International Journal of Engineering & Technology, 7 (2.7) (2018) 225-229

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Study and analyze the locky ransomware using malware analysis techniques

K. Sri Vayuputra [1] *, Dr. K. V. D Kiran [2]

[1] *M.Tech , Department of Computer Science & Engineering &KLEF, Guntur, Vaddeswaram Andhra Pradesh, India – 522502*
[2] *Professor, Department of Computer Science & Engineering &KLEF, Guntur, Vaddeswaram Andhra Pradesh, India – 522502*
**Corresponding author E-mail: Vayuputra.k@gmail.com*

Abstract

Today most important tasks are carried in digital form this leads to increase in digital assets like laptops, smart phones, smart watches this involves in generate wide range of unique data storing in digital format like photos, voice clips, Documents, Videos, contacts etc. These all devices are connected to internet particularly laptops and smart phones. Weak security architectures always leads a chance to attackers to attack systems related to individuals, Corporates, Governments, Hospitals, Educational institutions etc. This attacks will bring huge data breaches, stealing of intellectual properties, encrypting the personal and confidential data.

Keywords: *Ransom; Ransomware; Digital Assets; Locky; Encryption; Decryption.*

1. Introduction

Ransomware is a kind of malware which encrypts our personal data without the victim's knowledge and the attackers demand money(ransom) to decrypt the files. There are large number of ransomware variants in market. We choose a ransomware called locky which is very well known and largely effected by many computer.

2. Locky ransomware

Ransomware is a kind of malicious software which encrypts the files in the victims systems and demand for ransom. locky ransomware is first centered in 2016 and termed as one of the most spreading ransomware. It locks every file with a locky extension. Then the locky asks for ransom to recover the files. It spreads in the form of phishing mails with the extensions of please print, photos, videos, images, scans etc. This has extorted more that $7.8 million in payments according to recent study by google, Chainalysis, UC san Diego. Recently India is effecting with this locky ransomware and strict instructions are passed to not open the spam mails.

3. working of locky ransomware

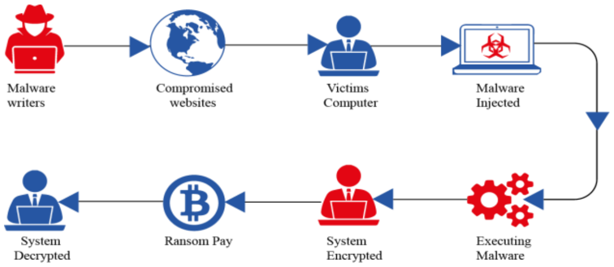


Fig. 1: Locky Ransomware Working Process.

1) Malware writers: Malware writers will design the ransomware according to their requirements and targets they use their own encryption techniques and attack methods. Mainly this ransomware will encrypt the users data but won't delete and stress user to pay ransom in bitcoins to decrypt the files.
2) Compromised Websites: Malware writers will compromise some websites like torrents and spread that malware to the end users.
3) Victims Computer: Victims computer will always contain the personal and confidential data. When that data is corrupted. End user will suffer a lot and lost the personal data.
4) Malware Injected: When a victim or end user visits that compromised site then the ransomware will automatically inject into the victims pc and reside over some memory.
5) Executing the malware: When the malware is injected this will execute in background without interrupting the users work. After final execution this will encrypt all the files in the system.
6) System encryption: Ransomware will encrypt all the fill with some ransomware extensions. Mainly ransomware will target the extensions like .png, .jpeg, .ppt, .doc, .docx, .mp3, .mp4, .rar, .xls, .exe and some other type of extensions present in the ransomware database.
7) Ransom Pay: This is the main phase in ransomware attack paying ransom to the attacker. After infecting the files attacker leaves some instructions to pay ransom by installing tor browser and pay some ransom using the bitcoins.
8) System Decryption: After paying the ransomware the attacker with send the decryption key to decrypt the system. In most cases the attacker won't send the decryption key.

4. Malware analysis

Dissecting malware into small parts and observing the every functionality in it. This procedure will reveal the core functionalities of the malware and generate the detail report on particular malware. This report will helpful in generating the anti-malware software. Generally antivirus companies will perform this kind of analysis to develop anti-virus software's.

5. Types of malware analysis

There are different kind of techniques used to analyse the malware.

1) Static malware analysis.
2) Dynamic Malware analysis.
3) Automated Malware analysis.
1) Static malware analysis: In static analysis. Analyst won't execute the code before executing the malware they will analyse the binary of the code by studying the functionalities. There are different methods used to study the malware.
1) Scanning it with Anti-virus tools
2) Generating the hashes and comparing
3) Observing the strings in code

Scanning it with Anti-virus tools: Anti-virus software mainly works on database. When the developers update the malware signatures then the anti-virus software's can able to detect the malwares. When new variants of malware evolves they can't able to detect them. At this point anti-virus software's will fail. There is an another online tools know as virus total by uploading the malware into that website it will scan with different types of antivirus software and display the final analysis report to the user.

Generating the hashes and comparing: Analyst will generate different kind of hashes and search them in some repositories. These hashes are useful in sharing to other analyst.

Observing the strings in code: Every binary will contain some string related to imports and exports. When the analyst try to retrieve those strings this will be very helpful and the analyzation will become easy. But some malware are packed. A wrapper program is executed before the program is executed this program will hide the strings. Analyst will face difficulty in analysing the malware. Analyst can use some tools to find weather the binary is packed or not.

2) Dynaminc Malware analysis: While performing the dynamic analysis analyst will execute the code and observe the changes happing in the system. We use windows xp as analysis environment. There are different kinds of tools and techniques to observe the behavior.

Process explorer: This tool is used to observe every process in the system.

Regshot: Regshot is another tool used to capture the data pre and post execution of mawlare.

Wireshark: To perform the network analyzation we use wireshark to capture full packet data. While analyzing the network there is a chance to get the attacker IP address because some variants in malware will communicate with attacker's server and downloads some support files into the system.

IDAPro: This tool is used to observe the functionalities in the binary. But IDA pro will show every function in assemble language so the analyst should have good idea on the assembly language.

Ollydgb: Olly debugger is a kind of binary code analyzer which scans every functions in code without using the source code this recognizes registries, API calls, constants, strings and procedures. Ollydgb is also used for cracking the software also.

3) Automated Analysis: The term automated analysis reflects automation of malware analysis. We use cuckoo sandbox as a tool and upload the malware samples into it. Now the sandbox will execute the malware in the controlled environment and observe the behavior of the malware and generate the analysis report to the analyst. But this is quick and dirty approach to analyze the malware. Sometimes this tools wont observe some important functions in the malware. There is an online tool known as malwr (www.malwr.com). This is designed by using cuckoo sandbox.

6. Analysis part

Malware should be analysed in a controlled environment. When a malware is analyzed in controlled environment it won't spread to other systems. To configure a controlled environment we use a virtualisation tool know as VMware workstation.

1) Configuring the secure environment for analyzing

Create a new virtual machine with 1 GB Ram, Hard disk space of 40 Gb, Network in Host only mode. Host only mode won't spread the malware through network. This safeguards the host system.

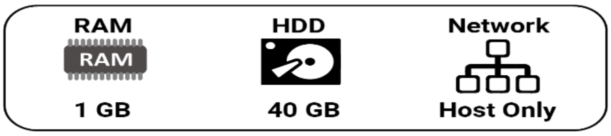
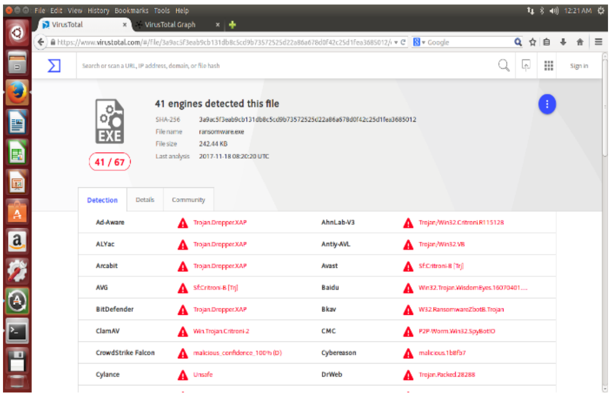


Fig. 2: Virtual Machine Configuration.

After configuring the vm ware now install the windows XP. After completing the installation take a snap shot. This is termed as fresh state if anything goes worse analyst can able to roll back into fresh state. In this way secured analysis environment is created. This secure environment will maintain a thin layer of separation between the VM ware and host machine.

7. Basic Malware Analysis

Analysing the malware using basic malware analysis techniques. Here we choose a ransomware sample ransom.exe. Before diving into the secure environment we should upload the sample into the virustotal website and observe the results there.


File Edit View History Bookmarks Tools Help
12:21 AM
VirusTotal
VirusTotal Graph
https://www.virustotal.com/#/file/3a9ac5f3eab9cb131db8c5cd9b73572525d22a86a678d0f42c25d1fea3685012/
Google
Search or scan a URL, IP address, domain, or file hash
Sign in
EXE
Detection
Details
Community

41 engines detected this file

41 / 67

SHA-256 3a9ac5f3eab9cb131db8c5cd9b73572525d22a86a678d0f42c25d1fea3685012
File name ransomware.exe
File size 242.44 KB
Last analysis 2017-11-18 08:20:20 UTC

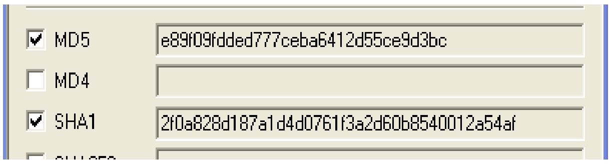
Ad-Aware	Trojan.Dropper.XAP	AhnLab-V3	Trojan/Win32.Critroni.R115128
ALYac	Trojan.Dropper.XAP	Antiy-AVL	Trojan/Win32.VB
Arcabit	Trojan.Dropper.XAP	Avast	Sf:Critroni-B [Trj]
AVG	Sf:Critroni-B [Trj]	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Trojan.Dropper.XAP	Bkav	W32.RansomwareZbotB.Trojan
ClamAV	Win.Trojan.Critroni-2	CMC	P2P-Worm.Win32.SpyBot!O
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.1b8fb7
Cylance	Unsafe	DrWeb	Trojan.Packed.28288

Fig. 3: Virus Total Analysis Report.

Hash SHA256 - z3a9ac5f3eab9cb131db8c5cd9b7357572525d22a678d0f42c25d1fea3685012

Scan Report showed that the ransomware is scanned by 67 antivirus and 41 detected that file as virus. So we should be very care while handling this file.

Calculating Hash using MD5 : Hash can be calculated using Hashcal tool as shown in the below screen shot [1].



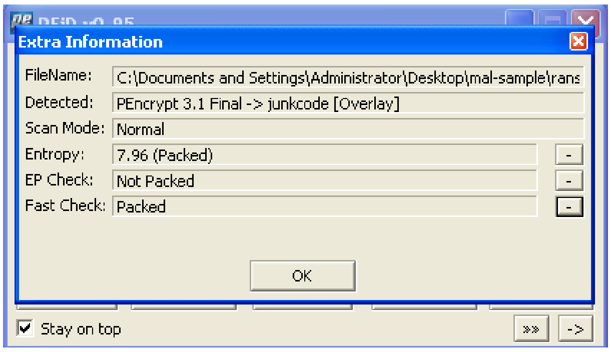
☑ MD5 e89f09fdded777ceba6412d55ce9d3bc

□ MD4

☑ SHA1 2f0a828d187a1d4d0761f3a2d60b8540012a54af

Fig. 4: Hash Calculation for Malware.Exe Sample after Calculating the Hash this can be shared among Different Analyst and Mainly this Hash Calculation Is Used for Integrity Check.

Observing the Strings: Several malware variants of malware's are packed or obfuscated. A small consolidate program is executed before the malware is executed this will hide the functionalities and strings in ransomware. To identify weather the malware is packed or not we will use a tool known as PEid which show weather the malware is packed or not. As shown in the below screenshots.



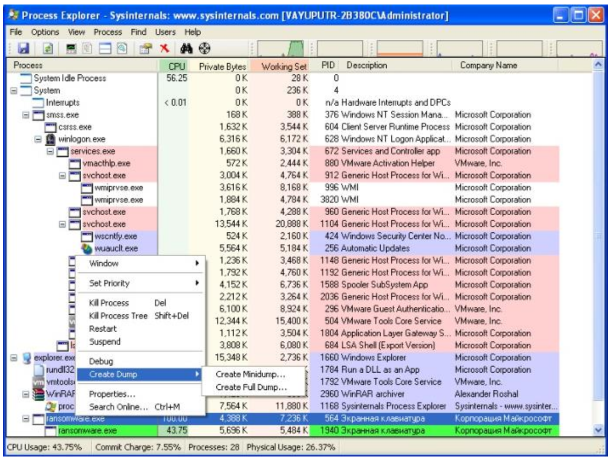
FileName:	C:\Documents and Settings\Administrator\Desktop\mal-sample\rans
Detected:	PEncrypt 3.1 Final -> junkcode [Overlay]
Scan Mode:	Normal
Entropy:	7.96 (Packed)
EP Check:	Not Packed
Fast Check:	Packed

Fig. 5: PEID Packer Detection.

By using a tool peid we have detected that the malware is packed so we want to extrac strings from them using different techniques.

Detection of strings in packed malware:

When we try to extract strings from packed malware all the strings will hide. Now we want to extract the strings from the malware. Take a snapshot of present state in VMware. Now open a tool known as process explorer and execute the binary now. After some time take a full process dump of that process and save on the desktop.



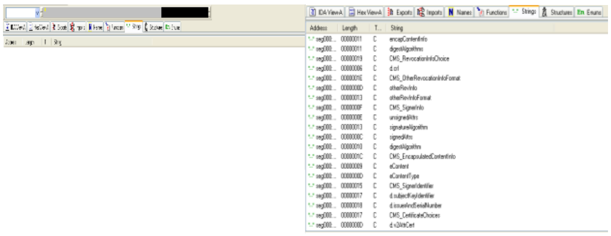
Process Explorer - Sysinternals: www.sysinternals.com [VAYUPUTR-2B380C\Administrator]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	56.25	0 K	28 K	0		
System		0 K	236 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		168 K	388 K	376	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1,632 K	3,544 K	604	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,316 K	6,172 K	628	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,660 K	3,304 K	672	Services and Controller app	Microsoft Corporation
vmacthlp.exe		572 K	2,444 K	880	VMware Activation Helper	VMware, Inc.
svchost.exe		3,004 K	4,764 K	912	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe		3,616 K	8,168 K	996	WMI	Microsoft Corporation
wmiprvse.exe		1,884 K	4,784 K	3820	WMI	Microsoft Corporation
svchost.exe		1,768 K	4,288 K	960	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13,544 K	20,888 K	1104	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		524 K	2,160 K	424	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		5,564 K	5,184 K	256	Automatic Updates	Microsoft Corporation
		1,236 K	3,468 K	1148	Generic Host Process for Wi...	Microsoft Corporation
		1,792 K	4,760 K	1192	Generic Host Process for Wi...	Microsoft Corporation
		4,152 K	6,736 K	1588	Spooler SubSystem App	Microsoft Corporation
		2,212 K	3,264 K	2036	Generic Host Process for Wi...	Microsoft Corporation
		6,100 K	8,924 K	296	VMware Guest Authenticatio...	VMware, Inc.
		12,344 K	15,400 K	504	VMware Tools Core Service	VMware, Inc.
		1,112 K	3,504 K	1804	Application Layer Gateway S...	Microsoft Corporation
ls		3,808 K	6,080 K	684	LSA Shell (Export Version)	Microsoft Corporation
explorer.ex		15,348 K	2,736 K	1660	Windows Explorer	Microsoft Corporation
rundll32				1784	Run a DLL as an App	Microsoft Corporation
vmtools				1792	VMware Tools Core Service	VMware, Inc.
WinRAR				2960	WinRAR archiver	Alexander Roshal
proc		7,564 K	11,880 K	1168	Sysinternals Process Explorer	Sysinternals - www.sysinter...
ransomware.exe	100.00	4,388 K	7,236 K	564	Экранная клавиатура	Корпорация Майкрософт
ransomware.exe	43.75	5,696 K	5,484 K	1940	Экранная клавиатура	Корпорация Майкрософт

CPU Usage: 43.75% | Commit Charge: 7.55% | Processes: 28 | Physical Usage: 26.37%

Fig. 6: Taking Process Dump Using Process Explorer.

After taking process dump now load that process dump file into IDA pro. We can able to see several strings in the malware. By using them we can able to find valuable information like how the malware is executing. Below screenshot shows the difference between the packed malware and unpacked malware.



Address	Length	T...	String
seg000:...	00000011	C	encapContentInfo
seg000:...	00000011	C	digestAlgorithms
seg000:...	00000019	C	CMS_RevocationInfoChoice
seg000:...	00000006	C	d.crl
seg000:...	0000001E	C	CMS_OtherRevocationInfoFormat
seg000:...	0000000D	C	otherRevInfo
seg000:...	00000013	C	otherRevInfoFormat
seg000:...	0000000F	C	CMS_SignerInfo
seg000:...	0000000E	C	unsignedAttrs
seg000:...	00000013	C	signatureAlgorithm
seg000:...	0000000C	C	signedAttrs
seg000:...	00000010	C	digestAlgorithm
seg000:...	0000001C	C	CMS_EncapsulatedContentInfo
seg000:...	00000009	C	eContent
seg000:...	0000000D	C	eContentType
seg000:...	00000015	C	CMS_SignerIdentifier
seg000:...	00000017	C	d.subjectKeyIdentifier
seg000:...	00000018	C	d.issuerAndSerialNumber
seg000:...	00000017	C	CMS_CertificateChoices
seg000:...	0000000D	C	d.v2AttrCert

Fig. 7: Packed Malware Unpacked Malware

Strings identified in the locky ransomware using IDA pro:

1) Ntdll, kernal32, user32, gdi32, rsdstx, shell32, crypt32, ws2_32 these are the dynamic link libraries which are the core functionalities and always run when the system turned on. When this ransomware is executed it is accessing all this libraries so it is impacting the core libraries in operating system.
2) The mail library it was accessing is crypt. dll which contains all cryptography algorithms. So one suspect is it is using this dll to perform some encryption tasks.
3) Another string is the location from where the ransomware is executing. This is very important in string analysis that shows the source of the ransomware.
4) This is showing some ip address so there is a possibility for communication using that IP address
5) There are some instructions like pop-up menu, delete menu and create hash. This concludes that this is showing some pop-up and deleting some functionalities.

Dynamic Analysis: (Executing the ransomware)

Using regshot we can compares the changes happened in system before and after executing the malware. It also displays the clear information about where the changes

Using regshot we can compares the changes happened in system before and after executing the malware. It also displays the clear information about where the file is executing

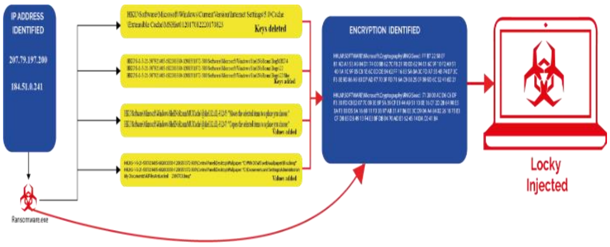
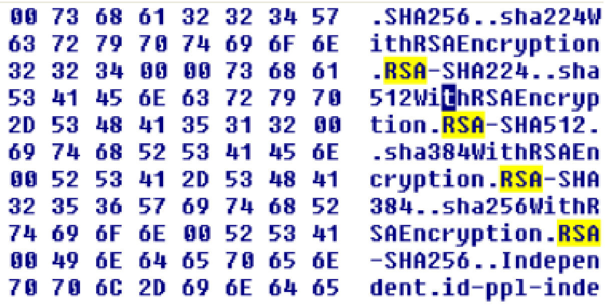


Fig. 8: Showing Which Libraries the Malware Is Accessing.

When we execute the ransomware there are several changes in the system. This execution will add some keys and delete some keys in the registries as shown In the figure. While we analyzing the network using wire shark it was sending some requests to some ip address they are 207.79.197.200, 184.51.0.241. So the attackers are sending instructions using this is. This will also change the wall paper by giving some instructions. This also shows some cryptographic hashes which are used to encrypt the files in the system. This Locky ransomware encrypts using RSA algorithm as referred to string analysis. This generates a hash values using the SHA 256, 512 algorithm.

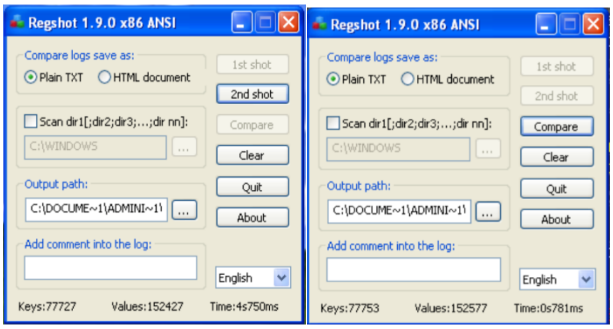


```
00 73 68 61 32 32 34 57  .SHA256..sha224W
63 72 79 70 74 69 6F 6E  ithRSAEncryption
32 32 34 00 00 73 68 61  .RSA-SHA224..sha
53 41 45 6E 63 72 79 70  512WithRSAEncryp
2D 53 48 41 35 31 32 00  tion.RSA-SHA512.
69 74 68 52 53 41 45 6E  .sha384WithRSAEn
00 52 53 41 2D 53 48 41  cryption.RSA-SHA
32 35 36 57 69 74 68 52  384..sha256WithR
74 69 6F 6E 00 52 53 41  SAEncryption.RSA
00 49 6E 64 65 70 65 6E  -SHA256..Indepen
70 70 6C 2D 69 6E 64 65  dent.id-ppl-inde
```

Fig. 9: Encryption Types Observed in IDA Procedure.

Regshot Analysis

Analysis in regshot is quite easy because it shows the changes happened in system before and after executing the malware in the analysis environment. Before infecting the malware to host take 1st shot. Now effect the host environment with malware and take 2nd shot. After capturing the results click on compare this will give the text document showing the changes.

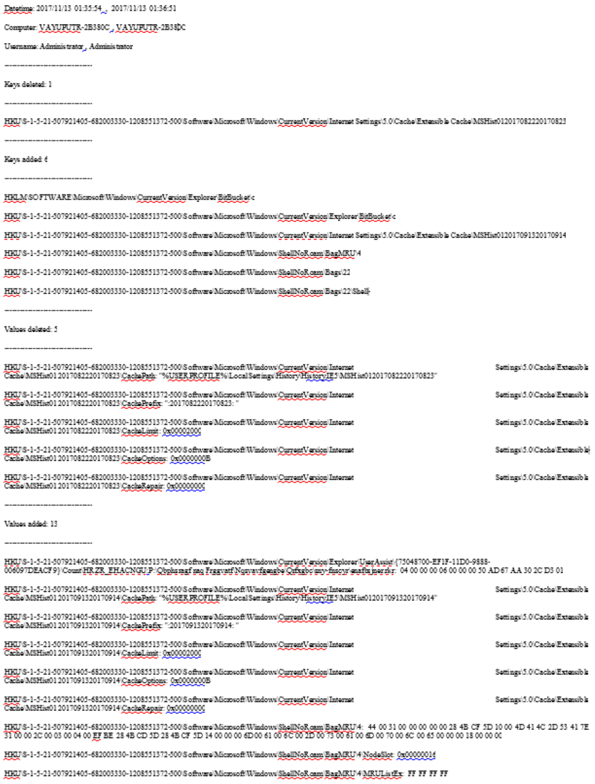


● Plain TXT ○ HTML document
□ Scan dir1[;dir2;dir3;...;dir nn]: C:\WINDOWS
Output path: C:\DOCUME~1\ADMINI~1\
English
Keys:77727 Values:152427 Time:4s750ms

● Plain TXT ○ HTML document
□ Scan dir1[;dir2;dir3;...;dir nn]: C:\WINDOWS
Output path: C:\DOCUME~1\ADMINI~1\
English
Keys:77753 Values:152577 Time:0s781ms

Fig. 10: First Shot Second Shot.

After opening the comparison file we have several changes happen in the system. Totally 31 changes happen in system. These changes are classified as Keys deleted 1, Keys added 6, Values Deleted 5, Values Added 13. In document it is showing clear changes and it will mention paths also. As mentioned in below screenshot.

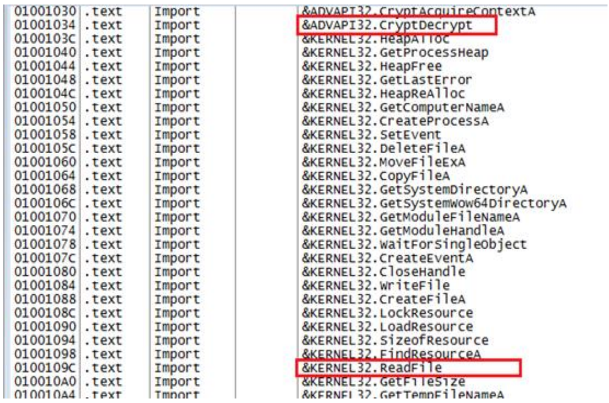


```
Datetime: 2017/11/13 01:35:54 , 2017/11/13 01:36:51

Computer: VAYUPUTR-2B380C , VAYUPUTR-2B380C

Username: Administrator , Administrator

----------------------------------

Keys deleted: 1

----------------------------------

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012017082220170823

----------------------------------

Keys added: 6

----------------------------------

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\c

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\c

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012017091320170914

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\4

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\ShellNoRoam\Bags\22

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\ShellNoRoam\Bags\22\Shell

----------------------------------

Values deleted: 5

----------------------------------

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet                    Settings\5.0\Cache\Extensible
Cache\MSHist012017082220170823\CachePath: "%USERPROFILE%\Local Settings\History\History.IE5\MSHist012017082220170823"

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet                    Settings\5.0\Cache\Extensible
Cache\MSHist012017082220170823\CachePrefix: ":2017082220170823: "

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet                    Settings\5.0\Cache\Extensible
Cache\MSHist012017082220170823\CacheLimit: 0x00002000

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet                    Settings\5.0\Cache\Extensible
Cache\MSHist012017082220170823\CacheOptions: 0x0000000B

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet                    Settings\5.0\Cache\Extensible
Cache\MSHist012017082220170823\CacheRepair: 0x00000000

----------------------------------

Values added: 13

----------------------------------

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\Qrfxgbc\zny-fnzcyr\anafxn jnerzkr: 04 00 00 00 06 00 00 00 50 AD 67 AA 30 2C D3 01

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet                    Settings\5.0\Cache\Extensible
Cache\MSHist012017091320170914\CachePath: "%USERPROFILE%\Local Settings\History\History.IE5\MSHist012017091320170914"

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet                    Settings\5.0\Cache\Extensible
Cache\MSHist012017091320170914\CachePrefix: ":2017091320170914: "

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet                    Settings\5.0\Cache\Extensible
Cache\MSHist012017091320170914\CacheLimit: 0x00002000

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet                    Settings\5.0\Cache\Extensible
Cache\MSHist012017091320170914\CacheOptions: 0x0000000B

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\CurrentVersion\Internet                    Settings\5.0\Cache\Extensible
Cache\MSHist012017091320170914\CacheRepair: 0x00000000

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\4: 44 00 31 00 00 00 00 00 28 4B CF 5D 10 00 4D 41 4C 2D 53 41 7E
31 00 00 2C 00 03 00 04 00 EF BE 28 4B CD 5D 28 4B CF 5D 14 00 00 00 6D 00 61 00 6C 00 2D 00 73 00 61 00 6D 00 70 00 6C 00 65 00 00 00 18 00 00 00

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\4\NodeSlot: 0x00000016

HKU\S-1-5-21-507921405-682003330-1208551372-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\4\MRUListEx: FF FF FF FF
```

Fig. 11: Shows the Changes Happened in the System.

Loading the malware into Ollydgb:

Ollydgb is used to debug the executable file. The ransomware sample we are using is fully protected and it wont load into the ollydgb. So we use the memory dum file and load it into the ollydgb. Ollydgb consists of Dissembler, Registers, Memory Dumps, Stack windows. Olly Dgb analysis by controlling the executing In assembler window it is clearly mentioned that this is importing cryptDecrypt functions for encryption mechanism

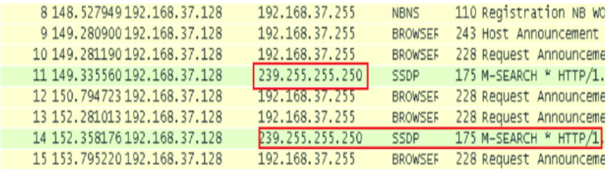


```
01001030 .text  Import      &ADVAPI32.CryptAcquireContextA
01001034 .text  Import      &ADVAPI32.CryptDecrypt
0100103C .text  Import      &KERNEL32.HeapAlloc
01001040 .text  Import      &KERNEL32.GetProcessHeap
01001044 .text  Import      &KERNEL32.HeapFree
01001048 .text  Import      &KERNEL32.GetLastError
0100104C .text  Import      &KERNEL32.HeapReAlloc
01001050 .text  Import      &KERNEL32.GetComputerNameA
01001054 .text  Import      &KERNEL32.CreateProcessA
01001058 .text  Import      &KERNEL32.SetEvent
0100105C .text  Import      &KERNEL32.DeleteFileA
01001060 .text  Import      &KERNEL32.MoveFileExA
01001064 .text  Import      &KERNEL32.CopyFileA
01001068 .text  Import      &KERNEL32.GetSystemDirectoryA
0100106C .text  Import      &KERNEL32.GetSystemWow64DirectoryA
01001070 .text  Import      &KERNEL32.GetModuleFileNameA
01001074 .text  Import      &KERNEL32.GetModuleHandleA
01001078 .text  Import      &KERNEL32.WaitForSingleObject
0100107C .text  Import      &KERNEL32.CreateEventA
01001080 .text  Import      &KERNEL32.CloseHandle
01001084 .text  Import      &KERNEL32.WriteFile
01001088 .text  Import      &KERNEL32.CreateFileA
0100108C .text  Import      &KERNEL32.LockResource
01001090 .text  Import      &KERNEL32.LoadResource
01001094 .text  Import      &KERNEL32.SizeofResource
01001098 .text  Import      &KERNEL32.FindResourceA
0100109C .text  Import      &KERNEL32.ReadFile
010010A0 .text  Import      &KERNEL32.GetFileSize
010010A4 .text  Import      &KERNEL32.GetTempFileNameA
```

Fig. 12: Loding into Ollydgb.

Network Analysis using Wireshark:

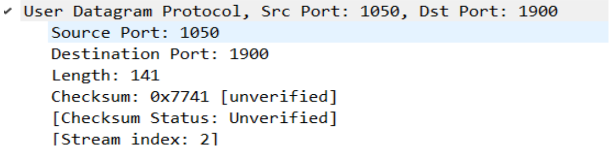
Key point to analyze the network is keep the analysis environment in Host only mode. When any malware is executed in the analysis environment it wont effect the host system. Best practice is to turnoff the firewall in analysis environment then the ransomware will easily connect to the attacker network. After following all the steps. Open the wireshak before executing the malware and select the network adapter to capture the network. Now execute the malware in the system. A bit later every file in the system will be encrypted. And now follow the instructions as shown on the screen while doing that start capturing packets in wireshark. After sometime we will find some ip address in wireshark where the ramsomware is trying to contact the attackers ip address. As shown in the below screen shot.



```
 8 148.527949 192.168.37.128   192.168.37.255    NBNS      110 Registration NB WO
 9 149.280900 192.168.37.128   192.168.37.255    BROWSER   243 Host Announcement
10 149.281190 192.168.37.128   192.168.37.255    BROWSER   228 Request Announceme
11 149.335560 192.168.37.128   239.255.255.250   SSDP      175 M-SEARCH * HTTP/1.
12 150.794723 192.168.37.128   192.168.37.255    BROWSER   228 Request Announceme
13 152.281013 192.168.37.128   192.168.37.255    BROWSER   228 Request Announceme
14 152.358176 192.168.37.128   239.255.255.250   SSDP      175 M-SEARCH * HTTP/1.
15 153.795220 192.168.37.128   192.168.37.255    BROWSER   228 Request Announceme
```

