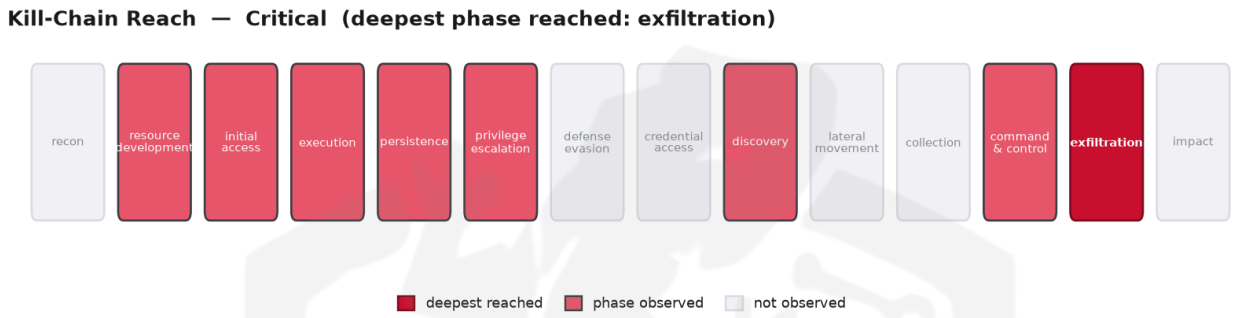
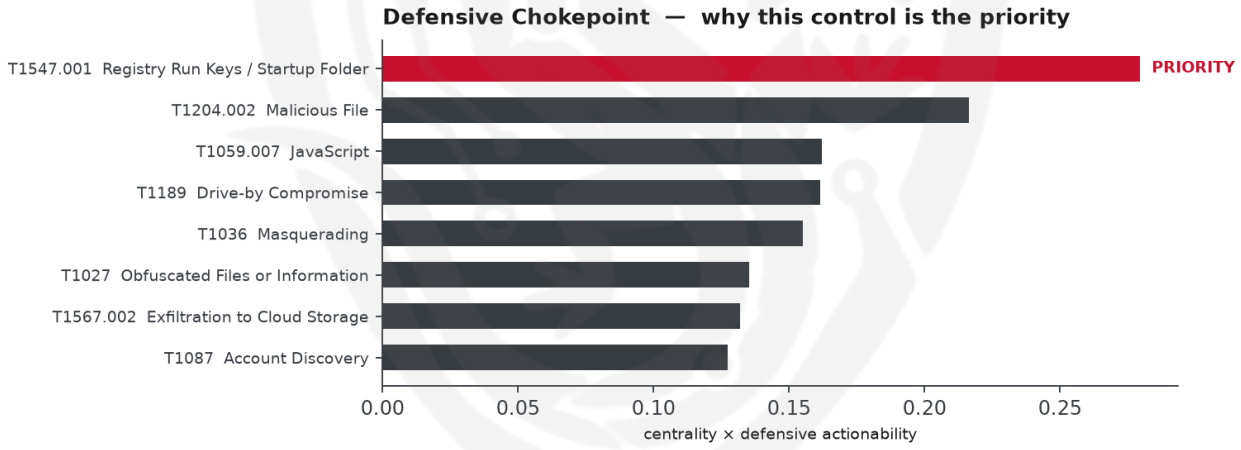
THREAT REPORT: GOLD PRELUDE OPERATION ENDGAME

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 GOLD PRELUDE, a threat actor utilizing various malware families, including SocGholish and IcedID, to target multiple sectors such as Government, Education, and Finance. The actor's campaign involves exploiting vulnerabilities to gain unauthorized access, with a priority defensive action being to audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. Priority should be given to monitoring for suspicious activity, particularly the creation of .lnk or script files in Startup by browser or email temporary paths.

Threat Overview

GOLD PRELUDE, the attributed threat actor, is associated with a range of malware families including SocGholish, IcedID, Smokeloader, and others, targeting various sectors. The central vulnerability

exploited is not specified, but the actor's techniques include system discovery, encoding, and masquerading, indicating a sophisticated approach to gaining and maintaining access to victim systems.

Attack Chain and Priority Control

The observed techniques form a complex chain, starting with initial access and proceeding through system and account discovery, encoding, and finally, exfiltration. The priority technique identified is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. To mitigate this, the priority 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."

Infrastructure and Corroboration

Although specific hosting providers or ASNs are not identified, abuse.ch corroborates the presence of the FAKEUPDATES malware family, which is associated with the campaign. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, suggesting that while there is some external validation of the threat, the primary intelligence remains the initial source report.

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
- T1033 System Owner/User Discovery
- T1132.001 Standard Encoding
- T1059.007 JavaScript
- T1069 Permission Groups Discovery
- T1204.002 Malicious File
- T1082 System Information Discovery
- T1036 Masquerading
- T1087 Account Discovery
- T1583.003 Virtual Private Server
- T1083 File and Directory Discovery
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1567.002 Exfiltration to Cloud Storage
- T1518.001 Security Software Discovery
- T1189 Drive-by Compromise
- T1071.001 Web Protocols
- T1584.001 Domains

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2943).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5401; 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
Windshift	0.5401
Winter Vivern	0.4725
Confucius	0.4643
MuddyWater	0.4483
Sidewinder	0.4374

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: FAKEUPDATES.
- 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	trademark[.]iglesiaelarca[.]com	malware_download
Domain	content[.]garretttrails[.]org	malware_download
Domain	promo[.]summat10n[.]org	
Domain	billing[.]roofnrack[.]us	
Domain	devel[.]asurans[.]com	

Type	Indicator	Context
Domain	storehouse[.]beautysupplysalonllc[.]com	FAKEUPDATES
Domain	samples[.]addisgraphix[.]com	
Domain	api-app[.]uppercrafteroom[.]com	FAKEUPDATES
Domain	pa-portal[.]benningtonspringsmhp[.]com	
Domain	shop[.]steadycompanion[.]com	
Domain	platform[.]exathomeswebuyarizona[.]com	
Domain	app-front[.]anmaradigital[.]com	FAKEUPDATES

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