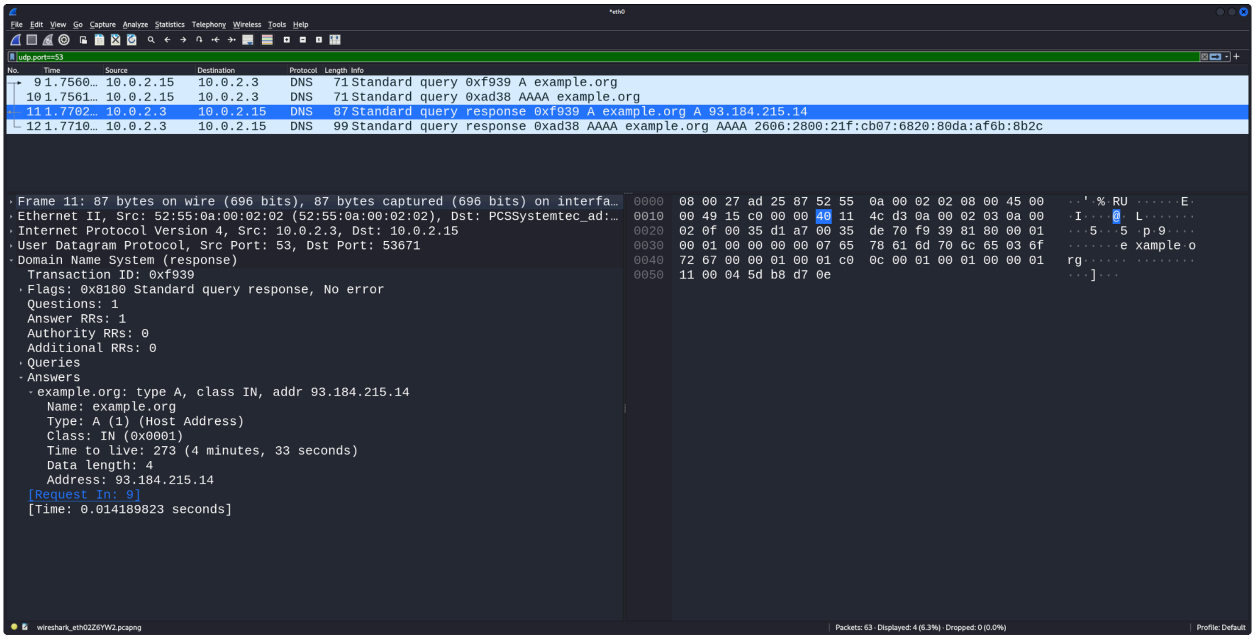
Tyler Ebra
CSEC 2003
November 5, 2024
Incident Report

1. The network protocols involved in the incident were DNS and HTTP. The DNS was used to push the network traffic to the malicious website that had malware. HTTP requests the data from a website onto the computer. This was used to request the malware from the malicious fake website.



udp.port==53

```
No.  Time       Source     Destination  Protocol Length Info
  9 1.7560…  10.0.2.15  10.0.2.3     DNS      71 Standard query 0xf939 A example.org
 10 1.7561…  10.0.2.15  10.0.2.3     DNS      71 Standard query 0xad38 AAAA example.org
 11 1.7702…  10.0.2.3   10.0.2.15    DNS      87 Standard query response 0xf939 A example.org A 93.184.215.14
 12 1.7710…  10.0.2.3   10.0.2.15    DNS      99 Standard query response 0xad38 AAAA example.org AAAA 2606:2800:21f:cb07:6820:80da:af6b:8b2c
```

```
Frame 11: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interfa…
Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_ad:…
Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 53671
Domain Name System (response)
  Transaction ID: 0xf939
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    example.org: type A, class IN, addr 93.184.215.14
      Name: example.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 273 (4 minutes, 33 seconds)
      Data length: 4
      Address: 93.184.215.14
  [Request In: 9]
  [Time: 0.014189823 seconds]
```

```
0000  08 00 27 ad 25 87 52 55  0a 00 02 02 08 00 45 00   ··'·%·RU ······E·
0010  00 49 15 c0 00 00 40 11  4c d3 0a 00 02 03 0a 00   ·I····@· L·······
0020  02 0f 00 35 d1 a7 00 35  de 70 f9 39 81 80 00 01   ···5···5 ·p·9····
0030  00 01 00 00 00 00 07 65  78 61 6d 70 6c 65 03 6f   ·······e xample·o
0040  72 67 00 00 01 00 01 c0  0c 00 01 00 01 00 00 01   rg······ ········
0050  11 00 04 5d b8 d7 0e                               ···]···
```

