**Cyber Security Task2**

**Incident Scenario**

**Sbuwear.com** has had several customers contact the company helpline stating that when they visited the website, they were prompted to download and run a file that asked them to update their browsers. Their personal computers have been operating slowly ever since. The company IT team tried logging into the web server but noticed they were locked out of their account.

The cybersecurity analyst used a sandbox environment to test the website without impacting the company network. Then, the analyst ran tcp dump to capture the network and protocol traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would update the user’s browser, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com) that looked identical to the original site (**sbuwear**.**com**).

# Scope

The scope of this vulnerability assessment relates to the current safe guarding of company website and system. The assessment will cover a period of three months, from June 2024 to August 2024.And that website will be thoroughly tested and that best practices are followed to ensure the is safe use of website.

**OBJECTIVE**

The overall objective is that customers should be able to access the company website freely and have information available to them without having to run into problems. The tools or measures put in place are the to ensure that everything runs properly and that the site is properly available to people. And well to educate about phishing techniques and how to spot and prevent them.

**INCIDENT DETECTION**

**ROLES**

**Sifiso Ntuli- Junior Analyst**

**Kamani Mudaly- Admin**

**Sibusiso Sekhoto- CSO**

**Reenay Charles-Blue Team**

**Lizel Thomson- Red team**

This reading explains how to identify the brute force attack using tcpdump.

The protocol impacted in the incident is Hypertext transfer protocol (HTTP). Running tcpdump and accessing the Sbuwear.com website to detect the problem, capture protocol, and traffic activity in a DNS & HTTP traffic log file provided the evidence needed to come to this conclusion. The malicious file is observed being transported to the users’ computers using the HTTP protocol at the application layer.

**Incident Response**

**Prepare**

Proper communication channels, should be implemented and response checklist and we going to provide staff with quality cybersecurity training that will help them prevent attacks or potential attacks.

**Detection and Analysis**

Since the potential problem of malicious files being posted on the company website, we need to determine how dangerous is the identified action, at this point we have labeled it as high because company website has been compromised and further malicious intent can be conducted.

**Containment**

We have isolated the affected system as we do now want the rest of the company system being affected by the attack. The affected part of the system is isolated from the rest of the network so we can further investigate the cause and mitigation strategies.

**Eradication** **and Recovery**

We go deep into the root cause of the problem and in this situation, we have identified that it is unpatched website that has allowed the penetration of our system and further taken over and used for malicious intent like redirecting customer to malicious websites and stealing their credentials. We have to now restore the company the affected system to its pre-incident state so we can have the company website running back to normal knowing that we have eradicated the problem and ensured its safe for future use.

**Post Incident activity**

The importance of patching and employee awareness and training all go hand in hand, this cannot go unsaid as it is very important to ensuring the safety of company websites. Legal guidelines such as security framework or NIST framework play a huge role to the safeguarding of security systems. They provide guidelines on how to respond to incidents and mitigation strategies.

**Coordination**

To ensure the safe guarding of website we are going to strengthen or security posture through continuous testing and evaluating or incident response plan to ensure that it remains current that it remains current and effective in the face of ever-evolving cyber threats.

**FORENSIC ANALYSIS**

A screenshot of a computer

Description automatically generated

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

The first section of the DNS & HTTP traffic log file shows the source computer (**your.machine.52444**) using port **52444** to send a DNS resolution request to the DNS server (**dns.google.domain**) for the destination URL (**yummyrecipesforme.com**). Then the reply comes back from the DNS server to the source computer with the IP address of the destination URL **(203.0.113.22**).

|  |
| --- |
| 14:18:36.786501 IP **your.machine.36086** > **Sbuwear.com.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 |

The next section shows the source computer sending a connection request (**Flags [S]**) from the source computer using port **36086** directly to the destination (**Sbuwear.com.http**)

The next section shows the source computer sending a connection request (**Flags [S]**) from the source computer (**your.machine.36086**) using port **36086** directly to the destination (**yummyrecipesforme.com.http**). The **.http** suffix is the port number; **http** is commonly associated with port 80. The reply shows the destination acknowledging it received the connection request (**Flags [S.]**). The communication between the source and the intended destination continues for about 2 minutes, according to the timestamps between this block (**14:18**) and the next DNS resolution request (see below for the **14:20** timestamp).

**TCP Flag codes include:**

**Flags [S]**  - Connection **S**tart

**Flags [F]**  - Connection **F**inish

**Flags [P]**  - Data **P**ush

**Flags [R]**  - Connection **R**eset

**Flags [.]**  - Acknowledgment

|  |
| --- |
| 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** |

The log entry with the code **HTTP: GET / HTTP/1.1** shows the browser is requesting data from **yummyrecipesforme.com** with the **HTTP: GET** method using **HTTP** protocol version **1.1**. This could be the download request for the malicious file.

|  |
| --- |
| **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 **192.0.2.172** (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 |

Then, a sudden change happens in the logs. The traffic is routed from the source computer to the DNS server again using port **.52444** (**your.machine.52444 > dns.google.domain**) to make another DNS resolution request. This time, the DNS server routes the traffic to a new IP address (**192.0.2.172)** and its associated URL (**shopforme.com.http**). The traffic changes to a route between the source computer and the spoofed website (outgoing traffic: **IP your.machine.56378 > shopforme.com.http** and incoming traffic: **shopforme.com.http >** **IP your.machine.56378**). Note that the port number (**.56378**) on the source computer has changed again when redirected to a new website.

**Post incident Assessment**

The response plan is very effective because of the way things get done in the correct way ,guidelines are followed and it also acts as a future reference of how to prevent those certain incidents .The response plan helps us save time so actions take are of correct.

The actions taken are effective because we get to resolve the problem and have things running in order again.

We also learned that no system is fully secure and constant tests need to be done so we can ensure the safety of our sites malicious actors mature in their attacks so we also need sophisticated systems to deal with these threats.