Blue Callisto orbits around US Laboratories in 2022

pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html

Blue Callisto (a.k.a SEABORGIUM[1], Callisto Group[2]) is likely a Russia-based threat actor which primarily conducts phishing attacks for espionage purposes since at least 2017. The threat actor is interested in acquiring credentials from US and European government officials and organisations linked to national security matters. In 2017 it was reported that the threat actor targeted the UK foreign office,[3] and we have also observed its interest in UK and US universities in 2020 and 2022.[4] Since the Russo-Ukraine war began in 2022, we have observed Blue Callisto taking an increased interest in Ukraine, targeting at least one private Ukrainian company related to logistics. We assess Blue Callisto is highly likely still primarily focused on governmental organisations based in Europe and the US.

In this blog post we detail 2022 phishing activity the PwC threat intelligence team attributes to Blue Callisto and list indicators for defenders to query. The activity ranges from February 2022 to October 2022. Some of the domains resolve to IPs which we assess are likely operated by Blue Callisto to service fake webpages and gather credentials as of 24th October 2022.

Fingerprinting activity

In February 2022, we observed a domain we attribute likely to Blue Callisto redirecting to a different domain, which we also assess is likely Blue Callisto due to the similarities in technologies, network providers and infrastructure setup.[5] When visiting the domain cache-dns-forwarding[.]com a user is redirected to accounts[.]hypertexttech[.]com due to a remote script shown in **Figure 1.** The remote script was located on hypertextteches[.]com.

Figure 1 – Javascript code link observed on cache-dns-forwarding[.]com

The web response from the remote script was obfuscated JavaScript code created by a popular JavaScript obfuscator[6], which uses a combination of the following characters: ![ ]() as shown in **Figure 2.**

Figure 2 – Obfuscated JavaScript code

The deobfuscated code contains multiple client side checks, shown in **Figure 3,** to determine whether the request should be redirected or not. We assess it is likely the threat actor is using this code to identify automated scanners and antivirus technologies, and block them from the final phishing URL. The code queries several browser constants, such as:

- window.webdriver;
- window.domAutomation; and,
- window.spawn.

If the code does not identify any problems with the request the script will redirect to the following URL:

hxxps[:]//hypertextteches[.]com/patrified.php

Figure 3 – Deobfuscated code

Microsoft referenced Blue Callisto fingerprinting browser behaviour in one of its public blogs[7]. We assess the fingerprinting Javascript methods and code is likely similar to the deobfuscated code we have observed. The JavaScript code redirect has several further redirections before reaching its final URL: a Google themed phishing page shown in **Figure 4**. An example redirection chain is listed below:

- hxxps[:]//hypertextteches[.]com/patrified.php;
- hxxps[:]//accounts[.]hypertexttech[.]com/oOzMeNTe?FtC=DLOJmne17BQw5JRQ74YDgmHxR52d0Ng
- hxxps[:]//accounts[.]hypertexttech[.]com/signin/v2/identifier?passive=1209600&continue=https%3A%2F%2Faccounts[.]google[.]com%2F&followup=https%3A%2F%2Faccounts[.]google[.]com%2F&flowName=GlifWebSignIn&flowEntry=ServiceLogin
- hxxps[:]//accounts[.]hypertexttech[.]com/ServiceLogin?continue=https%3A%2F%2Faccounts[.]google[.]com%2F&flowEntry=ServiceLogin&flowName=GlifWebSignIn&followup=https%3A%2F%2Faccounts[.]google[.]com%2F&passive=1209600

Figure 4 – Google themed phishing page

The phishing page contains an email address that we assess is likely used by Blue Callisto for testing. The page statically sets the email address value to tr333lopex as shown in **Figure 5**.

Figure 5 – Statically set email observed in code

US National Labs interest

Blue Callisto often inputs emails of interest statically into form input fields. In one of these instances, we observed phishing activity spoofing US National Laboratories in July 2022. Specifically, on 12th June 2022 we observed the domain registration goo-ink[.]online, which resolved to 89.147.108[.]182 from 25th July 2022 (which we assess is phishing infrastructure used by Blue Callisto). The goo-ink[.]online domain contained a Brookhaven National Laboratory phishing page, statically setting a Brookhaven Lab email in the input form field as shown in **Figure 6**. The email address of interest observed on the phishing page is linked to non-proliferation and accountability initiatives for nuclear materials in Russia and elsewhere. During this phishing activity we also observed interest by Blue Callisto in Lawrence Livermore National Laboratory based on URLs we observed on goo-ink[.]online.

