Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

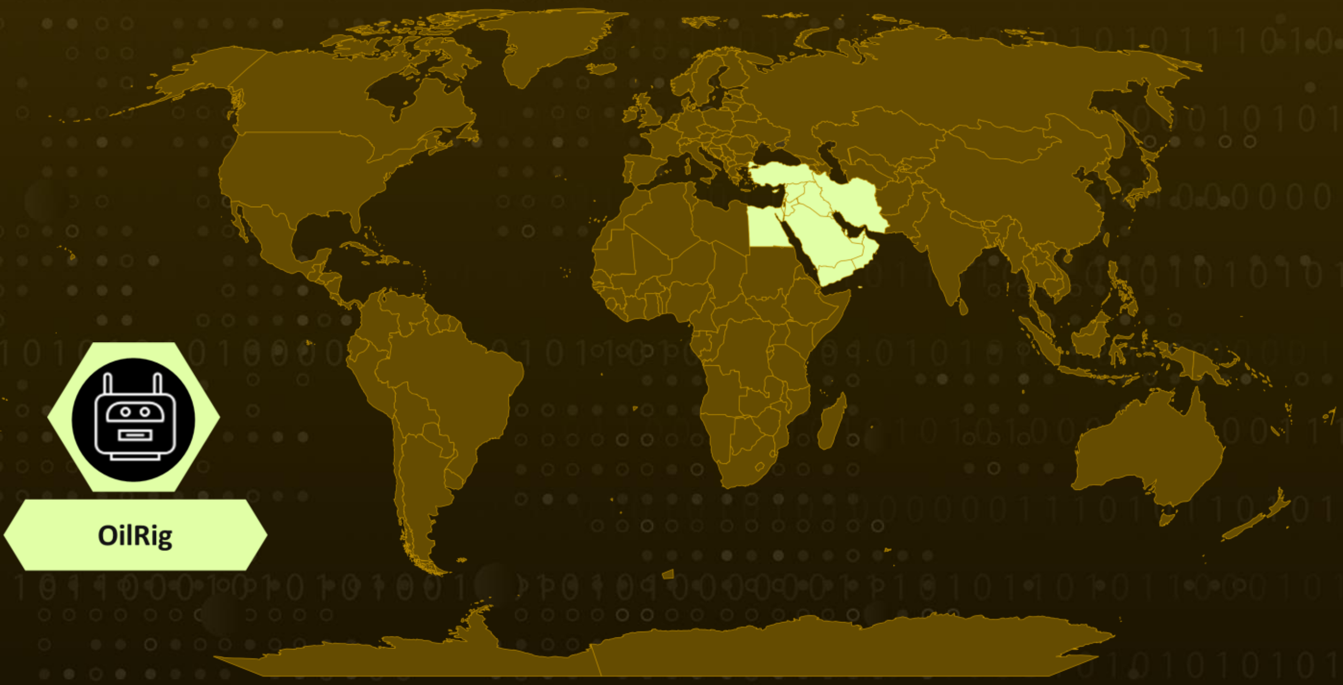
Prolonged Pursuit of OilRig APT Targeting Middle East Government

Date of Publication	Admiralty Code	TA Number
October 20, 2023	A1	TA2023428

Summary

Attack Began: February 2023
Actor Name: OilRig (aka Crambus, Helix Kitten, APT 34, Twisted Kitten, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13, EUROPIUM, Hazel Sandstorm)
Malware: PowerExchange, Clipog
Attack Region: Middle East
Targeted Industry: Government
Attack: The Iran-affiliated threat actor known as OilRig orchestrated a sophisticated eight-month campaign directed at the Middle East government, during which the attackers managed to steal sensitive files and passwords.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

An extensive eight-month campaign between February and September 2023 was orchestrated by a threat actor known as OilRig, which has affiliations with Iran and is also identified as APT34 and Crambus. The campaign was directed at the Middle East government. During this operation, the attackers not only stole sensitive files and passwords but, in one instance, also discreetly installed access points and keyloggers on numerous systems.

#2

During this recent attack, OilRig introduced three previously undisclosed strains of malware, along with the PowerExchange backdoor, and an array of legitimate tools and living-off-the-land techniques, such as Mimikatz and Plink. While the specific method of initial access remains undisclosed, there is suspicion that it involved phishing emails. This malicious activity endured on the government network until September 9, 2023.

