MALWARE ANALYSIS: ANALYSIS REPORT OF INFO STEALER

Analysis report of Info stealer

Malware is one of the root causes for email spams and denial of service. So definitely yeah, malware is the most serious security threat today. With the increasing significance of the malware, more and more research is focused on the developing the tools and techniques to collect, detect and study the malware found. In this paper I propose analysis of malware using five different tools. Here the approach is to first analyze the malware sample which is collected in a controlled environment. Experiment here will show that the approach can effectively detect the behavior of the malware code running on the host machine.

Kerin Shah, CS458

4/19/2019

MALWARE ANALYSIS: ANALYSIS REPORT OF INFO STEALER

Section I: Introduction

Now-a-days internet has been become a part of everyone's life. As the technology advances so do the malware families. Everything including baking service, ordering food, online shopping and many more are the examples of internet services which are being used widely. Just like the physical world, there are many people who want to harm other people wherever the money is involved. So malware helps this kind of people to accomplish their goals. This paper contains the four sections. Section II describes the malware background. Section III presents the aims and objectives of this paper. Section IV describes the methodology of malware how it is analyzed. Finally section V describes the time line of this research.

Section II: Background

Now what is malware analysis: It is the process of determining the different properties of a given malware sample that not only includes Trojan horse but also virus, worms, etc. There are different tools which are used for studying this type of malicious behavior under some safe environment. Either you can do it on Virtual Machine or you can create honeypot environments for data safety. Now analysis can be divided into two types: static and dynamic (live) analysis. Static analysis tries to analyze the binary file without actually implementing it. Dynamic analysis focuses more on execution of malicious file in safe environment. More detailed knowledge about static and dynamic analysis is shown in [1]

Many researches are already being done on how to detect and analyze the malware [2]. Malware attacks have been around since the first well known malicious software, which was written in the early 1950s, widely known as a "self-reproducing machine". The evolution of malware over the years has contributed towards major security incidents or breaches which have caused major financial losses as well as reputational damage to many organizations. One of the examples of these malware attacks was the Sony Pictures hack in December 2014. According to a number of reports and security researchers, the malware that infected computers systems at Sony Pictures was named "Wiper" malware [2]. The malware was involved in the vast majority of these attacks according to the Verizon's 2016 Data Breach Investigation Report. Many researches are going which includes dynamic and static analysis of malware [3].

Section III: Aims and Objectives

This research is performed to increase understanding with tool Procmon, Process Explorer, Regshot, ApateDNS and Netcat that will be used for malware dynamic

analysis. This experiment will give a better picture about how malware analysis is actually performed in safe environment.

Section IV: Methodology

I have started my work by already installing Windows XP on my host machine. All tools which are required for analyzing the malicious file are described below. This malicious file is already available on [4].

Procmon: This is a real time windows based monitoring tool to understand modification in registry, network, and file system and process activity. The most useful feature of procmon is its capability to filter event based on various criteria like process, threat, operation and many other. So in malware analysis if you know the executable and function then you can use that as a filter. This will narrow down your search. Since it is showing event from process, system, registry and network it would be very easy to correlate activity in between. Procmon has ability log boot time operation that will help to find rootkit. It can be downloaded from https://technet.microsoft.com/en-us/library/bb896645.aspx.

Process Explorer: As name implies this tool helps to explorer process details. This tool shows the process opened or loaded dll. Process explorer helps to track down DLL version problems or handle leaks and provide insight into the way Windows and application work. It also shows all child processes. When you click on any process you can verify the process by checking their online signature and you have an option to upload process executable on VirtusTotal to scan it against various antivirus signatures. It also shows CPU utilization, private byte and description of the process. In malware analysis, you can use this tool to explorer related file like which process it is injecting or effective. Verify the process and check executable string.

RegShot: Regshot is command based tool to monitor only registry modification. It is useful to compare registry entries that have been changed during an installation or a change in your system. This tool is open source. When you deal with malware take the first snapshot, it will capture and record all registry entry then execute malware and after few minutes take second screenshot. Now to compare screenshot use compare option and it will show txt file which has information about modified and new registry entry.

ApateDNS: This tool is developed by Mandiant and available for free. This tool is use to control DNS response through easy to use GUI. User can define the address by listening on UDP port 53 on local machine. When you run the malware , if it tries to phone home DNS request then ApateDNS has ability to record that all entries.

NetCat: NetCat is known as Swiss Army for network security professional. It has ability to read write data across TCP or UDP network connections. Malware does

communication on port 80 or 443 because those ports are not blocked on network. NetCat will be used to listen on those ports to record network activity.

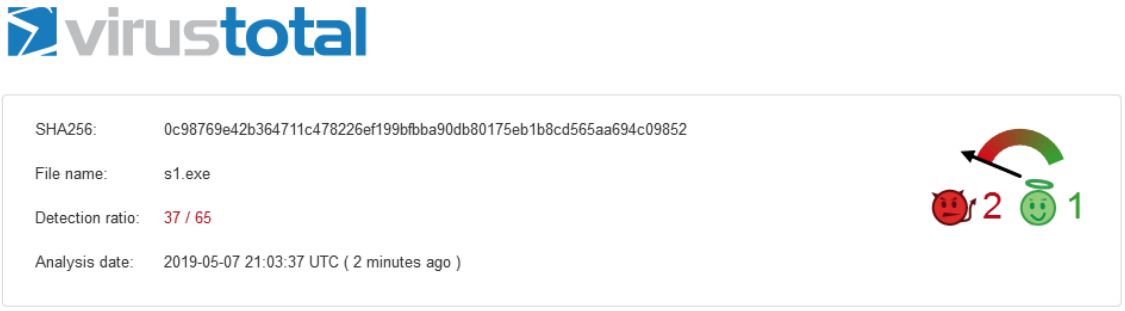
This experiment allows me to compare the behavior of the infected machine. Hence this small experiment will give me better knowledge about how the malicious code works and how the malware analysis is done.

