## Malware Analysis of Phishing Email

Overview

In this section I want show phishing scenario when our user ‘fcastle’ got mail and this mail attached with malicious macro word document, our user will download the file and open to see what he got there.

On the attacker screen we will see meterpreter session will opened which mean now the attacker has shell access to our user.

For this demonstration we will use windows 7 for the user.

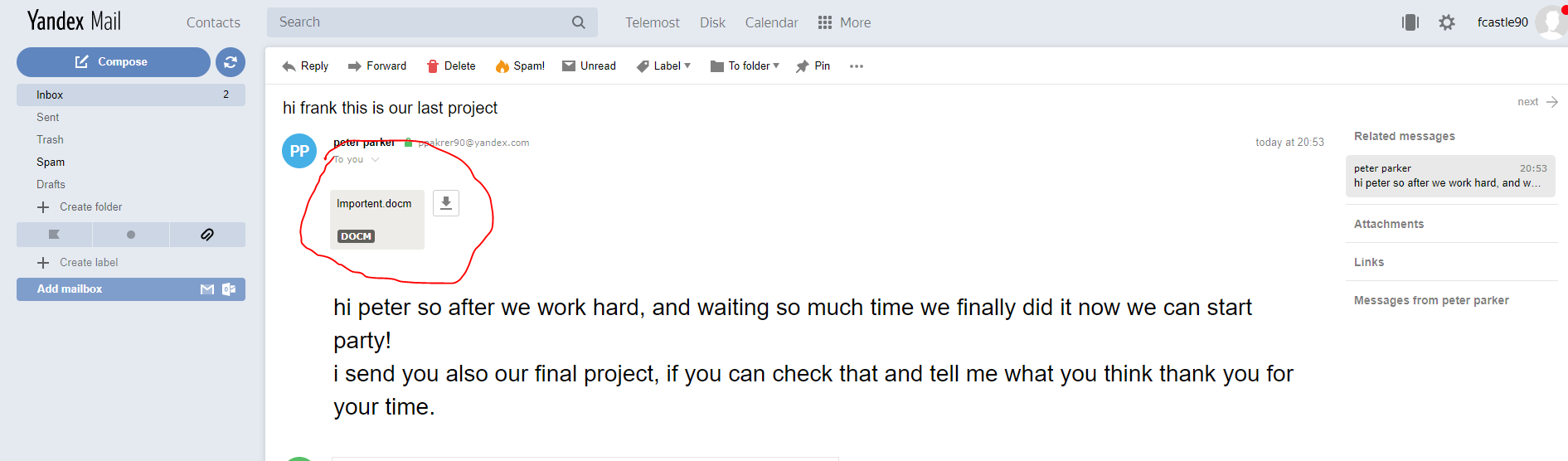
We first get alert coming from our SOC and this alert will be the first lead. Then will start our investigation:

We dump the volatile memory from our user computer with the tool WinPmem and then we will use Volatility tool to start our investigation. F

For the last part we will also perform static and dynamic malware analysis on the detected malicious word document.

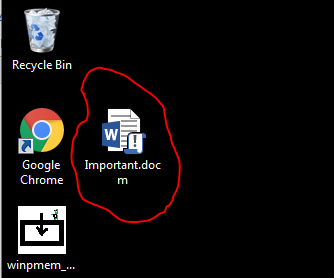
So… we got a lot of work, let’s start! ☺

Email Attachment



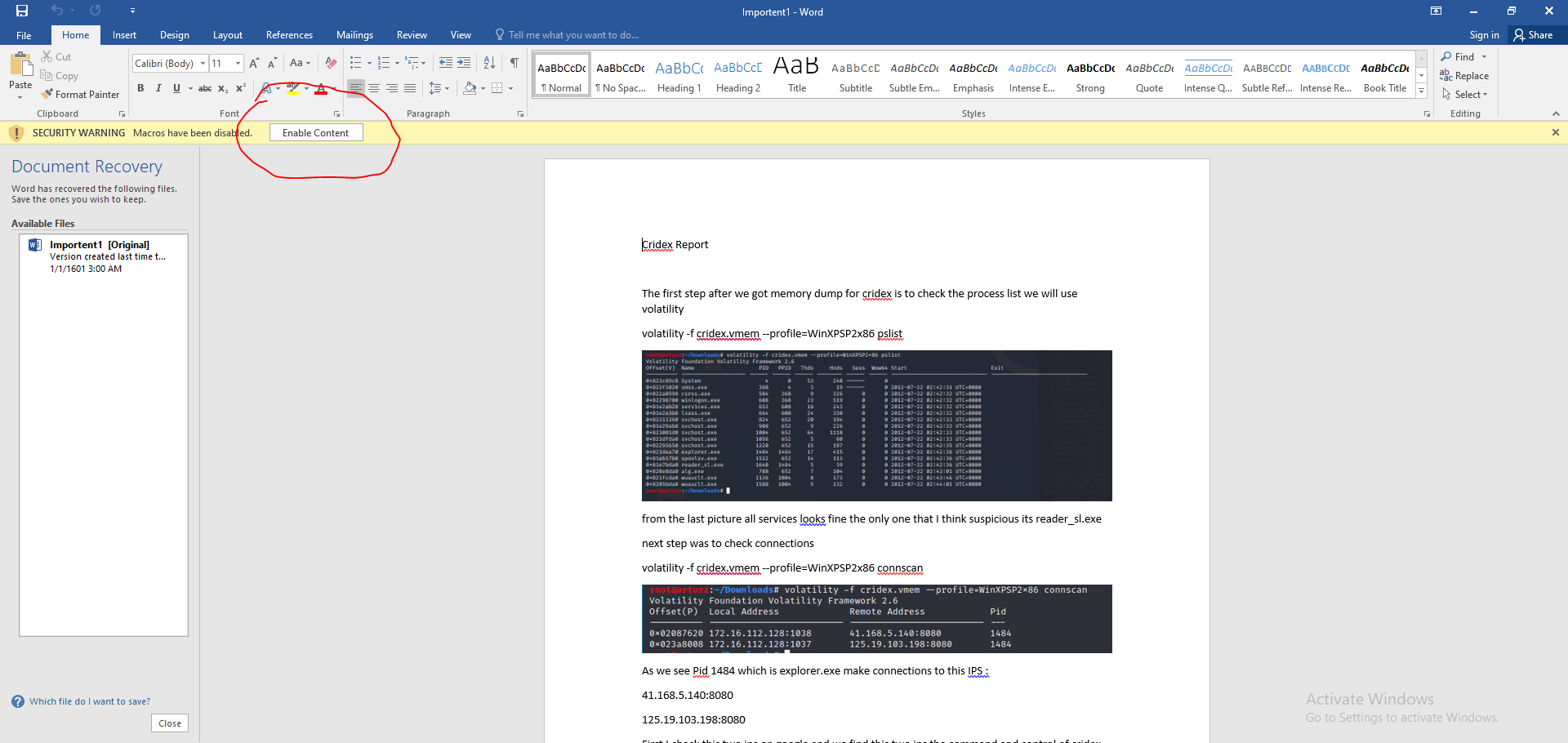
From above we first start when our user ‘frank’ got mail from his friend ‘peter’ that work with them together at the same company.