#3

PowerExchange, a PowerShell-based malware, has the capability to access an Exchange Server using hardcoded credentials and monitor emails sent by the attackers. It utilizes the Exchange Server as a command and control (C&C) center. This malware establishes an Exchange rule to automatically filter these messages and move them to the Deleted Items folder.

#4

Additionally, Clipog is an information-stealing malware with the ability to copy clipboard data, capture keystrokes, and record the processes of the entered keystrokes. OilRig employs a combination of tools, scripts, and methodologies to extend their influence and sustain a presence across a multitude of systems within a compromised network.

#5

Their activities involve reconnaissance using netstat commands, lateral movement through Plink for Remote Desktop Protocol (RDP), and the exfiltration or harvesting of data using tools like Mimikatz and Infostealer.Clipog, which highlights the extensive capabilities of this threat group. OilRig is a well-established and experienced espionage organization with comprehensive expertise in conducting prolonged campaigns targeting entities of interest to Iran.

Recommendations

Enhanced Email Security: Given the suspicion that email phishing was involved in the initial access, organizations should reinforce their email security systems to detect and prevent phishing attempts. This includes email filtering, employee training, and multi-factor authentication.

Network Monitoring and Intrusion Detection: Implement robust network monitoring and intrusion detection systems to swiftly identify and respond to suspicious activities. Early detection is crucial in mitigating potential threats.

Access Control and Privilege Management: Employ stringent access control measures to restrict user permissions to only what is necessary for their roles. This reduces the potential damage that malicious actors can cause if they gain access to a system.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1566 Phishing	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1003 OS Credential Dumping	T1016 System Network Configuration Discovery	T1021.001 Remote Desktop Protocol
T1005 Data from Local System	T1041 Exfiltration Over C2 Channel	T1105 Ingress Tool Transfer	T1056.001 Keylogging
T1113 Screen Capture			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4d04ad9d3c3abeb61668e52a52a37a46c1a60bc8f29f12b76ff9f580caeefba8, 41672b08e6e49231aedf58123a46ed7334cafaad054f2fd5b1e0c1d5519fd532, 497e1c76ed43bcf334557c64e1a9213976cd7df159d695dcc19c1ca3d421b9bc, 75878356f2e131cefb8aeb07e777fcc110475f8c92417fcade97e207a94ac372, d884b3178fc97d1077a13d47aadf63081559817f499163c2dc29f6828ee08cae, a1a633c752be619d5984d02d4724d9984463aa1de0ea1375efda29cadb73355a, 22df38f5441dec57e7d7c2e1a38901514d3f55203b2890dc38d2942f1e4bc100, 159b07668073e6cd656ad7e3822db997d5a8389a28c439757eb60ba68eaff70f, 6964f4c6fbfb77d50356c2ee944f7ec6848d93f05a35da6c1acb714468a30147, 661c9535d9e08a3f5e8ade7c31d5017519af2101786de046a4686bf8a5a911ff, db1cbe1d85a112caf035fd5d4babfb59b2ca93411e864066e60a61ec8fe27368, 497978a120f1118d293906524262da64b15545ee38dc0f6c10dbff3bd9c0bac2, db1cbe1d85a112caf035fd5d4babfb59b2ca93411e864066e60a61ec8fe27368, 6b9f60dc91fbee3aecb4a875e24af38c97d3011fb23ace6f34283a73349c4681, 497978a120f1118d293906524262da64b15545ee38dc0f6c10dbff3bd9c0bac2, be6d631fb2ff8abe22c5d48035534d0dede4abfd8c37b1d6cbf61b005d1959c1, 22df38f5441dec57e7d7c2e1a38901514d3f55203b2890dc38d2942f1e4bc100, 661c9535d9e08a3f5e8ade7c31d5017519af2101786de046a4686bf8a5a911ff, 159b07668073e6cd656ad7e3822db997d5a8389a28c439757eb60ba68eaff70f,

