Threat Research & Intelligence (https://blog.sekoia.io/category/threat-research/)

French NGO Reporters Without Borders targeted by Calisto in recent campaign

Sekoia TDR
December 3 2025

9 minutes reading

Some portions of this article were first distributed as a private report to our customers in June 2025.

In May and June 2025, TDR team analysts were contacted by two organisations — including the French NGO **Reporters Without Borders (RSF)** — over suspicions of a new spear phishing attempts by the intrusion set **Calisto** (also known as **ColdRiver** or **Star Blizzard**).

Calisto is a Russia-nexus intrusion set active since at least April 2017, attributed by the USA, the UK, New Zealand and Australia to the Russian intelligence service **FSB**, more specifically to the **Center 18 for Information Security** (TsIB), military unit 64829 (https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet), also known to operate the intrusion set Gamaredon. Sekoia.io concurs with such attribution as past Calisto operations investigated by TDR analyst showed (https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support/) objectives and victimology that align

closely with Russian strategic interests.

Calisto mainly conducts **cyber espionage operations**, targeting Western countries, especially Eastern European countries and any countries supporting Ukraine. The group was observed carrying out phishing campaigns aiming at credential theft and code execution using recently the ClickFix technique (https://attack.mitre.org/techniques/T1204/004/), 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 intelligence officials, experts in Russian matters, and Russian citizens abroad.

Calisto spear-phishing campaigns often involve the **impersonation of trusted contacts**, sending email either **forgetting the attachment**, or sending a dysfunctional yet benign PDF file, in order to trigger a response for the victim asking for a resend. We assess this technique is likely to increase the credibility of the exchange.

TDR analysts have been following Calisto TTPs and their C2 infrastructure tactics since 2022. We have published in 2022 an investigation (https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support/) showing that this group conducts intelligence collection activities targeting parties involved in Ukraine support, especially those in the tactical equipment logistics, probably to contribute to Russian efforts to disrupt Kiev supply-chain for military reinforcements.

Later, in 2023, we published (https://blog.sekoia.io/calisto-doxxing-sekoia-io-findings-concurs-to-reuters-investigation-on-fsb-related-andrey-korinets/) a follow-up investigation focusing on Andrei Korinets, a Russian individual whose name was disclosed (https://www.reuters.com/world/europe/russian-hackers-targeted-us-nuclear-scientists-2023-01-06/) by Reuters, who was likely registering phishing domains used previously by Calisto to conduct at least a phishing campaign targeting UK entities, including the British Parliament.

Reporters Without Borders targeting

On march 2025, TDR was contacted by the NGO **Reporters Without Borders** regarding a strange phishing email receveid by one of its core member. Reporters Without Borders is an international non-profit organisation that defends press freedom worldwide. It monitors violations against

journalists, provides support to reporters under threat, and advocates for free, independent, and pluralistic media. The organisation, which has assisted Russian journalists in fleeing the country, has been designated an “undesirable organisation” in Russia in august 2025 (https://rsf.org/fr/rsf-class%C3%A9e-organisation-ind%C3%A9sirable-en-russie-ou-le-droit-%C3%A0-l-information-consid%C3%A9r%C3%A9-comme-une).

As usual for Calisto, **the phishing email came from a ProtonMail address made to look like a trusted contact**. It asked the recipient to review a document, but no document was attached. This tactic, seen before in the Calisto credential-harvesting campaign, is meant to make the recipient ask for the missing file. The attacker can then send a “follow-up” document that contains the malicious payload.

Here is the email sent by the Calisto operator. As shown in the screenshot, the message is written in French and includes the proper signature of the trusted contact, but **the link to the PDF at the end of the document is not active**.

After the victim requested the document, the Calisto operator responded with another email — this time in English — containing **a link to a previously compromised website**, as shown below. The site acted as a **redirector** to a ProtonDrive URL that likely presented a malicious PDF to the user. However, the file itself could not be retrieved because ProtonMail had blocked the operator's account. It is worth mentioning that Proton Security is very cooperative regarding this kind of spear phishing operations that impersonate real persons belonging to NGOs.

Other targeting

We came aware of a second case against a second victim. This time, **the attacker did attach a file labeled as a PDF**. However, it was in fact a ZIP archive with a .pdf extension. Although not malicious, the file could not be opened as a PDF, furthering the deception of the victim.

