Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

OilRig Group Unleashes Three New Malware Strains

Date of Publication	Admiralty Code	TA Number
December 19, 2023	A1	TA2023511

Summary

First appeared: 2022
Targeted Industry: Healthcare sector, Manufacturing company, Local governmental organization
Attack Region: Israel
Malware: ODAgent, OilCheck, OilBooster, SC5k downloader
Actor: OilRig (aka APT 34, Helix Kitten, Twisted Kitten, Crambus, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13, DEV-0861, EUROPIUM, Hazel Sandstorm, Scarred Manticore)
Attack: The Iranian state-sponsored threat actor, commonly referred to as OilRig, implemented three distinct downloader malware variants throughout the year 2022. The primary objective was to sustain persistent access to targeted organizations located in Israel. OilRig demonstrated active development and deployment of a series of downloaders sharing a similar logic. The three new downloaders introduced were ODAgent, OilCheck, and OilBooster, in addition to updated versions of the SC5k downloader.

Attack Regions

Attack Details

#1 Throughout 2022, the Iranian state-sponsored threat actor known as OilRig introduced three new downloader malware strains—ODAgent, OilCheck, and OilBooster—alongside updated versions of the SC5k downloader. The primary objective was to maintain persistent access to organizations in Israel targeted by OilRig. Active since at least 2014, OilRig primarily focuses on cyberespionage, targeting Middle Eastern governments and businesses across various sectors.

#2 OilRig strategically leverages cloud service providers such as Microsoft Graph OneDrive, Microsoft Graph Outlook, and Microsoft Office EWS API for both command-and-control communication and data exfiltration. This approach enables them to conceal their activities within legitimate network traffic, blending in with authentic communications.

#3 The SC5k downloader, a C#/.NET application designed for cloud communication, utilizes the Microsoft Office EWS API to engage with a shared Exchange mail account. Its core functions involve downloading payloads and commands, along with uploading data, using email drafts and attachments as the primary means for C&C traffic. Subsequent versions, like SC5k v3, increase the complexity of the C&C protocol, while SC5k v2 introduces capabilities for evading detection.

#4 OilCheck, C#/.NET downloader, adopts a unique C&C communication method. It utilizes draft messages from a shared email account and leverages the REST-based Microsoft Graph API to access a shared Microsoft Office 365 Outlook email account. On the other hand, OilBooster, coded in Microsoft Visual C/C++, features statically linked OpenSSL and Boost libraries. This downloader uses the Microsoft Graph API to establish connections.

#5 ODAgent, a C#/.NET application, establishes a connection, retrieves payloads and backdoor commands, and parses metadata for each file. ODAgent uses the mimeType key to differentiate between backdoor commands and encrypted payloads. After locally processing a file, ODAgent deletes the original file from the remote OneDrive directory, facilitating efficient data management and manipulation within the attacker-controlled OneDrive account.

#6 These downloaders leverage cloud service accounts controlled by the attackers signaling OilRig's strategic shift away from HTTP/DNS-based protocols towards legitimate cloud service providers to enhance the concealment of their malicious activities. While not highly sophisticated, the ongoing development and testing efforts by OilRig enhance the significance of these threats.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise the systems.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0005** Defense Evasion	**TA0007** Discovery
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**T1583** Acquire Infrastructure
T1583.001 Domains	**T1583.004** Server	**T1583.006** Web Services	**T1587** Develop Capabilities
T1587.001 Malware	**T1585** Establish Accounts	**T1585.003** Cloud Accounts	**T1585.002** Email Accounts
T1608 Stage Capabilities	**T1059** Command and Scripting Interpreter	**T1059.003** Windows Command Shell	**T1106** Native API
T1140 Deobfuscate/Decode Files or Information	**T1480** Execution Guardrails	**T1564** Hide Artifacts	**T1564.003** Hidden Window
T1070 Indicator Removal	**T1070.004** File Deletion	**T1202** Indirect Command Execution	**T1036** Masquerading

T1036.005 Match Legitimate Name or Location	**T1027** Obfuscated Files or Information	**T1082** System Information Discovery	**T1033** System Owner/User Discovery
T1560 Archive Collected Data	**T1560.003** Archive via Custom Method	**T1074** Data Staged	**T1074.001** Local Data Staging
T1132 Data Encoding	**T1132.001** Standard Encoding	**T1573** Encrypted Channel	**T1573.001** Symmetric Cryptography
T1008 Fallback Channels	**T1105** Ingress Tool Transfer	**T1102** Web Service	**T1102.002** Bidirectional Communication
T1020 Automated Exfiltration	**T1041** Exfiltration Over C2 Channel	**T1567** Exfiltration Over Web Service	**T1567.002** Exfiltration to Cloud Storage

