Security Incident Report

TCPDump

Stephen Langford
2/17/25

Section 1: Identify the Network Protocol Involved in the Incident

The network protocols involved in this incident include:

- **Domain Name System (DNS)**: Used to resolve the domain names `yummyrecipesforme.com` and `greatrecipesforme.com` into their respective IP addresses.
- **Transmission Control Protocol (TCP)**: Used to establish and maintain communication between the client and the web server.
- **Hypertext Transfer Protocol (HTTP)**: Used for data transfer between the web server and the user's browser, including the malicious file download.

The logs indicate that the attack involved standard **DNS lookups**, **HTTP requests**, and **TCP connections**, which were leveraged to redirect users to a fake website and distribute malware.

Section 2: Document the Incident

Incident Overview

A security breach occurred on `yummyrecipesforme.com`, resulting in unauthorized access to the website's admin panel. The attacker modified the website's source code, embedding JavaScript that prompted users to download a malicious executable file.

Incident Details

1. **Unauthorized Access:**
   - The attacker performed a **brute force attack** to guess the administrative password, which was left at its default setting.
   - Once inside the admin panel, they altered the website's HTML and JavaScript.
2. **Malicious Code Execution:**
   - The attacker inserted a JavaScript snippet that automatically prompted users to download an executable file upon visiting the website.
   - The downloaded file contained malicious code that altered browser behavior and redirected users to a fake website, `greatrecipesforme.com`, which hosted additional malware.
3. **Network Activity:**
   - The browser sent a **DNS request** for `yummyrecipesforme.com`, receiving its legitimate IP address.
   - A subsequent **HTTP request** retrieved the compromised webpage, triggering the forced download of a malicious file.
   - The browser then sent another **DNS request** for `greatrecipesforme.com` after the malicious file was executed.
   - The connection to `greatrecipesforme.com` established a secondary malware delivery mechanism.
4. **Detection and Response:**
   - The breach was discovered after multiple customers reported unusual website behavior and slow computer performance.
   - Upon investigation, the **tcpdump logs** confirmed unauthorized DNS lookups and redirections.
   - A cybersecurity analyst confirmed the presence of malicious JavaScript within the website's source code.

Impact

- **Compromised User Data:** Potential theft of sensitive customer information.
- **Reputation Damage:** Loss of customer trust due to malware distribution.
- **Operational Downtime:** Website access was disrupted while remediation efforts were in progress.

Section 3: Recommend One Remediation for Brute Force Attacks

To prevent future brute force attacks, it is recommended to **enforce Two-Factor Authentication (2FA)** for all administrative logins.

Why 2FA is Effective:

- Even if an attacker guesses the password, they will require a secondary authentication method (such as a mobile verification code) to gain access.
- 2FA significantly reduces the risk of unauthorized access by adding an additional security layer beyond just passwords.
- It helps mitigate the risks associated with weak or default passwords.

Additional Recommendations:

- **Enforce Strong Password Policies:** Require complex passwords with a mix of characters and prohibit default passwords.
- **Limit Login Attempts:** Implement account lockouts after multiple failed login attempts to prevent brute force attacks.
- **Monitor Login Activity:** Set up alerts for multiple failed login attempts or logins from unfamiliar IP addresses.

By implementing these security measures, `yummyrecipesforme.com` can significantly reduce the risk of future attacks and improve overall cybersecurity resilience.

Tcpdump traffic log:

```
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?
yummyrecipesforme.com. (24)
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A
203.0.113.22 (40)

14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859
ecr 0,nop,wscale 7], length 0
14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS
val 3302576859 ecr 3302576859,nop,wscale 7], length 0
14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr
3302576859], length 73: HTTP: GET / HTTP/1.1
14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
...<a lot of traffic on the port 80>...

14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A?
greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A
192.0.2.17 (40)
14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags
```

```
[S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649
ecr 0,nop,wscale 7], length 0
14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags
[S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS
val 3302989649 ecr 3302989649,nop,wscale 7], length 0
14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr
3302989649], length 73: HTTP: GET / HTTP/1.1

14:25:29.576597 IP greatrecipesforme.com.http > your.machine.56378: Flags
[.], ack 74, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
...<a lot of traffic on the port 80>...
```