Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

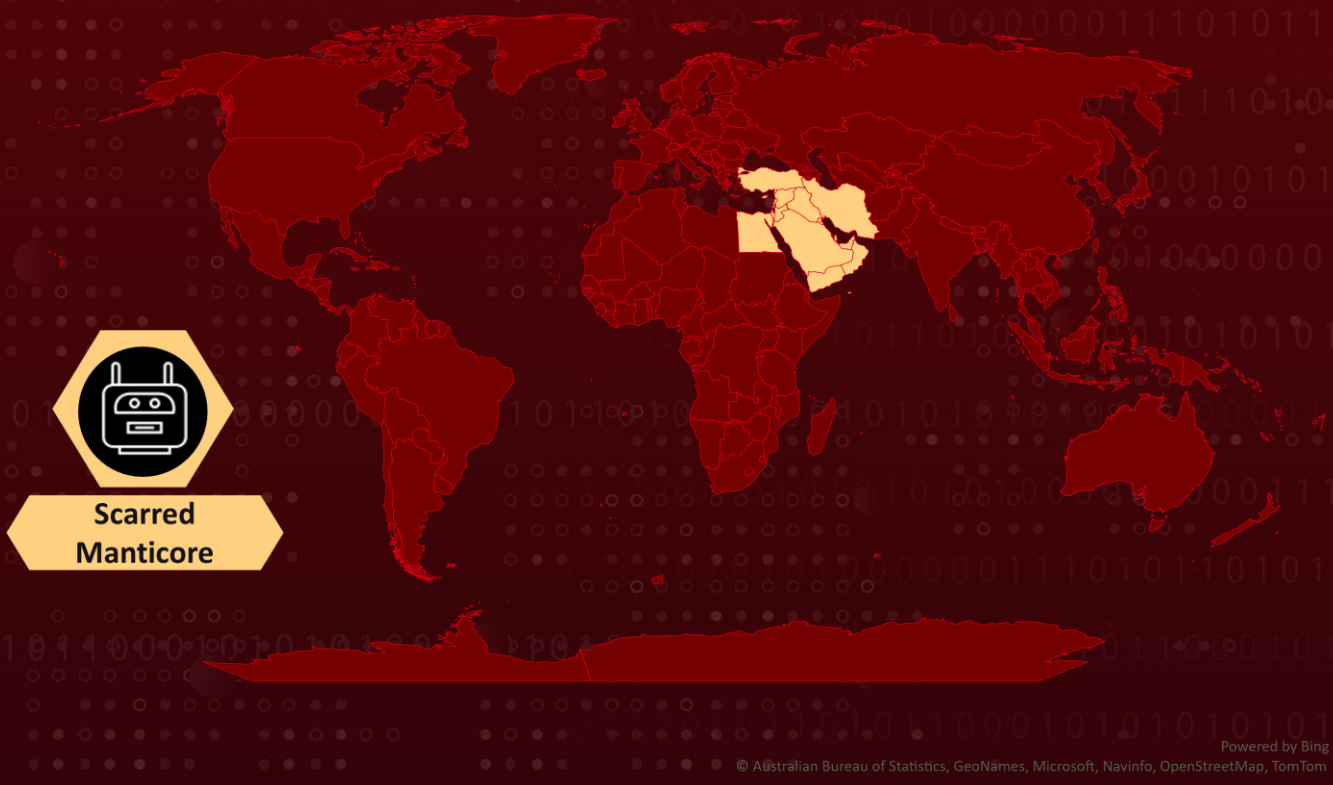
Scarred Manticore's Middle Eastern Gambit

Date of Publication	Admiralty Code	TA Number
November 2, 2023	A1	TA2023443

Summary

Active Since: 2019
Threat Actor: Scarred Manticore
Malware: LIONTAIL
Affected Platform: Windows
Attack Region: Middle East
Targeted Industries: Government, Military, IT Service Providers, Financial Organizations, NGOs, and Telecommunications Sectors
Attack: Scarred Manticore, an actor associated with Iran's Ministry of Intelligence and Security (MOIS), has been conducting a highly sophisticated cyber espionage campaign with a strong focus on the Middle East. This campaign utilizes the advanced LIONTAIL malware framework deployed on Windows servers.

Attack Regions



Attack Details

#1 A threat actor associated with Iran's Ministry of Intelligence and Security (MOIS), Scarred Manticore, has been observed orchestrating a highly sophisticated cyber espionage campaign focusing on the Middle East. These attacks are carried out using LIONTAIL, an advanced passive malware framework deployed on Windows servers.

#2 The campaign primarily targets prominent institutions in the Middle East, with a particular emphasis on government, military, and telecommunications sectors. It also encompasses IT service providers, financial organizations, and non-governmental organizations (NGOs). Scarred Manticore, who is connected to the well-known Iranian actor **OilRig** (also known as APT34 or Sandstorm), has consistently targeted high-profile organizations, exploiting their access to exfiltrate data using carefully customized tools systematically.

#3 Furthermore, there are identified tactical similarities between Scarred Manticore, and an intrusion set known as **ShroudedSnooper**. Attack sequences orchestrated by ShroudedSnooper have focused on telecommunications providers in the Middle East and have involved a discreet backdoor named HTTPSnoop. In their latest campaign, Scarred Manticore utilized the formidable LIONTAIL framework, which includes a sophisticated array of custom loaders and memory-resident shellcode payloads.

#4 LIONTAIL's implants utilize undisclosed functionalities within the HTTP.sys driver to extract payloads from incoming HTTP traffic. Multiple observed variations of LIONTAIL-associated malware indicate that Scarred Manticore develops custom implants for each compromised server, enabling their malicious activities to blend seamlessly with legitimate network traffic, making them nearly indistinguishable.

