Technical Report

on

Callisto Threat Actor Group

By Israel Okezie Ozomagbo

Executive Summary

The Callisto Group is an advanced Persistent Threat(APT) actor whose known targets include military organizations, government agencies, think tanks, NGOs, academic institutions, and individuals involved in security and foreign policy affairs, particularly those supporting Ukraine and NATO countries.

The Callisto group operations are known for using persistent credential-phishing, impersonation campaigns, and use of custom-built malware, occasionally leveraging leaked surveillance tools. They are state sponsored and believed to align with Russia, and their focus is on long-term intelligence(related to Eastern Europe and South Caucasus regions) collection rather than financial gain or destructive activity.

Recent law enforcement actions by Microsoft and the U.S. Department of Justice (DOJ) in 2024–2025 disrupted over 100 domains used by the group for spear-phishing, signalling active and continuing operations despite global pressure.

Our investigation conducted on the group yielded a comprehensive information to adequately profile this threat actor group against new and future attacks, understanding its modus operandi and techniques, has enabled CERT to recommend pre-emptive mitigation to detect, contain, and remove this wave of attacks going into the future.

Table of Content

1.Introduction

Callisto is an advanced threat actor group whose primary purpose appears to be intelligence gathering related to European foreign and security policies. This threat actor group has launched consistent credential phishing campaigns, targeting several US based NGOs and think tanks, the military of a Balkans country, and a Ukraine based defence contractor.

This report focuses on describing activities gathered from MISP through docker compose on kali, extracting the real world feeds based on their recent on their activities., and collaborating these findings on MITRE ATT&CK and Cisco Talos platform gives a full picture of the groups profile

investigation to adequately profile the group, IOCs, TTP, techniques employed, malware, domains used for operation, IP addresses, file

hashes, pattern, geographical location and its technical capabilities.

2.Objectives

There has been a very worrisome increase in malicious activities targeting critical infrastructures and government agencies in Europe. As a member of the CERT(Computer Emergency Response Team),we have been mandated to carry out a threat intelligence analysis on Callisto as this was suspected to be the threat actors behind the attacks.

This project is aimed at investigating the suspected threat actor groups Callisto, identifying their attack infrastructure,analyze to investigate, using real-world intelligence feeds from MISP. Your job is to identify their attack infrastructure, analyse associated Indicators of Compromise (IOCs), and build a threat profile to advise local organizations on potential risks.

3.Methodology

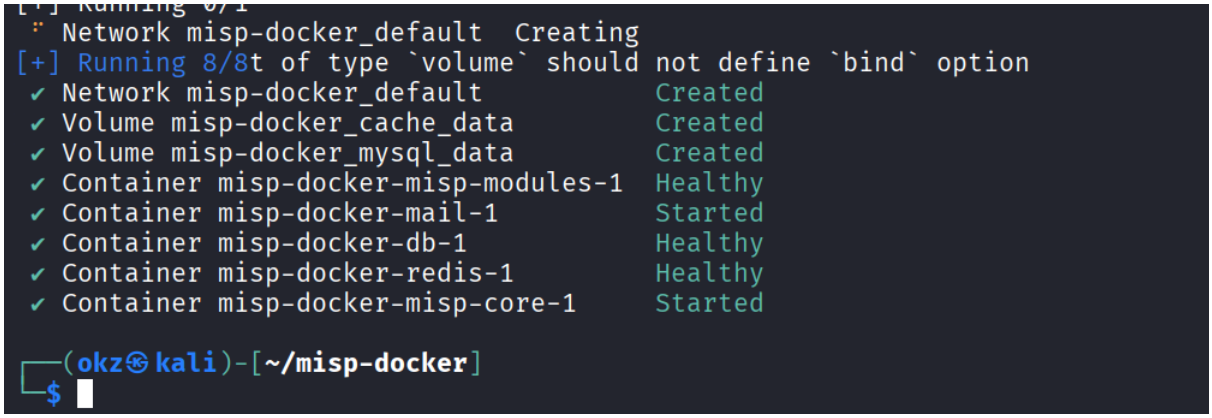
We installed a docker compose to run a real-world intelligence feeds from MISP in a containerized environment on kali Linux. This helped the team to aggregate necessary information on the threat actors group.

The enable feeds and event lists provide UUID that is associated with Callisto

UUID fbd279ab-c095-48dc-ba48-4bece3dd5b0f

With the UUID, we were able to search for the attributes**.**

Screenshot showing The dockers containerized MISP pull



4.Outcomes

After adding some filters for a better results ,the following metadata were gathered from the events list on MISP, to provide valuable insight on the threat actor under review.

Threat Actor :: Callisto

Cluster ID	28917
Name	Callisto
Parent Galaxy	Threat Actor
Description	The Callisto Group is an advanced threat actor whose known targets include military personnel, government officials, think tanks, and journalists in Europe and the South Caucasus. Their primary interest appears to be gathering intelligence related to foreign and security policy in the Eastern Europe and South Caucasus regions.
Default	Yes
Version	335
UUID	fbd279ab-c095-48dc-ba48-4bece3dd5b0f
Collection UUID	7cdff317-a673-4474-84ec-4f1754947823
Source	MISP Project
Authors	Alexandre Dulaunoy, Florian Roth, Thomas Schreck, Timo Steffens, Various
Distribution	All communities
Owner Organisation	MISP
Creator Organisation	MISP
Connector tag	misp-galaxy:threat-actor="Callisto"
Events	2 events
Attributes	80 attributes