Figure 6 – Brookhaven National Laboratory phishing page

In August 2022, Microsoft reported on Blue Callisto infrastructure that they had taken action against,[8] including the domain goo-link[.]online. This domain was registered on 21st April 2022 and started to resolve to the IP address 93.95.227[.]41 on 22nd April 2022, and which was used for phishing activity. A list of attributes with some comparison of server features and headers is shown in **Table 1**. We assess both domains are likely Blue Callisto activity.

	goo-link[.]online	goo-ink[.]online

Registrar	Hostinger	Hostinger
Server Technology	Apache 2.4.37	Apache 2.4.37
Server Technology	OpenSSL 1.1.1k	OpenSSL 1.1.1k
IP resolution	93.95.227[.]41	89.147.108[.]182
IPs ASN	1984-Ehf (AS44925)	1984-Ehf (AS44925)
Observations	Phishing	Phishing

Table 1 - Domain attributes and links

Conclusion

Despite limited observations of broad activity, Blue Callisto is highly likely to remain active. In October 2022, we observed the threat actor is interested in an organisation which investigates war crimes; motives that would broadly align with a Russia-based threat group's collection objectives. The threat actor's tools, techniques and procedures (TTPs) contained slight shifts during 2022, such as network provider preferences and use of phishing technologies such as Evilginx. However, the threat actor continues to use some TTPs observed as far back as 2019 and continues to enjoy success from its phishing activity using legacy tradecraft.

Indicators of Compromise

Indicator	**Type**
cache-dns-forwarding[.]com	Domain
accounts[.]hypertexttech[.]com	Domain
hypertextteches[.]com	Domain
goo-link[.]online	Domain
goo-ink[.]online	Domain
hxxps[:]//hypertextteches[.]com/patrified.php	URL
hxxps[:]//accounts[.]hypertexttech[.]com/oOzMeNTe?FtC=DLOJmne17BQw5JRQ74YDgmHxR52d0Ng	URL
hxxps[:]//accounts[.]hypertexttech[.]com/signin/v2/identifier?passive=1209600&continue=https%3A%2F%2Faccounts[.]google[.]com%2F&followup=https%3A%2F%2Faccounts[.]google[.]com%2F&flowName=GlifWebSignIn&flowEntry=ServiceLogin	URL
hxxps[:]//accounts[.]hypertexttech[.]com/ServiceLogin?continue=https%3A%2F%2Faccounts[.]google[.]com%2F&flowEntry=ServiceLogin&flowName=GlifWebSignIn&followup=https%3A%2F%2Faccounts[.]google[.]com%2F&passive=1209600 URL	URL

93.95.227[.]41	IPv4 Address
89.147.108[.]182	IPv4 Address
92.38.169[.]241	IPv4 Address
138.124.187[.]128	IPv4 Address
185.164.172[.]128	IPv4 Address
37.9.35[.]62	IPv4 Address
92.38.176[.]66	IPv4 Address

MITRE ATT&CK

Phishing: Spearphishing Link - https://attack.mitre.org/techniques/T1566/002/Command and

Scripting Interpreter: JavaScript - https://attack.mitre.org/techniques/T1059/007/

Deobfuscate/Decode Files or Information - https://attack.mitre.org/techniques/T1140/

System Information Discovery - https://attack.mitre.org/techniques/T1082/

Footnotes

[1] 'Disrupting SEABORGIUM's ongoing phishing operations', Microsoft, https://www.microsoft.com/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/ (15th August 2022)

[2] Callisto Group, F-Secure, https://www.f-secure.com/content/dam/f-secure/en/labs/whitepapers/Callisto_Group.pdf (n.d)

[3] 'Callisto Group hackers targeted Foreign Office data', BBC News, https://www.bbc.co.uk/news/technology-39588703 (13th April 2017)

[4] *CTO-TIB-20200820-01A - Callisto targets UK Government and Universities*

[5] *CTO-TIB-20220511-01A - Tracking Callisto infrastructure*

[6] JSFuck, JSFuck, http://www.jsfuck.com/

[8] 'Disrupting SEABORGIUM's ongoing phishing operations', Microsoft, https://www.microsoft.com/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/ (15th August 2022)

[9] 'Disrupting SEABORGIUM's ongoing phishing operations', Microsoft, https://www.microsoft.com/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/ (15th August 2022)

We welcome your comments

Your request / feedback has been routed to the appropriate person. Should you need to reference this in the future we have assigned it the **reference number "refID"** .

Thank you for your comments / suggestions.

Required fields are marked with an asterisk(*)

Please correct the errors and send your information again.

By submitting your email address, you acknowledge that you have read the Privacy Statement and that you consent to our processing data in accordance with the Privacy Statement (including international transfers). If you change your mind at any time about wishing to receive the information from us, you can send us an email message using the Contact Us page.

Hide