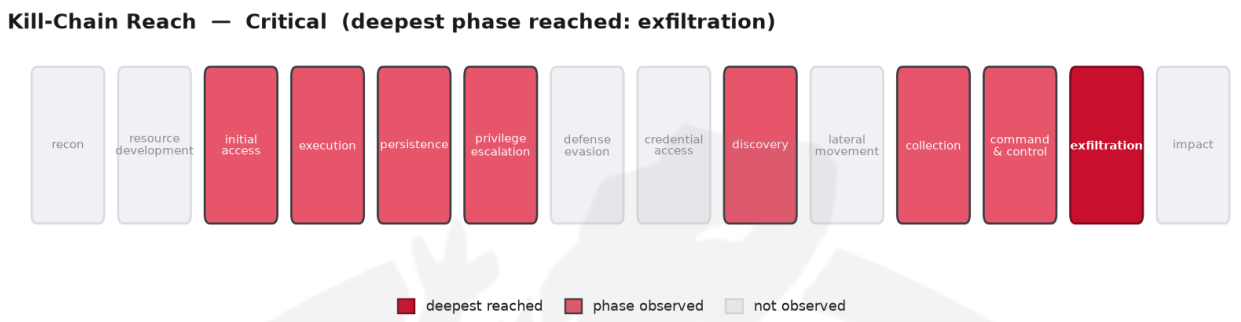
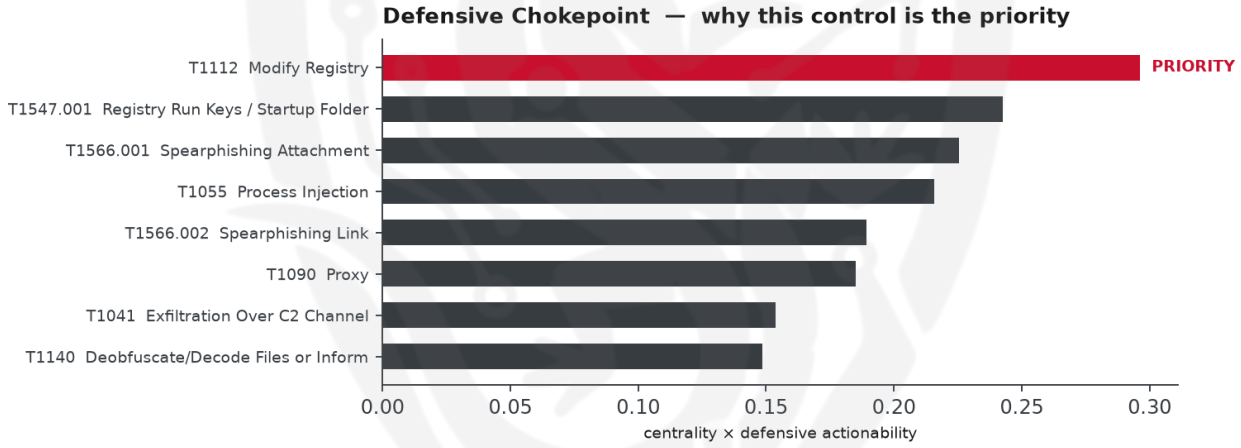
THREAT REPORT: TURLA

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 Turla, a threat actor that has been observed using various malware families, including STOCKSTAY, Kazuar, and others, to target government and defense sectors in Italy and Ukraine. The actor's primary goal is intelligence gathering, and priority should be given to monitoring sensitive registry keys for modification to prevent data exfiltration. The threat actor's use of multiple techniques, including spearphishing and process injection, poses a critical operational risk.

Threat Overview

Turla, the observed threat actor, has been using a range of malware families, including STOCKSTAY, Kazuar, WILDDAY, DIAMONDBACK, and several STOCKSTAY variants, to target government and defense sectors in Italy and Ukraine. The actor's activities are focused on intelligence gathering, and the malware families used are designed to capture sensitive information from compromised systems.

