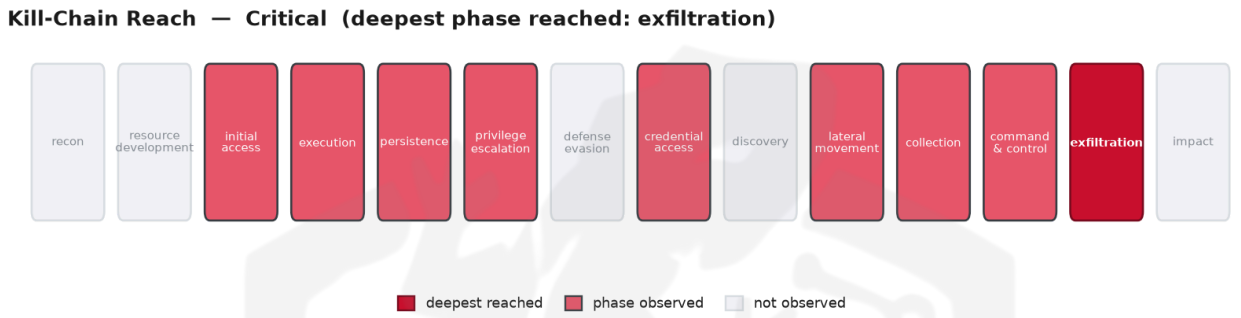
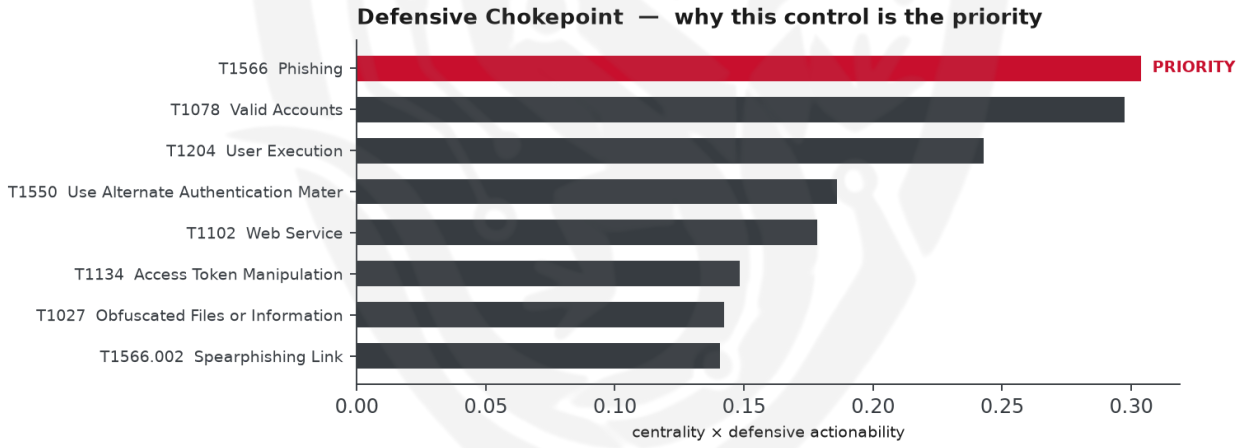
THREAT REPORT: UNKNOWN_ADVERSARY "GHOST" CODE PHISHING

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 has been targeting various sectors in the United States of America, including Technology, Manufacturing, Education, Finance, and Government, with a focus on phishing attacks. The malware family involved is EvilTokens. Priority should be given to defensive actions that mitigate phishing attacks, as the threat actor's techniques have reached the exfiltration stage. The lack of specific information on the threat actor and central CVE highlights the need for a proactive approach to security.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, is utilizing the EvilTokens malware family to conduct phishing attacks. The targeted sectors are diverse, indicating a broad range of potential

victims. The absence of specific information on the central CVE exploited by the threat actor means that defenders must focus on the techniques, tactics, and procedures (TTPs) observed.

Attack Chain and Priority Control

The attack chain involves several techniques, including phishing, stealing web session cookies, and exfiltration over web services. The priority technique identified is T1566 Phishing, which serves as a critical chokepoint in the attack chain. To counter this, the priority control is to "Enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button."

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed in relation to this activity. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence level of 80% or higher. This lack of corroboration highlights the need to rely on the primary techniques and controls identified to mitigate the threat.

Technical Appendix

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

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

- T1539 Steal Web Session Cookie
- T1114 Email Collection
- T1566.002 Spearphishing Link
- T1071 Application Layer Protocol
- T1140 Deobfuscate/Decode Files or Information
- T1567 Exfiltration Over Web Service
- T1550 Use Alternate Authentication Material
- T1185 Browser Session Hijacking
- T1102 Web Service
- T1204 User Execution
- T1566 Phishing
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1114.002 Remote Email Collection
- T1567.002 Exfiltration to Cloud Storage
- T1134 Access Token Manipulation
- T1071.001 Web Protocols
- T1204.001 Malicious Link
- T1550.001 Application Access Token
- T1078.004 Cloud Accounts

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.3037).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.45; 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
FIN4	0.45
Mofang	0.3727
Confucius	0.3381
TA577	0.3371
Elderwood	0.3227

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	fcd1b654a0b3e8f85ca7cfdafe494d4b

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:** T1566 Phishing (initial-access)

- **Observed here:** the threat actor used T1078 Valid Accounts here as an alternative initial-access technique.
- **Projected pivot:** T1078 Valid Accounts (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The threat actor could pivot to using T1078 Valid Accounts by attempting to leverage compromised or stolen credentials to maintain access to the target network, potentially exploiting weak password policies or unsecured account management practices. This approach may allow the actor to bypass the blocked phishing control and continue pursuing their objectives. To counter this potential move, the mandated defensive control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

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