Turkish espionage campaigns in the Netherlands

Hunt & Hackett Research Team ⋮⋮ 1/5/2024

Hunt & Hackett Research Team @

Jan 5, 2024 10:02:13 AM

In the past year, Hunt & Hackett has observed cyberattacks in the Netherlands, which are believed to have been orchestrated by a cyber threat actor operating in alignment with Turkish interests, signalling an escalation in Turkey's pursuit of objectives within Western nations. Hunt & Hackett has started tracking this group known by aliases such as Sea Turtle, Teal Kurma, Marbled Dust, SILICON and Cosmic Wolf. This blog aims to contribute to the current existing knowledge base by aligning our observations with the known modus operandi of this threat actor. The information is intended to help (security) organizations better prepare for and safeguard against the methods and tools used by this APT group.

Background, Motivations & Targets

Hunt & Hackett believes that Sea Turtle is a Turkey based Advanced Persistent Threat (APT) actor that is motivated by espionage by means of information theft that targets public and private entities. From 2017 to 2019, this actor has been mainly known for DNS hijacking[1] to achieve their ultimate objectives. The threat actor has since continued to target similar sectors but has altered its capabilities in a likely attempt to evade detection. Since then, the public information on this threat actor has remained limited. In October 2021, Microsoft[2] shed light on SILICON, also recognized as Sea Turtle[3], revealing their pursuit of intelligence gathering aligned with strategic Turkish interests. Other organizations such as the Greek National CERT[4] have observed this actor as well and shared a number of Indicators of Compromise (IOCs) related to this group and their modus operandi in 2022. Other than that, the flow of information has remained limited, and this actor seemed to be operating primarily under the radar. The limited public knowledge base was recently enriched with the PwC threat intelligence report[5] '*The Tortoise and The Malwahare*', and a blogpost by StrikeReady[6], detailing this threat actor's methods.

What is known to date is that the Sea Turtle group focuses primarily on targeting organizations in Europe and the Middle East. Research suggests this threat actor primarily focuses on governmental bodies, Kurdish (political) groups such as PKK, NGOs, telecommunication entities, ISPs, IT service providers, and Media & Entertainment organisations, mainly aiming at repositories housing valuable and sensitive data. As noted by PwC, telecommunication companies safeguard customer information such as metadata pertaining to website connections and call logs. Additionally, companies providing technological services such as ISP hosting, IT, and cybersecurity are susceptible to attacks directly or through supply chains and island-hopping strategies. When successful, the stolen information is then most likely utilized for surveillance or gathering intelligence on specific targets. The modus operandi of Sea Turtle involves intercepting internet traffic directed at victimized websites, potentially allowing unauthorized access to government networks and other organizational systems. This targeting approach aids in associating actions with the threat actor and provides valuable insights for organizations operating within similar geographic zones or sectors. Their use of a reverse shell mechanism in operations streamlines the collection and extraction of sensitive data, furthering their agenda. An in-depth analysis of victimology reveals the specific types of data sought by this threat actor.

Threat Actor Highlights

- **Threat Actor Group:** Sea Turtle is also known under the aliases; Teal Kurma, Marbled Dust, SILICON and Cosmic Wolf;
- **Motivation**: primarily focused on acquiring economic and political intelligence through espionage and information theft that targets public and private entities;
- **Targeted Sectors**: Government entities, Kurdish (political) groups like PKK, telecommunication, ISPs, IT-service providers (including security companies), NGO and Media & Entertainment sectors;
- **Geographical Focus**: focuses primarily on targeting organizations in Europe, Middle East and North Africa;
- **Modus Operandi**: is based on redirecting user traffic, obtaining valid encryption certificates, performing man-in-the-middle attacks to harvest credentials and achieve initial access in to targeted organization’s network;
- **Sophistication:** although some techniques are more technical in nature, the threat actor is considered moderate in sophistication. They primarily focus on using public vulnerabilities to get initial access to an organization and from an operational security perspective their hygiene can be considered sloppy.
- **Information Acquisition**: The use of a reverse shell in their operations assists the threat actor in achieving their goal of collecting and exfiltrating sensitive data.

Sea Turtle campaigns in the Netherlands

Hunt & Hackett observed Sea Turtle conducting multiple campaigns in the Netherlands. The modus operandi used in these attacks is largely consistent with the modus operandi and information published in the earlier mentioned threat intelligence reports.

