Tracking cyber activity in Eastern Europe

Threat Analysis Group
Mar 30, 2022

Billy Leonard

In early March, Google's Threat Analysis Group (TAG) published an update on the cyber activity it was tracking 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. 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. For example, one actor is impersonating military personnel to extort money for rescuing relatives in Ukraine. TAG has also continued to observe multiple ransomware brokers continuing to operate in a business as usual sense.

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 over the past two weeks:

Curious Gorge, a group TAG attributes to China's PLA SSF, has conducted campaigns against government and military organizations in Ukraine, Russia, Kazakhstan, and Mongolia. While this activity largely does not impact Google products, we remain engaged and are providing notifications to victim organizations.

Recently observed IPs used in Curious Gorge campaigns:

- 5.188.108[.]119
- 91.216.190[.]58
- 103.27.186[.]23
- 114.249.31[.]171
- 45.154.12[.]167

COLDRIVER, a Russian-based threat actor sometimes referred to as Calisto, has launched credential phishing campaigns, targeting several US based NGOs and think tanks, the military of a Balkans country, and a Ukraine based defense contractor. However, for the first time, TAG has observed COLDRIVER campaigns targeting the

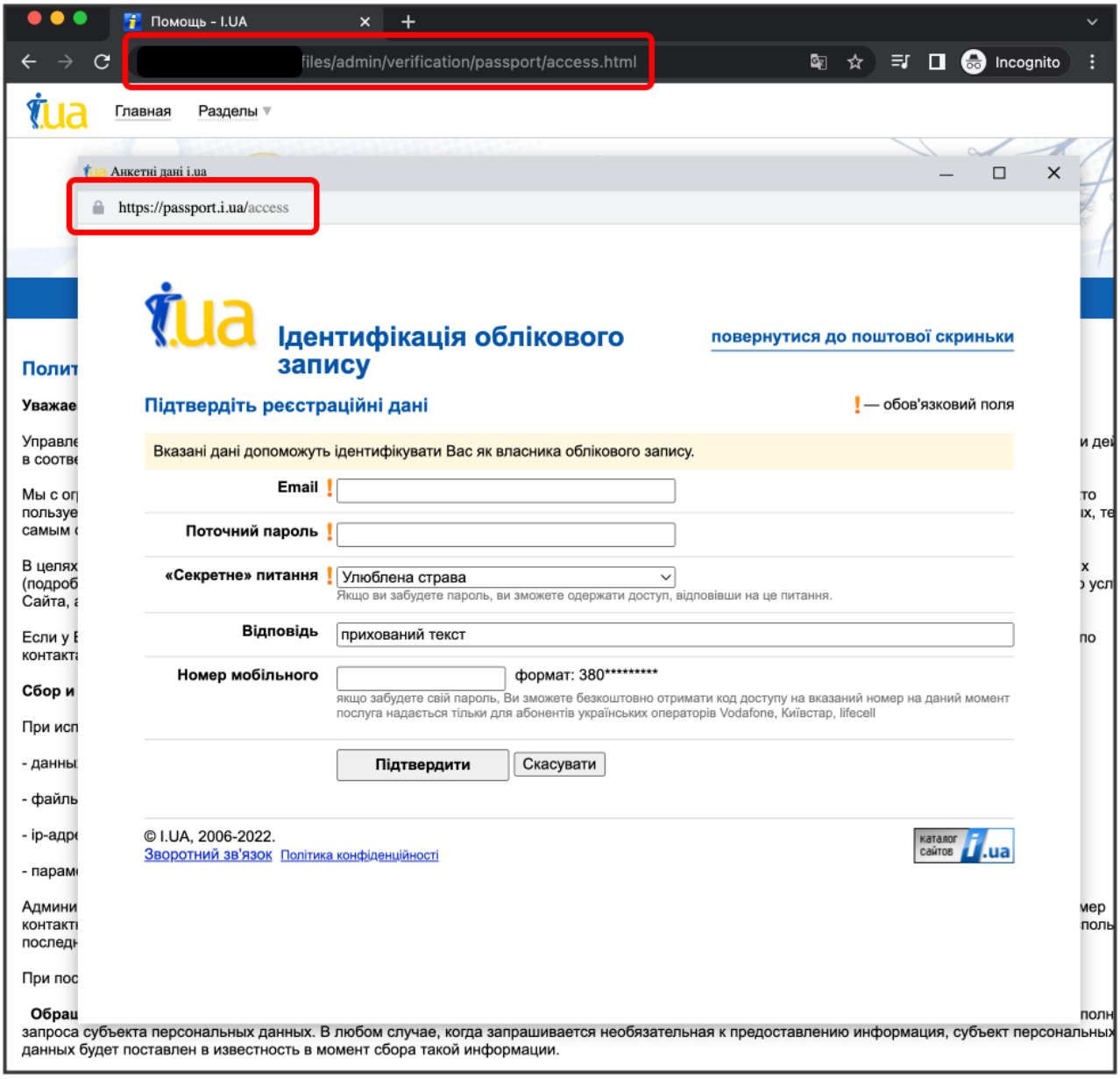
military of multiple Eastern European countries, as well as a NATO Centre of Excellence. These campaigns were sent using newly created Gmail accounts to non-Google accounts, so the success rate of these campaigns is unknown. We have not observed any Gmail accounts successfully compromised during these campaigns.

Recently observed COLDRIVER credential phishing domains:

- protect-link[.]online
- drive-share[.]live
- protection-office[.]live
- proton-viewer[.]com

Ghostwriter, a Belarusian threat actor, recently introduced a new capability into their credential phishing campaigns. In mid-March, a security researcher released a blog post detailing a 'Browser in the Browser' phishing technique. While TAG has previously observed this technique being used by multiple government-backed actors, the media picked up on this blog post, publishing several stories highlighting this phishing capability.

Ghostwriter actors have quickly adopted this new technique, combining it with a previously observed technique, hosting credential phishing landing pages on compromised sites. The new technique, displayed below, draws a login page that appears to be on the passport.i.ua domain, overtop of the page hosted on the compromised site. Once a user provides credentials in the dialog, they are posted to an attacker controlled domain.



Example of hosting credential phishing landing pages on compromised sites

Recently observed Ghostwriter credential phishing domains:

- login-verification[.]top
- login-verify[.]top
- ua-login[.]top
- secure-ua[.]space
- secure-ua[.]top

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.