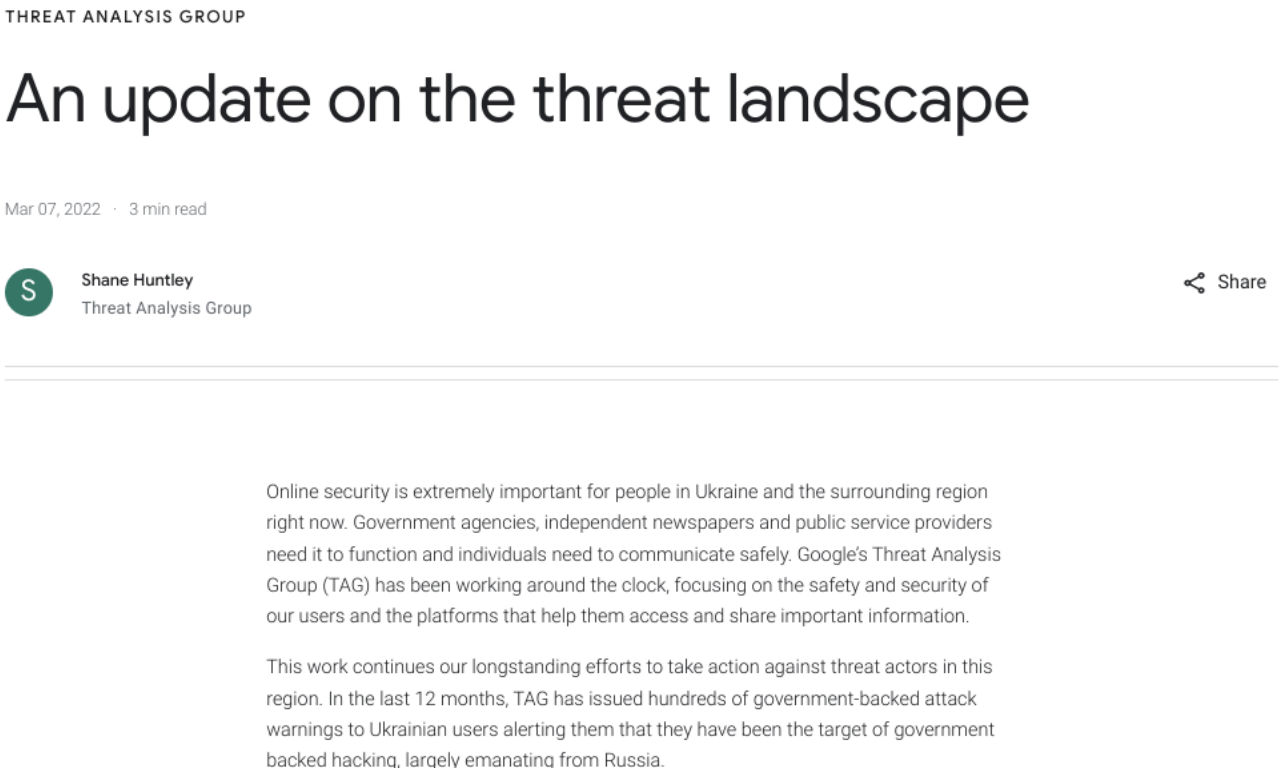
An update on the threat landscape

blog.google/threat-analysis-group/update-threat-landscape-ukraine/

Shane Huntley March 7, 2022



THREAT ANALYSIS GROUP

An update on the threat landscape

Mar 07, 2022 · 3 min read

Shane Huntley
Threat Analysis Group

Share

Online security is extremely important for people in Ukraine and the surrounding region right now. Government agencies, independent newspapers and public service providers need it to function and individuals need to communicate safely. Google's Threat Analysis Group (TAG) has been working around the clock, focusing on the safety and security of our users and the platforms that help them access and share important information.

This work continues our longstanding efforts to take action against threat actors in this region. In the last 12 months, TAG has issued hundreds of government-backed attack warnings to Ukrainian users alerting them that they have been the target of government backed hacking, largely emanating from Russia.

Online security is extremely important for people in Ukraine and the surrounding region right now. Government agencies, independent newspapers and public service providers need it to function and individuals need to communicate safely. Google's Threat Analysis Group (TAG) has been working around the clock, focusing on the safety and security of our users and the platforms that help them access and share important information.

