ITSC 303

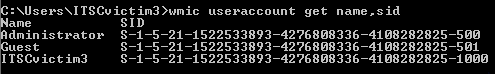
Malware Analysis

Final Project - Weekly Report 7

D’Artagnan Boocock & Coleton Sanheim

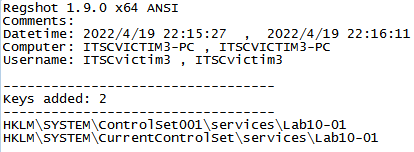
19/04/2022

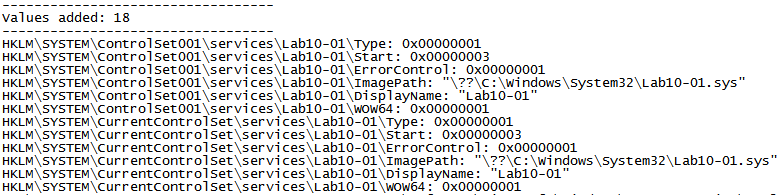
**RegShot analysis:**



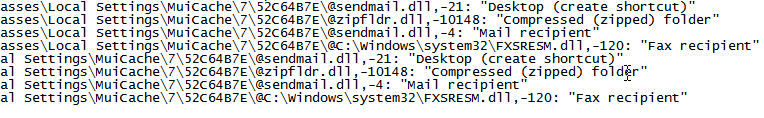
**Sample 1:**

**Machine 1**

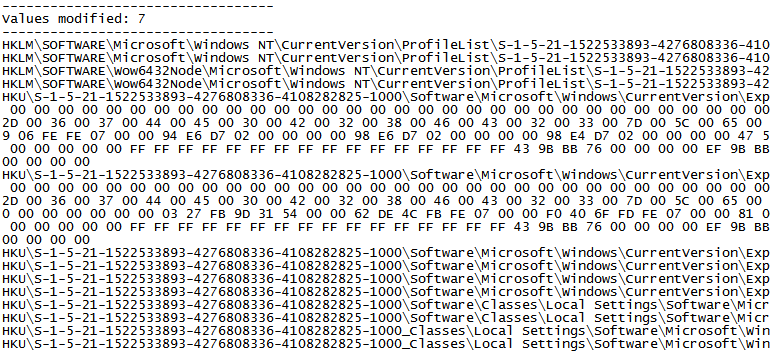




Here we see the sample editing the Current Control Set keys, which deal with the boot loader and settings on boot. We can assume that this sample is creating and editing these keys to establish persistence for the next reboot.



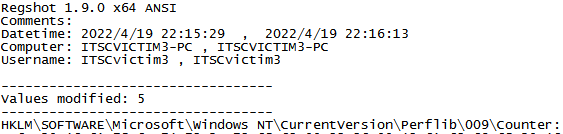
Here it looks like the sample is adding “Desktop (create shortcut)”, “Compressed (zipped) folder”, “Mail recipient” and “Fax recipient” to the registry. These hive values are likely used to tamper with existing application functionality or obfuscate the workings of the malware.

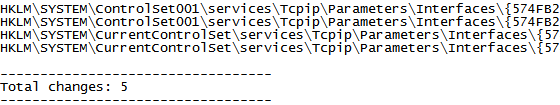




The Wow6432Node is modified in accordance to spawning a process. The edits of Windows keys are likely an attempt for the malware to integrate itself with core processes to obfuscate its presence on the machine.

**Machine 2**



 Again we see the Control Set keys being edited, presumably this was done to establish persistence.

**Wireshark Analysis**



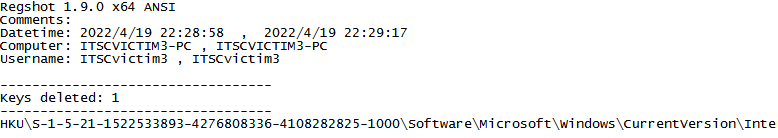
Here we can see wireshark has captured a connection to 74.125.142.188

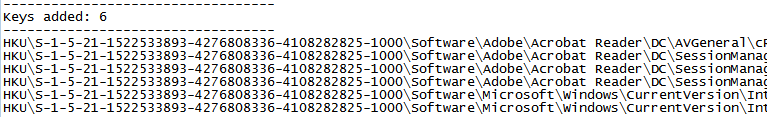
Upon further investigation the IP is discovered to be associated with Google and is therefore ruled out as being malicious.

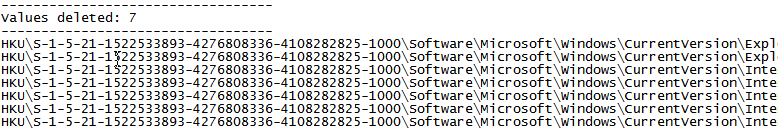


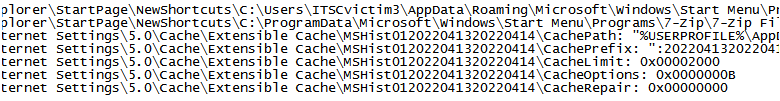
**Sample 2:**

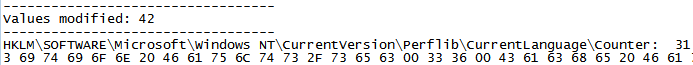
**Machine 1**

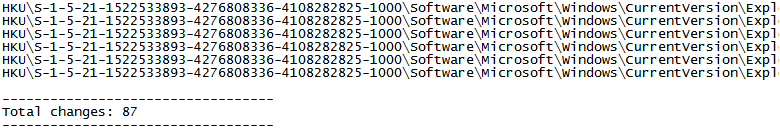
This is likely deleting itself, or perhaps a previous version of itself, off of the victim before the malware itself detonates.

