



Ranzy Locker Technical Analysis Report



Contents

Introduction.....	3
Summary	3
deleteme.exe Analysis.....	4
Yara Rule.....	14
Prepared BY	15

Introduction

The malware known as Ranzy Locker belongs to the ThunderX ransomware family. It encrypts all important files on your computer.

Ranzy Locker malware was first spotted on October 21, 2020. When the victim infects the computer, it encrypts important files and demands a ransom for decryption. It performs the request process by communicating with the proton e-mail address through the key of the infected system in the readme.txt file it creates after encrypting the files.

The malware usually targets Windows systems.

Summary

Deleteme.exe takes snapshots of many applications and their information. The list of these applications is listed in detail in the detailed analysis section.

It tries to make the pest unanalyzable by applying various anti-debug methods and tries to complicate the analyst's job.

It deletes the data in the recycle bin and system backups, if any.

It receives the information of how many disks are defined in the system and the adapter information.

Finally, the victim encrypts all important data on the computer and demands a ransom.

deleteme.exe Analysis

The MD5, SHA-1 and SHA-256 information of the malware are given in the table below.

File Name	Exe File
MD5	84e8bf44a339c6c2a51aedb17b52e83e
SHA-1	6681ac4c02f2b2696590eebad5f8e94cf1723678
SHA-256	0db6f0721b23aba59852382dad8042be26832c7bb182d79f4734e17da3bcd5ee

It is understood that it is a 32-bit exe file of Portable Executable type.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ .!...J...ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	08	01	00	00C ..
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	p °p. 'í!, Lí!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is.program.canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t.be.run.in.DOS.
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$.....
00000080	E1	6C	A8	3C	A5	0D	C6	6F	A5	0D	C6	6F	A5	0D	C6	6F	ál"<¥.Æc¥.Æc¥.Æo
00000090	FE	65	C5	6E	AF	0D	C6	6F	FE	65	C3	6E	30	0D	C6	6F	geÅn".ÆogeÅn0.Æo
000000A0	FE	65	C2	6E	B7	0D	C6	6F	6E	62	C2	6E	B4	0D	C6	6F	geÅn".ÆonbÅn'.Æo
000000B0	6E	62	C5	6E	B0	0D	C6	6F	6E	62	C3	6E	8F	0D	C6	6F	nbÅn".ÆonbÅn .Æo
000000C0	FE	65	C7	6E	B0	0D	C6	6F	A5	0D	C7	6F	2E	0D	C6	6F	geÇn".Æc¥.Ço..Æo
000000D0	23	7D	CF	6E	AF	0D	C6	6F	23	7D	39	6F	A4	0D	C6	6F	#}În".Æo#}9o».Æo
000000E0	A5	0D	51	6F	A4	0D	C6	6F	23	7D	C4	6E	A4	0D	C6	6F	¥.Ço».Æo#}Ån».Æo
000000F0	52	69	63	68	A5	0D	C6	6F	00	00	00	00	00	00	00	00	Rich¥.Æo.....
00000100	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	04	00PF..T. J.

```

0018FE2C 00000004
0018FE30 00000000
0018FE34 0018FE60
0018FE38 0040E103 return to delete.me.0040E103 from delete.me.0040E8EF
0018FE3C 00000004
0018FE40 0018FEE8
0018FE44 0018FE98 "43"
0018FE48 00000000
0018FE4C 0040C0B5 return to delete.me.0040C0B5 from delete.me.0040E0E6
0018FE50 00401F36 return to delete.me.00401F36 from delete.me.0040C0B0
0018FE54 0018FEE8
0018FE58 00420BF8 &"433A5C50726F6772616D2046696C65735C4D6963726F736F66742053514C20536572766572"
0018FE5C 0018FE98 "43"
0018FE60 0018FEC0
0018FE64 00406081 return to delete.me.00406081 from delete.me.00401F29
0018FE68 0018FE98 "43"
0018FE6C 19E5D7E3
0018FE70 00000036
0018FE74 00421D38 delete.me.00421D38

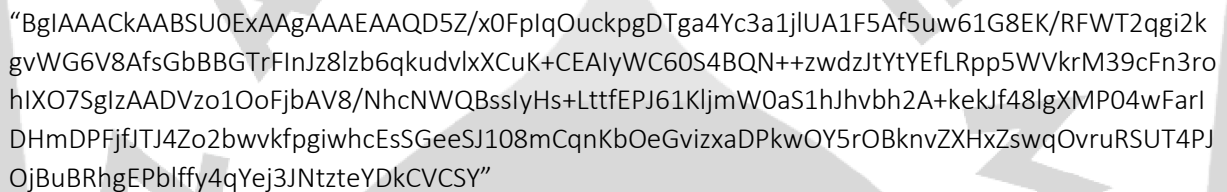
```

