Security incident report

Reference materials: tcpdump traffic log - Google Docs

Section 1: Identify the network protocol involved in the incident

The network protocols that are involved in this incident are HTTP and DNS. When visitors attempt to visit the company webpage, they are first directed to the correct webpage. The DNS request retrieves the correct IP address and HTTP is used to retrieve the correct webpage. However, when visitors run the file that has been placed in the source code, another DNS request is made for the webpage that contains malware. The IP address of this webpage is retrieved and an HTTP request retrieves this webpage.

Section 2: Document the incident

At around 2 p.m., the company website help desk began receiving complaints from multiple customers stating that the company webpage, www.yummyrecipesforme.com, had prompted them to download a file to access free recipes. Upon opening of the downloaded file, customers were redirected to a different address. Afterwards, customers stated that their computers had begun to run more slowly. At around 2:18 p.m., the cybersecurity team began to investigate this incident by accessing the company website in a sandbox environment in order to avoid contaminating the company network. Upon reaching the company website, we were prompted to download a file containing free recipes. On download of the file, the tcpdump logs indicate that the malicious file was transported to the computer using HTTP. Upon opening the file, a new DNS request occurs, requesting the IP address of this new webpage. Afterwards, a connection is established with the webpage using the IP address obtained in the DNS request. We suspect that this webpage contains malware injected by the malicious actor.

We believe that the malicious actor is a former employee who used brute force to gain access to the webpage's administrative account using known default passwords. Since the website owner reported being locked out of the administrative account, we believe that the malicious actor changed the password after gaining access. Upon gaining access to the account, the malicious actor added javascript to the page’s source code prompting the visitor to download and open the file. Upon opening the malicious file, the end user’s computer is compromised.

Section 3: Recommend one remediation for brute force attacks

There are several steps that can be taken to prevent this type of attack from occurring in the future. Because malicious actors using brute force attempt to gain access to an account with known default passwords, utilizing a stricter password policy can make it increasingly difficult for an attacker to gain access. In addition to a stricter password policy, utilizing 2-factor or multi-factor authentication will make gaining access to an account using brute force extremely difficult. This is due to the fact that a malicious actor would need access to further information or a completely different account to gain access with 2-factor or multi-factor authentication. Overall, I recommend using one or both of stricter password policies and multi-factor authentication in order to reduce the likelihood of an attack utilizing brute force in the future.