

# Conti Ransomware Practical Study of Static and Dynamic Methodologies

Sarthak Thakur

Amity Institute of Information Technology, AUR, 303002

**Abstract:- Ransomware viruses have grown to represent a serious concern over the past few years. Ransomware called Conti is one of the variations. Data on the victim's PC was encrypted, transmitting distributing it to other machines on the same network and demanding a ransom, attacks turn into a serious threat and harm the system. Families of ransomware usage sophisticated encryption, dissemination techniques, removing all prospects for data recovery. Analysis of ransomware is essential to determine its characteristics and prevent its spread to design and create appropriate detection and mitigation methods. In this paper, we provide the results of our investigation of the notorious Conti malware. The research that is being presented in particular looks at the behaviour of Conti; it is detonated in a designated created virtual lab environment. We employ several malware analysis technologies to do static and dynamic analysis. The information may be utilised to develop efficient Conti detection and mitigation tools in addition to those for other ransomware families that exhibit similar behaviours.**

## I. INTRODUCTION

Ransomware is widely regarded as the primary method for cybercriminals to monetize their activities and the biggest threat to web users. Ransomware that encrypts files, often known as crypto ransomware, seeks to prevent victims from accessing their systems by requesting to unlock the data and restore the machine to its pre-attack state, you must pay a ransom. Typically, the ransom is settled using a cryptocurrency, which is an untraceable and anonymous payment option. Unfortunately, since 2012, the threat posed by this particular type of malware has escalated due to a lack of specialised security solutions.

An emerging trend in the ransomware industry is ransomware as a service (RaaS). As seen in Fig. A, it represents a business structure which is similar to Software as a Service (SaaS). Anyone can begin a ransomware assault using pre-made ransomware tools thanks to RaaS. Affiliates of RaaS make money by taking a portion of each successful ransom. The RaaS ecosystem is used by ransomware variations including Ryuk, Satan, Netwalker, Egregor, and many [17] others. Conti is among the most hazardous Ransomware as a Service ransomware programmes.

### ➤ History of Conti Ransomware:

In October 2019, the first signs of the distinct Conti ransomware gang surfaced. It wasn't until early 2020 that the gang launched its own website at <http://fylszpcqfel7joif>

.onion. Since then, the CONTI extortion websites <https://continews.click> and <http://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion> have been used to transfer data from 567 different firms. Only victims whose identities are posted on the extortion website or whose data is exchanged and then erased are included in this total. Additionally, Conti serves the victim data that was obtained via another covert TOR service.

- The Conti ransomware attacked ExaGrid, a backup storage business, in May 2021. The Conti group of Conti sought a \$7 million ransom; ExaGrid was able to bargain and ultimately paid \$2.6 million [17]. In May 2021, the Conti ransomware targeted the Health Services Executive (HSE) in Ireland [17] and demanded a \$20 million ransom, which Ireland [17] refused to go for a settlement.
- Conti is most aggressive and lucrative ransomware, with ransom demands as high as \$25 million, according to the FBI. The invasion in Ukraine, the Conti group declared in February 2022 that it would fully back the Russian government.

The Conti group additionally promised to use key infrastructure as a target for retaliation actions in the event that cyberattacks were conducted against Russia. Due to such announcement, an unidentified person who supported Ukraine disclosed almost 60000 communications from internal Jabber chat logs [17]. The leaker releases the stolen files using recently created Twitter account [17] with the handle @ContiLeaks [17]. Along with the sources for further internal projects that Conti group uses to conduct their business. The disclosed files also contain the Conti ransomware's source code.

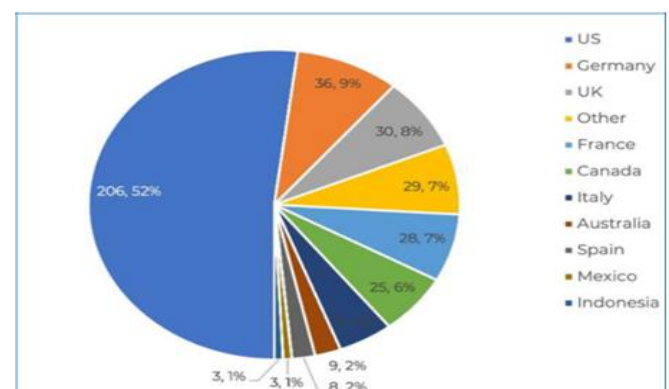


Fig 1 Victims of the Conti Dark Web by Location  
<https://arcticwolf.com/resources/blog-uk/conti-ransomware-an-analysis-of-key-findings>

➤ *The Business Model for Raas:*

The various affiliates of RaaS owners use to compromise victim’s networks and encrypt their files. Among highly experienced hackers with histories in penetration testing, these affiliates are primarily chosen from forums. If a person has a network set up for gaining access to information from other cybercriminals, they may also become affiliates. Before hiring affiliates in both situations, RaaS owners request references from well-known online criminals.

With the RaaS business model, success for cybercriminals depends on their reputation. The majority of affiliates give the proprietors of RaaS a commission of between 10 and 30 percent of each ransom payment they receive. In some circumstances, the operators' fee may also be automatically subtracted from the ransom money. In order to facilitate affiliate assaults, RaaS owners frequently offer virtual machines, exploitation tools, and other technologies. Each affiliate has access to a management panel through which they can keep track of and contact victims. Typically, an affiliate panel has the following resources:

- A generator of ransomware executables
- A different ransomware decryption tool
- A platform enabling victims to pay with cryptocurrencies
- Tools and statistics for victim monitoring
- Using secure chat to negotiate with victims

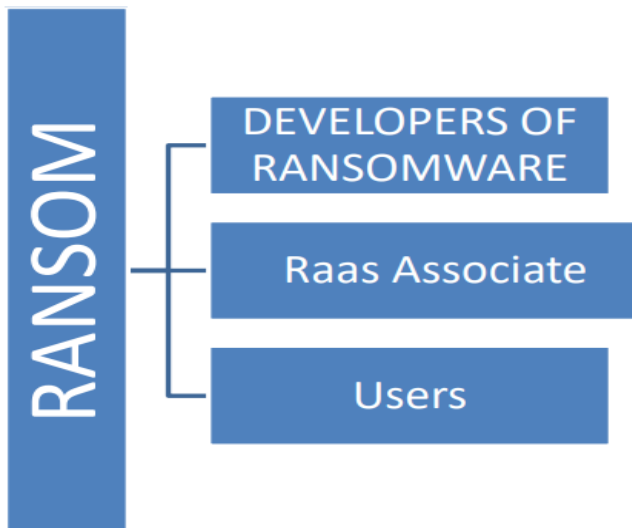


Fig 2 Less complexity model of RaaS Business. To find potential victims, RaaS associate employ ransomware that has already been created by the industry. Associates of the RaaS receive a portion of the ransom on every successful assault.

The infamous Conti ransomware has been thoroughly examined in this work. Results of static and dynamic analyses are presented. The strategies described here can be used against additional ransomware families that share traits with Conti. Conti Ransomware malware is a complex 2021 model. It can transmit malicious and encrypted data concurrently, the sample used in this investigation. Conti

has the ability to encrypt data without establishing a connection to a C2 server, propagate swiftly via networks of computers following execution, and target encrypts data with the "TIYSV" file extension. These traits make Conti assaults a serious hazard that may propagate throughout computer networks.

➤ *Categories of Ransomware:*

A type of malicious program called ransomware encrypts data or locks down the interface in order to prevent users from accessing the machine until the ransom payment is done.

Lockers and cryptors are the two main categories of ransomware that are usually separated.

- **Lockers:** They are less complex kind of ransomware that only locks the user interface of the device, restricting access to applications and data. The user is typically only given a small number of alternatives, such as letting the victim communicate with the attacker and paying a ransom. Lockers often keep underlying system and files intact, allowing for a clean removal. Due of this, cryptors, lockers' more damaging relatives, are more successful at extorting ransom payments.
- **Cryptors:** A more sophisticated kind of ransomware, cryptors encrypts just certain files on the infected machine. Different cryptographic algorithms, including symmetric and public-key based ones, are used by cryptors. Since the encryption keys are kept on a remote command and control (C&C) server, public-key cryptors are particularly challenging to counteract. Cryptors generally provide a deadline for the ransom to be paid, an unique website where users may buy cryptocurrency (like Bitcoins), and detailed instructions on how to do so. The following processes often make up the lifespan of current ransomware: dissemination, infection, communications, file search, file encryption, and ransom demand.

