Post-Breach Report

Date: 12-16-2022
Investigated by: Max, Geoff, Tyler
Report Typed by: Max
Fwd To: (Details removed for privacy reasons)

What Happened:

The affected protocol in this incident is the Hypertext Transfer Protocol (HTTP). By executing tcpdump and accessing the yummyrecipesforme.com website, we were able to discern the issue, capture relevant protocol data, and log traffic activity in a DNS & HTTP traffic file, leading to this conclusion.

Furthermore, our analysis revealed that the malicious file is being delivered to users' computers via the HTTP protocol at the application layer. This indicates a potential threat originating from this particular channel.

What Happened (Client Facing):

Many customers contacted the website owner, saying that when they visited the site, they were asked to download a file that claimed to update their browsers. As a result, their personal computers slowed down. The website owner tried to log into the web server but found they couldn't access their account.

Our team of cybersecurity analysts used a special environment to test the website without affecting the company network. They then used a tool called tcpdump to capture the network and protocol traffic that happened when they interacted with the website. The analyst was asked to download a file that claimed to update the browser. They agreed to the download and ran it. Afterward, the browser took them to a fake website (fakewebsite.com) that looked just like the real one (realwebsite.com).

The cybersecurity analyst looked at the tcpdump log and saw that the browser first asked for the IP address for REDACTED. Once it connected to the website using the HTTP protocol, the analyst remembered downloading and running the file. The logs showed a sudden change in network traffic when the browser asked for a new IP address for the (realwebsite.com) website. Then, the traffic was directed to the new IP address for the (fakewebsite.com website.

Our senior cybersecurity expert examined the code for the websites and the downloaded file. They found that an attacker had changed the website to make it tell users to download a file that pretended to be a browser update. Because the website owner couldn't get into their administrator account, the team thinks the attacker used a method to repeatedly guess the password and get in. When the malicious file was run, it caused problems on the end users' computers.

Preventative Measures (Client Facing):

To safeguard against brute force attacks, the team will introduce two-factor authentication (2FA). This 2FA approach will involve an extra step for users to verify their identity by entering a one-time password (OTP) sent to either their email or phone. Upon successful verification using both their login credentials and the OTP, users will be granted access to the system. This additional layer of authorization will likely deter malicious actors attempting brute force attacks from gaining unauthorized entry to the system.