Hive Pro

THREAT ADVISORY

OilRig is back with another Phishing Email attack, delivering the Saitama Backdoor	TA2022104
Threat Level AMBER	**Publish Date –** May 17, 2022

An Iranian cyber espionage gang known as **OilRig** has began delivering malicious email to a Jordanian government employee at the foreign ministry. The email includes a malicious Excel sheet that installs the **Saitama** backdoor. Since at least 2014, the Iranian threat group has targeted Middle Eastern nations and victims across the world. The firm is noted for concentrating on the financial, governmental, energy, chemical, and telecommunications industries.

Threat actors send a malicious email, with the subject "Confirmation Receive Document" and an Excel file named "Confirmation Receive Document.xls," sent to the victim via a Microsoft Outlook account. The excel sheet also delivers a payload with a small backdoor written in .Net known as Saitama Backdoor. The DNS protocol is used by the Saitama backdoor for command-and-control connections. In addition, the actor makes clever use of compression and extended random sleep durations. They used these techniques to hide harmful traffic among legal traffic.

The MITRE ATT&CK TTPs commonly used by **OilRig** are:

TA0001: Initial Access
TA0002: Exécution
TA0005: Defense Evasion
TA0003: Persistence
TA0011: Command and Control
T1059.001: PowerShell
T1059.003: Windows Command Shell
T1053.005: Scheduled Task
T1204.002: Malicious File
T1047: Windows Management Instrumentation
T1480: Execution Guardrails
T1087.001: Local Account
T1083: File and Directory Discovery
T1049: System Network Connections Discovery
T1071.004: DNS
T1132.002: Non-Standard Encoding
T1568.002: Domain Generation Algorithms
T1041: Exfiltration Over C2 Channel

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
OilRig (APT 34, Helix Kitten, Twisted Kitten , Crambus, Chrysene , Cobalt Gypsy , TA452 , IRN2, ATK 40, ITG13)	Iran	Azerbaijan, Iraq, Israel, Jordan, Kuwait, Lebanon, Mauritius, Pakistan, Qatar, Saudi Arabia, Turkey, UAE, UK, USA.	Aviation, Chemical, Education, Energy, Financial, Government, High-Tech, Hospitality, Oil and gas, Telecommunications.	Information theft and espionage

Indicators of Compromise (IoCs)

Type	Value
SHA256	82A0F2B93C5BCCF3EF920BAE425DD768371248CDA9948D5A8E70F3C34E9F7CCA, 7EBBEB2A25DA1B09A98E1A373C78486ED2C5A7F2A16EEC63E576C99EFE0C7A49, C744DA99FE19917E09CD1ECC48B563F9525DAD3916E1902F61B79BDA35298D87, E0872958B8D3824089E5E1CFAB03D9D98D22B9BCB294463818D721380075A52D
URL	joexpediagroup[.]com, asiaworldremit[.]com, uber-asia[.]com

References

https://www.fortinet.com/blog/threat-research/please-confirm-you-received-our-apt