DNS Hijacking Perils: How to Address Threats Like the Sea Turtle Cyberespionage Campaign with DNS & IP Lookup

Posted on February 6, 2020

Cyber attackers continuously enhance their tools, tactics, and procedures (TTPs) to remain undetected for as long as they can while in their targets' networks. Despite the increased sophistication of attacks, however, old techniques die hard and keep causing extensive damage. Case in point: Domain Name System (DNS) hijacking remains a favored attack type among threat actors.

This post provides reasons why cybercriminals never seem to get tired of launching DNS hijacking attacks. We also take a close look at how cyberspies hijacked entire nations' domains and provide recommendations to potential targets, notably through the use of tools like DNS Lookup API and IP Geolocation API, so they can avoid the same fate as the victims of the Sea Turtle Cyberespionage Campaign.

Table of Contents

- A Primer: Why DNS Hijacking?
- The Case Facts: How DNS Hijacking Enabled the Sea Turtle Cyberespionage Campaign
- Featured Tools: How DNS Lookup API and IP Geolocation API Can Fend Off DNS Hijacking Attacks
- The Verdict: Conclusion and Countermeasures

A Primer: Why DNS Hijacking?

In a nutshell, DNS is an Internet protocol that functions much like a phonebook. It translates URLs into their corresponding IP addresses. And so, when a domain is attacked, threat actors successfully affect not just a single user but everything connected to that user's network.

DNS hijacking, also known as a “redirection attack,” occurs when DNS queries are incorrectly resolved to redirect unknowing users to malicious sites. It can be done through the following categories of attacks.

- **Man-in-the-middle (MitM):** In this scenario, attackers intercept DNS requests from a system to a DNS server to point users to malicious sites instead.

- **Use of malware:** In this case, threat actors entice their targets to click on a link or download an attachment sent via email. When clicked on or downloaded, the link or attachment installs a piece of malware on the user’s computer. That malware then modifies the computer’s DNS settings to lead users to malicious websites.

- **Router DNS hijacking:** At other times, attackers exploit firmware vulnerabilities in routers to divert all traffic that passes through to malicious sites. In some cases, all they need to do is modify the router settings to set their intended redirects, which is easy to do when users do not change their routers’ default passwords.

- **Rogue DNS servers:** More sophisticated threat actors hack DNS servers to modify their records, so that all users under the affected domains are taken to malicious destinations.

Attackers often employ DNS hijacking in campaigns because most organizations do not monitor DNS requests.

What Can Happen to the Users of Hijacked Domains?

DNS hijacking can lead to the following:

- Users end up on phishing sites where they may carelessly hand over their personally identifiable information (PII) to cybercriminals.

- Attackers can inject malicious scripts into the sites hosted on the domains, causing more infections on visitors’ computers.

- Threat actors can turn the sites hosted on the domains into malware hosts.
- Attackers can quickly intercept emails sent from and directed to users of the affected domains, which can lead to data leaks.
- Threat actors can easily siphon off user credentials, especially those saved in browsers or on affected systems.

The Case Facts: How DNS Hijacking Enabled the Sea Turtle Cyberespionage Campaign

The Sea Turtle Cyberespionage Campaign is a state-sponsored attack that presumably began in January 2017 and is still ongoing. Unlike other campaigns, however, despite its exposure, its perpetrators remain unfazed.

Most threat actors lie low when their operations are laid bare. Instead of hiding, though, the actors behind Sea Turtle only enhanced their DNS hijacking tactics and even added more entities to their target list.

Attack Stages

The technical analysis of the attack shows that unpatched old vulnerabilities and spearphishing emails were employed to enter target networks. Once inside the target network, attackers moved laterally to search for credentials that they planned to exfiltrate later.

In the next stage, the attackers used the stolen credentials to access the targets' DNS records and altered their nameservers to redirect communications to servers under their control. Every time a user enters his credentials into any page, these are first sent to the attackers before reaching their intended destinations.

Attackers also created MitM servers that mimicked legitimate services to harvest more user credentials for future use. They even crafted Secure Sockets Layer (SSL) certificates to make their MitM servers appear valid. These methods allowed them to collect even users' virtual private network (VPN) credentials, which later on enabled them to access the target networks remotely without being detected.

Affected Organizations

The Sea Turtle Campaign targeted and compromised around 40 high-profile organizations, including ministries of foreign affairs, military institutions, intelligence agencies, and energy-related organizations from 13 countries in the Middle East and Africa. To get to them, the attackers first infiltrated DNS registrars, telecommunications companies, and Internet service providers (ISPs).

Deception Point: What Made the Campaign Successful?

The Sea Turtle Campaign is an excellent example of how attackers can effectively abuse insufficiently secured DNS infrastructure to pull off a massive cyberespionage operation without being detected immediately.

Once infiltration is complete, the ease of intercepting traffic can be one of the reasons why we continue to see DNS hijacking attacks to this day. Time and again, redirecting traffic to hacker-owned servers has proven to be an effective means to gather user credentials that allow attackers to dig deeper and deeper into target networks. And the more connected the initial target is (i.e., DNS registrars, telecommunications companies, and ISPs), the greater the gain (i.e., access to

their high-profile clients).

The Sea Turtle operators are not the first to use this tactic, in any case. We have, for instance, seen attackers breach a reseller of Melbourne IT to get to their real targets. By compromising the company's DNS servers, they gained access to the networks of the New York Times, Twitter, and Huffington Post, among others. The result? End-users accessing the affected sites were led to malicious sites.

All in all, a company's domain is a crucial part of its infrastructure. When its security is overlooked, its weaknesses can be abused, giving threat actors a way into a network. While there is no silver bullet against DNS hijacking, preventing its occurrence and mitigating associated risks is doable.

Organizations can further protect their networks by integrating tools such as DNS Lookup API and IP Geolocation API into their security processes. How? Read on to find out.

Featured Tools: How DNS Lookup API and IP Geolocation API Can Fend Off DNS Hijacking Attacks

Let us take a closer look at how DNS Lookup API can be of help to organizations' cybersecurity teams. This tool allows users to map any domain to an IP address.

- 1. First, use one of the known domains listed as an indicator of compromise (IoCs) — ns1[.]intersecdns[.]com — into DNS Lookup API (the full API response is available at the end of the piece).

- 2. Five DNS records are associated with the domain. Each of them shows data that cybersecurity team members can take note of for potential blocking. This information includes related IP addresses.

- 3. We subjected the other three identified domains—ns2[.]intersecdns[.]com, ns1[.]lcjcomputing[.]com, and ns2[.]lcjcomputing[.]com—to the same checks. After the

queries, we obtained the following IP addresses:

- 198.54.117.197
- 198.54.117.198
- 198.54.117.199
- 198.54.117.200

As these IP addresses emerged from known IoCs of the Sea Turtle Campaign, organizations may want to avoid interacting with them and their connected domains listed above. Cybersecurity teams may also find it wise to add them to their blocklists.

As a second step of our analysis, we want to find out more about the attack and identify other related information so we used IP Geolocation API. This tool allows users to check the attackers' geographic locations.

- 1. Using 198.54.117.197 as a search string, here is the result output (note that the ouput here is the same for 198.54.117.198, 198.54.117.199, and 198.54.117.200):

Using 198.54.117.197 as a search string

Image not found or type unknown

- 2. Having looked up the other addresses with the tool, we now know that the four IPs point to a location in the U.S. It looks like it is not tied to a specific domain, however. Apart from an IP address's geolocation, the API also reveals associated domains. These could be added to cybersecurity specialists and law enforcement agencies' lists of IoCs to investigate.

- 3. We also know that the attackers used this IP address "45.32.100.62." We ran it through the tool and got this result:

We also know that the attackers used this IP address “45.32.100.62.”g

Image not found or type unknown

We also know that the attackers used this IP address “45.32.100.62.”g

Image not found or type unknown

- 4. As shown above, the IP address points to a location in Singapore and is connected to a company called Choopa, LLC. It also resolved to the domain choopa[.]com. We ran the other IP addresses in the list of IoCs on the tool and found these connected domains:
    - digitalocean[.]com
    - reliablesite[.]net
    - netnod[.]se
    - linode[.]com
    - belcloud[.]net

- 5. We then ran WHOIS searches on the domains above to find out more about them. Here is the result for Digital Ocean:

We then ran WHOIS searches on the domains above to find out more about them.

Image not found or type unknown

- 6. Digital Ocean is a legitimate cloud computing company. While a more thorough investigation is required before drawing any solid conclusions, it’s not impossible that the attackers may be mimicking or have compromised it to progress their attacks further. It is,

after all, a common tactic to take advantage of legitimate services to evade detection and blocking. By piggybacking on legitimate communications, malicious activities remain hidden even to the most discerning eyes. All the other four domains were legitimate companies as well and were just being used as camouflage, it seems.

The Verdict: Conclusion and Countermeasures

The Sea Turtle cyberespionage campaign succeeded because the attackers:

- Chose to hit the right initial targets to get to their ultimate victims
- Attacked the core of the organizations—their DNS infrastructure, which allowed them to add, remove, and delete records or to redirect domains to carry out subversive MitM attacks
- Stole valid user credentials through ingenious means so they can create valid SSL certificates for their malicious servers
- Hid behind legitimate companies so their communications would be impossible or at least very hard to block

Threat actors often employ DNS hijacking as an initial step for large-scale attacks because it is not easy to stop. In such cases, proactive solutions and preventive measures are likely to be more effective in lessening their impact. Here is a list of best practices that all organizations can benefit from:

- Keep all systems up-to-date by regularly applying patches. Using intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) is a good start. Regular vulnerability scanning and penetration testing also help. Remember that security bugs are always exploited to serve as points of entry into target networks.
- Log DNS requests as this was the loophole the campaign’s operators took advantage of.

You can use our Reverse IP/DNS API for that.

- Always use secure connections (i.e., HTTPS) when visiting sites. Go the extra mile even and use HTTP Strict Transport Security (HSTS) to allow only encrypted connections.
- Set registry-level locks to avoid nameserver, domain, and similar records from being modified without the owners' knowledge. This process provides an extra layer of protection against this particular attack. If your registrar does not offer this option, use a multifactor authentication (MFA) tool.
- Use security solutions that can detect malicious URLs, spam, malware, and exploits.
- Regularly check your DNS records for anomalies that may suggest you are currently being attacked.
- Check your entire network for potential attack vectors or security loopholes that threat actors can abuse. You can use our Threat Intelligence Platform to identify open ports, security vulnerabilities, dangling records, and system and record misconfigurations for that.
- Stay abreast of the latest security threats and cyberattacks not only to enhance your awareness but more so to gather threat intelligence.

Traditional security solutions such as IDSs and IPSs may not work that well in combating a DNS hijacking attack since they do not monitor DNS requests. And with the increasing number of sophisticated campaigns such as Sea Turtle using DNS hijacking, organizations need to add extra layers of protection to their networks.

As our demonstrations showed, DNS Lookup API and IP Geolocation API can aid in fending off DNS hijacking attacks and their nasty consequences. Even better, they can be integrated into existing security solutions and frameworks to make sure cyber attackers won't be able to exfiltrate confidential data from your networks.

For more information on DNS Lookup API and IP Geolocation API, contact us at support@whoisxmlapi.com.

Appendix

Full API response for DNS Lookup API when using "ns1.intersecdns[.]com" as the search string:


```
{
  "DNSData": {
    "domainName": "ns1.intersecdns.com",
    "types": [
      -1
    ],
    "dnsTypes": "_all",
    "audit": {
      "createdDate": "2019-11-25 09:58:25.974 UTC",
      "updatedDate": "2019-11-25 09:58:25.974 UTC"
    },
    "dnsRecords": [
      {
        "type": 1,
        "dnsType": "A",
        "name": "ns1.intersecdns.com.",
        "ttl": 1800,
        "rRsetType": 1,
        "rawText": "ns1.intersecdns.com.\t1800\tIN\tA\t198.54.117.200",
        "address": "198.54.117.200"
      },
      {
        "type": 1,
        "dnsType": "A",
        "name": "ns1.intersecdns.com.",
        "ttl": 1800,
        "rRsetType": 1,
```

```
      "rawText": "ns1.intersecdns.com.\t1800\tIN\tA\t198.54.117.198",
      "address": "198.54.117.198"
    },
    {
      "type": 1,
      "dnsType": "A",
      "name": "ns1.intersecdns.com.",
      "ttl": 1800,
      "rRsetType": 1,
      "rawText": "ns1.intersecdns.com.\t1800\tIN\tA\t198.54.117.199",
      "address": "198.54.117.199"
    },
    {
      "type": 1,
      "dnsType": "A",
      "name": "ns1.intersecdns.com.",
      "ttl": 1800,
      "rRsetType": 1,
      "rawText": "ns1.intersecdns.com.\t1800\tIN\tA\t198.54.117.197",
      "address": "198.54.117.197"
    },
    {
      "type": 2,
      "dnsType": "NS",
      "name": "ns1.intersecdns.com.",
      "additionalName": "dns102.registrar-servers.com.",
      "ttl": 1797,
      "rRsetType": 2,
      "rawText": "ns1.intersecdns.com.\t1797\tIN\tNS\tdns102.registrar-se
      "target": "dns102.registrar-servers.com."
    },
    {
      "type": 2,
      "dnsType": "NS",
      "name": "ns1.intersecdns.com.",
      "additionalName": "dns101.registrar-servers.com.",
      "ttl": 1797,
      "rRsetType": 2,
      "rawText": "ns1.intersecdns.com.\t1797\tIN\tNS\tdns101.registrar-se
      "target": "dns101.registrar-servers.com."
    },
```

```
        {
          "type": 6,
          "dnsType": "SOA",
          "name": "ns1.intersecdns.com.",
          "ttl": 1800,
          "rRsetType": 6,
          "rawText": "ns1.intersecdns.com.\t1800\tIN\tSOA\tdns101.registrar-s
          "admin": "support.namecheap.com.",
          "host": "dns101.registrar-servers.com.",
          "expire": 8640,
          "minimum": 120,
          "refresh": 28800,
          "retry": 7200,
          "serial": 1574675457
        },
        {
          "type": 2,
          "dnsType": "NS",
          "name": "ns1.intersecdns.com.",
          "additionalName": "dns101.registrar-servers.com.",
          "ttl": 1800,
          "rRsetType": 2,
          "rawText": "ns1.intersecdns.com.\t1800\tIN\tNS\tdns101.registrar-se
          "target": "dns101.registrar-servers.com."
        },
        {
          "type": 2,
          "dnsType": "NS",
          "name": "ns1.intersecdns.com.",
          "additionalName": "dns102.registrar-servers.com.",
          "ttl": 1800,
          "rRsetType": 2,
          "rawText": "ns1.intersecdns.com.\t1800\tIN\tNS\tdns102.registrar-se
          "target": "dns102.registrar-servers.com."
        }
      ]
    }
  }
```