Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

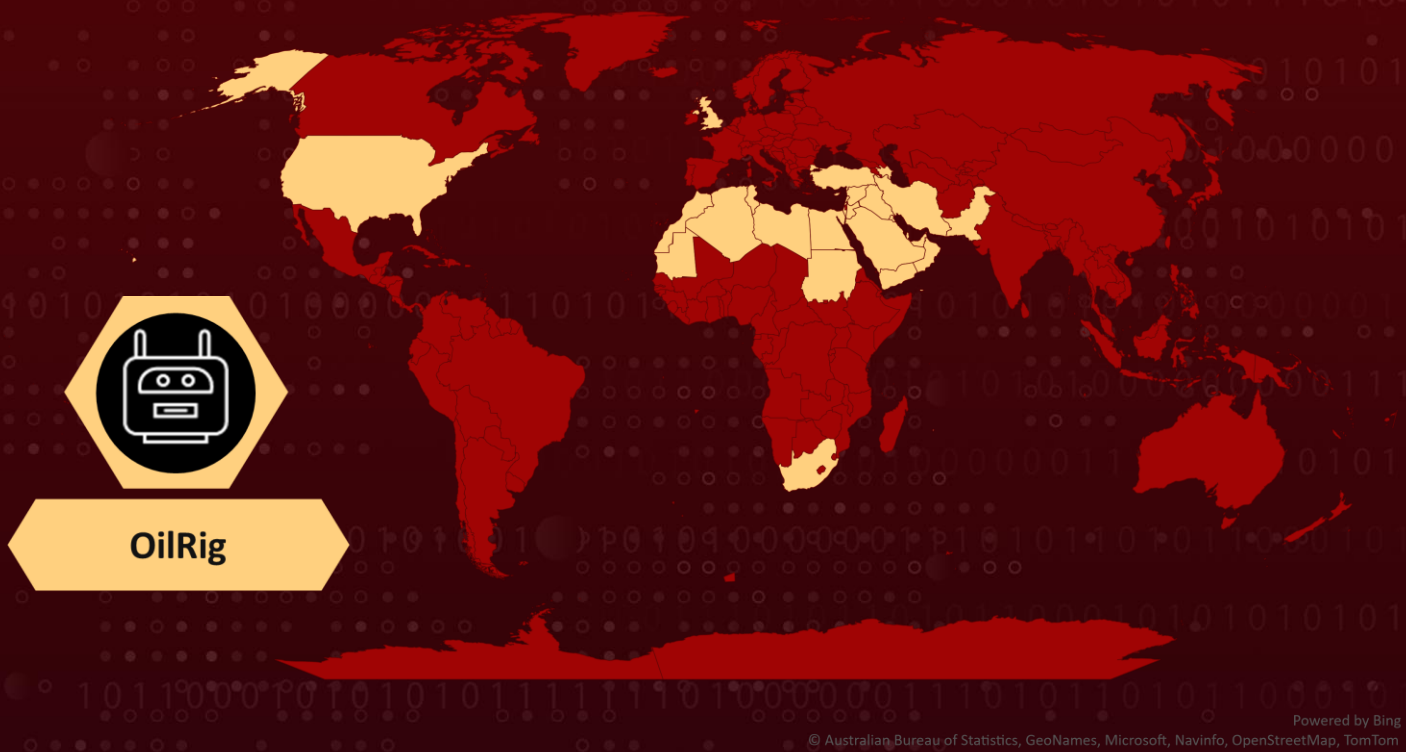
Iranian OilRig Group Strikes with AutoHotkey Keylogger and Malicious Macro

Date of Publication	Admiralty Code	TA Number
February 7, 2023	A2	TA2023065

Summary

First appeared: August 2022
Threat Actor: OilRig (APT 34, Helix Kitten, Twisted Kitten, Crambus, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13)
Attack Region: Oman, Azerbaijan, Bahrain, Iraq, Israel, Jordan, Kuwait, Lebanon, Mauritius, Qatar, Saudi Arabia, South Africa, Turkey, United Arab Emirates, Middle East, North Africa, Pakistan, Turkey, UK, USA.
Attack Sector: Chemicals, Education, Energy, Financial, Government, Legal, Oil and Gas, Telecommunications, Aviation, High-Tech, Hospitality.
Attack: In a recent intrusion, a threat actor utilized AutoHotkey to launch a keylogger. The Iranian Oilrig group is suspected to be the culprit behind this attack. The initial compromise was initiated with a malicious VBA macro embedded in a Word document.

Attack Regions



Attack Details

#1

An attack began with the activation of a malicious macro in a Word document disguised as a job application. Upon opening the file, the victim was prompted to enable macros to complete the form, which then triggered the malware's execution. The macro generated a VBS script and two PowerShell scripts (temp.ps1 and Script.ps1) and installed a persistent presence through a scheduled task.

