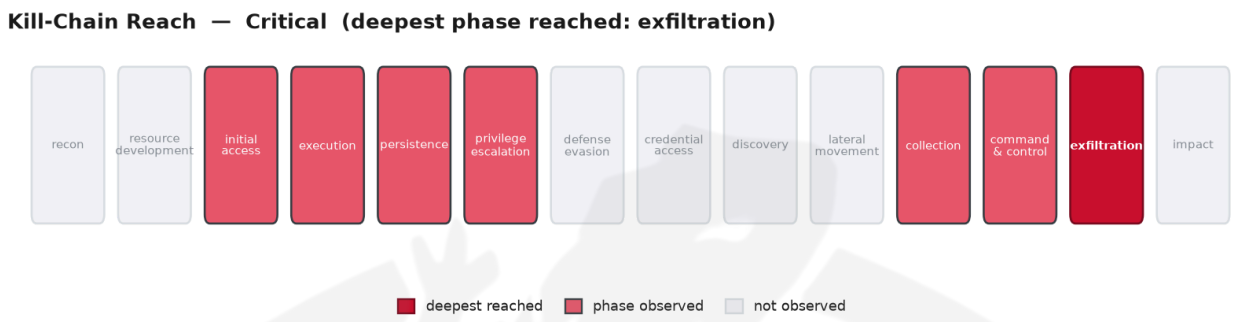
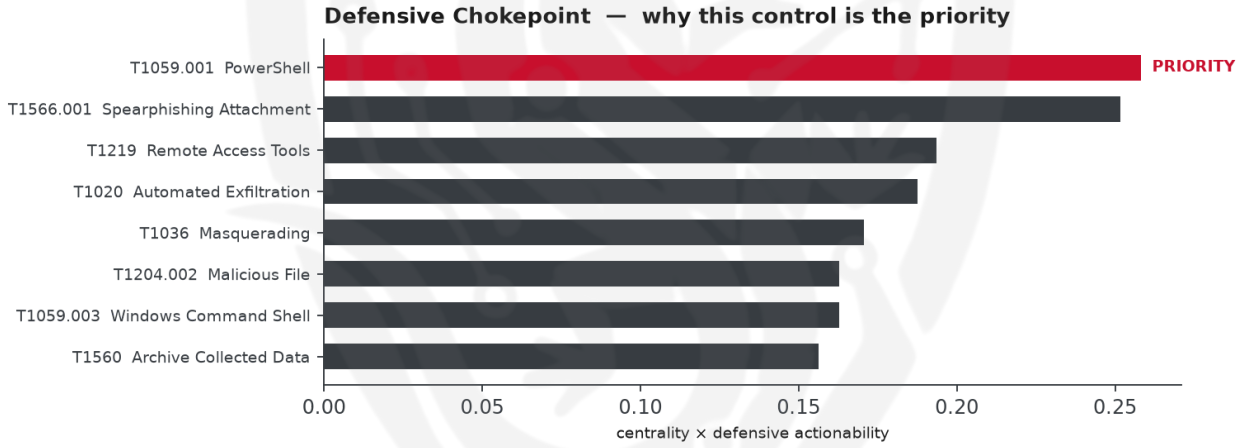
THREAT REPORT: RARE WEREWOLF

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 Rare Werewolf, a threat actor targeting Russian aerospace organizations with a phishing campaign. The campaign's goal is to gain access to sensitive information, with the ultimate priority defensive action being to constrain PowerShell to prevent further exploitation. Priority should be given to defending against this campaign, as it has been assessed as critical due to its potential for exfiltration. The threat actor's use of various techniques, including scheduled tasks and spearphishing attachments, highlights the need for a comprehensive defense strategy.

Threat Overview

The threat actor, Rare Werewolf, is observed using a range of techniques to target Russian aerospace organizations. While the specific malware families and central CVE used in the campaign are not identified, the actor's tactics involve exploiting various vulnerabilities to gain access to sensitive

information. The targeted organizations are primarily in the Russian Federation, and the aerospace sector is the primary focus of the campaign.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving scheduled tasks, boot or logon autostart execution, and malicious file usage, among others. The priority technique identified is T1059.001 PowerShell, which serves as a critical chokepoint in the attack chain. To defend against this, the priority control is to Constrain PowerShell (Constrained Language Mode + AppLocker/WDAC); enable script-block and module logging; alert on encoded commands.

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted on providers such as MT Finance LLC, Your Hosting B.V., and Namecheap Inc. Additionally, abuse.ch has corroborated the presence of the DYEPACK malware family in relation to this activity. 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)

- T1053.005 Scheduled Task
- T1547 Boot or Logon Autostart Execution
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1005 Data from Local System
- T1219 Remote Access Tools
- T1036 Masquerading
- T1560 Archive Collected Data
- T1020 Automated Exfiltration
- T1059.001 PowerShell
- T1027 Obfuscated Files or Information
- T1564.003 Hidden Window
- T1059.003 Windows Command Shell
- T1070.004 File Deletion
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1059.001 PowerShell (centrality 0.3226).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6428; 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
Nomadic Octopus	0.6428
RedCurl	0.5505
Rancor	0.533
Gallmaker	0.5143
BRONZE BUTLER	0.5039

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: DYEPACK.
- 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	194[.]87[.]57[.]81	AbuseIPDB 0% (RU) · AS214822 MT Finance LLC
IP	109[.]106[.]178[.]14	AbuseIPDB 0% (NL) · AS48635 Your Hosting B.V.
IP	198[.]54[.]120[.]13	AbuseIPDB 0% (US) · AS22612 Namecheap Inc.
Domain	vniir-info[.]space	
Domain	vniir-avia[.]space	

Type	Indicator	Context
Hash	0dc0fa727f900ed5033f46f8ba6cf2d97d20ab95fd334cabc0f216da6e0622b0	DYEPACK
Hash	144a0a499e007931628c98f38929466f	DYEPACK
Hash	c7eccd855d2e97b57420afd23a4b9261f42f5b84	DYEPACK
Hash	12648cd9d425f78db2dbc6e03c14f11e6ac6aadf8b3975c23cce9519e2b58d33	
Hash	47854deb456cb08c651b7f9ae2f9d87c72d0719de6af233340632efb3c1980f4	
Hash	f57e010541fb4ccbf23aefc4a827f753a6ff3f8792d9c04c3eea83f6963c6bae	
Hash	6cc3c68c56e099792fdeadde76256d56	
Hash	7884be8a701f31421717c0835add92d5	
Hash	eabd440c996846d0992e37ab01d01208	
Hash	5d9d91cf9da3b37d8eee87d5d4dd38dbfec28358	
Hash	7d415612a00d99617bd89670e1570c145863ad08	
Hash	ee577f1880397a00480b210fcd6bc84d2330a19e	

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