Section V: Plan of Action

Date	Task
4/17	Downloaded all the tools and windows XP in Virtual machine
4/21	Running the file on VirusTotal
4/24	Perform the actual running of the file and observe on the Regshot and ApateDNS
4/26	Compare the two screenshots took through Regshot before and after host infection
4/26	Now it's time to observe in Netcat
4/30	Explore Procmon which continuously records all process events and explore the details about registry
5/2	Gathering all the raw data and observing the exact behavior change in host.
5/3	Documenting the results and experiments performed
5/4	Submission

Demo:

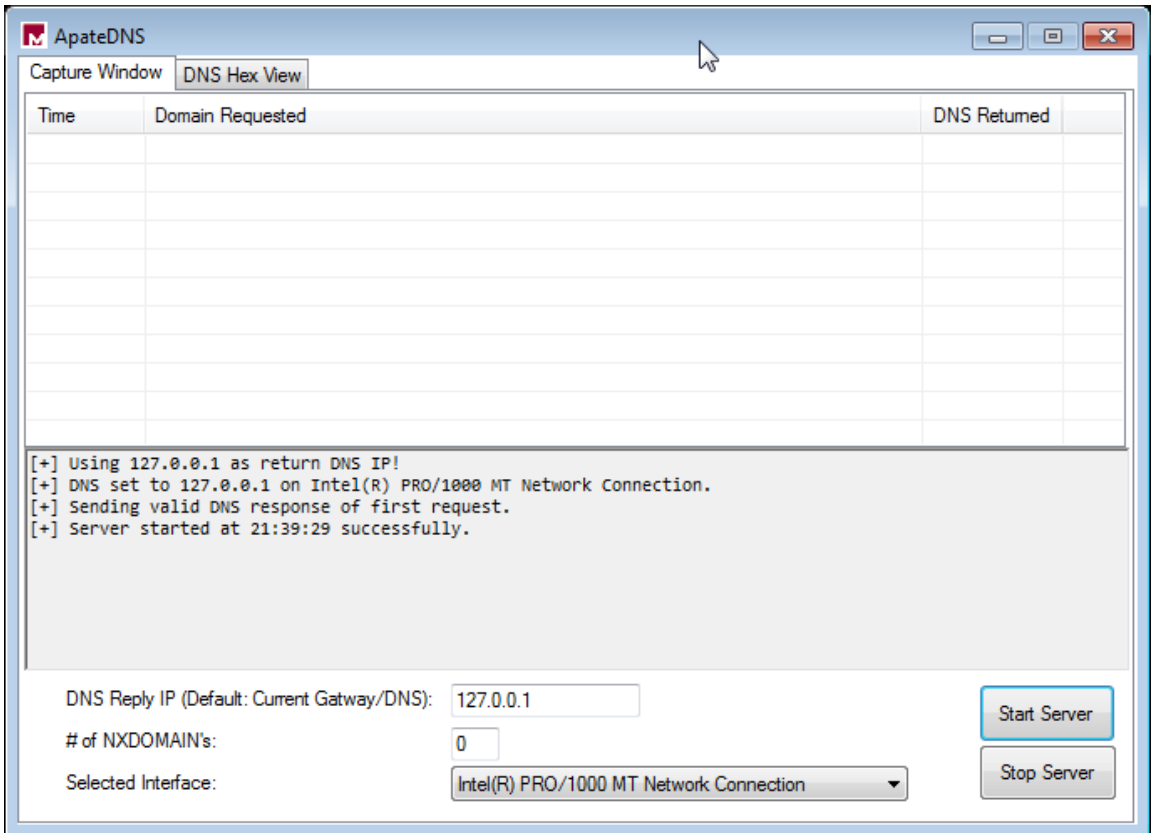
For demo I will be using s1.exe, which is an info stealer. My next step would be to upload a file on VirusTotal for scanning. VirusTotal aggregates many antivirus products and online scan engines [6] to check for viruses that the user's own antivirus may have missed, or to verify against any false positives.



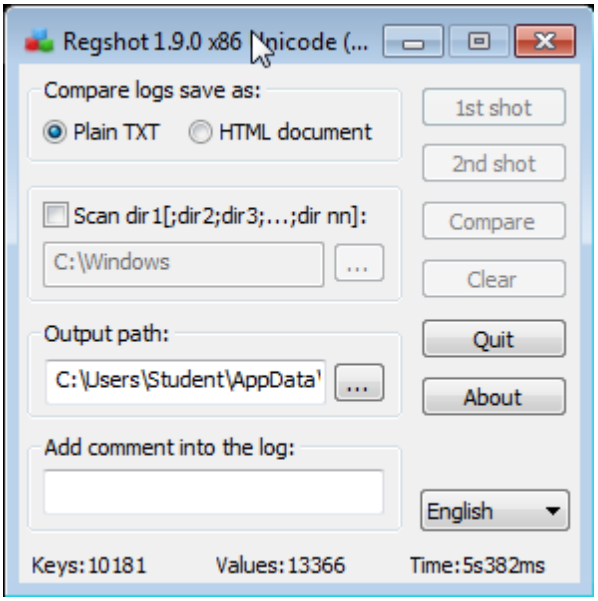
Antivirus	Result	Update
Acronis	suspicious	20190504
Ad-Aware	Gen:Variant.Jaik.18436	20190507
AegisLab	Trojan.Win32.Generic.4!c	20190507
Alibaba	TrojanClicker:Win32/Tiggre.55f4f681	20190426
ALYac	Gen:Variant.Jaik.18436	20190507
Antiy-AVL	Trojan/Win32.TSGeneric	20190507
Arcabit	Trojan.Jaik.D4804	20190507
Avast	Win32:Trojan-gen	20190507
AVG	Win32:Trojan-gen	20190507
Avira (no cloud)	HEUR/AGEN.1010968	20190507
BitDefender	Gen:Variant.Jaik.18436	20190507
CAT-QuickHeal	Genvariant.Jaik	20190507

So as you can see in the above screen shot all antivirus marked “s1.exe” as malicious.

