CALISTO doxxing: Sekoia.io findings concurs to Reuters' investigation on FSB-related Andrey Korinets

By Sekoia TDR

Published: 2023-12-13 · Archived: 2026-04-05 15:02:32 UTC

Investigation context

On 7 December 2023, a joint advisory from the UK, USA, Canada, Australia and New Zealand attributed the previously known intrusion set Star Blizzard (aka CALISTO for Sekoia.io) to Russian Federal Security Bureau (FSB). The USA and UK government announced sanctions against two Russian nationals, **Ruslan Peretyatko** and **Andrey Korinets**, accused to be actively involved into CALISTO operations.

One year ago, on 6 January 2023, Sekoia.io distributed to our customers a FLINT (Flash Intelligence report) about our findings on Andrey Korinets. This investigation began when a trusted source contacted Sekoia.io TDR analysts regarding our previous publication on CALISTO, informing us about a possible link between a known infrastructure used by CALISTO and Andrey Korinets.

Sekoia.io conducted further technical investigation that confirmed **an existing relation from at least 2015 to 2020 between CALISTO and Korinets**. In order to avoid doxxing activities, we restained from publishing this investigation. Then, when Reuters published about Andrey Korinet, we sent our investigation to our CTI customers.

With this CALISTO follow-up FLINT, we wanted to share our investigation that disclose links between **Korinets activities** and **a large technical cluster** composed of dozens of CALISTO phishing domains and multiple servers, including some exposed by F-Secure(1) in 2017 in a white paper on "Callisto Group".

We are now publishing our technical investigation that concurs Reuters' and the UK-USA's designation of Andrey Korinet.

An investigation based on Korinets' emails

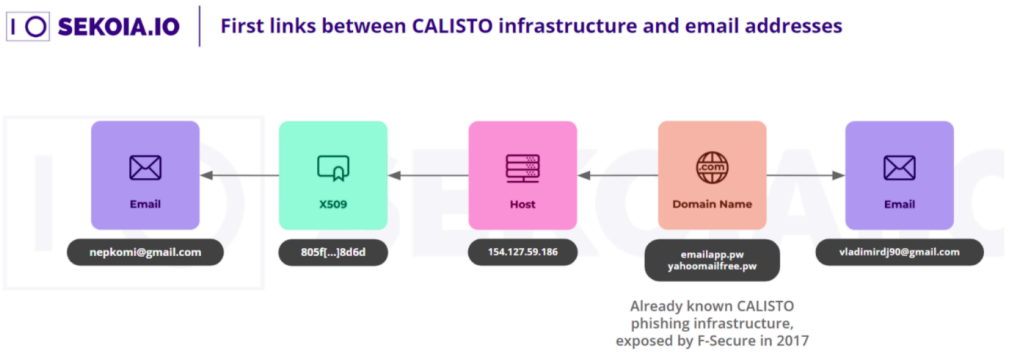
Following the intelligence on Korinets provided by a trusted source, SEKOIA.IO conducted research on a former CALISTO infrastructure, allowing us to identify several email addresses used by Andrey Korinets associated with it.

This former CALISTO infrastructure was used to conduct phishing campaigns from at least 2015 and up to 2020, when new domains were allegedly used to target several Ukrainian and **United Kingdom entities,** such as the **British Parliament** and the Cambridge University.

Emails associated with Korinets can be retrieved in historical WHOIS records and SSL certificates associated with CALISTO infrastructure. It is worth mentioning that the same infrastructure was also used by

Korinets to host his own websites, including online shops selling steroids, which matches its personal interests as described in Reuters' article.

According to our contact, two email addresses (nepkomi@gmail[.]com and yuuuka333@gmail[.]com) were allegedly owned and used by Korinets.
SEKOIA.IO identified a **technical link** that **connects** the nepkomi@gmail[.]com to a **known CALISTO phishing server** (154.127.59[.]186) and another email address.



Email : vladimirdj90@gmail[.]com

In addition to the previous technical link with Korinets' email address as shown above, we were able to find a second connection with vladimirdj90@gmail[.]com through a US public procedure related to TopCoin, a former and now shutdown crypto currency blockchain, accessible in open sources.

Google result associating Korinets to vladimirdj90@gmail[.]com

Pivoting on this email, we were able to find an **associated self-signed Vesta Control Panel SSL certificate** (e7b0[…]168e), hosted on the IP address 86.110.117[.]172. This IP was resolved by the domains shared-docs[.]download and eu-office365[.]co which present the **same pattern** as **recent CALISTO domains** such as eu-office365[.]com, **registered** under the name "ANDREY Korinets" based on an historical WHOIS record.