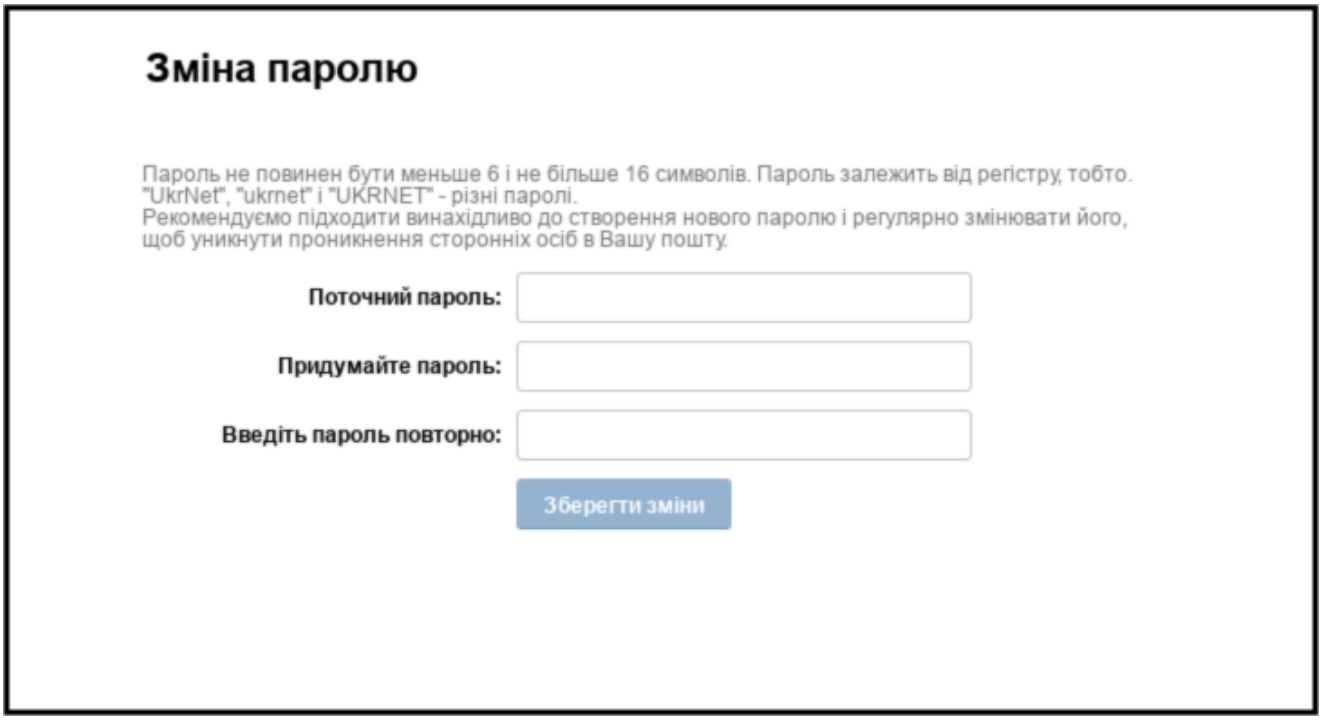
This work continues our longstanding efforts to take action against threat actors in this region. In the last 12 months, TAG has issued hundreds of government-backed attack warnings to Ukrainian users alerting them that they have been the target of government backed hacking, largely emanating from Russia.

Over the past two weeks, TAG has observed activity from a range of threat actors that we regularly monitor and are well-known to law enforcement, including FancyBear and Ghostwriter. This activity ranges from espionage to phishing campaigns. We're sharing this information to help raise awareness among the security community and high risk users:

FancyBear/APT28, a threat actor attributed to Russia GRU, has conducted several large credential phishing campaigns targeting ukr.net users, UkrNet is a Ukrainian media company. The phishing emails are sent from a large number of compromised accounts (non-

Gmail/Google), and include links to attacker controlled domains.

In two recent campaigns, the attackers used newly created Blogspot domains as the initial landing page, which then redirected targets to credential phishing pages. All known attacker-controlled Blogspot domains have been taken down.



Example of APT28 credential phishing page

Example credential phishing domains observed during these campaigns:

- id-unconfirmeduser[.]frge[.]io
- hatdfg-rhgreh684[.]frge[.]io
- ua-consumerpanel[.]frge[.]io
- consumerspanel[.]frge[.]io

Ghostwriter/UNC1151, a Belarusian threat actor, has conducted credential phishing campaigns over the past week against Polish and Ukrainian government and military organizations. TAG has also identified campaigns targeting webmail users from the following providers:

- i.ua
- meta.ua
- rambler.ru
- ukr.net
- wp.pl
- yandex.ru

Example credential phishing domains observed during these campaigns:

- accounts[.]secure-ua[.]website
- i[.]ua-passport[.]top
- login[.]creditals-email[.]space
- post[.]mil-gov[.]space
- verify[.]rambler-profile[.]site

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.

Mustang Panda or Temp.Hex, a China-based threat actor, targeted European entities with lures related to the Ukrainian invasion. TAG identified malicious attachments with file names such as 'Situation at the EU borders with Ukraine.zip'. Contained within the zip file is an executable of the same name that is a basic downloader and when executed, downloads several additional files that load the final payload. To mitigate harm, TAG alerted relevant authorities of its findings.

Targeting of European organizations has represented a shift from Mustang Panda's regularly observed Southeast Asian targets.

DDoS Attacks

We continue to see DDoS attempts against numerous Ukraine sites, including the Ministry of Foreign Affairs, Ministry of Internal Affairs, as well as services like Liveuamap that are designed to help people find information. We expanded eligibility for Project Shield, our free protection against DDoS attacks, so that Ukrainian government websites, embassies worldwide and other governments in close proximity to the conflict can stay online, protect themselves and continue to offer their crucial services and ensure access to the information people need.

Project Shield allows Google to absorb the bad traffic in a DDoS attack and act as a "shield" for websites, allowing them to continue operating and defend against these attacks. As of today, over 150 websites in Ukraine, including many news organizations, are using the service. We encourage all eligible organizations to register for Project Shield so our systems can help block these attacks and keep websites online.

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. And 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.

POSTED IN:

Threat Analysis Group