Sea Turtle keeps on swimming, finds new victims, DNS hijacking techniques

blog.talosintelligence.com/sea-turtle-keeps-on-swimming

Paul Rascagneres July 9, 2019

By Paul Rascagneres

Tuesday, July 9, 2019 10:07

Threat Advisory

By Danny Adamitis with contributions from Paul Rascagneres.

Executive summary

After several months of activity, the actors behind the "Sea Turtle" DNS hijacking campaign are not slowing down. Cisco Talos recently discovered new details that suggest they regrouped after we published our initial findings and coverage and are redoubling their efforts with new infrastructure. While many actors will slow down once they are discovered, this group appears to be unusually brazen, and will be unlikely to be deterred going forward.

Additionally, we discovered a new DNS hijacking technique that we assess with moderate confidence is connected to the actors behind Sea Turtle. This new technique is similar in that the threat actors compromise the name server records and respond to DNS requests with falsified A records. This new technique has only been observed in a few highly targeted operations. We also identified a new wave of victims, including a country code top-level domain (ccTLD) registry, which manages the DNS records for every domain uses that particular country code, that access was used to then compromise additional government entities. Unfortunately, unless there are significant changes made to better secure DNS, these sorts of attacks are going to remain prevalent.

New DNS hijacking technique

Talos now has moderate confidence that the threat actors behind Sea Turtle have been using another DNS hijacking technique. This new technique has been used very sparingly, and thus far have only identified two entities that were targeted in 2018, though we believe there are likely more.

This new technique once again involved modifying the target domain's name server records to point legitimate users to the actor-controlled server. In this case, the actor-controlled name server and the hijacked hostnames would both resolve to the same IP address for a short period of time, typically less than 24 hours. In both observed cases, one of the hijacked hostnames would reference an email service and the threat actors would presumably harvest user credentials. One aspect of this technique that makes it extremely difficult to track is that the actor-controlled name servers were not used across multiple targets — meaning that every entity hijacked with this technique had its own dedicated name server hostname and its own dedicated IP address. Whereas previously reported name server domains such as ns1[.]intersecdns[.]com were used to target multiple organizations.

In one case, a private organization primarily used a third-party service as their authoritative name server. Then, for a three-hour window in January 2018, their name server records were changed to a name server hostname that mimicked a slightly different version of the organization's name. During that three-hour window, the actor-controlled IP address hosted three hostnames, the two actor-controlled name servers and the webmail hostname. This would allow the threat actors to perform a man-in-the-middle (MitM) attack, as outlined in our previous post, and harvest credentials. This technique was also observed against a government organizations in the Middle East and North African region.

Continued activity against ccTLD

The Institute of Computer Science of the Foundation for Research and Technology - Hellas (ICS-Forth), the ccTLD for Greece, acknowledged on its public website that its network had been compromised on April 19, 2019. Based on Cisco telemetry, we determined that the actors behind the Sea Turtle campaign had access to the ICS-Forth network.

Cisco telemetry confirmed that the actors behind Sea Turtle maintained access to the ICS-Forth network from an operational command and control (C2) node. Our telemetry indicates that the actors maintained access in the ICS-Forth network through at least April 24, five days after the statement was publicly released. Upon analysis of this operational C2 node, we determined that it was also used to access an organization in Syria that was previously redirected using the actor-controlled name server ns1[.]intersecdns[.]com. This indicates that the same threat actors were behind both operations.

We also saw evidence that the threat actors researched the open-source tool PHP-Proxy. Notably, this particular C2 node searched for both blog.talosintelligence.com and ncsc.gov.uk, presumably to view Talos' previous reports on DNS hijacking and this DNS hijacking advisory from the United Kingdom's National Cyber Security Centre.

New actor-controlled nameserver

We recently discovered a new actor-controlled nameserver, rootdnservers[.]com, that exhibited similar behavior patterns as name servers previously utilized as part of the Sea Turtle campaign. The domain rootdnservers[.]com was registered on April 5, 2019 through the registrar NameCheap. The new actor-controlled name server rootdnservers[.]com was utilized to perform DNS hijacking against three government entities that all used .gr, the Greek ccTLD. It's likely that these hijackings were performed through the access the threat actors obtained in the ICS-Forth network. Below is a table showing the three most recent actor-controlled name servers that we have associated with this activity and their current operational status.

