To: All Employees
From: Jacob Suveges
Re: Recent Website Defacement

Executive Summary

Overview of happenings

At 5:05:30 PM we detected an Israeli IP address that would go and deface our website on our Apache2 server. The attacker started by scanning our network to detect any open services. The attacker saw that our SSH service was open to the internet and they then continued with trying to guess the password of the root account. The attacker started this at 5:10:00 PM and was able to find the correct password by 5:10:17 PM. The attacker then logged into the Apache2 SSH service and continued to upload an image to the server with the name “hacked2z.png” along with the “index.html” file. This change went straight to production and we saw that the website on Apach2 was defaced with this image and html file.

CIA

This attack breached all three categories in the CIA model: confidentiality, integrity, and availability. This breached confidentiality as the attacker was able to access source code for the website along with all other files on the Apache2 server. It breached integrity as well since the attacker was able to alter the information on the website. Finally, it breached availability as the website was completely defaced and unusable during this time.

Attacker Profile

We determined that this was not the act of a sophisticated attacker, but was instead the act of a script kiddie who broke into our network for the thrill of defacing our website. They were able to do so due to our weak passwords and the fact that the SSH service was available from the internet. This was only compounded by the fact that we took no action to stop it.

Threat Hunting

There were several indicators of the attack from both the network and the files on the Apache2 server. We first saw a lot of network activity that comes from port scanning when trying to determine the services running on the Apache2 server. We then saw some traffic trying to guess the SSH password for the root account. After the attacker got into the server they uploaded two files: “hacked2z.png” and “index.html”. Finally, anybody could see that the website was defaced with the uploaded “index.html” file.

Recovery, Remediation, and Prevention

To recover from the attack we will restore the website code from a backup and ban the IP address. Then we will change the SSH root password along with any other weak password we find. We will also remove the malicious files including: “hacked2z.png” and “index.html”. Finally, to prevent this from happening in the future we will limit SSH to the internal network only and implement an IP blocker that will block IP addresses if they are detected to be port scanning or brute forcing our services.

Technical Report

Impact on the CIA Triad

Confidentiality: preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity: guarding against improper information, data, or service modification or destruction, including ensuring information nonrepudiation and authenticity.
Availability: ensuring timely and reliable access to and use of information, data, or services.

Confidentiality
Choose One: Breached Not Breached
Justification of breached status: The attacker gained access to the root account of the Apache2 server. This means that authorized restrictions on information access were not preserved.

Integrity
Choose One: Breached Not Breached
Justification of breached status: The attacker was able to change the information on the website.

Availability
Choose One: Breached Not Breached
Justification of breached status: The attacker took down the website preventing users from accessing it.

Attacker Profile

1. ***Reconnaissance:***
   The attacker started by performing a port scan on our environment.
2. ***Weaponization/Resource Development:***
   The attacker prepared the .png file before delivery and used a brute forcing program that was made or installed.
3. ***Delivery/Initial Access/Execution:***
   The attacker uploaded a .png file to our Apache2 server and defaced the website.
4. ***Exploitation/Execution/Privilege Escalation/Defense Evasion/Credential Access/Discovery/Lateral Movement/Collection:***
   The attacker exploited a weak SSH password through brute force.
5. ***Installation/Persistence/Defense Evasion/Discovery/Lateral Movement:***
   No malware was detected. Only the .png that was used to deface the website along with the altered index.html file.
6. ***Command and Control/Discovery/Exfiltration:***
   The attacker was able to gain root access to the Apache2 web server, but no further C2 was established.
7. ***Actions on Objectives/Impact:***
   The attacker was a script kiddy who exploited our weak password to deface our website. This breach shows our customers that their websites can be easily taken down. This makes us as a company much less trustworthy.

Threat Hunting

Provide a list describing the Indicators of Compromise that were present in the attack scenario:

Network:

IP Address - 199.203.100.193

QRadar - Port scan network traffic

QRadar - Brute force attempts

QRadar - Successful/failed root login

Files:

Apache2 Server - hacked2z.png

Apache2 Server - Altered index.html

Recovery, Remediation, and Prevention

Recovery: To recover from the attack we should ban the IP address and recover the website through backup files.

Remediation: We need to change our root SSH passwords to something much stronger. We also need to remove the malicious files: hacked2z.png and the index.html file.

Prevention: To prevent this attack we need to limit SSH to the internal network only. We could also automatically block IP addresses that are detected when they are port scanning or brute forcing.