# CALISTO continues its credential harvesting campaign

**blog.sekoia.io**/calisto-continues-its-credential-harvesting-campaign

22 June 2022

## Log in

Whoops! You have to login to access the Reading Center functionalities!

Forgot password?

### Search the site...

- All categories
- Blogpost
- Blogpost

Reset

Blogpost Blogpost

APT
CTI

Threat & Detection Research Team June 22 2022
2333 0

Read it later Remove

3 minutes reading

*This blog post on CALISTO threat actor is an extract of a FLINT report (SEKOIA.IO Flash Intelligence) sent to our clients on June 16, 2022.*

March 30, 2022, Google TAG published several IOCs related to CALISTO – a Russia-nexus threat actor also known as COLDRIVER which targeted several Western NGOs, think tanks and the defense sector in the past. According to Google TAG, the operators used freshly created Gmail accounts to carry out a spear-phishing campaign.

Based on TAG's findings, CALISTO used, at least on one occasion, decoys documents hosted on Google Docs as well as Microsoft One drive, to entice the victim to click on a link leading to the phishing domain, purporting to display the document's content. The tactic consists in using a legit service as a proxy for credential phishing, this aims at bypassing controls from the victim's mail gateways as the email itself does not contain a malicious link any longer.

Additionally, TAG uncovered that On April 21, 2022, a new website named "*Very English Coop d'Etat*" surfaced. This website allegedly aims at revealing a plot related to the Brexit. However, as mentioned by security researcher Costin Raiu on Twitter, at least one leaked document seems to be a fake from the attackers. Based on the leveraged design, method and screenshots,this activity reminds the "Hack and Leak" campaigns operated between 2015 and 2019 and associated to Russia-nexus intrusion sets SOFACY and HADES.

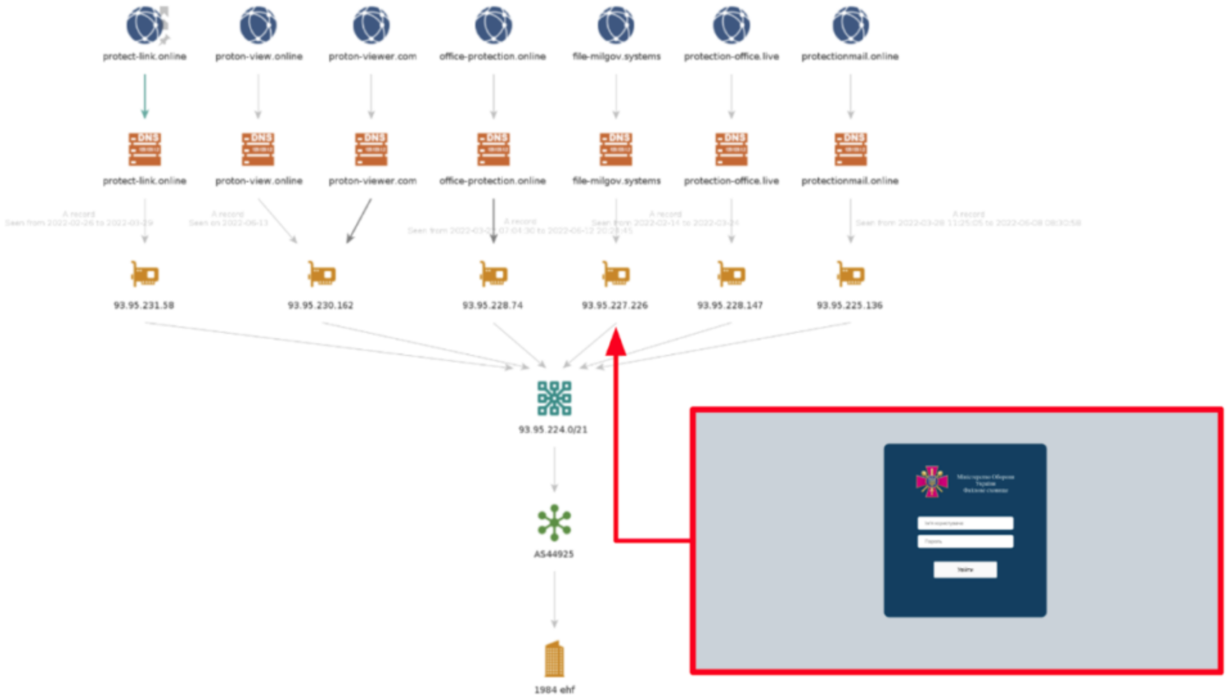
Even if the new website reminds the old ones from SOFACY, Google TAG declared in an interview to Reuters that they've been able to " technically link this website to CALISTO operations", without mentioning the technical details leading to this attribution. As of today, while weak links can be established between past GRU associated cyber operations TTPs and this documented activity, SEKOIA.IO refrains from associating CALISTO's operations to Russian Intelligence and Security Services.

## Infrastructure analysis of CALISTO

Following these two publications, SEKOIA investigated the Calisto phishing domains in order to protect our customers. CALISTO uses Evilginx on its VPS to capture the victim's credentials. This well known open source tool creates an SSL reverse proxy between the victim and a legitimate website to capture web credentials, 2FA tokens…

It’s worth mentioning that CALISTO operators just followed the Github README of the EvilGinx project, creating default redirection for some of their VPS to the Youtube Rick’roll video. Additional servers redirect to the New York Times home page, these two OPSEC fails allowing us to find more servers easily.

By digging deeper a phishing domain *(file-milgov[.]systems)* targeting the Ukrainian MOD drew our attention. Unlike the previous CALISTO domains, this one uses a webpage written in PHP to capture credentials. It is worth mentioning that this domain have been catched also by Trellix in their article “Growling Bears Make Thunderous Noise” without attribution.



While it doesn’t match our Evilginx heuristic, it was operated in the same network range as several CALISTO domains during the same time frame. Therefore, it is likely possible that this domain is associated with a spear-phishing operation from CALISTO, the link being determined with a low degree of confidence.

As of today, SEKOIA.IO has been able to link 24 unique domains operating Evilginx related to CALISTO operations with medium to high confidence.

## IOCs of CALISTO

### Domain names

*Please blacklist these domains and the associated FQDNs*

```
documents-cloud[.]com
cache-docs[.]com
protect-link[.]online
docs-shared[.]com
documents-cloud[.]online
drive-share[.]live
hypertextteches[.]com
proton-docs[.]com
docs-drive[.]online
cloud-docs[.]com
drive-docs[.]com
file-milgov[.]systems
cache-dns[.]com
office-protection[.]online
proton-view[.]online
pdf-shared[.]online
proton-viewer[.]com
protectionmail[.]online
pdf-docs[.]online
documents-pdf[.]online
docs-cache[.]com
pdf-cloud[.]online
docs-info[.]com
protection-office[.]live
```

## Chat with our team!

Would you like to know more about our solutions? Do you want to discover our XDR and CTI products? Do you have a cybersecurity project in your organization? Make an appointment and meet us!

**Contact us**

**Comments are closed.**