COMP2216 Principles of Cyber Security- Cyber Attack Analysis

Username: at2n19
Cyber Attack: Attack on High-profile Websites

Task 1 – Impact and Response Analysis

Impact

A DNS cache poisoning attack occurred in Sri Lanka on the 6th of February 2021, exactly two days after Sri Lanka's official national independence day. While local businesses and news sites comprised the largest number of affected websites, two high profile domains for Google.lk and Oracle.lk were involved as well. The victim websites were redirected to a webpage describing several social issues impacting the Sri Lankan population, and as such, a group of hacktivists was linked to the attack.

Thanks to the redirection, the attackers were able to gain access to several machines within one of the target organisations by stealing credentials used by its employees.
By exploiting the privileges of one of these machines, the attackers defaced the target's website. Besides, the forensic analysis found that the attackers navigated the machine's local directories and exfiltrated sensitive files (whose nature is unknown). The attackers successively disclosed these files to the public.

Thus, it is fairly reasonable to claim that while the attack did not have a significant economic impact (as it was eradicated in a few hours), it considerably affected the availability, integrity, and authenticity of the target's websites and the exfiltrated files' confidentiality.

Response

The attack was detected by the Sri Lankans authorities a few hours after it started, and the public was alerted of the ongoing DNS redirection at 5:49 AM by the Telecommunications Regulatory Commission of Sri Lanka (TRCLS) via a tweet. Besides disclosing the attack, the tweet assured the public that the LK Domain registry was in the process of resolving the issue and that a hotline number for assistance was set up.

At 10.30 AM, the LK Domain registry communicated that the attack was successfully eradicated at 8:30 AM, but nonetheless, the public had still to be cautious as some machines outside the domain registry system may have had the malicious DNS records still cached.

Even though the LK Domain registry's message outlined that the public would be informed about the attack as soon as concrete information is available, details about the attack and the number of impacted domains have not been made public yet.

Besides official communications, several affected Sri Lankans helped spread out information about the ongoing attack via Twitter.

Task 2 - Weaknesses and Attack Techniques Analysis

Weaknesses

#	CWE entry	Justification
1	CWE-330 (Use of Insufficiently Random Values)	This CWE derives directly from the fact that the third-party DNS server was compromised via **CVE-2020-25705**. In addition, the generation of the DNS 16-bit Transaction ID is more predictable than required.
2	CWE-308: Use of Single-factor Authentication	This CWE is referenced via **CAPEC-560** (see below). A number of related CWEs are referenced but this CWE is the most relevant one. Indeed, the use of a single-factor authentication let the adversary trivially compromise the target's employees accounts as acquiring the account's credentials (username, password) was sufficient to gain access.
3	CWE-923: Improper Restriction of Communication Channel to Intended Endpoints	This CWE derives from 'the software used by the victims to connect to the target's domain did not properly ensure that it was communicating with the correct endpoint'. The description of CWE-923 is as follows: 'The software establishes a communication channel to (or from) an endpoint for privileged or protected operations, but it does not properly ensure that it is communicating with the correct endpoint'.

Attack Techniques

#	CAPEC entry	ATT&CK Technique	ATT&CK Tactic	Justification
1	CAPEC-142 (DNS Cache Poisoning)	T1584.002 (Compromise Infrastructure: DNS Server)	TA0042 (Resource development)	Derived from the fact that the adversary compromised a third-party DNS server via **CVE-2020-25705** and run a DNS poisoning attack to tamper with DNS entries corresponding to the target's domain. The adversary aimed to poise the third-party DNS server's cache so that to steal target's employees credentials by redirecting traffic to a malicious server. By definition of the **Resource**

				Development tactic in the ATT&CK KB, the latter seems suitable for the tactic of this entry. The adversary altered the third-party DNS server records for traffic redirection. By definition of the **Compromise Infrastructure: DNS Server** technique in the ATT&CK KB, the latter seems suitable for the technique of this entry. The **CAPEC-142** seems suitable because the adversary ran a DNS cache poisoning attack.
2	CAPEC-569 (Collect Data as Provided by Users) CAPEC-89 (Pharming)	T1056 (Input capture)	TA0006 (Credential Access)	Derived from the fact that the adversary was able to steal credentials used by the target's employees redirecting traffic to a malicious server. The adversary aimed to steal the credentials of target's employees. By definition of the **Credential access** tactic in the ATT&CK KB, the latter seems suitable for the tactic of this entry. The adversary deceived the target's employees into providing input into what they believed to be a genuine service while they were actually redirected to a malicious server. By definition of the **Input capture** technique in the ATT&CK KB, the latter seems suitable for the technique of this entry. The **CAPEC-569** is directly referenced from the Input capture technique.