**II. ANALYSIS OF RANSOMWARE**

There are common methods for ransomware analysis. Static analysis and dynamic analysis are included in these methods. Static analysis concentrates on looking at malware files without running it. In [7], the authors explained the statically examine an Avaddon ransomware Portable Executable (PE) file using programmes like PeStudio, x64dbg, and BinaryNinja. The extraction of import functions and strings in the PE file is successful. Before running the ransomware, these strings and functions might display useful information about the malware's capabilities.

The most current ransomware families frequently use obfuscated approaches to delay the analyst or conceal their data from static analysis tools. Additionally, they may contain an anti-debugging technique to cover up their true behaviour while running in a debugger. The ransomware creator may change PE files towards misleading information to deceive the analyst, which is another drawback of static analysis.

Dynamic analysis, often known as behaviour analysis, is the second form of analysis. This kind of ransomware operates in a regulated, segregated setting. The writers of [18] examine more than 20 distinct ransomware's tendencies. The writers build a sandbox environment to run the ransomware inside the safe environment. They observe that certain ransomware employs a variety of evasion strategies, including antidetection and anti-virtual machine technologies. The malware does not start or act differently when it realises it is operating in a virtual environment.

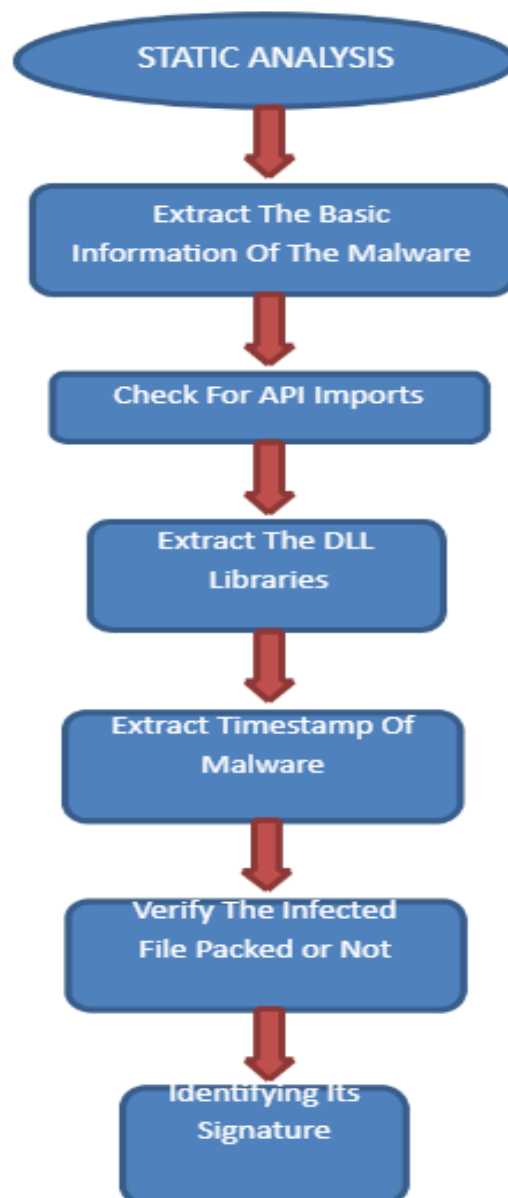
The dynamic link library, API function calls, and assembly levels can all be used to access these behaviour aspects. These attributes are then given to a ransomware validation and detection model made up of machine learning classifiers and Natural Language Processing (NLP) classifiers to assess if the sample is ransomware or benign.

While some ransomware employs dynamic analysis, others use obfuscation to conceal their APIs. Even if they are executed, some may not display their true API calls since they can identify virtual environments.

### III. CONTI STATIC METHODOLOGIES

We give our conclusions from our static study of Conti in this section. Two virtual machines (VMs) were used to the analysis. The host computer features are as follows: 2.4 GHz Intel Core i7 and 8 GB of RAM. The first virtual machine was infected with Conti and was running Windows 10. REMnux, a free Linux toolset for reverse engineering and malware investigation, was operating on the second virtual machine. From MalShare, samples of Conti were taken.

In Flowchart 1, we have shown the work flow of our practical Static Methodologies.



Flowchart 1 Workflow of Static Methodologies

We analysis the malware sample and found some details which is mentioned in the below table 1.

Table 1 Conti Components

Basic Components	
MD5	0c4502d6655264a9aa420274a0ddeaeab
SHA1	b5510bd27327c7278843736aac085e16a508ed99
SHA256	14f9538dd611ca701bdbc6b34a0562e8b18c2492ff323b32557b3667343454
	1a
File Type	Win32 EXE

Dynamic-link libraries (DLLs) are present in the malware components, as seen in figure 3, according to analysis with the Pestudio tool. The dynamic link libraries we have found are: KERNEL32.dll, USER32.dll, WS2 32.dll. The malware calls WS2 32.dll during execution in order to get the host's network configuration information. The libraries kernel32.dll and USER32.dll are frequently called by encryption module. This indicates two libraries process the primary Conti encryption functionality.

library (3)	duplicate (0)	flag (1)	bound (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (67)	description
KERNEL32.dll	-	-	-	0x0002D6A4	0x00028000	implicit	64	Windows NT BASE API Client
USER32.dll	-	-	-	0x0002D7A8	0x00028104	implicit	1	Multi-User Windows USER API Client Library
WS2_32.dll	-	x	-	0x0002D7B0	0x0002810C	implicit	2	Windows Socket Library

Fig 3 Dll Libraries

Since Conti uses internal APIs for various operations, we were able to get useful import information with the aid of this Pestudio tool as well. This information will aid us in determining the functionality and capabilities of Conti. The below figure 4, shows the details.

imports (67)	flag (11)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (10)	type (1)	ordinal (2)	library (3)
InitializeListHead	-	0x0002D924	0x0002D924	867 (0x363)	synchronization	implicit	-	KERNEL32.dll
EnterCriticalSection	-	0x0002D96C	0x0002D96C	305 (0x131)	synchronization	implicit	-	KERNEL32.dll
LeaveCriticalSection	-	0x0002D984	0x0002D984	957 (0x3BD)	synchronization	implicit	-	KERNEL32.dll
DeleteCriticalSection	-	0x0002D99C	0x0002D99C	272 (0x110)	synchronization	implicit	-	KERNEL32.dll
InitializeCriticalSectionAndS...	-	0x0002D9B4	0x0002D9B4	863 (0x35F)	synchronization	implicit	-	KERNEL32.dll
GetLocalTime	-	0x0002D7CA	0x0002D7CA	610 (0x262)	reconnaissance	implicit	-	KERNEL32.dll
IsProcessorFeaturePresent	-	0x0002D89E	0x0002D89E	902 (0x386)	reconnaissance	implicit	-	KERNEL32.dll
IsDebuggerPresent	-	0x0002D88A	0x0002D88A	895 (0x37F)	reconnaissance	implicit	-	KERNEL32.dll
GetStartupInfoW	-	0x0002D89E	0x0002D89E	720 (0x2D0)	reconnaissance	implicit	-	KERNEL32.dll
QueryPerformanceCounter	-	0x0002D8C4	0x0002D8C4	1101 (0x44D)	reconnaissance	implicit	-	KERNEL32.dll
GetCurrentProcessId	x	0x0002D8DE	0x0002D8DE	536 (0x218)	reconnaissance	implicit	-	KERNEL32.dll
111 (WSAGetLastError)	x	0x8000096F	0x8000096F	0 (0x000)	network	implicit	x	WS2_32.dll
9 (htonl)	x	0x80000009	0x80000009	0 (0x000)	network	implicit	x	WS2_32.dll
HeapAlloc	-	0x0002DAA2	0x0002DAA2	837 (0x345)	memory	implicit	-	KERNEL32.dll
HeapFree	-	0x0002DAAE	0x0002DAAE	841 (0x349)	memory	implicit	-	KERNEL32.dll
GetProcessHeap	-	0x0002D8C0	0x0002D8C0	692 (0x2B4)	memory	implicit	-	KERNEL32.dll
GetStringTypeW	-	0x0002D8E2	0x0002D8E2	727 (0x2D7)	memory	implicit	-	KERNEL32.dll
HeapSize	-	0x0002D8F4	0x0002D8F4	846 (0x34E)	memory	implicit	-	KERNEL32.dll
HeapReAlloc	-	0x0002DC00	0x0002DC00	844 (0x34C)	memory	implicit	-	KERNEL32.dll
CreateFileW	-	0x0002DC58	0x0002DC58	203 (0x0CB)	file	implicit	-	KERNEL32.dll

