Calisto show interests into entities involved in Ukraine war support

12/5/2022

Calisto (aka Callisto, COLDRIVER) is suspected to be a **Russian-nexus intrusion set** active since at least April 2017. Although it was not publicly attributed to any Russian intelligence service, past Calisto operations showed objectives and victimology that align closely with **Russian strategic interests**.

Calisto mainly focuses on Western countries, especially the United States, and Eastern European countries. The group was observed carrying out **phishing campaigns** aiming at **credential theft**, targeting military and strategic research sectors such as NATO entities and a Ukraine-based defense contractor, as well as NGOs and think tanks. Additional victimology includes former ntelligence officials, experts in Russian matters, and Russian citizens abroad.

While Security Service of Ukraine (SBU) publicly associated Calisto with Gamaredon Group, an intrusion set attributed to the Russian Federal Security Service (FSB) that focuses essentially on Ukraine operations since the beginning of the Russian invasion in February 2022, this link is not supported by other security companies or researchers. SEKOIA.IO conducted further technical investigations but did not find any overlap between Calisto and Gamaredon activities.

Technical analysis

Based on **SEKOIA.IO EvilNgix trackers**, we came across domains, known to us as aligning with past **Calisto activities**. Further investigations led to a larger infrastructure composed of more than 80 domains, including domains typosquatting entites.

As several of these domains were already known and resolving IP addresses already attributed to Calisto activities, **SEKOIA.IO associates these domains to Calisto with high confidence**.

In past observed campaigns, Calisto operators sent malicious PDF attachments to their victims. The first page of the PDF mimics **an error in the PDF renderer engine**, inciting the victim to open a link leading to a malicious web page. This webpage aims at gathering the victim's credentials by using EvilGinx. Here are a few examples of PDF retrieved in this investigation:

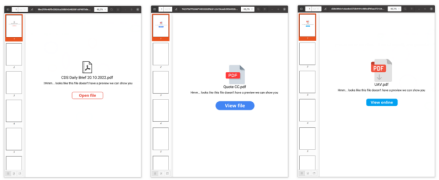

Figure 1. First pages of malicious PDF sent by Calisto

The last pages of the documents contain blobs of spirals and text, as shown below. SEKOIA.IO analysts still don't know why such gibberish is used as it appears useless as an anti-detection trick. However, the idea to put the phishing link in a PDF instead of in the email body prevents link analysis from email gateways and is a good tactic to remain undetected from an attacker point of view.

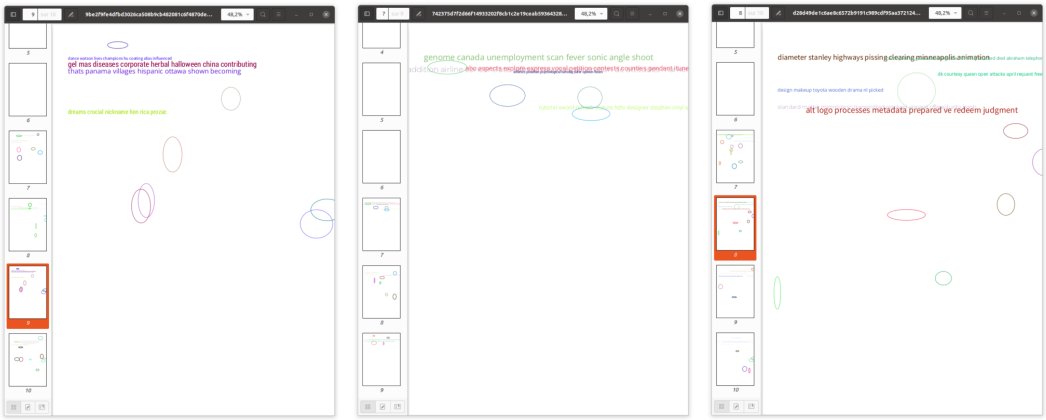

Figure 2. Garbage present in the last document pages

Victimology analysis

SEKOIA.IO conducted open-source research on the typosquatted domains, to identify targets. As we redact this paper, we found **six private companies based in the US and Eastern Europe**, and **four Non-governmental organizations (NGOs)**, all involved in Ukraine support. SEKOIA.IO contacted the NGOs to get the phishing email or payload.

One of them shared the email exchange between the victim and the attacker using a spoofed email from a “trusted source”, including the malicious PDF payload, a technique previously observed in Calisto campaigns. The email exchange shows that the attacker did not include the malicious payload in the first email, but **waited to get an answer** to build a relationship and avoid suspicion **before sending the payload** to the victim. That Calisto social engineering technique was already observed by Microsoft.

Most of the targeted private organizations are involved in **military equipment**, **military logistics** or **humanitarian support for Ukraine**, including a US company that provides humanitarian logistics and possibly tactical equipment to Kiev. Other sectors include communication technologies and cybersecurity (medium confidence) :

- **UMO**, Polish company, military equipment (high confidence);
- **Emcompass**, Ukrainian company, military logistic (high confidence);
- **DTGruelle**, US company, logistics (high confidence);
- **Global Ordnance**, US company, military and tactical equipment (high confidence);
- **BotGuard**, Estonian company, cybersecurity (medium confidence);
- **Blue Sky Network**, US company, satellite communications (high confidence).