Attack Chain and Priority Control

The threat actor's attack chain involves multiple techniques, including spearphishing, process injection, and registry modification. The priority technique is T1112 Modify Registry, which is used to establish persistence on compromised systems. To mitigate this threat, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs used by the threat actor, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with high confidence by AbuseIPDB, 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)

- T1560.001 Archive via Utility
- T1113 Screen Capture
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- 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
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3119).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5715; 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
Windshift	0.5715
Dark Caracal	0.5506
Higaisa	0.531
Inception	0.5145
APT37	0.506

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	391e51354118fb87dc57650cbbd94258c3f7c0a0d6868040b7a473ad626ff25e
Hash	123508dbce0c72623756ccf793eb7183
Hash	2ee228def4ab5f4f75b978be1f2d474d
Hash	86a75cdc7c5f2a9cc87bbf56e925e544
Hash	9f89939b8b3cbf015b85b67974e15ce7
Hash	ff9f6af06c64a51a576333da5c780263
Hash	4ec2ba1fdc083f69a6132afba72c21f456f6d0af
Hash	5c96ada9b79fa8bd2feb496a8bd6ac7d17287c99
Hash	b5939b7b8925a83d715429aaa2603ae85746d485

Type	Indicator
Hash	c214c62867aae327fbaa4f35dadc786cbe213727
Hash	fb3dbf671ff7c72e02ab03837bd9ce72dca799bd
Hash	0a545dd1b703cddfb3d582c8c70f65f556bbd580bfa836a387121eb837bda61b
Hash	0d6b083208097d5b3e189891338540f6c64faaaaf268b0bb0b085dd53d5857b4
Hash	1682e8d82016b3f10434d2ebac995fd3b6aa812f079bfd7888652e94a994d851
Hash	19e6ed42248f9d03beb343a7c09a864dcd3cd671c29e1e5eac93579225224ac9
Hash	1a2ca8b8e0344fe3d80da7352206a470245443e2349a237bc093df934ddc011f
Hash	1fc23ec18a94a599a34c74ef5f49a1e27acd37a07d5846661702b5e7e81a6a24
Hash	249a4c7cacdd8e99a2a089a5c0ce904f2eff22e0e40fcfb10f7824dca6c51ecb
Hash	2623c6e3c1f5a7b5e735a64813bc0e1382ae45831f5fadffb08c0e7b096627f7
Hash	2af7b513c05e76d7da5f75bb0a223c894a706c99ef2c2ddfe4eae542f95a08e0
Hash	34fcbe7e90fc87a4f3766469c19a64f24672d7adb99e0198f5ba10d58911368b
Hash	3627f582420ad2782d452fe6d13fae42658d1484296351d3916703e25dcadd14
Hash	40a3b969d81ef1ef35dd9ebcc6774e060b1b8949d3d74f38ca6b7d789c95cdb3
Hash	40b1208dda0cd5dd95c6b57764b2cfe7145b3ed9457f498408b4aaa05bf3ef50
Hash	447f430b46fad5a3f8e8c5aad1f8f7f79af069489c3d9c29224bb9f14f0c7bf4
Hash	45bb8d1ab2c13bf4354294e13d3c9be15de625d807301905b98462f43f93e893
Hash	4e3bed10a8eff3e9205c1f37f647512464271d5ac65df7ae4709735621a38320
Hash	55249f296b63a8bcf911b8bc96de43c1ac2b4a56c150a19d33d892a47e57352c
Hash	626330d22f77d9cbca9d40cc06568041703f194610c4c5a84bbb05a2e4ee7459
Hash	6298f3150ad94a242e649886d47c59c634a4d04b9af5ee15e3bf335c40b5e58e
Hash	667a8f568a611f2f3d84a366b7946b360e055bece9699c95aad619637ab72a38
Hash	6cee9e838792ac5e2098362d68ce93a9a2c095d476dc16b289fe8509c99b2b8b
Hash	6da0b4c1a5d0d3fb6e6a2990a82ba51db1f68a3bba818baa46526a29731e2342
Hash	7615140f78d9a0ce31cc9fe8c54c60028a7439cb32526fd97b10afef7145dd78

Type	Indicator
Hash	77417df21b4b4e8d86b8bda4afeef93fd36f355362586b2d1f51121a82244167
Hash	80f6c010fd260d0bcf18a4b6a8d62505adbed50d2e615ed9522c4bfd61c00661
Hash	813c78b5b6ef28a9c0ed35f2c6cd88fc50880ab91f8777dfe7aaccb1c24b08d5
Hash	81aabf646619ea5f4a72457cd3aa17c5988003d67e6454f45e7cb33613021bac
Hash	82707cfdf24dcb762f4615f01e1ba4d3dfdec4abe9cd588558d2634d7e6a5eeb
Hash	9164054d0bf0b7c8820da4f742860940998984555e65820e4fa8dd07b6bd67ec