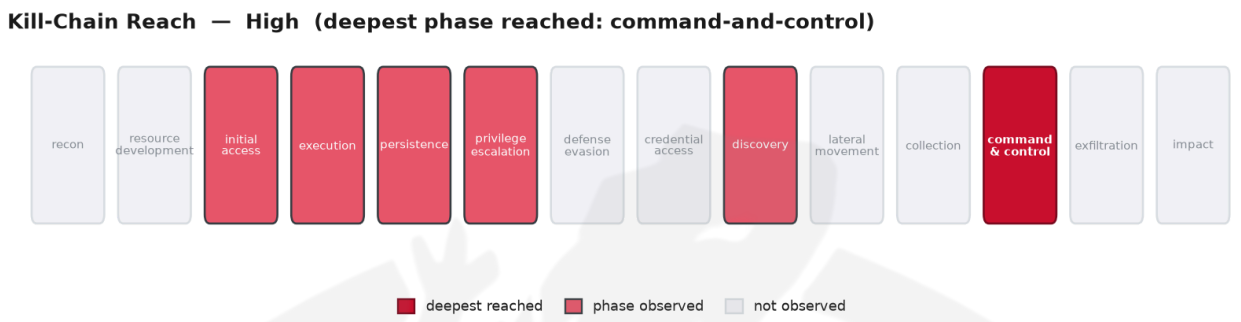
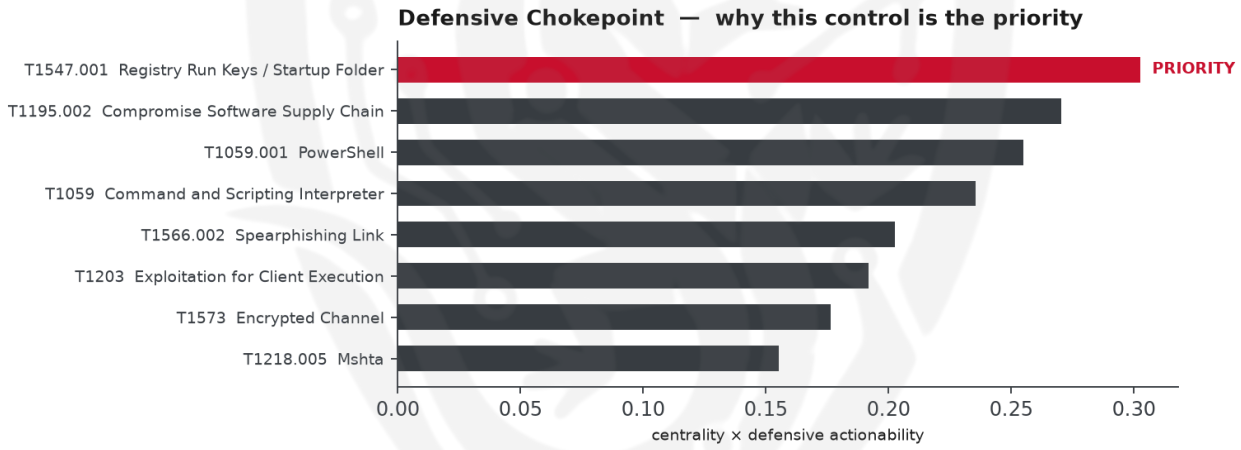
THREAT REPORT: SMARTAPESG

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 SmartApeSG, a threat actor who has been observed targeting the retail sector with a range of malware families, including NetSupport, Remcos, StealC, Sectop RAT, and SmartRAT. The actor's campaign has been identified as a supply chain attack, with a focus on exploiting vulnerabilities to gain control of targeted systems. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. The threat actor's use of various techniques, including scheduled tasks and spearphishing links, highlights the need for robust defensive measures.

Threat Overview

The threat actor, SmartApeSG, has been observed using a range of malware families to target the retail sector. The central vulnerability exploited in this campaign is currently unknown, but the actor has been linked to several techniques, including scheduled tasks, Windows Management Instrumentation, and

spearphishing links. The actor's victimology is focused on the retail sector, although the targeted country is not specified.

Attack Chain and Priority Control

The observed techniques used by SmartApeSG can be described as a chain of events, starting with initial exploitation and leading to command-and-control. The priority technique in this chain is T1547.001 Registry Run Keys / Startup Folder, which serves as a chokepoint for the actor's malicious activity. To mitigate this threat, 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

There is currently no information available on the hosting providers or ASNs used by SmartApeSG, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with a confidence level of 80% or higher by 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)

- T1053.005 Scheduled Task
- T1047 Windows Management Instrumentation
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1059 Command and Scripting Interpreter
- T1218.005 Mshta
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1195.002 Compromise Software Supply Chain
- T1203 Exploitation for Client Execution
- T1071.001 Web Protocols
- T1059.005 Visual Basic
- T1105 Ingress Tool Transfer
- T1204.001 Malicious Link

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 0.6803; 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
Confucius	0.6803
Molerats	0.64
Windshift	0.6124
TA2541	0.5864
Cobalt Group	0.5824

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
URL	hxxp://cdn-static[.]okendo[.]io/reviews-widget-plus/js/okendo-reviews[.]js
URL	hxxps://api[.]wigetticks[.]com/logout/private-response[.]php?8D1V4th3
URL	hxxps://api[.]wizzleticks[.]com/claims/scope-schema[.]php?4ManBBdA

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:** SmartApeSG 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 SmartApeSG actor could pivot to utilizing Scheduled Task (T1053.005) to maintain persistence and achieve their objectives, potentially by creating a new task that blends in with legitimate system activity, which may allow them to evade detection. This technique would likely involve creating a task that appears benign, making it harder for defenders to distinguish from legitimate tasks. 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.

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