

HiveForce Labs

THREAT ADVISORY



ATTACK REPORT

Zero-Day Stealth: Inside Stealth Falcon's Abuse of CVE-2025-33053

Date of Publication

June 12, 2025

Admiralty Code

A1

TA Number

TA2025183

Summary

Attack Discovered: March 2025

Targeted Region: Middle East, Africa

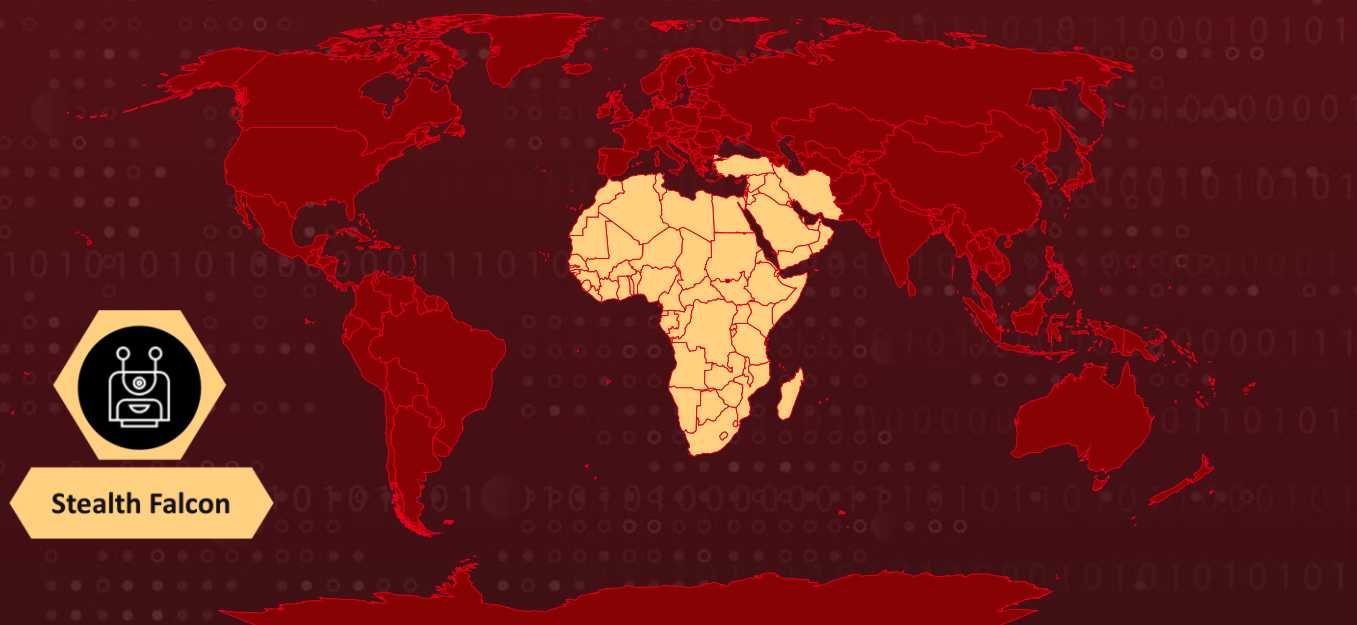
Targeted Industries: Defense and Government Organizations

Malware: Horus Agent, Horus Loader

Actor: Stealth Falcon (aka FruityArmor, Project Raven, G0038)




Attack: Stealth Falcon, a long-active cyber-espionage group, exploited a zero-day vulnerability in Windows (CVE-2025-33053) to target a Turkish defense firm using a malicious file disguised as a PDF. The attack leveraged the WebDAV protocol to stealthily execute a multi-stage infection chain that deployed a custom-built spying tool named Horus Agent. This advanced implant, designed for stealth and resilience, showcased heavy obfuscation, anti-analysis techniques, and custom payload delivery, highlighting the group's deep technical sophistication and long-term surveillance goals.

🔪 Attack Regions



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-33053	Web Distributed Authoring and Versioning (WebDAV) External Control of File Name or Path Vulnerability	Web Distributed Authoring and Versioning (WebDAV)			

Attack Details

#1

In March 2025 a sophisticated cyberattack attempt was uncovered targeting a major defense company in Turkey. The attackers exploited a previously undisclosed technique to execute files hosted on a WebDAV server, leading Microsoft to assign and patch the vulnerability as CVE-2025-33053 on June 10. This campaign was attributed to [Stealth Falcon](#), a long-active cyberespionage group linked to state-sponsored activity. Their ultimate goal is to deliver a new, custom backdoor known as Horus Agent, built atop the Mythic C2 framework and evolved from their earlier Apollo implant.

#2

The infection began with a deceptive file uploaded to VirusTotal from a machine linked to the targeted defense firm. This seemingly harmless shortcut was likely delivered through a phishing email. It disguised its payload by leveraging trusted Windows tools, the latter planted on a malicious WebDAV server instead of its legitimate location. This trick allowed the attackers to sidestep traditional detection mechanisms and initiate a multi-stage infection chain using living-off-the-land binaries (LOLBins).

