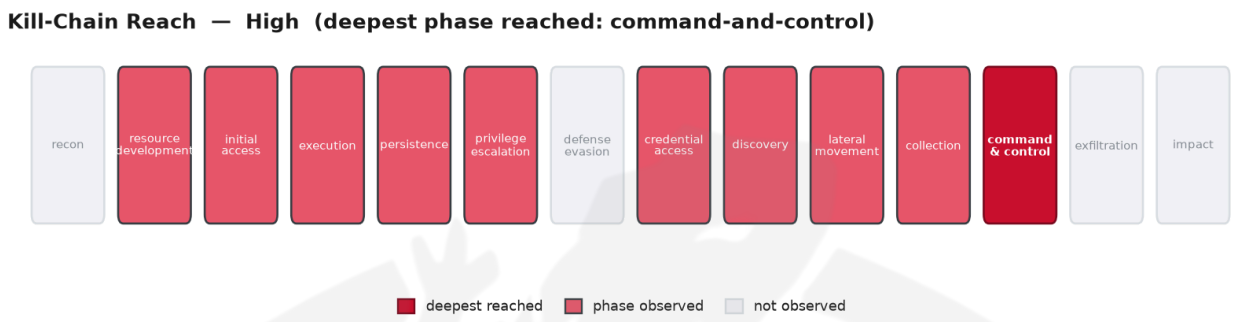
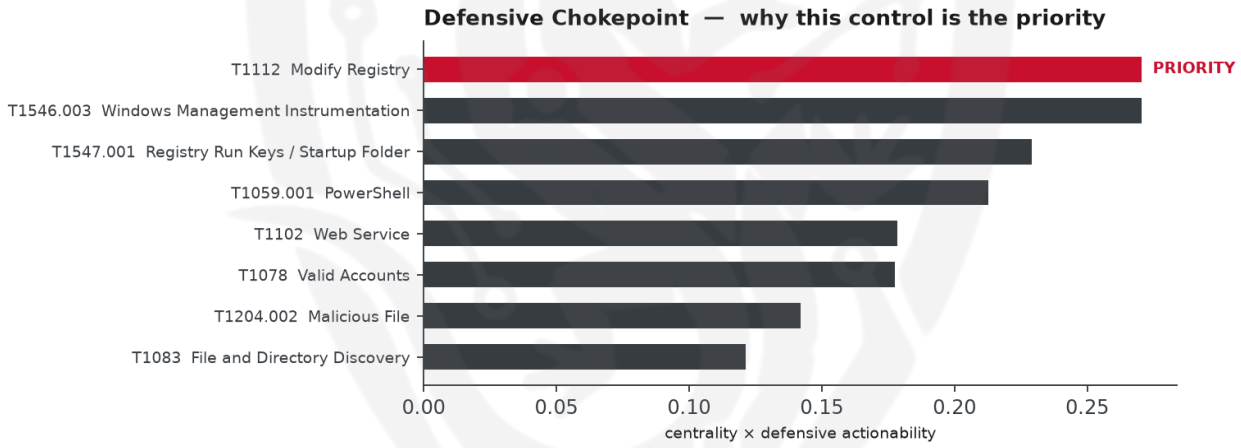
THREAT REPORT: BANDCAMPRO

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 bandcampro, a threat actor who has been targeting the healthcare sector in the United States of America and Canada. The actor's techniques include various methods to gain and maintain access to compromised systems. Priority should be given to monitoring sensitive registry keys for modification to prevent further compromise. The threat actor's ability to reach command-and-control status poses a high operational risk.

Threat Overview

The bandcampro actor has been observed using multiple techniques to compromise systems, including scheduled tasks, password guessing, and email collection. The targeted sectors are primarily healthcare in the United States and Canada. The actor's malware families and central CVE are currently unknown.

Attack Chain and Priority Control

The observed techniques used by the bandcampro actor form a complex chain, including scheduled tasks, password guessing, and network share discovery. The priority technique is T1112 Modify Registry, which is the graph chokepoint. To mitigate this, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The bandcampro actor's infrastructure has been observed to be hosted on NetCrafters OU. According to abuse.ch, there are no corroborated malware families associated with this activity. AbuseIPDB has flagged indicators with a confidence level of up to 1%, but none have reached the 80% confidence threshold, indicating a low reputation flag confidence.

Technical Appendix

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

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

- T1053.005 Scheduled Task
- T1110.001 Password Guessing
- T1114 Email Collection
- T1204.002 Malicious File
- T1135 Network Share Discovery
- T1082 System Information Discovery
- T1005 Data from Local System
- T1112 Modify Registry
- T1583.003 Virtual Private Server
- T1083 File and Directory Discovery
- T1586 Compromise Accounts
- T1102 Web Service
- T1546.003 Windows Management Instrumentation Event Subscription
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1588.002 Tool
- T1078 Valid Accounts
- T1573 Encrypted Channel
- T1071.001 Web Protocols
- T1021.001 Remote Desktop Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2846).
- 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 0.4871; 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
FIN10	0.4871
Inception	0.4697
FIN8	0.4636
APT33	0.4527
APT39	0.4518

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 1%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	213[.]165[.]51[.]115	AbuseIPDB 1% (US) · AS203273 NetCrafters OU
Domain	tralalarkefe[.]com	

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

The bandcampro actor could pivot to using T1078 Valid Accounts by attempting to leverage existing credentials to maintain access and achieve their objectives, potentially exploiting weak passwords or authentication protocols. They may try to use compromised accounts to blend in with normal network activity, making it harder to detect their presence. The defensive countermeasure to mitigate this would be 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