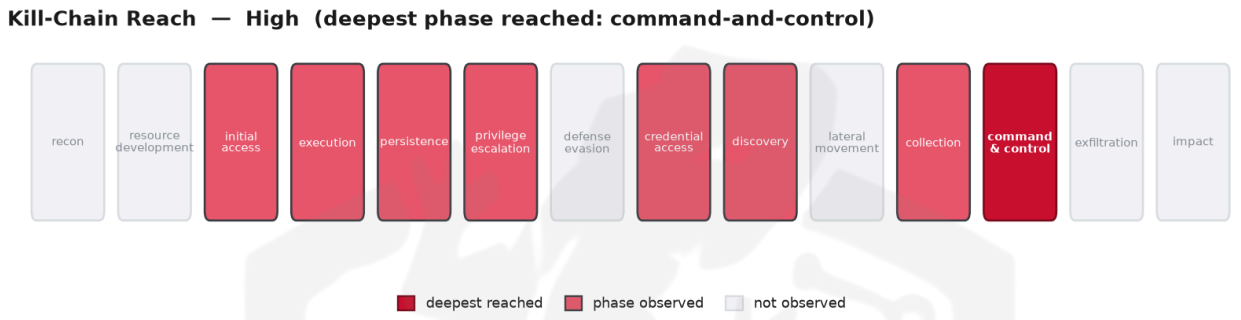
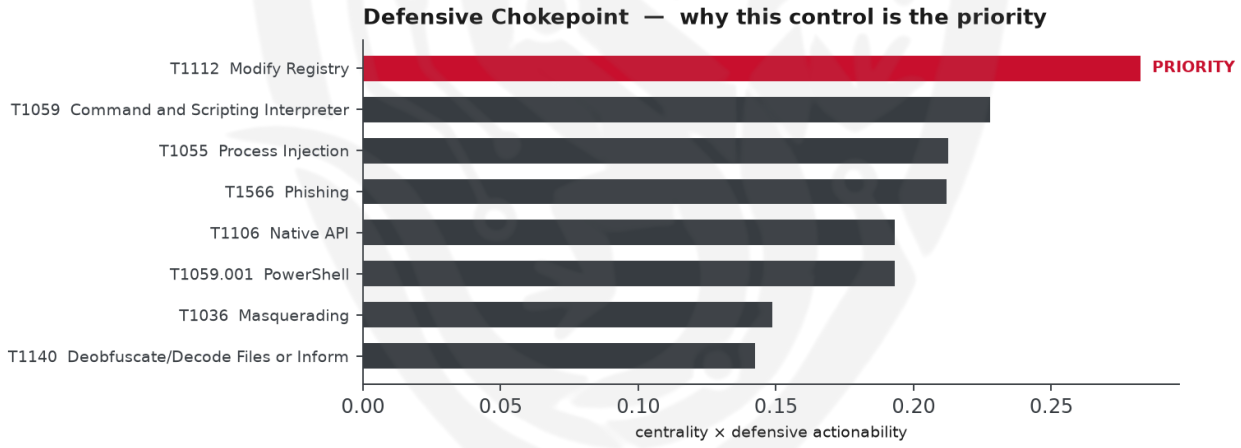
THREAT REPORT: BRAZIL FINANCE SECTOR TARGETED WITH SMARTRAT

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 delivering SmartRAT, along with other malware families such as Banana RAT, Remcos RAT, and GhostLoader, to targets in the finance sector in Brazil. The threat actor's identity remains unknown. Priority should be given to monitoring sensitive registry keys for modification to mitigate the threat. The finance sector in Brazil is at high risk due to the potential command-and-control capabilities of the malware.

Threat Overview

The threat actor, whose identity is not specified, is utilizing a range of malware families including SmartRAT, Banana RAT, Remcos RAT, and GhostLoader to target the finance sector in Brazil. The actor is

leveraging various techniques to achieve their goals, including screen capture, keylogging, and system information discovery. The targeted country is Brazil, with a focus on the finance sector.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including screen capture, keylogging, and system information discovery. The priority technique is T1112 Modify Registry, which is the graph chokepoint. To mitigate this threat, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

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

- T1113 Screen Capture
- T1056.001 Keylogging
- T1543.003 Windows Service
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1106 Native API
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1055 Process Injection
- T1185 Browser Session Hijacking
- T1112 Modify Registry
- T1059 Command and Scripting Interpreter
- T1497 Virtualization/Sandbox Evasion
- T1059.001 PowerShell
- T1566 Phishing
- T1027 Obfuscated Files or Information
- T1070.004 File Deletion
- T1518 Software Discovery
- T1569.002 Service Execution

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (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 0.4885; 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
APT38	0.4885
Group5	0.4629
Silence	0.4047
Tropic Trooper	0.3819
BlackByte	0.3769

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	crefisa[.]online
Domain	windowsupdate-cdn[.]com
Domain	c[.]windowsupdate-cdn[.]com
Domain	cartaobb[.]com
Domain	cartaobrb[.]com[.]br
Domain	vfsgloball[.]net
URL	hxxp://64[.]95[.]13[.]238/payload[.]php'

Type	Indicator
Hash	297eb45f028d44d750297d2f932b9c91
Hash	3c72e1f37f115b00c3ad6ed31bacfe8a
Hash	6bf4d4c62b5138ace281ce3d08297787
Hash	b17ccdb5531555e43f082d6e77c07227

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:** T1112 Modify Registry 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 19+ groups that use Modify Registry, 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 leveraging the Windows Task Scheduler to blend in with legitimate system activity, which may allow them to bypass defenses that are focused on immediate execution. This technique in particular may be appealing to the actor because it enables them to schedule tasks to run under the context of a specific user or system account, which could help them to evade detection. To counter this potential move, 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): T1547 Boot or Logon Autostart Execution (n=17, lift 1.7), T1505 Server Software Component (n=11, lift 2.0)

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