Jordan Schalter

IT417 A.TOMA

5/30/2023

1. Provide the following information
   1. 2021-09-24 12:56:44.440 -4:00
   2. 10.9.23.102
   3. 63494
   4. 208.91.128.6
   5. 80
   6. ET MALWARE SQUIRRELWAFFLE loader Activity (POST)

A screenshot of a computer

Description automatically generated

1. Investigate the domain using the sample analysis methodology from previous labs. DO NOT NAVIGATE to that website. Use your tools, sandboxes, googlefu to tell me what you think this website is. Provide screenshots and a detailed explanations of your analysis.

A screenshot of a computer

Description automatically generated with medium confidence

1. Analyze the H-worm pcap. Using the previous exercise, the in class pcap analysis / review and via security onion pcap parser or utilizing wireshark. Provide the source IP, destination IP, host domain of the potentially malicious website, URI, username, operating system, and if the host has Anti-Virus on it.

Host: pm2bitcoin.com:6969

Op System: Windows 7

Source IP: 192.168.100.71

Destination IP: 46.243.189.128

URL: HTTP/1.1 404 Not Found

Username: C4BA3647

Antivirus: nan-av

Sever Level: HIGH

1. A screenshot of a computer

   Description automatically generated
2. 1. <https://medium.com/@denton.o/using-cyberchef-as-a-forensics-tool-8a4bfbab43f3>

You can use hex in CyberChef to extract photos and files, this is cool and can be useful for many things but, mainly I think it is neat for the reason that if something is locked in hex code you can input it into the bake and extract the information.

A screenshot of a computer

Description automatically generated

1. <https://blog.intigriti.com/2021/07/13/hacker-tools-cyberchef/>

You can resolve a list of domain names that you can use to find the IP address for specific websites of interest. This can be useful in many ways but, I can imagine from a blue team perspective even more so due to having another ability to find an IP of a potentially malicious site.

A screenshot of a computer

Description automatically generated

1. <https://www.socinvestigation.com/cooking-malicious-documents-with-cyberchef-detect-respond/>

You can perform malware analysis on a Microsoft document that contains hidden malware within its code, and then replace the line that is hiding the malware with another less intrusive code. This is obviously useful since it can easily sniff out malicious behavior within Microsoft documents.

A screenshot of a computer

Description automatically generated

1. <https://docs.securityonion.net/en/2.3/cyberchef.html>

This documentation describes some of the operations available within CyberChef and I thought it would be neat to include it since I found it an interesting read. I had no idea that something like CyberChef existed (even if my dreams of using something like this would be a more red team, its is neat that something like this can be used both ways.)

A screenshot of a computer

Description automatically generated

1. <https://udel.codes/cyberchef.html>

Within CyberChef there is a magic wand that can attempt to predict what you are trying to accomplish – this is something that I think is also cool as a programmer because it allows the user to focus less on debugging and more on the task that they are trying to accomplish.

A screenshot of a computer

Description automatically generated