ADVISORY FOR ICM SECTORS

Sea Turtle group targets cPanel with reverse shell

Original report published on: Jan 05, 2024[1]

Executive Summary

Sea Turtle is an APT group known for cyberespionage campaigns targeting organisations in Europe, Middle East and North Africa with a focus on telecommunication and media sectors, Internet Service Providers (ISP), IT-service providers and Kurdish websites[1]. Recent reports on their activities have shown that they have changed their tools to better avoid detection.

Background

Also known as Teal Kurma, Marbled Dust, SILICON and Cosmic Wolf, this APT group was previously known for their use of DNS hijacking between 2017 to 2019 but has more recently switched to using a simplistic reverse shell designed for Linux and Unix systems[1] .

In 2023, during one of their most recent campaigns in the Netherlands, Sea Turtle accessed the target organisation's cPanel Web hosting environment via SSH from a VPN connection, dropped an information-gathering Linux reverse TCP shell called "SnappyTCP” and exfiltrated a copy of the email archive created in the public web directory of the website through a command-and-control (C2) channel using TCP and HTTP. To avoid detection, Sea Turtle unset the Bash command and MySQL history file and overwrote Linux system logs. It is unclear how they managed to obtain the legitimate cPanel credentials[1].

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 and create detection rules and deny processes related to these techniques if there is no business need.
- Validate and add the Indicators of Compromise to blocklist(s) in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR).
- Store log files in a central location and ensure sufficient storage capacity for historic forensic investigation purposes.
- Limit logon attempts on accounts to reduce the chance of successful brute force attacks.
- Reduce the number of systems that can be reached over the internet using SSH. Where this is still necessary, it is recommended to implement an SSH-login rate-limit.
- Limit outgoing connections to only required ports and known IP addresses through whitelisting.
- Create and enforce a password policy with adequate complexity requirements or use an access management system.
- Enable multi-factor authentication (MFA) on all externally exposed accounts.

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]

Indicator	Type	Description

82.102.19[.]88	IP-address	The IP-address is of M247 Europe SRL located in Belgium and was used as VPN by Sea Turtle to logon to a cPanel account.
62.115.255[.]163	IP-address	The IP-address is of Arelion and located in Denmark and was used as VPN by Sea Turtle to logon on to a cPanel account.
193.34.167[.]245	IP-address	The IP-address is of Snel.com and located in the Netherlands. The IP-address was used to logon to a cPanel account and to download the source code of the malware SnappyTCP.
Forward.boord[.]info	Domain name	The malware SnappyTCP was used by Sea Turtle to establish a command-and-control channel with the domain name.
f1a4abd70f8e56711863f9e7ed0a4a865267ec7	SHA-1 Get 256	A modified version of the tool Socat used by Sea Turtle to setup a command-and-control channel.

MITRE ATT&CK Tactics and Techniques[1]

Tactic	Technique ID	Technique Title
Resource Development	T1588.001	Obtain Capabilities: Malware
Initial Access	T1133	External Remove Services
	T1078.004	Valid Account: Cloud Accounts
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
Persistence	T1505.003	Server Software Component: Web Shell
Defense Evasion	T1070.003	Indicator Removal: Clear Command History
	T1070.002	Indicator Removal: Clear Linux or Mac System Logs
Collection	T1114.001	Email Collection: Local Email Collection
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
	T1095	Non-Application Layer Protocol
Exfiltration	T1567	Exfiltration Over Web Service

References

1. ^ “ Turkish espionage campaigns in the Netherlands” .