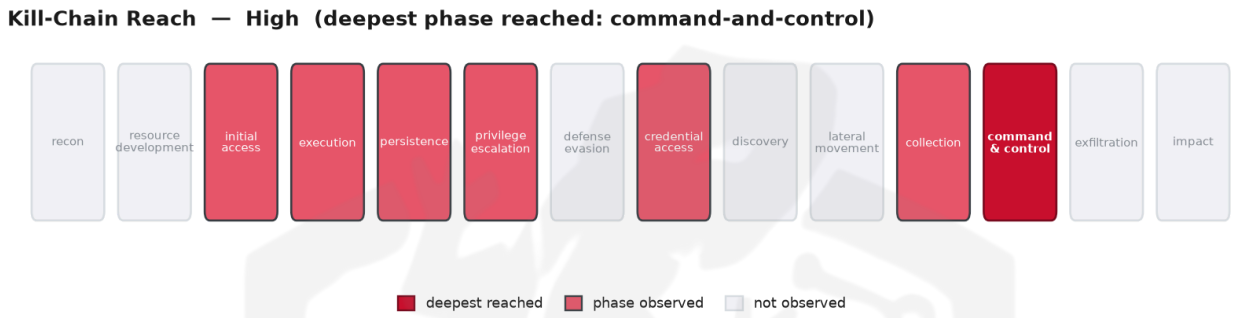
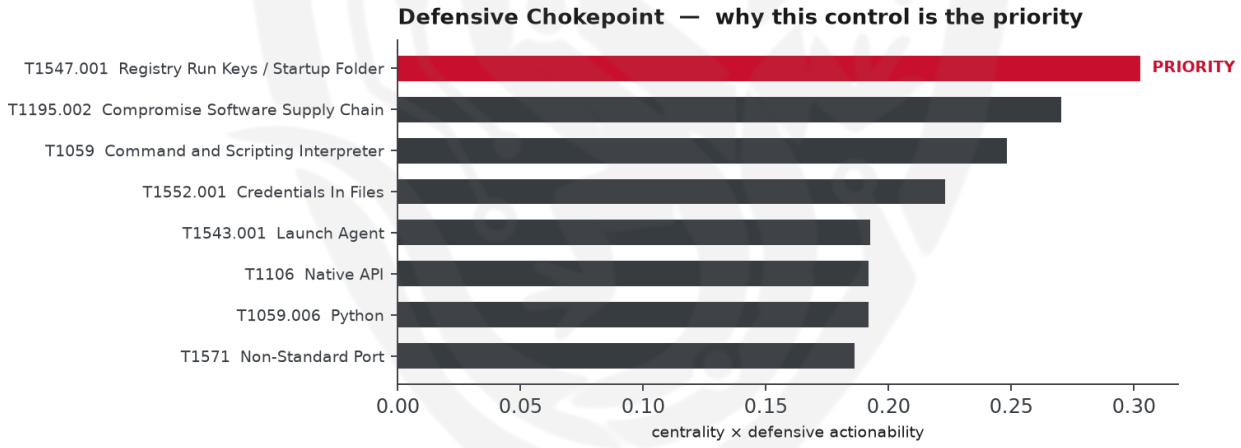
THREAT REPORT: MIASMA WORM TARGETS TECHNOLOGY SECTOR

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 involves the Miasma v3 malware family, targeting the technology sector. The threat actor's identity and targeted country are unknown. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to mitigate the threat. The operational risk band is considered high, indicating a significant command-and-control capability.

Threat Overview

The threat actor, whose identity is insufficient to determine, is utilizing the Miasma v3 malware family to compromise software dependencies and development tools. The targeted sector is technology, although the specific country and central CVE exploited are unknown. The malware family employs various techniques, including standard encoding, JavaScript, and symmetric cryptography.

Attack Chain and Priority Control

The observed techniques form a complex chain, including compromise of software dependencies, encoding, and symmetric cryptography. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which serves as a 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 is hosted on SOLLUTIUM EU Sp z.o.o., as observed by third-party sources. However, no malware families have been corroborated by abuse.ch, and no indicators have reached an 80% confidence level on AbuseIPDB, 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)

- T1132.001 Standard Encoding
- T1059.007 JavaScript
- T1195.001 Compromise Software Dependencies and Development Tools
- T1573.001 Symmetric Cryptography
- T1106 Native API
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1059 Command and Scripting Interpreter
- T1552.001 Credentials In Files
- T1547.001 Registry Run Keys / Startup Folder
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1059.006 Python
- T1543.001 Launch Agent
- T1071.001 Web Protocols
- T1543.002 Systemd Service
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.3187).
- 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 0.4168; 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
APT33	0.4168
Rocke	0.3753
BRONZE BUTLER	0.3752
APT19	0.3608
MuddyWater	0.3579

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	85[.]137[.]53[.]71	AbuseIPDB 0% (NL) · AS43641 SOLLUTIUM EU Sp z.o.o.
Domain	obfuscator[.]io	
URL	hxxp://85[.]137[.]53[.]71:8080	
URL	hxxp://85[.]137[.]53[.]71:8081	
URL	hxxp://85[.]137[.]53[.]71:8091	

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.

The actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious code at a later time, potentially exploiting the fact that scheduled tasks can be used to bypass some security controls and blend in with legitimate system activity. This technique may be particularly appealing as it allows the actor to execute tasks with elevated privileges, which could be leveraged to regain a foothold in the system. To counter this, the defensive control of alerting on new scheduled tasks (Event ID 4698), restricting schtasks/at to admins, and baselining legitimate task creators should be implemented.

Also plausible (same tactic): T1098 Account Manipulation (n=12, lift 2.0), T1112 Modify Registry (n=17, lift 1.7)

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