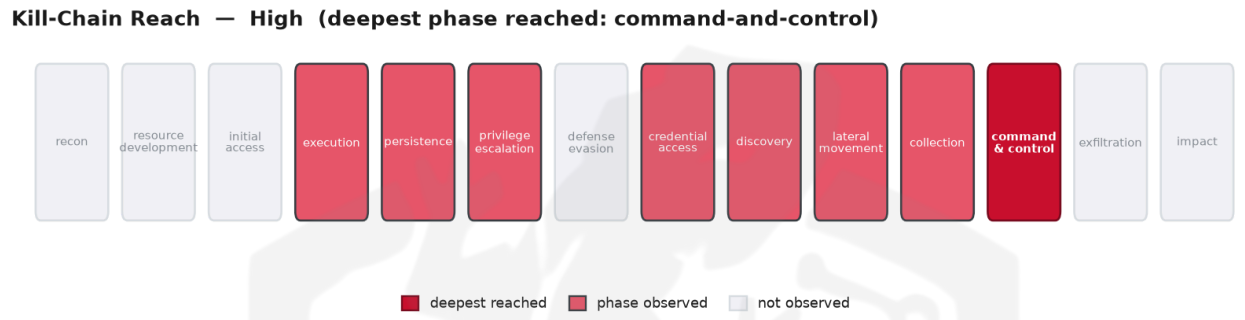
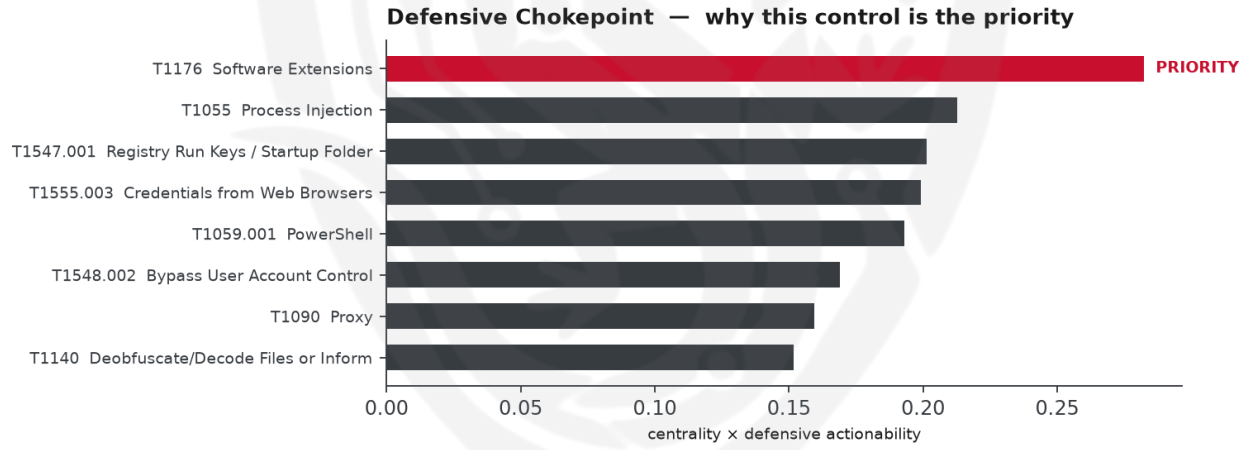
THREAT REPORT: OKOBOT FRAMEWORK INFECTION CHAIN

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 TookPS, TeviRAT, Rilide, SeedHunter, OkoSpyware, HDUtil, with no single central CVE identified, affecting Brazil, Canada, Mexico. 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 T1176 Software Extensions.

Threat Overview

The activity is associated with an as-yet unattributed cluster of activity. Malware observed: TookPS, TeviRAT, Rilide, SeedHunter, OkoSpyware, HDUtil. Reported victimology: Brazil, Canada, Mexico.

Attack Chain and Priority Control

The source records the following techniques: - T1053.005 Scheduled Task - T1113 Screen Capture - T1033 System Owner/User Discovery - T1056.001 Keylogging - T1539 Steal Web Session Cookie - T1548.002 Bypass User Account Control - T1115 Clipboard Data - T1082 System Information Discovery - T1176 Software Extensions - T1140 Deobfuscate/Decode Files or Information - T1055 Process Injection - T1185 Browser Session Hijacking - T1555.003 Credentials from Web Browsers - T1090 Proxy - T1059.001 PowerShell - T1547.001 Registry Run Keys / Startup Folder - T1562.001 Impair Defenses: Disable or Modify Tools - T1059.003 Windows Command Shell - T1027.002 Software Packing - T1021.001 Remote Desktop Protocol

Priority should be given to T1176 Software Extensions. Recommended control: Apply the specific MITRE ATT&CK mitigation for this technique; add host/network detections and least-privilege controls around it.

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
- T1113 Screen Capture
- T1033 System Owner/User Discovery
- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1548.002 Bypass User Account Control
- T1115 Clipboard Data
- T1082 System Information Discovery
- T1176 Software Extensions
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1185 Browser Session Hijacking
- T1555.003 Credentials from Web Browsers
- T1090 Proxy
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1059.003 Windows Command Shell
- T1027.002 Software Packing
- T1021.001 Remote Desktop Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1176 Software Extensions (centrality 0.2973).
- 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 0.4668; 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
FIN10	0.4668
Patchwork	0.4364
APT37	0.426
APT3	0.417
APT39	0.4082

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
Domain	coffeesaloon[.]online
Domain	livewallpapers[.]online
Domain	2baserec2[.]guru
Domain	kbeautyreviews[.]com
Domain	recavb22[.]online
Domain	thatwascringe[.]com
Hash	b07d451ee65a1580f20a784c8f0e7a46
Hash	187a1f68ae786e53d3831166dc84e6d2
Hash	d84e8dc509308523e0209d3cd3544619
Hash	83e6b8fcb92a0b13e109301f8ff649cf

Type	Indicator
Hash	7306885bb4c98f2a9f056104cf092bc9
Hash	b4c2e16cdb513be4dc798f88e2527334
Hash	2157d2429124ad28db7a26f2477cb985
Hash	77cecf5e2a622ae07d8ae9913457ab57
Hash	e0c3bc27a65750e740c4f1719e531c7d
Hash	3d2b43f91f65bfbf36a9c71b6b418876
Hash	70fef9fd6e351f4d53cfeee8dcdfcd99
Hash	acd31c9941b6c1cabd4e45e6877b9038
Hash	dd52f5108a176c62ad807c327734ad12
Hash	ac93a821617aea1f56d4bc0bef4af327
Hash	11dbc8a2bea04b15f8f68f3f01e8faf9

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:** T1176 Software Extensions (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).

With T1176 Software Extensions blocked, the threat actor could preserve the same objective by pivoting to T1053.005 Scheduled Task, a technique observed in this campaign. Defensive countermeasure: 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