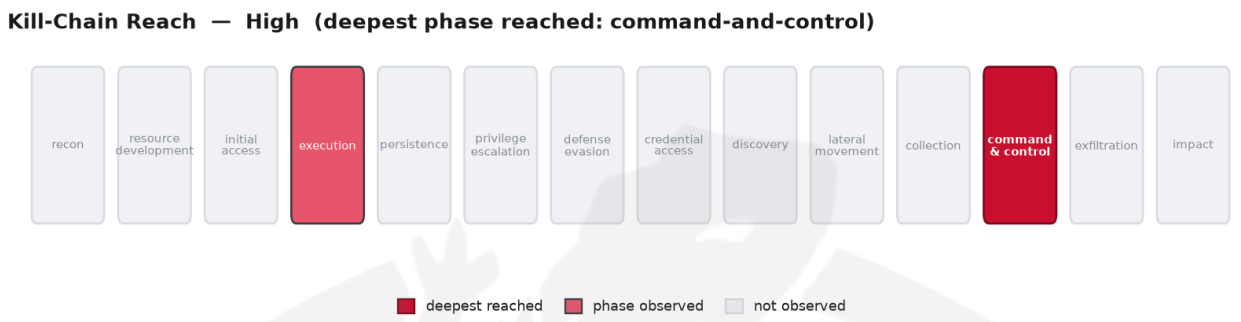
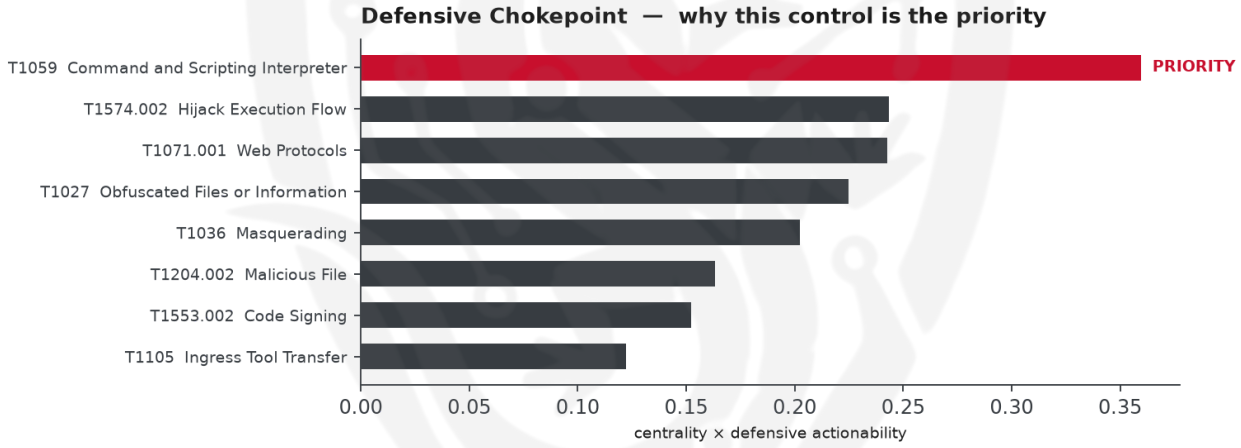
THREAT REPORT: APT-Q-27

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 APT-Q-27. The threat actor has been observed utilizing various techniques to gain control over targeted systems. Priority should be given to constraining PowerShell for unprivileged users to mitigate the threat. The operational risk band is considered High, indicating a significant potential impact.

Threat Overview

The threat actor, APT-Q-27, has been observed using multiple techniques, including malicious files, code signing, and masquerading. The victimology and targeted sectors are not well understood due to insufficient data. The threat actor's tactics, techniques, and procedures (TTPs) involve a range of activities, from obfuscated files to web protocols and hijacking execution flow.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with malicious files and code signing, followed by masquerading, obfuscated files, and command and scripting interpreter. The priority technique is T1059 Command and Scripting Interpreter, which serves as a chokepoint in the attack chain. To mitigate this threat, the recommended control is: 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 activity. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence 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)

- T1204.002 Malicious File
- T1553.002 Code Signing
- T1036 Masquerading
- T1059 Command and Scripting Interpreter
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1059 Command and Scripting Interpreter (centrality 0.4495).
- Operational risk: High (score 0.552, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5449; 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
Whitefly	0.5449
TA551	0.503
Daggerfly	0.4954
Windshift	0.4924
Nomadic Octopus	0.4545

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	api[.]keensie[.]com
URL	hxxp://api[.]keensie[.]com:5198/
Hash	8838df7298abf4d4312648e2ee80bdee
Hash	c0aca5dfbbfcb1c9796b3d974b1ee78b
Hash	1d1808686dbf36138f3067c34566d627
Hash	130fbe74fea31b30b59b071ccf22bf68

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:** APT-Q-27 used T1204.002 Malicious File here as an alternative execution technique.
- **Projected pivot:** T1204.002 Malicious File (execution)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The adversary, APT-Q-27, could pivot to using T1204.002 Malicious File to maintain their campaign momentum, potentially embedding malicious code within seemingly innocuous files to evade detection. This technique may allow them to bypass the blocked command and scripting interpreter control, as malicious files could be designed to execute without relying on command-line interfaces. To counter this, the mandated defensive control of blocking execution of downloaded HTA/JS/LNK/archive payloads, enforcing mark-of-the-web, and disabling Office macros from the internet should be implemented.

Detection and hardening for the pivot (T1204.002 User Execution)

- **Telemetry:** Endpoint process telemetry; Email/proxy logs
- **Detect:**
  - User double-clicking archive/ISO/LNK contents that spawn interpreters
  - Mark-of-the-Web on delivered files; LOLBIN execution from user temp paths
- **Harden:**
  - Block risky file types; ASR rules; user awareness training
  - Application control to stop execution from user-writable directories
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1017 User Training · DS0009 Process, DS0022 File