Filters: All: Callisto | My Events | Org Events | Callisto | All fields | Filter

Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
CUDESO		456	Microsoft Activity Group actor Star Blizzard Threat Actor Callisto Sector Academia - University Government, Administration Military NGO Country russia Target Information Ukraine	tlp:white	9		admin@admin.test	2024-01-20	Russian threat group COLDRIVER expands its targeting of Western officials to include the use of malware	All	
CUDESO		382	Threat Actor Callisto Attack Pattern Phishing - T1566 Spearphishing Attachment - T1566.001 Spearphishing Link - T1566.002	tlp:white	71		admin@admin.test	2022-08-15	Disrupting SEABORGIUM's ongoing phishing operations	All	
		1042		type:OSINT tlp:white osint:source-type="technical-report"	57		admin@admin.test	2017-04-13	OSINT - Callisto Group	All	

Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3

« previous next »

Attributes

« previous next »

Search

Date	Event	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2023-03-22	382	CUDESO	Network activity	domain	cache-dns.com			Via Sekoia.io Via GoogleTag	✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	cache-dns-forwarding.com				✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	cache-dns-preview.com				✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	cache-docs.com			Via Sekoia.io	✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	cache-pdf.com				✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	cache-pdf.online				✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	cache-services.live				✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	cloud-docs.com			Via Sekoia.io	✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	cloud-drive.live				✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	cloud-storage.live				✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	docs-cache.com			Via Sekoia.io	✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	docs-forwarding.online				✓		2	✓	Inherit event	(0/0/0)		
2023-03-22	382	CUDESO	Network activity	domain	docs-info.com			Via Sekoia.io	✓		2	✓	Inherit event	(0/0/0)		

The Callisto Group is Russian aligned advanced threat actor group whose known targets include military personnel, government officials, think tanks, and journalists in Europe and the South Caucasus.
Their primary interest appears to be gathering intelligence related to foreign and security policy in the Eastern Europe and South Caucasus regions.
In October 2015 the Callisto Group targeted a handful of individuals with phishing emails that attempted to obtain the target's webmail credentials.
In early 2016 the Callisto Group began sending highly targeted spear phishing emails with malicious attachments that contained, as their final payload, the ***"Scout"*** malware tool from the HackingTeam RCS Galileo platform.
The Callisto Group has been active at least since late 2015 and continues to be so, including continuing to set up new phishing infrastructure every week.
Some of the Sample Hashes:
SHA1 af364ff503da71875b6d7c401a1e98e31450a561
SHA1 db2b8f49b4e76c2f538a3a6b222c35547c802cef
SHA1 29968b0c4157f226761073333ff2e82b588ddf8e

5.Threat Actor Activities Summary

- Callisto is widely assessed as a Russian-aligned cyber-espionage actor, with observed operations aligned with Russian state interests (especially around Eastern Europe, Caucasus, and Ukraine).
- Their known targeting includes government, military personnel, think tanks, journalists, NGOs, individuals connected to Ukraine, and intelligence / defence staff

- The U.S. Department of Justice and Microsoft have jointly disrupted a portion of their infrastructure, seizing dozens of domains used for spear-phishing and credential harvesting
- Callisto is an example of a hybrid espionage threat: while they use criminal or proxy infrastructure (e.g. domains sold for profit) and shift infrastructure rapidly, their targeting, focus, and mission suggest a persistent state actor.
- Callisto's operations are characterized by persistent credential-phishing, impersonation campaigns, and use of custom-built malware, occasionally leveraging leaked surveillance tools.

6.Notable Targets/Campaign

- Targeting including spear-phishing of UK parliamentarians from multiple political parties, from at least 2015 through to this year
- The hack of UK-US trade documents that were leaked ahead of the 2019 General Election – previously attributed to the Russian state via Written Ministerial Statement in 2020
- The 2018 hack of the Institute for Statecraft, a UK thinktank whose work included initiatives to defend democracy against disinformation, and the more recent hack of its founder Christopher Donnelly, whose account was compromised from December 2021; in both instances documents were subsequently leaked.
- US, UK, NATO, and Ukraine hacking campaign: In 2023, the Department of Justice announced charges against two individuals associated with Callisto for a campaign to hack networks in the US, UK, other NATO countries, and Ukraine on behalf of the Russian government.
- Targeting the UK Foreign Office: In 2017, the group was reported to have targeted the UK Foreign Office.
- Increased focus on Ukraine: Following the 2022 invasion, the group increased its activity to target Ukraine, including a private logistics company.

7.Attribution and Aliases

Source / Vendor	Alias
F-Secure (initial public identification, 2017)	Callisto Group
UK NCSC & Microsoft	Star Blizzard
Microsoft Threat Intelligence	SEABORGIUM
Google Threat Analysis Group	COLDRIVER
Proofpoint	TA446
Mandiant (uncategorized cluster)	UNC4057

Assessed Origin: Russian Federation

Assessed Motivation: Strategic espionage aligned with Russian state objectives

Confidence Level: High

8.Targeting and Objectives

Primary Targets:

- Government and diplomatic entities (especially in Europe, the UK, and the US)
- Defence contractors and research organizations

- NGOs and human rights groups focusing on Russia/Ukraine
- Academia and think tanks (policy, security, and foreign relations)
- Journalists and individual researchers involved in geopolitics

Strategic Objectives:

- Gathering geopolitical and defence intelligence
- Compromising communications and policy documents
- Supporting Russian strategic interests through information collection
- Potentially facilitating influence operations or disinformation campaigns

9.Malware, and Infrastructure

Malware

- Scout – A lightweight reconnaissance implant derived from the leaked HackingTeam RCS toolset.
- Custom Credential Harvester – HTML-based phishing kits designed to imitate Outlook Web Access and Microsoft 365 portals.

Infrastructure

- Domains registered via Namecheap, Hostinger, and GoDaddy, often mimicking government or defence entities.
- Short-lived redirect chains using legitimate content distribution networks or cloud storage links.
- Use of compromised personal email accounts (e.g., Gmail, ProtonMail) for outreach and exfiltration.