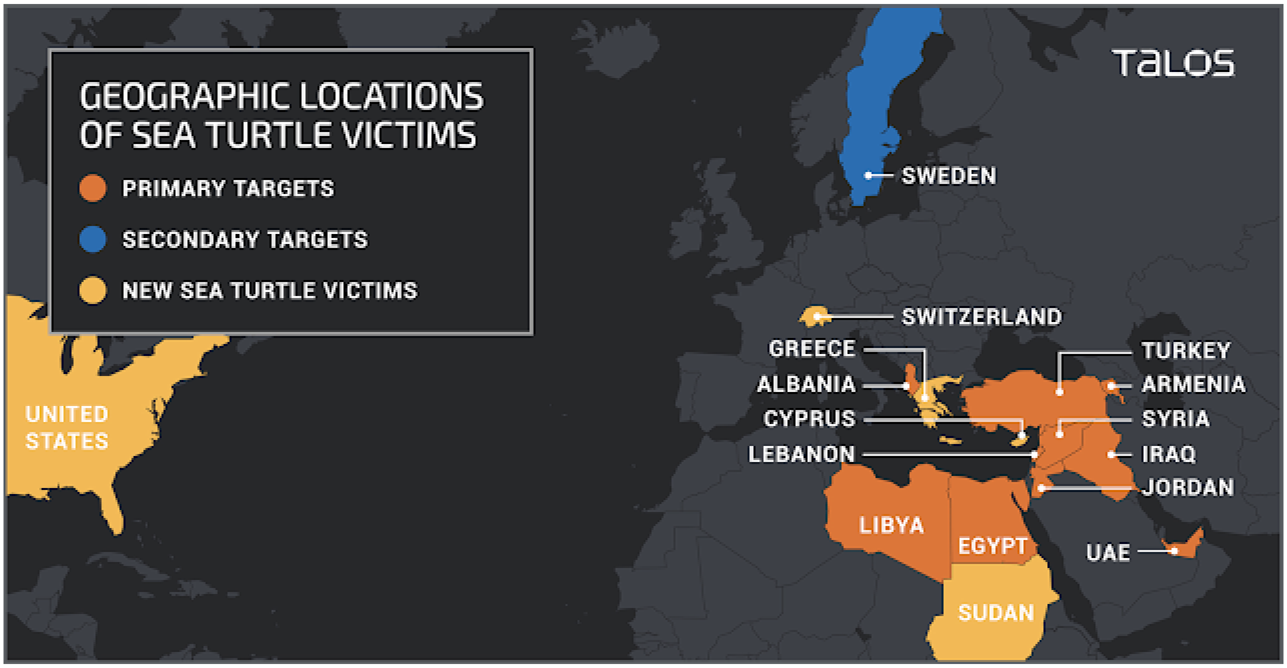
Hostnames	IP addresses	Operational Status
ns1[.]rootdnservers[.]com.	45[.]32[.]100[.]62	Active
ns2[.]rootdnservers[.]com.	45[.]32[.]100[.]62	Active
ns1[.]intersecdns[.]com	95[.]179[.]150[.]101	Inactive
ns2[.]intersecdns[.]com	95[.]179[.]150[.]101	Inactive

New IP addresses associated with man-in-the-middle activity

By identifying the targeted domains, we were able to identify the hijacked hostnames and the corresponding actor-controlled MitM nodes. The threat actors, again employing previously documented tradecraft, by performing a "certificate impersonation" technique. This is where the threat actors procure an SSL certificate for the targeted hostname from a different SSL provider. Below is a table showing the dates and associated IP addresses.

Date	IP address
April 13, 2019	95[.]179[.]131[.]225
April 16, 2019	95[.]179[.]131[.]225
April 11, 2019	95[.]179[.]131[.]225
April 11, 2019	140[.]82[.]58[.]253
April 10, 2019	95[.]179[.]156[.]61

Updated victimology



Since our initial report, Sea Turtle has continued to compromise a number of different entities to fulfill their requirements. We have identified some of the new primary targets as:

- Government organizations

- Energy companies
- Think tanks
- International non-governmental organizations
- At least one airport

In terms of secondary targets, we have seen very similar targets as those previously reported, such as telecommunications providers, internet service providers and one registry.

Coverage and mitigations

In order to best protect against this type of attack, we compiled a list of potential actions. We have included additional security recommendations, that were highlighted by Bill Woodcock during his presentations on DNS/IMAP attacks.

- We recommend implementing multi-factor authentication, such as DUO, to secure the management of your organization's DNS records at your registrar, and to connect remotely to your corporate network via a Virtual Private Network (VPN).
- Talos suggests a registry lock service on your domain names, which will require the registrar to provide an out-of-band confirmation before the registry will process any changes to an organization's DNS record.
- DNSSEC sign your domains, either in-house, or using a DNS service provider which performs DNSSEC key-management services.
- DNSSEC validate all DNS lookups in your recursive resolver, either using in-house nameservers, or a service like Cisco Umbrella / OpenDNS.
- Make Internet Message Access Protocol (IMAP) email servers accessible only from your corporate LAN and to users who have already authenticated over a VPN.
- If you suspect you were targeted by this type of activity, we recommend instituting a network-wide password reset, preferably from a computer on a trusted network.
- Lastly, network administrators can monitor passive DNS record on their domains, to check for abnormalities.

Indicators of compromise

IP address	Characterization	Date Range
185[.]64[.]105[.]100	Operational Node	March - April 2019
178[.]17[.]167[.]51	Operational Node	June 2019
95[.]179[.]131[.]225	Mitm Node	April 2019

140[.]82[.]58[.]253	Mitm Node	April 2019
95[.]179[.]156[.]61	Mitm Node	April 2019
196[.]29[.]187[.]100	Mitm Node	December 2018
188[.]226[.]192[.]35	Mitm Node	January 2018
ns1[.]rootdnservers[.]com	Actor-controlled nameserver	April 2019
ns2[.]rootdnservers[.]com	Actor-controlled nameserver	April 2019
45[.]32[.]100[.]62	Hosted malicious nameserver	April 2019
ns1[.]intersecdns[.]com	Actor-controlled nameserver	February - April 2019
ns2[.]intersecdns[.]com	Actor-controlled nameserver	February - April 2019
95[.]179[.]150[.]101	Hosted malicious nameserver	February - July 2019