Investigation of group 2
By group 14 (_undefined)
4/23/16

Preface

We were given given a VM with instructions to find a key logger hidden on it and where told we would eventually get a method to view the key logs.

Our approach

Now that we knew that we were dealing with a key logger we decided to split this investigation into 2 parts. The First part is if we where average users, we would just do some security scans and try to see if anything was off during normal activity. The second part of the investigation was if we couldn't find anything with the scan we where to dive deeper into the system to see if we could find it manually. In this step we assumed that we the users where just overly paranoid. In the first step we were to use the following tools, Malwarebytes, Super AntiSpyware, AVG anti virus, and Spybot Search & Destroy. If we had to go to the second step we would use the Microsoft system internals utilities to dive deep into the system. Some of the tools in this suit are Auto Runs, Process Explorer, and Process Monitor.

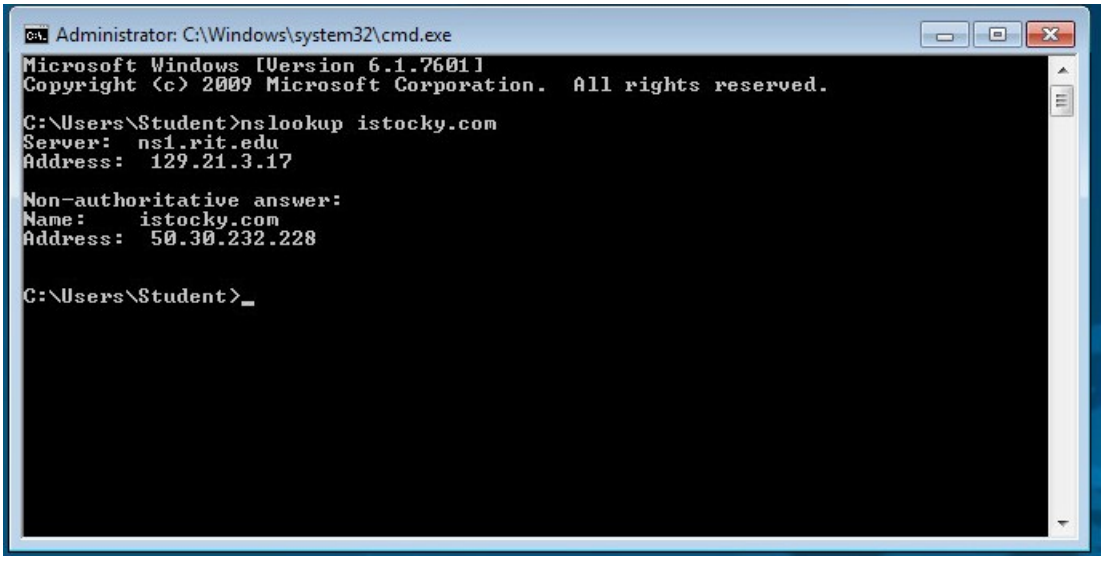
Phase 1 Results

To our amazement none of the first 4 scans found the key logger! From this we decided to expand the software for scanning a little. We then tried to use the enterprise McAfee that is provide from RIT. To no avail, none of the scans found the key logger.

