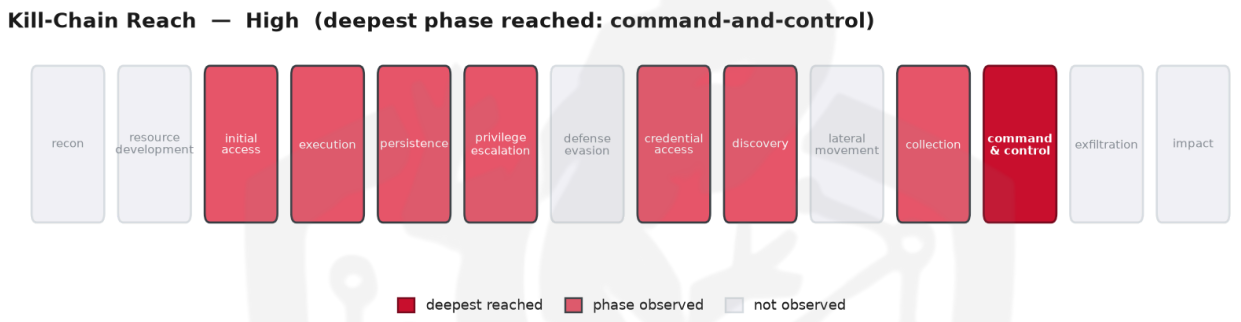
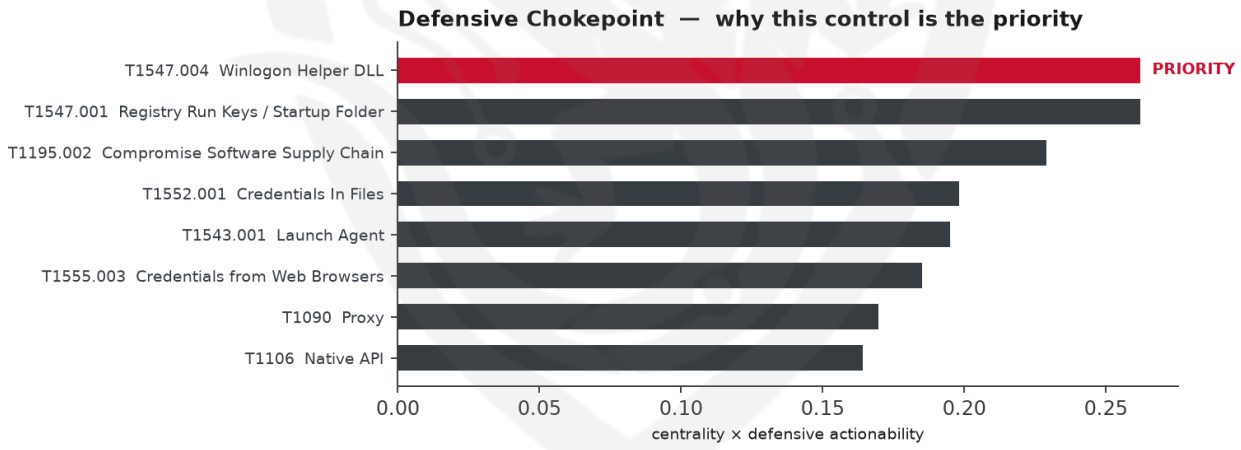
THREAT REPORT: UNPACKING THE ASYNCAPI NPM SUPPLY CHAIN COMPROMISE AND IMPORT-TIME PAYLOAD DELIVERY

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

This brief covers activity involving Miasma, BLUERABBIT, GigaWiper, with no single central CVE identified, affecting targets not specified by the source. The source does not attribute this activity to a named actor. The operational risk is assessed as High. Priority should be given to the control described below, centred on T1547.004 Winlogon Helper DLL.

Threat Overview

The activity is associated with an as-yet unattributed cluster of activity. Malware observed: Miasma, BLUERABBIT, GigaWiper. Reported victimology: targets not specified by the source.