#3

The attackers employed a specially crafted loader protected by Code Virtualizer a tool that transforms code into a custom instruction set, making analysis harder. This loader, although not heavily obfuscated, performed anti-analysis checks and scanned for endpoint protection tools. It decrypted a blob in memory that, instead of shellcode or a PE file, contained an unusual list of IPv6 addresses a technique dubbed "IPfuscation." These were used to mask communications and payload retrieval.

#4

At the core of this operation was the Horus Agent, a stealthy and modular implant written in C++. Though based on Mythic, it bore minimal resemblance to existing agents. It used advanced protections like custom string encryption, control flow flattening, and API hashing to resist analysis. Its configuration and command-and-control (C2) communications were concealed using RC4 encryption and HTTP-based profiles. The implant could fingerprint victims, inject shellcode into legitimate processes, and maintain a low profile until further commands were issued.

#5

Stealth Falcon's infection chain reflects a deep understanding of security products, Windows internals, and the defense industry. From earlier use of a modified Apollo agent to more recent tools like keyloggers, credential dumpers, and passive backdoors, the group continues to refine its capabilities. Notably, their credential dumper accessed Active Directory files by mounting VHDs, bypassing standard OS locks and protections a clever method to steal sensitive data without triggering alarms.

#6

This campaign shows how Stealth Falcon merges legitimate tools, open-source frameworks, and custom implants to build resilient, evasive malware ecosystems. Their strategy prioritizes stealth, persistence, and minimal exposure, ensuring only high-value targets receive full infection chains. By blending phishing, WebDAV exploitation, and advanced malware design, they continue to push the boundaries of modern cyberespionage, particularly in regions like Turkey, Qatar, Egypt, and Yemen, where strategic defense and governmental entities have been among their primary targets.

Recommendations



Apply Patch: Install the June 2025 Windows security update as soon as possible. It fixes the flaw that hackers are already using to break in.



Turn Off WebDAV if You Don't Need It: If you're not using WebDAV (a file-sharing feature), switch it off. Hackers are abusing it to sneak malware into systems.



Monitor for Unusual Activity: Keep an eye out for strange system behavior, like built-in tools running from weird locations. It could be a sign of hidden malware.



Strengthen Email Filters: Block risky attachments like .lnk or .hta files and be cautious of Dropbox links. These are common tricks used in phishing emails.



Strengthen Endpoint Defense: Implement advanced Endpoint Detection and Response (EDR) solutions to effectively detect, analyze, and mitigate in-memory malware activity, ensuring comprehensive protection against sophisticated threats.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence
<u>TA0005</u> Defense Evasion	<u>TA0006</u> Credential Access	<u>TA0007</u> Discovery	<u>TA0011</u> Command and Control
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1566</u> Phishing	<u>T1566.001</u> Spearphishing Attachment
<u>T1574</u> Hijack Execution Flow	<u>T1574.001</u> DLL	<u>T1027</u> Obfuscated Files or Information	<u>T1140</u> Deobfuscate/Decode Files or Information
<u>T1003</u> OS Credential Dumping	<u>T1105</u> Ingress Tool Transfer	<u>T1056</u> Input Capture	<u>T1056.001</u> Keylogging
<u>T1095</u> Non-Application Layer Protocol	<u>T1059</u> Command and Scripting Interpreter	<u>T1218</u> System Binary Proxy Execution	<u>T1016</u> System Network Configuration Discovery
<u>T1106</u> Native API			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	ba5beb189d6e1811605b0a4986b232108d6193dcf09e5b2a603ea4448e6f263c, e0a44274d5eb01a0379894bb59b166c1482a23fede1f0ee05e8bf47e4e2fcc6, da3bb6e38b3f4d83e69d31783f00c10ce062abd008e81e983a9bd4317a9482aa, ddce79afe9f67b78e83f6e530c3e03265533eb3f4530e7c89fdc357f7093a80b, 1d95a44f341435da50878eea1ec0a1aab6ae0ee91644c497378266290a6ef1d8, 700b422556f070325b327325e31ddf597f98cc319f29ef8638c7b0508c632cee,

