Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

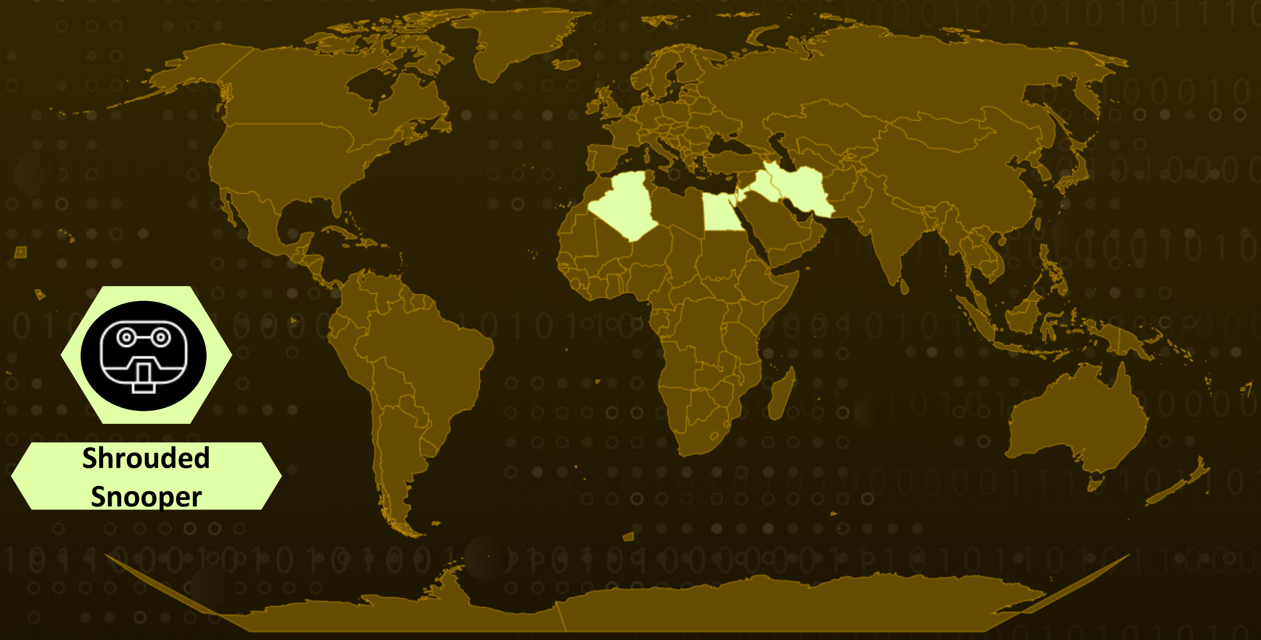
HTTPSnoop and PipeSnoop Malware Target Telecoms in the Middle East

Date of Publication	Admiralty Code	TA Number
September 20, 2023	A1	TA2023378

Summary

First Seen: April 17, 2023
Actor Name: ShroudedSnooper
Attack Region: Middle East
Targeted Industry: Telecommunications
Malware: HTTPSnoop and PipeSnoop
Attack: HTTPSnoop and PipeSnoop malware targeting Middle East telecom providers, part of the ShroudedSnooper intrusion set, masquerading as legitimate components while executing shellcode via HTTP and IPC pipes, posing a threat to critical infrastructure.

Attack Regions



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

Attack Details

#1 A new malware family called "HTTPSnoop" targeting telecommunications providers in the Middle East. This malware acts as a backdoor and uses novel techniques to interact with Windows HTTP kernel drivers, allowing it to listen for specific HTTP(S) URLs and execute content on infected endpoints. Additionally, a related implant called "PipeSnoop" can accept and execute arbitrary shellcode.

#2 Both HTTPSnoop and PipeSnoop can masquerade as legitimate security software components, making them hard to detect. Cisco Talos attributes these implants to a new intrusion set called "ShroudedSnooper" and believes they are used to gain initial access through internet-facing servers, particularly those mimicking Microsoft's Exchange Web Services.

#3 This activity is part of a broader trend of sophisticated actors targeting telecoms, which are crucial due to their control over critical infrastructure assets. Cisco Talos' findings align with reports from other cybersecurity firms detailing attacks on telecom companies worldwide.

#4 HTTPSnoop relies on low-level Windows APIs to bind to specific HTTP(S) URL patterns and execute shellcode received from incoming requests.

