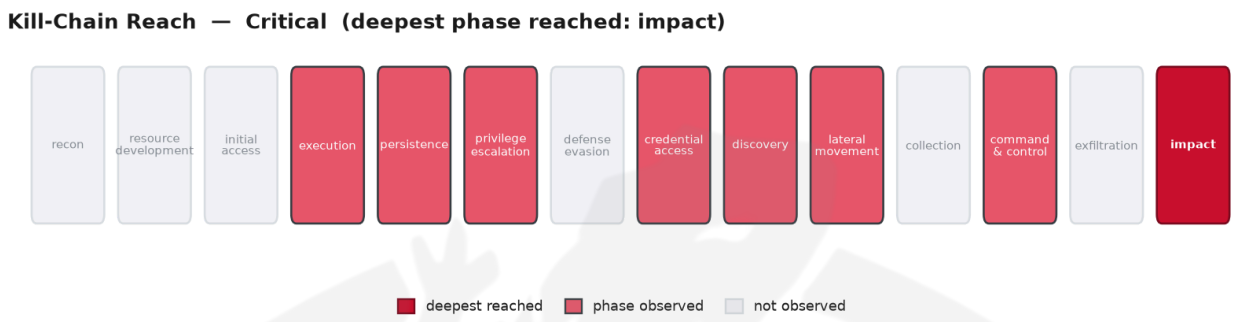
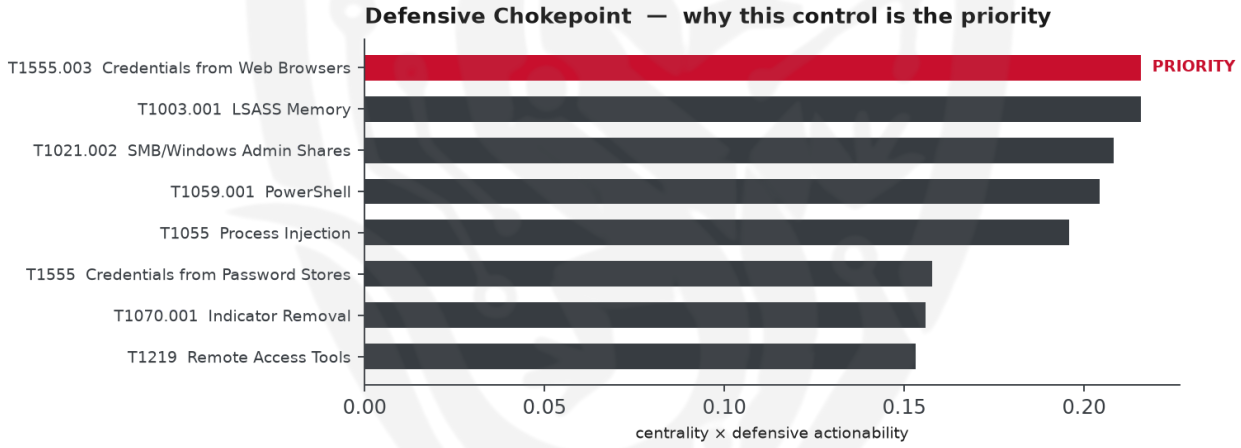
THREAT REPORT: HYADINA

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 Hyadina, a threat actor utilizing the GodDamn ransomware, among other malware families, to target unknown sectors and countries. The actor's techniques include credential dumping, network share discovery, and process injection, making it a critical threat. Priority should be given to restricting access to browser credential stores and enforcing disk encryption to mitigate the attack. The threat actor's ability to impair defenses and encrypt data for impact poses a significant risk.

Threat Overview

Hyadina, the attributed threat actor, employs a range of malware families including GodDamn, Beast, Monster, PoisonX, and Mimikatz. The central vulnerability exploited is currently unknown, but the actor's techniques include OS credential dumping, Windows service manipulation, and network share discovery. The victimology of this campaign is not well-defined due to insufficient data on targeted countries and sectors.

Attack Chain and Priority Control

The observed techniques form a complex chain, starting with system information discovery and network share discovery, followed by credential dumping and process injection. The priority technique is T1555.003, Credentials from Web Browsers, which serves as a critical chokepoint in the attack chain. To counter this, the recommended priority control is: Restrict access to browser credential stores; alert on reads of Login Data / cookies files by non-browser processes; enforce disk encryption.

Infrastructure and Corroboration

Although there is no observed hosting provider or ASN, abuse.ch corroborates the presence of the Mimikatz malware family. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, and the highest confidence seen is 0%, indicating a lack of independently verified malicious activity associated with the known indicators.

