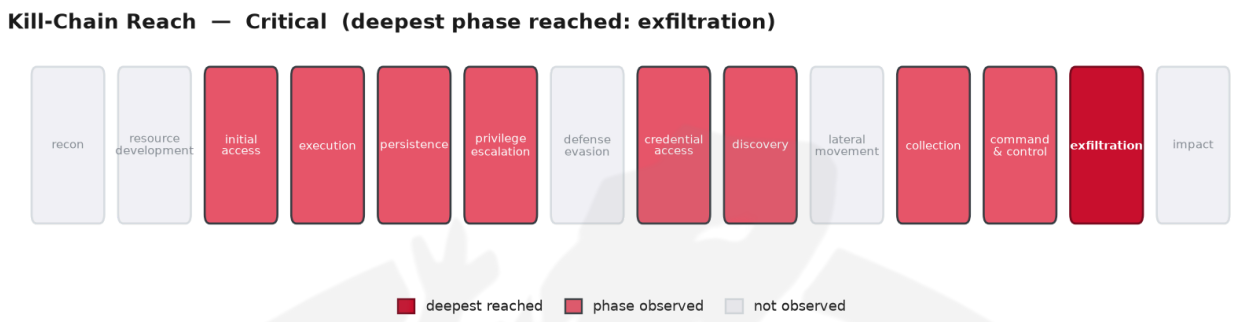
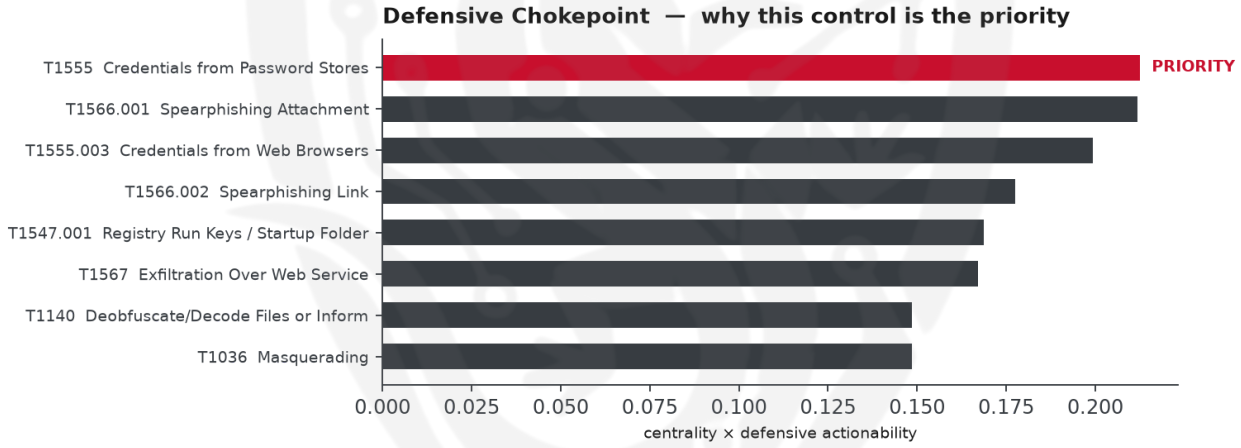
THREAT REPORT: VANTA STEALER CAMPAIGN

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 Vanta Stealer malware, which targets unspecified sectors and countries, with a focus on stealing sensitive information. The threat actor's identity remains unknown, and the central CVE exploited is insufficiently documented. Priority should be given to restricting access to browser and OS credential stores to mitigate the threat. The campaign's ability to exfiltrate data poses a critical operational risk.

Threat Overview

The threat actor, whose identity is unknown, utilizes the Vanta Stealer malware family to steal web session cookies, capture screens, and collect system information. The malware's techniques include stealing credentials from password stores, which is identified as the priority technique. The victimology of this campaign is not well-documented, but it is clear that the malware is designed to steal sensitive information from compromised systems.

Attack Chain and Priority Control

The attack chain involves various techniques, including screen capture, stealing web session cookies, and system information discovery, ultimately leading to the exfiltration of sensitive data. The priority technique is T1555 Credentials from Password Stores, which is the graph chokepoint. To mitigate this threat, the priority control is to: Restrict access to browser/OS credential stores; alert on credential-vault access; enforce disk encryption.

