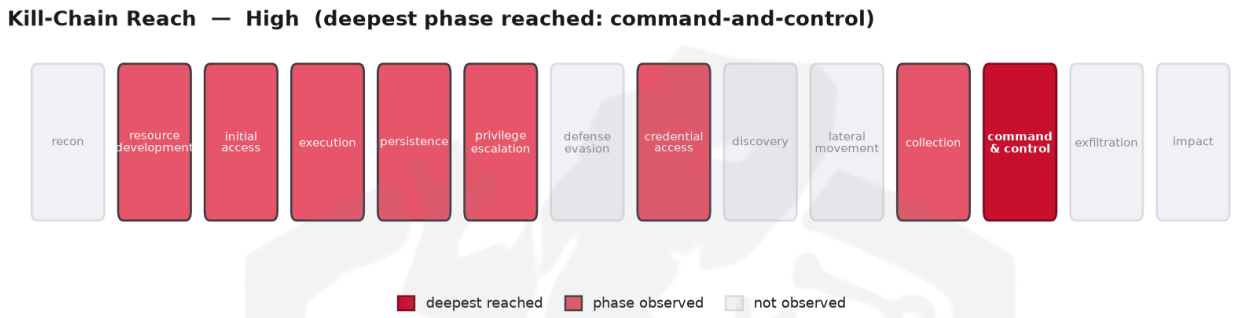
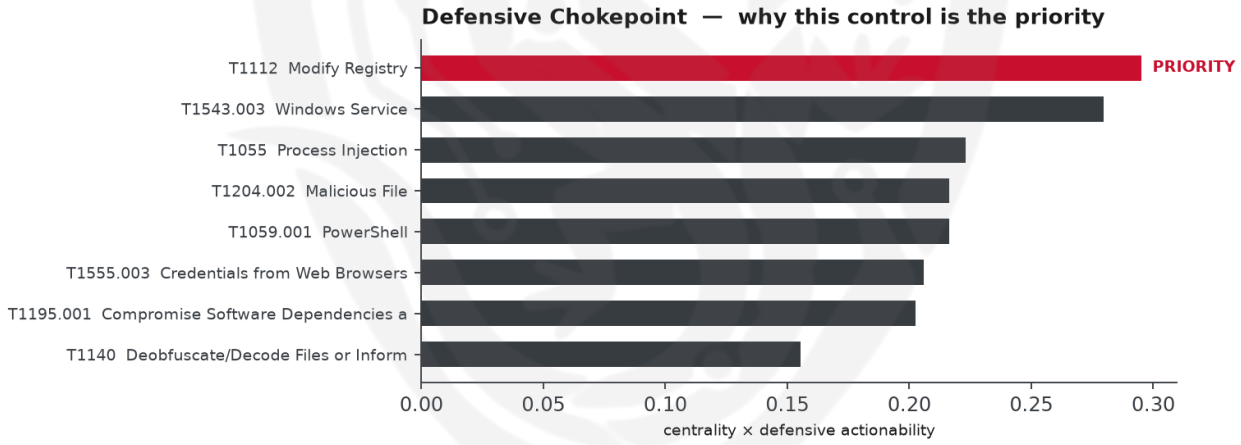
THREAT REPORT: UNKNOWN_ADVERSARY MALICIOUS GO MODULE CAMPAIGN

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 linked to a network of 222 repositories on GitHub, utilizing malicious Go modules to spread malware. The malware families involved include AsyncRAT, Quasar, Remcos, Vidar, and XMRig. Priority should be given to monitoring sensitive registry keys for modification and restricting registry-edit tools for unprivileged users. The threat actor's targets and motivations are currently unknown.

Threat Overview

The threat actor, whose identity is unknown, has been observed using a range of malware families, including AsyncRAT, Quasar, Remcos, Vidar, and XMRig. The central vulnerability exploited is currently

unknown. The actor's techniques include scheduled tasks, screen capture, bypassing user account control, and compromising software dependencies and development tools.

Attack Chain and Priority Control

The observed techniques form a complex chain, starting with compromising software dependencies and development tools, followed by scheduled tasks, screen capture, and bypassing user account control. 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

The malicious infrastructure is not associated with any specific hosting providers or ASNs. However, abuse.ch has corroborated the presence of RustyStealer and Vidar malware families. 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)

- T1053.005 Scheduled Task
- T1113 Screen Capture
- T1548.002 Bypass User Account Control
- T1195.001 Compromise Software Dependencies and Development Tools
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1543.003 Windows Service
- T1140 Deobfuscate/Decode Files or Information
- T1608.001 Upload Malware
- T1055 Process Injection
- T1112 Modify Registry
- T1555.003 Credentials from Web Browsers
- T1059.001 PowerShell
- T1027 Obfuscated Files or Information
- T1564.003 Hidden Window
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3105).
- 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 0.4698; 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
APT37	0.4698
Nomadic Octopus	0.4479
BRONZE BUTLER	0.4389
APT19	0.4267
Patchwork	0.4211