Technical Appendix

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

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

- T1003 OS Credential Dumping
- T1543.003 Windows Service
- T1135 Network Share Discovery
- T1082 System Information Discovery
- T1555 Credentials from Password Stores
- T1219 Remote Access Tools
- T1055 Process Injection
- T1021.002 SMB/Windows Admin Shares
- T1555.003 Credentials from Web Browsers
- T1070.001 Indicator Removal
- T1003.001 LSASS Memory
- T1049 System Network Connections Discovery
- T1057 Process Discovery
- T1059.001 PowerShell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1486 Data Encrypted for Impact
- T1018 Remote System Discovery
- T1569.002 Service Execution
- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1555.003 Credentials from Web Browsers (centrality 0.3082).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4461; 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
BlackByte	0.4461
Medusa Group	0.4002
Blue Mockingbird	0.3964
APT3	0.385
Wizard Spider	0.3779

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: MimiKatz.
- 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
Hash	141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944	
Hash	d28f0cfae377553fcb85918c29f4889b	
Hash	df218168bf83d26386dfd4ece7aef2d0	
Hash	32e24780735a0148c3cc4ce7dda30ed9365397a9	
Hash	4a3418d78d8fe36b39d1ee5435796369b88a8762	

Type	Indicator	Context
Hash	816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019	
Hash	5e85446910e732111ca9ac90f9ed8b1dee13c3314d2c5117dcf672994ce73bd6	
Hash	7a313840d25adf94c7bf1d17393f5b991ba8baf50b8cacb7ce0420189c177e26	
Hash	8e4b218bdbd8e098fff749fe5e5bbf00275d21f398b34216a573224e192094b8	
Hash	c92580318be4effdb37aa67145748826f6a9e285bc2426410dc280e61e3c7620	
Hash	31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc	MimiKatz
Hash	faca9e856c369b63d6698c74b1d59b062a9a8d9fe84b8f753c299c9961026395	
Hash	863fa58aa1fe8a88626625b191d4722e	
Hash	e7fb4bf69be5ac4583c0c02e26a17bd3cdef4c02	
Hash	45126297c07c6ef56b51440cd0dc30acf7b3b938e2e9e656334886fe2f81f220	
Hash	fc3b93e042de5fa569a8379d46bce506	
Hash	1ba499bafaa369be58e795a150403c8729ef5d95	
Hash	5be325905df8aab7089ab2348d89343f55a2f88dadd75de8f382e8fa026451bd	
Hash	e736229e890a138ccf7810e00a6bb50d	
Hash	10955a02ef3fd3f80f20062c401bf7960ff6ce94	
Hash	17fb52476016677db5a93505c4a1c356984bc1f6a4456870f920ac90a7846180	
Hash	2d91a78e739891c9854c254f5b2a6b84c0e167dfa253466cbccd2cdd1c20145d	
Hash	07e9f0b8627a95960e79e930fb099e84	
Hash	56bee9df5833a637f5c54d5911df98b0812fe643	
Hash	d29670e684e40ddc89b47010c37cbc96737035b6	
Hash	233b795102dd9cd630aebddfe3c15bbb	
Hash	b29f91a440527fb621d106a2048f6379fff3263c60aeda9c82ff8c1d5ae880a8	
Hash	4277a6be9b121a30564aca6ba32db272	
Hash	8e776dbb71eb8f42dffd3020175edef5	
Hash	7b01f64b7818d315ef7a2485c4ce2a5d6896cb58	

Type	Indicator	Context
Hash	7d33e173819ecd502f790bf6d3da260a82dedfa2	
Hash	19bab15a34d5ad838ccf4d187eb40379c335fa56446d0f9621865b2767d4ac7d	
Hash	35296e7a34688ca3e3159bcdf92b4d60ba4173a2369aca531bb7bc959f68ed9c	
Hash	5c4c98d774eb100f9a89ae4e984c27a4f532e58c7cf8c87046dc87db5a065404	
Hash	8ff1c1967841a595d996a649c8134b7a5970dcf94624b237d1b089e7c6266167	
Hash	9fae3f15900e13ec3860a109555ecd33ca43d38907c63438c50a2d6d91bfee1d	
Hash	e097f3b445b63b07afacde8d6a67f0be654dd51e228a3610fb0710a1f7e29a69	
Hash	ece33e4b7e2d26eeca8ad9db4439f9801a7a77e332611116156738b1b0316046	

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