As we can see this mail attached with word document, now our user see this mail got from his friend everything looks legit. So now this is the time to download the word document and see what we got there.



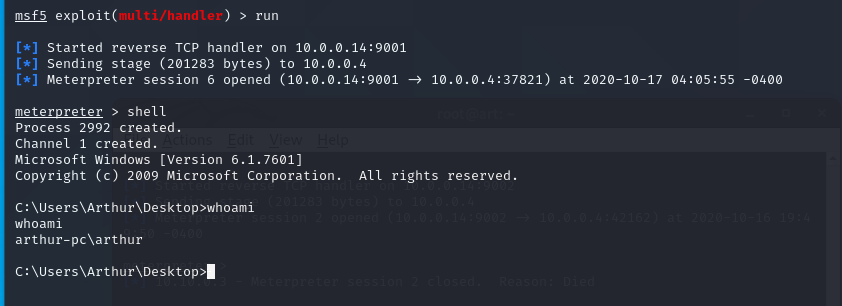
From the picture above our user ‘Frank’ downloaded the word document with the name ‘Important’

Now the user wants to read the file lets open the file.



Meterpreter Shell

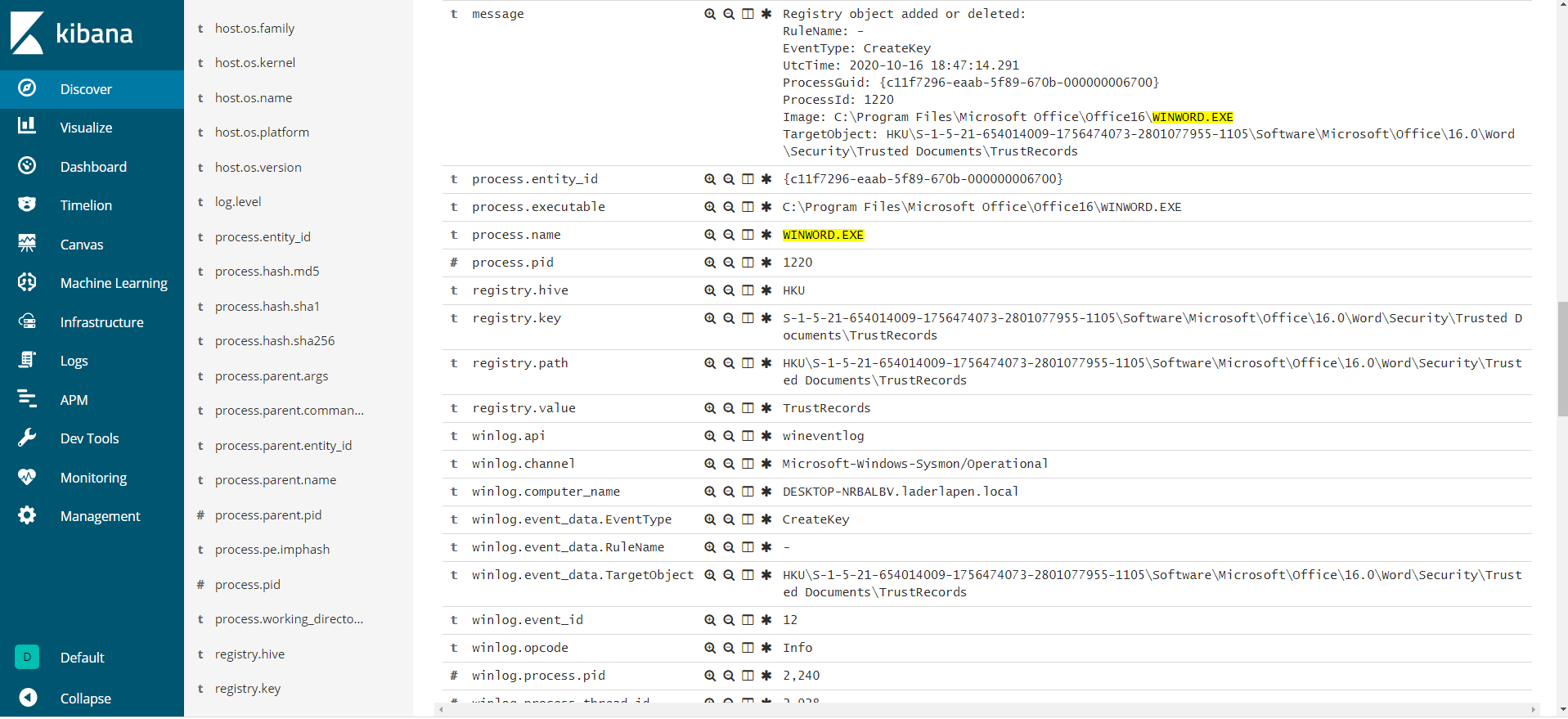
From above our user open the document see the content and also message about to enable macro lets enable and see what’s happing on the attacker screen.