				The **CAPEC-89** seems suitable because the target's employees are fooled into entering sensitive data into supposedly trusted locations.
3	CAPEC-560 (Use of Known Domain Credentials)	T1078 (Valid accounts)	TA0004 (Privilege escalation)	Derived from 'they discovered that one of these machines was configured and had the permissions to manage and update the contents of the target's website'. The adversary was able to manage and update the contents of the target's website by taking advantage of the permissions of one of the accessed machines. By definition of the **Privilege escalation** tactic in the ATT&CK KB, the latter seems suitable for the tactic of this entry. The adversary was capable of taking advantage of the permissions by simply exploiting the stolen credentials. By definition of the **Valid accounts** technique in the ATT&CK KB, the latter seems suitable for the technique of this entry. The **CAPEC-560** is directly referenced from the Valid accounts technique.

Task 3 - Attack Analysis

The synthetic technical description of this attack does not provide all necessary information for every phase of the Lockheed Martin's kill chain analysis. Such lack of information is filled by using the information contained in the paper **DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels** (https://dl.acm.org/doi/10.1145/3372297.3417280).
It is not guaranteed that the attack was carried out exactly as described in the analysis below but it is fairly reasonable that Keyu Man's paper was used by the attackers as a source of inspiration given that Keyu Man reported fist how the ICMP rate limiter could be used by attackers to perform DNS cache poisoning attacks. Additionally, Keyu Man's paper was published a few months before the attack.

Reconnaissance Phase

The adversary ran an active reconnaissance operation on the third-party DNS server in order to gather precious information that could be used for the later phases of the attack such as:

- DNS server MAC address
- DNS server OS and version
- whether the DNS server deployed DNSSEC
- supported communication protocols
- supported encryption algorithms
- average requests handled per hour

In addition, the attacker needed to know the authoritative name server for the target's domain.

Weaponization Phase

Exactly four weapons were created by the adversary so that as to carry out the three key steps in modern DNS cache poisoning attacks: (1) DNS query issuing, (2) Inferring source port and (3) Extending attack window.

- **DNS query message (DNSm)**: a DNS query message directed to the third-party DNS server asking for a A record of a non-existent subdomain of the target's domain. It supports key step (1) in modern DNS cache poisoning attacks.

- **Probe packet**: a UDP packet directed to the third-party DNS server containing the target's domain authoritative server's IP address as the source address. It supports key step (2) in modern DNS cache poisoning attacks.

- **Verification packet**: a UDP packet directed to the third-party DNS server containing the adversary's IP address as the source address. It supports key step (2) in modern DNS cache poisoning attacks.

- **DNS query extend message (DNSem)**: a DSN query message directed to the target's domain authoritative server containing the third-party DNS server's IP address as the source address. It supports key step (3) in modern DNS cache poisoning attacks.

Delivery Phase

1. The adversary sent the **DNSm** to the third-party DNS server via Network.

2. The adversary carried out the **Inferring port strategy** and contemporaneously sent a large number of **DNSem** to the authoritative server for the target's domain at a higher rate than the configured response rate limit (**RRL**).

Inferring port strategy

Continue the procedure until all 65536 source ports of the third-party DNS are probed:

1. Send 50 **Probe packets** to different ports of the third-party DNS server which have not been previously probed (50 ICMP packets is the maximum globally allowed burst in Linux servers).

2. Send the **Verification packet** to a known closed port.

   - If the open port is not found (no ICMP message is received back), wait for at least 50ms for the rate limit counter to recuperate, and then restart from step 1.

   - Otherwise, carry out a binary search-like procedure. Probe the left half of the currently probed ports first. If there is a match, continue to search its left half. Otherwise, continue this approach in the right half.

Exploitation Phase

- CVE-2020-25705 (CWE-330) was exploited using the **Inferring port strategy**. Consequently, the active source port of the third-party DNS server was known to the adversary.

- CVE-2013-5661 was exploited by sending a large number of **DNSem** to the authoritative server for the target's domain at a higher rate than the configured response rate limit (RRL). Consequently, the authoritative server for the target's domain was muted so that the legitimate third-party DNS server query had an extremely low probability of getting a response.

