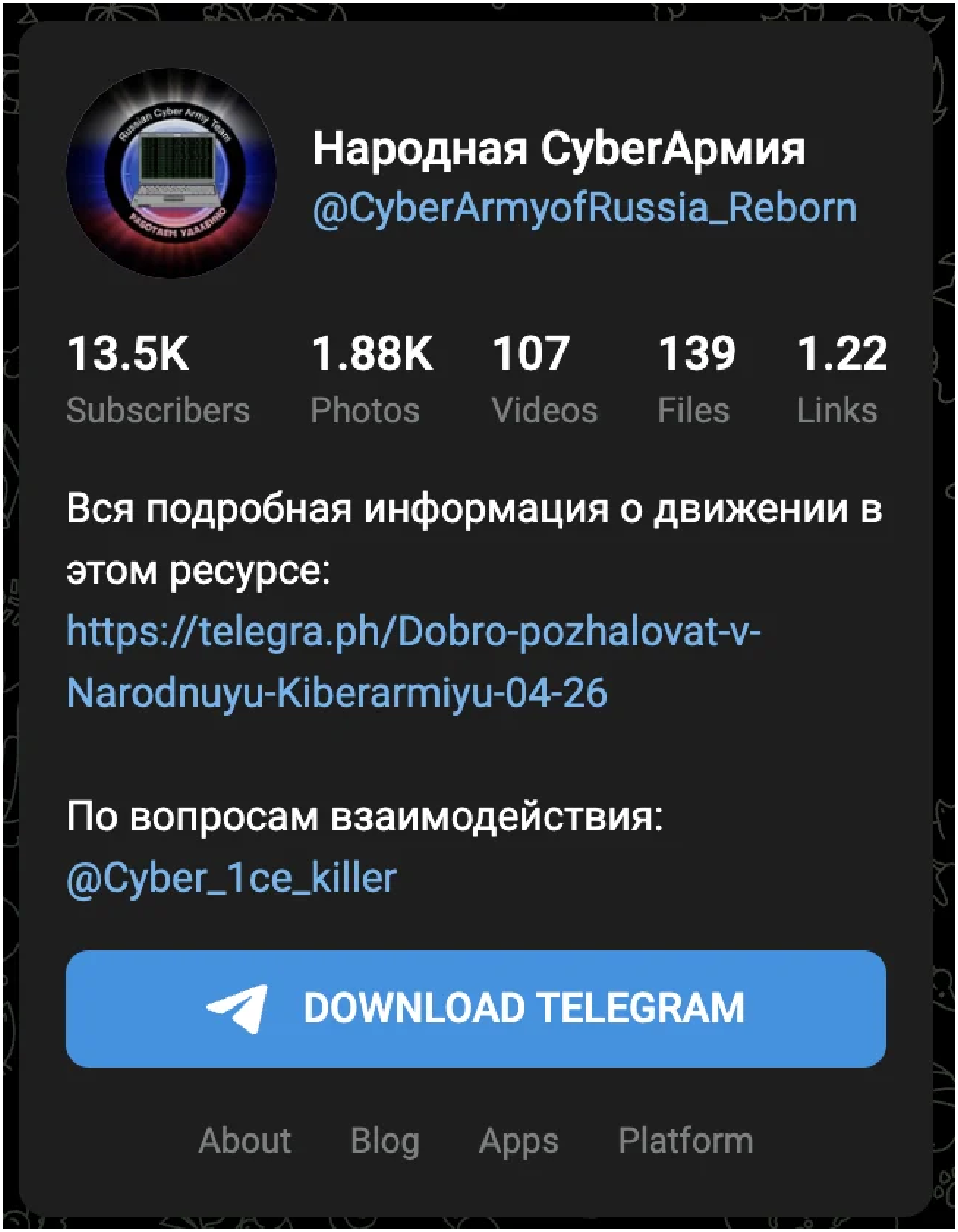
Active in the IO space, FROZENBARENTS actors create online personas to create and disseminate news content as well as leak stolen data. These actors promote narratives that are pro-Russia, and against Ukraine, NATO and the West. One persona, which TAG assesses is created and controlled by FROZENBARENTS actors, is 'CyberArmyofRussia' or 'CyberArmyofRussia_Reborn', which has a presence on Telegram, Instagram and YouTube. Both the YouTube channel, terminated upon identification, and Instagram account received minimal engagement with a negligible number of subscribers or followers.

