Update on cyber activity in Eastern Europe

Billy Leonard ⋮⋮ 5/3/2022

Threat Analysis Group

Google's Threat Analysis Group (TAG) has been closely monitoring the cybersecurity activity in Eastern Europe with regard to the war in Ukraine. Since our last update, TAG has observed a continuously growing number of threat actors using the war as a lure in phishing and malware campaigns. Similar to other reports, we have also observed threat actors increasingly target critical infrastructure entities including oil and gas, telecommunications and manufacturing.

Government-backed actors from China, Iran, North Korea and Russia, as well as various unattributed groups, have used various Ukraine war-related themes in an effort to get targets to open malicious emails or click malicious links. Financially motivated and criminal actors are also using current events as a means for targeting users.

As always, we continue to publish details surrounding the actions we take against coordinated influence operations in our quarterly TAG bulletin. We promptly identify and remove any such content but have not observed any significant shifts from the normal levels of activity that occur in the region.

Here is a deeper look at the campaign activity TAG has observed and the actions the team has taken to protect our users over the past few weeks:

APT28 or Fancy Bear, a threat actor attributed to Russia GRU, was observed targeting users in Ukraine with a new variant of malware. The malware, distributed via email attachments inside of password

protected zip files (ua_report.zip), is a .Net executable that when executed steals cookies and saved passwords from Chrome, Edge and Firefox browsers. The data is then exfiltrated via email to a compromised email account.

Malware samples:

- 710faabf217a5cd3431670558603a45edb1e01970f2a8710514c2cc3dd8c2424
- 39d242660c6d5dbe97d5725bbfed0f583344d18840ccd902fffdd71af12e20ec

TAG would like to thank the Yahoo! Paranoids Advanced Cyber Threats Team for their collaboration in this investigation.

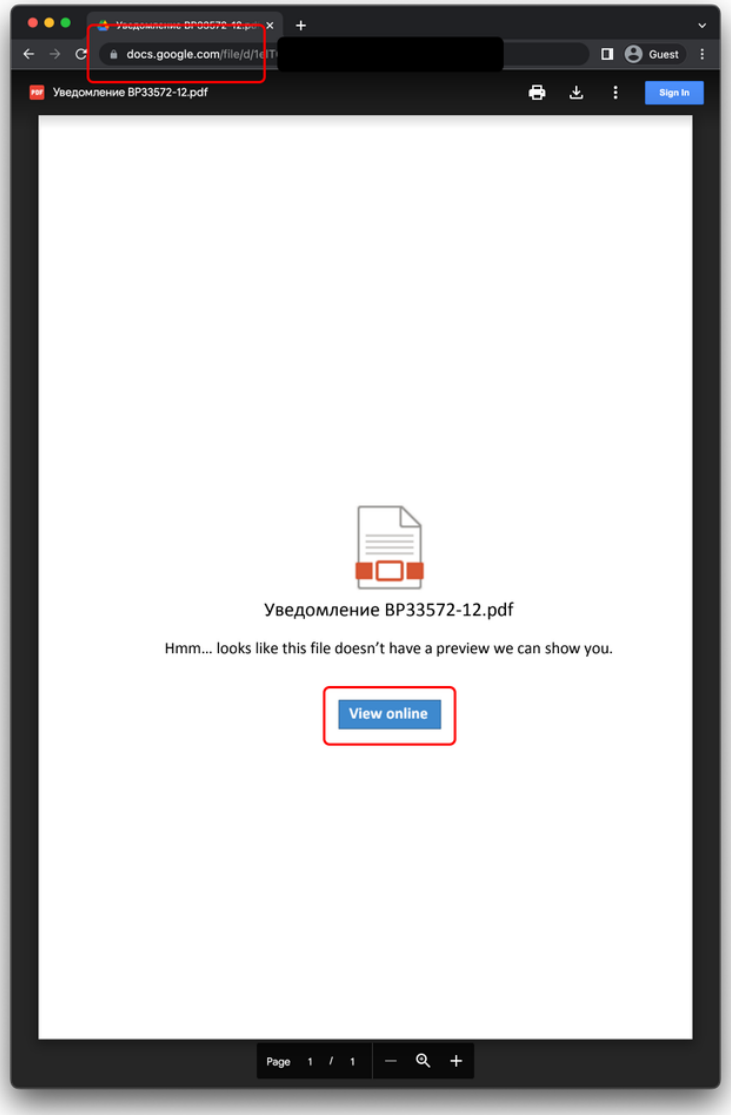
Turla, a group TAG attributes to Russia FSB, continues to run campaigns against the Baltics, targeting defense and cybersecurity organizations in the region. Similar to recently observed activity, these campaigns were sent via email and contained a unique link per target that led to a DOCX file hosted on attacker controlled infrastructure. When opened, the DOCX file would attempt to download a unique PNG file from the same attacker controlled domain.