Our contact was able to obtain the final PDF from the Calisto operators. The retrieved file is a

typical Calisto decoy: it displays **an icon and a message claiming that the PDF is encrypted**, instructing the user to click a link to open it in ProtonDrive. When the user clicks the link, they are first redirected to a Calisto redirector hosted on a compromised website, which then forwards them to the threat actor's phishing kit.

Example of typical Calisto PDFs leading to phishing webpages (from 2022)

Thanks to our contacts cooperation, **we've been able to detonate a phishing kit in a controlled environment**, allowing us to compare the differences between real and decoy protonmail webpages created by Calisto.

This redirector is a PHP script deployed on **compromised websites**, likely breached through credentials leaked by information stealers. In our case, the PHP file accepts a token passed as a `GET` parameter named `utm_refferer`, mimicking a standard Urchin Tracking Module (UTM) parameter. When the link is clicked, the user is redirected via JavaScript to the final webpage, as shown below.

Phishing kit analysis

The phishing kit we were able to analyze, hosted on `account.simpleasip[.]org`, was designed to target ProtonMail accounts. It appears to be a homemade kit, as we were unable to link any atomic indicators to known frameworks such as Evilginx. The kit can relay two-factor authentication and seems to employ an **Adversary-in-the-Middle (AiTM) technique**, allowing the threat actor to inject malicious JavaScript into the sign-in page.

Although we were unable to retrieve the server-side of this kit, the client-side code provides enough insight to understand its logic. When users are redirected to the login page, they are presented with a modified ProtonMail sign-in screen. **The username field is pre-filled with the victim's email address**, and malicious JavaScript is injected to keep the user's cursor focused on the password field. This forced focus runs every 250 milliseconds, meaning that if the victim clicks anywhere on the page, they are immediately redirected back to the password field.

Another, more complex JavaScript code is injected into the webpage. This code interacts with **an attacker-controlled API** hosted on another server but using the same second-level domain (`scorelikelygateway.simleasip[.]org`). This attacker-controlled API is used to process the credentials and acts as an **intermediary between the real ProtonMail authentication interface and the victim**. This is reminiscent of the two-factor authentication (2FA) phishing kit that APT28 used to target UKR.NET, which we wrote about a few years ago (http://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/).

Once the page is fully loaded, the injected JavaScript code defines the `ownershipSubmitCallback` method as a constant, which is called when the user submits the sign-in form. It then interacts with the attacker-controlled API to handle authentication, such as presenting the CAPTCHA or the 2FA form. It is worth mentioning that the JavaScript code also hijacks the GUI components of ProtonMail to present CAPTCHA/2FA modals or errors to the user during the authentication process.

As we mentioned earlier, this phishing kit seems to use the **Adversary-in-The-Middle (AiTM)** technique. However, during our investigation, we observed that the Webpack'ed JavaScript bundle on the phishing webpage (`public-index.7162a3fd.js`) differs from the one hosted on ProtonMail at the URL `hxxps://account.proton.me/assets/static/public-index.7162a3fd.js` . Even if both have the same name, the JavaScript present on the phishing webpage was patched at multiple places, to call, for example the `ownershipSubmitCallback` method.

Upon successful authentication, the JavaScript attempts to fetch the endpoint `/api/core/v4/events/latest` (a valid endpoint on ProtonMail) and then reloads the webpage. However, after successfully signing ourselves on the phishing webpage, the endpoint `/api/core/v4/events/latest` returned an Nginx 404 error, and all subsequent requests also resulted in 404 errors.

In spite of returning 404 errors on the phishing kit interface, the login attempt was successful on Protonmail, and we saw the IP address `196.44.117[.]196` accessing our decoy email account, as shown below. According to spur.us (https://app.spur.us/search?q=196.44.117.196) the `196.44.117[.]196` is associated with the **Big Mama Proxy** service.

Infrastructure analysis

As mentioned earlier, we identified two types of servers used by Calisto intrusion set during these recent attack campaigns: servers used to host phishing web pages, and others acting as API endpoints. It was possible, by using simple passive DNS analysis or service analysis, to identify domains used by this threat actor.

