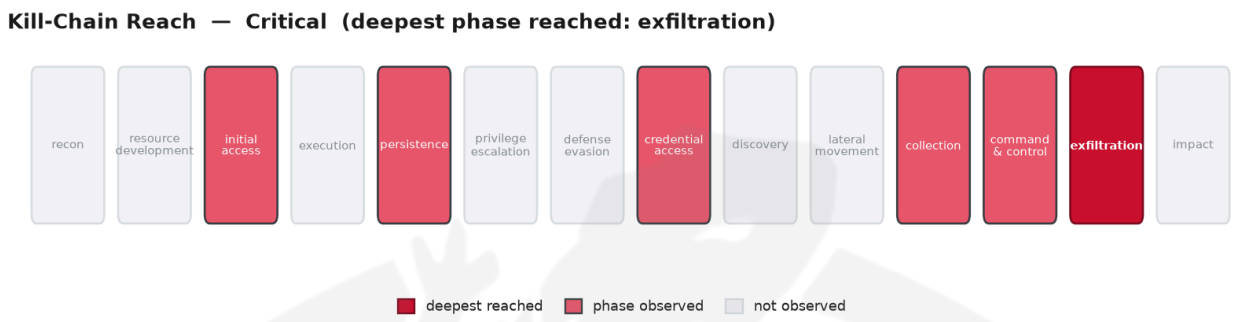
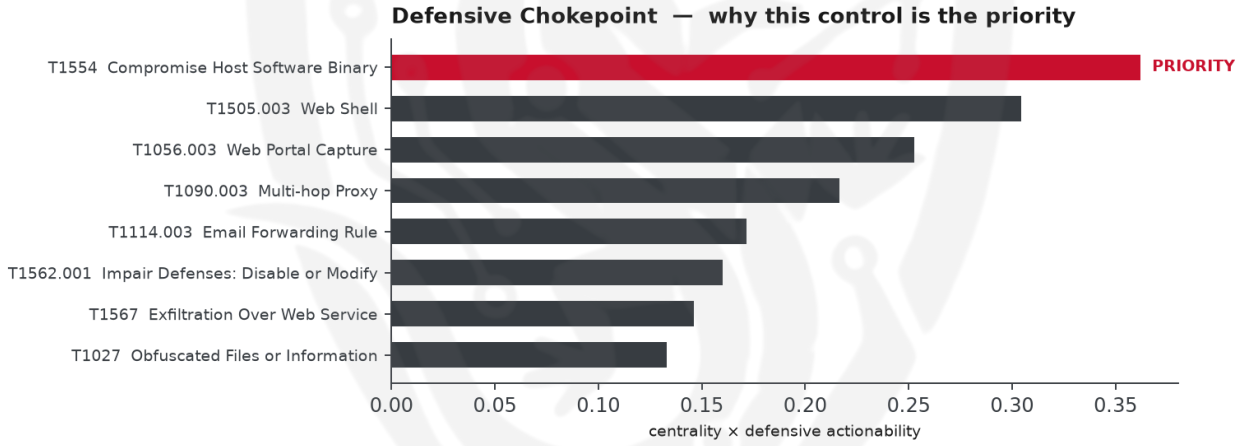
THREAT REPORT: UNC6508

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 UNC6508, a threat actor targeting the public and private medical community in the United States and Canada. The actor is pursuing research in artificial intelligence, cyber, medical, and national defense, using the INFINITERED malware family. Priority should be given to defending against the compromise of host software binaries. The targeted sectors include healthcare, education, defense, and government, making this a critical operational risk.

Threat Overview

UNC6508, the observed threat actor, is utilizing the INFINITERED malware family to target organizations in the United States and Canada. The central vulnerability exploited is currently insufficiently documented, but the actor is using various techniques to achieve their goals. The victimology indicates a focus on the healthcare, education, defense, and government sectors.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including exploiting public-facing applications, credential theft, and exfiltration over web services. The priority technique is T1554 Compromise Host Software Binary, which is the graph chokepoint. To mitigate this, the recommended control is to Apply the specific MITRE ATT&CK mitigation for this technique; add host/network detections and least-privilege controls around it.

Infrastructure and Corroboration

The malicious infrastructure is hosted on Direct Communications Cedar Valley LLC. There are no corroborated malware families from 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)

- T1190 Exploit Public-Facing Application
- T1555 Credentials from Password Stores
- T1567 Exfiltration Over Web Service
- T1505.003 Web Shell
- T1056.003 Web Portal Capture
- T1114.003 Email Forwarding Rule
- T1554 Compromise Host Software Binary
- T1090.003 Multi-hop Proxy
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1213 Data from Information Repositories
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1554 Compromise Host Software Binary (centrality 0.3812).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3354; 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	0.3354
Sea Turtle	0.3162
Volatile Cedar	0.2835
HAFNIUM	0.277
APT39	0.2652

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	Context
IP	23[.]169[.]65[.]49	AbuseIPDB 0% (US) · AS19045 Direct Communications Cedar Valley LLC
Hash	4efbef69eb3b09bacff892d6a55778d07c418e7f15eba3cf1245e8cdfd8dda0b	
Hash	51a57bfc9ed3eb6451c1c289607814d59e1698c666fb97ac5f694c398f23d045	
Hash	58bb25777e0aa86bcd2125101e0bca4e8732b03d91bd8d2f205b446a2a8d5c86	
Hash	8f0158855a656b629ca76ebca565f18bc25563ded34b65d6771632c20edb68ec	
Hash	ba6b73b0ca0dc7f86b3b397893ac32d729fd53f9df20643288f141f29d020af7	
Hash	c1ac43d23f89d41eb4ff131678ab562ab2cfed9aa334b13767ef141d303b0e5b	
Hash	db65c1b9f9e4cb4d729f45ad4b6fcf3e277caf9eb4c875425dec93fd883f9136	

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