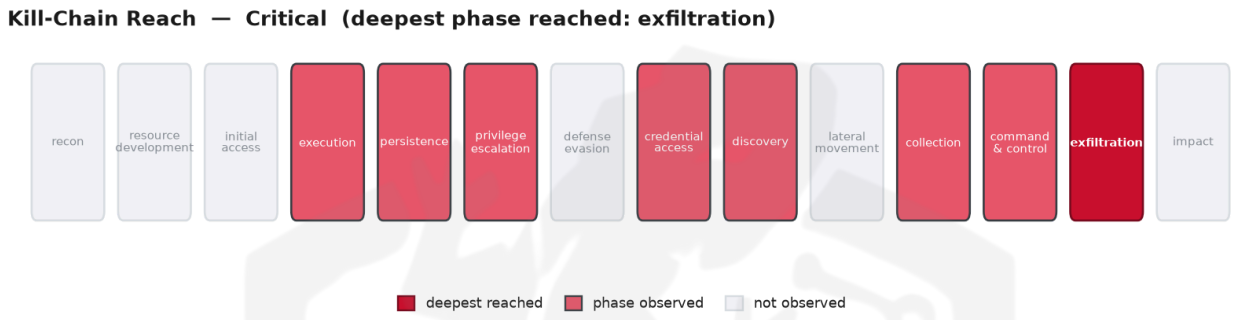
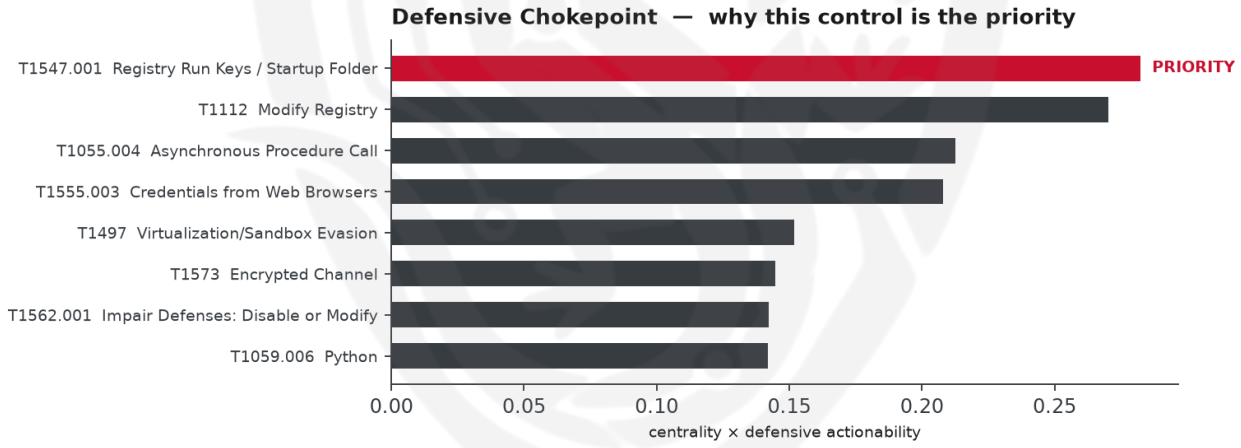
THREAT REPORT: LENAI'S BLOCKCHAIN-BASED C2 OPERATIONS

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The source attributes this activity to LenAI, a threat actor utilizing various malware families, including Aeternum, XWorm, XMRig, and ZingoStealer, to target unspecified countries and sectors. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. The threat actor's operations involve a range of techniques, including DNS, system information discovery, and data exfiltration to cloud storage. Defensive actions should focus on detecting and preventing these techniques to mitigate the risk of data exfiltration.

Threat Overview

LenAI, the attributed threat actor, employs a range of malware families, including Aeternum, XWorm, XMRig, and ZingoStealer, to conduct its operations. The central vulnerability exploited is currently

unknown, but the actor utilizes various techniques, including system information discovery, registry modifications, and encrypted channels. The victimology of this threat is not well-defined due to insufficient data on targeted countries and sectors.

Attack Chain and Priority Control

The observed techniques used by LenAI form a complex attack chain, involving initial system checks, DNS interactions, and application layer protocol manipulation. The priority technique identified is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. To counter this, the priority control is to "Audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries; alert on .lnk or script creation in Startup by browser/email temp paths."