There is an ASCII like

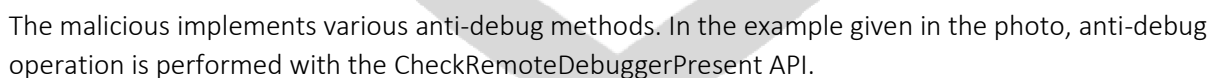
"433A5C50726F6772616D2046696C65735C4D6963726F736F66742053514C20536572766572".

This ASCII means "C:\Program Files\Microsoft SQL Server". Here, the malware controls the SQL database servers.

It creates and opens a mutex object named "Global\35355FA5-07E9-428B-B5A5-1C88CAB2B488".



It then performs encryption operations.



```

0018FDDC 0040E103 return to delete.me.0040E103 from delete.me.0040E8EF
0018FDE0 00000004
0018FDE4 0018FE80
0018FDE8 0018FE3C "72"
0018FDEC 00000000
0018FDF0 0040C0B5 return to delete.me.0040C0B5 from delete.me.0040E0E6
0018FDF4 00401F36 return to delete.me.00401F36 from delete.me.0040C0B0
0018FDF8 0018FE80
0018FDFC 00420988 &"72651646D652E747874"
0018FE00 0018FE3C "72"
0018FE04 0018FE68
0018FE08 00402288 return to delete.me.00402288 from delete.me.00401F29
0018FE0C 0018FE3C "72"
0018FE10 19E5D74B
0018FE14 005718CE
0018FE18 00588D18 L"Application Data"
0018FE1C 00000000
0018FE20 0018FE80
0018FE24 0018FE00 &"72"

```

When the string is decoded as “72651646D652E747874” which is encoded with ASCII, it is observed that the “readme.txt” document is created and it is understood that this document is the ransom demand document included in the continuation of the analysis.

Ransomware changes the extensions of the files it encrypts to “.lock”.

The malware takes snapshots of the processes and some applications running on the system and checks whether they are running. These files are listed below;