Attack Chain and Priority Control

The source records the following techniques: - T1132.001 Standard Encoding - T1059.007 JavaScript - T1071.004 DNS - T1036.005 Match Legitimate Resource Name or Location - T1082 System Information Discovery - T1106 Native API - T1005 Data from Local System - T1140 Deobfuscate/Decode Files or Information - T1555.003 Credentials from Web Browsers - T1547.004 Winlogon Helper DLL - T1090 Proxy - T1083 File and Directory Discovery - T1552.001 Credentials In Files - T1547.001 Registry Run Keys / Startup Folder - T1027 Obfuscated Files or Information - T1573 Encrypted Channel - T1195.002 Compromise Software Supply Chain - T1543.001 Launch Agent - T1071.001 Web Protocols - T1543.002 Systemd Service - T1105 Ingress Tool Transfer - T1102.001 Dead Drop Resolver - T1552.007 Container API

Priority should be given to T1547.004 Winlogon Helper DLL. Recommended control: Baseline and monitor autostart locations (Run keys, startup folders); alert on new persistence entries.

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
- T1071.004 DNS
- T1036.005 Match Legitimate Resource Name or Location
- T1082 System Information Discovery
- T1106 Native API
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1555.003 Credentials from Web Browsers
- T1547.004 Winlogon Helper DLL
- T1090 Proxy
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1195.002 Compromise Software Supply Chain
- T1543.001 Launch Agent
- T1071.001 Web Protocols
- T1543.002 Systemd Service
- T1105 Ingress Tool Transfer
- T1102.001 Dead Drop Resolver
- T1552.007 Container API

Analytical Scores

- Priority technique (graph chokepoint): T1547.004 Winlogon Helper DLL (centrality 0.2761).
- 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 0.4488; 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
Tropic Trooper	0.4488
Inception	0.4244
APT18	0.4167
MuddyWater	0.4011
Rocke	0.4

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.
Hash	34014776d3d3ff11bc4439b02fd7ac0f02a887eb3a052eeafff236e2f6db8ad1	
Hash	082d733db0687dcd768104972b065d4b58cb1e6043688c6c20fa3702337f36ab	
Hash	bfaeb987faa6de2b5a5eb63b1233d055215b09b0349a9394f2175fd7cdf385e4	

Type	Indicator	Context
Hash	9b2e65db653ca8575c9b10eefb9a80c6006404812c2ec212bf5675e3c690233b	
Hash	d425e4583cc6185d41e95c45eda00550045a5d1919b9a012236a4520d009dbd7	
Hash	8351d251cf0b5a0bd82242deaa0a14e3e1394418d55c0f4259dac4303b79fc0c	
Hash	c70e105e212ff3c1daa04bb2a62507717f296b0b	
Hash	d602f4eeb914cf32782799376a8c5953	
Hash	93d8cffab1171a115228808e526d9bd7fe935e4e	
Hash	69813c330d52f2a93082651c071a302c	
Hash	71e67d32d2a6e052893dc0c679f9f7fd	
Hash	8c09a52a15a6e617e2b6ccee11046805	
Hash	cd961d0b7b29996b795ddc80c09cc5d9	
Hash	e67c6be63e55148de424e030cf6bed3b	
Hash	1f5c2e809d1ebd369d34ac22b771c522ced6e5b4	
Hash	46a236cc9f140deb62bbcfb055e7865d5b23ad81	
Hash	9b65b9f1bb27cef7b8a2b0327a47a539b8e473fb	
Hash	ef2d28477befaa103031c7182a6f0dd6b4bb82dd	

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:** T1547.004 Winlogon Helper DLL (persistence)
- **Observed here:** the threat actor used T1543.001 Launch Agent here as an alternative persistence technique.
- **Projected pivot:** T1543.001 Launch Agent (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

With T1547.004 Winlogon Helper DLL blocked, the threat actor could preserve the same objective by pivoting to T1543.001 Launch Agent, a technique observed in this campaign. Defensive countermeasure: Restrict service/daemon creation to admins; monitor service and driver installs.

Detection and hardening for the pivot (T1543.001 Create or Modify System Process)

- **Telemetry:** Windows Security / System log; Sysmon
- **Detect:**
  - System 7045 (new service installed); Security 4697 (service installed)
  - Sysmon 1 for sc.exe / services created; unusual ImagePath or user-context services
  - Registry writes under HKLM\SYSTEM\CurrentControlSet\Services
- **Harden:**
  - Restrict service creation to admins; application control on service binaries
  - Baseline installed services and alert on new/anomalous ones
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0019 Service, DS0024 Windows Registry, DS0009 Process