Most of the domain names used by Calisto rely on free authoritative servers from Namecheap (`freedns*.registrar-servers.com`) or on Namecheap's standard servers (`dns1.registrar-servers.com`). However, the domains used during Q1 and Q2 were initially registered through Regway. This change over time made it possible to track them, and can serve as an indicator to attribute these domain names to the Calisto threat actor with medium confidence.

Conclusion

Despite numerous publications on this threat actor, Calisto continues its spear-phishing campaigns for **credential harvesting** or **code execution** via the ClickFix technique. It targets a wide range of entities supporting Ukraine, including organisations previously targeted, in line with Calisto's historically observed TTPs.

Therefore, if you are an NGO involved in Ukraine, or an individual or researcher with intelligence on this conflict and partnering with Ukrainian bodies, **you are possibly one of the targets of this threat actor.** We are at the disposal of any NGO wishing to analyse and/or attribute attack campaigns to a cluster of activity.

Thank you for reading this blog post. Please don't hesitate to provide your feedback on our publications by clicking here (https://framaforms.org/sekoiaio-blogposts-feedback-1721899427). You can also contact us at tdr[at]sekoia.io for further discussions or future IOCs.

IOCs

Known redirector URLs:

```
hxxps://admin.artemood[.]com/vendor/plugx/*.php
hxxps://mbtalcpa[.]com/wp-content/plugins/bungs/*.php
hxxps://esclerosemultiplario[.]com.br/wp-content/plugins/areada/*.php
hxxps://myoseguridad[.]net/prueba/phantomrise/*.php
hxxps://esourcesol[.]com/wp-content/plugins/leykos/*.php
hxxps://cranium[.]id/plugins/unite/*.php
```

Domains used in recent Calisto campaigns, non exhaustive list. Note that some of them are already Sinkholed by MSTIC.

sopatrasoftware[.]net
setingfont[.]com
ageyehoo[.]com
doggiewalkietalkie[.]company
napsubrow[.]com
collappendrow[.]net
acmathj[.]org
partizan-cryptobox[.]com
drivenginfra[.]com
proton-decrypt[.]com
astrocosmograv[.]com
bridgevisionassetmanagement[.]net
sysgentuore[.]com
enepascm[.]net
cloudmediaportal[.]com
addnamestamp[.]net
agentsbreakcursor[.]org
agilegapvalue[.]com
applicationformsubmit[.]me
argosurflooms[.]com
atheismatoninoosers[.]net
baayaygnu[.]com
biochemsys[.]org
bridgevisionassets[.]net
ceehogrho[.]org
checkshowlabel[.]org
classmechthermo[.]com
cowsetmom[.]com
documentsec[.]com
fohmaspub[.]org
forcelistcon[.]com
gemtarfad[.]com
gymaisbad[.]org
harmenganaleng[.]com
inkwaxmil[.]com
inmeoaf[.]com
jamyexraw[.]com
kwargsdirgrid[.]com
lamiderot[.]eu
layoutdatatype[.]org
leaseselfid[.]com
lekgodmop[.]com

levtawrig[.]eu
logmanzoo[.]com
maddeehot[.]online
mainboxtype[.]net
mapaji[.]com
menustatusbar[.]org
midemucoped[.]org
mobtuxawe[.]org
mofamole[.]com
ned-application-proposal[.]org
ned-granting-opportunitis[.]org
ned-granting-potential[.]com
netyintry[.]com
nextgenscloud[.]com
noonevinedreammer[.]org
objectwidgetfont[.]org
onlineviewdoc[.]com
ovaradiumnon[.]org
owntrywad[.]com
parkcaprigra[.]com
pietabyew[.]org
prostaffcover[.]org
psybehavconf[.]com
raxpoprig[.]org
reftospy[.]com
requestspatchcopy[.]net
returnselfdata[.]net
saghughap[.]com
sendhostargs[.]com
setproxytrue[.]net
simleasip[.]org
sizarebabrhino[.]org
slacksfulgurbairn[.]org
sobcozsee[.]com
soborsshe[.]com
socalstrategy[.]info
towegospa[.]com
trekpoofedbange[.]org
tryledsox[.]com
tucklocsqueal[.]org
weblangdata[.]com
yenmaways[.]com