#5 Over time, Scarred Manticore's toolkit has undergone significant evolution, shifting from open-source web-based proxies to more powerful tools that combine open-source and custom components. This evolution includes the adoption of various IIS-based backdoors to infiltrate Windows servers, such as custom web shells, bespoke DLL backdoors, and driver-based implants.

#6 It is anticipated that Scarred Manticore's operations will persist and may expand to other regions in line with Iran's long-term strategic interests. Currently, Scarred Manticore's recent activities are primarily focused on maintaining covert access and extracting data.

Recommendations

Network Segmentation: Implement network segmentation to limit lateral movement within the network in case of a breach. This can help contain and isolate malicious activity and minimize potential damage.

Encryption for Data in Transit and at Rest: Implement encryption for sensitive data both in transit and at rest. This safeguards against data interception during communication and protects stored data in case of unauthorized access.

Behavioral Anomaly Detection: Implement advanced behavioral anomaly detection systems to identify deviations from normal user and system behavior. These systems should be capable of flagging activities like frequent and unusual execution of commands.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact	T1059 Command and Scripting Interpreter
T1190 Exploit Public-Facing Application	T1574 Hijack Execution Flow	T1078 Valid Accounts	T1543 Create or Modify System Process
T1003 OS Credential Dumping	T1082 System Information Discovery	T1005 Data from Local System	T1041 Exfiltration Over C2 Channel
T1490 Inhibit System Recovery	T1036 Masquerading	T1083 File and Directory Discovery	T1105 Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	daa362f070ba121b9a2fa3567abc345edcde33c54cabefa71dd2faad78c10c33,

TYPE	VALUE
SHA256	f4639c63fb01875946a4272c3515f005d558823311d0ee4c34896c2b66122596, 2097320e71990865f04b9484858d279875cf5c66a5f6d12c819a34e2385da838, 67560e05383e38b2fcc30df84f0792ad095d5594838087076b214d849cde9542, 4f6351b8fb3f49ff0061ee6f338cd1af88893ed20e71e211e8adb6b90e50a3b8, f6c316e2385f2694d47e936b0ac4bc9b55e279d530dd5e805f0d963cb47c3c0d, 1485c0ed3e875cbdfc6786a5bd26d18ea9d31727deb8df290a1c00c780419a4e, 8578bff36e3b02cc71495b647db88c67c3c5ca710b5a2bd539148550595d0330, c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0, 9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0ceb, e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d, a2598161e1efff623de6128ad8aafba9da0300b6f86e8c951e616bd19f0a572b, 7495c1ea421063845eb8f4599a1c17c105f700ca0671ca874c5aa5aef3764c1c, 6f0a38c9eb9171cd323b0f599b74ee571620bc3f34aa07435e7c5822663de605, 3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7, 1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb, b71aa5f27611a2089a5bbe34fd1aafb45bd71824b4f8c2465cf4754db746aa79, Da450c639c9a50377233c0f195c3f6162beb253f320ed57d5c9bb9c7f0e83999

References

https://research.checkpoint.com/2023/from-albania-to-the-middle-east-the-scarred-manticore-is-listening/

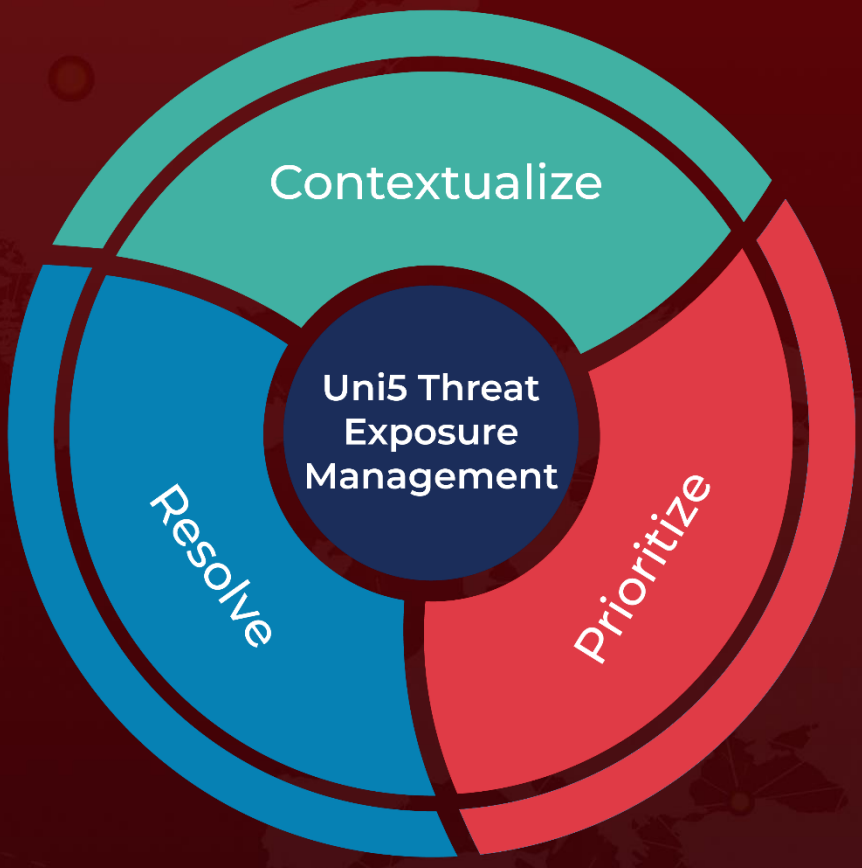
https://www.hivepro.com/prolonged-pursuit-of-oilrig-apt-targeting-middle-east-government/

https://www.hivepro.com/httpsnoop-and-pipesnoop-malware-target-telecoms-in-the-middle-east/

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

November 2, 2023 • 10:30 PM

More at www.hivepro.com