Fig 4 List of API Components



We also extracted the timestamps of the malware figure 5, because it gives the indication about the compile time of the execution of the malware. In this case the malware timestamps is Wednesday February 03 2021 and the time is 13:43:54.

general		
compiler-stamp	0x601AA89A	Wed Feb 03 13:43:54 2021   UTC
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	Intel-386
sections	0x0005	5
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000

Fig 5 Malware Timestamps

Now we will be analysing the File Type Identification. Knowing the file type is crucial since it allows us to determine the destination OS and the appropriate architecture. In the below figure 6, by the help of the Pestudio tool we found out the valuable information i.e. first-bytes-hex the value of the hexadecimal is 4D 5A in the first 2bytes, first-bytes-text i.e. MZ. And also we can see that the file type is executable and the CPU architecture is 32-bit.

property	value
md5	<a href="#">0C4502D6655264A9AA420274A0DDEAEB</a>
sha1	<a href="#">B5510BD27327C7278843736AAC085E16A508ED99</a>
sha256	<a href="#">14F9538DD611CA701BDBC6B34A0562E8B18C2492FF323B32557B36673434541A</a>
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	MZ .....@ .....
file-size	196608 bytes
entropy	6.406
imphash	n/a
signature	Microsoft Visual C++
tooling	Visual Studio 2017
entry-point	<a href="#">E8 DB 04 00 00 E9 7A FE FF FF 55 8B EC F6 45 08 01 56 8B F1 C7 06 D0 81 42 00 74 0A 6A 0C 56 E8 F3</a>
file-version	n/a
description	n/a
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	Wed Feb 03 13:43:54 2021   UTC
debugger-stamp	Wed Feb 03 13:43:54 2021   UTC
resources-stamp	0x00000000
import-stamp	0x00000000
exports-stamp	n/a

Fig 6 Identification of File Type, Architecture and First-byte hexadecimal values

To cross check the value of file type identification we are using another static tool name Exeinfo PE tool. The below figure 7, shows the analysis part of the Exeinfo PE tool.

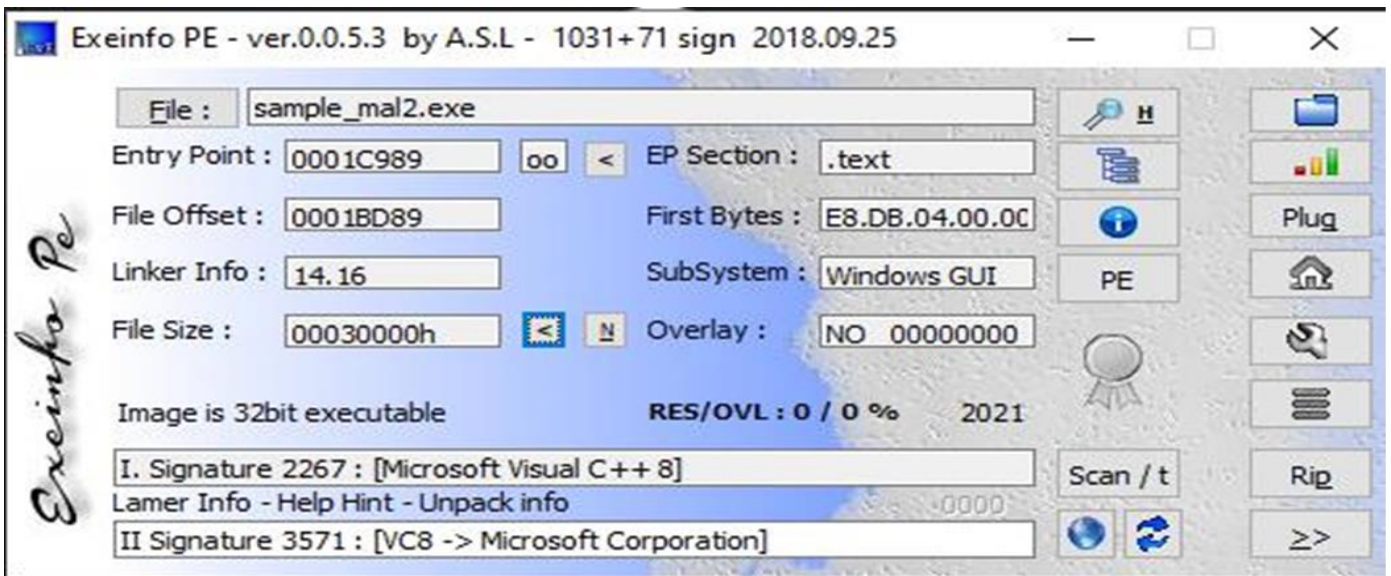


Fig 7 Analysis by Exeinfo PE Tool

The PE is a Windows executable file (Portable Executable). PE can take the shape of an .exe, .dll, etc. We must examine the file signature in order to recognize the file type and prevent false positives caused by duplicate extensions. And in here we also got to know about that the malware file we are analysing it is unpacked.

The file header contains the file signature. The first two bytes of PE files, file signatures include the hexadecimal numbers 4D 5A or MZ (0-1). The message "This application cannot be run in DOS mode" is also seen in PE programmes. Hex 50 45 marks the start of the PE header. Keeping all these values in mind we can say that it's represent a Portable Executable file. The below figure 8, shows the values.

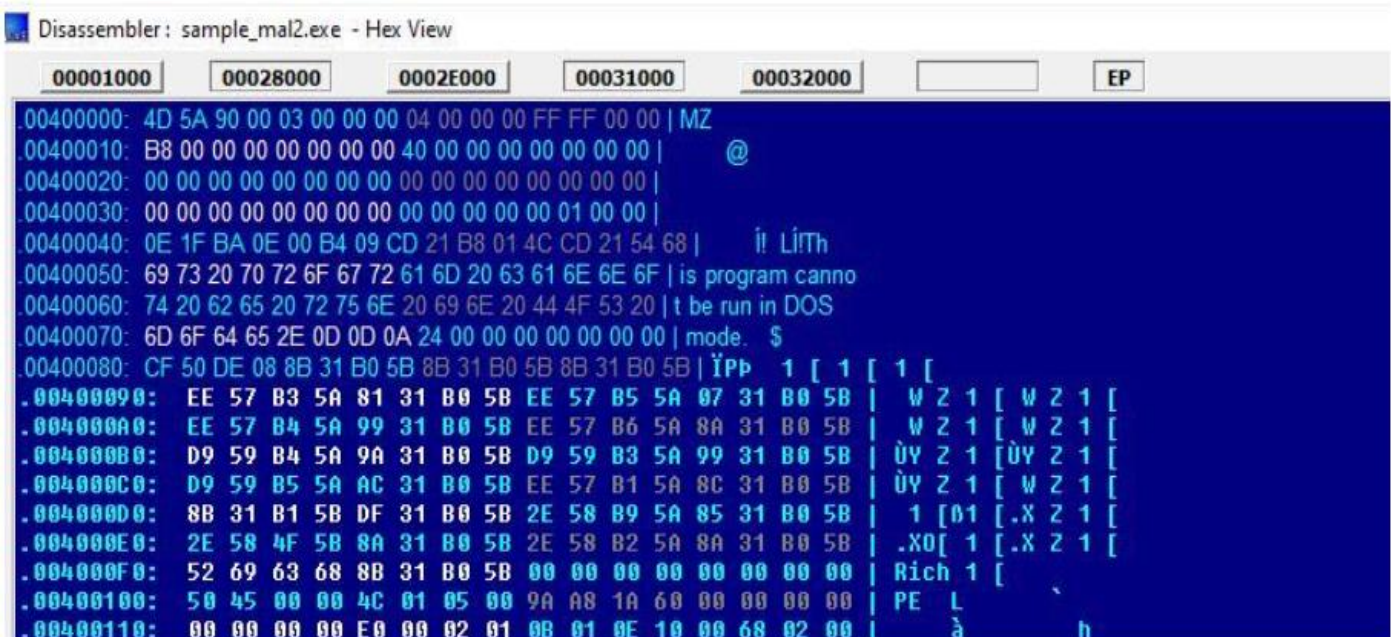


Fig 8 File Signature

Table 2 PE Header

Number of sections	5 { .text, .rdata, .data, .rsrc, .reloc }
Signature	PE
Size of Optional Header	0x00E0
Machine	IMAGE_FILE_MACHINE_I386
Time date stamp	03-Feb-2021 13:43:54
Pointer to Symbol Table	0x00000000
Number of symbols	0

In figure H, it showing the number of the sections that malware file contained total 5 sections i.e.