10.Indicators of Compromise

Here are some of the indicators of compromise associated with Callisto/ Star Blizzard as seen on the MISP docker. Note that this is not exhaustive.

a)

IP Addresses (may be outdated/rotated)	**Domains**
84.11.146.62	yandx-online.cloud
107.6.172.54	docs-drive.online
107.6.181.116	cloud-mail.online
223.130.11.165	y-ml.co
192.168.56.101	online365-office.com
104.223.120.159	officeonline365.live
117.184.105.34	hypertextteches.com
101.36.121.4	goo-link.online

b) Sample Hashes

SHA1 af364ff503da71875b6d7c401a1e98e31450a561

SHA1 db2b8f49b4e76c2f538a3a6b222c35547c802cef

SHA1 29968b0c4157f226761073333ff2e82b588ddf8e

c) URL

http://gulfc.haifa.ac.il/index.php/the-ezri-center-in-the-media/291-the-ezri-center-in-the-media

ks/36-56357e64599f6070.js\

hunks/480-93535f5bd3d87236.js\

d) Hostnames

www.we11point.com

webmail.vipreclod.com

oa.trustneser.com

oa.technical-requre.com

mycitrix.we11point.com

me.we11point.com

webmail.kaspersyk.com

vpn.we11point.com

e)Registry keys for Persistence Mechanism

{\"_time\":\"2025-05-31T11:42:00.016245+00:00\

{\"_time\":\"2025-05-31T11:47:26.280960+00:00\

{\"_time\":\"2025-05-31T11:52:55.897042+00:00\

{\"_time\":\"2025-05-31T11:58:24.340939+00:00\

{\"_time\":\"2025-05-31T12:03:28.106133+00:00\

{\"_time\":\"2025-05-31T12:08:56.821510+00:00\

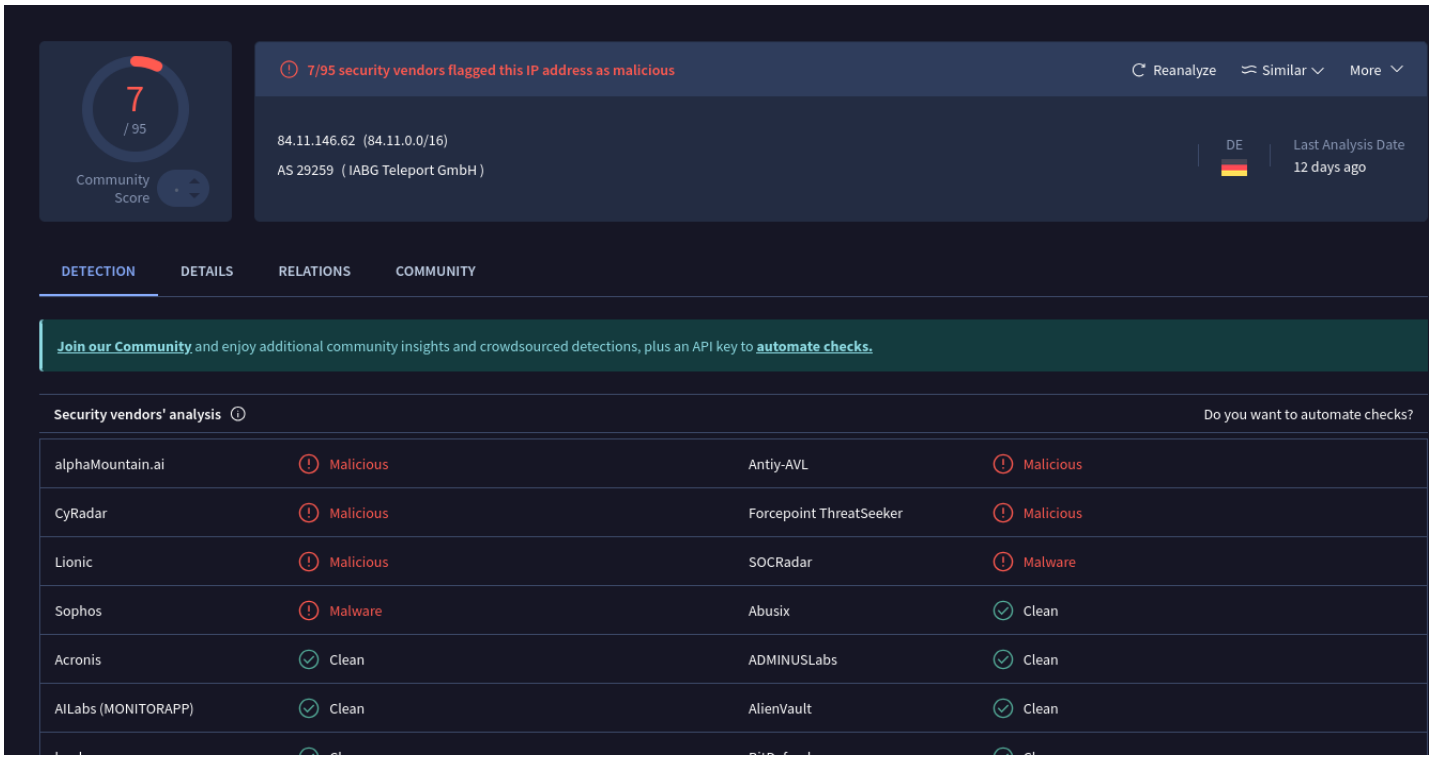
{\"_time\":\"2025-05-31T12:14:27.615637+00:00\

{\"_time\":\"2025-05-31T12:19:56.693257+00:00\

{\"_time\":\"2025-05-31T12:25:28.780108+00:00\

11.Investigations with Security Tools

We have investigated some of the these IOCs on VirusTotal and Abuseipdb. Most were flagged as malicious by security vendors like SOCRader, CyRadar, AlphaMountain.ai, Bitdefender. This is shown in the screenshots below:



Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (1)

Date resolved	Detections	Resolver	Domain
2015-06-24	0 / 95	VirusTotal	host-84-11-146-62.customer.teleport-iabg.de

Communicating Files (20)

Scanned	Detections	Type	Name
2025-03-06	58 / 72	Win32 EXE	.bin
2024-03-03	44 / 72	Win32 EXE	2d0c8372f9ab5a9cac980723a73501b7.bin
2025-03-06	60 / 72	Win32 EXE	19c1ba41f72296d05eab7066cb5a00e048486c2a30b1c93c0eca87420660ce65
2022-08-15	45 / 71	Win32 EXE	55ff220e38556ff902528ac984fc72dc_sig_replaced
2016-04-19	37 / 56	DOS EXE	exploit.exe
2022-07-28	55 / 71	Win32 EXE	b67572a18282e79974dc61fffb8ca3d0f4fca1b0_sig_replaced
2025-03-07	54 / 72	Win32 EXE	4357e8139aff59c30c8a4d4645ebf36467983d3031ac0921c488cd35c5c10b17
2022-08-17	51 / 71	Win32 EXE	8ed01ac79680d84c0ee7a5f027d8b86a_sig_replaced
2020-02-20	39 / 59	Office Open XML Spreadsheet	4707371e387f067e4881dd7b5ca46a627b87a0979e86cacbfccf1fdad56cdffa.xlsx
2025-03-08	53 / 72	Win32 EXE	f7f69c5ed94a03f6d57e9afd33c2627ff69205f2_sig_replaced

• • •

/ 95

Community Score

107.6.172.54 (107.6.128.0/18)

AS 32475 (SINGLEHOP-LLC)

NL

Last Analysis Date
1 month ago

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

HIGH 0 MEDIUM 0 LOW 1 INFO 0 SUCCESS 0

Rocket Kitten · according to source ArcSight Threat Intelligence · 2 years ago
↳ VirusTotal Link: https://www.virustotal.com/gui/ip-address/107.6.172.54/detection Abuse IPDB Link: https://www.abuseipdb.com/check/107.6.172.54 Postal Code: 1119 This IP resolves to 1018 domains.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	Dr.Web	Malicious
Forcepoint ThreatSeeker	Malicious	alphaMountain.ai	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	benkow.cc	Clean

More screenshots are posted on the appendix.

12.Key Findings from the IOCs/Infrastructures

It is clear that most public IOCs or infrastructure components associated with Callistor/Star Blizzard have limited longevity.

i) Domain / Infrastructure IOCs (Seized / Disrupted Domains)

- Microsoft and the DOJ seized or restrained 41 domains used by Callisto in spear-phishing operations, and Microsoft additionally filed to seize 66 domains associated with the actor.
- In total, claims suggest 107 domains were disrupted.
- Some domain names were built to mimic Russian government services (e.g. typo-variants of taxation or internal ministry domains).
- Microsoft's "SEABORGIUM" blog and related CTI disclosed lists of known malicious domains associated with Star Blizzard.

Consequently, because domain names rotate and are often short-lived, they are most useful for retrospective detection or threat hunting rather than long-term blocking.

ii)Malware / Payload IOCs

- Variants of Scout (from the HackingTeam RCS Galileo platform) have been used as post-infection payloads.
- Use of exploit documents leveraging CVE-2017-11882 (Equation Editor) has been observed in at least one campaign attributed to Callisto

We findings have shown that public reporting has not (so far) revealed a large, stable set of malware hashes or signatures consistently tied to Callisto. That means reliance on IOCs alone is insufficient and must be augmented with behavioural and anomaly detection.

iii)Infrastructure / IP-Related Indicators

- Sekoia's C2 infrastructure tracking (2022) lists that Callisto ("Calisto") uses infrastructure detected via web scanning and C2 heuristics, though specific IP addresses are typically short-lived

- Reports of infrastructure links in China, Ukraine, and Russia in WHOIS or hosting data for some domains associated with Callisto.

Given IP churn, blocking IPs is rarely reliable beyond a narrow detection window, but they can be useful for retrospective correlation.

13.Tactics, Techniques & Procedures (TTPs) & Attack Infrastructure as Listed by Mitre Att&ck Framework

TACTIC	TECHNIQUE	PROCEDURE
Reconnaissance	**Active Scanning - T1595**	**Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.**
	Social Media - T1593.001	**Adversaries may search social media for information about victims that can be used during targeting**
Resource Development	**Acquire Access - T1650**	**Adversaries may purchase or otherwise acquire an existing access to a target system or network**
	Acquire Infrastructure - T1583	**Adversaries may buy, lease, rent, or obtain infrastructure that can be used during targeting**
	Botnet - T1584.005	**Adversaries may compromise numerous third-party systems to form a botnet that can be used during targeting**

Initial Access	**Phishing - T1566** **Spearphishing Attachment - T1566.001** **Spearphishing Link - T1566.002**	**Adversaries may send phishing messages to gain access to victim systems.** **Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files** **Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems**
Execution	**AppleScript - T1059.002** **At (Linux) - T1053.001** **Cloud API - T1059.009**	**Adversaries may abuse AppleScript for execution.** **Adversaries may abuse the at utility to perform task scheduling for initial, recurring, or future execution of malicious code.** **Adversaries may abuse cloud APIs to execute malicious commands**
Persistence	**Account Manipulation - T1098** **Active Setup - T1547.014** **Add-ins - T1137.006** **Additional Email Delegate Permissions - T1098.002**	**Adversaries may manipulate accounts to maintain and/or elevate access to victim systems** **Adversaries may achieve persistence by adding a Registry key to the Active Setup of the local machine** **Adversaries may abuse Microsoft Office add-ins to obtain persistence on a compromised system** **Adversaries may grant additional permission levels to maintain persistent access to an adversary-controlled email account.**