Our investigation into one of their attacks indicated that this group exhibits characteristics of a state-supported cyber espionage group, primarily focused on acquiring economic and political intelligence through espionage with the aim of advancing Turkey’s interests. Hunt & Hackett has started tracking this group and has observed more campaigns from this threat actor targeting specific organizations in the Netherlands. These cyberattacks are believed to be orchestrated by Sea Turtle operating in alignment with Turkish interests, signalling an escalation in Turkey's pursuit of objectives within the Netherlands.

The campaigns observed in the Netherlands appear to focus on telecommunication, media, ISPs and IT-service providers and more specifically Kurdish websites (among others PPK affiliated). The infrastructure of the targets was susceptible to supply chain and island-hopping attacks, which the attack group used to collect politically motivated information such as personal information on minority groups and potential political dissents. The stolen information is likely to be exploited for surveillance or intelligence gathering on specific groups and or individuals. This appears to be consistent with claims from US officials in 2020 about hacker groups acting in Turkey’s interest, focusing on the

identities and locations of the victims, which included governments of countries that are geopolitically significant to Turkey[7].

Hunt & Hackett has observed the threat actor executing defense evasion techniques to avoid being detected, and the threat actor has also been observed collecting potentially sensitive data such as email archives. Their modus operandi includes intercepting internet traffic to victim websites, and potentially granting unauthorized access to government networks and other organizations.

Key Observations

Before diving into the nitty gritty details, Hunt & Hackett would like to provide a summary of key observations. These key points of the overall analysis were specific for the campaigns observed in the Netherlands:

- Hunt & Hackett has observed campaigns from the threat actor between 2021 and 2023, where during one of the most recent campaigns in 2023, a reverse TCP shell named SnappyTCP for Linux/Unix with basic command-and-control capabilities has been used to establishing persistence on systems;
- Hunt & Hackett has observed the threat actor to use code from a publicly accessible GitHub account, assess with high probability that this account is controlled by the threat actor. Upon request a copy of this GitHub account can be provided, since the repository has been taken down either by GitHub, or the user;
- Hunt & Hackett has observed the threat actor compromising cPanel accounts and using SSH to achieve initial access to the IT-environment of an organization;
- Hunt & Hackett has observed the threat actor executing defense evasion techniques to avoid being detected, and;
- Hunt & Hackett has observed the threat actor collecting at least one e-mail archive, of one of the multiple victim organizations.

Modus Operandi

MITRE ATT&CK is a framework of adversary tactics and techniques based on real-world observations. Leveraging this framework helps to understand and document the attack path per phase, as shown in *Table 1*. The first column describes the tactical goal, the reason for performing an action by the threat actor. Next to which the corresponding findings are described to validate the modus operandi and compared the observations of the recent threat report of PwC and StrikeReady with the observations of Hunt & Hackett to validate the modus operandi of Sea Turtle.

Tactic	Technique	Finding	Observed by Hunt & Hackett	Observed by PwC
Reconnaissance				
The threat actor is trying to gather information they can use to plan future operations	There are no findings related to this phase of the attack.			
Resource development				
The threat actor is trying to establish resources they can use to support operations	T1588.001	Sea Turtle used the malware SnappyTCP from which the source code is available on GitHub.	✓	✓
Initial access	T1133 T1078.004	Sea Turtle compromised cPanel accounts and used SSH to get into the IT-infrastructure.	✓	