Above, right after our user enable macro on the word document, on the attacker screen we can see meterpreter session opened which mean now the attacker has shell access to the user.

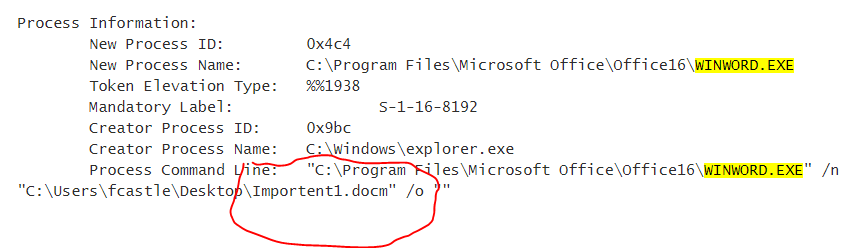
Now we finish with the attacking scenario now let’s move to defense and start our investigation, the first lead will be that our SOC get log from our user machine about the malicious word document. We will dump the memory from the user, and then use volatility and start with static and dynamic malware analysis.

SOC&IR



Log from SOC

Here above we got log from the user machine, this log comes right after the user open the word document, from the log above we can understand that when the user run the word document some registry keys modified. This can show us that maybe there is malicious activity because when we run word documents the registry keys should not modified.

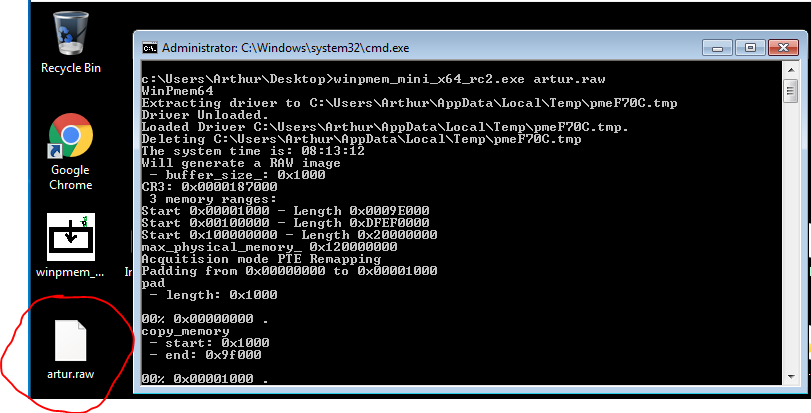


Here above we also got log from the same time that we got alert about the registry keys and we see the file that alerting about the registry keys its Important.docm which is the file that comes from the mail of the user.

Now as soc analyst we know this information: First the user downloaded word document from the mail services and run the file, second we got log that show us when the user run this word document there is some registry keys that modified this is can be very suspicious.

Using WinPmem – Memory dump

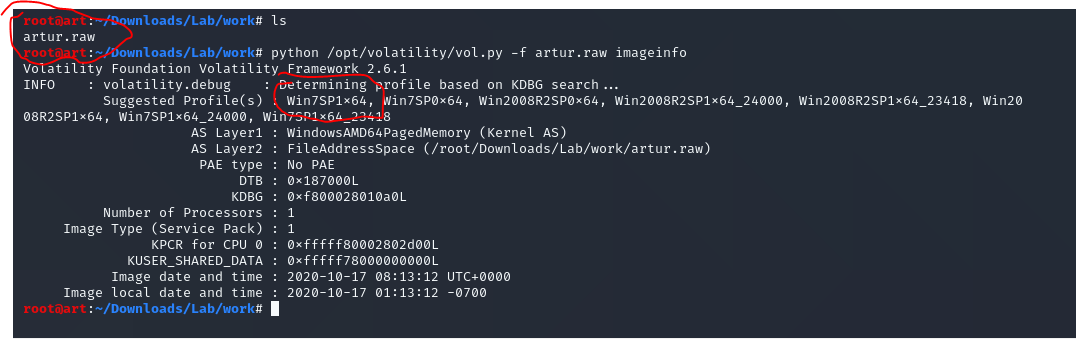
Now the next step as soc analyst we will dump the memory from the user machine we will use WinPmem and then we will move to our kali machine to continue investigate with Volatility.



