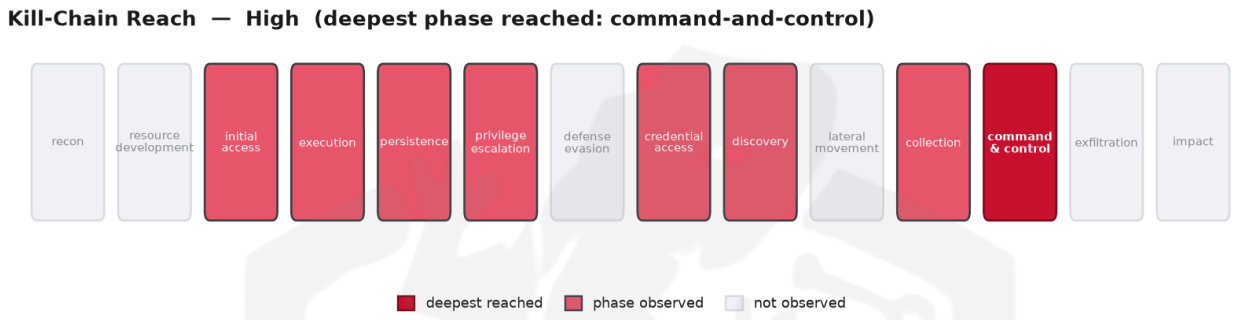
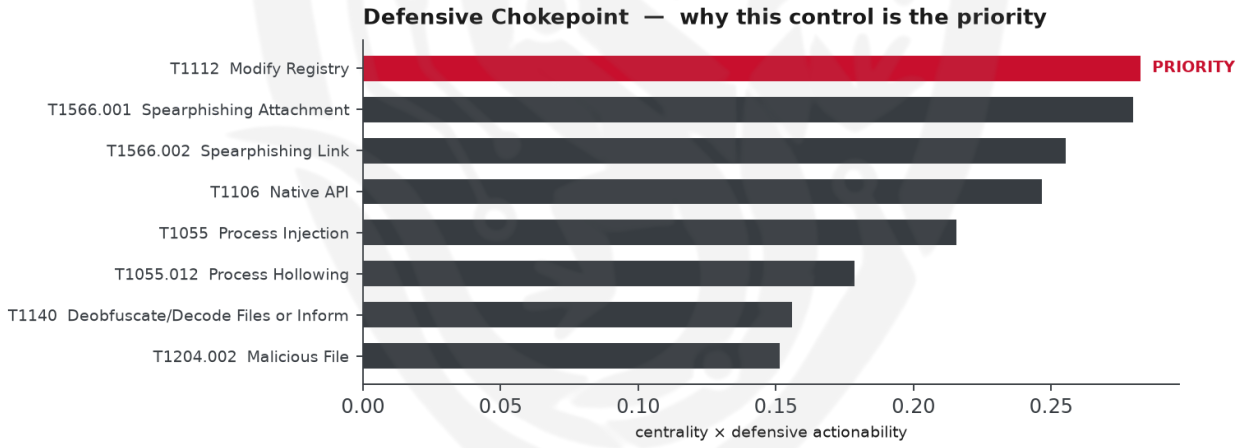
THREAT REPORT: UNKNOWN_ADVERSARY LUA LOADER CAMPAIGN

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 observed cluster of activity has been identified as utilizing a Lua loader to deliver various malware families, including Agent Tesla, Remcos, XWorm, Best Private LOGGER, and Snake Keylogger. The threat actor's targets and motivations are currently unknown. Priority should be given to monitoring sensitive registry keys for modification to mitigate the threat. The campaign's ability to reach command-and-control levels poses a high operational risk.

Threat Overview

The threat actor, whose identity is currently unknown, is employing a range of techniques to compromise systems, including keylogging, scheduled tasks, and system checks. The malware families used in the

campaign are diverse, suggesting a potential focus on flexibility and adaptability. The lack of specific targeting information makes it challenging to determine the actor's goals or motivations.

Attack Chain and Priority Control

The attack chain involves various techniques, including scheduled tasks, keylogging, and system checks, ultimately leading to the modification of registry keys. The priority technique identified is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To counter this, the lead control measure is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted by Stellar Group SAS. According to abuse.ch, several malware families, including AgentTesla, MASS Logger, Remcos, RemcosRAT, and XWorm, have been corroborated, providing additional context to the campaign's scope and reach. However, AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, indicating a need for continued vigilance and monitoring.