TYPE	VALUE
SHA256	aa612f53e03539cdc8f8a94deee7bf31f0ac10734bb9301f4506b9113c691c97, 66a893728a0ac1a7fae39ee134ad4182d674e719219fbf5d9b7cd4fd4f07f535, cd6335101e0187c33a78a316885a2cbf4cbbd2a72daf64a086edb4a2615749fb, 257c63a9e21b829bb4b9f8b0e352379444b0e573176530107a3e6c279d1919da, 5671b3a89c0e88a9bfb0bd5bc434fa5245578becfdeb284f4796f65eecbd6f15, 3259ecfb96d3d7e2d1a782b01073e02b3488a3922fd2fd35c20eeb5f44b292ec, 8065c85e387654cb79a12405ff0f99fd4ddd5a5d3b9876986b82822bd10c716f, 0598e1af6466b0813030d44fa64616eea7f83957d70f2f48376202c3179bd6b1, f27020cd88b045630f6d2dec6d5823aa08aa66949b9ccd20f6e924c7992fea7, 092c344330bd5cba71377dead11946f7277f2dd4af57f5b636b70b343bc7ebe0, dc7cb53c5dc2e756822328a7144c29318cb871890727eff9c8da64a01e8e782d, db7364296cc8f78981797ffb2af7063bba97e2f6631c29215d59f4979f8b4fce, 4e045c83cf429210e71e324adccad8818540b9805a44c8d79a8c16c3d5f6fbb6, 62797e28a334e392cb56fcc26dd07f04ac031110f0e9ed8489ec0825beea75eb, dec6dda0559e381c23f1dfbe92fa4705c8455430f8278c78c170a7533b703296, 32f2773ceb6503f8a1c3e456d34ceda5c188974a115e5225a1315e7ec3f8eb5e, 50a2b6c1b0a0d308e8016aece9629c1bf6ca4ecc6f4cef34c904e9c3e82355fb, 9ed8f51548a004ac61b7176df12a0064dc3096088cbf3c644a9abdb5c92936f7, 9a82e21c2463d6c23a48409a862e668ed9c205468d216d2280f7debe1ab1ddd8, 46c95af6fea41b55fa0ab919ec81d38a584e32a519f85812fe79a5379457f111, c5b00e8312e801dc35652c631a14270ed4eec8f6d90d08cdde3c6e7fd1ec24b6, 3b83250383c2a892e0ca86e54fcc6aca9960fc4b425ab9853611ff3e5aa2f9c6, 8291b886cce1f0474db5b3dc269adf31d1659b7d949f62ea23608409d14b9ceb



TYPE	VALUE
Domains	roundedbullets[.]com, summerartcamp[.]net, downloadessays[.]net, joinushealth[.]com, healthherofit[.]com, worryfreetransport[.]com, radiotimesignal[.]com, fastfilebackup[.]com, cyclingonlineshop[.]com, luxuryfitnesslabs[.]com, purvoyage[.]com

Patch Link

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053>

References

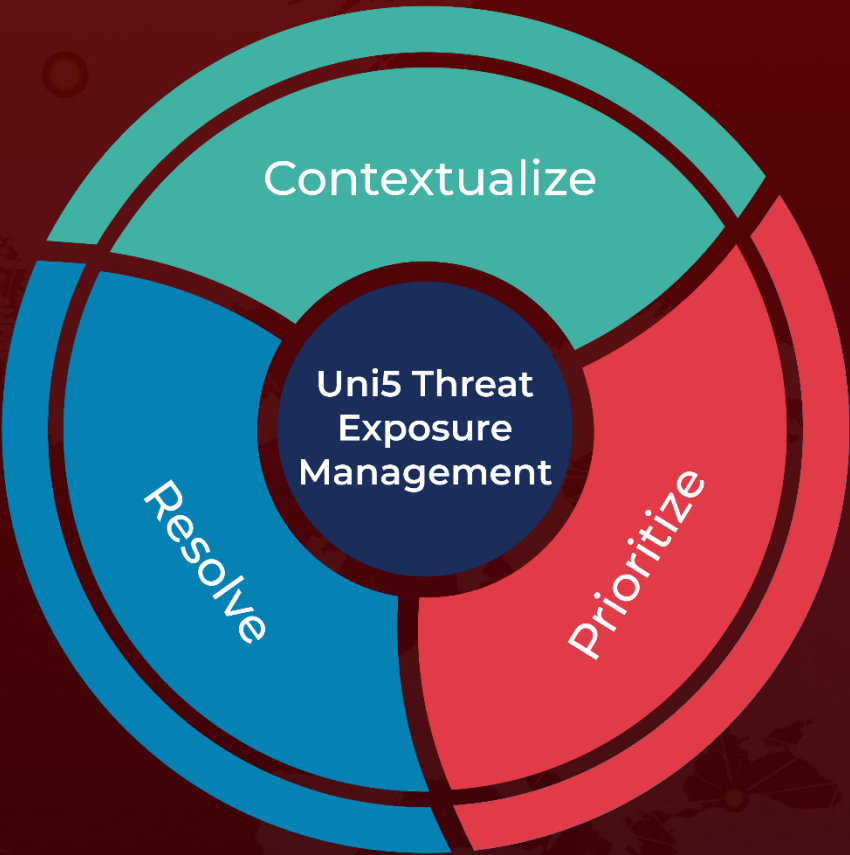
<https://research.checkpoint.com/2025/stealth-falcon-zero-day/#single-post>

<https://hivepro.com/threat-advisory/deadglyph-malware-emerges-as-a-game-changer-for-stealth-falcon/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON
June 12, 2025 • 6:45 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com