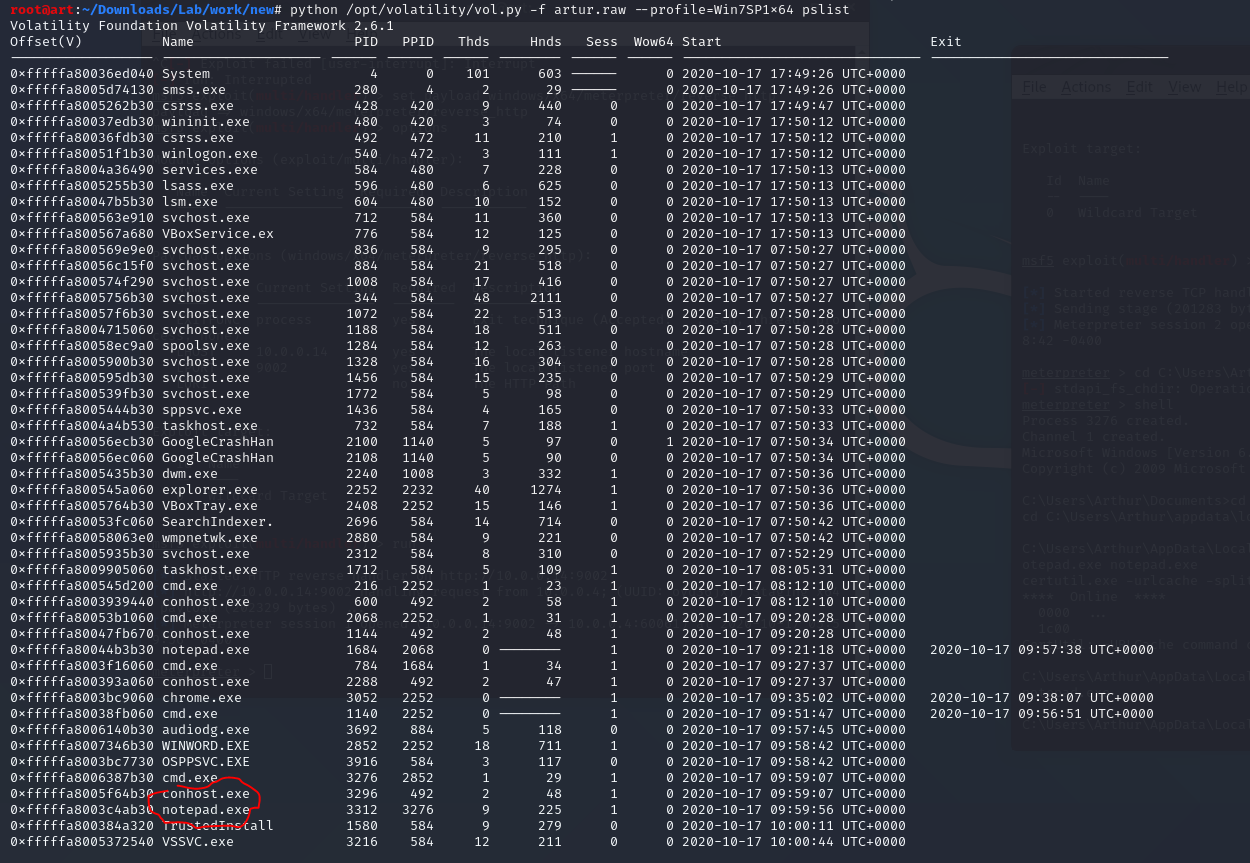
Next step from the picture above we use the tool WinPmem to dump the memory to raw file as we see the name of the raw file: artur.raw

Next step will be transfer the raw file to our kali machine and we will use volatility for the next steps to see live about process files and network activities and much more.