Infrastructure and Corroboration

The malicious infrastructure associated with LenAI's operations is hosted on providers such as Alinda LLC. Corroborating sources, such as abuse.ch, have identified additional malware families, including Sliver, Unknown Stealer, and Unknown malware, which may be related to LenAI's activities. However, according to AbuseIPDB, there are currently no indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1071.004 DNS
- T1036.005 Match Legitimate Resource Name or Location
- T1497.001 System Checks
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1112 Modify Registry
- T1555.003 Credentials from Web Browsers
- T1055.004 Asynchronous Procedure Call
- T1497 Virtualization/Sandbox Evasion
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1567.002 Exfiltration to Cloud Storage
- T1059.006 Python
- T1543.001 Launch Agent

- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2973).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4341; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
APT37	0.4341
ZIRCONIUM	0.4237
APT18	0.416
Darkhotel	0.4036
Tropic Trooper	0.3931

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Sliver, Unknown Stealer, Unknown malware.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	193[.]221[.]200[.]219	AbuseIPDB 0% (NL) · Sliver · AS209946 Alinda LLC

Type	Indicator	Context
Domain	endpoints[.]omniatech[.]io	
Domain	polygon-zkevm[.]drpc[.]org	
Domain	cdnjsdelivr[.]beer	Unknown malware
Domain	polygon-mumbai[.]gateway[.]tenderly[.]co	
Domain	sekirolegion[.]duckdns[.]org	Unknown Stealer
Domain	api[.]zan[.]top	
Domain	download[.]sftp-api-group-wechat[.]com	
Domain	update[.]constant-path[.]xyz	
Domain	update-launcher[.]xyz	
Domain	test-steve[.]cyou	
Domain	api[.]noderpc[.]xyz	
Domain	polygon-amoy[.]gateway[.]tenderly[.]co	
Domain	polygon-amoy[.]therpc[.]io	
Domain	polygon-mumbai-bor-rpc[.]publicnode[.]com	
Domain	polygon-zkevm-mainnet[.]public[.]blastapi[.]io	
Domain	polygon[.]rpc[.]hypersync[.]xyz	

Type	Indicator	Context
Domain	polygontestapi[.]terminet[.]io	
Domain	rpc[.]polygon-zkevm[.]gateway[.]fm	
Domain	rpc[.]polygonsupernet[.]public[.]arianee[.]net	
Domain	rpc[.]poolz[.]finance	
URL	hxxps://rpc[.]polygon-zkevm[.]gateway[.]fm	
Hash	5bfb25b8255b61e5ffdf6804451534bcfa9f1dfd225e6c8cdcefb5f50d846898	
Hash	1505eda3da68e2ff9919b55a31018bd30a991236f041aee835f3bc4e430ce505	
Hash	f2a326cff405299e4ebdfaac955c52fc7e496544eaa0921ecad4816cb3ae3a27	
Hash	4e24bbd0fabac6c3efcec943046afbfd332b2c0108a13becfda23a0e26f9ff5f	
Hash	81bb80d9c5a97dc41b65f6248c131963c91346eb4fb672836b3d53ae67564d9f	
Hash	ea1b6ff3a0c1a749b9f09d66789973321d63d8896b48f7345193bdad512950a2	
Hash	673a51a179a78fbdf2b8770f868f883a	
Hash	848b1440f5f52bfddf2e1b3e9e248f12	
Hash	a45e8679d2695d10a45a3f78268fab64	
Hash	96f6794fa4b7414e38be4ef497cd8611d50a59ec	
Hash	d224dde23da2faff57235192333fc7998762c645	
Hash	d3e0f9448c94b1017f26e4da63b710a886a2b426	
Hash	1ef50e9d715245e29220936a66c0bece	
Hash	66575cc1df33e40a47fe00abdc067fe5	
Hash	cd8b231a2101c7de3f0b118f99279cbd	

Type	Indicator	Context
Hash	326a4305420a5c57950a7ee8c1e41b31132dd027	
Hash	b51a50ffc57565c8488cb8101252db0e60619750	
Hash	cfd101963a4e791fc59bda97bfc87f33ce7ce379	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Observed here:** T1547.001 Registry Run Keys / Startup Folder was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (persistence)
- **Basis:** of the 37+ groups that use Registry Run Keys / Startup Folder, this pairing runs 1.9x above base rate, a disproportionately-coupled move rather than the obvious one.

LenAI could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious code at a later time, potentially leveraging the Windows Task Scheduler to blend in with legitimate system activity and evade detection. This technique may be particularly appealing to LenAI as it allows for flexibility in execution timing and can be used to bypass other security controls, making it a suitable alternative to the blocked Registry Run Keys / Startup Folder method. To counter this potential move, the defensive control would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1098 Account Manipulation (n=12, lift 2.0), T1197 BITS Jobs (n=5, lift 2.9)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it

- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File