On Sea Turtle campaign targeting Greek governmental organisations

threatintel.eu/2020/02/25/on-sea-turtle-campaign-targeting-greek-governmental-organisations-timeline

andreas.sfakianakis 25 February 2020

On 23 February 2020, greek news media reported that Greece Prime Minister's office, the Ministry of Foreign Affairs, the National Intelligence Service and the Greek Police were the targets of an international cyber espionage campaign in April 2019 named Sea Turtle. This is one of the most significant cyber espionage activities against Greece that is publicly known. Sea Turtle campaign has been initially reported by Cisco Talos Intelligence Group last year.

See the below timeline:

1. *17 April 2019*: Talos reported the initial findings related to Sea Turtle campaign. Talos investigation revealed that at least 40 different organizations across 13 different countries (mostly located primarily in the Middle East and North Africa) were compromised during this campaign. Talos also assessed that this campaign was carried out by an advanced, state-sponsored actor that seeks to obtain persistent access to sensitive networks and systems. Finally, Talos assessed that Sea Turtle operations were distinctly different and independent from the operations performed by DNSpionage campaign, which was reported on in November 2018.
   See link

2. *19 April 2019*: ICS-FORTH is the institution that manages the .gr and .ελ top-level domains for Greece. ICS-FORTH notified the domain name owners about a cyber attack against the registry of .gr and .ελ domain names.
   See link (in greek)
3. *9 July 2019*: Talos reported additional findings of Sea Turtle campaign that included the targeting of ICS-FORTH. According to Talos, the adversaries behind the Sea Turtle campaign had access to the ICS-FORTH network at least until 24 April 2019 (for another five days after ICS-FORTH publicly disclosed the incident on 19 April 2019).
   See link
4. *27 January 2020*: Reuters reported that hackers acting in the interests of the Turkish government believed to be behind cyber-attacks against Greek government's email services (among other targets). According to senior Western officials, the above assessment was conducted based on victimology, infrastructure, and other confidential information.
   See link
5. *23 February 2020*: Greek media reports that during April 2019 the domains @primeminister[.]gr (Greek Prime Minister), @mfa[.]gr (Greek Ministry of Foreign Affairs), @nis[.]gr (Greek Intelligence Service) and @astynomia[.]gr (Greek Police) have been impacted by Sea Turtle campaign. According to the article, the victims reckoned that an email malfunction was due to a cyberattack against the .gr and .el domain names registry, whose technical support is provided by ICS-FORTH. While there are a lot of speculations, the impact of the cyber-attack is still not known.
   See link
   See link (in greek)

Based on the public information available, one could assess with low confidence that the intrusion activity reported by Reuters (#4) is linked to the Sea Turtle campaign because of the similar TTP used (DNS hijacking technique), victimology (Greece, Cyprus, Iraq, Ministries of foreign affairs, Intelligence agencies, governmental email services), and attack timestamp (early 2019 for Greek governmental organisations).

One major lesson learned that needs to be captured is what Christopher Glyer mentioned in Twitter:

> "They reckoned that the malfunction was due to a cyberattack against the .gr and .el domain names registry, whose technical support is provided by FORTH"
>
> Small companies running domain registration is a/the weak underbelly of the internet that few consider when building defenses https://t.co/gBGjkRVJb7
>
> — Christopher Glyer (@cglyer) February 24, 2020

Securing (inter)national critical infrastructure should be of utmost priority. This infrastructure will inevitably be targeted by capable adversaries and potentially compromised (assume breach mentality). What we can do as defenders is to better prepare and develop the capabilities needed to prevent and respond to such activities. This requires the relevant strategy and commitment from a resources perspective (think about people, processes and technology).

Moreover, it is also important to use the proper narrative when talking in public about such security incidents. Attribution in the cyber space is a difficult and an expensive activity. During the past month, there was a lot of media reporting in Greece about "*cyber-attacks coming from Turkey*" presenting no evidence or no structure approach on the attribution. "*Turkey did it/Turkish hackers did it*" was such a wrong way to present it. In cyber space, infrastructure can be reused and we have also seen false flag operations where adversaries try to fool the victim on their identity. Public discussion on such cyber security incidents should be more professional and responsible to prevent circulation of information that is not backed by evidence or a solid assessment.