Technical Appendix

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

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

- T1053.005 Scheduled Task
- T1056.001 Keylogging
- T1059.007 JavaScript
- T1204.002 Malicious File
- T1497.001 System Checks
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1112 Modify Registry
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1012 Query Registry
- T1071.001 Web Protocols
- T1055.001 Dynamic-link Library Injection

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2974).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4685; 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
Higaisa	0.4685
Malteiro	0.4588
Rancor	0.45
FIN4	0.4472
Darkhotel	0.4459

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: AgentTesla, MASS Logger, Remcos, RemcosRAT, XWorm.
- 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	104[.]239[.]66[.]86	AbuseIPDB 0% (FR) · XWorm · AS214961 Stellar Group SAS
Domain	mail[.]taikei-rmc-co[.]biz	

Type	Indicator	Context
Domain	mail[.]allportcargoservice[.]com	
Domain	newremupdate[.]duckdns[.]org	Remcos
Domain	mail[.]trimnt[.]com	MASS Logger
Domain	mail[.]teamengineersgroup[.]com	
Hash	511ba918e1781ff38310530801b8cec5	
Hash	c029ceede8f8f8c8a4f58687e6681536fe4cc97b	
Hash	41ad1f28134f4b4a443b53af04aeb3fa57a2f72a3cc58a6466e84fc3225f38be	
Hash	2b1248d89fd9a7c716816f9688402942827fc1bfa89d5dccd741521725104279	
Hash	417fc4d6119dac40f276b563498a0ad3f9bf42262ec650a4463cbdbe78da388b	RemcosRAT
Hash	619d2628dcf0c8e15a6febb0e562609556ca57f9f8216800ee77a39e336b8bf4	AgentTesla
Hash	96e22da4d5c0ea4b0efde0ad3eaa8fdedc60228f84fb3c56899afbb9338da2a1	AgentTesla
Hash	ba2793c45a12e96683a8b1b7cb5a5c3e	
Hash	c5724b86aae0e637b8b0b6f3c8d31168	
Hash	efd92efb0321bf811e74717974b14897	AgentTesla
Hash	ff3db8cc2d38ca5878a32fe40d7a8ba5	AgentTesla
Hash	409f57557a91d2a7a424d122aef4e73f2b533b18	
Hash	425ba7d4138a0e72e0e32db5438ee4bd88aa2982	AgentTesla
Hash	9d8a4d41058d5d7934d55f2c97d032124a0d74e3	
Hash	f17ee43fda3735a0eea7330774ed6c10c0749fa5	AgentTesla
Hash	05390dd0d2c84f77475c0c6aa082638e23977da591302e911cbcb071c42a9451	

Type	Indicator	Context
Hash	1539468a21a439dd4f8d72a6c34ce503f0585281fc2e885 35c3c33727bfdc717	
Hash	16516e3298278719123068bf0ed808ea4e00f73c970a8a 83377066b4e3c3c950	
Hash	16f9692debe0d4e35d76b48312979e5a90a85ce066e737 5269ce78f43da52769	
Hash	1c4419d687bf45bdc5474b6347e41e89459fc0f5115f0d01 2c46c57280b242bf	
Hash	1d9dd914cf623dcae4b88834744a005e5e3eae827ded1a afd23ed1d7be57b90a	
Hash	2fe30eccd36f4346cb117af0cf626c2bca84b50c658b0c9af 09110b9f86a53f4	
Hash	3ace400380bd1fc51e83d008dbbe9ceb70b2572da95264 be09d85979a6276a37	
Hash	4c001e107a42d65c1b1e6092e4aa6932dbd1544d097d1 a432ba27e3b4bddfcc1	
Hash	5409b3fa21dcc2f854697ec731f9574603dd0b6bdfd892e 968a2b412ed85f52c	
Hash	5b271a1b1ffe2716ae420f8e9d40dbc8e9e682f6e4125d4f 174a335bf070ac29	
Hash	6700e6d2a0c285d3ebf1a55aecec63b1e42d7d581f6913 31c667a8920dac7029	
Hash	775ae9a8c7363e2368cbb559f9c2d26a6c479d4e7998fe 71d45830885ccde429	
Hash	7df42fc54f053d1bb65f43d4386a75be02770f7923b66e71 3fb04631582e864e	
Hash	81edd5e740bea0fefb5c1bbd14a671bd1daff37bf3641e34 f3a1f7e93559184a	
Hash	8c28bc87eb4f2613117d41a716e78f62d55c19edaeea573 c2c96e787da055167	
Hash	9674da676ee226ee456d35c774715d9b58655423806f28 1de19dc9ef899e9532	

Type	Indicator	Context
Hash	986d1d5270822af7d7744762ecd8fc4e9b2886c85b3660e9fdf0b5906d6c4117	
Hash	b12b743d4ecc0fe7320b6c1533e2a60bb89f94ca39a5be37143e7af27daacf04	

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:** T1112 Modify Registry (persistence)
- **Observed here:** the threat actor used T1053.005 Scheduled Task here as an alternative persistence technique.
- **Projected pivot:** T1053.005 Scheduled Task (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to utilizing Scheduled Task (T1053.005) to maintain persistence and execute malicious code at a later time, potentially bypassing the blocked registry modification technique. This approach may allow the actor to achieve their objective by scheduling a task that runs with elevated privileges, which would likely evade detection if not properly monitored. The defensive control to counter this would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Detection and hardening for the pivot (T1053.005 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