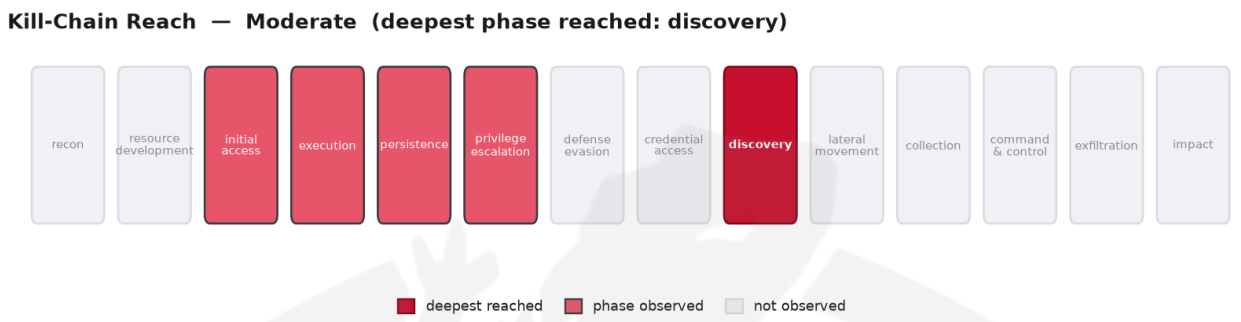
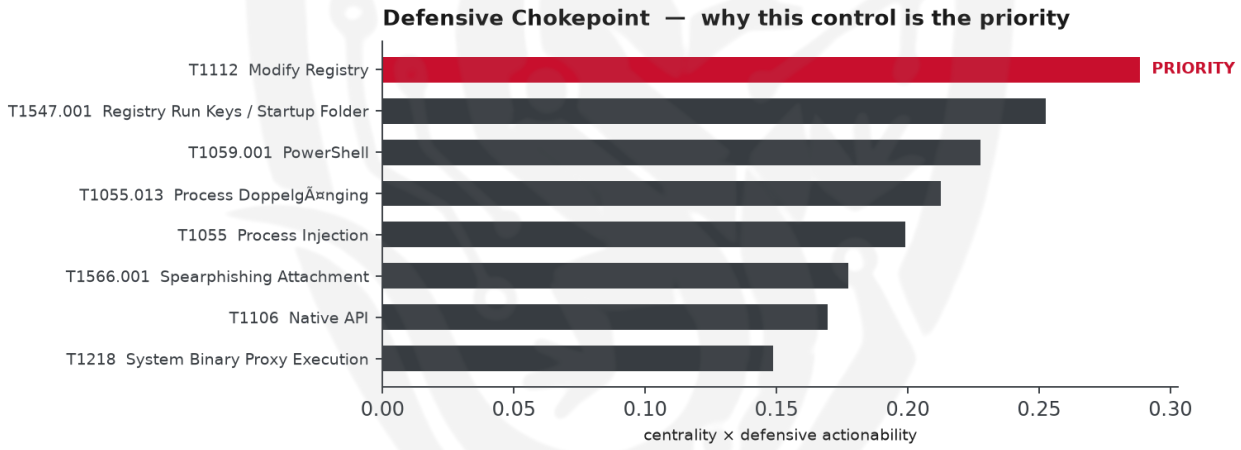
THREAT REPORT: TA4922

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 TA4922, a threat actor utilizing a sophisticated crypter service to deploy various malware families, including Cruciferra, zgRAT, and AgentTesla, among others. The targeted sectors include Finance, Healthcare, Government, and Hospitality. Priority should be given to monitoring sensitive registry keys for modification to mitigate the threat. The actor's techniques suggest a moderate operational risk band, reaching the 'discovery' stage.

Threat Overview

TA4922, the observed threat actor, employs a range of malware families to target multiple sectors. The malware families used include Cruciferra, zgRAT, AgentTesla, and several others. The victimology indicates that the threat actor is targeting the Finance, Healthcare, Government, and Hospitality sectors. The central vulnerability exploited is not specified due to insufficient data.