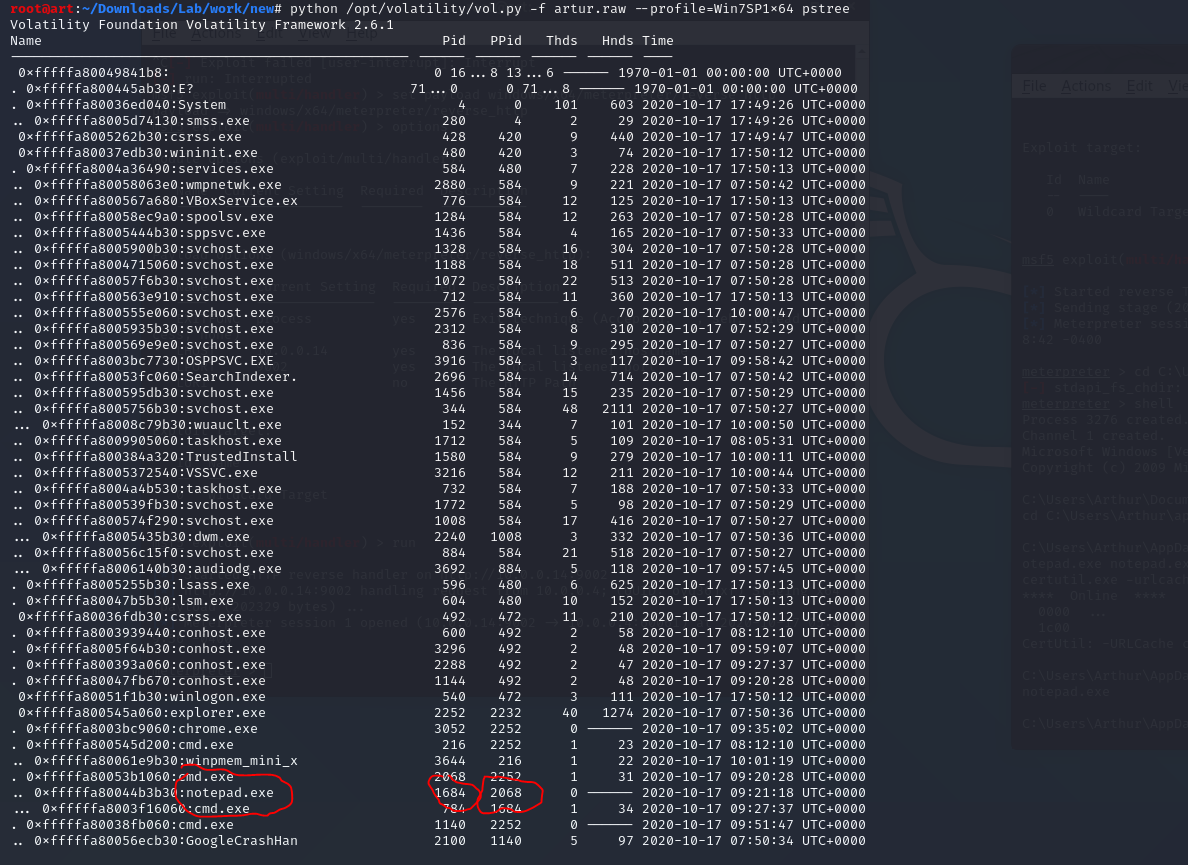
**Volatility**



From the picture above we transfer the raw file from windows7 to our kali machine and we will start use volatility as we can see we find the right profile lets continue!