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: RustyStealer, Vidar.
- 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
Domain	rlim[.]com	
Domain	muckdeveloper[.]com	malware_download
Domain	muckcoding[.]com	
URL	hxxps://muckcoding[.]com/LG-LW/Api-Certificate	
URL	hxxps://rlim[.]com/MicrosoftCur/raw	
URL	hxxps://muckdeveloper[.]com/LGTV/MicrosoftCur	

Type	Indicator	Context
URL	hxxp://muckcoding[.]com/LG-LW/Api-Certificate	
Hash	b27f694c974b44fe2f4a8a25680997db574fa35686c30fa4c4dc9dd4ec40005e	
Hash	ec1cac2ada6726623b4bafb94c204c359ce7cdf5325909137fc0e6aef506783f	
Hash	2f416aac027f19f563cc45e3b4b72e992aaafb63da27f968b9a76a391134dc7d	Vidar
Hash	458e4c64738e8f46e997eea7cb32a296	Vidar
Hash	1a9bbae96ab7a852312b802fd3694211f3bbc43f	Vidar
Hash	9df11356c5ac61d2aa7b5425e6322fc016b0ed5790dacb201396500b3eee03f7	RustyStealer
Hash	129de16fe69763f767d8249279a2c4a1a6deafadd1a84563bd84b258ea010bff	
Hash	86819efe7319b664920ba2e1fd4b079a4e6b5eaaebeeb1adb2c1c8dc3c81ee0c	
Hash	57e0449fb13766b0b2f7c057b1f89911e9ed23cac7e71d5d69fde47571239629	
Hash	e576a61e1a2ba71e764647bb2f0883c2f8fa4d591799c60d21a84230ee7a5b63	
Hash	51cada347262d7b2bcde70552fcdae221625ad75435cee8a9c3e7b67cc47a807	
Hash	969b0bfd605aa2cddf353f3638b0dee26b1c2305600231e055fa6d7786a879fe	
Hash	73c807df26427d6631088a822fa54c30975afbe681a9d83eff5d19e5b075d6c2	
Hash	a628ad47fe93ee7413cca90aeca8f9540bfcd5ccdbeb4d9914670b3ef66247f4	
Hash	4ea1c577247b149489506b230e7aa203e1a2fa124109c6056d1986e944f520a4	
Hash	235a64e3520b1c2c27763122b303f78aee8d7c083dfd9f1eb936cd5174383609	
Hash	33497c69c21fa96bbc96f1d7f09608e462f8ab22555364977c0bd35fef27bc29	
Hash	45126b353f1636103da356121cd00b229b635b41b99d91166e6d7d9037482242	
Hash	810614290bdb14d2ddf10f65f8adc988a8272764f2a9e2c378e52fad162da344	
Hash	938054c6bb7dc737fce16513b2882808f199c2f892f808d439525a1650d49089	
Hash	a2e7989742c6b6436ebb47507881946e4f662080dff71d104eb9a9554f38af7a	
Hash	d7747e7a3c782009f4ceb6e9c10611587638685392956 3b509da5258e3968d15	
Hash	d95bba20f04687b0b821d4fc0a17137db8b9eda5fe3fb34da319abefc45fe0d1	
Hash	e73491065d86b1ad69229bb5d2019e08b947e11a2a57adf5c2d9a2b5d8f4acad	

Type	Indicator	Context
Hash	f245956c930f220f0bedf355a751a5cd738b4ec6bb6c5d584199ab3fa6c0a1c4	
Hash	0aaea95ad6ef4a9baf02ae05289af617	
Hash	64eb7ad3aaf9b6639ccc5c0b30b6e59f	RustyStealer
Hash	cba1927cf6959dc99ecbd0c553e4db6f	
Hash	ebf10abb661350779d24d849f828eb0b	
Hash	1eb377e01e1e649b3290efb0160f25cb5d13bd21	RustyStealer
Hash	25d585a291235936eca70402fbb567017aad860a	
Hash	2d1887930758b98b1a09f2f656079599f88a6bf6	
Hash	7f2d59cfdf2b0550d22ac54d0b1fa5ac8f8b5f57	

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:** 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).

The threat actor could pivot to utilizing Scheduled Task (T1053.005) to maintain persistence and execute malicious code at a later time, potentially bypassing initial defenses. This technique may allow the actor to blend in with legitimate system activity, making it more challenging to detect. To counter this potential move, the defensive control would be to 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