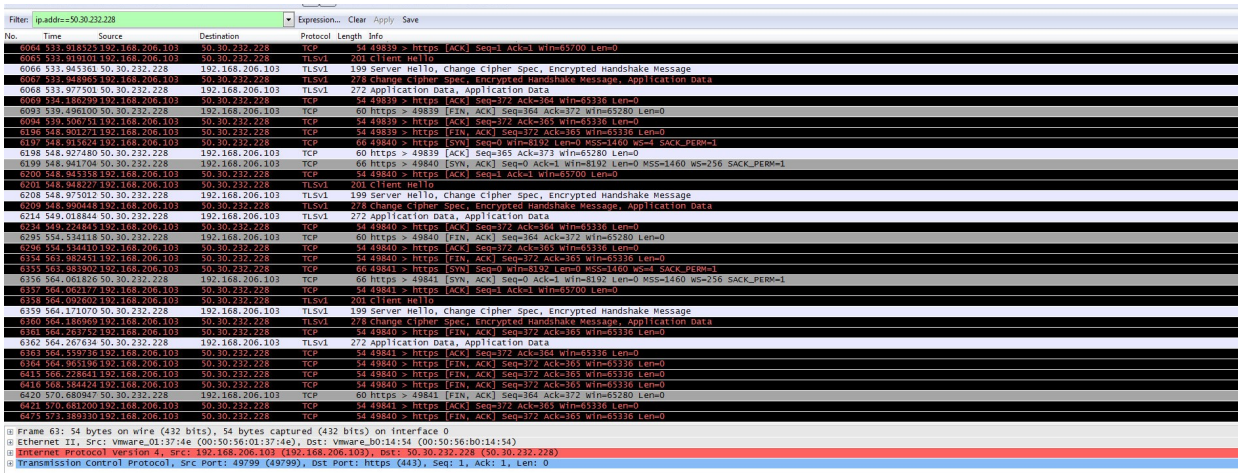
Phase 2 Results

With our prides wounded we began the manual search for the key logger. Using Auto Runs we examined the start up programs looking specifically for programs that didn't have a publisher or a legit sounding description. To our surprise everything had a publisher and a legit sounding description of the program. We then moved onto viewing the running processes using Process Monitor, then once again we found nothing.

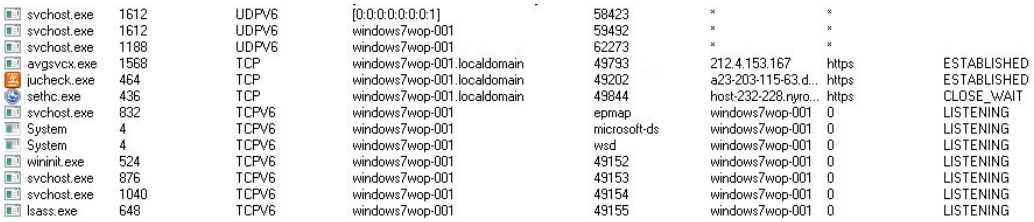
At this point it was person and we weren't letting this one go. Then we got a break, group 2 told gave us login information to a ftp server so we could view the logs. First thing we do is a “nslookup” on the given domain.



From this we could filter Wireshark on this IP and we got the following information.



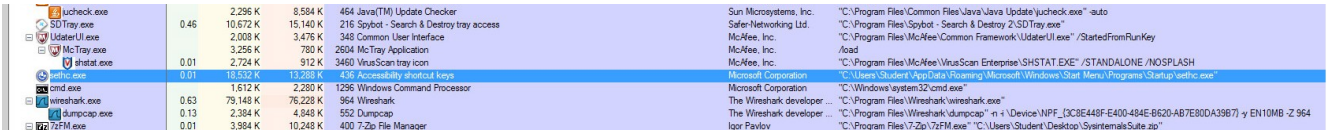
This is a lot of encrypted traffic on port 443 also known as https. From here we used TCPView to seee what processes are using ports and we specifically looked for those using 443 (https).



