Hive Pro®

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## ACTOR REPORT

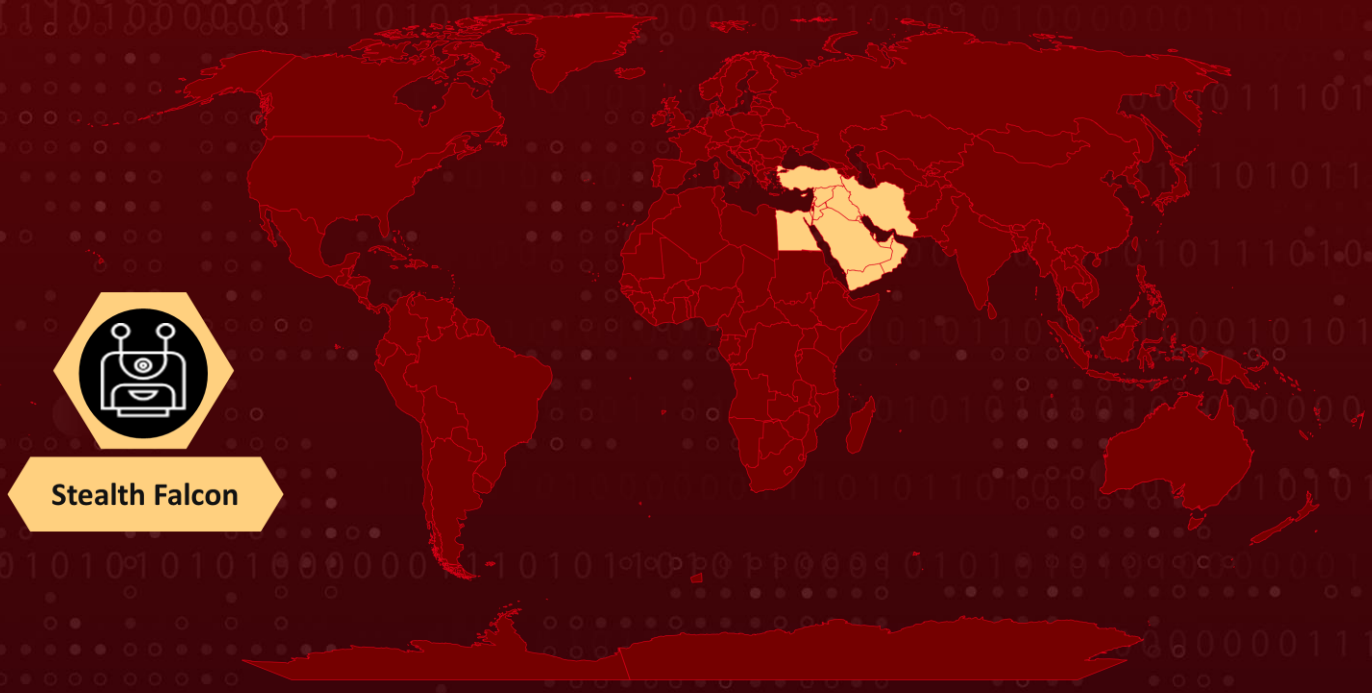
# Deadglyph Malware Emerges as a Game Changer for Stealth Falcon


| Date of Publication | Admiralty code | TA Number |
| --- | --- | --- |
| September 26, 2023 | A1 | TA2023388 |

# Summary

**First Appearance:** 2012
**Actor Name:** Stealth Falcon (aka FruityArmor, Project Raven)
**Target Industries:** Media, Civil Society, Human Rights, Government, Politics, and Nonprofits
**Target Region:** Middle East
**Malware:** Deadglyph Backdoor

## Actor Map



# Actor Details

**#1** Starting in 2012, the cyber espionage collective recognized as Stealth Falcon, alternatively identified as FruityArmor and Project Raven, embarked on its covert operations. The debut exposure of Stealth Falcon transpired in 2016, drawing a connection between the group and a series of precisely targeted spyware attacks within the Middle East.

