Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

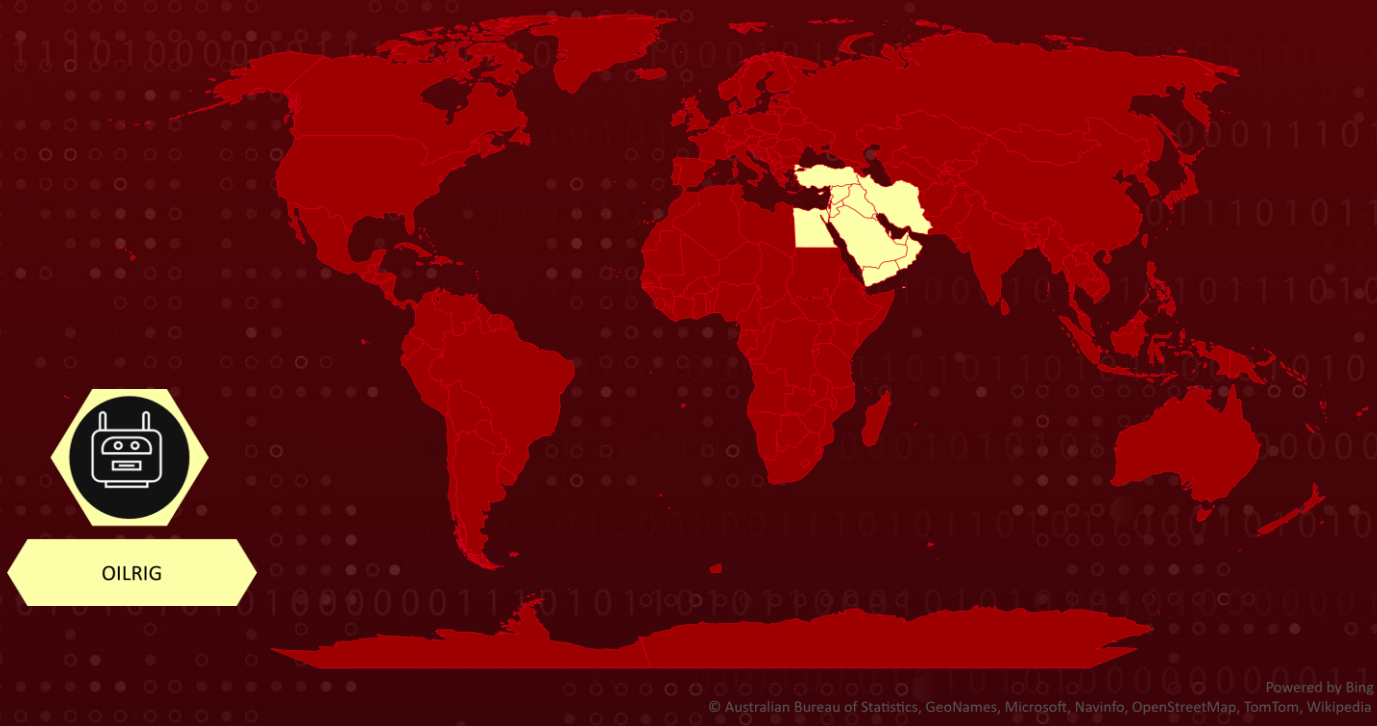
Arab countries are being targeted by multiple malware families

Date of Publication	Admiralty Code	TA Number
November 23, 2022	A1	TA2022269

Summary

Date: November 17, 2022
Attack Region: Middle-East
Threat Actors: Oilrig
Attack: Financial fraud, exfiltration of confidential data, and spying

Attack Regions



Attack Details

#1

Malicious actors have already begun World Cup-themed phishing attacks targeting specific organizations partnered with the tournament are more vulnerable victims in Arab countries. The goal of such assaults could vary, such as financial fraud or reputational damage to the organization.

#2

Following the initial access via phishing attachments, which could contain the banking Trojan and an information stealer called Qakbot and Formbook that can also operate as a downloader, enabling it to download and execute more malicious files, and the Emotet Trojan to access foreign devices and spy on sensitive data. The QuadAgent PowerShell backdoor is yet another piece of malware used by the OilRig gang to perform attacks on susceptible systems.

