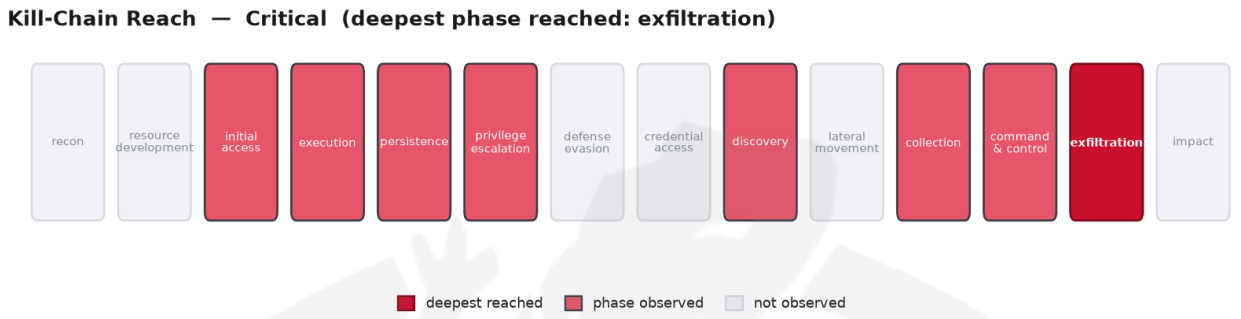
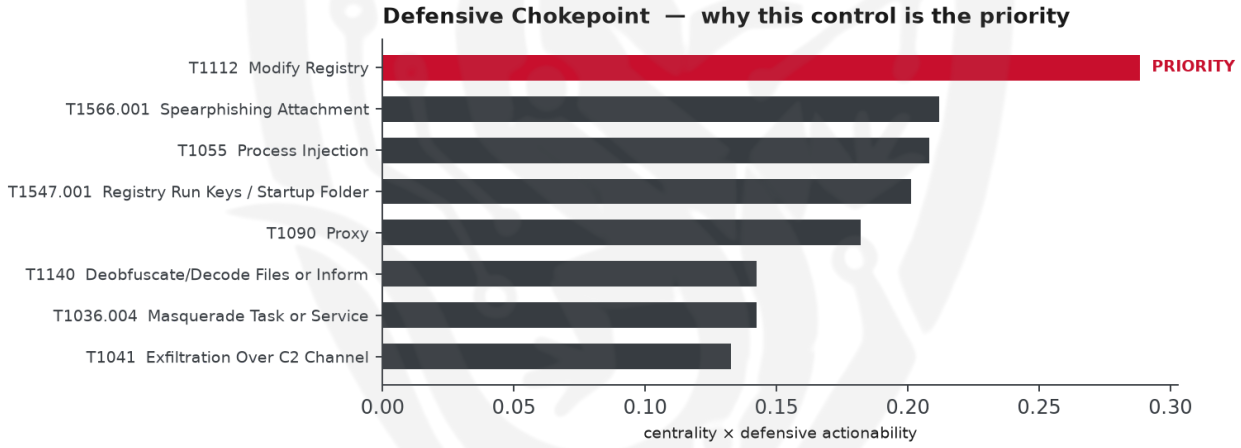
THREAT REPORT: GHOSTSHELL

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 GhostShell, a threat actor targeting Ukraine's defense sector with a malware chain themed around Besomar. The malware families used include Vidar, and the threat actor's activities have been observed to pose a critical operational risk due to the potential for exfiltration. Priority should be given to monitoring sensitive registry keys for modification to mitigate the threat. The threat actor's use of various techniques, including screen capture and system owner/user discovery, further emphasizes the need for vigilance.

Threat Overview

The threat actor, attributed by the source to GhostShell, has been observed using the Vidar malware family to target Ukraine's defense sector. The central vulnerability exploited is currently insufficiently documented, but the threat actor's techniques include screen capture, system owner/user discovery, and

symmetric cryptography, among others. The victimology indicates that the threat actor is targeting Ukraine's UAV supply chain.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including initial spearphishing attachment, followed by system information discovery, file and directory discovery, and process injection. The priority technique identified is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

Although no specific hosting providers or ASNs have been observed, the malware families used by the threat actor have been corroborated by abuse.ch, including Cobalt Strike, GhostShell, and Vidar. However, according to AbuseIPDB, there are no 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
- T1033 System Owner/User Discovery
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1112 Modify Registry
- T1090 Proxy
- T1083 File and Directory Discovery
- T1036.004 Masquerade Task or Service
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1564.001 Hidden Files and Directories

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (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 0.5711; 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
Higaisa	0.5711
Windshift	0.55
Inception	0.5281
Tropic Trooper	0.5143
Darkhotel	0.4951

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Cobalt Strike, GhostShell, 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
Hash	ab5681266f70af7df24383f15de876e411fc18e35cb6f24603b12f580b05ccb3	GhostShell
Hash	8de34006dafd990853a45cbe9aaab4ee18c8cd4c1ad0a98fe71f8d63cd60db25	Vidar
Hash	b1834634820ae696f0514ca2b6723061f115857232306e573f4d115bc6ead012	Cobalt Strike
Hash	16a59e1fece21ca5394a8ec9ea596fec	Cobalt Strike
Hash	6da30ad8677b058fad4d3d3031a428ec	GhostShell

Type	Indicator	Context
Hash	d0a66dd44ee64b76de79cddab13d2745	Vidar
Hash	4b5f407f5966f49f8c1005a94a822c83b20fa325	Cobalt Strike
Hash	52a1b02e4fe0998069c777bec37eb394781e8fda	GhostShell
Hash	c4834de90f419c5517f3a1c13d219d71fc85e742	Vidar

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