wireshark_eth02Z6YW2.pcapng | Packets: 63 · Displayed: 4 (6.3%) · Dropped: 0 (0.0%) | Profile: Default

2. The network protocols involved in the incident were DNS and HTTP. The DNS was used to push the network traffic to the malicious website that had malware. HTTP requests the data from a website onto the computer. This was used to request the malware from the malicious fake website.
3. The attack on yummyrecipiesforme.com was attacked by a former employee through a brute force attack. The former employee was able to easily guess the admin password for the website as it was still using the default password which allowed them to alter the website. The former employee gained access to the website and changed the code to redirect the traffic to a fake website that was downloading malware on the devices of those who were taken to the website. This had an adverse effect on the customers using the website as they experienced a slowdown on their device after they automatically downloaded the malware file from the fake website.
4. This attack could have been completely avoided if the password was not just the default password. To be secure the admin account should regularly change the

password and have more complex requirements. Additionally the best security measure would be to add 2FA as it would require additional measures to enter the admin account making it much more difficult for attackers to succeed.

5. There are multiple network hardening tools that would greatly improve the security posture of the social media organization but the single most important tool is MFA. The reason MFA is the most important is because it would resolve the majority of the issues they are currently experiencing provided a more secure network. With MFA it would not matter if the employees share passwords as it would still need that added level of verification that only the specific employees would be able to provide. This makes it very difficult for someone who has access to a leaked password to actually get into the network. MFA is extremely easy to set up and maintain so this could be done immediately after the breach and would not require much to run it. It helps with both external and internal network access as not only will malicious actors have a difficult time entering into the network but so will employees who have shared passwords.
6. **Summarize the security event:** At the e-commerce company a recent security breach compromised millions of valuable customers' data including names, addresses, purchase history, and payment information. The reason the company experienced the breach was due to a known unpatched vulnerability in a web application, weak employee password requirements and insufficient network monitoring. This allowed the attacker to enter through the known vulnerability. Once inside they utilized the compromised employee credentials to navigate through the system and remained undetected due to the weak network monitoring.
7. **Identify the type of attack and the systems affected:** The attack involved multiple stages the first being exploitation of a vulnerable system. The second part involved the use of stolen employee credentials that allowed for movement within the network. The final part of the attack involved data extraction of the customers PII and SPII. The systems affected during the attack were the employee authentication system and the customer database.
8. **Protect the assets in your organization being compromised:** The first course of action should be isolation of the attacker. This can be accomplished by disconnecting and removing access to any systems that contain valuable information. The next step would be to remove the access that the attackers have by taking away any administrative privileges that are given to the compromised employee account. This would be the most effective course of action to take to stop further damage within the company.
9. **Detect similar incidents in the future:** The best way to detect future incidents would be to have sufficient network monitoring tools in place that can monitor the network traffic. This along with alerts for any suspicious activity such as abnormal logins, data transfers or changes within the network. Setting up and IDS will also help review the network traffic for any malicious actors.

10. ***Respond*** **to future cybersecurity incidents:** In the future these incidents should be actively monitored for a speedy response. The first step is to limit access to the attacker by cutting off and disconnecting all important information the attacker may be after. After this, remove admin access from the attacker so they can no longer cause damage or remove that user from the network completely.
11. ***Recover*** **from the incident:** To recover from the incident the first step would be to patch the vulnerability. After that data backups of customer information would need to be verified if they contain all the necessary data that was stolen; if not, restoring the missing information would be the next step. After that stronger password policies need to be put into place and then network monitoring should be implemented to prevent future attacks.