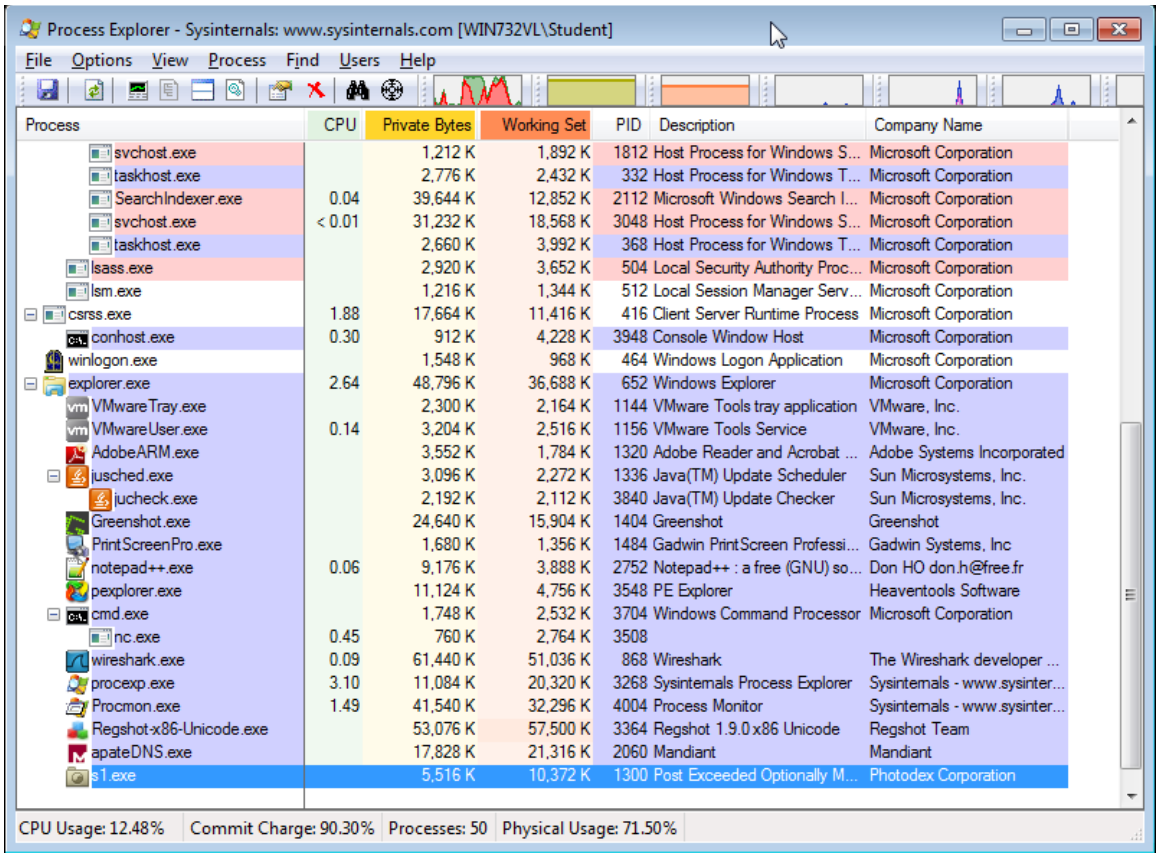
Before running the malware file i.e. s1.exe, setup the ApateDNS and Netcat to detect network activity. We are running DNS server on localhost so use DNS reply IP as 127.0.0.1.



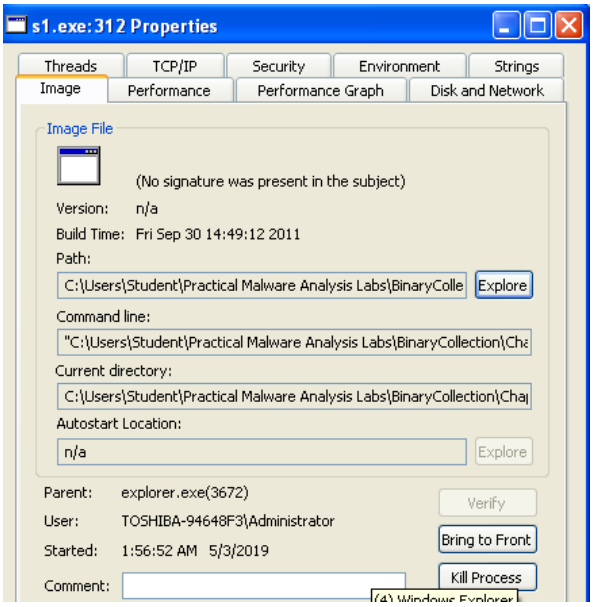
Now open the Regshot, It has following GUI. It doesn't require much configuration since default setting works perfectly. Take the 1st screenshot of all registry.



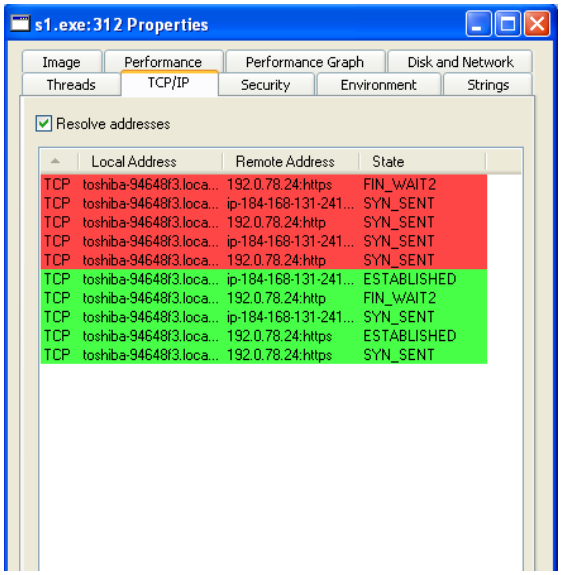
Now all setup is done. It is time to run executable. First, I would start with tool Process Explorer to get understanding about process. Below screenshot, you can see the s1.exe which is signed by the Photodex Corporation. As seen in that we have other tool running like Netcat, Wireshark, Procmon, Regshot and ApateDNS. Now click on the process and select properties.



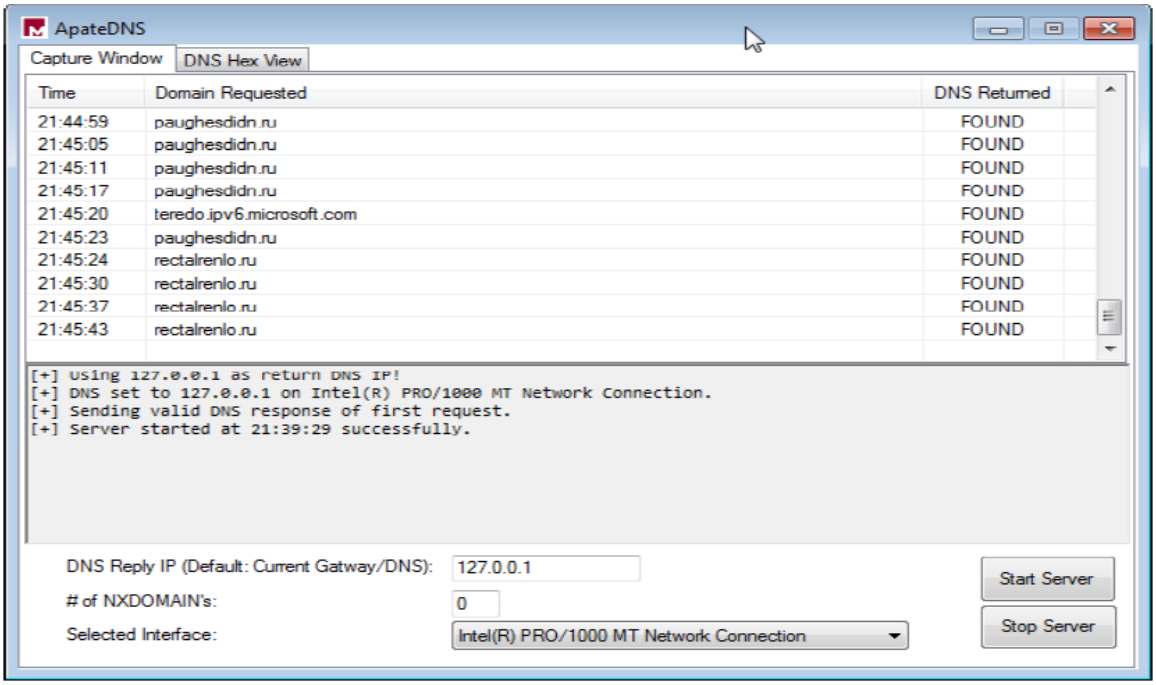
It provides the various information like GPU uses, modified or created threat, TCP/IP network activity, executable string info, disk and network uses. In this window you can see the executable file path. I clicked on verify button so it showing that “No Signature was Present in the subject”. You can also submit the file on VirusTotal for scan. This provides basic information about running process.