Attack Chain and Priority Control

The threat actor's attack chain involves various techniques, including rootkit usage, bypassing user account control, and process injection. The priority technique identified is T1112 Modify Registry, which serves as a chokepoint in the attack chain. 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

The malicious infrastructure is hosted on Dedik Services Limited. Additionally, abuse.ch has corroborated the presence of StormKitty and XWorm malware families. However, according to AbuseIPDB, there are no 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)

- T1014 Rootkit
- T1548.002 Bypass User Account Control
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1055 Process Injection
- T1218 System Binary Proxy Execution
- T1112 Modify Registry
- T1055.013 Process DoppelgÃ¤nging
- T1497 Virtualization/Sandbox Evasion
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1564.003 Hidden Window
- T1134 Access Token Manipulation
- T1574.002 Hijack Execution Flow

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3037).
- Operational risk: Moderate (score 0.539, reaches discovery).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6255; 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
Gorgon Group	0.6255
Nomadic Octopus	0.5427
APT19	0.5303
DarkHydrus	0.4619
Molerats	0.44

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: StormKitty, XWorm.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	89[.]34[.]90[.]99	AbuseIPDB 0% (DE) · AS207043 Dedik Services Limited
Domain	almacensantangel[.]com	malware_download
Domain	gatuso[.]duckdns[.]org	XWorm
Domain	0zbqnac1t4dv2t2wuodv1m[.]com	
Domain	digital-magicians[.]com	malware_download

Type	Indicator	Context
Domain	fiusyevr[.]live	
Domain	fvxcuvuyte[.]live	
URL	hxxps://almacensantangel[.]com/wp-includes/assets/YourSSA_Documents_0000000676152_05_187_2026_Document_0000000676152[.]rar	
URL	hxxp://faeytrdeaw[.]gu[.]cc	
URL	hxxp://figyuyrqwr[.]gu[.]cc	
URL	hxxp://fiusyevr[.]live	
URL	hxxp://fuaytrwese[.]love	
URL	hxxp://hfyuayustrv[.]gu[.]cc	
URL	hxxp://hsahyteiows[.]gu[.]cc	
URL	hxxp://jaiydteds[.]love	
URL	hxxp://jsiruytrawey[.]gu[.]cc	
URL	hxxp://kawosyetw[.]gu[.]cc	
URL	hxxp://kawuuterta[.]gu[.]cc	
URL	hxxp://laiwutrencr[.]gu[.]cc	
URL	hxxp://lasiduutfe[.]gu[.]cc	
URL	hxxp://lisiutegrm[.]live	
URL	hxxp://maisytawe[.]gu[.]cc	
URL	hxxp://mksfuuerwo[.]live	
URL	hxxp://ncduuyese[.]live	
URL	hxxp://nciyeyrawoe[.]gu[.]cc	
URL	hxxp://nviuawusye[.]gu[.]cc	
URL	hxxp://nvsieyrrawe[.]gu[.]cc	
URL	hxxp://paiwudyea[.]love	

Type	Indicator	Context
URL	hxxp://pmcjsuyraw[.]gu[.]cc	
URL	hxxp://qeuasytua[.]love	
URL	hxxp://svuatwea[.]love	
URL	hxxp://syfiaydytea[.]live	
URL	hxxp://viuyeyrwqs[.]gu[.]cc	
URL	hxxp://vusuydryt[.]love	
URL	hxxp://xkcifgieusr[.]gu[.]cc	
URL	hxxp://xnbscuya[.]love	
URL	hxxp://xuastyrdqk[.]love	
URL	hxxp://yicoweytcbtw[.]gu[.]cc	
Hash	09bedbf7a41e0f8dabe4f41d331db58373ce15b2e9204540873a1884f38bdde1	
Hash	5b4f59236a9b950bcd5191b35d19125f60cfb9e1a1e1aa2e4f914b6745dde9df	

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:** T1112 Modify Registry (persistence)
- **Observed here:** TA4922 used T1547.001 Registry Run Keys / Startup Folder here as an alternative persistence technique.
- **Projected pivot:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The adversary could pivot to using T1547.001 Registry Run Keys / Startup Folder to maintain persistence, potentially by adding malicious entries to the Startup folder or Run/RunOnce registry keys, which may allow them to regain a foothold after the block on modifying the registry. This technique could be used to execute malicious code automatically when a user logs in, which would likely undermine the defender's previous control. To counter this potential move, the mandated defensive 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.

Detection and hardening for the pivot (T1547.001 Boot or Logon Autostart Execution)

- **Telemetry:** Sysmon (registry + process); EDR autostart/ASEP inventory
- **Detect:**
  - Sysmon 13 (registry value set) on Run/RunOnce keys under HKLM & HKCU ...\CurrentVersion\Run*
  - Sysmon 11 for shortcuts/scripts created in Startup folders
  - Periodic ASEP (autostart extensibility point) diff against a known-good baseline
- **Harden:**
  - Restrict write access to autostart registry keys and Startup folders
  - Application control to block unsigned autostart binaries
- **MITRE:** M1047 Audit, M1038 Execution Prevention · DS0019 Service, DS0024 Windows Registry, DS0022 File