TYPE	VALUE
SHA256	6bad09944b3340947d2b39640b0e04c7b697a9ce70c7e47bc2276ed825e74a2a, ba620b91bef388239f3078ecdcc9398318fd8465288f74b4110b2a463499ba08, d0bfdb5f0de097e4460c13bc333755958fb30d4cb22e5f4475731ad1bdd579ec, 5a803bfe951fbde6d6b23401c4fd1267b03f09d3907ef83df6cc25373c11a11a, 1698f9797f059c4b30f636d16528ed3dd2b4f8290e67eb03e26181e91a3d7c3b, 23db83aa81de19443cafe14c9c0982c511a635a731d6df56a290701c83dae9c7, 41ff7571d291c421049bfbd8d6d3c51b0a380db3b604cef294c1edfd465978d9, c488127b3384322f636b2a213f6f7b5fdaa6545a27d550995dbf3f32e22424bf, 6964f4c6fbfb77d50356c2ee944f7ec6848d93f05a35da6c1acb714468a30147, 927327bdce2f577b1ee19aa3ef72c06f7d6c2ecd5f08acc986052452a807caf2, a6365e7a733cfe3fa5315d5f9624f56707525bbf559d97c66dbe821fae83c9e9, c3ac52c9572f028d084f68f6877bf789204a6a0495962a12ee2402f66394a918, 7e107fdd6ea33ddc75c1b75fdf7a99d66e4739b4be232ff5574bf0e116bc6c05
IPv4	78.47.218[.]106, 192.121.22[.].46, 151.236.19[.]91, 91.132.92[.]90

References

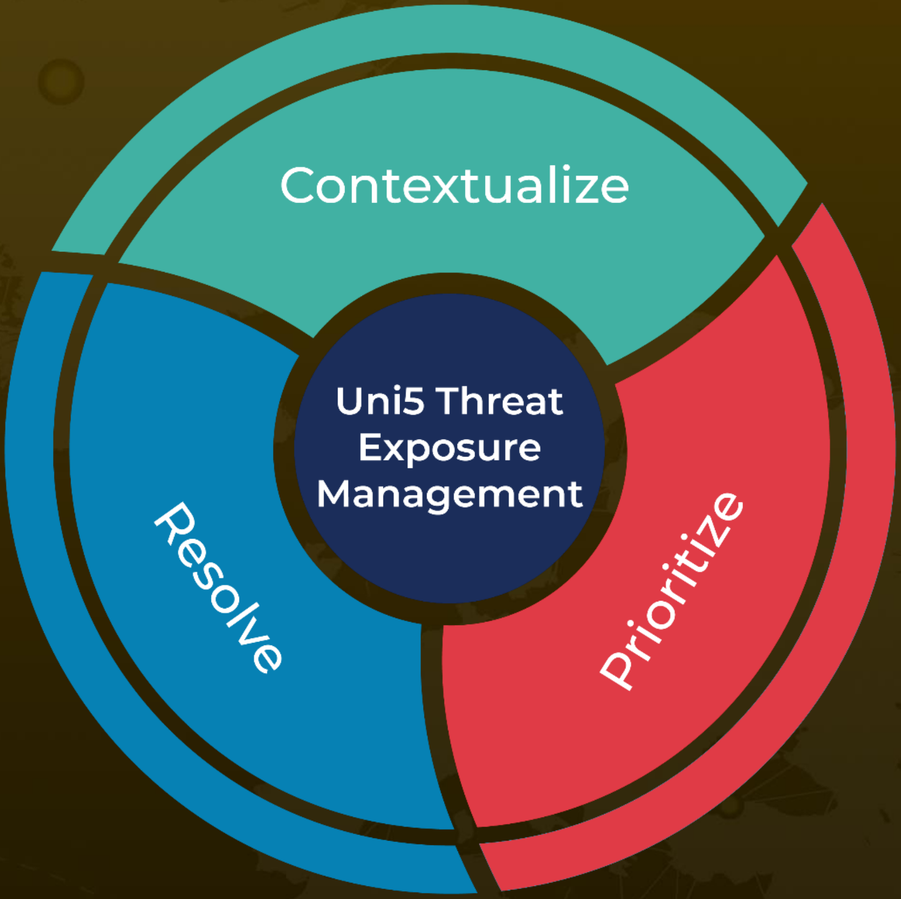
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/crambus-middle-east-government

https://www.hivepro.com/iranian-oilrig-group-strikes-with-autohotkey-keylogger-and-malicious-macro/

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

October 20, 2023 • 5:30 AM

More at www.hivepro.com