#2

The PowerShell script established a secure connection to the C2 server. The Iranian OilRig group initiated discovery operations using basic commands executed through PowerShell cmdlets or standard Windows tools such as whoami, net, time, tzutil, and tracert. The information gathered from LDAP discovery was saved in an XML file prior to exfiltration. Several files collected during discovery tasks, such as domain user account information and later the keylogger collected data, were exfiltrated to the C2 server via POST requests.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1204 User Execution	T1204.002 Malicious File
T1087 Account Discovery	T1087.002 Domain Account	T1082 System Information Discovery	T1057 Process Discovery
T1033 System Owner/User Discovery	T1049 System Network Connections Discovery	T1053 Scheduled Task/Job	T1113 Screen Capture
T1056 Input Capture	T1056.001 Keylogging	T1573 Encrypted Channel	T1573.001 Symmetric Cryptography
T1560 Archive Collected Data	T1560.001 Archive via Utility	T1518 Software Discovery	T1518.001 Security Software Discovery
T1083 File and Directory Discovery	T1124 System Time Discovery	T1007 System Service Discovery	T1112 Modify Registry
T1566 Phishing	T1566.001 Spearphishing Attachment	T1053.005 Scheduled Task	T1027 Obfuscated Files or Information

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://45.89.125[.]189/get hxxp://45.89.125[.]189/put
IPV4	45.89.125[.]189

TYPE	VALUE
SHA256	7ae52c0562755f909d5d79c81bb99ee2403f2c2ee4d53fd1ba7692c8053a63f6,eb2a94ee29d902c8a13571ea472c80f05cfab8ba4ef80d92e333372f4c7191f4,b92be3d086372fc89b3466e8d9707de78a5b6dff3e4a2eecc92c01d55a86fd7d,e4b2411286d32e6c6d3d7abffc70d296c814e837ef14f096c829bf07edd45180,45f293b1b5a4aaec48ac943696302bac9c893867f1fc282e85ed8341dd2f0f50,ac933ffc337d13b276e6034d26cdec836f03d90cb6ac7af6e11c045eeae8cc05,d4857156094963c8e38f6e88f4d72cb910aa537e3811eae0579f7abc568c9ae8,be0e75d50565506baa1ce24301b702989ebe244b3a1d248ee5ea499ba812d698,16007ea6ae7ce797451baec2132e30564a29ee0bf8a8f05828ad2289b3690f55,bda4484bb6325dfccaa464c2007a8f20130f0cf359a7f79e14feeab3f
MD5	691332c86dd568f87b7fff4601c37895 fc5f490dbe375779b2c6bbccdd869ca6 9a7d5f126904adc194df4dcbc2c5715c c65b10c1113c0f0d4e06609fa60d9aad f769f67681707e8f69ecdf9e62fb944c 34a2677a7776f87e810814c2d3845f47 f7611e77c5f99b81085e61b17b969afe 850b8d07180601417193a6f88227130a c3aedb781a5b96674764cd43ef076d10 a3c14604fb4454ba5722f07f89780e73
SHA1	0b676ea2ad205b70b9feb1eedbfdec72137e08e5 b8c8171b6e8efd2bb0ae8d5b22749564edd38109 a86088cf31c72cc4648ee8dfa082979a74044203 2ca263fc5f1e505c1839ab0abf56571af6c7809d c5f6a48fa52a279e1f3424b97662b479716229af 79b1f6b0afe943a60560eb20677d5b801dc29ba3 475320a5bf0ba52fc9ff711d8e6dba512b3fefbf e1f4a8e434638c56b7a0d2d0317f4d0d84987a40 86da0100bb6a07a89eaa4dc3ec220e9dbd6ecf71 ed7b9ddbaee794cecb80fac794b0e6cb0ae073b5

References

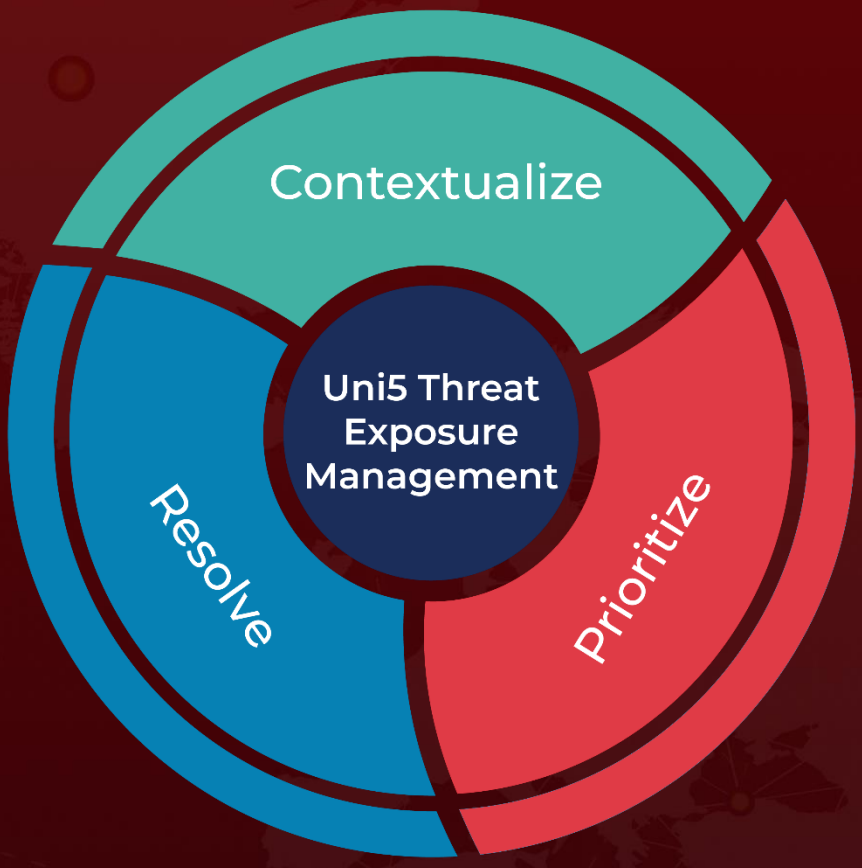
https://thedfirreport.com/2023/02/06/collect-exfiltrate-sleep-repeat/

https://attack.mitre.org/groups/G0049/

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

February 7, 2023 • 3:33 AM

More at www.hivepro.com