Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

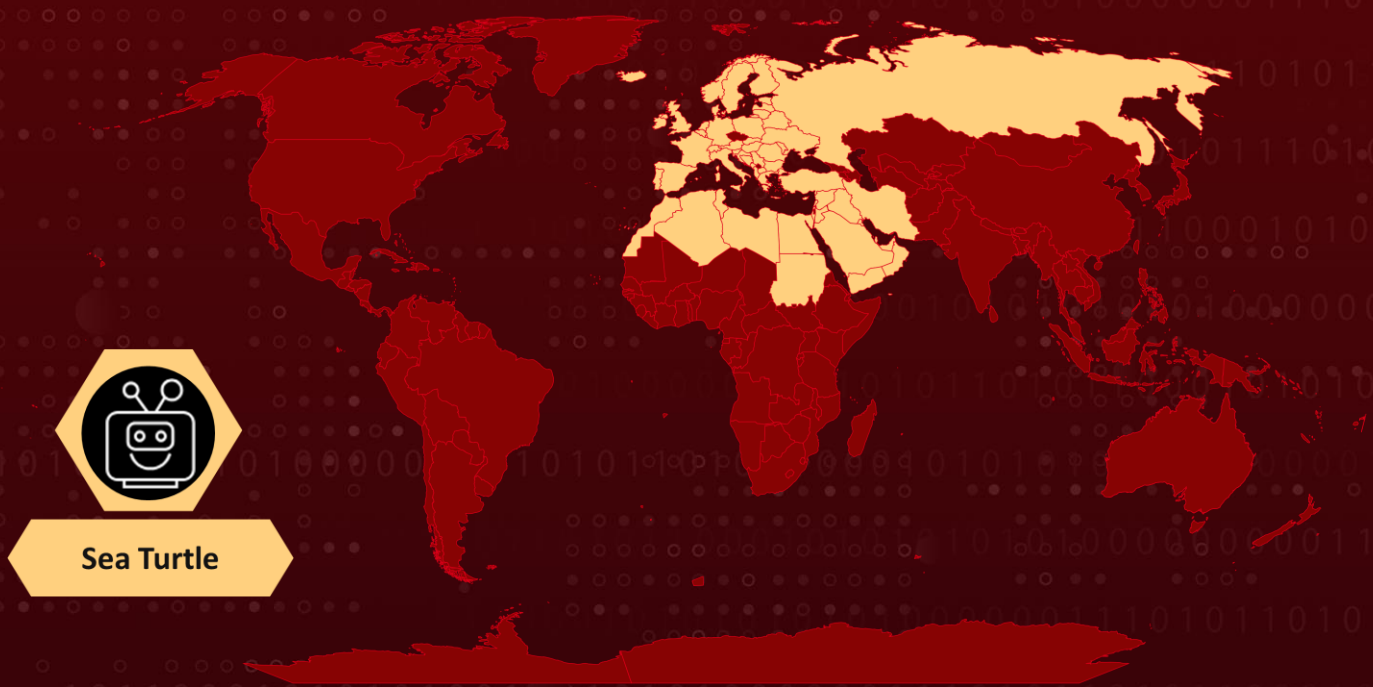
Unveiling the Sea Turtle Cyber Espionage Campaign

Date of Publication	Admiralty code	TA Number
January 10, 2024	A1	TA2024009

Summary

First Seen: January 2017
Actor Name: Sea Turtle (aka Teal Kurma, Marbled Dust, SILICON and Cosmic Wolf)
Target Industries: Government entities, Kurdish (political) groups like PKK, telecommunication, ISPs, IT-service providers (including security companies), NGO and Media & Entertainment sectors
Target Region: Europe, Middle East and North Africa
Malware: SnappyTCP

Actor Map



Actor Details

#1 Sea Turtle, a Turkey-based Advanced Persistent Threat (APT) actor, is known for information theft and DNS hijacking. Operating from 2017 to 2019, Sea Turtle primarily targeted European and Middle Eastern organizations, focusing on governmental bodies, Kurdish groups, NGOs, telecommunications, ISPs, IT service providers, and media and entertainment organizations. The group's objective is to compromise repositories containing valuable and sensitive data.

#2 Sea Turtle, the threat actor, exhibits moderate sophistication in its operations, leveraging public vulnerabilities to initiate access to targeted organizations. However, their operational security hygiene is considered sloppy. The group's tactics involve intercepting internet traffic directed at compromised websites, redirecting user traffic, obtaining valid encryption certificates, and conducting man-in-the-middle attacks.

#3 Sea Turtle has recently been detected executing multiple campaigns in the Netherlands, with activities spanning the timeframe from 2021 to 2023. In one of the most recent campaigns in 2023, the threat actor utilized a reverse TCP shell named SnappyTCP designed for Linux/Unix systems. This shell comes with basic command-and-control capabilities and is employed to establish persistence on compromised systems.

