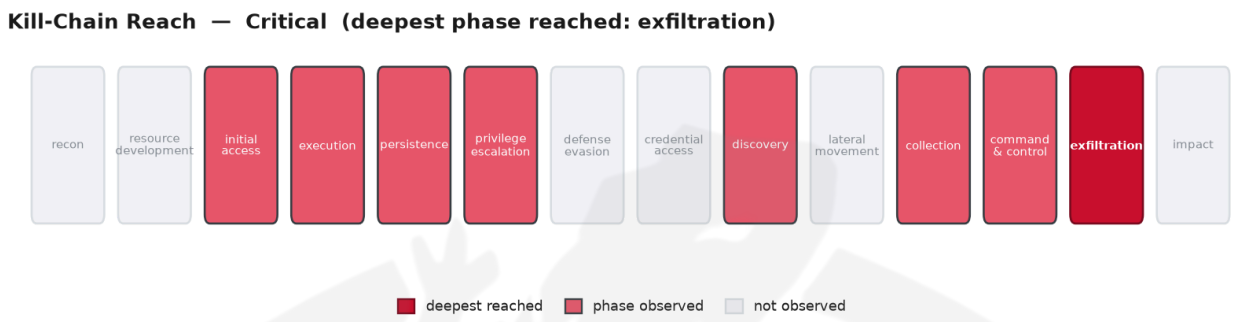
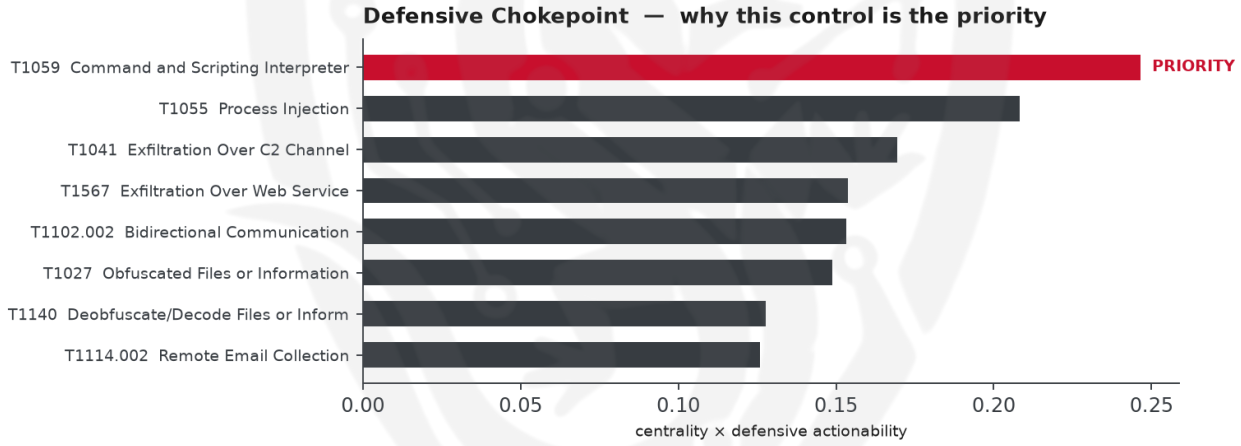
THREAT REPORT: LYCEUM

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 LYCEUM, a threat actor that has been observed exploiting Microsoft 365 calendars as covert command-and-control channels. The targeted country is Israel, and the priority defensive action should be to constrain PowerShell for unprivileged users to prevent further exploitation. The threat actor's use of various techniques, including encoding, DNS, and symmetric cryptography, highlights the need for a comprehensive defense strategy. Priority should be given to defending against the threat actor's ability to exfiltrate data over web services and cloud storage.

Threat Overview

LYCEUM, the observed threat actor, has been associated with the HOLLOWGRAPH and Cavern malware families. Although the central CVE is insufficient, the threat actor's techniques include standard encoding, DNS, local data staging, and symmetric cryptography, among others. The victimology indicates that the threat actor is targeting Israel, but the specific sectors are unknown.

Attack Chain and Priority Control

The threat actor's attack chain involves a series of techniques, including encoding, DNS, and data staging, ultimately leading to exfiltration over web services and cloud storage. The priority technique is T1059 Command and Scripting Interpreter, which is the graph chokepoint. 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 observed hosting provider or ASN associated with this threat actor, and no malware families have been corroborated by abuse.ch. Additionally, there are no indicators with an AbuseIPDB confidence 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)

- T1132.001 Standard Encoding
- T1071.004 DNS
- T1074.001 Local Data Staging
- T1573.001 Symmetric Cryptography
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1567 Exfiltration Over Web Service
- T1055 Process Injection
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1041 Exfiltration Over C2 Channel
- T1027 Obfuscated Files or Information
- T1114.002 Remote Email Collection
- T1102.002 Bidirectional Communication
- T1567.002 Exfiltration to Cloud Storage
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1078.004 Cloud Accounts
- T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1059 Command and Scripting Interpreter (centrality 0.3082).

- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3649; 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
APT33	0.3649
APT18	0.3629
MuddyWater	0.3573
Lazarus Group	0.3572
APT39	0.3402

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	cloudlanecdn[.]com
Domain	p[.]cloudlanecdn[.]com
Domain	q[.]cloudlanecdn[.]com
Hash	315bdba98c6fe863d39f6afccc727e17d5aea63bf21259444fa988cae56d61c1
Hash	1573e125197ec77d8e9930c611ba2802ee59e19629396b5e99b426b46c53bd25
Hash	75e51774b8f79e5f256eaae639635f911b3e744d4774fd6068dd980255621509
Hash	b3d0f6e4e3be395fd7cf9e8101c89963d77216578cbb117a6ac9bc3564485eff
Hash	f3f3006f8304788251b153d53b305322b8acab0c66ec816b8d9f101bcc851da3

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:** 54 of 170 documented groups that use Command and Scripting Interpreter also use Scheduled Task/Job (conditional 0.44, lift 1.3, i.e. ~1.3x base rate). Strongest same-tactic neighbour.

The LYCEUM actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious commands, potentially scheduling tasks to run at specific intervals to evade detection. This technique may allow them to continue their objective, as scheduled tasks can blend in with legitimate system activity. 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