svchost.exe	1612	UDPV6	[0:0:0:0:0:0:0:1]	58423	*	*	
svchost.exe	1612	UDPV6	windows7wop-001	59492	*	*	
svchost.exe	1188	UDPV6	windows7wop-001	62273	*	*	
avgsvcx.exe	1568	TCP	windows7wop-001.localdomain	49793	212.4.153.167	https	ESTABLISHED
jucheck.exe	464	TCP	windows7wop-001.localdomain	49202	a23-203-115-63.d...	https	ESTABLISHED
sethc.exe	436	TCP	windows7wop-001.localdomain	49844	host-232-228.nyro...	https	CLOSE_WAIT
svchost.exe	832	TCPV6	windows7wop-001	epmap	windows7wop-001	0	LISTENING
System	4	TCPV6	windows7wop-001	microsoft-ds	windows7wop-001	0	LISTENING
System	4	TCPV6	windows7wop-001	wsd	windows7wop-001	0	LISTENING
wininit.exe	524	TCPV6	windows7wop-001	49152	windows7wop-001	0	LISTENING
svchost.exe	876	TCPV6	windows7wop-001	49153	windows7wop-001	0	LISTENING
svchost.exe	1040	TCPV6	windows7wop-001	49154	windows7wop-001	0	LISTENING
lsass.exe	648	TCPV6	windows7wop-001	49155	windows7wop-001	0	LISTENING

Its hard to see but there are only 3 processes using 443 as the destination port. It was java update checker, AVG (a program I installed), and this “Sethc.exe”. Clearly this last one is suspicious. We then checked these in process explorer for confirm. We changed the default

settings to also display the cmd start path and this is what we found.



jucheck.exe		2,296 K	8,584 K	464	Java(TM) Update Checker	Sun Microsystems, Inc.	"C:\Program Files\Common Files\Java\Java Update\jucheck.exe" -auto
SDTray.exe	0.46	10,672 K	15,140 K	216	Spybot - Search & Destroy tray access	Safer-Networking Ltd.	"C:\Program Files\Spybot - Search & Destroy 2\SDTray.exe"
UdaterUI.exe		2,008 K	3,476 K	348	Common User Interface	McAfee, Inc.	"C:\Program Files\McAfee\Common Framework\UdaterUI.exe" /StartedFromRunKey
McTray.exe		3,256 K	780 K	2604	McTray Application	McAfee, Inc.	/load
shstat.exe	0.01	2,724 K	912 K	3460	VirusScan tray icon	McAfee, Inc.	"C:\Program Files\McAfee\VirusScan Enterprise\SHSTAT.EXE" /STANDALONE /NOSPLASH
sethc.exe	0.01	18,532 K	13,288 K	436	Accessibility shortcut keys	Microsoft Corporation	"C:\Users\Student\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\sethc.exe"
cmd.exe		1,612 K	2,280 K	1296	Windows Command Processor	Microsoft Corporation	"C:\Windows\system32\cmd.exe"
wireshark.exe	0.63	79,148 K	76,228 K	964	Wireshark	The Wireshark developer ...	"C:\Program Files\Wireshark\wireshark.exe"
dumpcap.exe	0.13	2,384 K	4,848 K	552	Dumpcap	The Wireshark developer ...	"C:\Program Files\Wireshark\dumpcap" -n -i \Device\NPF_{3C8E448F-E400-484E-B620-AB7E80DA39B7} -y EN10MB -Z 964
7zFM.exe	0.01	3,984 K	10,248 K	400	7-Zip File Manager	Igor Pavlov	"C:\Program Files\7-Zip\7zFM.exe" "C:\Users\Student\Desktop\SysinternalsSuite.zip"

Again its hard to see, but the thing to notice is that Sethc.exe's startup path is in appdata. No legit program will have a start up path in appdata. The final nail in the coffin was after we kill the process all traffic to the IP disappeared. WE HAD FOUND IT!

Our Thoughts

This group had done a wonderful job and if they hadn't told of the ftp server we probably wouldn't have thought to check Wireshark. We believe that none of the scans picked up the key logger because that it's file properties had been altered to look like a legit Microsoft program. A few things we believe would make the keylogger even better is decrease the frequency of transfers out to the server, because the SSL handshake creates a lot of attention if any one was watching. The last thing is that we question how useful the actual logs are that are collected. Due to the frequent transfers to the ftp server (it transfers once every 15 seconds so 5760 file in a day) it would be hard to get things like usernames and passwords. Also the format of the log makes reading it hard. The format is one key stroke per line of the file, making it human unreadable.

We had fun and look forward to the presentation.