“.text”, “.rdata”, “.data”, “.rsrc”, “.reloc”. And the different section contains different characteristics functions. The “x” sign denoted in the figure H, replicate that the section contains that particular characteristics function has the permissions. The “.text” section has an executable characteristic, “.rdata” has the permissions to initialized-data, “.rdata” has two permissions writable and initialized-data, “.rsrc” has the permission of initialized-data and lastly “.reloc” section has the permissions of both initialized-data and uninitialized-data. And also we have got some information of the various properties of sections like raw-address, raw-size, virtual-address and virtual-size. Based on these sections we can ensure that it is portable executable.

Table 3 Section Function

Name of the Sections	Functions
.rsrc	Stores Resources {strings, icons}
.reloc	Modify another section in the file
.text	Executable code
.rdata	Stores Data {Read Only}
.data	Stores Data {R/W}

property	value	value	value	value	value
<b>general</b>					
name	.text	.rdata	.data	.rsrc	.reloc
md5	C21F715BE9C42B50B7026CC...	68FF18271CADF47CD3DAA5...	6EE10635D34D01323B218C6...	AD7B78E84F1D02FC8833153...	ABA182FC0DD4B2754AD93...
entropy	6.501	4.822	2.958	4.718	6.372
file-ratio (99.48%)	80.21 %	12.24 %	4.43 %	0.26 %	2.34 %
raw-address	0x00000400	0x00026C00	0x0002CA00	0x0002EC00	0x0002EE00
raw-size (195584 bytes)	0x00026800 (157696 bytes)	0x00005E00 (24064 bytes)	0x00002200 (8704 bytes)	0x00000200 (512 bytes)	0x00001200 (4608 bytes)
virtual-address	0x00001000	0x00028000	0x0002E000	0x00031000	0x00032000
virtual-size (197475 bytes)	0x0002675D (157533 bytes)	0x00005C86 (23686 bytes)	0x00002C70 (11376 bytes)	0x000001E0 (480 bytes)	0x00001130 (4400 bytes)
<b>characteristics</b>					
value	0x60000020	0x40000040	0xC0000040	0x40000040	0x42000040
writable	-	-	x	-	-
executable	x	-	-	-	-
shareable	-	-	-	-	-
discardable	-	-	-	-	x
initialized-data	-	x	x	x	x
uninitialized-data	-	-	-	-	-
self-modifying	-	-	-	-	-
virtualized	-	-	-	-	-

Fig 9 Sections Details of Conti

The test file findings are shown in Figure 10, which demonstrates that malware sample we are analysing, includes Trojan virus. Based on it, the subsequent procedure analyses the actual assaults that took place.

The screenshot shows the VirusTotal analysis page for a file named 'ssms.bin'. At the top, a red circle indicates that 58 security vendors and 3 sandboxes have flagged the file as malicious. Below this, the file's MD5 hash, size (192.00 KB), and upload date (2022-05-28 03:50:28 UTC) are displayed. A list of security vendors and their detection results is shown below:

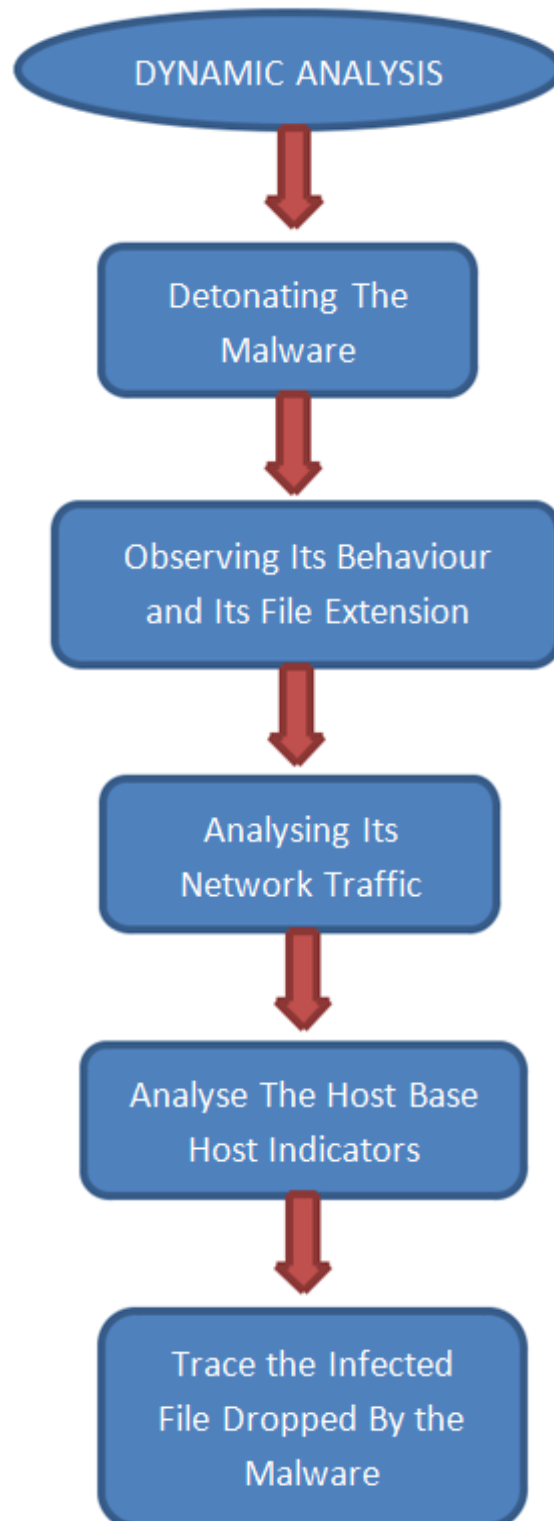
Security Vendor	Detection Result
Ad-Aware	Trojan.GenericKDZ.84287
Alibaba	Trojan.Win32/Phonzy.382f46ac
Arcabit	Trojan.Generic.D1493F
AVG	Win32.Conti-B [Ransom]
BitDefender	Trojan.GenericKDZ.84287
Bkav Pro	W32.AIDetect.malware2
Cybereason	Malicious.665526
Cynet	Malicious (score: 100)
AhnLab-V3	Ransomware/Win.Conti.R372647
ALYac	Trojan.Ransom.Conti
Avast	Win32.Conti-B [Ransom]
Avira (no cloud)	HEUR/AGEN.1213295
BitDefenderTheta	Gen.NN.ZexaF.34682.muW@a9yqXmpi
CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe
Cyren	W32/Trojan.ZPRI-6701

Fig 10 Virus Total Result

#### IV. CONTI DYNAMIC METHODOLOGIES

Dynamic analysis refers to the technique of evaluating and testing a programme utilising real-time data execution. The objective is to find bugs in software when it is being used, as opposed to continually analysing the code offline. So in this section we have created a sandbox environment, where we will detonate the malware sample and observed the behaviour of the malware. So for our sandbox we are using Windows 10 OS which will be infected by the malware and REMnux, a free Linux toolset for reverse engineering and malware investigation was operating on the second virtual machine.

In Flowchart 2, we have shown the work flow of our practical Dynamic Methodologies.



Flowchart 2 Workflow of Dynamic Methodologies



In figure 11, it's showing images of two random .jpg files that we have used for the test purpose before the Conti ransomware affects the system. On the other hand in figure 12 it's showing the after effect of the malware where the same images file has been encrypted with "TIYSV" extension and we cannot able to view the images. And in the figure 13, it's showing the ransom note where it has mentioned all the details and address of the URL of onion site to pay the ransom.