Fig. 13: Wireshark Analysis Detected Vulnerable IP.

After capturing the packets we traced out some malicious ip address. As mentioned in above screenshot 239.255.255.250 is treated as attackers destination IP and after analyzing the packet we find of some port numbers of the host system and destination system they are source port: 1050 and destination port 1900. as mentioned in below screenshot.



```
✓ User Datagram Protocol, Src Port: 1050, Dst Port: 1900
    Source Port: 1050
    Destination Port: 1900
    Length: 141
    Checksum: 0x7741 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
```

Fig. 14: Deep Packet Analysis for Port Numbers.

8. Conclusions

After analyzing the ransomware we find many key elements like what kind of encryption techniques used by malware writer to encrypt, What kind of file types it is encrypting in the system, What kind of network ports it is accessing, How many file directories it is accessing and making changes. We mainly find attackers destination ip address. To safeguard from ransomware we always have a healthy backup of files. And keep the firewalls in the environment and block the ip address find in the analysis. Always keep the softwares up-to-date. Further analysis are carried out on different kinds of malware and these key findings are updated in the antivirus database so they can always block the malware based on their behavior.

Acknowledgment

This work is supported by the Department of Science and Technology, India through the fund sanctioned for improvement of Science & Technology infrastructure, at department of CSE, K.L University, by order number SR/FST/ESI-332/2013.

References

[1] Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious-Book by Andrew Honig and Michael Sikorski.

[2] The Art of Computer Virus Research and Defense Book by Péter Ször.

[3] Practical Malware Analysis by Kris Kendall and Chad McMillan.

[4] Malware Analysis: Tools and Techniques Rakesh Singh Kunwar, Priyanka Sharma.

[5] Malware Analysis of WanaCry Ransomware Abdurrahman Akkas, Christos Nestoras Chachamis, Livio Fetahu.

[6] HTTPS traffic analysis and client identification using passiveSSL/TLS fingerprinting MartinHusák, Milan ˇCermák,TomášJirsík* andPavel ˇCeleda.

[7] K.V.D.KIRAN," MULTI CROSS PROTOCOL WITH HYBRID TOPOGRAPHY CONTROL FOR MANETS", Journal of Theoretical and Applied Information Technology, 2017. Vol.95. No.3, ISSN: 1992-8645.

[8] K.V.D.KIRAN,"Integrated Distributed Architecture to Integrate Wireless Sensor Networks (WSN) with Grid for Healthcare," International Journal of Bio-Science and Bio-Technology", Vol.7, No.3 (2015), pp.243-250, ISSN: 2233-7849 IJBSBT.

[9] K.V.D.KIRAN,"A Critical study of information security risk assessment using fuzzy and entropy methodologies," International Journal on Computers and Communications", Pages: 17-22,Vol1,Isuue1,Dec-,12, ISSN: 2319 – 8869.

[10] K.V.D.KIRAN," "Literature Review on RisK Literature Review on Risk and their Components" International Journal for Research in Emerging Science and Technology (IJREST) ",Volume-1, Issue-6, November 2014", (e-ISSN 2349-7610).

[11] K.V.D.KIRAN,"Performance Analysis of Layered Architecture to Integrate Mobile Devices and Grid computing with a resource scheduling algorithm", IEEE CS'07, SIVAKASI, TAMIL NADU, India.

[12] K.V.D.Kiran "Risk Assessment in Distributed Banking System," International Journal of Applied Engineering Research (IJAER)", ISSN 0973-4562 Volume 9, Number 19 (2014) pp. 6087-6100.

[13] K.V.D.Kiran, "Analysis and Classification Scheme of Risk Assessment Miniatures placed on Different Criteria for Reducing the Risk", International Journal of Applied Engineering Research"pp.12069-12085, ISSN 0973-4562 Volume 9, Number 22 (2014).

[14] K.V.D.Kiran," Information Security risk authority in critical informative systems",CSIBIG 2014.