

Continued cyber activity in Eastern Europe observed by TAG

blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag

Billy Leonard

July 19, 2022



[Threat Analysis Group](#)

Google's Threat Analysis Group (TAG) continues to closely monitor the cybersecurity environment in Eastern Europe with regard to the war in Ukraine. Many Russian government cyber assets have remained focused on Ukraine and related issues since the invasion began, while Russian APT activity outside of Ukraine largely remains the same. TAG continues to disrupt campaigns from multiple sets of Russian government-backed attackers, some of which are detailed in our [previous updates](#).

Similarly, Russian observed disinformation efforts are also focused on the war in Ukraine and TAG has disrupted coordinated influence operations from several actors including the Internet Research Agency and a Russian consulting firm as detailed in the [TAG Bulletin](#). Most of these coordinated influence operations are Russian language efforts aimed at ensuring domestic support in Russia for the war.

Here is a deeper look at some campaign activity TAG has observed since our last update:

Turla, a group publicly attributed to Russia's Federal Security Service (FSB), recently hosted Android apps on a domain spoofing the [Ukrainian Azov Regiment](#). This is the first known instance of Turla distributing Android-related malware. The apps were not distributed through the Google Play Store, but hosted on a domain controlled by the actor 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 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, not enough to be effective. The list of target websites for the app can be seen in the CyberChef recipe [here](#).

Cyber Azov Home Download About us Donate Contact

info@cyberazov.com UA

What we do

App Download


Join the Cyber Azov and help stop russian aggression against Ukraine!

We are a community of free people around the world who are fighting against russia's aggression. We recruit motivated people who are ready to help us in our cause. We have developed an Android application that attacks the Internet infrastructure of russia. At the moment the list of targets is predetermined

[Download](#) our application "CyberAzov"

How does it work?

It is a simple app that initiates a DoS attack on the web servers of occupants. All you need to do to launch the process is install the app, open it and press Start. The app immediately begins sending requests to the russian websites to overwhelm their resources and cause the denial of service.



Turla website disseminating fake DoS Android Apps.

During our investigation into the Turla CyberAzov apps, we identified another Android app first seen in the wild in March 2022 that also claimed to conduct DoS attacks against Russian websites. In this case, the Android app name was [stopwar.apk](#) (com.ddos.stopwar) and was distributed from the website [stopwar.pro](#). This app is quite different from the Turla apps described above and written by a different developer. It also downloads a list of targets from an external site, but unlike the Turla apps, it continually sends requests to the target websites until it is stopped by the user.

StopWar.pro
A mobile App integrates an anti-war cyber network


Instruction About Download EN


You don't have to be an IT specialist to join the Ukrainian cyber army and help us stop russian aggression against Ukraine!

Turn on the application on your smartphone, and it will load russian sites. As more of us, there will be, as soon their infrastructure will be overloaded and "will go to bed."

Before applying, set up a VPN!

If StopWar runs on your smartphone, you help Ukraine win





Pro-Ukrainian website used for disseminating StopWar.apk.

Based on our analysis, we believe that the StopWar app was developed by pro-Ukrainian developers and was the inspiration for what Turla actors based their fake CyberAzov DoS app off of.

Indicators:

- [https://cyberazov\[.\]com/apk/CyberAzov.apk](https://cyberazov[.]com/apk/CyberAzov.apk)
- [745e8c90a8e76f81021ff491cbc275bc134cdd7d23826b8dd23e58297fd0dd33](#)
- [3c62b24594ec3cacc14bdca068a0277e855967210e92c2c17bcf7c7d0d6b782a](#)

The Follina vulnerability ([CVE-2022-30190](#)), first disclosed in late May, received significant usage from both APT and cybercrime groups throughout June after it was patched by Microsoft. Follina is a remote code execution (RCE) vulnerability in the Microsoft Windows Support Diagnostic Tool (MSDT).

Consistent with CERT-UA reporting, TAG observed multiple Russian GRU actors - [APT28](#) and Sandworm - conduct campaigns exploiting the Follina vulnerability. The Sandworm campaign used compromised government accounts to send links to Microsoft Office

documents hosted on compromised domains, primarily targeting media organizations in Ukraine.

TAG has also observed an increasing number of financially motivated actors targeting Ukraine. One recent campaign from a group tracked by CERT-UA as UAC-0098 delivered malicious documents with the Follina exploit in password-protected archives, impersonating the State Tax Service of Ukraine. We assess this actor is a former initial ransomware access broker who previously worked with the Conti ransomware group distributing the IcedID banking trojan based on overlaps in infrastructure, tools used in previous campaigns, and a unique cryptor.