Fig 11 Before detonating the malware

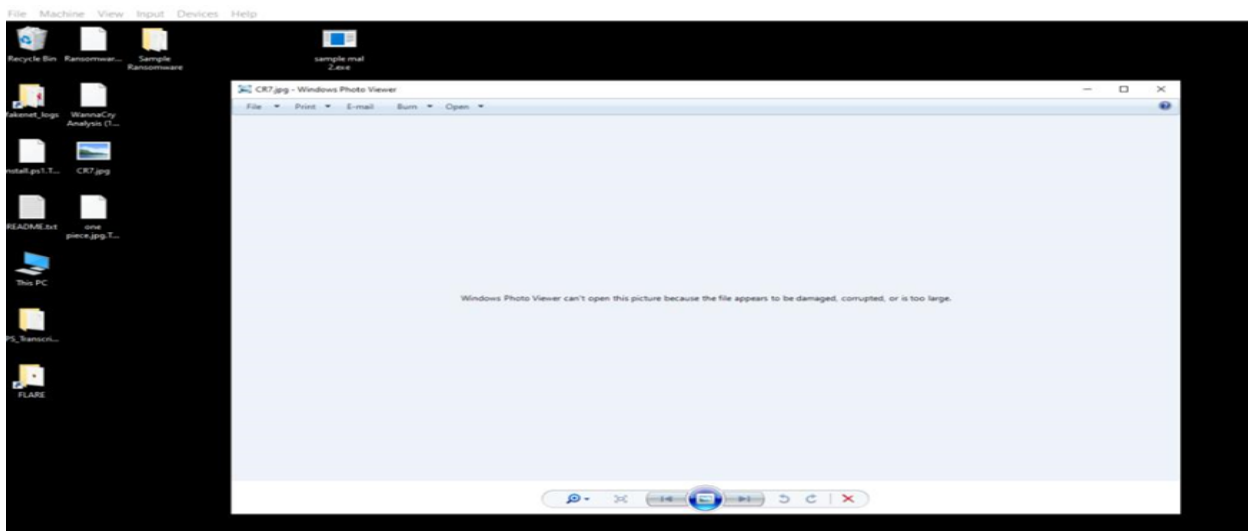


Fig 12 After Detonating The Malware

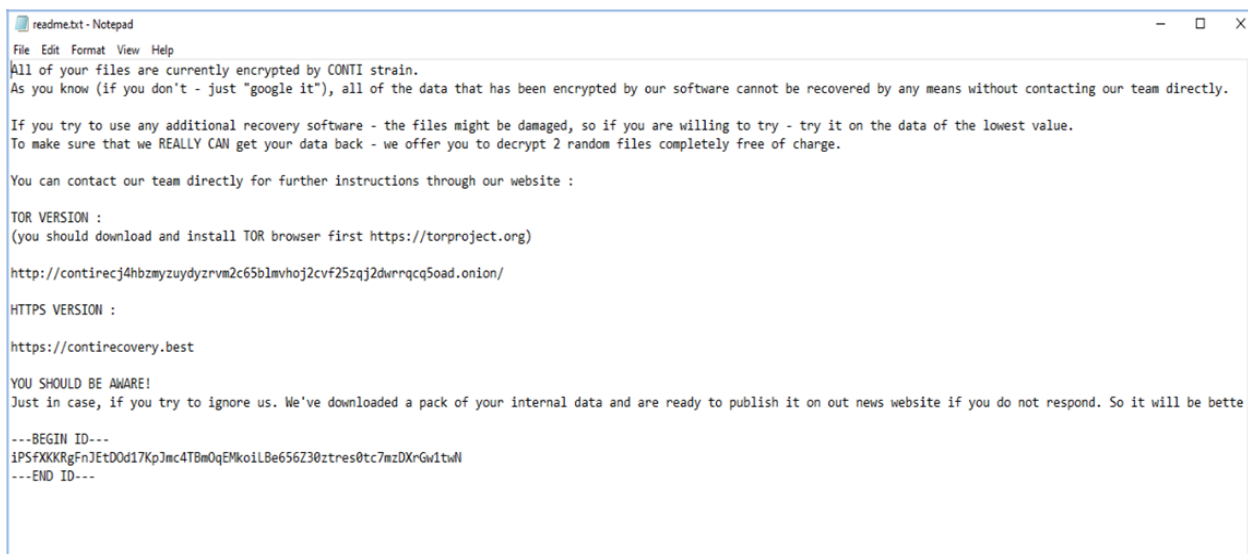


Fig 13 Ransom Notes of Conti

In the ransom note figure 13, we have found that the first ransom letter instructs victims to visit the websites contirecovery.best and contirecj4hbzmyzudyzrvmc65blmvhoj2cvf25zqj2dwrrqcq5oad.onion, which provide information on how to get decryption keys from Conti affiliate attackers. The TOR browser installation instructions are also included in the ransom message so that you may access the Conti group's covert web service.

At the conclusion of this ransom message, there is a distinct victim ID value (readme.txt). It is the string that is bounded by the delimiters —BEGIN ID— and —END ID—

On the website for Conti's ransom note recovery service, victims are urged to upload their ransom letter. The website directs the victim to a chat window where they may

negotiate with the affiliates once they post a legitimate ransom letter. For businesses, this style of ransom letter format poses a danger of data leaking. The malware itself contains hard coded victim IDs.

This implies that the conversation becomes publicly available once harmful files are posted to any malware service or the IDs are compromised.

Now to analyse the network artefacts we have used process monitoring tool to understand the behaviour of the Conti malware while detonating it. In the figure 14, it showing that once the malware detonated it's tried to send the Syn packet to port 445 and the protocol its using is TCP and its process ID (PID) is 3036.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	988	TCP	Listen	0.0.0.0	135	0.0.0.0	0	11/29/2022 7:27:38 AM	RpcSs
System	4	TCP	Listen	10.0.0.5	139	0.0.0.0	0	11/29/2022 7:27:38 AM	System
System	4	TCP	Listen	169.254.0.189	139	0.0.0.0	0	11/29/2022 7:27:43 AM	System
svchost.exe	2932	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	11/29/2022 7:27:44 AM	CDPSvc
lsass.exe	732	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	11/29/2022 7:27:38 AM	lsass.exe
winit.exe	580	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	11/29/2022 7:27:38 AM	winit.exe
svchost.exe	1344	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	11/29/2022 7:27:38 AM	EventLog
svchost.exe	1192	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	11/29/2022 7:27:38 AM	Schedule
spoolsv.exe	2488	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	11/29/2022 7:27:39 AM	Spooler
services.exe	724	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	11/29/2022 7:27:39 AM	services.exe
svchost.exe	2780	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	11/29/2022 7:27:40 AM	PolicyAgent
sample_mal2.exe	3036	TCP	Syn Sent	169.254.0.189	49926	169.254.255.0	445	11/29/2022 1:55:21 PM	sample_mal2.exe
sample_mal2.exe	3036	TCP	Syn Sent	169.254.0.189	49927	169.254.255.1	445	11/29/2022 1:55:21 PM	sample_mal2.exe
sample_mal2.exe	3036	TCP	Syn Sent	169.254.0.189	49928	169.254.255.2	445	11/29/2022 1:55:21 PM	sample_mal2.exe
sample_mal2.exe	3036	TCP	Syn Sent	169.254.0.189	49929	169.254.255.3	445	11/29/2022 1:55:21 PM	sample_mal2.exe
sample_mal2.exe	3036	TCP	Syn Sent	169.254.0.189	49930	169.254.255.4	445	11/29/2022 1:55:21 PM	sample_mal2.exe
sample_mal2.exe	3036	TCP	Syn Sent	169.254.0.189	49931	169.254.255.5	445	11/29/2022 1:55:21 PM	sample_mal2.exe
sample_mal2.exe	3036	TCP	Syn Sent	169.254.0.189	49932	169.254.255.6	445	11/29/2022 1:55:21 PM	sample_mal2.exe
sample_mal2.exe	3036	TCP	Syn Sent	169.254.0.189	49933	169.254.255.7	445	11/29/2022 1:55:21 PM	sample_mal2.exe
sample_mal2.exe	3036	TCP	Syn Sent	169.254.0.189	49934	169.254.255.8	445	11/29/2022 1:55:21 PM	sample_mal2.exe
sample_mal2.exe	3036	TCP	Syn Sent	169.254.0.189	49935	169.254.255.9	445	11/29/2022 1:55:21 PM	sample_mal2.exe

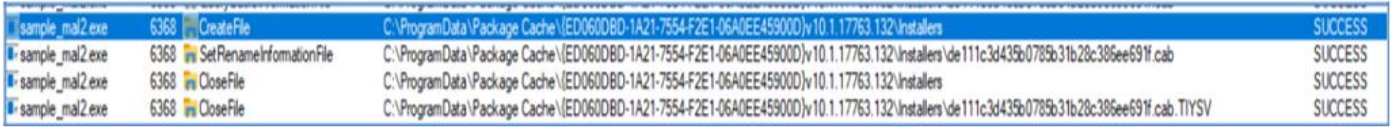
Fig 14 Network Traffic Capture

After observing it for some times when the Handshake get failed then the sample\_mal2.exe file infect the system with .TIYSV extension. The actual fact is that once the malware gets the successful Handshake it will create a backdoor for hacker. Due to the Handshake Failure the malware automatically encrypts the targeted file guiding with a ransom txt file to pay it for the decryption key.