-

  CyberArmyofRussia YouTube channel

- 

Instagram posts from CARR

- 

  Народная CyberАрмия
  @CyberArmyofRussia_Reborn

  13.5K Subscribers 1.88K Photos 107 Videos 139 Files 1.22 Links

  Вся подробная информация о движении в этом ресурсе: https://telegra.ph/Dobro-pozhalovat-v-Narodnuyu-Kiberarmiyu-04-26

  По вопросам взаимодействия: @Cyber_1ce_killer

  CyberArmyofRussia_Reborn Telegram channel

The CyberArmyofRussia_Reborn Telegram channel has primarily been used for posting stolen data and DDoS targets. In several recent incidents, FROZENBARENTS compromised a webserver of the target organization and uploaded a webshell to maintain persistent access to the compromised system. The attackers then deployed Adminer, a single file PHP script for managing databases, to exfiltrate data of interest. Shortly after exfiltration, the data appeared on the CyberArmyofRussia_Reborn Telegram channel.

Telegram phishing

FROZENBARENTS has targeted users associated with popular channels on Telegram, a social media platform popular in both Ukraine and Russia. Phishing campaigns delivered via email and SMS spoofed Telegram to steal credentials, sometimes targeting users following pro-Russia channels.

image of phishing site spoofing Telegram
Phishing site spoofing Telegram

An interesting artifact of the Telegram phishing campaigns is a ‘val’ URL parameter in the phishing links with a base64 encoded value, providing insight into the operators’ mindset and their condescending attitude towards Ukraine and the Cyber Police of Ukraine.

snippet of Base64 encoded values found in phishing link URL parameter
Base64 encoded values found in phishing link URL parameter

GRU @bio_genie IO Campaign on Telegram, Substack

Since April 2022, actors attributed to the GRU have maintained a Telegram channel to promote and amplify narratives related to the use of biological weapons in Ukraine and how the United States is responsible for the proliferation of biological weapons around the world. The Telegram channel publishes Russian-language content, and is likely aimed at Russian speaking audiences. In December 2022, they also created a similarly named Substack, published in English. While the Telegram channel receives regular updates, sometimes multiple times per day, the Substack has only received a single post.

The actors controlling this channel have conducted email campaigns soliciting input from prominent Russian and Belarussian researchers and medical professionals involved in epidemiology and microbiology. Additionally, they have attempted to engage with journalists globally in an attempt to drive traffic to the Telegram channel and further amplify their narratives.

While this activity has been conducted from infrastructure similar to known FROZENBARENTS infrastructure, TAG is currently unable to confidently assess if this activity has been conducted by FROZENBARENTS, or if this campaign is being conducted by a different GRU unit.

image of @bio_genie Telegram channel
@bio_genie Telegram channel

image of @bio_genie substack
@bio_genie substack

FROZENLAKE uses XSS in phishing against Ukranian users

In early 2023, another Russian GRU actor TAG tracks as FROZENLAKE (aka APT28) was especially focused on Ukraine. In February and March, they sent multiple large waves of phishing emails to hundreds of users in Ukraine, continuing the group's 2022 focus on targeting webmail users in Eastern Europe.

Starting in early February 2023 we saw FROZENLAKE using reflected cross-site scripting (XSS) on multiple Ukrainian government websites to redirect users to phishing pages - a new TTP for the group. Recent examples of these reflected XSS are included below.

image of code
image of code
Recent examples of reflected XSS

image of ukr.net phishing page
ukr.net phishing page

The majority of observed phishing domains were created on free services and used for a short time, often a single campaign. When a user submitted their credentials on the phishing sites, they were sent via HTTP POST request to a remote IP address, which TAG analysis identified as compromised Ubiquiti network devices.