Additional potential victims include NGOs and think tanks involved in conflict resolution and war crime investigation, including an organization also involved in the Syrian civil war crime investigation and previously targeted by an Indian hack-for-hire company in June 2020. Most of the NGOs and think tanks targeted are publicly supporting Ukraine.

- **International Center on Nonviolent Conflict**, US think tank promoting non-military strategies by civilian-based movements to defend human rights (high confidence);
- **Commission for International Justice and Accountability**, Europe-based NGO, proof collection for human rights violation and war crime (high confidence);
- **Centre for Humanitarian Dialogue**, Swiss-based NGO, mediation and diplomacy for conflict resolution (high confidence);
- **Foundation for support of reforms in Ukraine**, Ukraine-based NGO, economic reforms promotion, likely involved in post-war reconstruction planning (medium confidence).

SEKOIA.IO notes that the observed victimology through the investigation matches known Calisto victimology, namely strategic research, civil society and military equipment sectors, as well as entities and individuals involved in Russian matters.

Calisto targets non-directly related to Ukraine support

Among discovered Calisto malicious domains, three caught SEKOIA.IO analysts’ attention, mvd-redir[.]ru and dns-mvd[.]ru (high confidence) that are highly likely typosquatting the **Russian Ministry of Interior**, and lk-nalog-gov[.]ru (*low* confidence) the Russian Federal Taxation Service. Based on the fact that Calisto was observed targeting Russian individuals abroad, **SEKOIA.IO assess it is plausible that Calisto conducts domestic surveillance as well**. Another less plausible hypothesis would be a false-flag maneuver to raise doubts on the infrastructure’s attribution.

SEKOIA.IO found another potential victim that matches Calisto known targeting. The domain sangrail-share[.]com and sangrail-ltd[.]com are typosquatting **Sangrail Inc**., a private security company, registered in the UK on 31 July 2019 by Ian Walter Baharie. That name was used as well to register AC21,

a British private intelligence company focused on African politics. Interestingly, that name showed up in a 17-years-old data leak exposing a list of several MI6 officers on cryptome.org, a website dedicated to information leaks. That observation matches Microsoft assessment on **Calisto targeting former intelligence officers.**

Conclusion

Despite the absence of technical evidence associating Calisto activities with a known Russian cyber offensive service, SEKOIA.IO assess that this intrusion set intelligence collection activities targeting parties involved in Ukraine support, especially those in the tactical equipment logistics, probably **contribute** to **Russian efforts** to **disrupt Kiev supply-chain** for military reinforcements.

Discover our CTI and XDR products

Based on the targeting of Commission for International Justice and Accountability NGO, SEKOIA.IO assess that Calisto contributes to **Russian intelligence collection about identified war crime-related evidence** and/or international justice procedures, likely to anticipate and build counter narrative on future accusations.

To provide our customers with actionable intelligence, SEKOIA.IO analysts will continue to monitor state-sponsored advanced and persistent threats, including Calisto, as well as cybercrime related groups. **We welcome any feedback and / or additional input to further contribute to understanding and countering Calisto threat.**

IOCs & Technical Details

```
access-confirmation[.]com
allow-access[.]com
antibots-service[.]com
apicomcloud[.]com
as-mvd[.]ru
attach-docs[.]com
attach-update[.]com
blueskynetwork-drive[.]com
blueskynetwork-shared[.]com
botguard-checker[.]com
botguard-web[.]com
challenge-identifier[.]com
challenge-share[.]com
checker-bot[.]com
cija-docs[.]com
cija-drive[.]com
cloud-safety[.]online
cloud-us[.]online
default-dns[.]online
disk-previewer[.]com
dns-cache[.]online
dns-challenge[.]com
dns-cookie[.]com
dns-mvd[.]ru
docs-cache[.]online
docs-collector[.]com
docs-shared[.]online
docs-storage-ltd[.]com
docs-viewer[.]online
docs-web[.]online
document-guard[.]com
document-sender[.]com
drive-control[.]com
drive-defender[.]com
drive-global-ordnance[.]com
drive-globalordnance[.]com
drive-information[.]com
drive-previewer[.]com
drive-us[.]online
dtgruelle-drive[.]com
dtgruelle-us[.]com
encompass-drive[.]com
encompass-shared[.]com
filter-bot[.]com
global-ordnance-drive[.]com
```

```
goweb-protect[.]com
goweb-service[.]com
guard-checker[.]com
hd-centre-drive[.]com
hd-docs-share[.]com
hypertexttech[.]com
hypertextttech[.]com
land-of-service[.]com
live-identifier[.]com
mvd-cloud[.]ru
mvd-redir[.]ru
network-storage-ltd[.]com
nonviolent-conflict-service[.]com
nonviolent-conflict-storage[.]com
online-word[.]com
preview-docs[.]com
preview-docs[.]online
protectedshields-storage[.]com
protection-web-app[.]com
proxycrioisolation[.]com
redir-document[.]com
response-collector[.]com
response-filter[.]com
response-mvd[.]ru
response-redir[.]com
safe-proof[.]com
sangrail-ltd[.]com
sangrail-share[.]com
selector-drafts[.]online
share-drive-ua[.]com
soaringeagle-drive[.]com
storage-service[.]online
threatcenterofreaserch[.]com
threatcenterofresearch[.]com
transfer-dns[.]com
transfer-record[.]com
umo-drive[.]com
umopl-drive[.]com
umopl[.]com
webview-service[.]com
```