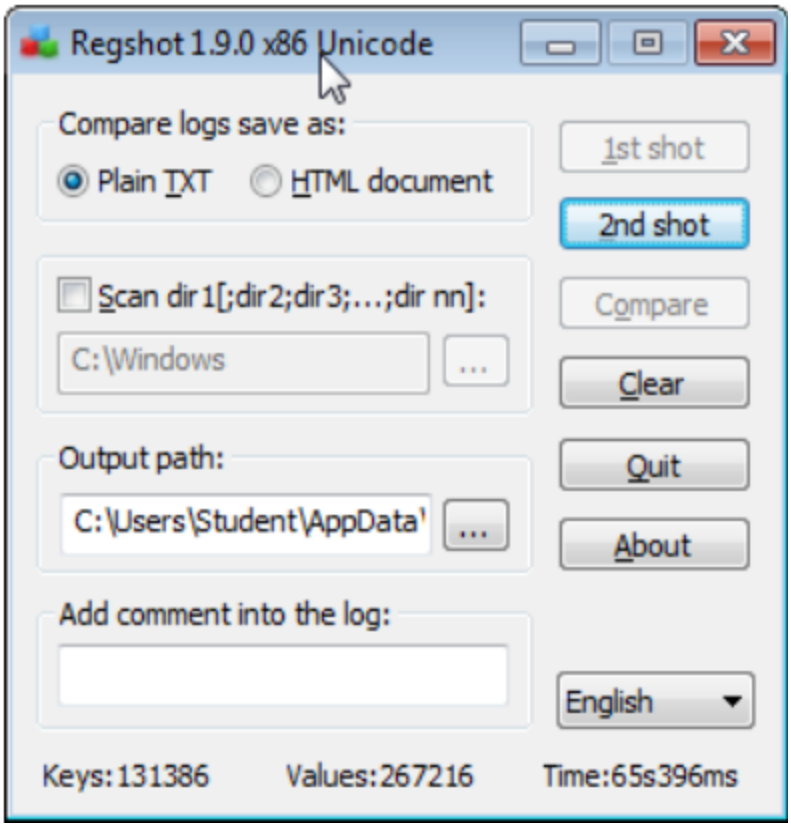
In the process properties, click on TCP/IP tab to see live network connection. As you can see host is connecting with external IP over http from source port 51909.



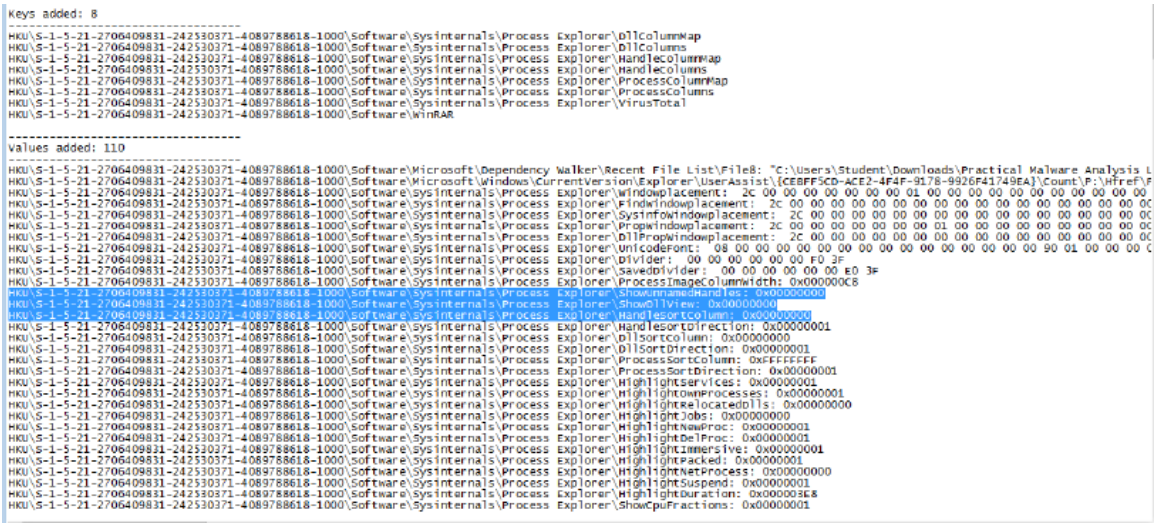
ApateDNS was able to capture some DNS lookup as result shows malware was trying to communicate with Russian domain. Paughesdidn.ru and rectalrenlo.ru. It doesn't provide any other information like full packet capture.



Now, we need to take the second registry record shot. So click on 2nd shot and when the process is done click on compare button and it will show registry comparison in text file.

