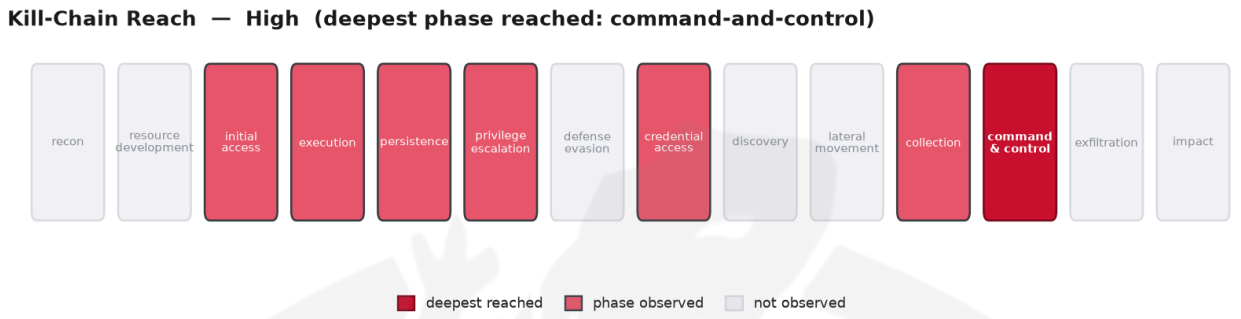
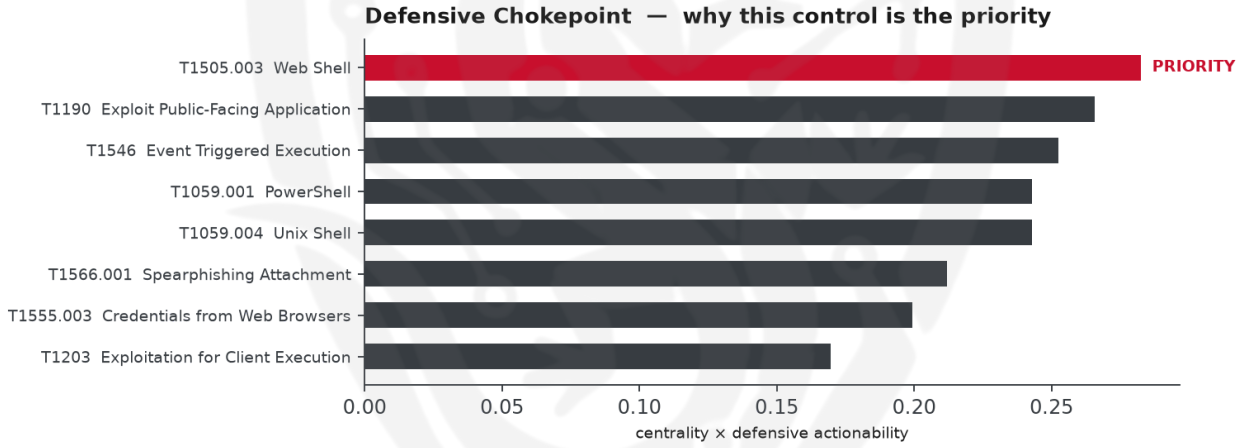
THREAT REPORT: TA458 OPERATION ROUNDPRESS

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 TA458, a threat actor exploiting the CVE-2026-8496 vulnerability to target government, defense, chemical, telecommunications, and technology sectors in Albania, Greece, Moldova, Ukraine. The malware family used is SpyPress. Priority should be given to patching the CVE-2026-8496 vulnerability on all affected systems to prevent further exploitation. The threat actor's activities have been observed to reach a high operational risk band, indicating a significant level of command-and-control capability.

Threat Overview

TA458, the observed threat actor, is utilizing the SpyPress malware family to exploit the CVE-2026-8496 vulnerability, primarily targeting government, defense, chemical, telecommunications, and technology sectors in several countries. The actor's techniques include exploiting public-facing applications, using web shells, and collecting email data, among others.

Attack Chain and Priority Control

The attack chain involves various techniques, including exploiting public-facing applications, creating or modifying system processes, and using web shells. The priority technique is T1505.003 Web Shell, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to: Patch CVE-2026-8496 on all affected systems as the top priority, then: Integrity-monitor web-server directories for web shells; restrict server module/plugin installation.

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 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
- T1543 Create or Modify System Process
- T1074.001 Local Data Staging
- T1114.001 Local Email Collection
- T1566.001 Spearphishing Attachment
- T1005 Data from Local System
- T1190 Exploit Public-Facing Application
- T1555.003 Credentials from Web Browsers
- T1505.003 Web Shell
- T1059.001 PowerShell
- T1059.004 Unix Shell
- T1027 Obfuscated Files or Information
- T1114.002 Remote Email Collection
- T1546 Event Triggered Execution
- T1573 Encrypted Channel
- T1203 Exploitation for Client Execution
- T1059.006 Python
- T1189 Drive-by Compromise
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1505.003 Web Shell (centrality 0.2973).

- 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 0.3961; 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
Inception	0.3961
APT37	0.3956
Sea Turtle	0.3956
APT39	0.3856
Winter Vivern	0.3849

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	upgybj[.]store
Domain	xsza[.]net
Domain	hgmydr[.]wiki
Domain	share-ya[.]space
Domain	zxzaq[.]com
Hash	625e4c166c7a1d5a1becf56b27d4f76a2f95935cbd8d556c30a493263d10dbf8
Hash	3a449148a0e3cac604fb93210dd7d91ccf48e06ed9aae064bc53a419a84ce9ba
Hash	6b2c02bf82087a3ca5fb7ef8046554ff29ce85d52202bdcfae2b2653aede139a

Type	Indicator
Hash	8b5a4dc237a4c89042176bc89864a4c357dcdd14fa544fe6496ccb6c31cd5b7f
Hash	a0c80cab70d6672b01710a70f93311fc1c1db2fbbf9cd6daa543c34b87e3444a
Hash	e27d1bf82249002a66395c89dbda6ec5d8df012a84b79d36fffbbf7808d28878
Hash	fb8ec4dbed14c0a91361abd82ebe9fb083615c3dbb15348f57317af7cc41dd34

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:** T1505.003 Web Shell (persistence)
- **Observed here:** TA458 used T1543 Create or Modify System Process here as an alternative persistence technique.
- **Projected pivot:** T1543 Create or Modify System Process (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The adversary could pivot to T1543 Create or Modify System Process to maintain persistence and evade detection, potentially creating a new system process that blends in with legitimate system activity to achieve their objectives. This technique may be used to create a backdoor or establish a covert channel, which would likely involve modifying existing system processes or creating new ones. The defensive control to counter this potential move would be to implement the mandated control: Restrict service/daemon creation to admins; monitor service and driver installs.

Detection and hardening for the pivot (T1543 Create or Modify System Process)

- **Telemetry:** Windows Security / System log; Sysmon
- **Detect:**
  - System 7045 (new service installed); Security 4697 (service installed)
  - Sysmon 1 for sc.exe / services created; unusual ImagePath or user-context services
  - Registry writes under HKLM\SYSTEM\CurrentControlSet\Services
- **Harden:**
  - Restrict service creation to admins; application control on service binaries
  - Baseline installed services and alert on new/anomalous ones
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0019 Service, DS0024 Windows Registry, DS0009 Process