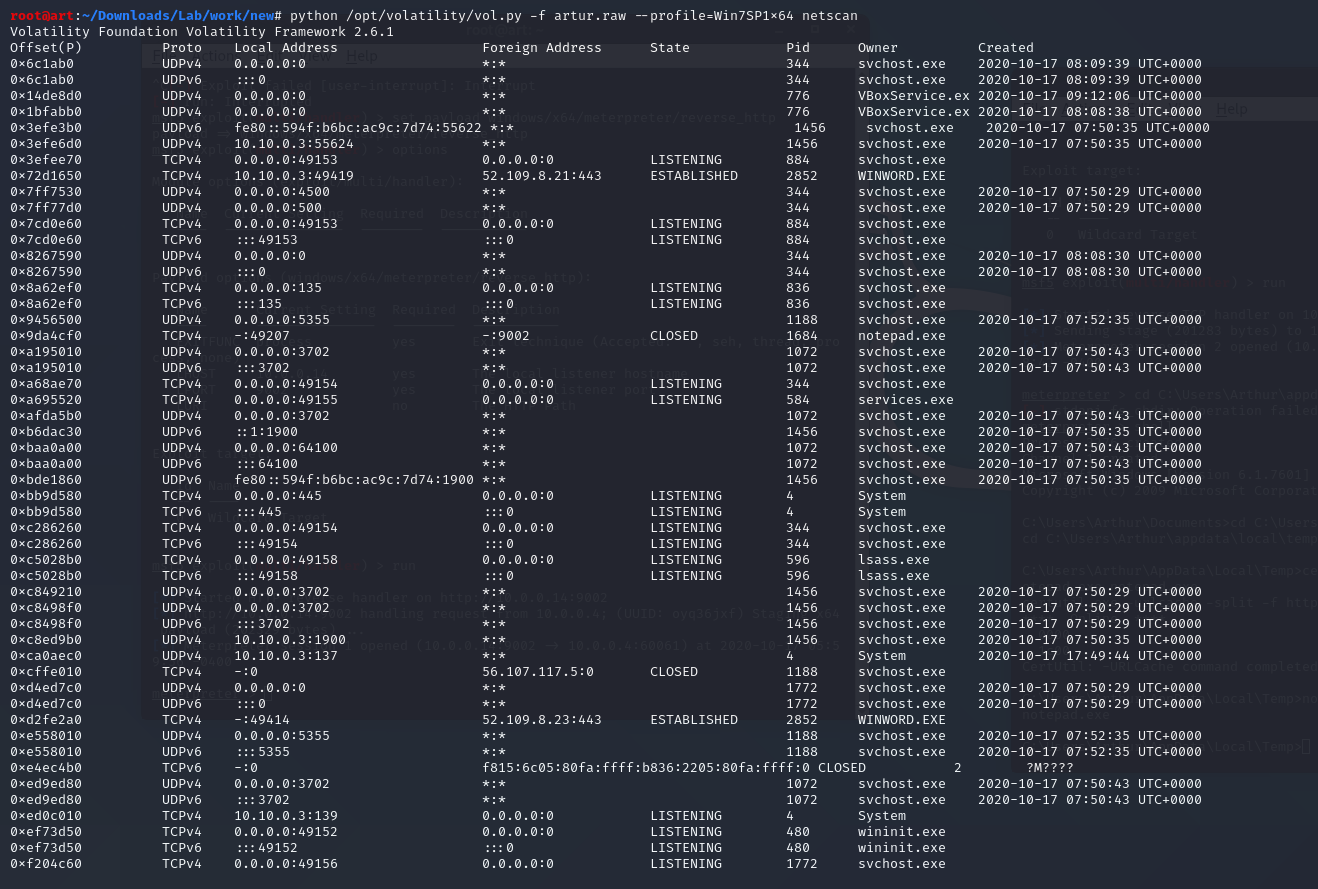


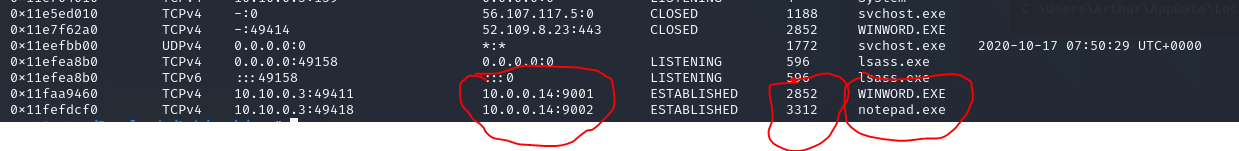
From above we first use the module pslist of volatility to get list of all the process, from here everything looks fine, as we can see I marked in red we find 1 suspicious process with the name notepad.exe lets continue investigate.



From above we use the module pstree of volatility to see the tree of the process that running live, as we can see everything looks fine, only 1 suspicious process with the name notepad.exe with number of ppid of 2292 which is the cmd.exe so as we know for now our suspicious process notepad.exe opened from the cmd which is very unique.

Now let’s continue use volatility and check about network connections.





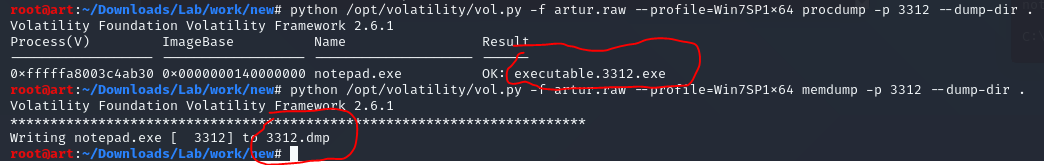
From 2 pictures above this time we use the module netscan of volatility and this module will show all the networks activities of this machine.

As we can see I marked in red, we find 2 suspicious sockets with remote ip: 10.0.0.14, there is 2 sockets that open one in port 9001 and 9002.

This 2 sockets running from the process WINWORD.exe and notepad.exe

We already find our suspicious notepad.exe and now we also see this process make remote connection to 10.0.0.14 which will be the first IOC.

Next step to download notepad.exe with pid number of 2280, and we will continue to investigate.



From the picture above after we find suspicious process with the name: notepad.exe and this process make remote connection to 10.0.0.14.

we used the modules procdump and memdump from volatility to download our suspicious executable and also downloaded the memory of the process.



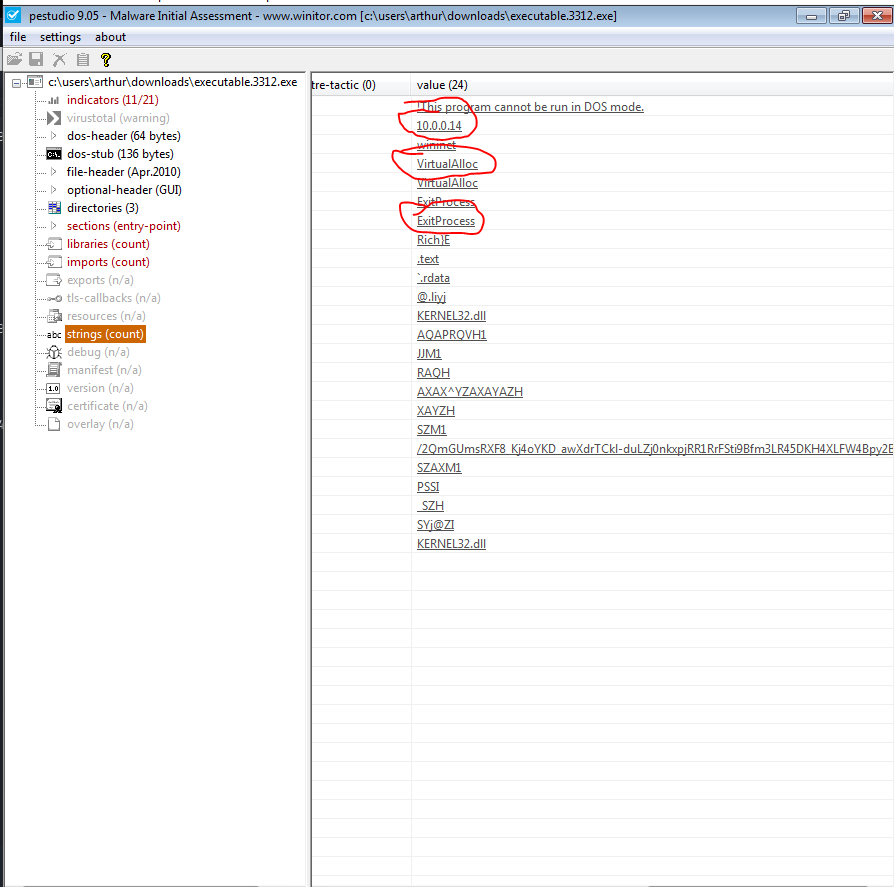


From the two pictures above we run strings on our 3312.dmp and we see from the output this process makes network connection to 10.0.0.14:9002. When this process executed he first make connection to 10.0.0.14 which will be the C&C of the attacker Great so we find our first IOC that indicates this process make remote connection to the attacker machine.