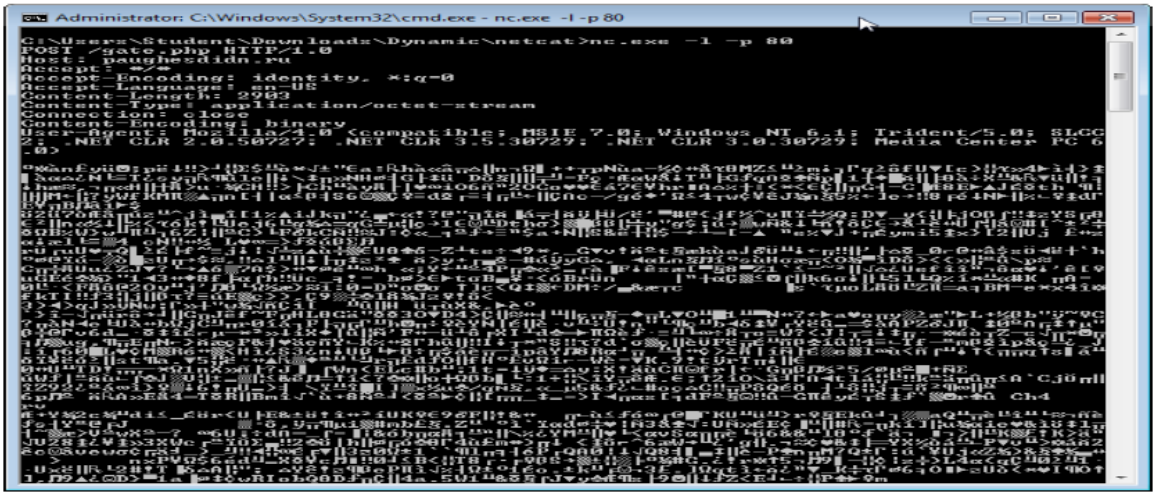


As you can see comparison shows full registry path with new registry key and value. We can use this path to explore registry details. Since this is a very sophisticated malware it did lots of modifications.

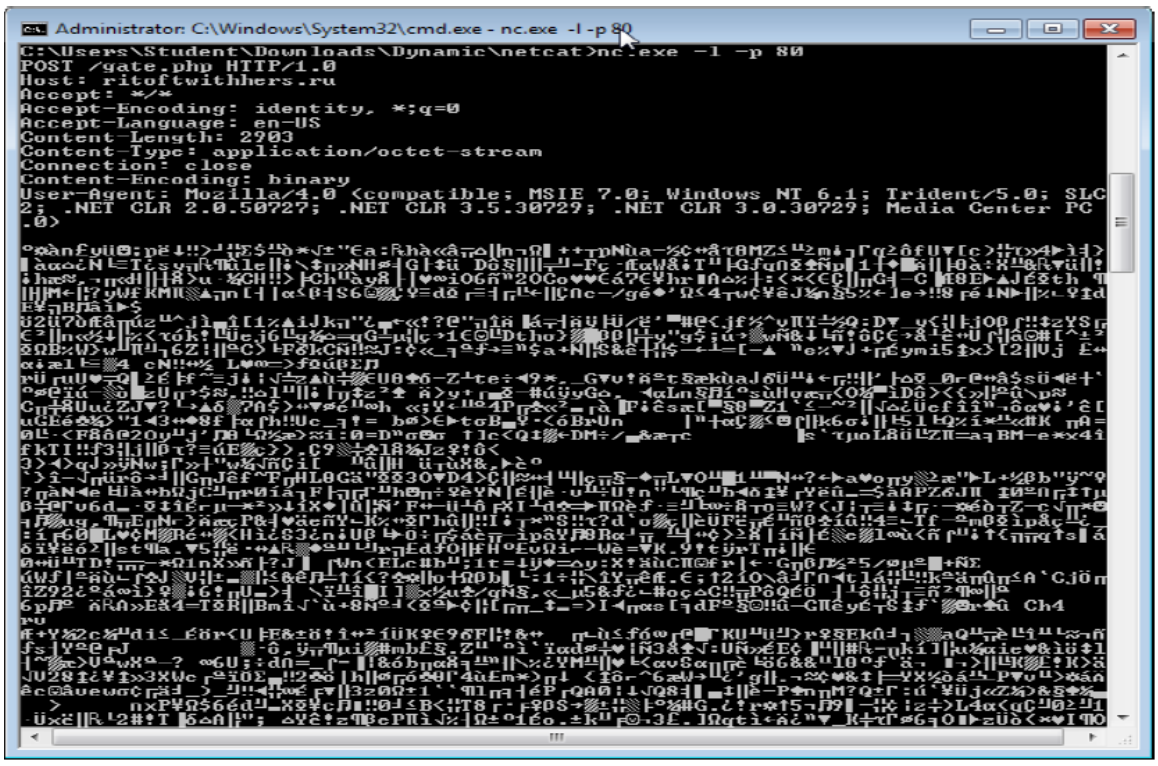


It's time to explorer Netcat. I used option –l for listen and –p for port. We are listening on port 80. I was able to capture first http post request which was sent to URL http://paughesdindu.ru/gate.php.

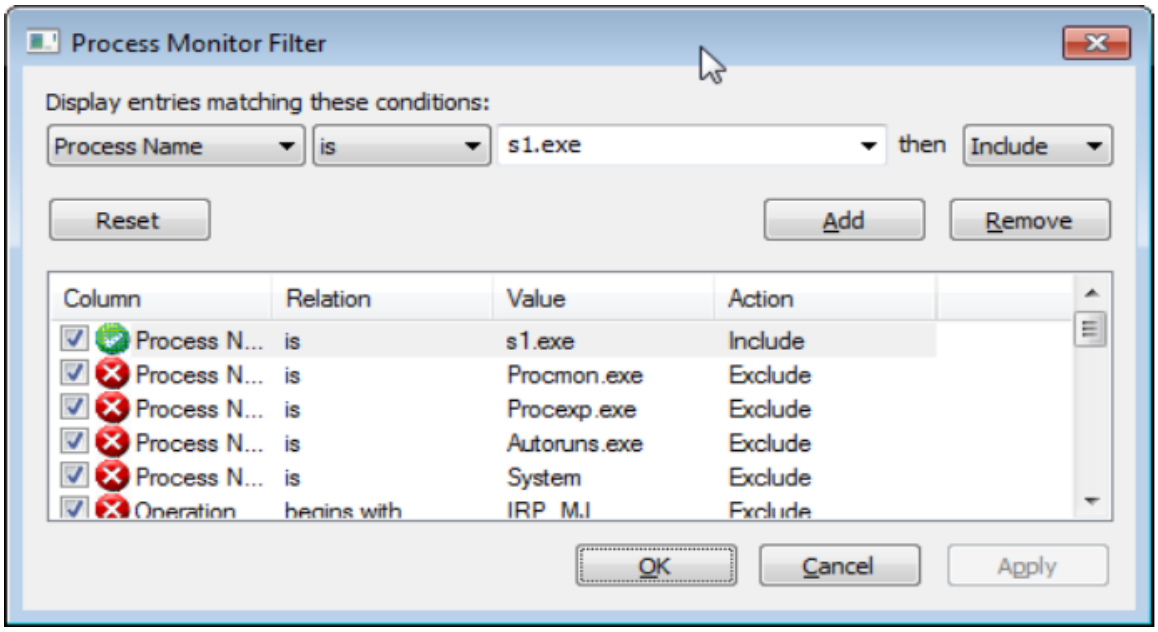
It also shows the information like Content type, content encoding, and user agent and host information. This information can be useful to create IDS signature to detect intrusion.