Our investigation showed that vladimirdj90@gmail[.]com is also present in the WHOIS records of several domains linked to the **sale** of **anabolic** and **steroids**, a Korinets personal interest, **known CALISTO phishing domains**, as well as a possibly other **phishing-related domains** such as:

```
qooqle-support-mail[.]pw *
emailapp[.]pw *
yahoomailfree[.]pw *
support-gmail[.]pw *
```

```
live-login[.]info *
google-plus[.]top *
gmail-techdoc[.]pw
login-live[.]review *
support-mail[.]top *
ukrnet[.]pw
```

Note: Domains associated in open sources with former CALISTO activities have an asterisk.

Email : sykt.support@gmail[.]com

It is worth noting that the previous phishing-related domains were also related to the email address sykt.support@gmail[.]com, sykt standing for “Syktyvkar”, the Komi Republic capital from where Korinets is assessed to originate from. An individual with this email address shares the same city and password with another profile linked to the email yuuuka333@gmail[.]com in a Russian social network dump, therefore SEKOIA.IO analysts associate sykt.support@gmail[.]com to Andrey Korinets with medium confidence.

Based on historical WHOIS database, this email is linked to 36 domains, several looking like phishing domains, such as:

```
node03-prevention-icloud[.]link *
node005-prevention-aol[.]link *
support-mail[.]top *
authentification-request[.]top *
yahoo2-srv[.]bid
yahoo-user[.]bid
secure-icloud[.]accountant
login-access[.]top *
gmail-techdoc[.]pw
secure-store-lcloud[.]top *
prevention-aol[.]top
auth-login[.]top *
hghshop[.]top
platforma[.]link *
screenname[.]click *
google-plus[.]top *
support-gmail[.]pw *
yahoomailfree[.]pw
emailapp[.]pw *
qooqle-support-mail[.]pw
live-login[.]info *
login-live[.]review *
ukrnet[.]pw
musclepharm[.]top
```

Note: Domains associated in open sources with former CALISTO activities have an asterisk.

Email : settings.personal@gmail[.]com

Three of the previously mentioned phishing domain names (ukrnet[.]pw, support-gmail[.]pw, qooqle-support-mail[.]pw) resolved the IP address 37.1.206[.]114, which was resolved at the same time by another domain name linked to another email address, namely icloud-service[.]pw and settings.personal@gmail[.]com. That last email settings.personal@gmail[.]com was used from 2014 to 2017 for **anabolic-related** and **phishing domains**:

```
anabol[.]in
yahoocentermail[.]info *
login-live-com[.]pw *
ukroboronprom[.]pw
icloud-service[.]pw *
screenname-aol[.]pw *
massa[.]pw
accounts-mail[.]asia *
service-mail[.]asia *
```

Note: Domains associated in open sources with former CALISTO activities have an asterisk.

In this domain list, it is interesting to point ukroboronprom[.]pw, which **typosquats Ukroboronprom (Укроборонпром)**, a **conglomerate of Ukrainian defense industries**. This domain is the first associated with a potential high profile targeting originating from this infrastructure cluster.

Another interesting domain name is screenname-aol[.]pw, which was resolving the IP address 139.162.145[.]184, resolved by several domains associated to Korinets online steroids shop activities based on their historical WHOIS records, such as muscle[.]ovh and ukrpharma[.]ovh.

```
Registrant Name: Korinets Andrey
Registrant Street: muscle.ovh, office #8930945
Registrant Street: c/o Owo, Bp80157
Registrant City: Roubaix Cedex 1
Registrant Postal Code: 59053
Registrant Country: FR
Registrant Phone: +33.899498765
Registrant Email: y8j4po1ih74l9akzmkq8@r.o-w-o.info
```

Infrastructure pivoting allowed us to swing from 139.162.145[.]184 to 95.213.194[.]163, both resolved the previously mentioned musclepharm[.]top, which brings us to another phishing domain drive-meet-goodle[.]ru.

Email: usa42014@yandex[.]ru

The previous IP addresses 139.162.145[.]184 and 95.213.194[.]163 have two distinct self-signed SSL certificates (0641[…]2299 – associated to the domain musclepharm[.]top and d68c[…]7393 – associated to the domain drive-meet-goodle[.]ru), both containing the email address usa42014@yandex[.]ru.