Privileged Escalation	**Abuse Elevation Control Mechanism - T1548** **Access Token Manipulation - T1134** **Additional Cloud Credentials - T1098.001**	**Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions** **Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls** **Adversaries may add adversary-controlled credentials to a cloud account to maintain persistent access to victim accounts and instances within the environment.**
Defence Evasion	**Abuse Elevation Control Mechanism - T1548** **Access Token Manipulation - T1134** **Asynchronous Procedure Call - T1055.004**	**Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions** **Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls.** **Adversaries may inject malicious code into processes via the asynchronous procedure call (APC) queue in order to evade process-based defenses as well as possibly elevate privileges.**
Credential Access	**ARP Cache Poisoning - T1557.002** **Brute Force - T1110**	**Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices** **Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.**

Discovery	**Account Discovery - T1087** **Application Window Discovery - T1010**	**Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment** **Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used.**
Lateral Movement	**Application Access Token - T1527** **Application Deployment Software - T1017** **Exploitation of Remote Services - T1210**	**Adversaries may use application access tokens to bypass the typical authentication process and access restricted accounts, information, or services on remote systems** **Adversaries may deploy malicious software to systems within a network using application deployment systems employed by enterprise administrators** **Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network**
Collection	**Adversary-in-the-Middle - T1557** **Archive Collected Data - T1560**	**Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access).** **An adversary may compress and/or encrypt data that is collected prior to exfiltration**
Command and Control	**Application Layer Protocol - T1071** **Custom Command and Control Protocol - T1094**	**Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic** **Adversaries may communicate using a custom command and control protocol instead of encapsulating commands/data in an existing Application Layer Protocol**

Exfiltration	**Automated Exfiltration - T1020**	**Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection**
	Data Encrypted - T1022	**Data is encrypted before being exfiltrated in order to hide the information that is being exfiltrated from detection or to make the exfiltration less conspicuous upon inspection by a defender**
	Exfiltration Over C2 Channel - T1041	**Adversaries may steal data by exfiltrating it over an existing command and control channel.**
Impact	**Cloud Service Hijacking - T1496.004**	**Adversaries may leverage compromised software-as-a-service (SaaS) applications to complete resource-intensive tasks, which may impact hosted service availability.**
	Data Destruction - T1485	**Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources**
	Data Manipulation - T1565	**Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data.(Citation: Sygnia Elephant Beetle Jan 2022**

14.Threat Profile & Risk Assessment for Local Organizations

From the intelligence gathered above, here is a tailored threat profile and guidance for organizations to consider.

Likelihood & Conditions of Attack

- While Callisto's known targeting skews toward high-value strategic targets (government, think tanks, NGOs, defence), any organization involved in foreign affairs, policy research, Ukraine support, or public diplomacy is within scope.
- If your organization publishes reports on Russia, Ukraine, or conducts transnational collaboration, you are at higher risk.
- Attackers are likely to use spear-phishing via email or impersonated domains targeting key individuals (executives, policy staff, diplomats).
- Given the active confiscation of their domains, the threat actor remains capable and adaptive, and is likely to spin up new infrastructure rapidly

Primary Risks / Impact Vectors

- **Credential compromise / account takeover**
  Phishing is their core vector; stolen credentials may be used for prolonged access or lateral movement
- **Reconnaissance / internal intelligence gathering**
  Once inside, they may quietly observe, pivot, or map environments to identify more sensitive assets.
- **Exfiltration of strategic documents / data leakage**
  They aim to steal policy documents, diplomatic communications, or analysis relevant to foreign policy.
- **Operational disruption / disinformation**
  While not their core known technique, given the nexus to war / political information, manipulation or leak-based influence operations cannot be discarded.

Severity

- High, for medium-to-large entities in sensitive sectors. A successful breach or credential compromise can lead to reputational, strategic, or national-security impact.
- The actor operates over long timeframes, allowing for stealth, persistence, and selective exfiltration.

Detection Gaps & Challenges

- Rapid infrastructure churn and domain rotation reduce effectiveness of static blocklists.
- Use of legitimate services or open redirects means phishing may appear benign or innocuous.
- Payloads may be customized or leverage zero-day exploits not broadly known.
- Attribution complexity: because infrastructure may intermingle with criminal or proxy services, tracking the actor is nontrivial.
- Some infrastructure (domains) may already have been seized or blacklisted, so defenders may miss new ones.

Defensive & Mitigation Recommendations

Below is a list of some concrete recommendations for local organizations to reduce exposure and detect possible intrusions by Callisto-like actors**.**

1. **User Awareness & Phishing Resilience**
    - Train users (especially senior staff) to scrutinize email senders, domain authenticity, links, attachments.
    - Employ phishing simulation exercises, especially focusing on spear-phishing (impersonation, lures).
    - Use email filtering / threat protection tools to block newly registered or suspicious domains, especially those near-typos or impersonating known services.
2. **Strong Authentication & Credential Protections**
    - Enforce multi-factor authentication (MFA) where possible; prefer hardware tokens (FIDO) or phishing-resistant MFA.

- Monitor unusual login activity (anomalous IP locations, multiple failed logins).
- Leverage conditional access policies (e.g. block legacy protocols, restrict sign-in from unmanaged devices).