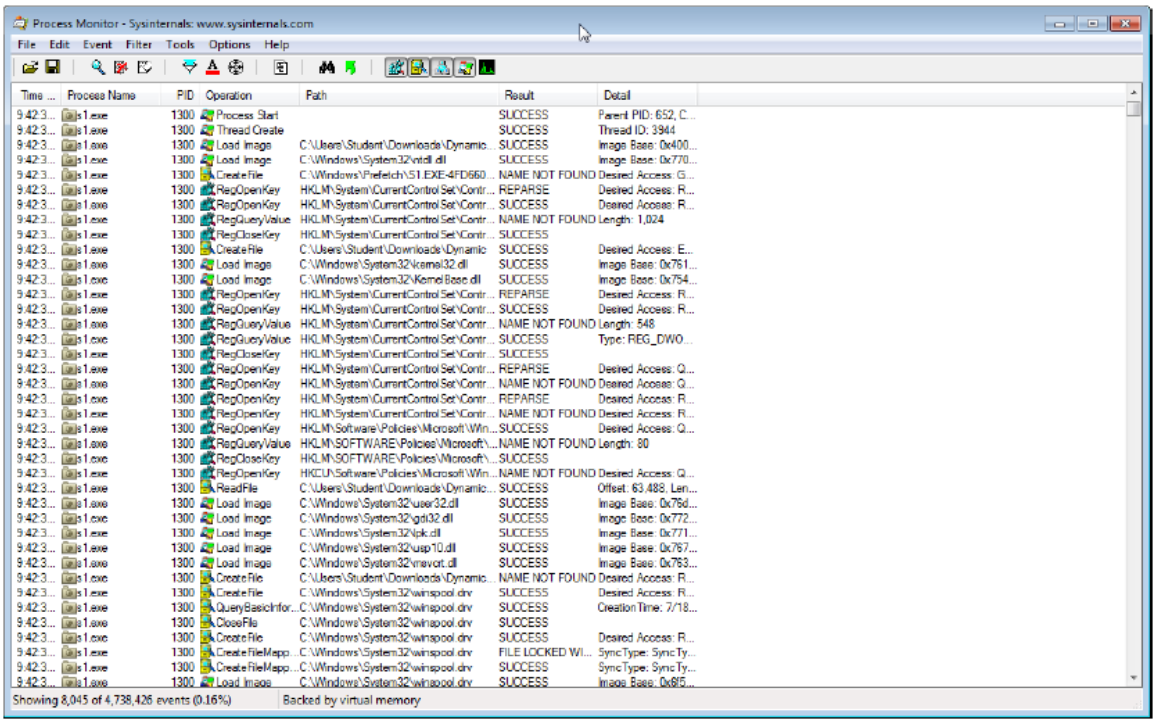
After continues monitoring, it detected connection with another domain but it has a similar directory path. This is also a Russian domain ritoftwithhers.ru. The payload detected in both communications was the same.



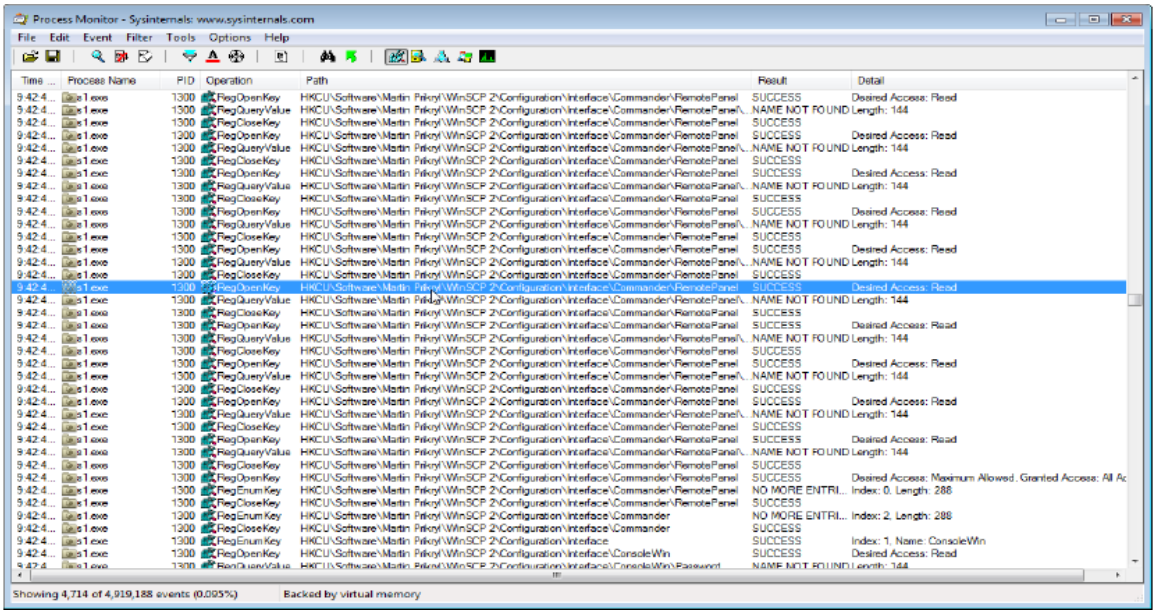
Now let's explore the Procmon, It continuously records all process events. For better outreach I added process filters which for s1.exe. So it will show all file system, registry, network and process events.



