

ShroudedSnooper targets Telecommunication Internet Facing Servers

Original report published on: September 19, 2023^[1]

Executive Summary

Cisco Talos discovered a threat group “ShroudedSnooper” deploying new backdoor implants named HTTPSnoop and PipeSnoop against telecommunication service providers in the Middle East, allowing threat actors to remotely execute commands on infected devices.^[1]

Background

The two new malware HTTPSnoop and PipeSnoop can masquerade as legitimate security software components, such as eXtended Detection and Response (XDR) agents. HTTPSnoop also mimics Microsoft Exchange Web Services platform. Therefore, it is likely that internet-facing servers were exploited to deploy HTTPSnoop to gain initial access.

HTTPSnoop is a backdoor implant that interfaces with Windows HTTP kernel drivers and devices to listen to incoming requests for specific HTTP(S) URLs and execute decoded shellcode on the infected internet facing endpoint(s).

To masquerade as benign traffic, HTTPSnoop listens to URL patterns that make it look like the infected system being contacted is a server hosting Microsoft’s Exchange Web Services (EWS) API. This involves URLs consisting of ‘ews’ and ‘autodiscover’ keywords over ports 443 and 444.

Another implant, PipeSnoop, can accept arbitrary shellcode from an Inter-Process Communication (IPC) pipe and execute it on the infected endpoint. It reads and writes to and from a Windows IPC pipe for its input/output operations which suggests that it is designed to function further within a compromised enterprise system. PipeSnoop is likely used in conjunction with another unknown component that is capable of feeding it the required shellcode.

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.
- Validate and add malicious file hashes to blacklist 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^[2]

SHA256

c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0
04cf425e57e7d511f03189749c8c0a95483eeeb4c423e9ee1a6a766d2fe0094c
3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7
7495c1ea421063845eb8f4599a1c17c105f700ca0671ca874c5aa5aef3764c1c
1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb
9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0ceb
e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d

URLs

http://+:80/Temporary_Listen_Addresses/
https://+:443/Temporary_Listen_Addresses/
https://+:443/autodiscover/autodiscover/
https://+:444/autodiscover/autodiscover/
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/autodiscover/
https://+:444/ews/autodiscover/
https://+:443/autodiscover/autodiscoverrrs/
https://+:444/autodiscover/autodiscoverrrs/
https://+:443/autodiscover/course/
https://+:443/autodiscover/because/



<https://+:443/autodiscover/oppose/>
<https://+:443/autodiscover/citizen/>
<https://+:443/autodiscover/surprise/>
<https://+:443/autodiscover/make/>
<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/
https://*:443/ofasdaqgrumm/
https://*:443/utkvvxwkwgseowps/
https://*:443/xewnsfqdcxmhwb/
https://*:443/vzixmvmvbvrzhoo/
http://+:80/test_srv/
https://+:443/test_srv/

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1559	Inter-Process Communication
Persistence	T1505.003	Server Software Component: Web Shell
	T1574.001	Hijack Execution Flow: DLL Search Order Hijacking
Defense Evasion	T1036.004	Masquerading: Masquerade as legitimate security software component
	T1140	Deobfuscate/Decode Files or Information
Discovery	T1040	Network Sniffing
Command and Control	T1071.001	Application Layer Protocol: Web Protocols

References

1. ^ "New ShroudedSnooper actor targets telecommunications firms in the Middle East with novel Implants"  .
2. ^ "Cisco-Talos Indicators of Compromise (IOCs)"  .