APT (https://blog.sekoia.io/tag/apt/)

coldriver (https://blog.sekoia.io/tag/coldriver/)

phishing (https://blog.sekoia.io/tag/phishing/)

Sekoia TDR

TDR is the Sekoia Threat Detection & Research team. Created in 2020, TDR provides exclusive Threat Intelligence, including fresh and contextualised IOCs and threat reports for the Sekoia SOC Platform TDR is also responsible for producing detection materials through a built-in Sigma, Sigma Correlation and Anomaly rules catalogue. TDR is a team of multidisciplinary and passionate cybersecurity experts, including security researchers, detection engineers, reverse engineers, and technical and strategic threat intelligence analysts. Threat Intelligence analysts and researchers are looking at state-sponsored & cybercrime threats from a strategic to a technical perspective to track, hunt and detect adversaries. Detection engineers focus on creating and maintaining high-quality detection rules to detect the TTPs most widely exploited by adversaries. TDR experts regularly share their analysis and discoveries with the community through our research blog, GitHub repository or X / Twitter account. You may also come across some of our analysts and experts at international conferences (such as BotConf, Virus Bulletin, CoRIIN and many others), where they present the results of their research work and investigations.

Share this post:

What's next

Advent of Configuration Extraction – Part 2: Unwrapping QuasarRAT's Configuration (https://blog.sekoia.io/advent-of-configuration-extraction-part-2-unwrapping-quasarrats-configuration/)

In the second part of our "Advent of Configuration Extraction" series, we unwrap QuasarRAT, a popular .NET remote access...

(https://blog.sekoia.io/advent-of-configuration-extraction-part-2-unwrapping-quasarrats-configuration/)

Jeremy Scion, Pierre Le Bourhis and Sekoia TDR

Mandating Security by Design: Sekoia's Blueprint for the EU Cyber Resilience Act (https://blog.sekoia.io/mandating-security-by-design-sekoias-blueprint-for-the-eu-cyber-resilience-act/)

Arnaud Dechoux and Maxime Arandel

(https://blog.sekoia.io/)

ut-bord ers-targe ted-by-calist o-in-recen t-cam paig n/)

out%20Bor ders%20t arget ed%20 0by%20Ca listo%20i n%20 recen t%20 cam paig n)

ut-bord ers-targe ted-by-calist o-in-recen t-cam paig n/)

ed%20 0by%20Ca listo%20i n%20 recen t%20 cam paig n)

ted%20by %20C alisto%20i n%20 recen t%20 cam paig n%0D %0ASome%20p ortio ns%20 0of%2 0thi s%20 articl e%20 were %20fi rst%2 0dist ribut ed%2 0as% 20a% 20pri vate %20r eport %20t

o%20our%20customers%20in%20June%202020.%20In%20May%20and%20June%2025,%20TDR%20team%20analysts%20were%20contacted%20by%20two%20organa

(https://blog.sekoia.io/)

nisati
ons%
20%E
2%80
%94
%20i
nclud
ing%
20the
%20F
renc
h%20
NGO
%20R
eport
ers%
20Wit
hout
%20B
order
s%20
%28R
SF%2
9%20
%E2%
80%9
4%20
over
%20s
uspic
ions
%20o
f%20
a%20

(https://blog.sekoia.io/)

new%20spear%20phishing%20attempts%20by%20the%20international%20set%20Calisto%20%20%28also%20%5B%26hellip%3B%5D%0D%0A%0D%0ARead%20more%20at%3A%20http

sekoias-blueprint-for-the-eu-cyber-resilience-act/)

Introduction The European Union (EU) continues to solidify its cybersecurity landscape through ambitious, horizontal regulations. In addition to the...

(https://blog.sekoia.io/advent-of-configuration-extraction-part-3-mapping-got-plt-and-disassembling-the-snowlight-loader/)

Advent of Configuration Extraction – Part 3: Mapping GOT/PLT and Disassembling the SNOWLIGHT Loader (https://blog.sekoia.io/advent-of-configuration-extraction-part-3-mapping-got-plt-and-disassembling-the-snowlight-loader/)

In-depth analysis of the Snowlight malware loader, focusing on GOT/PLT mapping and ELF disassembly for configuration extraction.

