# Iranian State-Sponsored OilRig Group Deploys 3 New Malware Downloaders

Date: 10th May 2024 | Severity: Medium

## Summary

The Iranian state-sponsored threat actor known as OilRig deployed three different downloader malware throughout 2022 to maintain persistent access to victim organizations located in Israel.

The three new downloaders have been named ODAgent, OilCheck, and OilBooster by Slovak cybersecurity company ESET. The attacks also involved the use of an updated version of a known OilRig downloader dubbed SampleCheck5000 (or SC5k).

## Attack Vectors

- These lightweight downloaders [...] are notable for using one of several legitimate cloud service APIs for [command-and-control] communication and data exfiltration: the Microsoft Graph OneDrive or Outlook APIs, and the Microsoft Office Exchange Web Services (EWS) API, security researchers Zuzana Hromcová and Adam Burgher said in a report shared with The Hacker News.
- By using well-known cloud service providers for command-and-control communication, the goal is to blend with authentic network traffic and cover up the group's attack infrastructure.
- The exact initial access vector used to compromise the targets is currently unclear and it's not known if the attackers managed to retain their foothold in the networks so as to deploy these downloaders at various points of time in 2022.
- OilRig, also known as APT34, Crambus, Cobalt Gypsy, Hazel Sandstorm (formerly EUROPIUM), and Helix Kitten, is an Iranian cyber espionage group that's known to be active since at least 2014, using a wide range of malware at its disposal to target entities in the Middle East.
- ODAgent, first detected in February 2022, is a C#/.NET downloader that utilizes Microsoft OneDrive API for command-and-control (C2) communications, allowing the threat actor to download and execute payloads, and exfiltrate staged files.
- SampleCheck5000, on the other hand, is designed to interact with a shared Microsoft Exchange mail account to download and execute additional OilRig tools using the Office Exchange Web Services (EWS) API.
- OilBooster, in the same way as ODAgent, uses Microsoft OneDrive API for C2, whereas OilCheck adopts the same technique as SampleCheck5000 to extract commands embedded in draft messages. But instead of using the EWS API, it leverages Microsoft Graph API for network communications.

- OilBooster is also similar to OilCheck in that it employs the Microsoft Graph API to connect to a Microsoft Office 365 account. What's different this time around is that the API is used to interact with an actor-controlled OneDrive account as opposed to an Outlook account in order to fetch commands and payloads from victim-specific folders.
- In all cases, the downloaders use a shared (email or cloud storage) OilRig-operated account to exchange messages with the OilRig operators; the same account is typically shared by multiple victims, the researchers explained. The downloaders access this account to download commands and additional payloads staged by the operators, and to upload command output and staged files.

# Indicator of compromise

| INDICATOR TYPE | INDICATORS |
|---|---|
| File Hash | • 26884f872f4fae13da21fa2a24c24e963ee1eb66da47e270246d6d9dc7204c2b<br>• 82A0F2B93C5BCCF3EF920BAE425DD768371248CDA9948D5A8E70F3C34E9F7CCA<br>• C744DA99FE19917E09CD1ECC48B563F9525DAD3916E1902F61B79BDA35298D87<br>• E0872958B8D3824089E5E1CFAB03D9D98D22B9BCB294463818D721380075A52D |
| Domains | • asiaworldremit[.]com<br>• joexpediagroup[.]com<br>• uber-asia[.]com |

# Recommendation

- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Never trust or open links and attachments received from unknown sources/senders.
- Passwords – Ensure that general security policies are employed including implementing strong passwords, correct configurations, and proper administration security policies.
- Admin Access – Limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.
- Patch and upgrade any platforms and software timely and make it into a standard security policy. Prioritize patching known exploited vulnerabilities and zero-days.
- Enable antivirus and anti-malware software and update signature definitions on time. Using multi-layered protection is necessary to secure vulnerable assets.

**NOTE:** The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

# Reference Links

- https://thehackernews.com/2023/09/iranian-apt-group-oilrig-using-new.html\
- https://cybermaterial.com/iran-oilrig-groups-new-malware/