PUSHCHA continues targeting regional webmail providers

PUSHCHA, a Belarusian threat actor, has consistently targeted users in Ukraine and neighboring countries throughout the war. Their campaigns typically target regional webmail providers such as i.ua, meta.ua and similar services. The phishing campaigns are targeted, focused on small numbers of users in Ukraine.

image of PUSHCHA i.ua phishing page
PUSHCHA i.ua phishing page

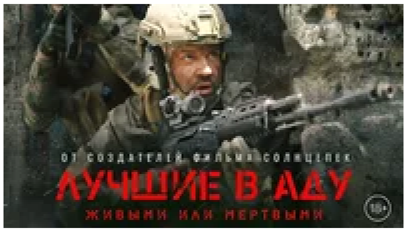
image of PUSHCHA meta.ua phishing page
PUSHCHA meta.ua phishing page

Russian Information Operations

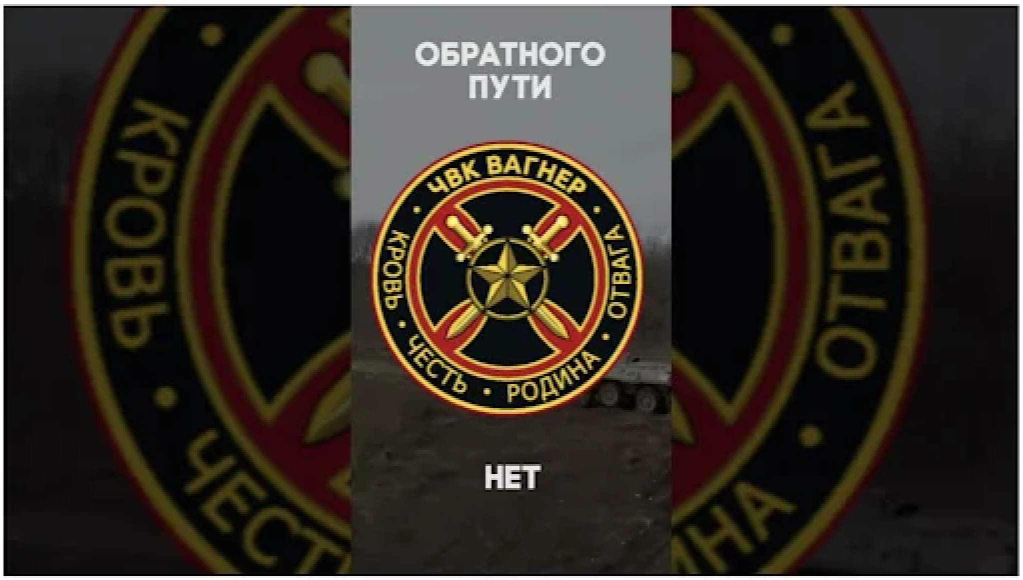
Moscow continues to leverage the full spectrum of information operations — from overt state-backed media to covert platforms and accounts — to shape public perception of the war in Ukraine. In the first quarter of 2023, TAG observed a coordinated IO campaign from actors affiliated with the Internet Research Agency (IRA) creating content on Google products such as YouTube, including commenting and upvoting each other's videos. The group has focused particularly on narratives supportive of Russia and the business interests of Russian oligarch Yevgeny Prigozhin, especially the Wagner Group.

As noted in the Fog of War report, TAG has continued to see IRA-linked actors create YouTube Shorts. The Shorts are crafted for a Russian domestic audience, and are often "news"-like narratives on the Ukraine war. The group was also promoting a new film by Aurum LLC, a film company partially owned by Prigozhin. This movie has a high production value and communicates narratives portraying the Wagner Group in a positive light.