Installation Phase

The adversary sent multiple NS record messages to the third-party DNS server claiming that the target's domain was a standalone zone with its own authoritative server (the adversary malicious server).

The NS record messages differ for the Transaction ID (it must be brute-forced) but contain the same following field values:

- **Source IP**: IP address of the authoritative server for the target's domain
- **Source port**: source port of the authoritative server for the target's domain
- **Destination IP**: IP address of the third-party DNS server
- **Destination port**: correct active port of the third party DNS server

One NS record message contained the correct Transaction ID (CWE-330) and was delivered to the third-party DNS server prior to the legitimate response from the authoritative server for the target's domain. As a consequence, the malicious NS record was cached in the third-party DNS server (CAPEC-142).

Command and Control Phase

For any query asking the A record of the victim's domain, the compromised DNS server queried the non-legitimate server which replied with a A record that mapped the target's domain to the adversary's malicious server IP.

Given that the software used by victims to connect to the target's domain did not properly verify the validity of the domain itself (CWE-923), the adversary was able to steal credentials used by the target's employees (CAPEC-569, CAPEC-89).

Reconnaissance Phase

The adversary exploited the stolen credentials to access several windows machines within the target organisation (CWE-308). The attacker discovered that one of these machines was configured and had the permissions to manage and update the contents of the target's website (CAPEC-560).

Weaponization Phase

The stolen credentials were used to access the machine with the permissions.

Delivery Phase

The stolen credentials were used to log into the machine with the permissions via Network.

Exploitation Phase

The adversary successfully logged into the machine with the permissions.

Installation Phase

Not relevant as the adversary installed nothing into the machine with the permissions.

Command and Control Phase

The adversary issued commands to update the target’s website and to navigate the local directory structure.

Actions on Objective Phase

The target’s website was defaced and important files were extracted and exposed to the public.

Task 4 - Attacker Analysis

Goals, Motivations and Skills

Given that the impact analysis section has outlined that the major impact of the cyberattack was the redirection of the target websites, it can be assumed that the defacement of the latter was the primary goal of the cyber actor.

The motivations that underpin such attack are to be traced back to the cyber actor's willingness to manifest opposition against the current Sri Lankan government's policies. Indeed, the webpage Sri Lankan users were redirected to accused Sri Lankan politicians for:

- the low salary of tea workers
- the mysterious disappearances and unjustified arrests of Tamil people and journalists
- the lack of freedom of information
- political corruption, militarisation and racism
- elections manipulation and brain drain

The motivations above explain why the attack took place only two days after Sri Lanka's official national independence day.

In light of the attack patterns (CAPEC entries) referenced in the analysis of the attack’s first step (Initial intrusion) in task 3, the attacker required a Medium level of skills. Indeed, both CAPEC-142 and CAPEC-89 are classified as medium-level difficulty attack patterns.
The first step of the attack involved the transmission of four different types of spoofed UDP packets. While spoofing a UDP packet is not rather complex, transmitting the packets as illustrated in the analysis requires a certain level of experience.

On the other hand, the cyber actor only needed low-level skills to perform the second step (Lateral movement) of the attack. This step only involved exploiting a known password to gain access to a computer with privileges and subsequently deface the target's website and exfiltrate sensitive data. In point of fact, CAPEC-560, which is listed in the second step of the Lockheed Martin's kill chain analysis in Task 3, requires low-level skills to be performed.

Actor Type

It is clear from the content of the webpage Sri Lankan users were redirected to that the attacker intended to pursue political, social and nationalistic ends rather than being interested in profits or self-entertainment.

For this reason, it is fairly reasonable to assume that a group of hacktivists conducted the attack. It is also rational to state that such a hacktivist group is Sri Lankan, as at the bottom of the malicious webpage, the attackers described themselves as follows:
"Who are we? We speak Sinhala, Tamil, English. We follow Buddhism, Hinduism, Christianity, Islam. We are Sri Lankans".

Another reason that supports the attackers being a group of hacktivists is that the skills required for such attack are congruous with hacktivist groups' average abilities and that website defacement is a typical hacktivist attack.

Given that hacktivists are not a mercenary hacking group but rather they aim to spread their personal political ideologies, then it is very likely that the Sri Lankan hacktivist group acted as both instigator and perpetrator.

It may be argued that nation-states are also interested in such social-political affairs, but they are excluded from being the actors of the attack in question as they usually have more extended goals which pursue with more subtle strategies.