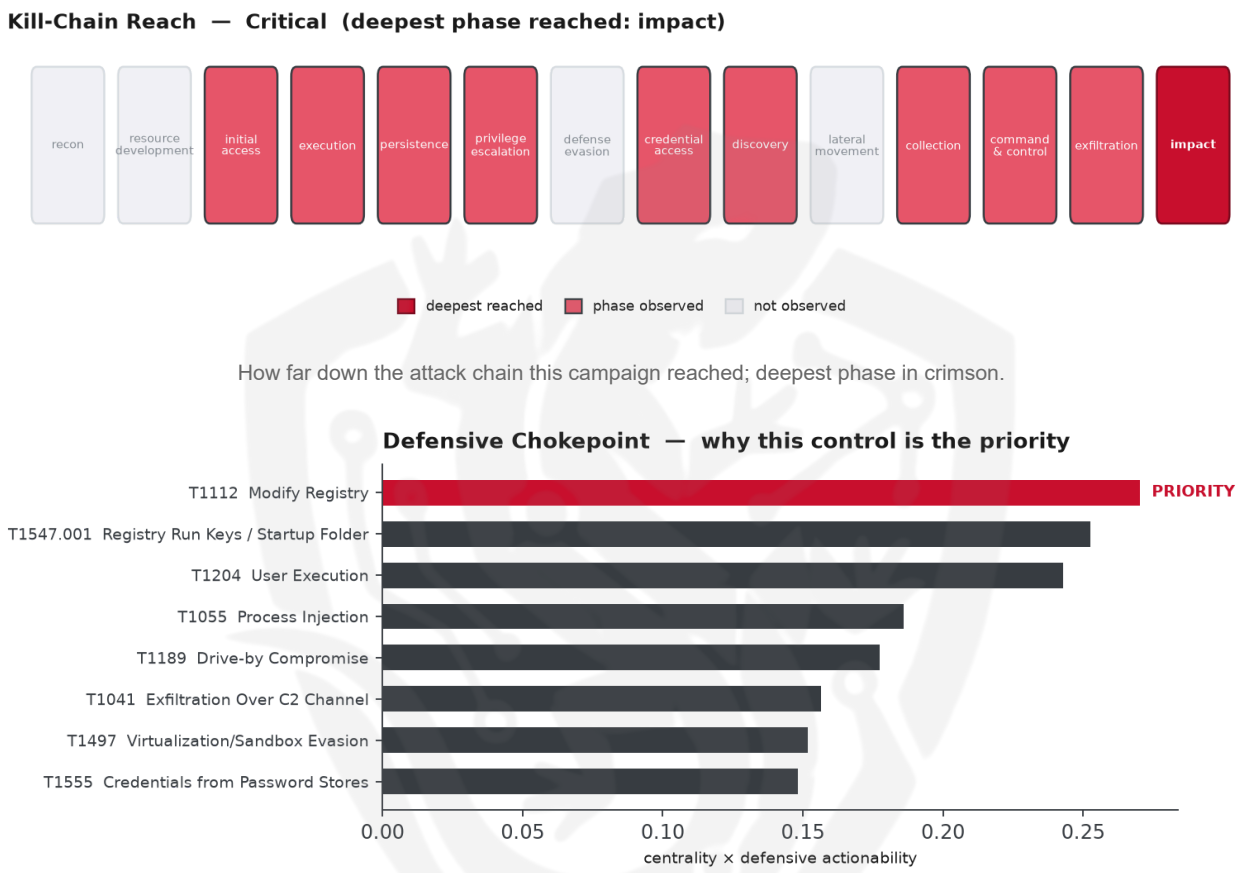
THREAT REPORT: X3D MINER

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 X3D MINER. This threat actor has been observed utilizing the Vidar and XMRig malware families to target entities in the United States of America. The actor's techniques include various methods of system information discovery, data exfiltration, and registry modification. Priority should be given to monitoring sensitive registry keys for modification to mitigate the threat.

Threat Overview

The threat actor, attributed to X3D MINER by the source, employs the Vidar and XMRig malware families. The central vulnerability exploited is not specified due to insufficient data. The threat actor targets the United States of America, with the targeted sectors being unknown due to insufficient data.

Attack Chain and Priority Control

The observed techniques form a complex chain, including scheduled tasks, system information discovery, data exfiltration, and registry modification. The priority technique is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To counter this, the recommended control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The malicious infrastructure is hosted on Hetzner Online GmbH. Additionally, abuse.ch has corroborated the presence of several malware families, including ClearFake, LummaStealer, RemusStealer, Smoke Loader, and Vidar, which are related to the observed activity. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher.