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	0F164894DC7D8256B66D0EBAA7AFEDCF5462F881, 2236D4DCF68C65A822FF0A2AD48D4DF99761AD07, 35E0E78EC35B68D3EE1805EECEEA352C5FE62EB6, 51B6EC5DE852025F63740826B8EDF1C8D22F9261, 6001A008A3D3A0C672E80960387F4B10C0A7BD9B, 7AD4DCDA1C65ACCC9EF1E168162DE7559D2FDF60, BA439D2FC3298675F197C8B17B79F34485271498, BE9B6ACA8A175DF61F2C75932E029F19789FD7E3, C04F874430C261AABD413F27953D30303C382953, C225E0B256EDB9A2EA919BACC62F29319DE6CB11, E78830384FF14A58DF36303602BC9A2C0334A2A4, EA8C3E9F418DCF92412EB01FCDCDC81FDD591BF1, 1B2FEDD5F2A37A0152231AE4099A13C8D4B73C9E, 3BF19AE7FB24FCE2509623E7E0D03B5A872456D4, AEF3140CD0EE6F49BFCC41F086B7051908B91BDD, A56622A6EF926568D0BDD56FEDBFF14BD218AD37, AAE958960657C52B848A7377B170886A34F4AE99, 8D84D32DF5768B0D4D2AB8B1327C43F17F182001, DDF0B7B509B240AAB6D4AB096284A21D9A3CB910, 7E498B3366F54E936CB0AF767BFC3D1F92D80687, A97F4B4519947785F66285B546E13E52661A6E6F

TYPE	VALUE
IP	188.114.96[.]2
Domain	host1[.]com

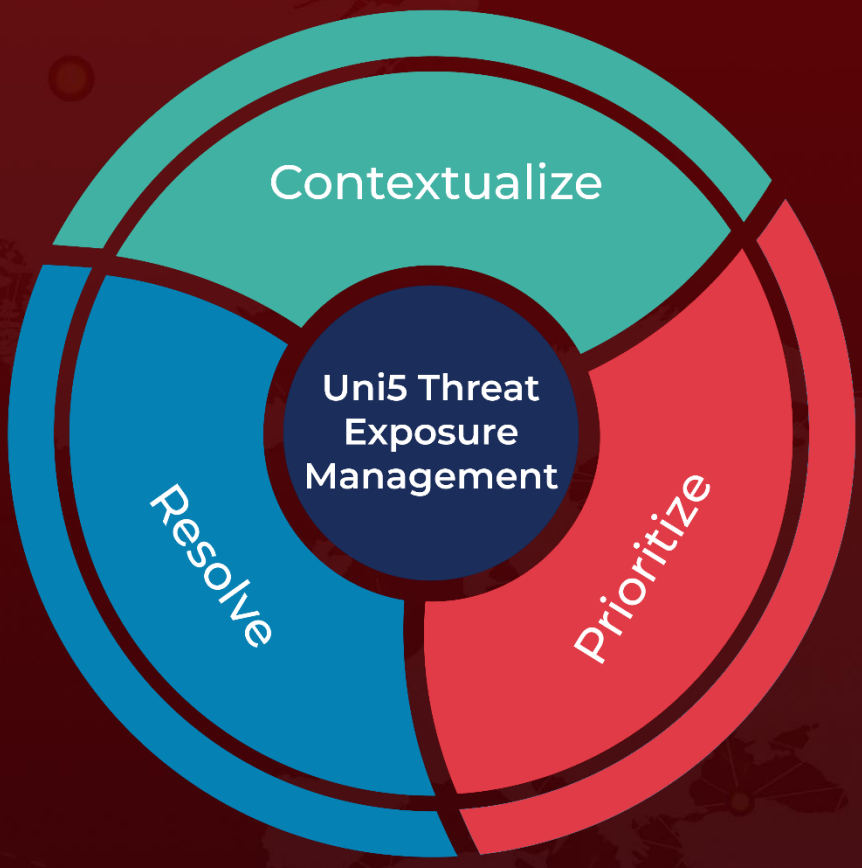
References

https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/

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

December 19, 2023 . 4:10 AM

More at www.hivepro.com