Process Name	PID	Operation	Path	Result
sample_mal2.exe	6820	CreateFile	C:\Windows\Prefetch\SAMPLE_MAL2_EXE-4F533B35.pf	SUCCESS
sample_mal2.exe	6820	QueryStandardInformationFile	C:\Windows\Prefetch\SAMPLE_MAL2_EXE-4F533B35.pf	SUCCESS
sample_mal2.exe	6820	ReadFile	C:\Windows\Prefetch\SAMPLE_MAL2_EXE-4F533B35.pf	SUCCESS
sample_mal2.exe	6820	CloseFile	C:\Windows\Prefetch\SAMPLE_MAL2_EXE-4F533B35.pf	SUCCESS
sample_mal2.exe	6820	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND
sample_mal2.exe	6820	QueryNameInformationFile	C:\Windows\System32\wow64log.dll	SUCCESS
sample_mal2.exe	6820	CloseFile	C:\Windows\System32\wow64log.dll	SUCCESS
sample_mal2.exe	6820	CreateFile	C:\Users\mak\Desktop	SUCCESS
sample_mal2.exe	6820	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS
sample_mal2.exe	6820	QueryBasicInformationFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS
sample_mal2.exe	6820	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS
sample_mal2.exe	6820	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS
sample_mal2.exe	6820	CreateFileMapping	C:\Windows\SysWOW64\apphelp.dll	FILE LOCKED WITH ONLY READERS
sample_mal2.exe	6820	CreateFileMapping	C:\Windows\SysWOW64\apphelp.dll	SUCCESS
sample_mal2.exe	6820	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS
sample_mal2.exe	6820	CreateFile	C:\Users\mak\Desktop\sample_mal2.exe	SUCCESS
sample_mal2.exe	6820	QuerySecurityFile	C:\Users\mak\Desktop\sample_mal2.exe	BUFFER OVERFLOW
sample_mal2.exe	6820	QuerySecurityFile	C:\Users\mak\Desktop\sample_mal2.exe	SUCCESS
sample_mal2.exe	6820	CloseFile	C:\Users\mak\Desktop\sample_mal2.exe	SUCCESS
sample_mal2.exe	6820	CreateFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS
sample_mal2.exe	6820	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	BUFFER OVERFLOW
sample_mal2.exe	6820	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS
sample_mal2.exe	6820	CloseFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS
sample_mal2.exe	6820	CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS
sample_mal2.exe	6820	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	BUFFER OVERFLOW
sample_mal2.exe	6820	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS

Fig 15 Host Based Indicators Processes

In this section we are analysing the host based indicators. We have used the Procmon tool to uncover all the processes the malware is operating. From figure N, shows that the process id (PID) 6820 running the sample\_ma2.exe which is our malware file that we have detonated. After detonating it first Create File and then QueryStandardInformationFile is generated then it go for the ReadFile and after that its close the file once the process is completed. This way the Conti malware is affecting the whole system files. In our static analysis we have noted the dynamic link libraries KERNEL32.dll, USER32.dll, WS2 32.dll. The malware calls WS2 32.dll during execution in order to get the host's network configuration information and the other two is using for the encryption method. On further analysis in figure 16, we got the .TIYSV extension has been added and once it's done its close the process. That means its encrypt with .TIYSV extension.



Process Name	PID	Operation	Path	Result
sample_ma2.exe	6368	CreateFile	C:\ProgramData\Package Cache\{ED0600BD-1A21-7554-F2E1-06A0EE45900D}\v10.1.17763.132\Installers	SUCCESS
sample_ma2.exe	6368	SetRenameInformationFile	C:\ProgramData\Package Cache\{ED0600BD-1A21-7554-F2E1-06A0EE45900D}\v10.1.17763.132\Installers\de111c3d435b0785b31b28c306ee691f.cab	SUCCESS
sample_ma2.exe	6368	CloseFile	C:\ProgramData\Package Cache\{ED0600BD-1A21-7554-F2E1-06A0EE45900D}\v10.1.17763.132\Installers	SUCCESS
sample_ma2.exe	6368	CloseFile	C:\ProgramData\Package Cache\{ED0600BD-1A21-7554-F2E1-06A0EE45900D}\v10.1.17763.132\Installers\de111c3d435b0785b31b28c306ee691f.cab.TIYSV	SUCCESS

Fig 16 TIYSV extension

Based on this analysis we have spotted a suspicious file name directory-hash has been installed it's the encryption program file once it installed it encrypts the entire file and tries to steal some valuable data. In the figure 16, it shows that the suspicious "directory-hash" file has installed after the malware detonation take place.

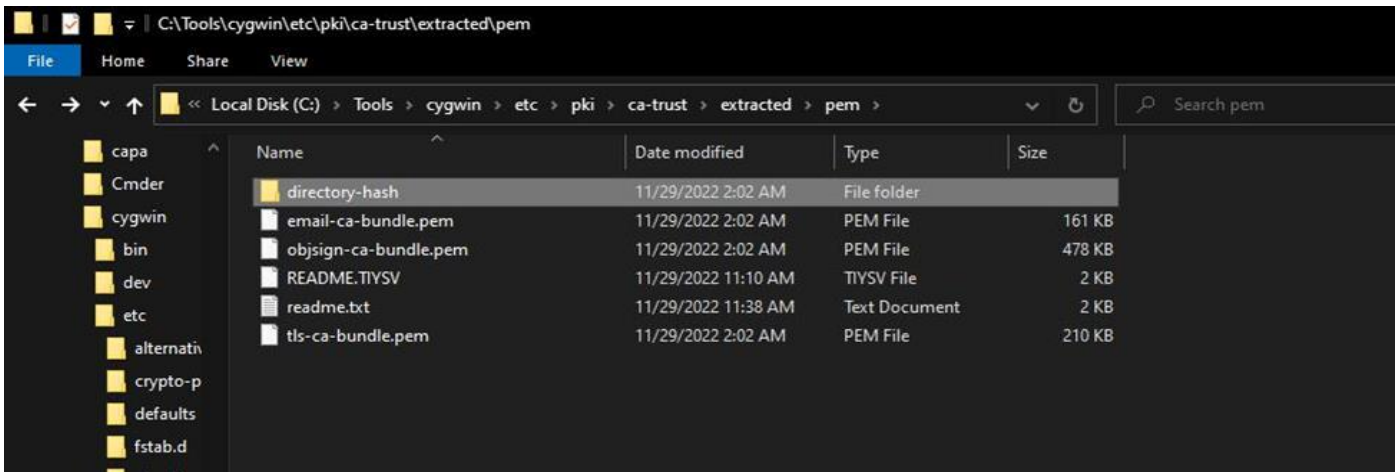


Fig 16 Malicious File Name Directory-hash been installed

In figure 17, showing the data what the directory-hash file contains. Unknown forms of data. It's the malicious data of the malware.

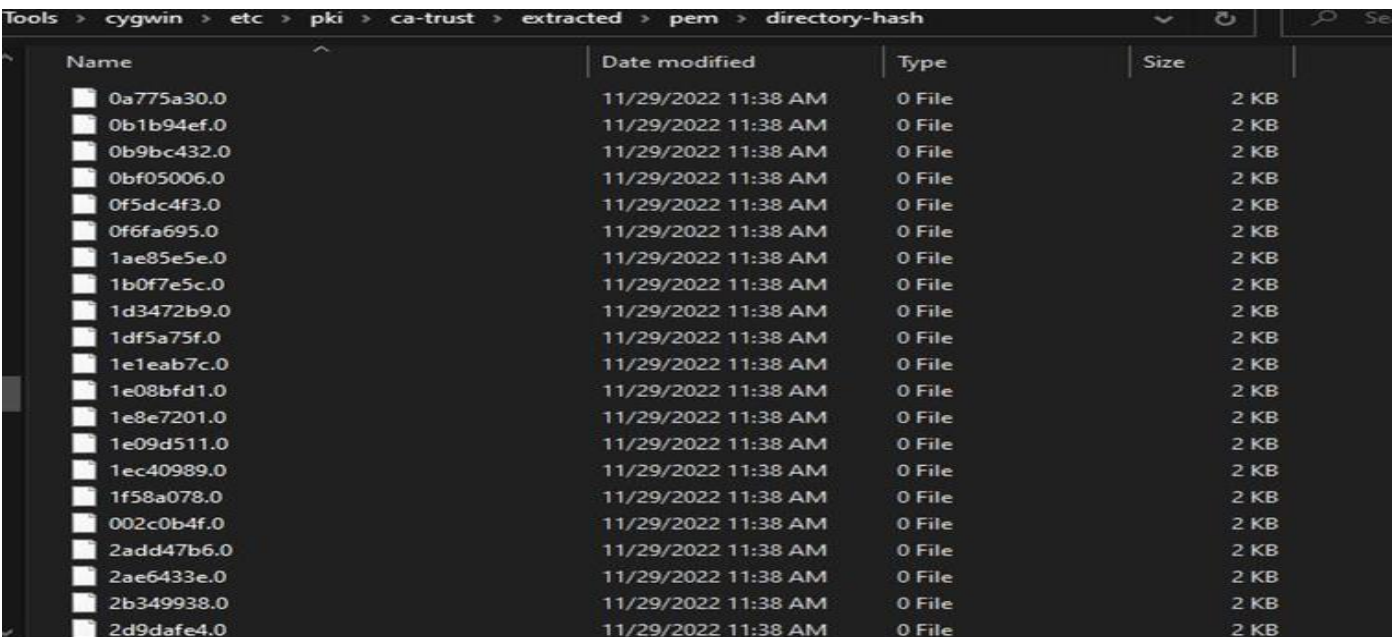


Fig 17 Data Containing in the Directory-Hash Folder



**V. ENCRYPTION TECHNIQUES OF COTNI**

Depending on the size and kind of the data, the Conti ransomware uses one of three possible encryption methods. The smallest file is 4 bytes, the largest is 8950410 bytes, and the middle file is 1790082 bytes (1.70 MB) (8.53 MB). Full Encryption, the initial encryption method, is intended for data under 1.4 MB [7]. Conti produces a random encryption key throughout the Full Encryption process. It uses this key to encrypt the entire file's content using a hard-coded RSA public key. The encrypted data is then written back into the file along with the encryption key, the encryption method value (24 for complete encryption), and the original file size.

The second encryption method, Header Encryption, is designed to protect data between 1.04 MB and 5.24 MB size [17]. Conti merely encrypts the highest 1 MB of the file throughout this encryption mode while writing the encrypted data back to the file. The remaining information that is not even encrypted, the encryption key, the encrypted method value (26 for Header Encryption) [17], and the file's starting size are all added on after this.

The Conti ransomware divides the file content into ten pieces for non-Virtual Machine disc files or seven chunks for Virtual Machine disc files in the most recent encryption, which speeds up the encryption process. For virtual machine disc files, each chunk size is equal to (file size / 100 \* 10) or (file size / 100 \* 7) [17]. Then, until the conclusion of the file, it begins encrypting the very first chunk, skipping to the next one, and so forth, encrypting five or three chunks total.

For every file, Conti produces an encrypted key. Each file receives an embedded RSA public key, which is used to encrypt this encryption key. It has to know the following information to decrypt the files: The encrypted key; the encrypted mode; the original file size; the RSA private key has the permission to access by the Conti group only and it is modified for every individual versions and attacks.

➤ *Report*

Based on our static and dynamic malware research, this section presents a general summary of data describing about the signature of a Conti ransomware assault in the network. The ultimate outcome of the static analysis that uncovers the indication compromise data (IOCs) displayed in Table 3 is as follows.

Table 3 IOC DATA

FILE	RESULT
sha1	0c4502d6655264a9aa420274a0ddeab
md5	b5510bd27327c7278843736aac085e16a508ed99
sha256	14f9538dd611ca701bdbcb6b34a0562e8b18c2492ff323b32557b36673434541a
File Extension	TIYSV
Size	196.6 Bytes
Signature	Microsoft Visual C++ 8
Library	ws2_32.dll, kernel32.dll, user32.dll

Table 3, displays the cost of employing IOCs data to identify and secure computers from Conti ransomware virus assaults. The hash values md5, sha1, and sha256 are used in the signature file to represent IOCs data. As shown in Table 4, we have showcase the behavioural activities of the Conti based on our analysis.

Table 4 Behavioural Activities of Conti

MALICIOUS	SUSPICIOUS	INFORMATIONS
Create files	Reads the computer name	Manual execution by user
Dropped file can have ransomware instructions	checks the languages it supports	Checks Windows Trust Settings
Actions that appear to be data theft	Create documents in the programme directory.	TOR URLs might be found in dropped items.
stealing login information from web browsers	Reads the cookies of the browsers	Checks supported languages
files in the Chrome extension folder are modified	PowerShell script executed	Dropped object may contain Bitcoin addresses
	Creates files in the user directory	



## VI. RESULTS OF DYNAMIC ANALYSIS

### A. Defense and Resistance:

- *Authenticate using many Factors*  
Impose multifactor authentication requirements for remote network access from outside sources.
- *Implement Traffic Filtering And Network Segmentation*
  - To stop the spread of ransomware, implement and make sure there is strong network segmentation across networks and functions. Establish a demilitarised zone to stop unchecked network connectivity.
  - Filter network traffic to block communications coming from or going out of known malicious IP addresses.
  - Enable strong spam filters to prevent phishing emails from reaching end users. To prevent consumers from accessing harmful websites or opening malicious attachments, implement a user education campaign. To stop emails with executable files from getting to end users, filter them.
  - To stop users from visiting harmful websites, implement a URL block list and/or allow list.
- *Check for Security Holes and keep your Software up to Date*
  - Set up antivirus and antimalware programmes to periodically check network assets for the newest signatures.
  - On network assets, promptly update apps, operating systems, software, and hardware. Think about implementing a central patch management system.
  - Apply controls and remove any unused programmes.
  - Remove any programme that isn't thought to be essential for regular business. To facilitate in the malicious exploitation of a company's enterprise, Threat actors from the Conti employ lawful tools like remote desktop software and programmes for surveillance and administration.
  - Any unapproved software should be looked at, especially any remote desktop or remote monitoring and management programmes.
- *Employ Endpoint Response and Detecting Tools*
  - Tools for endpoint detection and response provide high level of visibility towards the endpoint security which may successfully thwart hostile cyber actors.
- *Limit Network Resource Access, Particularly by Limiting RDP*
  - If RDP is determined to be operationally required after risk assessment, limit the sources and demand multifactor authentication.

Knowing the strategies that the Conti ransomware use to propagate allows us to defend our system from assaults of this nature. Phishing assaults are a common way for the

Conti ransomware to propagate before beginning an attack. These phishing attempts target people by delivering emails that contain links to fraudulent websites and BazarLoader download pages for Microsoft Office or Google Docs. The Conti gang can use this malware's backdoor access to spread the ransomware and further investigate the affected computers. Additionally, the phishing emails could include zip files containing malicious JavaScript scripts to run BazarLoader.

The Conti ransomware takes use of new security flaws where the users failed to patch, even though the bulk of these flaws are patchable, to elevate its privileges and move laterally via the victim's network. Some of the well-known flaws that the Conti group exploited in past assaults are included in the list below:

#### ➤ *PrintNightmare:*

With the help of the Windows Print Spooler service, the attacker [17] may access files with SYSTEM rights thanks to the remote code execution flaw known as PrintNightmare. The attacker has complete user access, so they may install applications, remove files, and even create new accounts.

#### ➤ *Zerologon*

This flaw affects Netlogon, a Windows Server function used to verify user identities within a domain. An attacker can launch an application on a network device using the Netlogon Remote Protocol to [17] establish a Netlogon secure channel connection to a domain controller [17].

#### ➤ *FortiGate*

The FortiGate SSL VPN from Fortinet has a route traversal vulnerability. This flaw enables an unauthenticated attacker to remotely access device files by sending a carefully constructed request to a Fortigate SSL VPN endpoint that includes a route traversal sequence.

Downloadable fixes are available for all of the above-mentioned vulnerabilities. It's crucial to patch systems with the most recent security patches to stave off ransomware assaults. The Conti ransomware may encrypt data using the SMB connection, according to the source code and dynamic analysis of the malware. Consequently, limiting network-wide access to resources can lessen harm; it's also strongly advised to disable SMBv1 use and mandate at least SMBv2. Last but not least, avoiding a complete business shutdown in the event of an attack requires having a reliable backup solution.

## VII. CONCLUSION

In the study investigation the Ransomware Conti assault on the sandbox machine, we were able to obtain a pictorial image of the behavioural signature based on the analysis utilising the practical methods of static and dynamic malware analysis methodologies with the aid of various tools. This study demonstrates a practical

investigation of the virus and its behavioural activities. Systems for network activity detection in network traffic records should be used with extreme caution. The study of how virus encrypts files once it affects the system is another important topic. Finally, it discussed the malware's mitigating measures. Future research might focus on the creation of online data backup systems as well as detection systems based on network traffic logs or certain internet protocols.