#5 HTTPSnoop comes in several variants, each configured to listen to specific URL patterns. It can masquerade as a legitimate security component, such as Palo Alto Networks' Cortex XDR application. PipeSnoop, on the other hand, is designed to work within compromised enterprises and communicates through Windows IPC pipes.

#6 Both HTTPSnoop and PipeSnoop attempt to blend in with benign network traffic, using URL patterns that mimic Microsoft Exchange Web Services, OfficeTrack, and other telecommunications-related services.

Recommendations

Network Segmentation: Isolate critical infrastructure and sensitive systems from the rest of the network to limit lateral movement in case of a breach. Implement network segmentation to reduce the potential impact of a successful attack.

Endpoint Protection: Deploy reputable endpoint protection software that includes anti-malware and behavior-based detection capabilities to identify and block suspicious activities. Regularly update antivirus and anti-malware software to ensure the latest threat definitions by the malware.

Regular Patching and Updates: Keep all operating systems, applications, and security software up-to-date with the latest patches and updates to address vulnerabilities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0042** Resource Development	**TA0005** Defense Evasion	**TA0002** Execution
TA0004 Privilege Escalation	**TA0011** Command and Control	**T1059** Command and Scripting Interpreter	**T1584** Compromise Infrastructure
T1036 Masquerading	**T1574.001** DLL Search Order Hijacking	**T1190** Exploit Public-Facing Application	**T1106** Native API
T1140 Deobfuscate/Decode Files or Information	**T1027** Obfuscated Files or Information		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0, 04cf425e57e7d511f03189749c8c0a95483eeeb4c423e9ee1a6a766d2fe0094c, 3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7, 7495c1ea421063845eb8f4599a1c17c105f700ca0671ca874c5aa5aef3764c1c, 1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb, 9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0ceb, e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d
URLs	http[:]//+[:]80/Temporary_Listen_Addresses/, https[:]//+[:]443/Temporary_Listen_Addresses/, https[:]//+[:]443/autodiscover/autodiscovers/, https[:]//+[:]444/autodiscover/autodiscovers/, https[:]//+[:]444/ews/exchange/, https[:]//+[:]443/ews/exchange/, https[:]//+[:]443/autodiscover/autodiscover/, https[:]//+[:]444/autodiscover/autodiscover/, https[:]//+[:]444/ews/exchanges/, https[:]//+[:]443/ews/exchanges/, https[:]//+[:]444/ews/exchange/, https[:]//+[:]443/ews/exchange/, https[:]//+[:]443/ews//, https[:]//+[:]444/ews//, https[:]//+[:]444/ews/ews/, https[:]//+[:]443/ews/ews/, https[:]//+[:]443/ews/autodiscovers/, https[:]//+[:]444/ews/autodiscovers/, https[:]//+[:]443/autodiscover/autodiscoverrs/, https[:]//+[:]444/autodiscover/autodiscoverrs/, https[:]//+[:]443/autodiscover/course/, https[:]//+[:]443/autodiscover/because/, https[:]//+[:]443/autodiscover/oppose/, https[:]//+[:]443/autodiscover/citizen/, https[:]//+[:]443/autodiscover/surprise/, https[:]//+[:]443/autodiscover/make/,

TYPE	VALUE
URLs	https[:]//+[:]443/autodiscover/tiger/, https[:]//+[:]443/autodiscover/verb/, https[:]//+[:]443/autodiscover/palace/, https[:]//+[:]443/autodiscover/congress/, https[:]//+[:]443/autodiscover/expire/, https[:]//+[:]443/autodiscover/this/, https[:]//+[:]443/ews/often/, https[:]//+[:]443/ews/evoke/, https[:]//+[:]443/ews/pitch/, https[:]//+[:]443/ews/sense/, https[:]//+[:]443/ews/six/, https[:]//+[:]443/ews/tower/, https[:]//+[:]443/ews/feature/, https[:]//+[:]443/ews/trip/, https[:]//+[:]443/ews/jazz/, https[:]//+[:]443/ews/second/, https[:]//+[:]443/ews/question/, https[:]//+[:]443/ews/powder/, https[:]//+[:]444/autodiscover/verb/, https[:]//+[:]444/autodiscover/palace/, https[:]//+[:]444/autodiscover/congress/, https[:]//+[:]444/autodiscover/expire/, https[:]//+[:]444/autodiscover/this/, https[:]//+[:]444/ews/feature/, https[:]//+[:]444/ews/trip/, https[:]//+[:]444/ews/jazz/, https[:]//+[:]444/ews/second/, https[:]//+[:]444/ews/question/, https[:]//+[:]444/ews/powder/, https[:]//+[:]444/ews/test/, http[:]//*[:]80/eye/, http[:]//*[:]80/delay/, http[:]//*[:]80/hill/, http[:]//*[:]80/uncle/, http[:]//*[:]80/ofasdaqgrumm/, http[:]//*[:]80/utkvvxwkwgseowps/, http[:]//*[:]80/xewnsfqdcxmhwb/, http[:]//*[:]80/vzixmvmvbvrzhoo/, https[:]//*[:]443/eye/, https[:]//*[:]443/delay/, https[:]//*[:]443/hill/, https[:]//*[:]443/uncle/,