The threat actor is trying to obtain access to your network.				
Execution				
The threat actor is trying to run malicious code.	T1059.004	Sea Turtle used the Unix shell Bash to execute malicious commands and the malware SnappyTCP.	✓	✓
Persistence				
The threat actor is trying to maintain their foothold.	T1505.003	Sea Turtle executed SnappyTCP using the tool NoHup, which keeps the malware running on a system after exiting the shell or terminal, and installed Adminer in the public web directory of a cPanel account.	✓	✓
Privilege Escalation				
The threat actor is trying to gain higher-level permissions.	There are no findings related to this phase of the attack.			
Defense Evasion				
The threat actor is trying to avoid being detected.	T1070.003 T1070.002	Sea Turtle unsets the command (Bash) and MySQL history file and has overwritten Linux system logs.	✓	
Credential Access				
The threat actor is trying to steal account names and passwords.	There are no findings related to this phase of the attack.			
Discovery				
The threat actor is trying to figure out your environment.	There are no findings related to this phase of the attack.			
L**ateral Movement**				
The threat actor is trying to move through your environment.	There are no findings related to this phase of the attack.			
Collection				
The threat actor is trying to gather data of interest to their goal.	T1114.001	Sea Turtle created a copy of the e-mail archive of a compromised cPanel account in the public web directory of a website that was accessible from the internet.	✓	
Command and Control				
The threat actor is trying to communicate with compromised systems to control them.	T1071.001 T1095	Sea Turtle configured SnappyTCP to establish a command-and-control channel to the domain name forward.boord[.]info on port 443 using the protocols TCP and HTTP.	✓	✓
Exfiltration	T1567	Sea Turtle created a copy of the e-mail archive of a compromised cPanel account in the public web directory of a website that was accessible from the internet. It is highly likely that Sea Turtle exfiltrated	✓	
The threat actor is trying to steal data.				

	the e-mail archive by downloading the file from the website.
Impact	
The threat actor is trying to manipulate, interrupt or destroy your systems and data	There are no findings related to this phase of the attack.

Table 1 - Overview of the attacker activity mapped to the MITRE ATT&CK framework and compared with the observations of PwC

Technical Campaign Details

While researching this actor, the most recent campaigns observed by Hunt & Hackett, were initiated early 2023 when the threat actor targeted multiple organizations. During one of the attacks, the threat actor logged on to cPanel, a web hosting control panel used by multiple organizations world-wide, from an IP address[8] that belonged to the range of a VPN provider. This was a legitimate cPanel account, compromised by the attacker. Unfortunately, it is unclear how they obtained access to the cPanel credentials. Days later a cPanel WebMail session was created for that same cPanel account, when it logged on from an IP address[9] belonging to the range of a hosting provider. In addition, the account was used to perform an SSH logon from that same IP-address. Following these logons, source codes files of a reverse shell written in the programming language 'C' were downloaded from that .245 IP-address. These source code files were then compiled using GCC. Analysis of the source code files revealed that they contained specific code identical to a reverse shell[10] that was stored in a publicly accessible GitHub repository[11] that is believed to be used by the Sea Turtle attack group. Independent from Hunt & Hackett, PwC recently observed usage of this reverse shell named SnappyTCP and similarly attributed this to the threat actor Sea Turtle.

Before executing SnappyTCP using the tool NoHup, the domain name forward.boord[.]info and port 443 was written to a configuration file, with which it connected over TCP using HTTP to establish a command-and-control (C&C) channel. NoHup ensured SnappyTCP remained running on the system even after the shell or terminal was exited. At the end of the SSH session anti-forensics was performed by unsetting the command history (Bash) and MySQL history file, and overwriting Linux system logs.

Weeks later, the cPanel Web Disk Feature accepted another connection. This was an indication that the threat actor was still using this cPanel feature. Based on the actions following the connection, combined with the source being an unfamiliar VPN connection, this activity was classified as malicious. Shortly after, the tool Adminer[12] was installed in the public web directory of one of the compromised cPanel accounts. Adminer is a publicly available database management tool that can be used to remotely logon to the MySQL service of a system. The earlier identified Github repository stores the source code of SnappyTCP, as well as the tool Adminer which indicated that the threat actor was using the software hosted in the earlier mentioned GitHub repository.

Several weeks after the second cPanel Web Disk connection, the threat actor logged on to cPanel from the VPN provider M247 (82.102.19[.]88), which can be interpreted as the compromise of a second cPanel account. Subsequently, a logon was performed on the same cPanel account and a WebMail session was created for that cPanel account.

Finally, using SnappyTCP the threat actor sent commands to the system to create a copy of an e-mail archive created with the tool tar, in the public web directory of the website that was accessible from the internet. It is highly likely that the threat actor exfiltrated the e-mail archive by downloading the file directly from the web directory.

