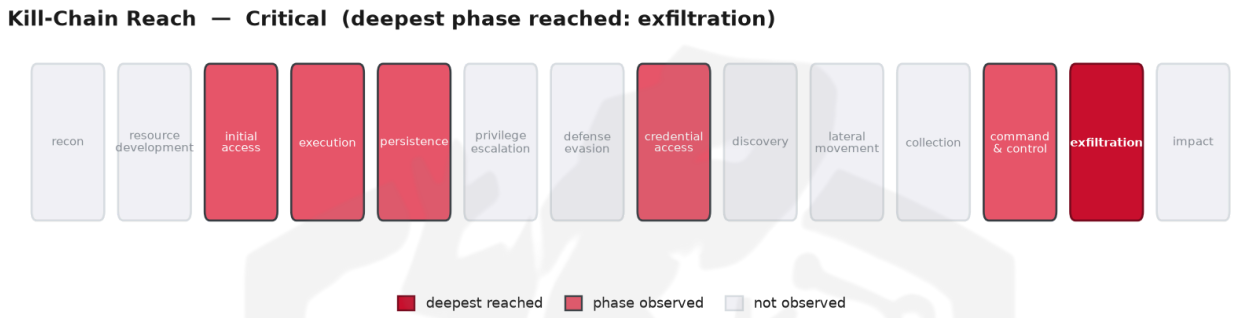
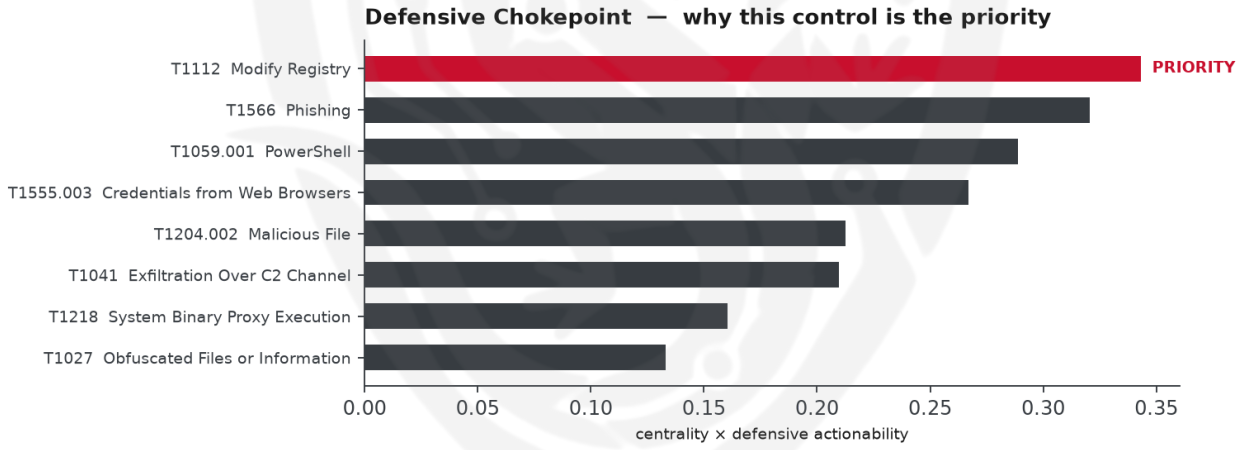
THREAT REPORT: CLICKFIX CAMPAIGN EVOLVES WITH RUNDLL32 ORDINAL EXECUTION

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 involves the exploitation of various techniques to gain unauthorized access and exfiltrate data. The threat actor utilizes Windows Management Instrumentation, Rundll32, and other methods to achieve their goals. Priority should be given to monitoring sensitive registry keys for modification and restricting registry-edit tools for unprivileged users. The campaign's ability to reach exfiltration poses a critical operational risk.

Threat Overview

The threat actor, whose identity is unknown, employs a range of techniques including Windows Management Instrumentation, Rundll32 ordinal execution, and System Binary Proxy Execution. The victimology and targeted sectors are not well understood due to insufficient data. The actor's use of

techniques such as Modify Registry, Exfiltration Over C2 Channel, and Phishing suggests a sophisticated and potentially high-impact campaign.

Attack Chain and Priority Control

The observed techniques form a complex attack chain, with the threat actor utilizing various methods to gain access, execute malicious code, and exfiltrate data. The priority technique is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the following control is recommended: Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users.

Infrastructure and Corroboration

Although the hosting providers and ASNs observed are not available, third-party corroboration suggests that the malware family ClearFake is associated with this activity, as reported by abuse.ch. However, AbuseIPDB has not flagged any indicators with high confidence, 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)

- T1047 Windows Management Instrumentation
- T1218.011 Rundll32
- T1204.002 Malicious File
- T1218 System Binary Proxy Execution
- T1112 Modify Registry
- T1555.003 Credentials from Web Browsers
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1566 Phishing
- T1027 Obfuscated Files or Information
- T1564.003 Hidden Window
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3611).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5574; 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
APT19	0.5574
Nomadic Octopus	0.5119
DarkHydrus	0.4901
Inception	0.4575
TA551	0.4551

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: ClearFake.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
Domain	gentletouchchiropracticclinicauroracol[.]com	ClearFake
Domain	hcwjcope[.]poundbahis[.]com	
Domain	uttepcheweaxtowxdj[.]gentletouchchiropracticclinicauroracol[.]com	
Domain	vqrlwsmzu[.]webyek[.]com	
Hash	f11057ab58bef936d98ba189829c64260a6a540cdaa046f93613138e820c98c6	
Hash	5ef7bf4ed52be2a6d5ebbcf3076fba5f	
Hash	9e03e983e26d4782a3fef0a6ebb47fdcd46974c9	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

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:** T1112 Modify Registry (persistence)
- **Observed here:** T1112 Modify Registry was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1543 Create or Modify System Process (persistence)
- **Basis:** of the 14+ groups that use Modify Registry, this pairing runs 2.8x above base rate, a disproportionately-coupled move rather than the obvious one.

With T1112 Modify Registry blocked, the threat actor could preserve the same objective by pivoting to T1543 Create or Modify System Process, a technique disproportionately paired with it across tracked groups. Defensive countermeasure: Restrict service/daemon creation to admins; monitor service and driver installs.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=19, lift 1.9), T1547 Boot or Logon Autostart Execution (n=17, lift 1.7)

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