**#2** These operations were primarily aimed at journalists, activists, and dissidents in the United Arab Emirates, executed through meticulously crafted spear-phishing schemes. In their most recent operation, Stealth Falcon deployed a cutting-edge and intricate backdoor malware known as "Deadglyph" to breach a Middle Eastern government organization that had already been compromised for espionage.

**#3** The architecture of Deadglyph stands out for its uniqueness, featuring the cooperation of two distinct components: one as a native x64 binary, and the other as a .NET assembly. This combination departs from the usual approach, as malware typically uses a single programming language for all its components. The threat actors also coupled a homoglyph attack in the VERSIONINFO resource using distinct Greek and Cyrillic Unicode characters to mimic Microsoft's information and appear as a legitimate Windows file.

**#4** This unconventional choice implies the potential for separate development of these two components, while also leveraging the distinctive features of their respective programming languages. The exact method used to deliver this implant remains undisclosed for now.

**#5** However, the initial component responsible for triggering its execution is a shellcode loader, which extracts and deploys shellcode from the Windows Registry. Following this, the loader initiates the execution of Deadglyph's native x64 module, referred to as the "Executor."

**#6** The Executor then proceeds to load a .NET component known as the "Orchestrator," which, in turn, establishes communication with the command-and-control (C2) server, ready to receive further instructions. If, for any reason, the backdoor fails to establish communication with the C2 server within a predetermined timeframe, it activates a self-removal mechanism.

# Actor Group

| NAME | ORIGIN | TARGET REGIONS | TARGET INDUSTRIES |
|---|---|---|---|
| Stealth Falcon (aka FruityArmor, Project Raven) | UAE<br>**MOTIVE**<br>Information theft and espionage | Middle East | Media, Civil Society, Human Rights, Government, Politics, and Nonprofits |

# Recommendations

**Registry Monitoring:** Keep a close eye on the Windows Registry for unusual activities, especially the extraction of shellcode. Implement monitoring and alerting systems to detect and respond to such activities promptly.

**Network Segmentation:** Consider segmenting your network to limit lateral movement for attackers. This can help contain any breach and minimize the potential damage.

**Application Whitelisting:** Implement application whitelisting to only allow approved and trusted applications to run on critical systems. This can prevent the execution of unauthorized or malicious code.

**Zero Trust Architecture:** Consider adopting a Zero Trust security model, where trust is never assumed, and strict access controls are enforced for every user and device attempting to connect to the network.

**Harden Server Configurations:** Apply server hardening techniques to reduce the attack surface by disabling unnecessary services, closing unused ports, and following industry best practices for server security.

**Implement DNS Filtering:** Employ DNS filtering services to block access to known malicious domains and prevent malware communication with command-and-control servers.

# Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0042** Resource Development | **TA0002** Execution | **TA0003** Persistence | **TA0005** Defense Evasion |
| **TA0007** Discovery | **TA0009** Collection | **TA0011** Command and Control | **TA0010** Exfiltration |
| **T1583.001** Domains | **T1583.003** Virtual Private Server | **T1587.001** Malware | **T1588.003** Code Signing Certificates |
| **T1047** Windows Management Instrumentation | **T1059.003** Windows Command Shell | **T1106** Native API | **T1204.002** Malicious File |
| **T1546.003** Windows Management Instrumentation Event Subscription | **T1027** Obfuscated Files or Information | **T1070.004** File Deletion | **T1112** Modify Registry |
| **T1134** Access Token Manipulation | **T1140** Deobfuscate/Decode Files or Information | **T1218.011** Rundll32 | **T1480.001** Environmental Keying |
| **T1562.001** Disable or Modify Tools | **T1620** Reflective Code Loading | **T1007** System Service Discovery | **T1012** Query Registry |
| **T1016** System Network Configuration Discovery | **T1033** System Owner/User Discovery | **T1057** Process Discovery | **T1082** System Information Discovery |
| **T1518.001** Security Software Discovery | **T1005** Data from Local System | **T1071.001** Web Protocols | **T1090** Proxy |
| **T1573.001** Symmetric Cryptography | **T1041** Exfiltration Over C2 Channel | | |