Command & Control

Hunt & Hackett was able to download the source code of the SnappyTCP from one of the servers used by Sea Turtle (http[://]193.34.167[.]245/c00n/connn.c) alongside other files. As previously described, the SnappyTCP malware reads a config file that contains a domain name and port number. Depending on the version of the malware and whether the connection must be encrypted or not, the malware does an HTTP GET with the request URI 'sy.php'. If the header 'X-Auth-43245-S-20' is returned by the server, SnappyTCP then checks if output has sufficient size and if the first character does not start with an '@'. If this is the case, a reverse shell is spawned using the IP and port returned by the server. Otherwise, the whole sequence will restart after a short amount of sleep.

The command-and-control (C&C) channel is setup with what Hunt & Hackett believes is a form of Socat, as detected by the THOR APT Scanner on Virustotal[13]. This also collaborates with the fact that Socat shares the same commandline characteristics and the fact that Socat was also found on the same server (http[://]193.34.167.245/c00n/socat). Running the tool Socat (or a modified version of it) targeting known C&C servers of Sea Turtle resulted mostly in the HTTP response '@8.8.8.8:443'. Since the code checks if the start of the string starts with '@', this output is ignored. As shown in Table 2, the C&C servers of Sea Turtle returned the IP-addresses and a domain name related to DNS services of Google, during the time of writing.

Host	Request URI	Response
93.115.22[.]212	sy.php	@8.8.8.8:443
95.179.176[.]250	sy.php	@8.8.8.8:443
lo0.systemctl[.]network	ssl.php	https[://]dns.google/ssl.php

Table 2 - The response returned by command-and-control servers used by Sea Turtle

At the time of writing it's unknown if these C&C servers are used to setup C&C channels for a long period by changing from C&C server when necessary of if they serve use in other campaigns.

Recommendations

During analysis of the campaigns by Sea Turtle, multiple observations were made. These observations all introduced cyber security risks, or directly contribute possibility of conducting similar attacks. Therefore Hunt & Hackett recommends organizations such as telecommunication providers, ISPs and managed service provider within the IT domain, to address the following recommendations to reduce both the attack surface as well as the likelihood of becoming a victim of this threat actor.

- Deploy EDR and monitor systems for network connections executed processes, file creation/modification/deletion and account activity, and store logfiles in a central location. Ensure sufficient storage capacity for historic forensic investigation purposes.
- Create and enforce a password policy with adequate complexity requirements for specific accounts.
- Store passwords in a secrets management system, that can also be used by development environments.
- Limit logon attempts on accounts to reduce the chance of successful brute force attacks.
- Enable 2FA on all externally exposed accounts.
- Keep software up to date to reduce number of vulnerabilities in externally exposed systems.
- Reduce the number of systems that can be reached over internet using SSH. Where this is still necessary, it is recommended to implement an SSH-logon rate-limit.
- Implement egress network filtering to prevent malicious processes such as reverse shells to successfully sent network traffic to not-allowed IP-addresses.

Appendix 1: Indicators of Compromise

This appendix provides an overview of the indicators of compromise that have been observed by Hunt & Hackett while tracking the threat actor Sea Turtle, in addition to indicators published by PwC[5] and StrikeReady[6].

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	A modified version of the tool Socat used by Sea Turtle to setup a command-and-control channel.

Table 3 - Indicators of compromise of the threat actor Sea Turtle

References

[1] DNS Hijacking Abuses Trust In Core Internet Service - Cisco Talos (talosintelligence.com)

[2] Microsoft Digital Defense Report (2021)

[3] How Microsoft Names Threat Actors (microsoft.com)

[4] Η Εθνική Αρτή Ανηιμεηώπιζης Ηλεκηρονικών Επιθέζεων μας ενημέρωζε για ηα παρακάηω

[5] The Tortoise and The Malwahare - PwC (pwc.com)

[6] Pivoting through a Sea of indicators to spot Turtles - Strike Ready (blog.strikeready.com)

[7] Exclusive: Hackers acting in Turkey’s interests believed to be behind recent cyberattacks - Reuters

[8] 62.115.255[.]163

[9] 193.34.167[.]245

[10] https://www.virustotal.com/gui/file/293703318fab4ad56124d37e6c93d1aecbce4c656782c40fce5d67f3b4149558/details

[11] https[://]github.com/jacksp7/webtest/

[12] https://www.adminer.org/

[13] https://www.virustotal.com/gui/file/71c81cb46dd1903f12f3aef844b0fc559f31e2f613a8ae91ffb5630bc7011ef5/community