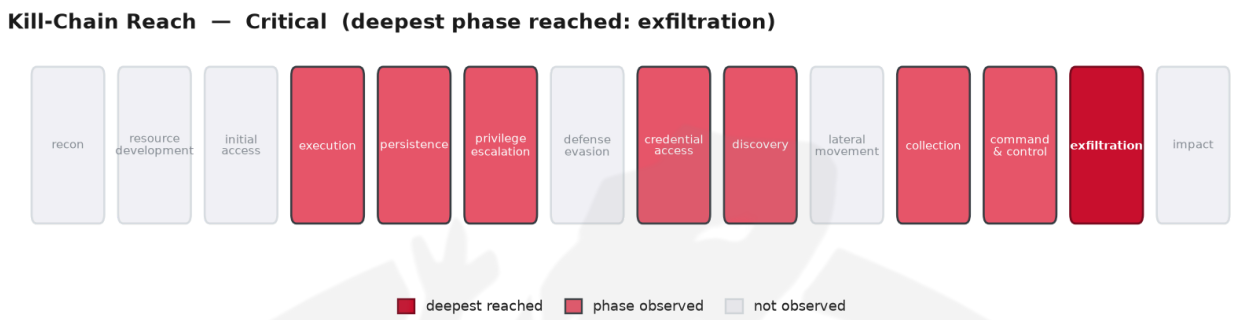
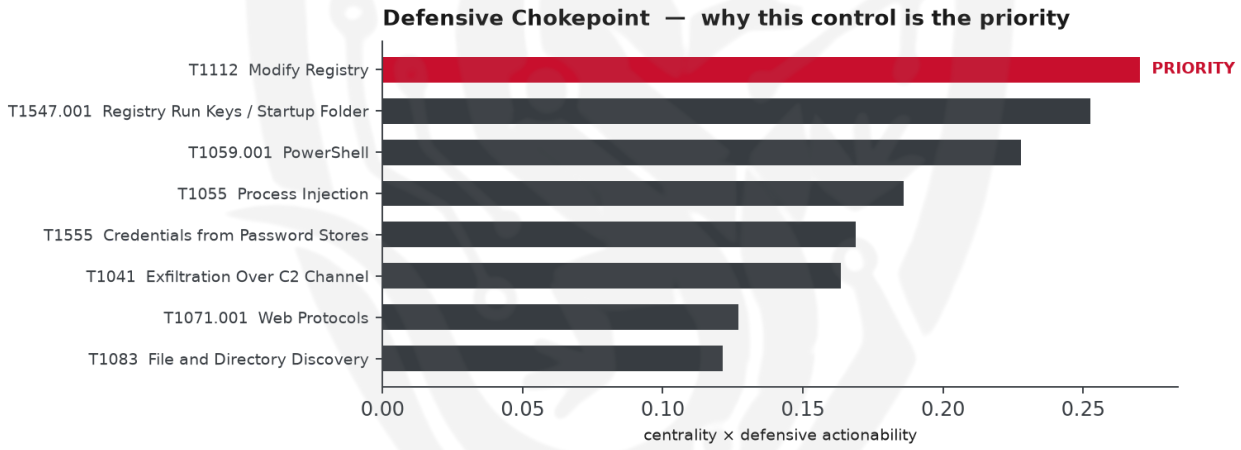
THREAT REPORT: WOODGNAT

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 Woodgnat, a threat actor that has been observed utilizing a range of malware families, including Backdoor.Mistic, ModeloRAT, and MintsLoader, to target organizations in the Insurance, Education, and Technology sectors. The actor's goals and motivations are not fully understood, but their use of techniques such as screen capture, system information discovery, and credentials theft suggests a high level of sophistication. Priority should be given to monitoring sensitive registry keys for modification and restricting registry-edit tools for unprivileged users. The threat actor's ability to exfiltrate data over command and control channels poses a significant risk to targeted organizations.

Threat Overview

The threat actor, attributed to Woodgnat by the source, has been observed using a variety of malware families to gain access to targeted systems. The malware families used include Backdoor.Mistic, ModeloRAT, GateKeeper, NexShield, MintsLoader, and D3F@ck Loader. The actor's targets include

organizations in the Insurance, Education, and Technology sectors, although the specific countries targeted are not known. The actor's use of techniques such as scheduled tasks, screen capture, and permission groups discovery suggests a high level of sophistication and a desire to maintain long-term access to compromised systems.