# Indicator of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA1 | c40f1f46d230a85f702daa38cfa18d60481ea6c2, 740d308565e215eb9b235cc5b720142428f540db, 1805568d8362a379af09fd70d3406c6b654f189f, 9cb373b2643c2b7f93862d2682a0d2150c7aec7e, f47cb40f6c2b303308d9d705f8cad707b9c39fa5, 3d4d9c9f2a5aceff9e45538f5ebe723acaf83e32, 3d2accea98dbdf95f0543b7c1e8a055020e74960, 4e3018e4fd27587bd1c566930ae24442769d16f0, 7f728d490ed6ea64a7644049914a7f2a0e563969, 43ed9a3ad74ed7ab74c345a876b6be19039d4c8c, 3a215912708eab6f56af953d748fbfc38e3bb468, 42fb165bc9cf614996027a9fcb261d65fd513527, e204cdcf96d9f94f9c19dbe385e635d00caaf49d, abd2db754795272c21407efd5080c8a705a7d151 |
| IPv4 | 185.25.50[.]60, 135.125.78[.]187, 45.14.227[.]55 |
| Domains | chessandlinkss[.]com, easymathpath[.]com, joinushealth[.]com |

# References

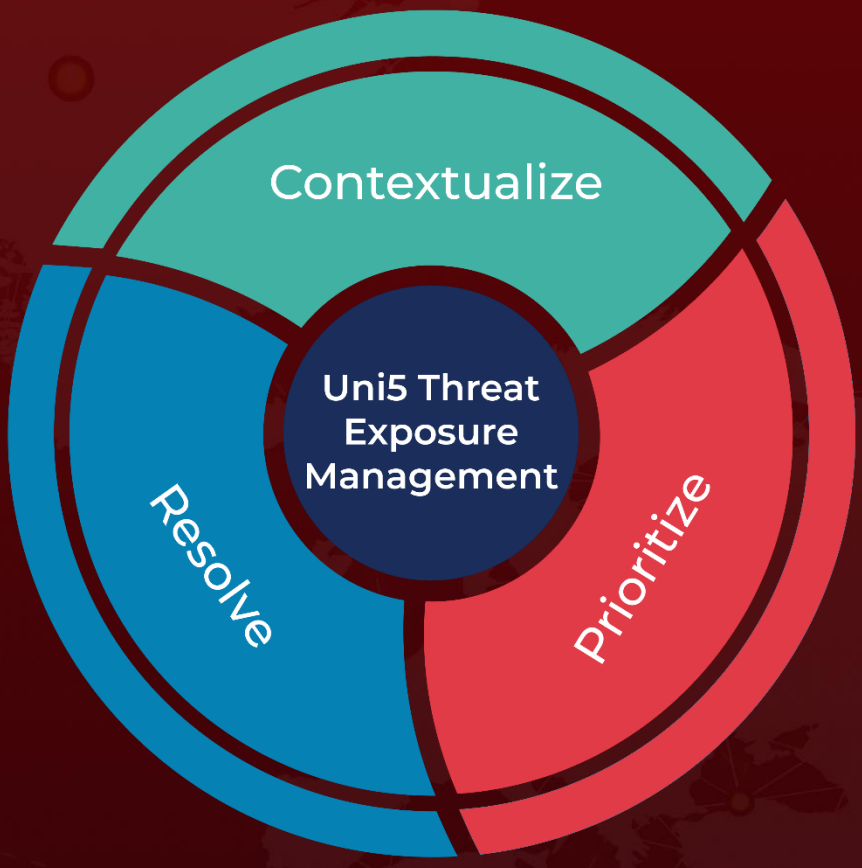

https://www.welivesecurity.com/en/eset-research/stealth-falcon-preying-middle-eastern-skies-deadglyph/

https://attack.mitre.org/groups/G0038/

# 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

**September 26, 2023 . 10:00 PM**



More at www.hivepro.com