As the malware is hidden in a PDF, this is either normal pdf behavior, or an attempt by the malware to further obfuscate itself inside of the pdf.

As in the previous sample, this is more than likely the malware integrating itself into core system processes so that it can hide its presence.

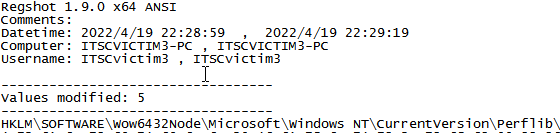
Here the malware appears to be deleting internet explorer history. This is likely the sample attempting to hide itself while it propagates.

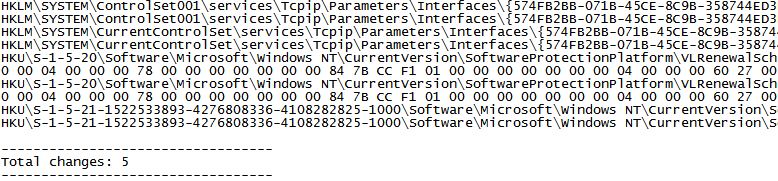




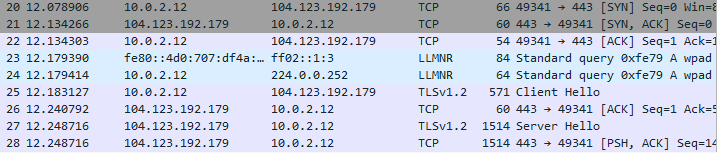
Here we can see the sample has made a total of 87 changes to the registry. 42 Values were modified with the last three values pertaining to the Windows Explorer. These three changes are likely used to mask the execution of the payload.

**Machine 2**

 This registry value has to do with spawning a process

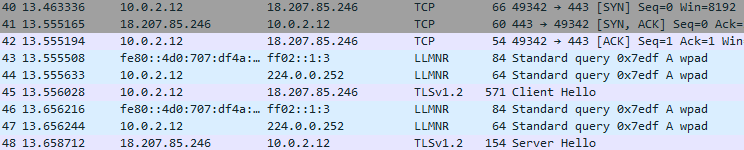
Once again we have more registry changes pertaining to boot loader persistence.

**Wireshark Analysis**



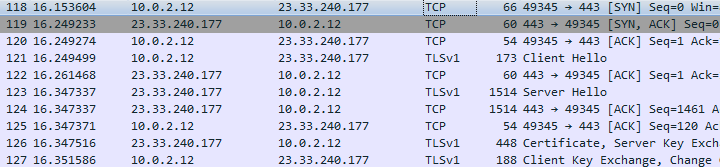
Here we can see the sample establishes a connection to 104.123.192.179



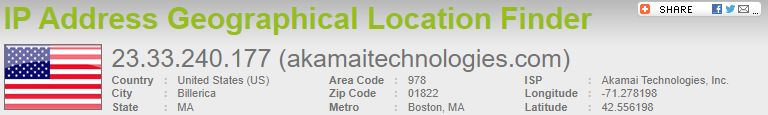


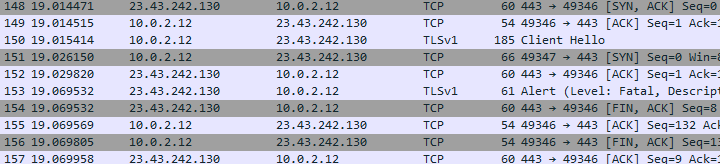
Here we can see the sample establishes a connection to 18.207.85.246. It is worth noting this address gets sent a Client Hello and then returns a Server Hello. This could signify the malware is some kind of back-door or Remote Access Trojan. Unfortunately, this packet uses TLS encryption and the data is therefore unreadable.





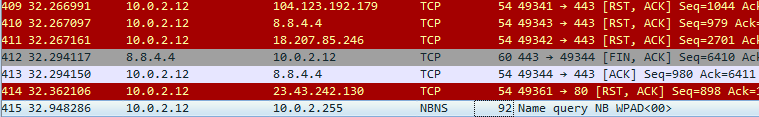
Here we can see the sample establishes a connection to 23.33.240.177





The connections to 23.43.242.130 continue for another 250 packets.





Here we can see the connections to 104.123.192.179, 18.207.85.246 and 23.43.242.130 are terminated once the pdf is closed.

Because the 23.43.242.130, the 23.33.240.177 and the 104.123.192.179 addresses all belong to Akamai Technologies we can assume these three addresses are part of regular adobe processes. However the 18.207.85.246 address is hosted by AWS and could possibly be a malicious domain used by attackers.

**Conclusion**

Sample 1 is a trojan which tampers with the registry creating faults in existing programs and possibly serves as an information gatherer. This means the sample could be categorized as some form of bloatware.

Sample 2 is likely a Remote Access Trojan. This pdf serves as a trojan horse for a backdoor payload which opens a socket allowing remote connection to the infected machine.