Example DFIR

*For this example, all PII has been changed to protect the client's identity. Herein, the client will be referred to as Mr. Client.

Executive Summary

On May 13th, 2019 I received a laptop from Mr. Client with a complaint of a terribly slow machine. He also informed me that during his browsing he encounters many popups and even full website redirections.

Objective

The purpose of this investigation is to resolve Mr. Client's complaints to the fullest extent. It will also be imperative to erase all traces of whatever may be hiding on his machine. A secondary task will be to figure out how this alleged virus got on his machine, time permitting.

Evidence Analyzed

Fortunately, Mr. Client has allowed me access to the physical machine making extraction an unnecessary step. However, when needed I had a secure removable flash drive at the ready to transfer to by Unix-based machine for further analysis.

The hash comparisons should be placed here for 'Chain of Custody's' sake.

Steps Taken

1. Immediately saw ss_files on desktop as well as other ss.html on desktop.
2. Ran offline windows defender
3. Ran regular windows defender & macafee next. Didn't find even the obvious files. Lolz.
4. Decided to not do this by hand and download an AV. My go to is malwarebytes free (with 14 day trial). Turns out there we 226 issues found and one was even a chrome extension. See appendix for detailed info in the ss_files.txt file.
5. See remediation

Analysis

Files have been created all over the machine and all of them were classified as PUPs (Potentially Unwanted Programs) by MalwareBytes. The files of a malicious Chrome extension were found at `C:\Users\Client\AppData\Local\Google\Chrome\User`

`Data\Default\Extensions\ hhhpajpnecmhngfgkclokcghcpfgbape`. Here we see all the javascript files which periodically open a new tab, or popup, in chrome with the background.js, content.js, install.js, and vsframe.js files all controlled by the malicious extension. The phishing uses many convincing splash pages imitating Hulu, Netflix, and Spotify sign in pages.

Conclusions

It is known that the attack took place on May 8th, 2019 at 2:41:13 PM EST. This can be determined from the first file creation MAC time found.

What stuck out to me was the custom Chrome extension as well as the registry (startup) modifications. Unfortunately the browsing history was wiped by this trojanized-phishing campaign so I was not able to identify or even surmise, with a reasonable amount of confidence, who or how this got on Mr. Client's machine. We also can see from the browsing history that on May 7th, and before there are no ad-like URL's and then on May 9th at 3:30 PM (2 minutes after the first internet search) is the first spam site opened (SUPERAntiSpyware)- and many more after that.

In my initial understanding of the virus's home directory being stored on the desktop was found to be technically wrong. After checking the file's properties it was understood the files were soft links to the files in the `.../Chrome/User Data` directory.

I regret not going further to explore this virus from a network forensics perspective to see what, if any, command and control channels existed as well as how exactly the timing of each phish is being done. This could be handled by simply downloading Wireshark to understand the network traffic going on, or using the `tcpvcon` Windows Command Line Tool.

Last, I would further this investigation by searching for attribution by providing the hashes to VirusTotal.com and other sites like it. Although, during the initial VirusTotal.com query of the index.html file none of the 60 AV's (including malwarebytes) flagged the file as known or malicious. This may prove problematic down the line however with only a couple hours to work on this I needed to remediate the machine quickly.

Remediation

After quarantining and then deleting the files (from the Recycling Bin) using MalwareBytes I then manually went to each directory to make sure there was no residue or residual files

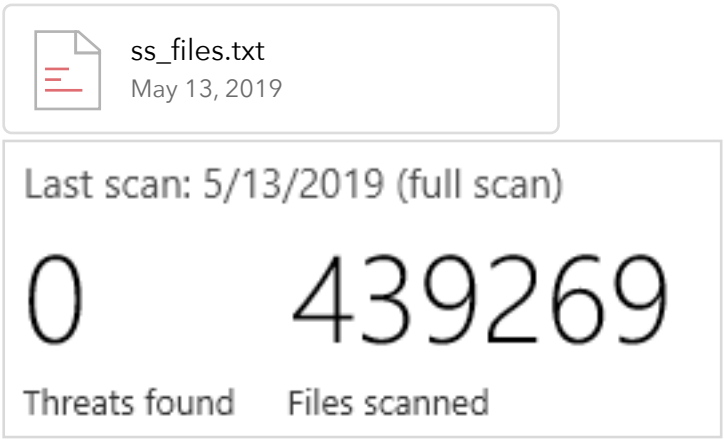
leftover.

I found that the system needed to update as well to its malware definitions for Windows Defender. The machine also needed an entire version update and Intel update from *(forgot to find this)* to KB4346084. Both were done promptly after file removal.

After, I scanned the machine one last time with both Windows Defender (Full Scan) and Malwarebytes to check that there were no more threats identified; there were not as seen in figures 1 & 2 in the appendix.

As of now, it is ready to be returned to Mr. Client faster (opinion, as it uses a Core i3 CPU) and without any popups while browsing.

Appendix



Your scan is complete.

No threats detected!

Scan time:	3m : 26s
Items scanned:	265,905
Threats detected:	0