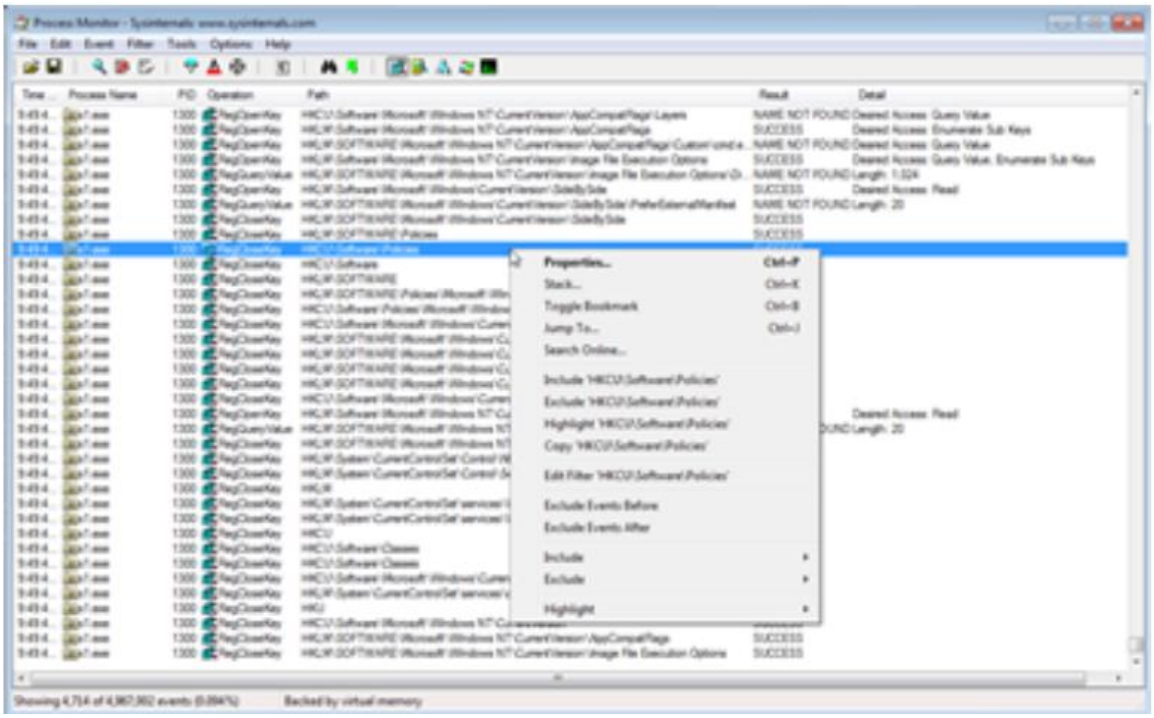
We can see below all the s1 process events. It shows the process ID, result of the operation and some details. Below screen shot shows file system event, registry entry and threat information. It shows the full path for further search.



In case if you only want to explorer registry event select registry option from the Toolbar. It shows RegistryOpenKey, RegQueryValue and RegistryCloseKey with Registry path and operation result. You can also confirm this result with Regshot.

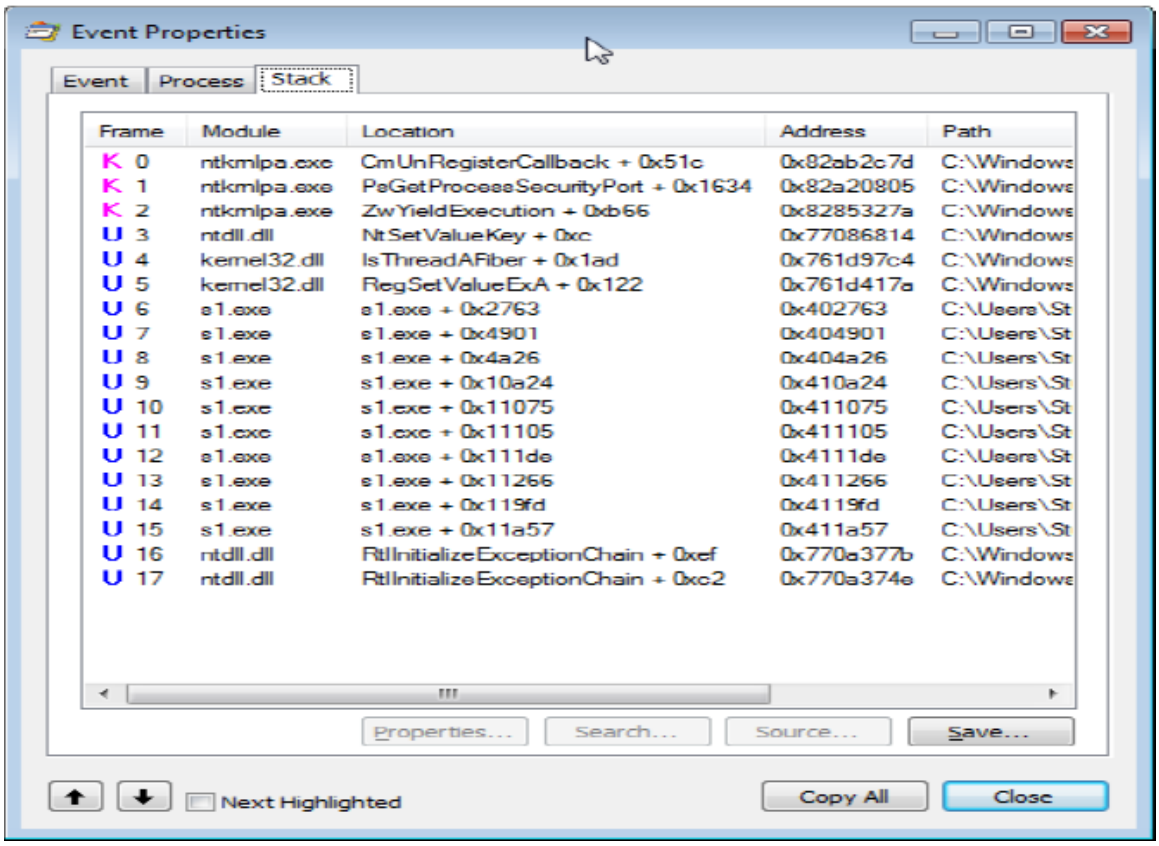


To explorer the details about Registry event right click on it and select properties.

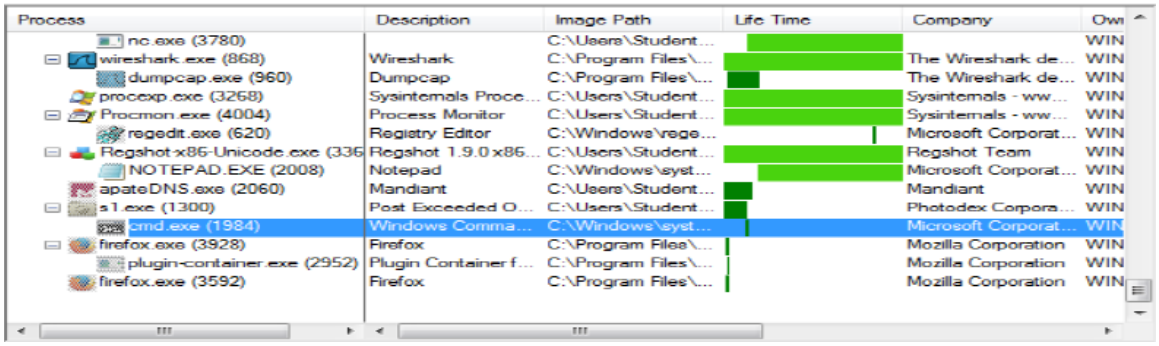


Event properties show the path of the executable, PID, Architecture info, AuthID and process start end time as well. Bottom of the windows it will show all module information that were run during process. To get more information about module select

stack option. As you can see take use various exe and dll module to perform various functions.



