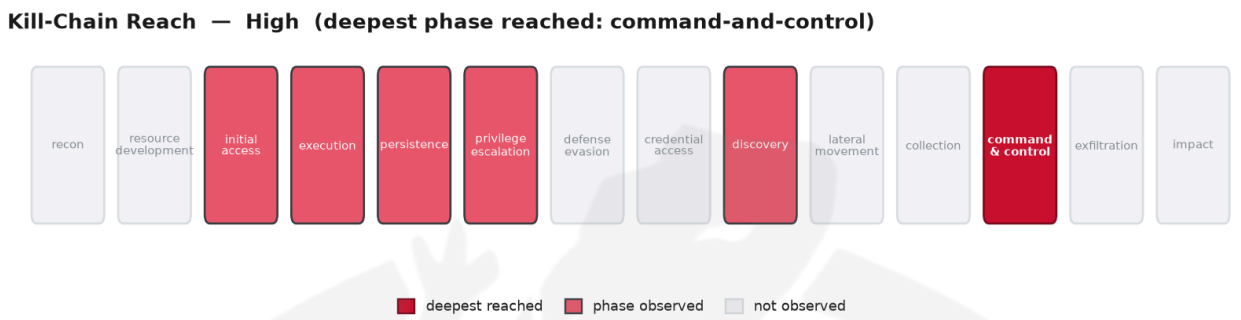
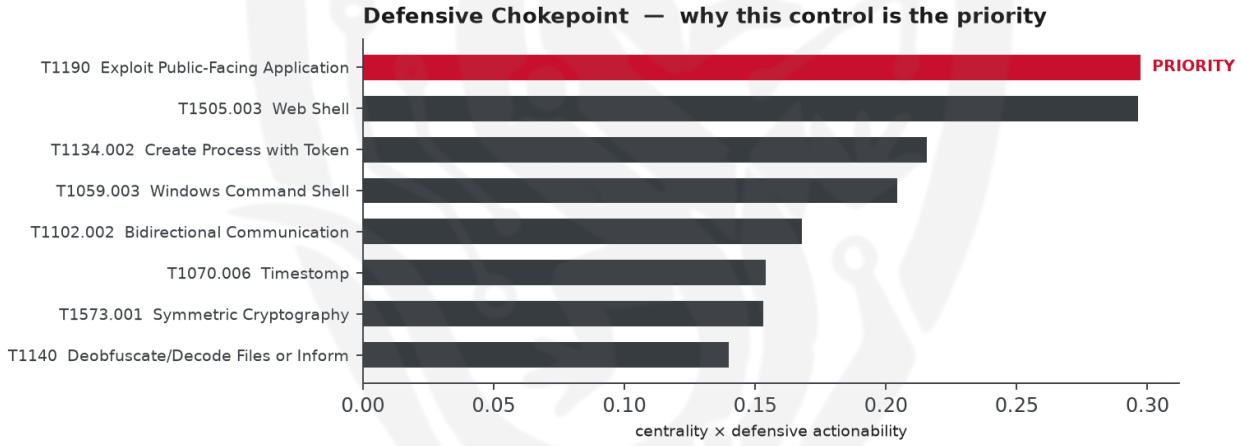
# THREAT REPORT: OP-512

## 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 OP-512, a threat actor utilizing various malware families, including GhostKit, BadPotato, and PlugX, to target unknown sectors and countries. The priority defensive action is to patch the affected public-facing vulnerability immediately. Given the operational risk band is High, reaching 'command-and-control', it is crucial to apply a Web Application Firewall (WAF) virtual patch and restrict management interfaces to VPN-only. Priority should be given to defending against the exploitation of public-facing applications.

## Threat Overview

OP-512, the observed threat actor, employs a range of malware families such as GhostKit, BadPotato, SweetPotato, and PlugX, among others, to conduct their operations. The central vulnerability exploited is currently insufficient to determine. The victimology and targeted sectors are also not specified due to insufficient data.

## Attack Chain and Priority Control

The attack chain involves various techniques, including system owner/user discovery, standard encoding, domain generation algorithms, and bypassing user account control, among others. The priority technique identified is T1190 Exploit Public-Facing Application, which serves as a critical chokepoint in the attack chain. To mitigate this, the priority control is to: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

## Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed in relation to OP-512's activities. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators at or above 80% confidence according to 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)

- T1033 System Owner/User Discovery
- T1132.001 Standard Encoding
- T1568.002 Domain Generation Algorithms
- T1548.002 Bypass User Account Control
- T1071.004 DNS
- T1573.001 Symmetric Cryptography
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1070.006 Timestomp
- T1505.003 Web Shell
- T1134.002 Create Process with Token
- T1057 Process Discovery
- T1102.002 Bidirectional Communication
- T1059.003 Windows Command Shell
- T1132.002 Non-Standard Encoding
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1055.001 Dynamic-link Library Injection
- T1090.001 Internal Proxy

### Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.2974).

- 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 0.408; 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 |
|---|---|
| Tropic Trooper | 0.408 |
| Lazarus Group | 0.3493 |
| APT37 | 0.3408 |
| TA551 | 0.3371 |
| MuddyWater | 0.3334 |

### 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 | hcgos[.]com |
| Domain | ashx[.]lhlsjcb[.]com |
| URL | hxxp://140[.]206[.]161[.]227:443 |
| URL | hxxp://43[.]160[.]202[.]246:8053 |

---

## 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:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** T1190 Exploit Public-Facing Application was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1078 Valid Accounts (initial-access)
- **Basis:** 32 of 170 documented groups that use Exploit Public-Facing Application also use Valid Accounts (conditional 0.73, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

OP-512 could pivot to using T1078 Valid Accounts if they have previously compromised or have access to valid credentials, which would likely allow them to maintain access to the target system despite the block on exploiting public-facing applications. This technique may be used to blend in with normal user activity, potentially evading detection. The defensive countermeasure to mitigate this would be to enforce the mandated control: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

**Also plausible (same tactic):** T1133 External Remote Services (n=17, lift 2.3), T1199 Trusted Relationship (n=9, lift 2.9)

**Detection and hardening for the pivot (T1078 Valid Accounts)**

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs; Proxy / DLP / data-egress volume telemetry
- **Detect:**
  - Security 4624/4625 (logon success/fail), 4768/4769 (Kerberos TGT/TGS), 4776 (NTLM)
  - Impossible-travel, new-geo, and off-hours sign-ins from the IdP
  - Service or dormant accounts logging on interactively
  - Under valid credentials the identity signal goes quiet: baseline per-account data-egress volume and alert on peer-group and historical deviation (the real exfiltration tell)
- **Harden:**
  - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
  - Least-privilege review; separate admin from daily-driver accounts
  - Set per-account and per-partner egress baselines with DLP thresholds on sensitive stores
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account