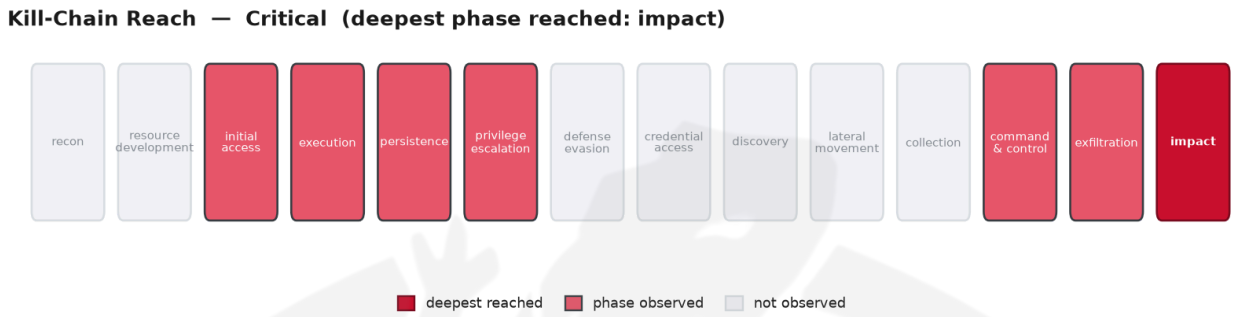
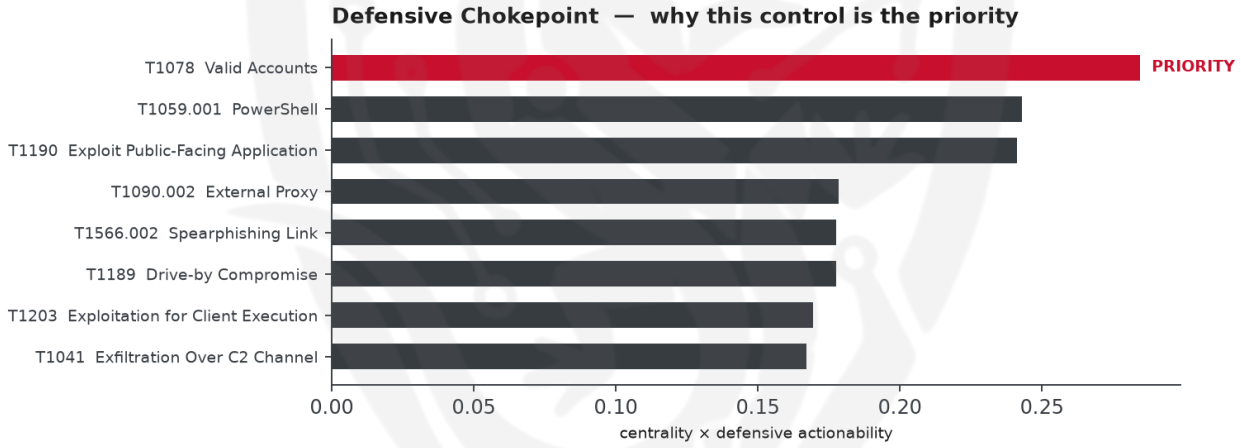
THREAT REPORT: GOLD PRELUDE

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 that has been observed utilizing various malware families, including SocGholish, GhoLoader, and LockBit, to target organizations in several countries, including the United States, Australia, and the United Kingdom. The targeted sectors include Media, Retail, Healthcare, Education, and Government. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The threat actor's activities have been deemed critical, reaching the impact stage.

Threat Overview

GOLD PRELUDE, the observed threat actor, has been associated with multiple malware families, including SocGholish, GhoLoader, FrigidStealer, WastedLocker, LockBit, and RansomHub. The victimology indicates that the threat actor has targeted organizations in the Media, Retail, Healthcare,

Education, and Government sectors across several countries. The central vulnerability exploited by the threat actor is currently unknown.

Attack Chain and Priority Control

The threat actor's attack chain involves a range of techniques, including JavaScript execution, boot or logon autostart execution, and spearphishing link attacks. The priority technique, which serves as a chokepoint in the attack chain, is T1078 Valid Accounts. To mitigate this threat, the priority control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs observed, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with a confidence level of 80% or higher by AbuseIPDB, 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)

- T1059.007 JavaScript
- T1547 Boot or Logon Autostart Execution
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1219 Remote Access Tools
- T1036 Masquerading
- T1090.002 External Proxy
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1203 Exploitation for Client Execution
- T1189 Drive-by Compromise
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1564.001 Hidden Files and Directories

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2846).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4899; 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	0.4899
Nomadic Octopus	0.4824
Higaisa	0.4685
Elderwood	0.4619
Transparent Tribe	0.4587

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	platform[.]exathomeswebuyarizona[.]com
Domain	js-new[.]newtoyourgame[.]com

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.k@3sdragon.eu

- **Control applied:** T1078 Valid Accounts (initial-access)
- **Observed here:** GOLD PRELUDE used T1189 Drive-by Compromise here as an alternative initial-access technique.
- **Projected pivot:** T1189 Drive-by Compromise (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

GOLD PRELUDE could pivot to T1189 Drive-by Compromise to maintain access and achieve their objectives by exploiting vulnerabilities in software or browsers, potentially using compromised websites to infect victim machines. This technique may allow them to bypass the blocked valid account control and establish a new foothold. To counter this, the defensive control would likely involve Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.

- **Defensive countermeasure:** Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.