Recently observed Turla domains:

- wkoinfo.webredirect[.]org
- jadlactnato.webredirect[.]org

COLDRIVER, a Russian-based threat actor sometimes referred to as Callisto, continues to use Gmail accounts to send credential phishing emails to a variety of Google and non-Google accounts. The targets include government and defense officials, politicians, NGOs and think tanks, and journalists. The group's tactics, techniques and procedures (TTPs) for these campaigns have shifted slightly from including phishing links directly in the email, to also linking to PDFs and/or DOCs hosted on Google Drive and Microsoft One Drive. Within these files is a link to an attacker controlled phishing domain.

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.



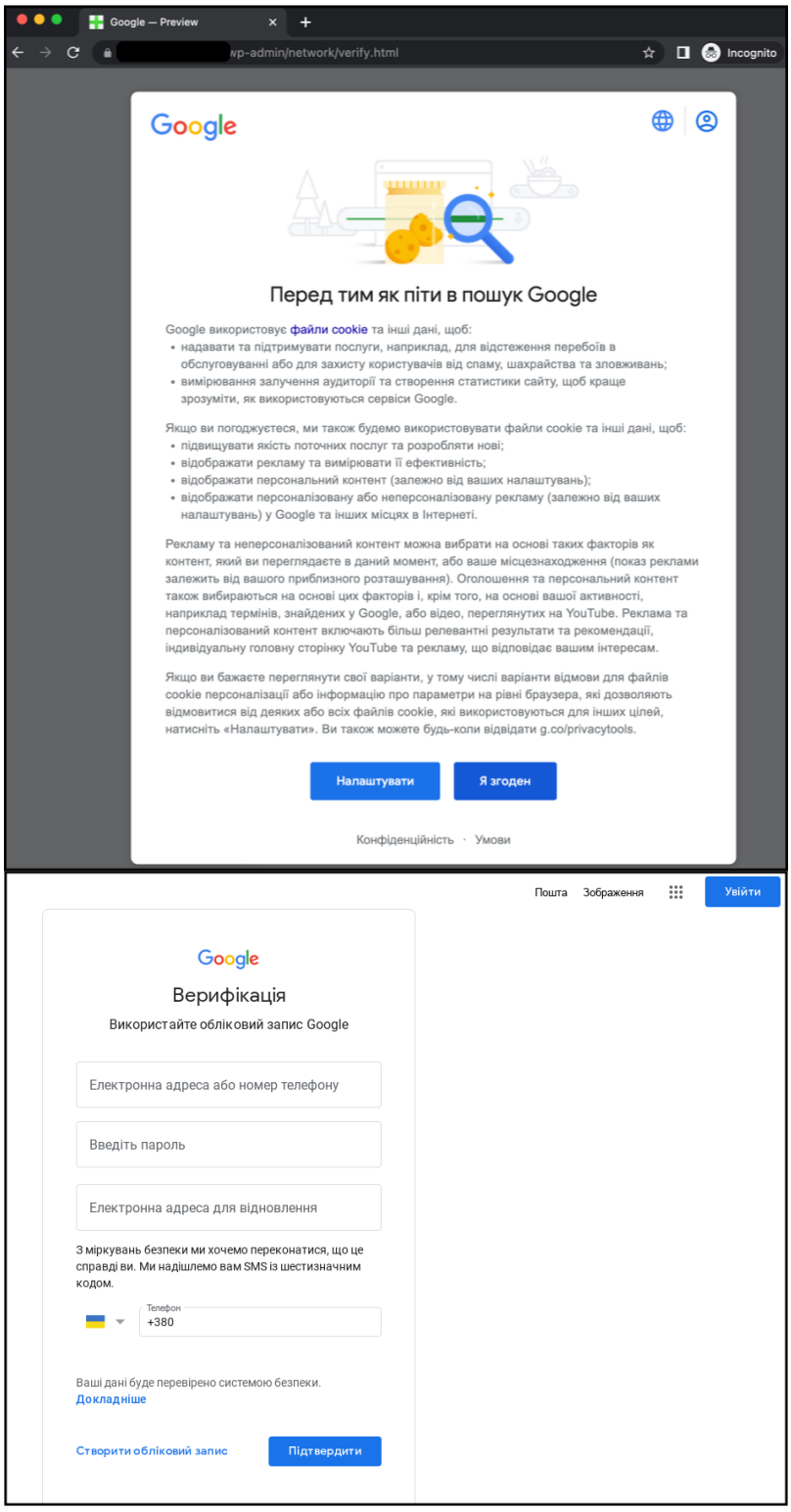
An example of this technique

Recently observed COLDRIVER credential phishing domains:

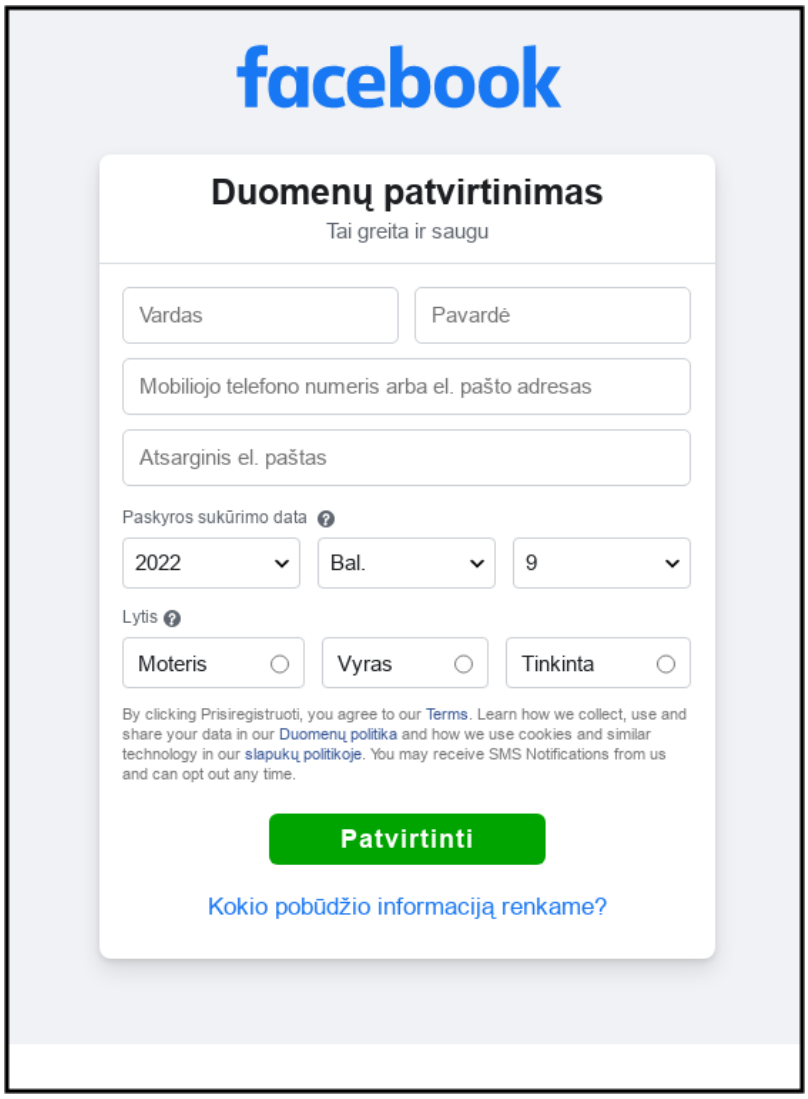
- cache-dns[.]com
- docs-shared[.]com
- documents-forwarding[.]com
- documents-preview[.]com
- protection-link[.]online
- webresources[.]live

Ghostwriter, a Belarusian threat actor, has remained active during the course of the war and recently resumed targeting of Gmail accounts via credential phishing. This campaign, targeting high risk individuals in Ukraine, contained links leading to compromised websites where the first stage phishing page was hosted. If the user clicked continue, they would be redirected to an attacker controlled site that collected the users credentials. There were no accounts compromised from this campaign and Google will alert all targeted users of these attempts through our monthly government-backed attacker warnings.

Both pages from this campaign are shown below.



In mid-April, TAG detected a Ghostwriter credential phishing campaign targeting Facebook users. The targets, primarily located in Lithuania, were sent links to attacker controlled domains from a domain spoofing the Facebook security team.



Recently observed Ghostwriter credential phishing domains and emails:

- noreply.accountsverify[.]top
- microsoftonline.email-verify[.]top
- lt-microsoftgroup.serure-email[.]online
- facebook.com-validation[.]top
- lt-meta.com-verification[.]top
- lt-facebook.com-verification[.]top
- secure@facebookgroup[.]lt

Curious Gorge, a group TAG attributes to China's PLA SSF, has remained active against government, military, logistics and manufacturing organizations in Ukraine, Russia and Central Asia. In Russia, long running campaigns against multiple government organizations have continued, including the Ministry of Foreign Affairs. Over the past week, TAG identified additional compromises impacting multiple Russian defense contractors and manufacturers and a Russian logistics company.

Protecting Our Users

Upon discovery, all identified websites and domains were added to Safe Browsing to protect users from further exploitation. We also send all targeted Gmail and Workspace users government-backed attacker

alerts notifying them of the activity. We encourage any potential targets to enable Google Account Level Enhanced Safe Browsing and ensure that all devices are updated.

The team continues to work around the clock, focusing on the safety and security of our users and the platforms that help them access and share important information. We'll continue to take action, identify bad actors and share relevant information with others across industry and governments, with the goal of bringing awareness to these issues, protecting users and preventing future attacks. While we are actively monitoring activity related to Ukraine and Russia, we continue to be just as vigilant in relation to other threat actors globally, to ensure that they do not take advantage of everyone's focus on this region.