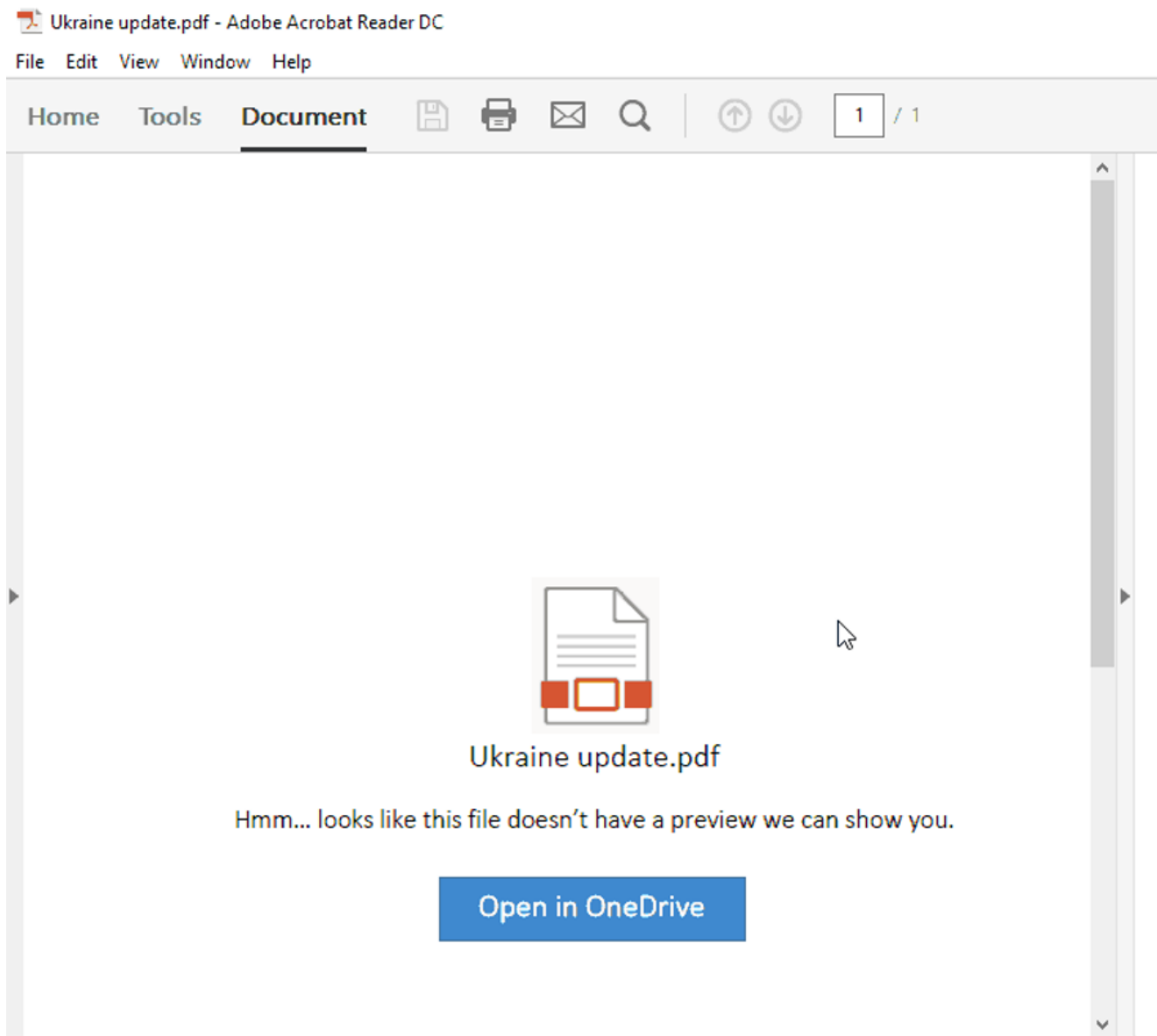
Ghostwriter/UNC1151, a threat actor attributed to Belarus, has remained active targeting accounts of webmail and social media networks of Polish users. They continue to use the 'Browser in the Browser' phishing technique that TAG first observed and described in March. An example of this technique, used to target Facebook users, can be seen in the screenshot below.



An example of this technique used to target Facebook users

COLDRIVER, a Russian-based threat actor sometimes referred to as Callisto, continues to send credential phishing emails to targets including government and defense officials, politicians, NGOs and think tanks, and journalists. In addition to including phishing links directly in the email, the attackers also link to PDFs and/or DOCs, hosted on Google Drive and Microsoft One Drive, that contain a link to an attacker-controlled phishing domain. In at least one case, unrelated to Ukraine, they have leaked information from a compromised account.

These phishing domains have been blocked through Google Safe Browsing – a service that identifies unsafe websites across the web and notifies users and website owners of potential harm.



Example of a recent COLDRIVER phishing lure

Recently observed COLDRIVER indicators:

- [7b95747eeea196c1485d089fa47a06bacb07d06399603d3a4fa153c21ce0a9ba](https://www.cache-pdf.com/7b95747eeea196c1485d089fa47a06bacb07d06399603d3a4fa153c21ce0a9ba)
- [cache-pdf\[.\]com](https://www.cache-pdf.com/)

In another campaign tracked by [CERT-UA](#) as [UAC-0056](#) we observed compromised email addresses of a Regional Prosecutor's office of Ukraine leveraged to send malicious Microsoft Excel documents with VBA macros delivering Cobalt Strike. In just two days, the volume observed and categorized as spam by Gmail exceeded 4,500 emails. Email contents vary from COVID-19 vaccine policy to the humanitarian crisis in Ukraine.