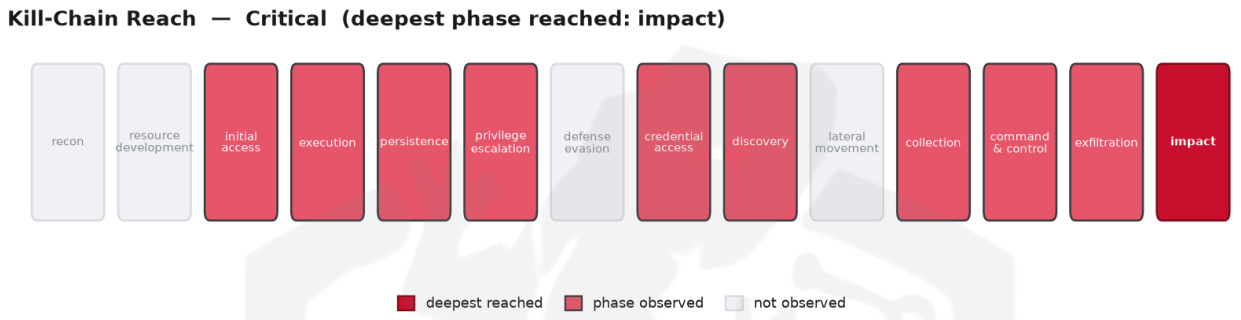
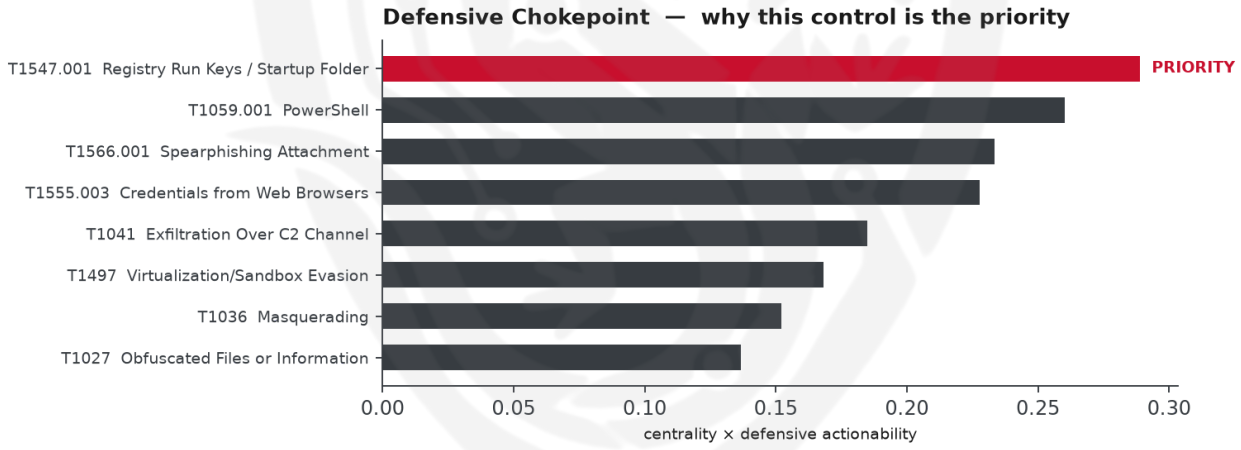
THREAT REPORT: SHADOW-EARTH-066, EARTH DAHU

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 SHADOW-EARTH-066, Earth Dahu, who are exploiting the CVE-2025-8088 vulnerability in WinRAR to target government and defense sectors in Ukraine. The threat actor is utilizing various malware families, including GIFTEDCROOK and GammaSteel, to carry out their attacks. Priority should be given to patching the CVE-2025-8088 vulnerability on all affected systems to prevent further exploitation. The observed cluster of activity highlights the importance of managing software updates to prevent such attacks.

Threat Overview

The threat actor, SHADOW-EARTH-066, Earth Dahu, is exploiting the CVE-2025-8088 vulnerability in WinRAR, leveraging malware families such as GIFTEDCROOK and GammaSteel to target government

and defense sectors in Ukraine. The victimology suggests a focused effort on compromising systems in Ukraine, with the threat actor employing various techniques to achieve their goals.

Attack Chain and Priority Control

The observed techniques employed by the threat actor form a complex chain, including stealing web session cookies, using malicious files, and symmetric cryptography, among others. The priority technique identified is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended control is to "Patch CVE-2025-8088 on all affected systems as the top priority, then: Audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries; alert on .lnk or script creation in Startup by browser/email temp paths."

