Talos reports on new, sophisticated hacking group manipulating DNS systems

April 22 2019, by Nancy Cohen

Credit: Talos

A hacking group has gone after government domains—they targeted 40 government and intelligence agencies, telecoms and internet giants in 13 countries for more than two years, said reports. This is a new, sophisticated team of hackers spying on dozens of targets, said *Wired*.

"This is a new group that is operating in a relatively unique way that we have not seen before, using new tactics, techniques, and procedures,"

Craig Williams, director, outreach at Cisco Talos, told *TechCrunch*.

Researchers identified the campaign and dubbed it "Sea Turtle." They are at Cisco's Talos cybersecurity unit. Zack Whittaker, security editor at *TechCrunch*, expanded on the discoveries: the unit "sounded the alarm after discovering a previously undiscovered hacker group targeting a core part of the internet's infrastructure."

How Sea Turtle works: It targets companies by hijacking their DNS—pointing a target's domain name to a malicious server instead of to its intended target, said Anthony Spadafora, *TechRadar*.

Ars Technica expanded on explaining what takes place:

Dan Goodin wrote, "the attackers first alter DNS settings for targeted DNS registrars, telecom companies, and ISPs—companies like Cafax and Netnod. The attackers then use their control of these services to attack primary targets that use the services."

Actually, the exploit was leveraging some long-known flaws in DNS, said Spadafora, and those flaws can be used "to trick unsuspecting victims into imputing their credentials on fake login pages."

He said that "By using their own HTTPS certificate for the target's domain, the attackers can make a malicious server appear genuine."

According to Talos, the hackers compromised the Swedish DNS provider Netnod. The Talos team blogged that " In another case, the attackers were able to compromise NetNod, a non-profit, independent internet infrastructure organization based in Sweden." *Ars Technica* said Netnod is also the operator of i.root, one of the Internet's foundational 13 DNS root servers.

According to Talos, the hackers used this technique to compromise the Swedish DNS provider Netnod as well as one of the 13 root servers that powers the global DNS infrastructure.

This was a "highly advanced" hacker group, and "likely" backed by a nation-state.

The Talos team posted a blog on April 17 with a note of concern of what may come:

"While this incident is limited to targeting primarily national security organizations in the Middle East and North Africa, and we do not want to overstate the consequences of this specific campaign, we are concerned that the success of this operation will lead to actors more broadly attacking the global DNS system."

Goodin noted, meanwhile, that "One of the things that makes Sea Turtle more mature is its use of a constellation of exploits that collectively allow its operators to gain initial access or to move laterally within the network of a targeted organization."

What has Talos recommended as a mitigation strategy?

Talos suggested using a registry lock service, to require an out-of-band message before any changes can occur to an organization's DNS record.

Should your registrar not offer a registry lock service, Talos recommended multi-factor authentication, e.g., DUO, to access the organization's DNS records.

"If you suspect you were targeted by this type of activity intrusion, we recommend instituting a network-wide password reset, preferably from a computer on a trusted network. Lastly, we recommend applying patches,

especially on internet-facing machines. Network administrators can monitor passive DNS record on their domains, to check for abnormalities."

More information: blog.talosintelligence.com/2019/04/seaturtle.html