ADVISORY FOR ICM SECTORS

“Scarred Manticore” Group Deliver Custom LIONTAIL Framework

Original report published on: October 31, 2023[1]

Executive Summary

Check Point Researchers and Sygnia’s Incident Response Team uncovered an Iranian nation-state threat group, Scarred Manticore. The threat actor primarily targets government and telecommunication sectors in the Middle East. Scarred Manticore, linked to the prolific Iranian actor OilRig (also known as APT34, EUROPIUM, Hazel Sandstorm) focuses on high-profile organisations, deploying customised tools to extract data.

In their recent campaign, the actor employed LIONTAIL framework, a custom toolset to stealthily extract data by exploiting HTTP traffic, creating unique implants for each server to blend in with legitimate network activity.

Background

LIONTAIL is a malware framework that includes a set of custom shellcode loaders and memory resident shellcode payloads. It takes advantage of undocumented functionalities of the HTTP.sys driver to extract payloads from incoming HTTP traffic. It essentially attaches itself to a Windows server, listening for, intercepting, and decoding messages matching specific URL patterns determined by the attacker.

The LIONTAIL framework is highly stealthy, due to its flexibility to customise for its target. It utilises various tools, such as reverse proxies and reverse shells, making it difficult to detect. But proper endpoint protection and network-level tapping can help defend against it.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory:
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Regularly monitor the attack surface and examine any unusual activities that could signal the lateral movement of a threat actor or the presence of malware.
- Regularly patch and update all software, operating systems, and applications to address known vulnerabilities that threat actors may exploit.
- Validate before adding malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR).
- Closely monitor inbound and outbound network traffic for suspicious communications or data transmissions

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

Indicators of Compromise[1]

SHA256 Hash	Description
daa362f070ba121b9a2fa3567abc345edcde33c54cabefa71dd2faad78c10c33	Trojan/Backdoor
f4639c63fb01875946a4272c3515f005d558823311d0ee4c34896c2b66122596	Trojan/Backdoor
2097320e71990865f04b9484858d279875cf5c66a5f6d12c819a34e2385da838	Trojan/Backdoor
67560e05383e38b2fcc30df84f0792ad095d5594838087076b214d849cde9542	Trojan/Backdoor
4f6351b8fb3f49ff0061ee6f338cd1af88893ed20e71e211e8adb6b90e50a3b8	Trojan/Backdoor
f6c316e2385f2694d47e936b0ac4bc9b55e279d530dd5e805f0d963cb47c3c0d	Trojan/Backdoor
1485c0ed3e875cbdfc6786a5bd26d18ea9d31727deb8df290a1c00c780419a4e	Trojan/Backdoor
8578bff36e3b02cc71495b647db88c67c3c5ca710b5a2bd539148550595d0330	Trojan/Backdoor
c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0	Trojan/Backdoor
9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0ceb	Trojan/Backdoor
e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d	Trojan/Backdoor
a2598161e1efff623de6128ad8aafba9da0300b6f86e8c951e616bd19f0a572b	Trojan/Backdoor
7495c1ea421063845eb8f4599a1c17c105f700ca0671ca874c5aa5aef3764c1c	Trojan/Backdoor
6f0a38c9eb9171cd323b0f599b74ee571620bc3f34aa07435e7c5822663de605	Trojan/Backdoor
3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7	Trojan/Backdoor
1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb	Trojan/Backdoor
b71aa5f27611a2089a5bbe34fd1aafb45bd71824b4f8c2465cf4754db746aa79	Trojan/Backdoor
da450c639c9a50377233c0f195c3f6162beb253f320ed57d5c9bb9c7f0e83999	Trojan/Backdoor

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1199	Trusted Relationship
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1106	Native API

Persistence	T1547	Boot or Logon Autostart Execution
	T1505	Server Software Component
Defence Evasion	T1140	Deobfuscate/Decode Files or Information
	T1036.004	Masquerading: Masquerade Task or Service
	T1127	Trusted Developer Utilities Proxy Execution
	T1027	Obfuscated Files or Information
Discovery	T1082	System Information Discovery
Lateral Movement	T1021	Remote Services
Collection	T1114	Email Collection
	T1213	Data from Information Repositories
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel

References

1. ^ “FROM ALBANIA TO THE MIDDLE EAST: THE SCARRED MANTICORE IS LISTENING”