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

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0009 Collection	TA0011 Command and Control	TA0040 Impact	T1598 Phishing for Information
T1598.002 Spearphishing Attachment	T1587 Develop Capabilities	T1566 Phishing	T1059 Command and Scripting Interpreter
T1204 User Execution	T1113 Screen Capture	T1105 Ingress Tool Transfer	T1496 Resource Hijacking

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	7d1f2798bd70c6cf04f5ad4de1aa68d2, f2752c991000ad9d807fcbe188f03695, d96c44db10ede8dc5c8df5b04bc5a5ab, 80886e4eeba4e683f5da925cd35289b6, 7610c370369217965b7ec150109850e4, 10ebdacd4ec7b3d913932dafc2163751, 38b228e51e7cfa48904fbcb4a106d5b4, 66f989018eabd937c731ddba40605146, 05204f26f8d5161ab487dc41b78624b0, Ce7c58ee6070e056beeb490a7889ac27, 5b5919db69b1912e0aaa9aca716d0857, a58a08ad2a24e8f17fa0b93cb4bcd71e
URLs	hxxps://reaatuae[.]com/ec/prticroanuigm hxxps://advpopovic[.]rs/ia/lorsvaopciptousr hxxps://bladna24[.]ma/fsin/ssnaiueamdsala hxxps://haz-int[.]jp/rlt/vlileol hxxps://dorsica[.]com/dq/caafnofmii hxxps://marcoshueteortega[.]com/ie/snaplvbitouuton hxxps://vivaviajesyvuelos[.]com/in/oseet hxxps://eygcontadores[.]com.mx/ibo/trldmieoiomaoll hxxps://printhomebd[.]com/de/qtaumlaptuvoe

References

https://www.trellix.com/en-us/about/newsroom/stories/research/email-cyberattacks-on-arab-countries-rise.html

https://www.trellix.com/en-us/assets/docs/arab-fifa-campaigns-poc.pdf

https://otx.alienvault.com/pulse/637cb7c3a016240ca7d2886b

https://attack.mitre.org/software/S0650/

https://attack.mitre.org/software/S0367/

https://attack.mitre.org/software/S0332/

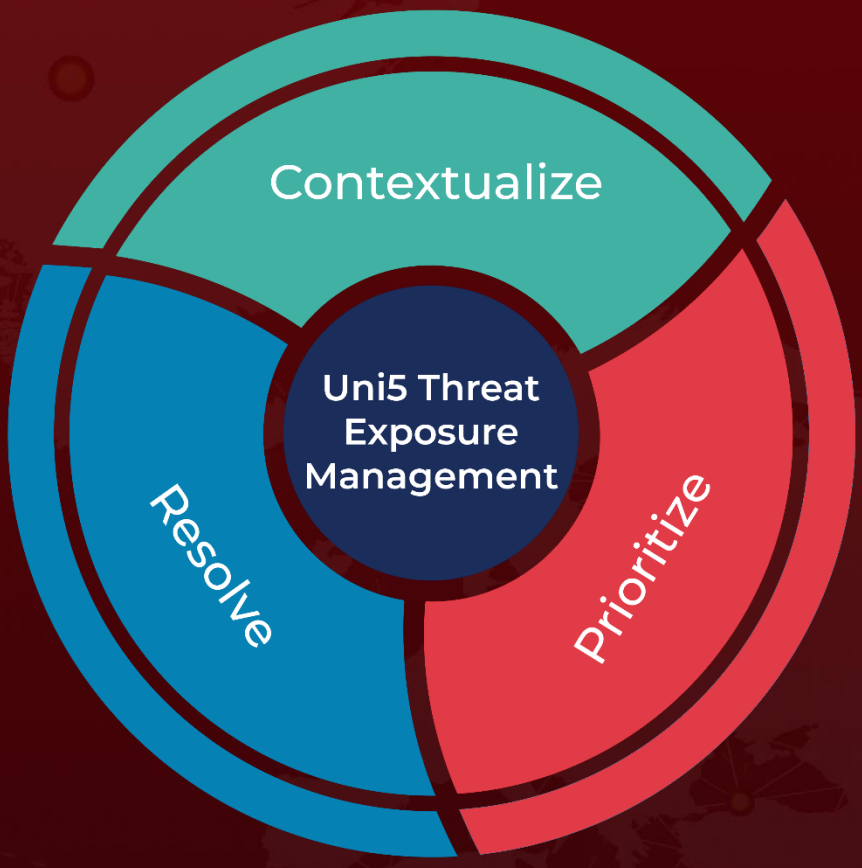
https://attack.mitre.org/software/S0269/

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

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 23, 2022 . 3:33 AM

More at www.hivepro.com