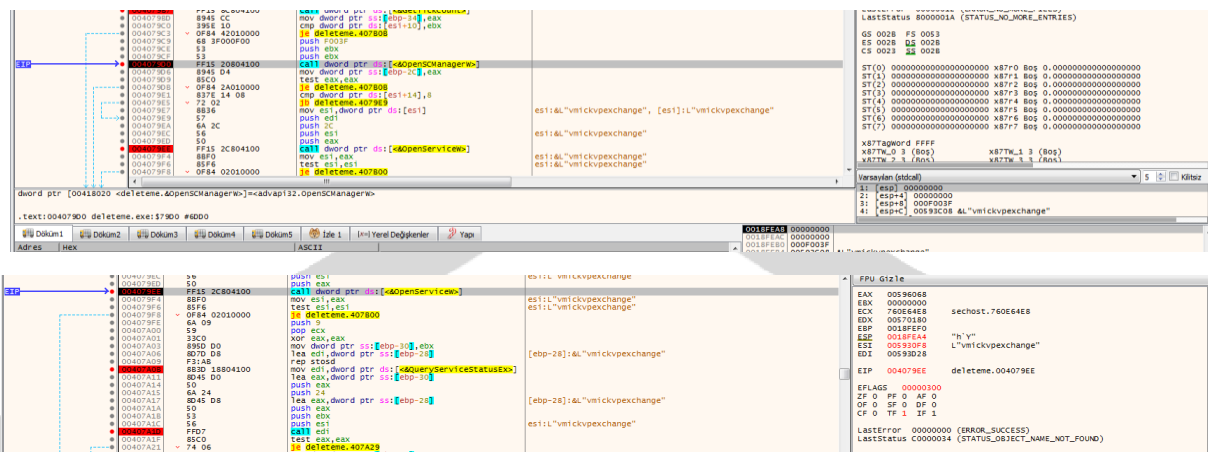
winword.exe	visio.exe	ensvc.exe	mysql_opt.exe
occsd.exe	thabat.exe	ocomm.exe	outlook.exe
mysqld.exe	sqlagent.exe	sqlservr.exe	infopath.exe
sqlbrowser.exe	thunderbird.exe	msftesql.exe	wordpad.exe
synctime.exe	agntsvc.exe	dbsnmp.exe	mydesktopservice.exe
ocautoupds.exe	thebat64.exe	sqbcoreservice.exe	isqlplussvc.exe
oracle.exe	tbirdconfig.exe	mysqld-nt.exe	

These applications include various SQL servers, e-mail clients, notebooks and some software from Oracle.

It implements anti debug with GetTickCount API.

Some WMI queries are being executed. These queries are listed below;

vmickvpexchange	vmicquestinterface	vmicshutdow	vmicheartbeat
MSSQLFDLauncher	MSSQLSERVER	SQLBrowser	SQLSERVERAGENT
SQLWriter	MSSQL	WRSVC	ekrn



It connects to Services Control Manager with OpenSCManagerW and starts the vmickvpexchange service listed above with the Open ServicesW API.

The vmickvpexchange service provides a mechanism for exchanging data between the virtual machine and the operating system running on the physical computer.

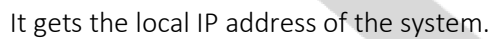
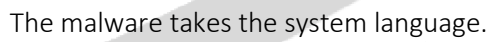
Malware tries to make it impossible to recover data after the files are encrypted by executing various commands. It encodes these commands as ASCII and decodes them one by one. All the commands it executes are listed below;

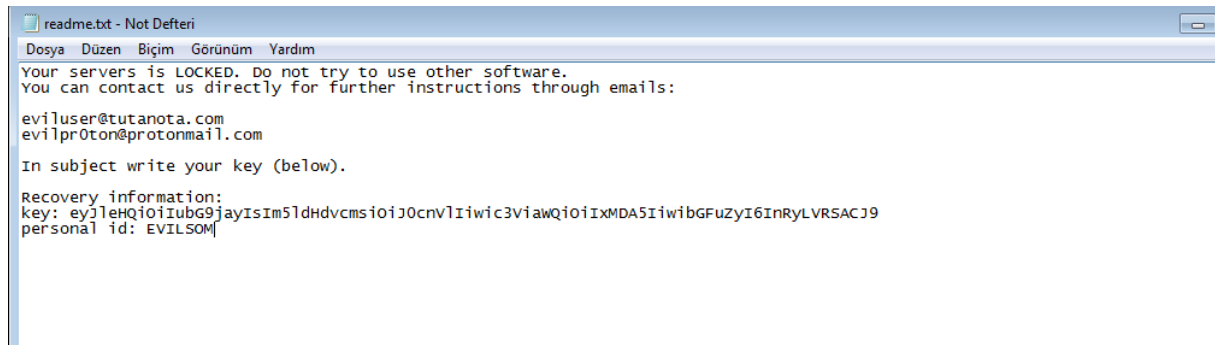
Command	Action
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest	Deletes all the oldest system backups.
wmic.exe SHADOWCOPY /nointeractiv	Deletes all Shadow Copies.
wbadmin DELETE SYSTEMSTATEBACKUP	Deletes all system backups.
bcdedit.exe /set {default} recoveryenabled No	Disables Windows recovery and repair.
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures	Disables Windows recovery. If an error occurs, it will attempt to boot the computer normally.
vssadmin.exe Delete Shadows /All /Quiet	Deletes all Shadow Copies.