#4 The initial access involved a compromised cPanel account used to deploy SnappyTCP on a system. The attackers created an email archive in the public web directory of the website. Logging in from an IP which belonged to VPN provider's range, the attacker created a cPanel WebMail session, downloaded source code files, and executed SnappyTCP using NoHup, ensuring persistence even after exiting the shell or terminal.

#5 Organizations, especially those in the telecommunications, ISP, and managed service provider sectors, are advised to enhance cybersecurity defenses and reduce vulnerability to threats like Sea Turtle by implementing necessary security measures.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGETED INDUSTRIES
Sea Turtle	Turkey **MOTIVE** Data Theft	Europe, Middle East and North Africa	Government entities, political groups, telecommunication, ISPs, IT-service providers (including security companies), NGO and Media & Entertainment sectors

Recommendations

- **Enforce MFA Across all Admin Accounts:** Ensure that MFA is mandatory for all administrator accounts. This reduces the risk of unauthorized access even if the password is compromised.
- **Robust Endpoint Security:** Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively, also monitor network traffic and analyze DNS requests for any abnormal or suspicious patterns.
- **Apply Strong Password Policies:** Ensure the use of strong and unique passwords across all accounts to prevent unauthorized access.
- **Regularly Update and Patch Systems:** Keep all systems and software up-to-date with the latest security patches to mitigate known vulnerabilities.
- **Educate Users on Cybersecurity Best Practices:** Provide cybersecurity awareness training to employees to recognize and avoid phishing attempts and other social engineering tactics.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
T1588 Obtain Capabilities	T1588.001 Malware	T1133 External Remote Services	T1078 Valid Accounts
T1078.004 Cloud Accounts	T1059 Command and Scripting Interpreter	T1059.004 Unix Shell	T1505 Server Software Component
T1505.003 Web Shell	T1070 Indicator Removal	T1070.003 Clear Command History	T1070.002 Clear Linux or Mac System Logs
T1114 Email Collection	T1114.001 Local Email Collection	T1071 Application Layer Protocol	T1071.001 Web Protocols
T1095 Non-Application Layer Protocol	T1567 Exfiltration Over Web Service		

Indicator of Compromise (IOCs)

TYPE	VALUE
IP	82.102.19[.]88, 62.115.255[.]163, 193.34.167[.]245
Domain	forward.boord[.]info
SHA1	f1a4abd70f8e56711863f9e7ed0a4a865267ec7

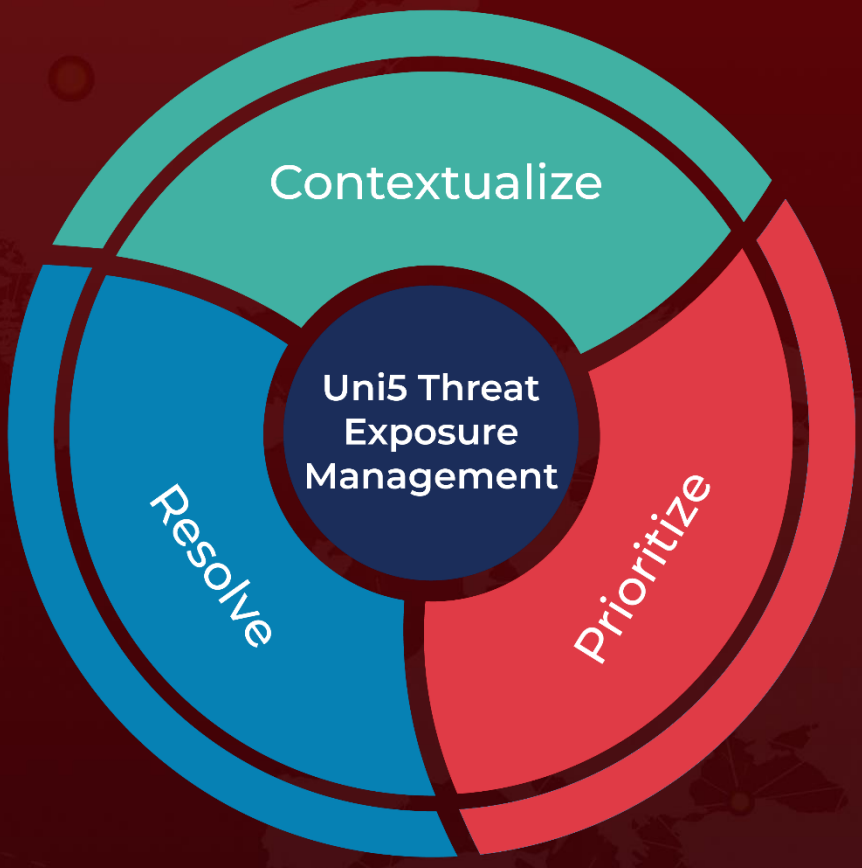
References

https://www.huntandhackett.com/blog/turkish-espionage-campaigns

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

January 10, 2024 • 5:50 AM

More at www.hivepro.com