3. **Domain & Infrastructure Monitoring / Threat Hunting**
    - Subscribe to CTI feeds (MISP, commercial, open sources) containing Callisto / Star Blizzard-associated IOCs and heuristics.
    - Monitor new domain registrations that mimic your domain namespace or sector-specific institutions (e.g. “ministry-of-x.net”, “tax-office[.]xyz”).
    - Set up alerts on redirector chains or abnormal HTTP behaviour (e.g. hiding content, VBScript inclusion, JavaScript redirects).
    - Conduct regular threat-hunting on logs (email logs, firewall, proxies) for matching domain, URL or redirect patterns.
4. **Endpoint & Network Detection / Logging**
    - Ensure robust endpoint detection and response (EDR) or next-generation antivirus (NGAV) with capability to detect suspicious process behaviour, script execution, network anomalies**.**
    - Log DNS queries and HTTP traffic to detect resolution to suspicious domains or to new/unusual C2 endpoints.
    - Use network segmentation, least privilege on network flows, so that if an endpoint is breached, lateral movement is constrained.
5. **Incident Response Readiness**
    - Maintain playbooks for phishing compromise, credential theft, and unusual outbound connections.
    - Predefine escalation paths and forensic capabilities (e.g. memory capture, endpoint triage).
    - Maintain “safe harbor” or backup environments where exfiltration is harder, and ensure periodic backups of critical data.
6. **Collaborative Disruption & Reporting**
    - Share any observed suspicious domains, indicators, or intrusion artifacts with local national CERT, intelligence/community CTI platforms (e.g. via MISP).

- When legally possible, request assistance to seek takedown or seizure of identified domains used against you.
- Monitor public domain-seizure announcements (e.g. Microsoft, DOJ) for updates to their infrastructure, to add to your defensive blocklists.

7. **Periodic Review & Intelligence Refresh**
    - Re-evaluate IOC validity periodically (domains expire, IPs change).
    - Supplement static IOCs with behavioural detection and anomaly-based coverage.
    - Recalibrate detection rules over time to anticipate new TTPs (e.g. domain obfuscation or new exploit techniques).

15.Conclusion

Callisto remains a persistent and adaptive espionage threat operating in alignment with Russian geopolitical goals. Their preference for credential harvesting and long-term infiltration over destructive attacks makes them particularly dangerous to organizations that handle sensitive political, defence, or policy data.

Despite successful infrastructure takedowns, Callisto's rapid regeneration and effective social engineering ensure the group will continue to pose a long term significant risk to Western and allied organizations.

However, by deploying the mitigation measures suggested in this report, and implementing the recommendation, the current wave of attacks and any future attacks based on the modus operandi of the group can be promptly detected, contained or most likely be prevented if fully implemented.

16.Reference

https://web.archive.org/web/20170417102235/https://www.f-secure.com/documents/996508/1030745/callisto-group

https://attack.mitre.org/techniques/T1566/002/

https://www.virustotal.com/gui/home/upload

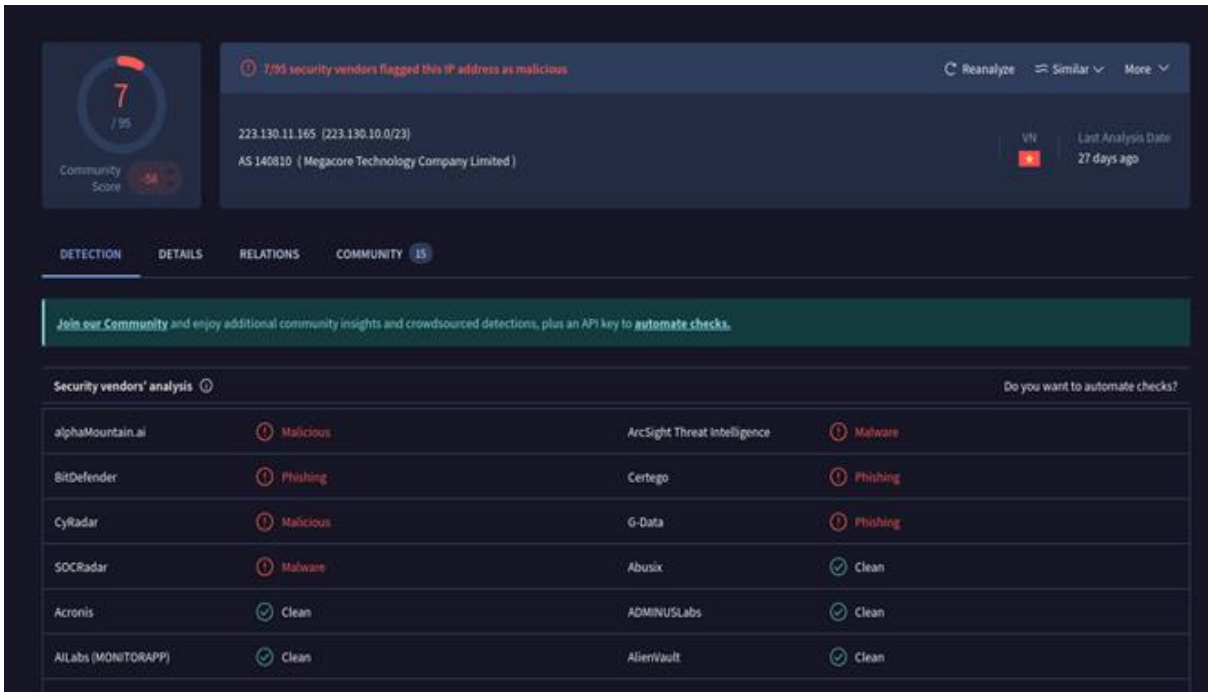
https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/

