Security incident report

`

Section 1: Identify the network protocol involved in the incident

The network protocol involved in this incident is the HTTP(DNS) protocol as this incident is involved with the internet specifically with yummyrecipesforme.com. The situation presented tells us that multiple customers contacted our help desk after finding themselves in a predicament and downloading an unwanted application. Furthermore, when running the tcpdump log we can see multiple detections of something going on with the timestamp at 14:18- 14:20 where the website changes and there is suspicion of the HTTP Get file along with domain and IP changing further imply HTTP network protocol (application layer).

Section 2: Document the incident

Customers reached out to yummyrecipesforme's helpdesk due to company website prompting them to download a file to access free recipes. Customers explained that after running the file, their computer began running more slowly. The downloaded file also redirected customers to a fake version of the website that contains malware that led to unhappy individuals.

This was due to a suspicion of a former employee/hacker who gained access due to a brute force attack where they entered several known default passwords for the administrative account until they correctly guessed the right one. Cybersecurity analysts can hypothesize early because the admin was locked out.

Cyber Security analysts created a sandbox environment to address the incident and observe the suspicious behavior. CA ran the network protocol analyzer tcpdump to address and here they can see that when it loads the logs for the URL yummyrecipesforme.com. Here CA see that the URL directs you to another website that prompts users to download a file with the suggestion of providing free websites.

When cybersecurity analyst's read the logs they inspect and find something suspicious. CA sees that the DNS request requests the IP address of yummyrecipesforme.com from the DNS server and receives a correct IP address. CA then initiates an HTTP request and here is where they get into some trouble with the brower initiating the download of the malware. The DNS server then responds with the IP address for greatrecipesforme.com, (the wrong URL) and sees that it was compromised indeed.

Found within the logs was the manipulated code/website update but really is the original the malicious file the CA team confirmed it was impacted due to a brute force attack and there were no additional controls in place to prevent this brute force attack due to seeing that the originals website code was manipulated with and due to the owner having no authority over the website later confirmed that it was due to an admin attack.

Section 3: Recommend one remediation for brute force attacks

Unfortunately, one of the reasons why this attack worked was because the password was a generic default password and had some vulnerabilities. Since brute force attacks are individuals just guessing passwords to log in it is vital that each password is unique and code sensitive meaning they involve many different. Furthermore, the company should make it an automatic patch update to remove all old passwords and require all employees to use new passwords with the prevention of old passwords. Once implemented, the company can also start looking at a 2FA. 2 Factor authentication requires a password and also confirming a code from a personal device to gain access to the system. This will make the task more difficult for the hacker and will likely help any malicious behavior.