Next step starts investigates about notepad.exe from the pictures above we downloaded the suspicious process now let’s move on to analyze this suspicious process.

**Static Malware Analysis**

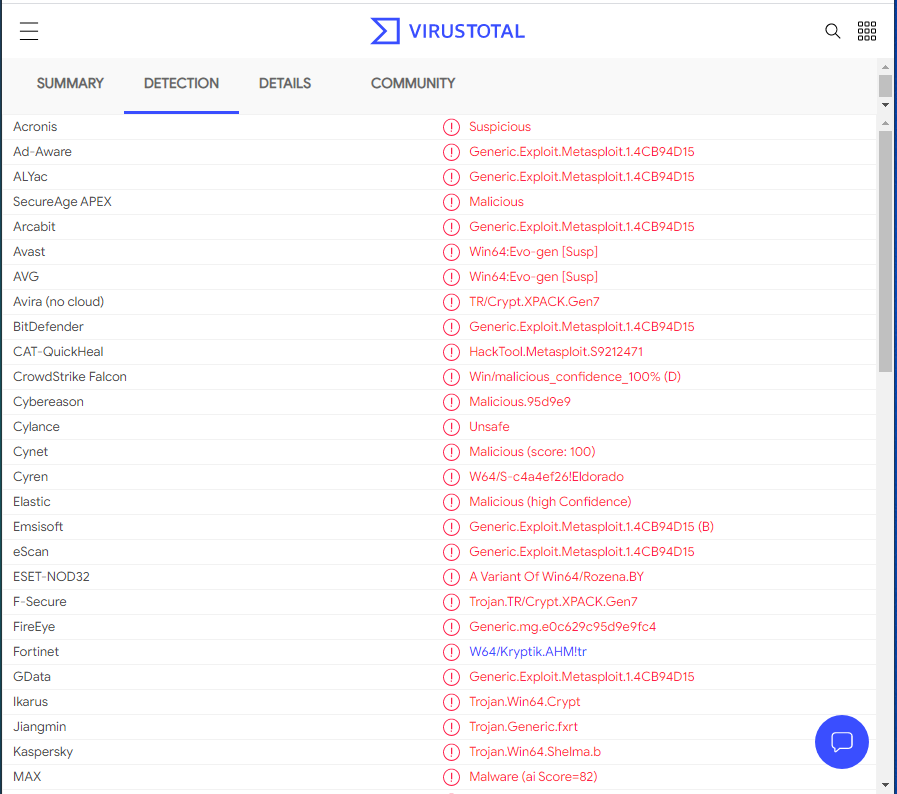
PEstudio



We use the tool pestudio to analyze suspicious process, as we can see from the picture on the strings ip of 10.0.0.14 which is the ip of the attacker and we see suspicious windows api’s that this executable running like VirtualAlloc and ExitProcess.

For now, we start understand that notepad.exe makes malicious activity with remote shell to the attacker machine. Let’s continue to upload our malicious file to virus total and see what result we got there.

Virus-Total



Clearly the executable is recoginized as malicious by virus total.

It is now time to sum up the different investigations we’ve made and our findings with the analyzed dump:

1. An odd process notepad.exe PID 3312 with explorer as ParentPID 2068

2. An opened connection towards 10.0.0.0.14:9001 and 9002 used by the PID 3312 and 2852

3. 3312 executable detected as malicious Trojan by sandboxing websites.

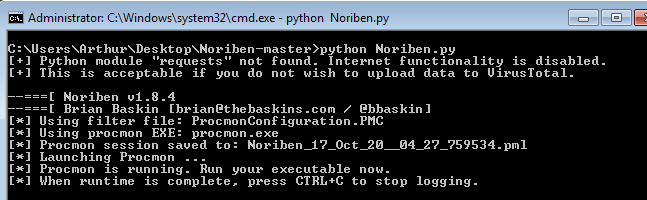
4.Word document on the user desktop with the name important.docm, which also open connection to 10.0.0.14 port 9001.

For now, we finished with our static malware analysis and we done great job with our findings, we find the malicious activity the first shell that comes to the attacker it’s when the user executed the word document, then the attacker drops another malware on the computer and open another socket this is why we saw 2 sockets open to 10.0.0.14 when we check network connections with volatility.

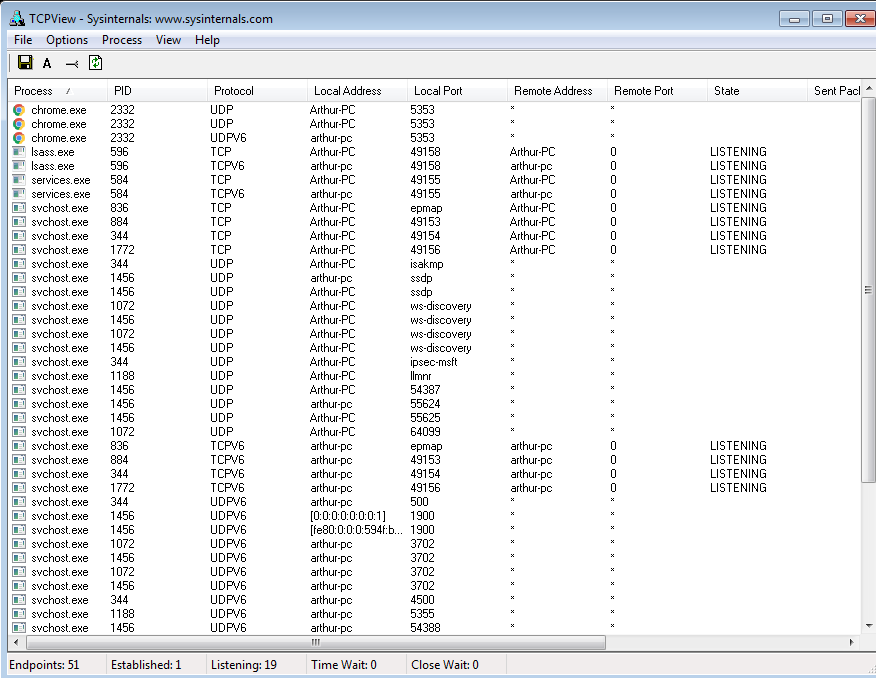
Next step will be move to dynamic malware analysis which we will run notepad.exe and we will check if this malware makes also modification to the registry keys or others. By now we know this malware makes remote connection to the attacker machine, so we need also check if this malware makes another modification.