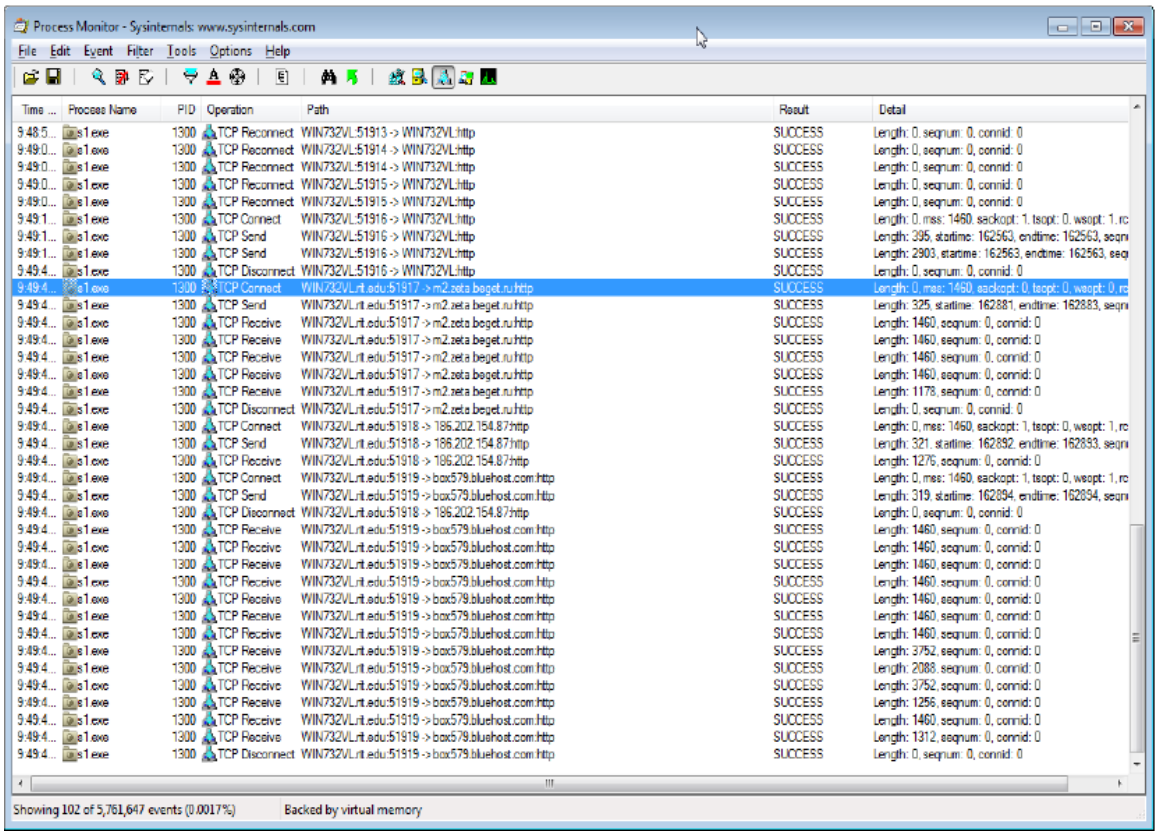
From menu bar select tool option and chose process tree option. It will show similar interface like process explorer. This will show the full life spam of process. It will help to understand how far the malware stay awake before going for sleep and what operation and process it access. You can click on any process and select GotoEvent option to relate process details.



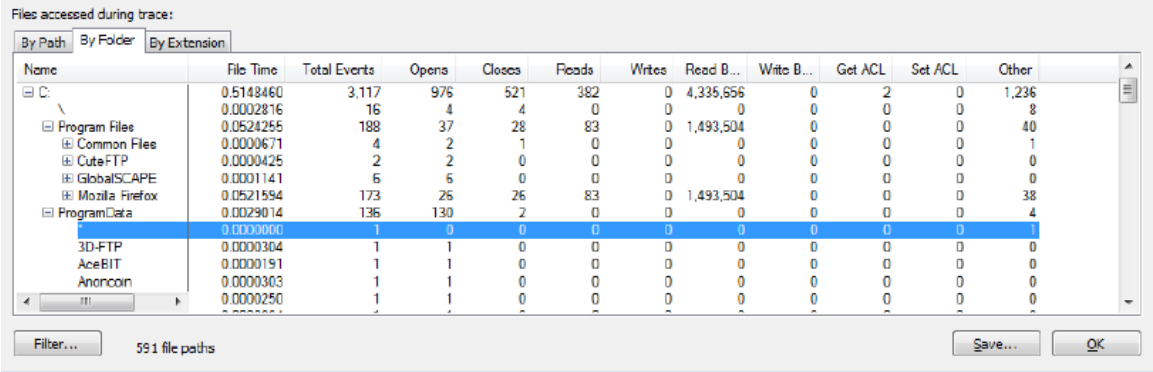
Event details of network show the static data like amount of data transfer and receive. This information is very useful during incident response process of data breach. This malware could send sensitive information over internet.

```
Length:                 0
mss:                    1460
sackopt:                1
tsopt:                  0
wsopt:                  1
rcvwin:                 8192
rcvwinscale:            8
sndwinscale:            8
seqnum:                 0
connid:                 0
```

Below is the network event that can be correlate with Netcat and ApateDNS for better understanding. We can say that initial http request were post request based on Netcat information.



In tool select file summary it will show information like which folder was access most and if you dive dipper it will also show the most accessed file.



Section VI: References:

[1] Malware Analysis: https://www.researchgate.net/publication/267777154_Malware_Analysis

[2] Effective and Efficient Malware Detection at the End Host: https://www.usenix.org/legacy/event/sec09/tech/full_papers/kolbitsch.pdf

[3] Malware Analysis and Detection in Enterprise Systems: https://sci-hub.tw/https://ieeexplore.ieee.org/document/8367429

[4] Labs: https://practicalmalwareanalysis.com/labs/

[5] Malware Behavioral Analysis System: TWMAN: https://sci-hub.tw/https://ieeexplore.ieee.org/document/5953604

[6] About VirusTotal: https://support.virustotal.com/hc/en-us/articles/115002146809-Contributors