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs observed, and no malware families have been corroborated by abuse.ch. Additionally, 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)

- T1113 Screen Capture
- T1539 Steal Web Session Cookie
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1119 Automated Collection
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1567 Exfiltration Over Web Service
- T1036 Masquerading
- T1555.003 Credentials from Web Browsers
- T1125 Video Capture
- T1083 File and Directory Discovery
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1027.002 Software Packing
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1555 Credentials from Password Stores (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 0.562; 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
Dark Caracal	0.562
Confucius	0.5015
Windshift	0.5
Inception	0.4901
APT37	0.4518

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	3bff25e745707056cf4ed6428ee8aace9a1bff2fb4030e32a7c0470a34cbfa62
Hash	4bdf15157fc0067af179d11e9ad168816ce99a849fd45332482b0b88a05aeabb
Hash	5dbddac39fda06acc703c22935fa24e0b4bcdbc26624a1869fe93cd568cdb9fc
Hash	6f20836eef6496695e5f2a5fd81e7dfb8770df38fb1bf67fcf024c1261352daa
Hash	09e3ce307b2af3f94a315eba97c094d8d755b3674208cc47ceab3c1630a84ad9
Hash	026c85b97a6ddac14c9835d0580228c0a82dd82ce12d8d921c2f3067a12bbb7e
Hash	31f3e50e764a090d2dbf759e6cb5f678c5c6a3a5a96ff3a2069ffda520580e52
Hash	34a01c2429161a8711adff3495ab1dee4419511c8f45c483f50ac71205f68512

Type	Indicator
Hash	44d48b4876cc99f1781877eae9d1e22e99925079a5a8cd0d9022176f5757baaf
Hash	64d85df47edd0187462786ff290f34b080f909a5dda946fa7e83fa3f40aaa878
Hash	96cc8dc992e465f5f959c7d1481e3789067a78c83706a3dd7ba5a20eaf32b701
Hash	467c192e3aeafbac29ab272575bc76545f371a50670fb4a1cf3104dae30622e0
Hash	785d6372f397470c48faa0a9a525b91cb990d0b3ed4b6452e31d75ed179a409c
Hash	858fcd9bd05d73d2dcc1496761e2f71fd0bf75fa0ae66eeb7405f788837ec384
Hash	3349f0cf1d4f294d7d98ee12e0ce03a40740668b50e5e553d843f233a0021d36
Hash	9339c056663e9f57d4b9d34b339cd85048176b9e7d9a20958b7ba190964acd47
Hash	a71c4149bcb8a77ca755ff235e91b1e774293cf3d653aaa2c41fe943cd0848f1
Hash	aa9268a758b5333d725b4b08350ec35e05b9a86f02d65b83b2d9a51e8859b5cd
Hash	b6a7d57fb37a0d9dab8a9e1a81ac6c228fefa4375611bbdf847a775c66cf96c5

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:** T1555 Credentials from Password Stores (credential-access)
- **Observed here:** T1555 Credentials from Password Stores was the only credential-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1003 OS Credential Dumping (credential-access)
- **Basis:** of the 21+ groups that use Credentials from Password Stores, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1003 OS Credential Dumping in an attempt to still obtain credentials, as this technique allows them to extract sensitive information from the operating system's memory, which may include credentials that were not stored in password stores. This technique may be particularly appealing to the actor because it can provide a broader set of credentials, including those of system and network services, which could facilitate lateral movement. To counter this potential move, the mandated defensive control of protecting LSASS (using RunAsPPL, Credential Guard), alerting on LSASS handle access, and disabling WDigest should be implemented.

Also plausible (same tactic): T1552 Unsecured Credentials (n=15, lift 3.5), T1110 Brute Force (n=12, lift 2.3)

Detection and hardening for the pivot (T1003 OS Credential Dumping)

- **Telemetry:** Sysmon (process access); EDR credential-theft telemetry
- **Detect:**
  - Sysmon 10 (process access) targeting lsass.exe with suspicious access masks
  - Access to ntds.dit / SAM / SYSTEM hives; vssadmin/shadow-copy abuse
  - comsvcs.dll MiniDump, procdump, or reg save of security hives
- **Harden:**
  - Enable Credential Guard and LSA protection (RunAsPPL)
  - Restrict debug privilege; tiered admin to limit credential exposure
- **MITRE:** M1043 Credential Access Protection, M1028 Operating System Configuration, M1026 Privileged Account Management, M1017 User Training · DS0009 Process, DS0022 File, DS0024 Windows Registry