https://www.abuseipdb.com/

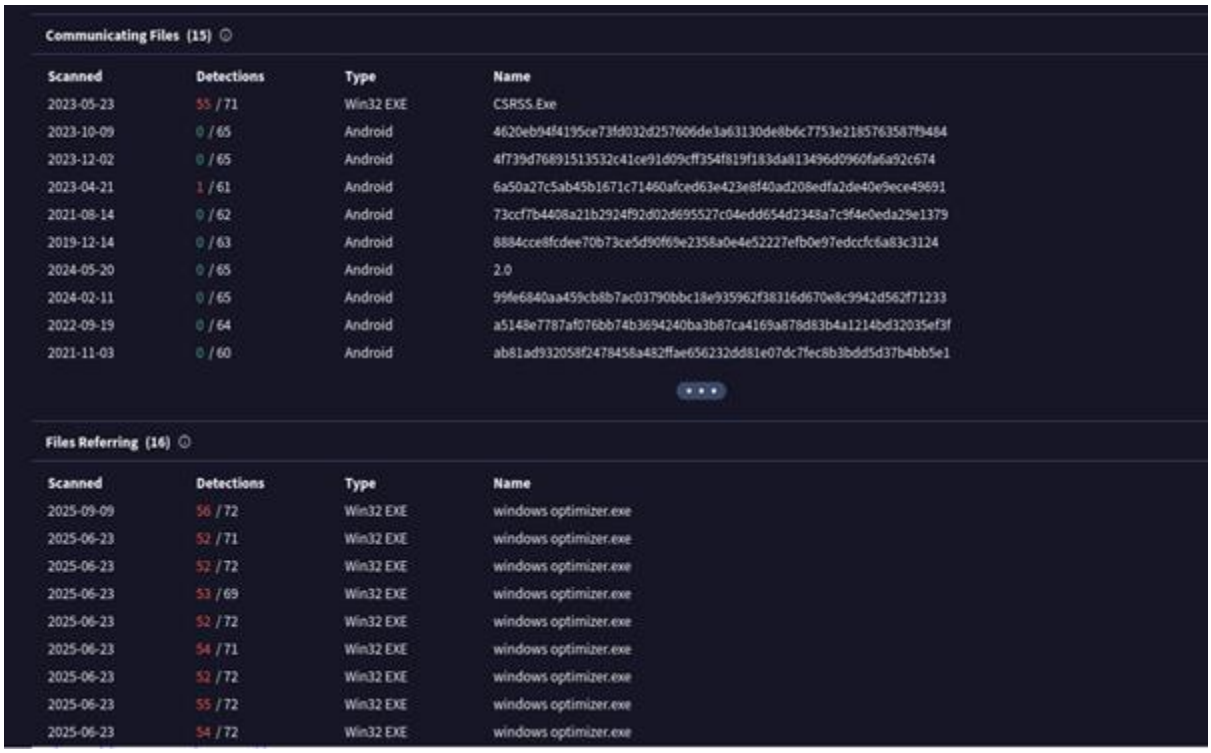
Whois nexusiotsolutions.net

17.Appendix

i)



ii)



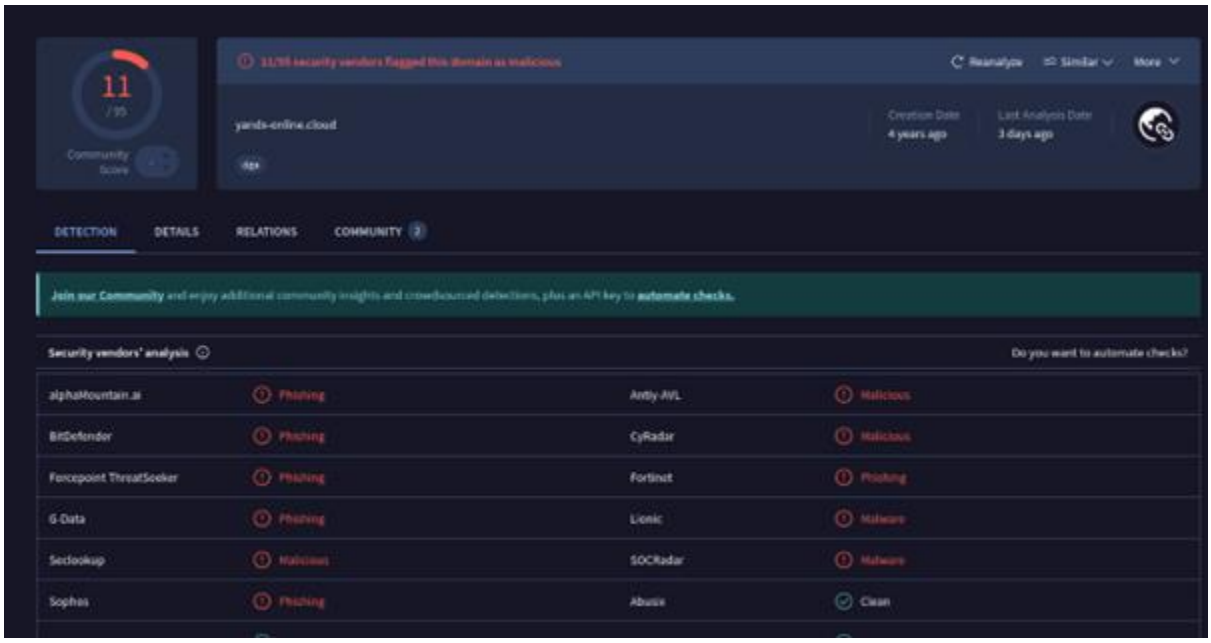
Communicating Files (15)

Scanned	Detections	Type	Name
2023-05-23	55 / 71	Win32 EXE	CSRSS.Exe
2023-10-09	0 / 65	Android	4620eb94f4195ce73fd032d257606de3a63130de8b6c7753e2185763587f9484
2023-12-02	0 / 65	Android	4f739d76891513532c41ce91d09cff354f819f183da813496d0960fa6a92c674
2023-04-21	1 / 61	Android	6a50a27c5ab45b1671c71460afced63e423e8f40ad208edfa2de40e9ece49691
2021-08-14	0 / 62	Android	73ccf7b4408a21b2924f92d02d695527c04edd654d2348a7c9f4e0eda29e1379
2019-12-14	0 / 63	Android	8884cce8fcdee70b73ce5d90f69e2358a0e4e52227efb0e97edccfc6a83c3124
2024-05-20	0 / 65	Android	2.0
2024-02-11	0 / 65	Android	99fe6840aa459cb8b7ac03790bbc18e935962f38316d670e8c9942d562f71233
2022-09-19	0 / 64	Android	a5148e7787af076bb74b3694240ba3b87ca4169a878d83b4a1214bd32035ef3f
2021-11-03	0 / 60	Android	ab81ad932058f2478458a482ffae656232dd81e07dc7fec8b3bdd5d37b4bb5e1