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this activity, 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)

- T1539 Steal Web Session Cookie
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1566.001 Spearphishing Attachment
- T1005 Data from Local System
- T1036 Masquerading
- T1555.003 Credentials from Web Browsers
- T1497 Virtualization/Sandbox Evasion
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1485 Data Destruction
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1564.004 NTFS File Attributes

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.3042).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5488; 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
Inception	0.5488
RedCurl	0.5164
Nomadic Octopus	0.4824
Higaisa	0.4685
Stealth Falcon	0.4588

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
Domain	astrocaf[.]com
Domain	astrocaf[.]com
Domain	malicious[.]workers[.]dev
Domain	joymobile[.]com[.]ua
URL	hxxps://136[.]0[.]141[.]138:8406/rcv/
URL	hxxps://136[.]0[.]141[.]41:9580/rcv/
URL	hxxps://166[.]0[.]132[.]237:7044/rcv/

Type	Indicator
URL	hxxps://38[.]225[.]209[.]229:9623/rcv/
Hash	2a8ea9f1ad8936fb302243faa64b91c5767df411923715cbdb1a869e3bfd7e6d
Hash	c0b73ff43312d442260328a8cefdf3b6
Hash	4528d5cf07bf0e1ac769b390236cab1bf34b938c
Hash	7200a9f1e1ea51b66ab9c9274e9d8f805633179634e8ff4dcb8ef82bc02518df
Hash	2af0a6135df3502a7f6de4d2de6db73b
Hash	b1c4a94df23638d70dae45f3193a64a6b036056d
Hash	3d371ef71e40c34a75c168d4647db096c2f386499d99a88d4e16b63cd4acda25
Hash	3d371ef71e40c34a75c168d4647db096c2f386499d99a88d4e16b63cd4acda25
Hash	a84375d4bd67c46d50fef7f7af31c7fb
Hash	526833a16669a85f0546809bfc35122e6f0bc17b
Hash	1c170b7470d507378ddb78e9d66305f1184e965baaf2d27ededb23a318a58953
Hash	2d9adb7932b7842dfb0e0f453b87e5d28dd4552094105e6340bad009956d8c2b
Hash	378809699c7252dc38b31969b9cc40858397759f15d6e418246dfaba9088fdd1
Hash	37b42a83715f7a34e00d3458d4f4b6e53b8c95372677ce020a2e38e80e60ba87
Hash	3c0330f9f934f86b6b70e108ff279a009b88a4a815acbed4adb3664e322e3e59
Hash	44f6f7ba668fc645129d66353e6f60402822ae929ce54648cae0bba6348a18ea
Hash	4e21c4c97aeb391473ee1e44961676f32de2ee8b56ecb136c1d8081df97c3db4
Hash	507b2fcdae058cebbd550965b90c44e878d7a2463058c846eeb68f0dc1b48eda
Hash	6083aac5376b7ca74cc363e0d66f70beaffee543d098c612b820b16fbfb0aa52
Hash	65c053030558b4a3588e2590c5c4961a9912180b731686deb3f4c831e765a095
Hash	718465f44c0680740fb61790eda3d2f4c5218c9de0c560299c580fa1602dc9c7
Hash	77963398e2c5c2fdf9d28d9c5f9c2791cfbf422ba02225e01635dd7f5b31eff8
Hash	7d3ba419751e5ea52b567e1162f6a366bf3d06c44c8956a9f14520e9fb6ed0b1
Hash	8150b2b39fa62fa2de177ed8526c621a3581c0eb481dd9740fc5894ce2b7c13b

Type	Indicator
Hash	82fda6ea769d61aba230c3487787087cec53dd378e22f22a8fb8f0bd5ae83ded
Hash	89d20418450b34efe698bd36214100cfa49f60adf1c39a8bc8d65991b1ce2c23
Hash	a717dd74c01fcfce35a28f374e1c6f9ded06d6f7b0cc04618ce9454ad64febb8
Hash	b01f31c9541579ad34f4e50acafec252eb419f5b1ca98155e0ec84c19d12c9e4
Hash	bf338d88f60c0d352cd0d1b5e4bc6a1d9f1ac8fe1df48516ec0042cafda821e9
Hash	ce78748acd8e9be741b143ad716d735dc682bd5a010427a199744b81456f8e35
Hash	d1d26b0f68e26ac591848796aeef7b9c766442bbff47af8823f9b23d1b588836
Hash	dc5082b07eb994ddee343a4080dce0a9ec2e891e5690654e24ae74ba9eabe422