Attack Chain and Priority Control

The observed techniques used by the threat actor can be described as a chain of events, starting with initial access and ending with exfiltration of sensitive data. The techniques used include scheduled tasks, screen capture, system information discovery, and credentials theft, among others. The priority technique, as identified by the source, is T1112 Modify Registry, which is used to maintain persistence and evade detection. The priority control, as recommended by the source, is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The threat actor's infrastructure has been observed to be hosted on providers such as BL Networks and VPSPay Networks Ltd. Additionally, malware families such as Havoc, KongTuke, and MintsLoader have been corroborated by abuse.ch, suggesting a possible connection to other malicious activity. However, according to AbuseIPDB, the confidence level of the indicators is relatively low, with the highest confidence seen being 13%.

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
- T1069 Permission Groups Discovery
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1055 Process Injection
- T1112 Modify Registry
- T1087 Account Discovery
- T1083 File and Directory Discovery
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols

- T1018 Remote System Discovery
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer
- T1558.003 Kerberoasting

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2846).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4714; 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
APT18	0.4714
Stealth Falcon	0.4588
Molerats	0.44
BRONZE BUTLER	0.4202
Confucius	0.4158

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 13%.
- Malware families corroborated by abuse.ch: Havoc, KongTuke, MintsLoader.
- 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	144[.]31[.]53[.]78	AbuseIPDB 13% (FI) · AS201988 VPSPay Networks Ltd

Type	Indicator	Context
IP	198[.]13[.]159[.]44	AbuseIPDB 0% (NL) · KongTuke · AS399629 BL Networks
IP	199[.]91[.]221[.]42	AbuseIPDB 0% (NL) · AS399629 BL Networks
Domain	mail[.]authorized-logins[.]net	KongTuke
Domain	mueleer[.]com	KongTuke
Domain	grande-luna[.]top	KongTuke
Domain	oeannon[.]com	KongTuke
Domain	thomphon[.]com	KongTuke · malware_download
Domain	human-check[.]top	
Domain	update[.]update-fall[.]com	
Domain	cwrtwright[.]com	KongTuke
Domain	carrolc[.]com	Havoc
Domain	w3xasv14culvnqj[.]top	MintsLoader
Domain	authorized-logins[.]net	KongTuke
Domain	b6w9m2z5x8q1v3k[.]top	
Domain	rotoa-upda-lo[.]com	
Domain	sql-updater-service[.]com	

Type	Indicator	Context
Domain	upd-domain-goloro[.]com	
Domain	updater-worelos[.]com	
Domain	upscale-kolo[.]com	
Domain	defs[.]updater-worelos[.]com	
Domain	ftps[.]upd-domain-goloro[.]com	
Domain	mailes[.]upd-domain-goloro[.]com	
Domain	mails[.]updater-worelos[.]com	
Domain	nano[.]upscale-kolo[.]com	
Domain	php[.]authorized-logins[.]net	
Domain	sss[.]authorized-logins[.]net	
URL	hxxp://thomphon[.]com/update[.]msi	
Hash	3f797a639bc855bc6d5471f327924b62d10900ddec49b970eca6604142bbb4be	KongTuke
Hash	fb3630822b70bacb56aa4cec29b5a0e3e9acb3920809e70310a4003385a6d34a	Havoc
Hash	59e3c4cb06331b4f2d78a9a0592f3747e573bd01c5a7650c26361d1e25520712	Havoc
Hash	afd5f1ed45a9867daf3bc64152cef460a06b164c8183e490db39146d4749a82c	
Hash	347a3f5f2ed2f503a22f68c4951c78c7	
Hash	6b8ec32dc76fa3138f00616156962f4f	
Hash	deb10789274bf903060d700b3472fdf094a14763	

Type	Indicator	Context
Hash	fd8e880cc32377af08327c9d187f6220c6ac449f	
Hash	b148626849c11dd5b3230632a38a6302	
Hash	e5c4e634b2f443f783cae1b5e8247a1069df0c9f	
Hash	1e41c7bfaa6aa3b93b6cc024274a10e33f3e12fe7c98c1db387ef8927f9d1984	
Hash	dc96668d007df0a545bf1334e10e80fa	KongTuke

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.