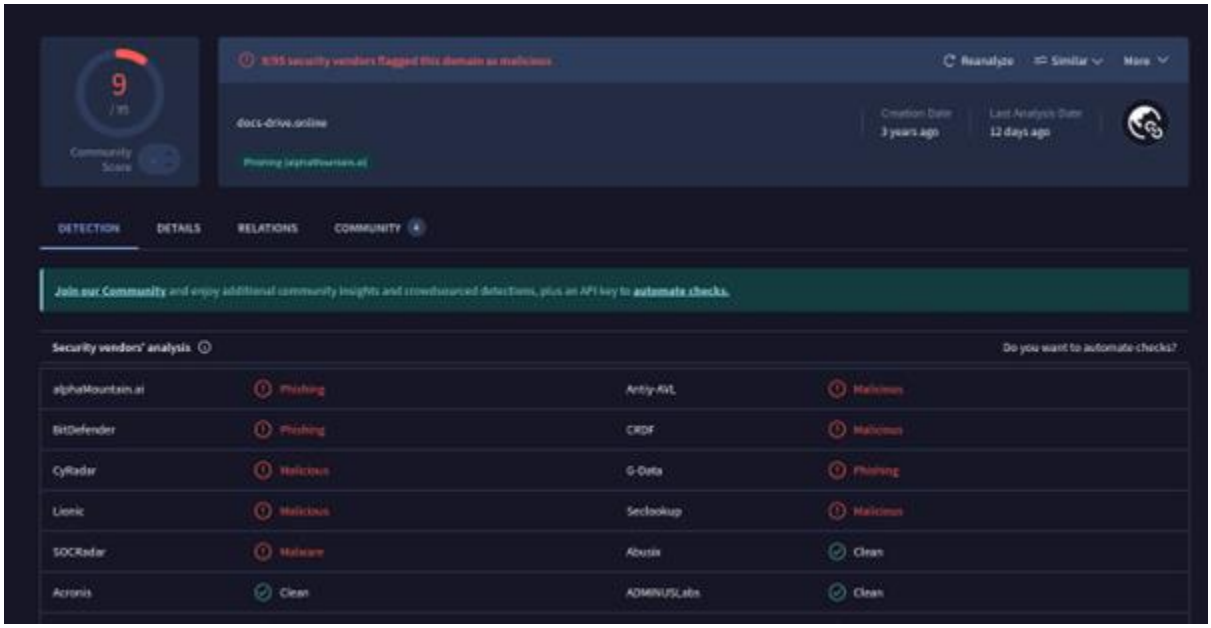
Files Referring (16)

Scanned	Detections	Type	Name
2025-09-09	56 / 72	Win32 EXE	windows optimizer.exe
2025-06-23	52 / 71	Win32 EXE	windows optimizer.exe
2025-06-23	52 / 72	Win32 EXE	windows optimizer.exe
2025-06-23	53 / 69	Win32 EXE	windows optimizer.exe
2025-06-23	52 / 72	Win32 EXE	windows optimizer.exe
2025-06-23	54 / 71	Win32 EXE	windows optimizer.exe
2025-06-23	52 / 72	Win32 EXE	windows optimizer.exe
2025-06-23	55 / 72	Win32 EXE	windows optimizer.exe
2025-06-23	54 / 72	Win32 EXE	windows optimizer.exe

iii)


11
/ 95
Community Score
11/95 security vendors flagged this domain as malicious
Reanalyze
Similar
More
yands-online.cloud
Creation Date
4 years ago
Last Analysis Date
3 days ago
DETECTION
DETAILS
RELATIONS
COMMUNITY 2
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
alphaMountain.ai
Phishing
Antiy-AVL
Malicious
BitDefender
Phishing
CyRadar
Malicious
Forcepoint ThreatSeeker
Phishing
Fortinet
Phishing
G-Data
Phishing
Lionic
Malware
Seclookup
Malicious
SOCRadar
Malware
Sophos
Phishing
Abusix
Clean

iv)


9
/ 95
Community Score
9/95 security vendors flagged this domain as malicious
Reanalyze
Similar
More
docs-drive.online
Phishing (alphaMountain.ai)
Creation Date
3 years ago
Last Analysis Date
12 days ago
DETECTION
DETAILS
RELATIONS
COMMUNITY 4
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
alphaMountain.ai
Phishing
Antiy-AVL
Malicious
BitDefender
Phishing
CRDF
Malicious
CyRadar
Malicious
G-Data
Phishing
Lionic
Malicious
Seclookup
Malicious
SOCRadar
Malware
Abusix
Clean
Acronis
Clean
ADMINUSLabs
Clean

v)

11 / 95

Community Score

11/95 security vendors flagged this domain as malicious

Reanalyze | Similar | More

cloud-mail.online

Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com

Creation Date: 1 year ago

Last Analysis Date: 17 days ago

DETECTION | DETAILS | RELATIONS | COMMUNITY 3

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Phishing	Antiy-AVL	Malicious
BitDefender	Phishing	CRDF	Malicious
CyRadar	Malicious	Fortinet	Phishing
G-Data	Phishing	Lionic	Phishing
Seclookup	Malicious	SOCRadar	Malware
Sophos	Phishing	Abusix	Clean