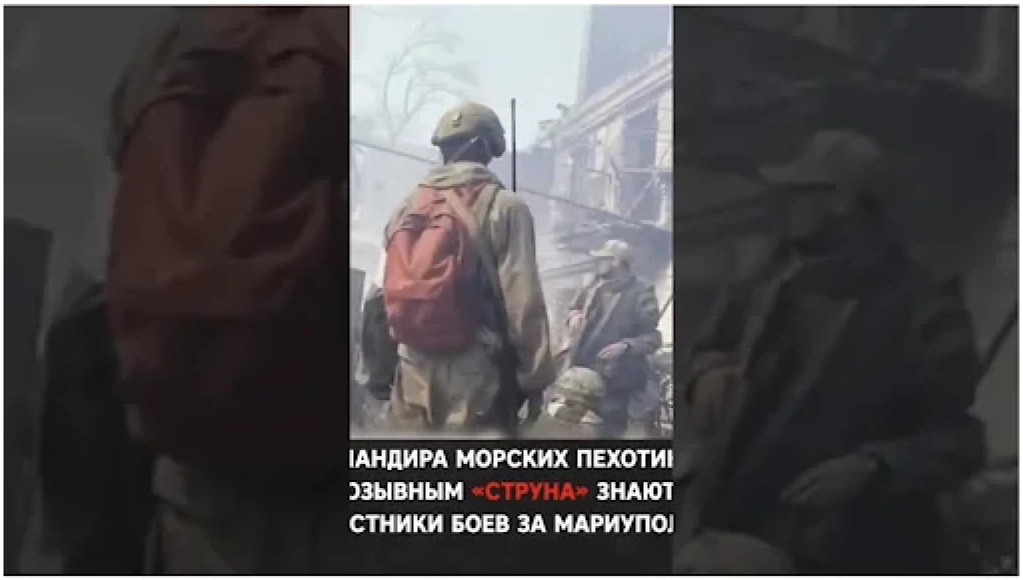
TAG also observed IRA-linked accounts publish coordinated narratives on Blogger. The narratives published by the group continue to focus on regional domestic Russian affairs.

- 

  Promotion for movie film about the Wagner Group

- 

  Screenshot from a YouTube short supporting the Wagner Group

- 

  Screenshot from a YouTube short with pro-Russian and anti-Ukrainian content

Financially motivated actors

CERT-UA previously reported on campaigns using RomCom malware to target government and military officials in Ukraine by the group behind Cuba ransomware (despite the name, US CISA reports no indication these actors are affiliated with the Republic of Cuba). This represents a large shift from this actor's traditional ransomware operations, behaving more similarly to an actor conducting operations for intelligence collection. TAG also observed campaigns from this actor targeting attendees of the Munich Security Conference and the Masters of Digital conference. The attackers are using phishing URLs with spoofed domain names related to ChatGPT and OpenAI. The campaigns have been relatively small in volume, sent from spoofed domains, and targeting users' Gmail accounts.

Protecting our users

Upon discovery, all identified websites and domains were added to Safe Browsing to protect users from further exploitation. We also send affected targeted Gmail and Workspace users government-backed attacker alerts notifying them of the activity. We encourage anyone who might be a potential target to enable Google Account Level Enhanced Safe Browsing and ensure that all devices are updated.

We remain committed to identifying bad actors, disrupting their campaigns, and sharing relevant information with others across industry and governments to raise awareness, protect users and prevent future attacks.

IOCs

FROZENBARENTS:

- cpcpipe[.]com
- cpcpipe[.]org
- 104.156.149[.]126
- c80656fe59bdeb3e701d1f7eeaaba2ef673368b2c4947945f598e3e84a6cb7f8
- telegram.org.security.ohsxy[.]com
- telegram.org.4234e8234ad0f.24o1[.]com
- ukroboronprom.com.ukr[.]pm
- 181.119.30[.]71
- 45.76.31[.]101
- 45.56.93[.]83
- 45.124.86[.]84

bio_genie IO campaign:

- https://t.me/s/bio_genie
- https://biogenie.substack.com

FROZENLAKE:

- setnewcreds.ukr.net[.]frge[.]io
- ukrprivatesite.frge[.]io
- robot-876.frge[.]io
- 85.240.182[.]23
- 68.76.150[.]97

PUSHCHA:

- passport-ua[.]site
- passport-log[.]online
- meta-l[.]space
- support@passport-ua[.]online

Cuba Ransomware / RomCom:

- openai@chatgpt4beta[.]com
- chatgpt4beta[.]com
- mod2023@masterofdigital[.]org
- masterofdigital[.]org
- 4f0b12caa97e52f3d2edada9133f2e4a3442953d14c8ed12deb7219c722ea197

POSTED IN:

Threat Analysis Group

Related stories

- Threat Analysis Group
  TAG Bulletin: Q1 2023

  Threat Analysis Group shares their Q1 2023 bulletin.