Dynamic Malware Analysis

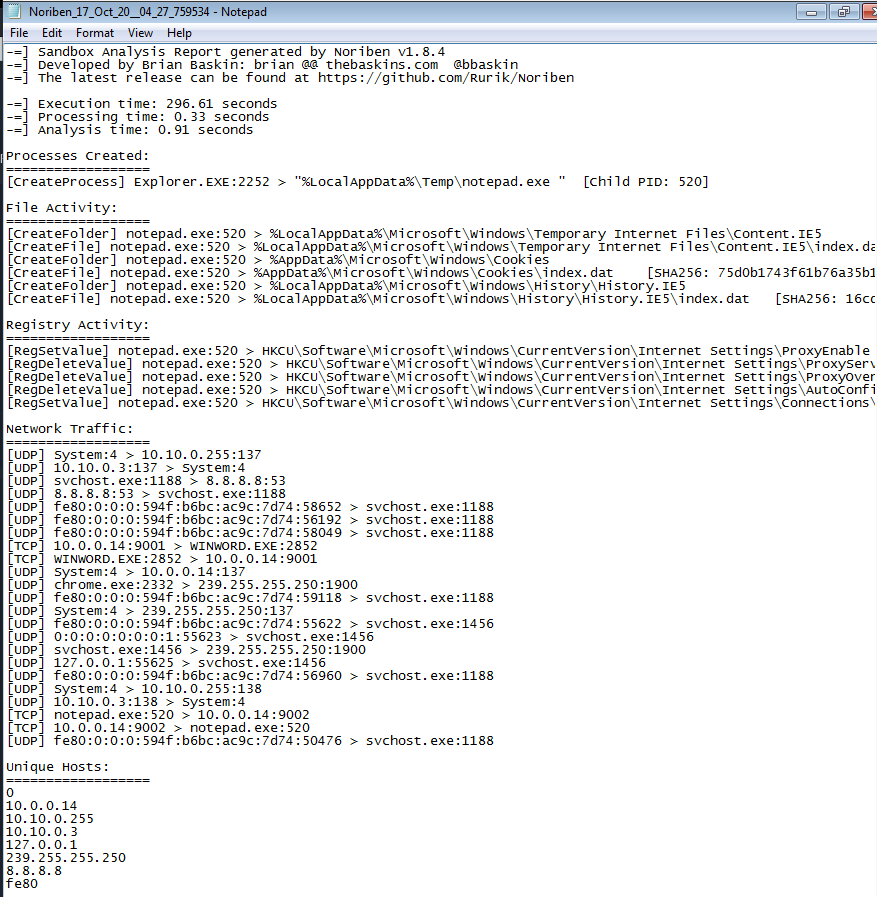
Noriben & TCP View



Next step from the picture above before we running our malicious file we start noriben which will display us all process interaction with the monitored pc.

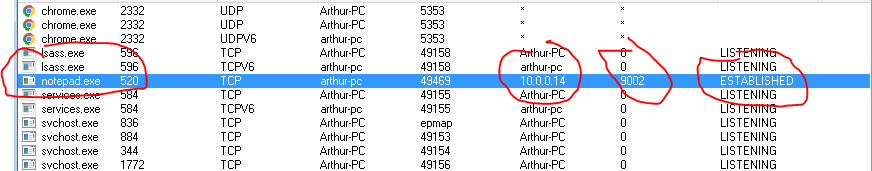


Here above we also running tcp view before we running our executable and this tool can help us understand if some process makes network connections. Now let’s run the executable!



Above we see the results after running noriben tool. The malware not modified something suspicious with the registry keys which mean we don’t see here persistency technique this malware only makes network connection to the C&C and by this the attacker have shell access to target.

Now let’s look at tcp view results after we running the executable.



As we can see above this is the result from tcp view which show us in clearly that this is a Remote Trojan, which make network connections to the attacker (10.0.0.14) right after the execution which mean this executable send information to the C&C that sits on 10.0.0.14.

For now, we find all we need about notepad.exe we know 100% that is remote Trojan.

Indicators of Compromise (IOCs)

1. SHA1 (executable.3312.exe) - b0f760973eadc7fb7be36f3fac655e12188479ad
2. SHA1 (Important.docm) - 8ea8ada673db9f4b0845f75f45949c3a90eb2ecd
3. Delivery URL – <http://10.0.0.14:9001>
4. Delivery URL - <http://10.0.0.14:9002>

We will add all IOC’s to our black list in order to prevent from this kind of malicious activity to take place in our network in the future.