SEKOIA.IO analysts link the email address usa42014@yandex[.]ru to Andrey Korinets activities with medium confidence as this email replaced the email yuuuka333@gmail[.]com in the WHOIS record of be-strong[.]org. **drive-meet-goodle[.]ru is one of the IoCs published by F-Secure in 2017.**

Four other certificates show ties with usa42014@yandex[.]ru. A first Vesta control panel self signed certificate (8efb[…]a7f4) is associated with the already-listed domain live-login[.]info. It was present on the IP address 185.72.179[.]132, resolved by live-login[.]info between 2015-12-19 and 2016-03-25.

A second certificate (994a[…]1c30) is associated with the domain name expert-service[.]tech and was present on the IP address 185.212.128[.]28. This IP address was resolved between 2019-01-10 and 2019-11-04 by two domains looking like phishing domains, such as yamail[.]press and drive-aoi[.]icu.

A third certificate (d3f1[…]593c) linked to usa42014@yandex[.]ru was on the IP addresses 158.69.149[.]52 and 185.99.134[.]22, both resolved by several phishing domains in 2019, such as:

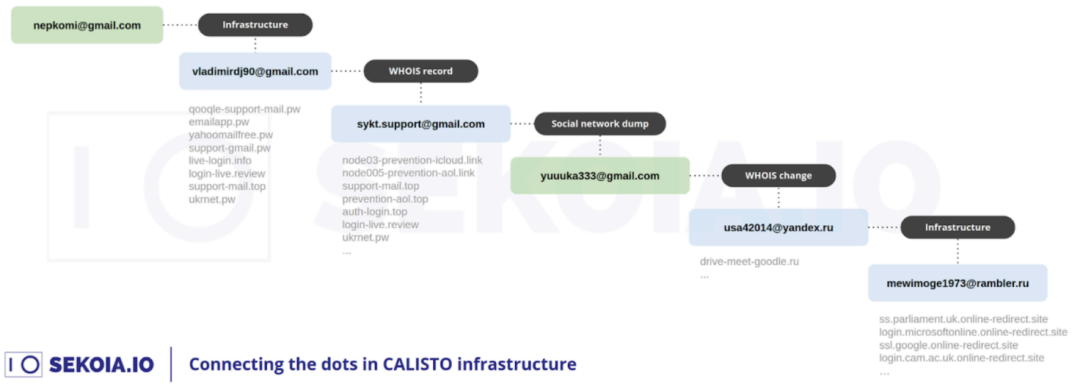
```
office-356pro[.]pw
en-office365[.]club
file-sharing[.]online
file-sharing[.]site
en-microsofl[.]live
online-1drv[.]world
```

Email: mewimoge1973@rambler[.]ru

The email address mewimoge1973@rambler[.]ru is quite interesting as it is associated to another certificate (fd21[…]3b61) linked to the IP address 95.171.17[.]36 and the domain name serv[.]safe-redirect[.]in.net. The IP address 95.171.17[.]36 was resolved in 2020 by two domain names (safe-redirect[.]in.net, online-redirect[.]site), and dozens of their subdomains, **targeting onlines services** as well as the **UK Parliament** and the **Cambridge University**.

Only a little information from open source can link the email address mewimoge1973@rambler[.]ru to a clear identity. This email address is present on several Russian offers websites in the Komi region of which Korinets is assessed to originate from, but without a good visibility on the real owner identity.

Korinets, a simple hoster or more than that?



With this infrastructure investigation, we demonstrated that a Russian individual, whose name was disclosed by Reuters, did in fact register phishing domains used by the CALISTO intrusion set to conduct at least a phishing campaign targeting UK entities, including the Parliament.

As we described in our last blogpost, **SEKOIA.IO assess that CALISTO contributes to Russian intelligence efforts** to support **Moscow's strategic interests**, as now confirmed by western intelligence services.

Questions now arise whether Korinets knew he was colluding with Calisto operators and/or with Russian intelligence. If so, his precise role remains unclear as SEKOIA.IO does not have technical evidence to assess it.

Based on open source information we could gather about that individual, it seems that **domain registration** was one of its main skills, plausibly **used by Russian intelligence**, either directly or through a contractor relationship.

Korinets – CALISTO relation may have ended in 2020, as SEKOIA.IO did not find any technical links afterwards. This may as well be due to a lack of visibility.

All indicators found during our investigation are available on our public Github page.

External references

[1] https://www.f-secure.com/content/dam/f-secure/en/labs/whitepapers/Callisto_Group.pdf. Accessed on 13th december, 2023.

Thank you for reading this blogpost. **We welcome any reaction, feedback or critics about this analysis. Please contact us on tdr[at]sekoia.io**.

Feel free to read other TDR analysis here :

APT calisto FSB Korinets Star Blizzard

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:
