Threat Intelligence

Chosen Tactics:

1. Browser Session Hijacking/Cookie Hijacking - Dridex (Bugat v5) Botnet Takeover Operation
2. Compromise Infrastructure: DNS Server - Celer Network cBridge Users Lose $240k in DNS Hijack, CELR Lists on Coinbase
    a. Event: “DNS cache poisoning attack on cBridge’s frontend UI”

1 - Describe the incident indicators leading towards the compromise

Browser Session Hijacking

An indicator of session hijacking can be seen through suspicious links sent via email or on the site you’re currently logged into. These links may execute malicious code which can send your session cookie to an attacker, essentially giving them access to your login session. This is dangerous because there is no real indicator of this happening. The attacker is completely undetected while they take over your session.

Compromise Infrastructure: DNS Server

One of the incidents that may mark an DNS compromise is the fact that some or all URLs are being redirected incorrectly or simply not in service.

You can check for a DNS compromise by accessing the targeted DNS record (usually a domain) via different networks. If compromised, the infected DNS server will hand out incorrect records.

2 - Based on the indicators of compromise, opine to determine the type of virus or malware used in the attack.

Browser Session Hijacking

Browser hijacking is an exploitation of security in cookies. Software can be injected by adversaries through links sent to users or processes that reveal their session cookie. This is known as cross-site-scripting. Through scripting, attackers can also inherit HTTP session and browser pivoting, which can bypass 2-factor-authentication.

Compromise Infrastructure: DNS Server

Infecting a DNS is not a virus in the colloquial sense, it does not install more malware or ask for money to unlock the system. It has the aspects of an *Injection*

attack where records are altered and are used by people as if they were the original records.

3 - Name and brief description of the attack method, what does it do?

Browser Session Hijacking/Cookie Hijacking

When a user session is taken over by an attacker using techniques such as IP spoofing, client-side attacks, or session sniffing to retrieve the session cookie. When the attacker has retrieved the user session cookie, they can now discreetly take over the session, granting them access to valuable user information, which they can then choose to do whatever they want with.

Compromise Infrastructure: DNS Server

By taking control of a DNS server threat actors are able to alter DNS records. If they are able to take control of an authoritative nameserver they can alter Type-A and Type-CNAME records to really cause issues with customers trying to access a company website.

4 - What type of attack method?

Browser Session Hijacking:

Attack method: Session Hijacking/Process Injection

Compromise Infrastructure: DNS Server

Attack type: Compromise Infrastructure

Compromised infrastructure allows an adversary to commit operations on the company's infrastructure whilst blending in with the regular traffic. Moreover the issue with Compromised Infrastructure is that it is harder for a investigator to tie the crime back to the threat actors.

5 - Who created it?

Browser Session Hijacking:

While it is unknown who created it, the earliest entry I could discover was Firesheep, a Mozilla Firefox extension that gave session hijackers an easy access point to attack users over unencrypted public Wi-Fi.

Compromise Infrastructure: DNS Server

Unknown

6 - How is it triggered?

Browser Session Hijacking:

It is triggered when a hijacker obtains a user's session cookie. This can be done through methods like IP spoofing, brute force attacks, or man-in-the-middle attacks such as session/packet sniffing, cross-site-scripting (XSS), and session puzzling.

Compromise Infrastructure: DNS Server

It is triggered when a hacker has access to a company DNS server. This can happen in many ways. For one they gain access to the DNS server by hacking something else (moving laterally) or they may directly target an exploit on the DNS server.

Once they have access they are free to alter records.

7 - According to Mitre Attack, where do we look for forensic evidence sources?

Browser Session Hijacking

According to Mitre Attack, it is possible to check authentication logs to view logins to specific web applications, although determining malicious versus benign logins is difficult if the adversary's activity is similar or matches the user's. It is also possible to monitor process injection against browser applications.

Compromise Infrastructure: DNS Server

Since the DNS server is just a database a NetAdmin can look for incorrect entries to detect DNS poisoning. Another way to find evidence **outside** of the DNS server is to check the DNS caches of the computers that have that DNS server as the default gateway. The DNS records there will also be incorrect.

8 - Describe How it works?

Browser Session Hijacking

An attacker can use various techniques and tactics to steal a user's session cookie. This can be either the fault of the user or the website, or both. If a website saves a user session despite leaving the site, an attacker can easily grab the user's session cookie and steal information. Other methods include sniffing packets to grab the session cookie, injecting malicious scripts or software to inherit the session cookie, HTTP session, and SSL certificates, accessing pages in an unexpected order (session puzzling), guessing the session cookie using predictable tokens such as the user's email or name in other base number systems. What the attacker does with the information after retrieving it is up to them, but usually it involves ransom, selling, or using.

Compromise Infrastructure: DNS Server

When a hacker has control of a DNS server they can delete records which may cause the DNS server to have to spend more time querying higher level DNS servers or it may cause a domain to go down (even partially). A hacker can also stop email services since DNS also contains (MX - Mail Exchange) records. They can also redirect users using a CNAME record mapping.

9 - Under normal circumstances, describe how the device works? Then describe, how does the attack method affect the device? In other words, what does normal look like? When the attack is executed, how does the normal device behavior change?

Browser Session Hijacking

Under normal circumstances, the server will create a session ID which stores the session cookie. A session cookie helps websites remember users, otherwise each request would be treated as a new request. A session hijack will use the session cookies to hijack the user's session. Normal device behavior actually doesn't change at all for the user, the only difference is that the attacker has discreetly taken control over the session.

Compromise Infrastructure: DNS Server

The DNS server is (basically) a database that fetches and records URL:IP mappings. When a url is queries (maybe by the browser) it will check if it has the record caches (and the record has an active TTL). However when infected the hacker can *point* the URL records to a different IP changing the DNS records.

If hackers are able to infect a nameserver anyone accessing this nameserver will be unable to access the website that is being targeted

10 - How is the victim impacted? What damage did it cause?
11 - What was the risk (the consequence) to the company or victim?
12 - Why does it matter?

This answer answers all three.

Browser Session Hijacking

The victim is the consumer/user and in some cases also the company/website used. Through a hijacking, the user is at a potential loss of anything that's been stored in their session on the website. This could be anything from sensitive information, bank account information, SSN, government identification, etc. If a website does not delete session ID and cookies on logout/webpage close, the attacker has even easier access to user information, as they can do it at any time. So overall, a hijacking can occur through user naivety or webpage security risks. It matters because user's are at risk of losing potentially all of their money and assets. This can also affect companies and websites' user trust, as even if it is the fault of the user and not the website, the user may be naive and will believe that security issues were the cause.

Compromise Infrastructure: DNS Server

The victim here is both the customer and the company. For one the customer is unable to get to the website (unless they have visited it recently and it is cached on their local machine). If a company nameserver is hacked then customers will be blocked or redirected from accessing the site or service. This causes monetary damage.

The reason this matters is because temporary outages may cost large companies millions of dollars. Moreover a DNS attack can affect systems that cache DNS addresses. DNS cache entries have a TTL (time-to-line) meaning that if an infected nameserver hands out a falsified DNS record to a user, it will be cached potentially causing the user issues too.

13 - What could/should be done to prevent the incident from happening again?

Browser Session Hijacking

The attack can be mitigated through user training and improving web page security. For one, users should be trained to close web pages when they are

finished using them. This can and will decrease the likelihood of cookie hijacking. Web developers should also increase their levels of security, and ensure that users are not only logged out when they close the page, but also have a logout timer on pages that require more critical information, such as banking, financial, government, or shopping pages.

Compromise Infrastructure: DNS Server

One mitigation strategy is to journal all changes to the DNS server or name server that way if unknown records are added/modified someone can be alerted early.

14 - How does knowing the information help the DFI?

General Answer for both tactics

Timing is critical for any forensic investigations. The more knowledge the DFI has on where to look for certain types of attacks the better the investigation will proceed. For example an adversary can use short time-to-live times on altered DNS records to ensure they are deleted after being used leading to a lower chance of them getting caught. Knowing where to look for these records can help recover malicious activity before it's too late. This example for TTL also applies to persistent cookies.

Moreover, knowing applicable targets(company, individual, …) and what is the objective (passwords, sessions, files, …) also helps the DFI narrow down what tactic was used and allows them to get closer to the APT group that can be responsible for the attack.