Ex110

Joshua Main-Smith

2020-11-23

Contents

Technical Report

Finding: Users Navigating to Outside Websites with Company Resources

Risk Assessment

Users are allowed to use company resources to browse websites outside the company network. A potential consequence of this is private information communicated from the user's browser may be captured by attackers hosting malicious websites.

Vulnerability Description

When a user visits a malicious website, such as the one crafted below in the attack narrative, private information communicated from the browser to the server may be capture by an attacker (such as cookie information). Further, there are a variety of other attacks an attacker may employ to gain further information, such as viewing webcams, html pages, known browser exploits, etc.

Mitigation or Resolution Strategy

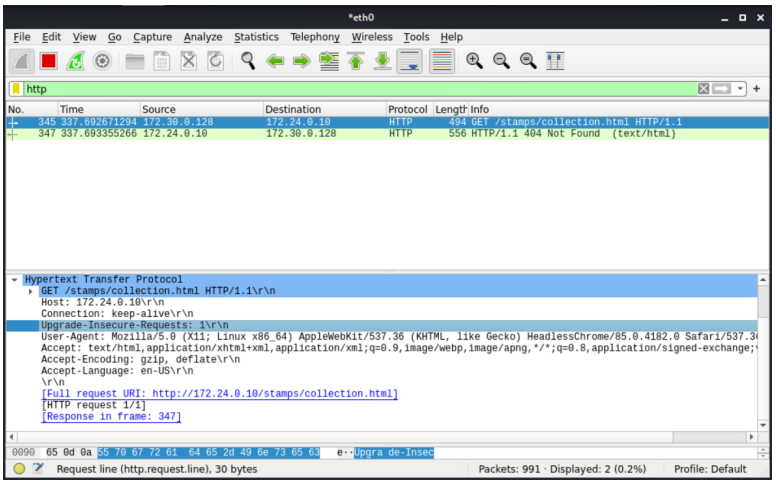
Prevent user's from navigating to unknown web hosts by employing white list rules in the firewall (for example). Additionally, giving the employees social engineering training may prove useful.

Attack Narrative

Monitoring HTTP Connections on Wireshark

With the knowledge that Phineas is attempting to contact a webpage on **kali.pr0be.com** (172.24.0.10), we began monitoring all web traffic that was attempting to connect to our host by first turning our apache2 server on with **sudo service apache2 start** then watched Wireshark traffic.

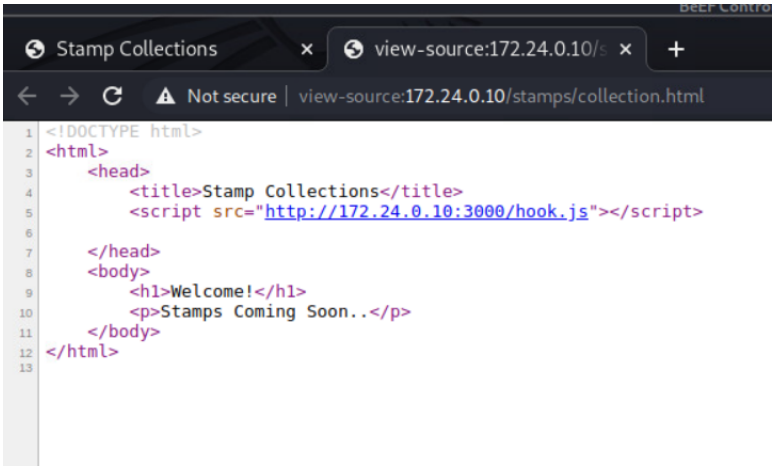
We found that **172.30.0.128** was attempting to connect to **http://172.24.0.10/stamps/collection.html** (the full URI request can be seen in the bottom pane of the image below).



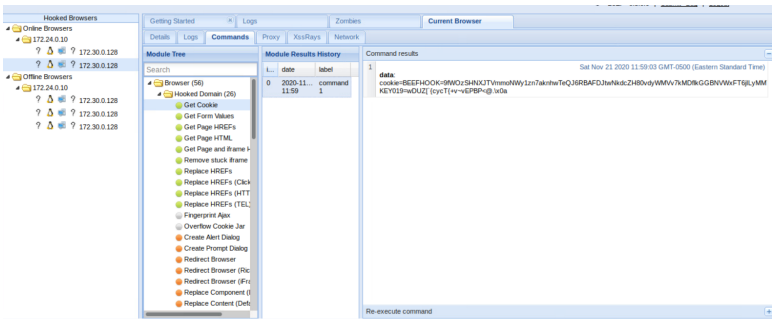
Given the above, we decided to create the webpage Phineas is attempting to connect to that contains a script that will hook the browser when opened.

BeEF Hook

After opening BeEf with **sudo beef-xss**, we created the webpage under **/var/www/html/stamps/collection.html**, containing the hook script to the BeEF generated server. The webpage can be seen below.



Phineas eventually connected to the webpage, allowing us to hook his browser. Once hooked, we were able to capture a token potentially granting access to highly sensitive information, as can be seen below.



One may notice that the cookie also contains KEY019.