#### REFERENCES:

- [1]. G. O. Ganfure, C. F. Wu, Y. H. Chang, and W. K. Shih, "DeepGuard: Deep Generative User-behavior Analytics for Ransomware Detection," *Proc. - 2020 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2020*, 2020, DOI: 10.1109/ISI49825.2020.9280508.
- [2]. S. Sibi Chakkaravarthy, D. Sangeetha, M. V. Cruz, V. Vaidehi, and B. Raman, "Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks," *IEEE Access*, vol. 8, pp. 169944–169956, 2020, DOI: 10.1109/access.2020.3023764.
- [3]. S. Il Bae, G. Bin Lee, and E. G. Im, "Ransomware detection using machine learning algorithms," *Concurr. Comput.*, no. December 2018, pp. 1–11, 2019, DOI: 10.1002/cpe.5422.
- [4]. Filip Truta, "City of Cartersville Admits Paying Ryuk Ransomware Operators \$380,000 - Security Boulevard," [www.securityboulevard.com](http://www.securityboulevard.com), 2020. <https://securityboulevard.com/2020/03/city-of-cartersvilleadmits-paying-ryuk-ransomware-operators-380000/> (accessed January 20, 2021).
- [5]. Filip Truta, "University of California San Francisco Pays \$1 Million to Ransomware Operators after June 1 Attack - Security Boulevard," [www.securityboulevard.com](http://www.securityboulevard.com), 2020. <https://securityboulevard.com/2020/06/university-of-californiasan-francisco-pays-1-million-to-ransomware-operators-after-june1-attack/> (accessed January 20, 2021).
- [6]. T. M. Liu, D. Y. Kao, and Y. Y. Chen, "Loocipher ransomware detection using lightweight packet characteristics," *Procedia Comput. Sci.*, vol. 176, pp. 1677–1683, 2020, DOI: 10.1016/j.procs.2020.09.192.
- [7]. Akbanov, M., Vassilakis, V. G., Moscholios, I. D., & Logothetis, M. D. (2018, July). Static and dynamic analysis of WannaCry ransomware. In *Proc. IEICE Inform. and Commun. Technol. Forum ICTF 2018*.
- [8]. A. H. Mohammad, "Ransomware Evolution, Growth and Recommendation for Detection," *Mod. Appl. Sci.*, vol. 14, no. 3, p. 68, 2020, DOI: 10.5539/mas.v14n3p68.
- [9]. Umar, R., Riadi, I., & Kusuma, R. S. (2021). Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method. *IJID (International Journal on Informatics for Development)*, 10(1), 53-61.
- [10]. Ferdiansyah, "Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware," *JUSIFO (Jurnal Sist. Informasi)*, vol. 2, no. 1, pp. 44–59, 2018, [Online]. Available: <http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis-Aktivitas-dan-Pola-Jaringan-Terhadap-Eternal-Blue-dan-Wannacry-Ransomware.pdf>.
- [11]. C. Manzano, C. Meneses, and P. Leger, "An Empirical Comparison of Supervised Algorithms for Ransomware Identification on Network Traffic," *Proc. - Int. Conf. Chil. Comput. Sci. Soc. SCCC*, vol. 2020-Novem, 2020, DOI: 10.1109/SCCC51225.2020.9281283.
- [12]. T. P. Setia, A. P. Aldya, and N. Widiyasono, "Reverse Engineering untuk Analisis Malware Remote Access Trojan," *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, p. 40, 2019, doi: 10.26418/jp.v5i1.28214.
- [13]. B. Nunes, M. Mendonca, X. N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, future of programmable networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1617-1634, Feb. 2014.
- [14]. A. Arabo, R. Dijoux, T. Poulain, and G. Chevalier, "Detecting ransomware using process behaviour analysis," *Procedia Comput. Sci.*, vol. 168, no. 2019, pp. 289–296, 2020, DOI: 10.1016/j.procs.2020.02.249.
- [15]. E. Berrueta, D. Morato, E. Magana, and M. Izal, "A Survey on Detection Techniques for Cryptographic Ransomware," *IEEE Access*, vol. 7, pp. 144925–144944, 2019, DOI: 10.1109/ACCESS.2019.2945839.
- [16]. N. Hildayanti, "Forensics Analysis of Router On Computer Networks Using Live Forensics Method," *Int. J. Cyber-Security Digit. Forensics*, vol. 8, no. 1, pp. 74–81, 2019, DOI: 10.17781/p002559.
- [17]. Alzahrani, S., Xiao, Y., & Sun, W. (2022). An Analysis of Conti Ransomware Leaked Source Codes. *IEEE Access*, 10, 100178-100193.
- [18]. K. Cabaj and W. Mazurczyk, "Using software-defined networking for ransomware mitigation: The case of CryptoWall," *IEEE Network*, vol. 30, no. 6, pp. 14-20, Dec. 2016
- [19]. M. Hikmatyar, Y. Prayudi, and I. Riadi, "Network Forensics Framework Development using Interactive Planning Approach," *Int. J. Comput. Appl.*, vol. 161, no. 10, pp. 41–48, 2017, DOI: 10.5120/ijca2017913352.
- [20]. S. R. Davies, R. Macfarlane, and W. J. Buchanan, "Evaluation of live forensic techniques in ransomware attack mitigation," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 300979, 2020, DOI: 10.1016/j.fsidi.2020.300979.
- [21]. A. Liu, H. Fu, Y. Hong, J. Liu, and Y. Li, "LiveForen: Ensuring Live Forensic Integrity in the Cloud," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 10, pp. 2749–2764, 2019, DOI: 10.1109/TIFS.2019.2898841.

- [22]. R. Umar, A. Yudhana, and M. Nur Faiz, "Experimental Analysis of Web Browser Sessions Using Live Forensics Method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, p. 2951, 2018, DOI: 10.11591/ijece.v8i5.pp2951-2958.
- [23]. M. KA, *Learning Malware Analysis*. Birmingham - Mumbai: Packt Publishing Ltd., 2018.
- [24]. R. Agrawal, J. W. Stokes, K. Selvaraj, and M. Marinescu, "University of California, Santa Cruz, Santa Cruz, CA 95064 USA Microsoft Corp ., One Microsoft Way, Redmond, WA 98052 USA," pp. 3222–3226, 2019.
- [25]. S. Sheen and A. Yadav, "Ransomware detection by mining API call usage," 2018 *Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2018*, pp. 983–987, 2018, doi: 10.1109/ICACCI.2018.8554938.
- [26]. S. Baek, Y. Jung, A. Mohaisen, S. Lee, and D. Nyang, "SSDassisted Ransomware Detection and Data Recovery Techniques," *IEEE Trans. Comput.*, vol. X, no. X, pp. 1–1, 2020, DOI: 10.1109/tc.2020.3011214.
- [27]. M. Ahmed and H. Saeed, "Malware in Computer Systems : Problems and Solutions," vol. 9, no. 1, pp. 1–8, 2020, DOI: 10.14421/ijid.2020.09101.
- [28]. T. Xia, Y. Sun, S. Zhu, Z. Rasheed, and K. Shafique, "Toward A network-assisted Approach for Effective Ransomware Detection," *arXiv*, Aug. 2020, [Online]. Available: <http://arxiv.org/abs/2008.12428>.
- [29]. Alzahrani, S., Xiao, Y., & Sun, W. (2022). An Analysis of Conti Ransomware Leaked Source Codes. *IEEE Access*, 10, 100178-100193.
- [30]. A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O'Kane, "A Multi-Classifer Network-Based Crypto-Ransomware Detection System: A Case Study of Locky Ransomware," *IEEE Access*, vol. 7, no. c, pp. 47053–47067, 2019, DOI: 10.1109/ACCESS.2019.2907485.
- [31]. S. H. Kok, A. Abdullah, and N. Z. Jhanjhi, "Early detection of crypto-ransomware using pre-encryption detection algorithm," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2020, doi: 10.1016/j.jksuci.2020.06.012.
- [32]. A. Adamov, A. Carlsson, and T. Surmacz, "An analysis of lockergoga ransomware," 2019 *IEEE East-West Des. Test Symp. EWDTs 2019*, pp. 1–5, 2019, DOI: 10.1109/EWDTs.2019.8884472