It creates a thread.

Checks how many disks are defined in the system.

It has been determined that when the data encoded as ASCII is decoded, it receives data such as "ext":, "network":, "subid":, "lang":, {PATTERN_ID}, {UID}.





```
readme.txt - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
Your servers is LOCKED. Do not try to use other software.
You can contact us directly for further instructions through emails:
eviluser@tutanota.com
evilpr0ton@protonmail.com
In subject write your key (below).
Recovery information:
key: ey3leHQi0iubG9jayisIm5ldHdvcm5ioiJ0cnVliiwic3ViaWQioiIXMDA5IiwibGFuZyI6InRyLVR5SACj9
personal id: EVILSOM
```

After the encryption process is completed, it creates the readme.txt file, defines a special key to the victim computer in this file, and then states that it is necessary to contact the protonmail address in this file in order to recover the encrypted files.

Protection Methods

Up-to-date anti-virus software should be used.

The operating system should be kept up to date.

File and printer sharing services should be disabled. If these services are required, strong passwords or Active Directory authentication should be used.

Multi-factor authentication should be used.

Users' permissions to install and run unwanted software applications should be restricted. Users should not be added to the local administrators group unless necessary.

Strong passwords should be used.

Care should be taken when opening e-mail attachments.

Unnecessary services should be disabled on agency workstations and servers.

Suspicious email attachments should be scanned or removed.

Users' web browsing habits should be monitored and access to sites with negative content should be restricted.

Care should be taken when using removable media (eg USB flash drives, external drives, CDs).

All software downloaded from the internet should be scanned before running.

Awareness of the latest threats should be maintained and appropriate access control lists should be implemented.

Yara Rule

```
import "hash"

rule Ranzy_Locker
{
  meta:
    author = "ZAYOTEM-TAHA HİCRET"
    description = "RanzyLocker"
    first_date = "21.10.2020"
    report_date = "05.08.2021"
    file_name = "deleteme.exe"
    strings:
      $s1 = "476C6F62616C5C33353335354641352D303745392D343238422D423541352D314338384341423242343838"
      $s2 = "776D69632E65786520534841444F57434F5059202F6E6F696E746572616374697665"
      $s3 = "776261646D696E2044454C4554452053595354454D53544154454241434B5550"
      $s4 = "776261646D696E2044454C4554452053595354454D53544154454241434B5550202D64656C6574654F6C64657374"
      $s5 = "626364656469742E657865202F736574207B64656661756C747D207265636F76657279656E61626C6564204E6F"
      $s6 = "626364656469742E657865202F736574207B64656661756C747D20626F6F74737461747573706F6C6963792069676E6F7265616C6C6661696C75726573"
      $s7 = "76737361646D696E2E6578652044656C65746520536861646F7773202F416C6C202F5175696574"
      $s8 = "433A5C50726F6772616D2046696C65735C4D6963726F736F66742053514C20536572766572"
      $s9 = "534F4654574152455C4D6963726F736F66745C45524944"
    condition:
      hash.md5(0, filesize) == "84e8bf44a339c6c2a51aedb17b52e83e"
      or
      all
      of
      them
}
```

A large, light gray watermark of the ZAYOTEN logo is centered on the page. The logo consists of a shield shape with the word "ZAYOTEN" in a stylized font along the top edge. Inside the shield is a central emblem featuring a star and crescent above a vertical staff with two wings at the base.

Prepared BY

Taha HİCRET

<https://www.linkedin.com/in/taha-hicret>