TYPE	VALUE
URLs	https[:]//*[:]443/ofasdaqgrumm/, https[:]//*[:]443/utkvvxwkwgseowps/, https[:]//*[:]443/xewnsfqdcxmhwb/, https[:]//*[:]443/vzixmvmvbvrzhoo/, http[:]//+[:]80/test_srv/, https[:]//+[:]443/test_srv/

References

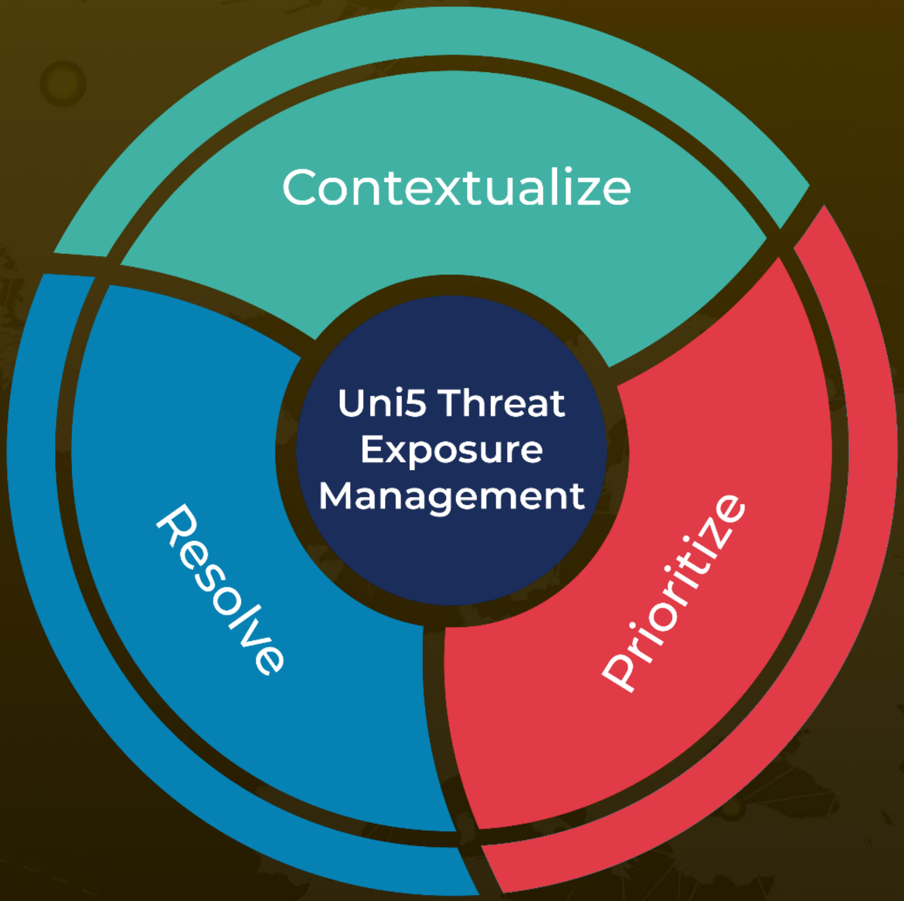
https://blog.talosintelligence.com/introducing-shrouded-snooper/

https://github.com/Cisco-Talos/IOCs/blob/main/2023/09/introducing-shrouded-snooper.txt

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

September 20, 2023 • 09:30 AM

More at www.hivepro.com