  By Shane Huntley

  May 01, 2023
- Threat Analysis Group
  How we’re protecting users from government-backed attacks from North Korea

  Google's Threat Analysis Group shares information on ARCHIPELAGO as well as the work to stop government-backed attackers.

  By Adam Weidemann

  Apr 05, 2023
- Threat Analysis Group
  Spyware vendors use 0-days and n-days against popular platforms

  Google’s Threat Analysis Group (TAG) tracks actors involved in information operations (IO), government backed attacks and financially motivated abuse. For years, TAG has…

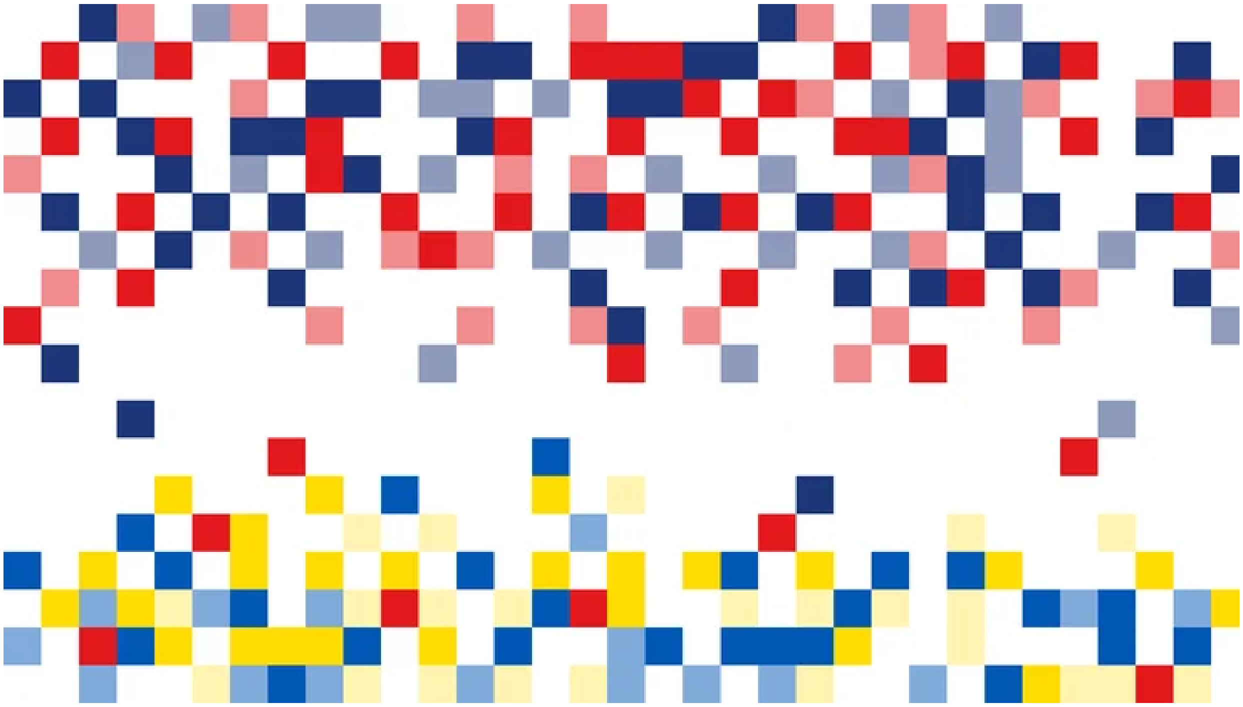
  By Clement Lecigne

  Mar 29, 2023
- Threat Analysis Group
  Magniber ransomware actors used a variant of Microsoft SmartScreen bypass

  New research from Threat Analysis Group on Magniber's exploitation of Microsoft 0-day vulnerability.

  By Benoit Sevens

  Mar 14, 2023

- 
  Threat Analysis Group
  Fog of war: how the Ukraine conflict transformed the cyber threat landscape

  By Shane Huntley

  Feb 16, 2023
- Threat Analysis Group
  Over 50,000 instances of DRAGONBRIDGE activity disrupted in 2022

  An update on TAG's work to disrupt the information operation network DRAGONBRIDGE.

  By Zak Butler Jonas Taege

  Jan 26, 2023
- .