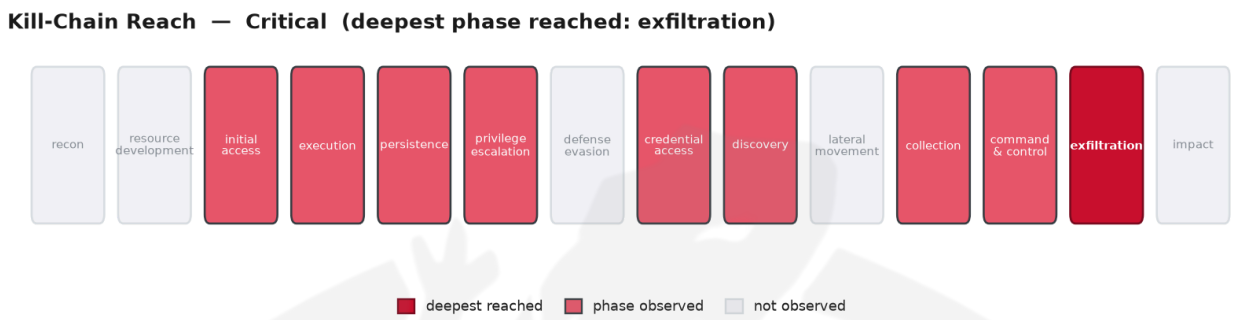
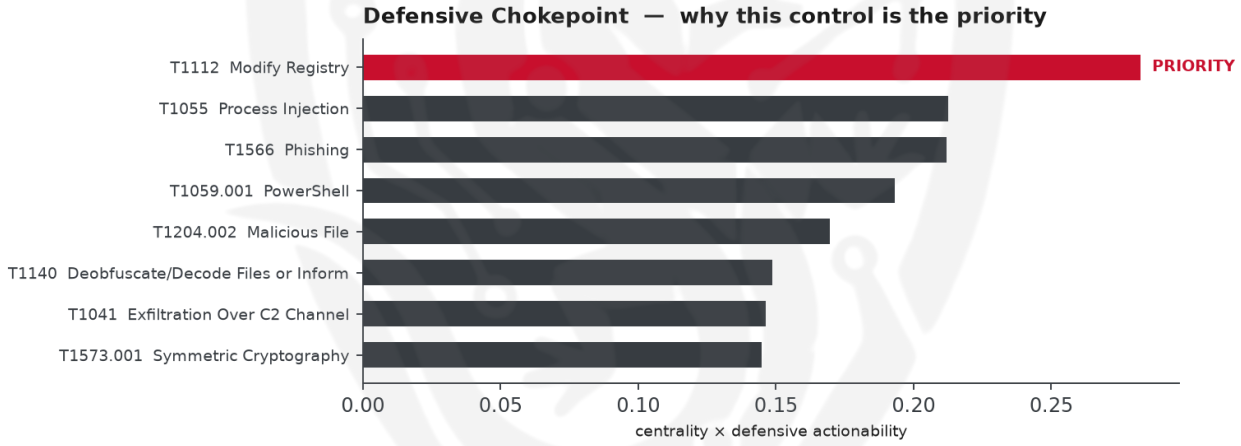
THREAT REPORT: SHADOW-WATER-063

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 SHADOW-WATER-063, a threat actor targeting the finance sector in Brazil. The actor utilizes various malware families, including Banana RAT and Grandoreiro, to carry out their operations. Priority should be given to monitoring sensitive registry keys for modification to prevent further damage. The threat actor's ability to exfiltrate data poses a critical operational risk.

Threat Overview

SHADOW-WATER-063, the observed threat actor, employs a range of malware families, including Banana RAT, Grandoreiro, Mekotio, and others, to target financial institutions in Brazil. The actor's tactics involve exploiting various techniques to gain access to sensitive information. The victimology suggests a focus on the finance sector, with the actor seeking to compromise financial data.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including scheduled tasks, screen capture, keylogging, and process injection, ultimately leading to data exfiltration. The priority technique is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this activity. Additionally, no malware families have been corroborated by abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level 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)

- T1053.005 Scheduled Task
- T1113 Screen Capture
- T1056.001 Keylogging
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1115 Clipboard Data
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1185 Browser Session Hijacking
- T1112 Modify Registry
- T1083 File and Directory Discovery
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1566 Phishing
- T1001 Data Obfuscation
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1564.001 Hidden Files and Directories

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2973).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5017; 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
Higaisa	0.5017
Winter Vivern	0.4725
RedCurl	0.4636
Darkhotel	0.4537
Stealth Falcon	0.4336

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	windowsk-cdn[.]com
Domain	c[.]windowsk-cdn[.]com
Domain	convitemundial2026[.]com
URL	hxxp://24[.]199[.]90[.]58/payload[.]php
URL	hxxp://24[.]199[.]90[.]58:80/payload[.]php
URL	hxxps://convitemundial2026[.]com/Consultar_NF-e[.]bat
Hash	38dfeb772afbd01c04eddda120d283acfb1147a6dc3d54ac62fe23ad06e39d8f
Hash	4912b1134e69ade7266e8508eec33ccb2d80ad693f1dbc4f1f4344c6dfcf2ff1
Hash	d7545b6dacebdae27effb3c778c5e349027ec789c76ae4f777bd9ba56a70cdaa
Hash	ecdc8fade561a75d68235859ad8b1fe131db2c458b4894268e38e90ecab1c47f