Jeremy Scion, Pierre Le Bourhis and Sekoia TDR

Comments are closed.

Trending topics

(https://blog.sekoia.io/tag/malware/)

Malware (https://blog.sekoia.io/tag/malware/)

(https://blog.sekoia.io/)

(https://blog.sekoia.io/tag/detection/)

Detection (https://blog.sekoia.io/tag/detection/)

(https://blog.sekoia.io/tag/soc/)

SOC (https://blog.sekoia.io/tag/soc/)

About us

This blog is your trusted source for cutting-edge insights in CTI and SOC. Curated by the Threat Detection & Research team (https://www.sekoia.io/en/about-threat-detection-research-team/) and other experts at Sekoia.io, it is dedicated to empowering cybersecurity professionals, researchers, and enthusiasts with actionable intelligence and industry-leading expertise.
Our mission is simple: to keep you informed, prepared, and empowered in an ever-evolving cyber

Tags

7777 botnet (https://blog.sekoia.io/tag/7777-botnet/) APT (https://blog.sekoia.io/tag/apt/) APT28 (https://blog.sekoia.io/tag/apt28/) AWS (https://blog.sekoia.io/tag/aws/) Botnet (https://blog.sekoia.io/tag/botnet/) calisto (https://blog.sekoia.io/tag/calisto/) China (https://blog.sekoia.io/tag/china/) Cloud (https://blog.sekoia.io/tag/cloud/) Compliance (https://blog.sekoia.io/tag/compliance/) CTI (https://

Categories

Detection Engineering (https://blog.sekoia.io/category/detection-engineering/)

Product News (https://blog.sekoia.io/category/product-news/)

SOC Insights & Other News (https://blog.sekoia.io/category/soc-insights-other-news/)

Threat Research & Intelligence (https://blog.sekoia.io/category/threat-research/)

threat landscape.

(https://blog.sekoia.io/)

blog.sekoia.io/tag/cti/) Cybercrime (https://blog.sekoia.io/tag/cybercrime/) Cybersecurity (https://blog.sekoia.io/tag/cybersecurity/) Dark Web (https://blog.sekoia.io/tag/dark-web/) DDoS (https://blog.sekoia.io/tag/ddos/) Detection (https://blog.sekoia.io/tag/detection/) Detection Engineering (https://blog.sekoia.io/tag/detection-engineering/) DFIR (https://blog.sekoia.io/tag/dfir/) Ecosystem (https://blog.sekoia.io/tag/ecosystem/) EU (https://blog.sekoia.io/tag/eu/) Features (https://blog.sekoia.io/tag/features/) Hackaton (https://blog.sekoia.io/tag/hackaton/) Hacktivism (https://blog.sekoia.io/tag/hacktivism/) Influence (https://blog.sekoia.io/tag/influence/) Infrastructure (https://blog.sekoia.io/tag/

(https://blog.sekoia.io/)

infrastructure/) Integration (https://blog.sekoia.io/tag/integration/) Iran (https://blog.sekoia.io/tag/iran/) Legislation (https://blog.sekoia.io/tag/legislation/) Loader (https://blog.sekoia.io/tag/loader/) Malware (https://blog.sekoia.io/tag/malware/) MSSP (https://blog.sekoia.io/tag/mssp/) Paris2024 (https://blog.sekoia.io/tag/paris2024/) phishing (https://blog.sekoia.io/tag/phishing/) plugx (https://blog.sekoia.io/tag/plugx/) Predator (https://blog.sekoia.io/tag/predator/) Quad7 botnet (https://blog.sekoia.io/tag/quad7-botnet/) Ransomware (https://blog.sekoia.io/tag/ransomware/) Reverse (https://blog.sekoia.io/tag/reverse/) russia (https://blog.sekoia.io/tag/russia/) Sigma (https://blog.sekoia.io/tag/sigma/) SOC (https://blog.sekoia.io/tag/soc/) SOC platform (https://blog.sekoia.io/tag/soc-platform/) Stealer (https://blog.sekoia.io/tag/stealer/) Strategic

(https://blog.sekoia.io/tag/strategic/) ukraine (https://blog.sekoia.io/tag/ukraine/)

XDR (https://blog.sekoia.io/tag/xdr/)

(https://blog.sekoia.io/)