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
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1036 Masquerading
- T1055 Process Injection
- T1112 Modify Registry
- T1083 File and Directory Discovery
- T1497 Virtualization/Sandbox Evasion
- T1204 User Execution
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1496 Resource Hijacking
- T1189 Drive-by Compromise
- T1071.001 Web Protocols
- T1518 Software Discovery
- T1574.002 Hijack Execution Flow

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2846).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4945; 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
APT37	0.4945
Windshift	0.4682
Higaisa	0.4559
Stealth Falcon	0.4305
Dark Caracal	0.4305

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: ClearFake, LummaStealer, RemusStealer, Smoke Loader, Vidar.
- 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
IP	136[.]243[.]203[.]109	AbuseIPDB 0% (DE) · Vidar · AS24940 Hetzner Online GmbH
IP	138[.]199[.]246[.]13	AbuseIPDB 0% (DE) · Vidar · AS24940 Hetzner Online GmbH
IP	136[.]243[.]203[.]111	AbuseIPDB 0% (DE) · Vidar · AS24940 Hetzner Online GmbH
IP	116[.]203[.]243[.]208	AbuseIPDB 0% (DE) · AS24940 Hetzner Online GmbH
Hash	d42595b695fc008ef2c56aabd8efd68e	

Type	Indicator	Context
Hash	1aae8bf580c846f39c71c05898e57e88	
Hash	d8b31f8c03e0c76ff245ed05a15ffe6c	
Hash	03e6f4f49cec3af38bbec9ed64c195c7a85a630ec989efb3669f04a2993c1dd7	LummaStealer
Hash	6b7ff061eebeb9ead8812c410247768a7ba90786aeeb1baafa6412cc5b08237b5	Vidar
Hash	b830f043076a12748b6a2dc0810ece85439ee77434d991ae7d84201b09ead756	ClearFake
Hash	68ced9d7c1b1ff8ffb5f56c7d3f849d4fd16a1b95324426811424b40043d6d25	Vidar
Hash	b9b6893fa6b04ee8daa29e515c08239ac5204af1a1fa2bc10006eede1b41329b	Vidar
Hash	d6446f2803444bd2200d48a01a9ad7d487e67e8e831c9cd13f89cbfec17fd4e2	Vidar
Hash	74df77b6a83d89fa137fd285a2efde36b1d62c00b3be81cc93df7d1e6e94837b	RemusStealer
Hash	b8b5f6991a3a61083461d5269245bebf28b90934c328848ba8c1e084a5a6216c	Vidar
Hash	95cd48130247525d8a7e966bd3fa07e9d6c39ebbe3058eccb336f66bb8e3d1e	Vidar
Hash	613e5314a7ded3155cdec49fd34e852e181f4651d78bd8bf3adad2f4dbf22b0d	Smoke Loader
Hash	8dbcde2a28a0b3de201214d7e3bd43acc97561924daa247c05c4b0536d42be85	Smoke Loader
Hash	634e89d8592d7c9e2bc1c098217a813947b44a4f80bc569e9a15c1e8b0864b91	Smoke Loader
Hash	6d49233b1fca22f3823e856e4c16749e9c45f384ea57055fead16df35b217226	Vidar
Hash	8cb8301f664e1e42dee8b7032fa321fc	LummaStealer

Type	Indicator	Context
Hash	f732e938a8fda479886576df82c611f9540db42c	LummaStealer
Hash	3e906ae47e9836a591f44d4b743e961d634a404fa8fd8bfae64f1d54c853be2b	
Hash	b6912c23cccc4b0964d55608916297f6978f0b38c80a4beac472004a786fcef7	ClearFake
Hash	03222c6ca2f60f70b95e454141ce8e25	
Hash	033a49eb29d1ca3979757f3263ff6417	Vidar
Hash	056207e13f91698b94ead7c21cc5a1ba	
Hash	3c5300ebbc140ec500d5ddc886b95cd5	
Hash	3e177cc39048ad17dce44452666bba0e	
Hash	4d40d9c6445cb096f24bbca6862042a7	Smoke Loader
Hash	5132da5f4c7c4693c7bdfbda5c047300	
Hash	55e7443b66c9c626abe71551233e0a30	
Hash	655393e472be5409bc0ff521aa1662de	
Hash	6695ae857e67b6283d49c6531a253db6	Vidar
Hash	684c8447df60b13bc258a33ed636ce93	
Hash	70f7dc41628613af7bb16490ca6c8510	
Hash	72633fc47f89679472f058be0177a494	

Type	Indicator	Context
Hash	874df2d775a5eb406bc9d2c8811ce8c7	
Hash	8c2b728e57531e24813e628cfba3f1c5	
Hash	8ff9f6c05dfde0ee639c36cb53cb29a5	

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