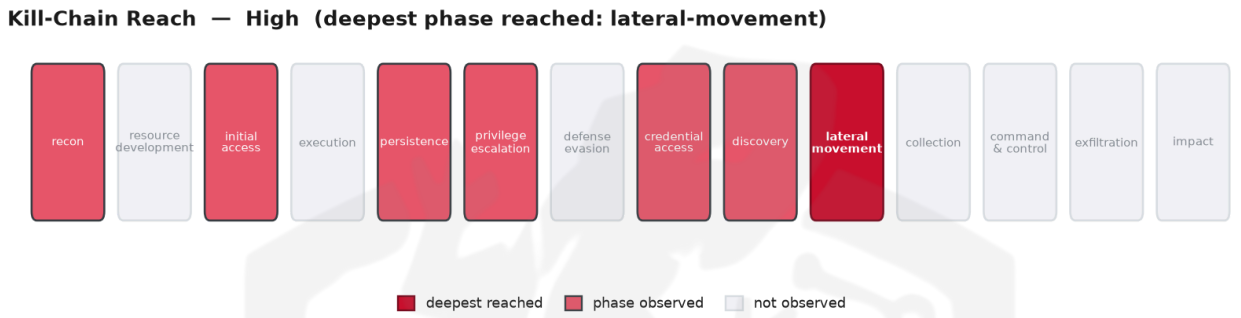
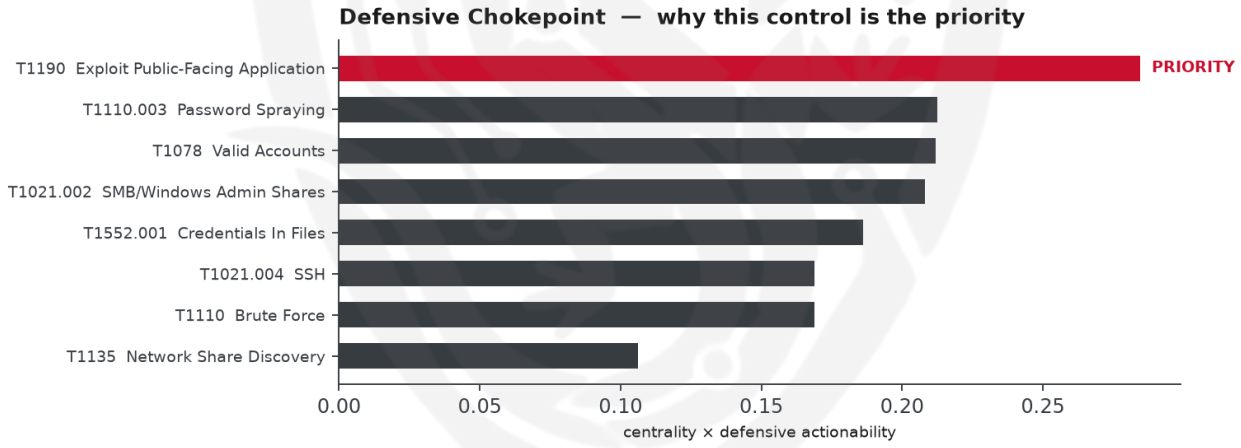
THREAT REPORT: UNATTRIBUTED CAMPAIGN TARGETS UNITED STATES AND GLOBAL ENTITIES

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 targeted entities in the United States, British Indian Ocean Territory, Colombia, India, Mexico, and Taiwan. While the specific malware families and central CVE exploited are unknown, the threat actor has utilized various techniques to gain access to and move laterally within targeted networks. Priority should be given to patching public-facing applications and restricting management interfaces to mitigate the risk. The operational risk band for this campaign is considered high due to the potential for lateral movement.

Threat Overview

The threat actor, whose identity is currently unknown, has employed a range of techniques including password guessing, external remote services, and security account manager manipulation. The

victimology indicates a broad targeting scope, affecting multiple countries and potentially various sectors, although specific sector information is insufficient. The techniques used suggest a focus on exploiting public-facing applications and leveraging valid accounts for network access.

Attack Chain and Priority Control

The observed techniques form a complex attack chain, with the threat actor leveraging techniques such as password guessing, external remote services, and network share discovery to gain access and move laterally within the network. The priority technique identified is T1190 Exploit Public-Facing Application, which serves as a critical chokepoint in the attack chain. To mitigate this risk, 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 used by the threat actor, as indicated by the lack of data in the infrastructure and corroboration section. Similarly, no malware families have been corroborated by abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level 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)

- T1110.001 Password Guessing
- T1133 External Remote Services
- T1003.002 Security Account Manager
- T1087.002 Domain Account
- T1069.002 Domain Groups
- T1021.004 SSH
- T1135 Network Share Discovery
- T1190 Exploit Public-Facing Application
- T1021.002 SMB/Windows Admin Shares
- T1595.002 Vulnerability Scanning
- T1110.003 Password Spraying
- T1589.002 Email Addresses
- T1589.003 Employee Names
- T1552.001 Credentials In Files
- T1110 Brute Force
- T1078 Valid Accounts
- T1589.001 Credentials
- T1018 Remote System Discovery

- T1046 Network Service Discovery
- T1558.003 Kerberoasting

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.3361).
- Operational risk: High (score 0.571, reaches lateral-movement).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3491; 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
FIN13	0.3491
Ember Bear	0.3388
Fox Kitten	0.3343
Dragonfly	0.313
Chimera	0.313

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

No indicators were attached to this pulse.

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 initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the

execution stage they must still reach.
- **Projected pivot:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 22+ groups that use Exploit Public-Facing Application, this pairing runs 2.0x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain access and gather information, as this technique allows them to leverage the existing Windows Management Instrumentation framework to execute commands and query system information, potentially evading detection by blending in with legitimate administrative activity. This technique may be particularly appealing as it enables the actor to interact with the system in a way that appears to be normal administrative behavior, making it harder to detect. The defender would likely counter this by implementing the mandated defensive control: Monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=23, lift 1.5), T1059 Command and Scripting Interpreter (n=38, lift 1.2)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command