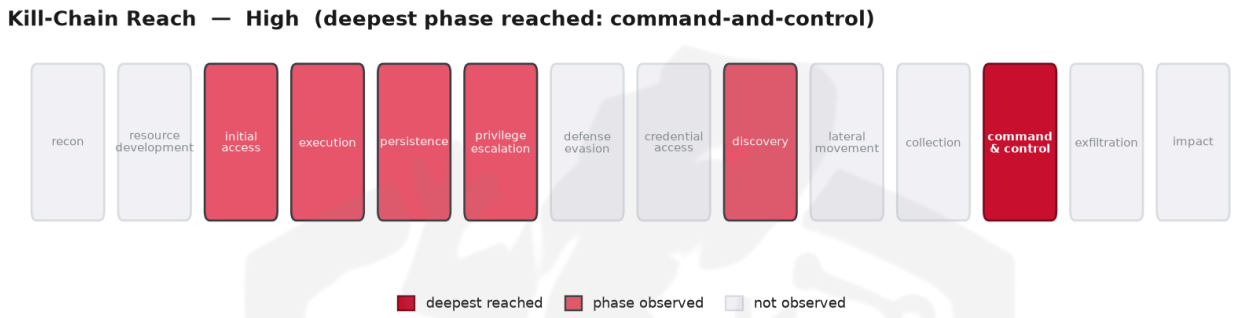
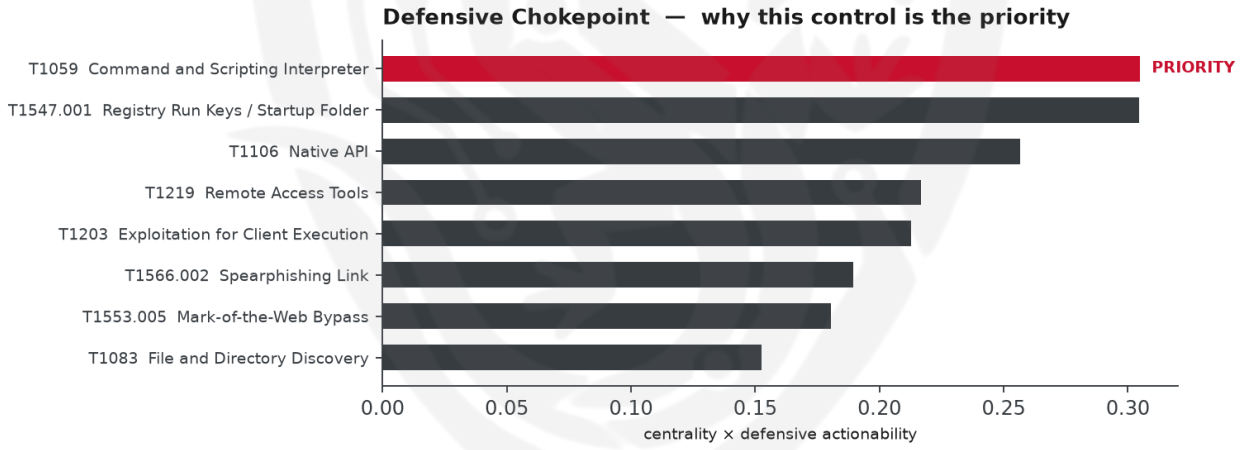
THREAT REPORT: VERCEL-HOSTED REMOTE ACCESS MALWARE CAMPAIGN

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 involves the delivery of LogMeIn malware, targeting unspecified countries and sectors. The threat actor's identity remains insufficiently determined. Priority should be given to constraining PowerShell for unprivileged users to mitigate the threat. The campaign's operational risk band is considered high due to its command-and-control capabilities.

Threat Overview

The threat actor, whose identity is not sufficiently determined, is utilizing LogMeIn malware to gain remote access. The central vulnerability exploited is not specified, but various techniques are employed, including malicious file delivery, spearphishing, and system information discovery. The victimology of this campaign is not well-defined due to insufficient data.

Attack Chain and Priority Control

The attack chain involves multiple techniques, including malicious file delivery, spearphishing, system information discovery, and the use of native APIs. The priority technique is T1059 Command and Scripting Interpreter, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to Constrain PowerShell for unprivileged users (Constrained Language Mode + AppLocker); enable script-block logging; block wscript/cscript where unneeded.

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed in this campaign, as indicated by the lack of data in the infrastructure and corroboration section. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1082 System Information Discovery
- T1106 Native API
- T1219 Remote Access Tools
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1553.005 Mark-of-the-Web Bypass
- T1547.001 Registry Run Keys / Startup Folder
- T1203 Exploitation for Client Execution
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1059 Command and Scripting Interpreter (centrality 0.3812).
- 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 0.55; 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
Confucius	0.55
Windshift	0.5446
Dark Caracal	0.5008
Sidewinder	0.4865
APT37	0.4602

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
Hash	322a92b443faefe48fce629e8947e4e2
Hash	e230bf859e582fe95df0b203892048df
Hash	f3f8379ce6e0b8f80faf259db2443f13
Hash	f782c936249b9786cc7fac580da3ae0f
Hash	5fd4bcca28553ebe759ec97fcbc3a2a732268f85
Hash	0a1a85a026b6d477f59bc3d965b07d0d06e6ff2d34381aff79ea71c38fed802b

---

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:** T1059 Command and Scripting Interpreter (execution)

- **Observed here:** T1059 Command and Scripting Interpreter was the only execution technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (execution)
- **Basis:** of the 54+ groups that use Command and Scripting Interpreter, this pairing runs 1.3x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1053 Scheduled Task/Job to maintain persistence and execute malicious commands at a later time, potentially leveraging the Windows Task Scheduler to blend in with legitimate system activity, which may allow them to bypass initial detection. This technique in particular could be appealing as it enables the actor to execute tasks at specific intervals or times, which would likely facilitate their objective of maintaining access to the compromised system. To counter this, the defensive control would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1047 Windows Management Instrumentation (n=40, lift 1.3), T1574 Hijack Execution Flow (n=32, lift 1.2)

Detection and hardening for the pivot (T1053 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