MALWATION

Malware Analysis Solutions

Ryuk Ransomware Technical Analysis Report

Sanayi Mah. Teknopark Bulvarı +90 850 577 4225
Teknopark 4A Apt. No: 1/4A/ 101info@malwation.com
34906 Pendik İstanbul www.malwation.com

Contents

Information about file paths, network movements and all indications for the Ryuk malware of type Ransomware has been analyzed and reported in detail.

Introduction

Ransomware type Ryuk is one of the first ransomware families with the ability to identify network drives and resources, encrypt them and delete shadow copies. It is estimated that the Ryuk malware first appeared in August 2018.

Ryuk is a type of ransomware used in targeted attacks where threat actors ensure that essential files are encrypted so they can request large amounts of ransom. The Ryuk ransom demand can reach several hundred thousand dollars.

Ryuk is one of the first ransomware families with the ability to identify network drives and resources, encrypt, and delete shadow copies. This means that attackers can then disable Windows System Restore for users and make recovery from this attack impossible without external backup or rollback technology.

Researchers in Deloitte Argentina, Gabriela Nicolao and Luciano Martins, linked Ryuk ransomware to CryptoTech, a little-known cybercriminal group that was observed to sell Hermes 2.1 on an underground forum in August 2017.

The Ryuk malware targets institutions / organizations that can pay by demanding high ransom. Ryuk's targets tend to be high-profile organizations where attackers know they can reap their large ransom demands. Among the victims are EMCOR, UHS hospitals and several newspapers. While targeting these organizations, Ryuk is known to collect as much as $ 64 million in payments for its operators between February 2018 and October 2019.

In late September, a hospital chain within Universal Health Services (UHS), one of the largest healthcare providers in the United States, was known to have been attacked by Ryuk ransomware.

As with many malware attacks, the delivery method is spam emails. A typical Ryuk attack starts when a user opens a malicious Microsoft Office document attached to a phishing email. Opening the document causes a malicious macro to execute a PowerShell command that tries to download the malicious Ryuk file, which then tries to infect different devices by discovering the current network.

The Russia-based group named Wizzard Spiders has been carrying out various attacks with the Ryuk malware since August 2018. The group, which specifically targets corporate companies, demands different ransom fees for each company. First of all, the system is discovered with the trojan malware infecting the system and a ransom fee is determined for the company. This price has been determined as minimum 1.7 BTC and maximum 99 BTC.

On November 29, 2018, WIZARD SPIDER changed the way it communicated with its victims. As seen in the previous ransom note version, WIZARD SPIDER included BTC addresses and email addresses. However, recent variants of Ryuk no longer include the BTC address, only email addresses.

The Wizzard Spiders group, which received a ransom of 705 BTC ($ 3.7 million) with 52 known transactions with 37 different BTC addresses in 5 months, has received a ransom of $ 61 million in two years since the Ryuk malware came out.

BTC addresses detected and ransom fees received;

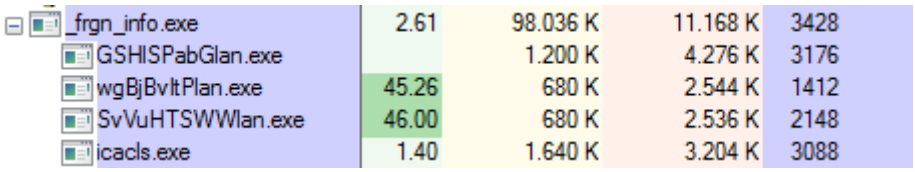
BTC ADDRESS	BTC PCS
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk	10.00
12vsQry1XrPjPCaH8gWzDJeYT7dhTmpcjL	55.00
1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY	182.99
1FtQnqvjxEK5GJD9PthHM4MtdmkAeTeoRt	48.250
14aJo5L9PTZhv8XX6qRPncbTXecb8Qohqb	25.00
1GXgngwDMSJZ1Vahmf6iexKVePPXsxGS6H	30.00
1CbP3cgi1Bcjuz6g2Fwvk4tVhqohqAVpDQ	13.00
1Jq3WwsaPA7LXwRNYsfySsd8aojdmkFnW	35.00
1ET85GTps8eFbgF1MvVhFVZQeNp2a6LeGw	3.325
1FRNVupsCyTjUvF36GxHZrvLaPtY6hgkTm	38.99
1CW4kTqeoedinSmZiPYH7kvn4qP3mDJQVa	24.077
1KUbXkjDZL6HC3Er34HwJiQUAE9H81Wcsr	10.00
19AE1YN6Jo8ognKdJQ3xeQQL1mSZyX16op	25.00
1L9fYHJJxeLMD2yyhh1cMFU2EWF5ihgAmJ	40.035
18eu6KrFgzv8yTMVvKJkRM3YBAyHLonk5G	30.00
1C8n86EEttnDjNKM9Tjm7QNVgwGBncQhDs	30.0082
1ChnbV4Rt7nsb5acw5YfYyvBFDj1RXcVQu	28.00
1CN2iQbBikFK9jM34Nb3WLx5DCenQLnbXp	15.00
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj	50.41
1NuMXQMUxCngJ7MNQ276KdaXQgGjpjFPhK	10.00

Preview

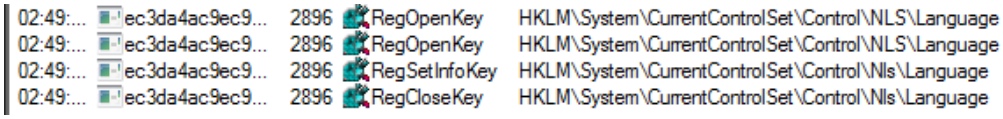
This version of Ryuk malicious, which continues its classic propagation in this version with mail phishing method, first appeared on 04.11.2020. The first name of the malicious file "**_frgn_info.exe**".

Ryuk uses RSA and AES encryption methods as a malicious encryption method.
Ransomware deletes backup files and copies of Windows Shadow, complicate the restore of data from backups. To avoid detection by antiviruses, Ryuk uses obfuscation technique.

The process pre-impression image of the Ryuk malicious is as follows.



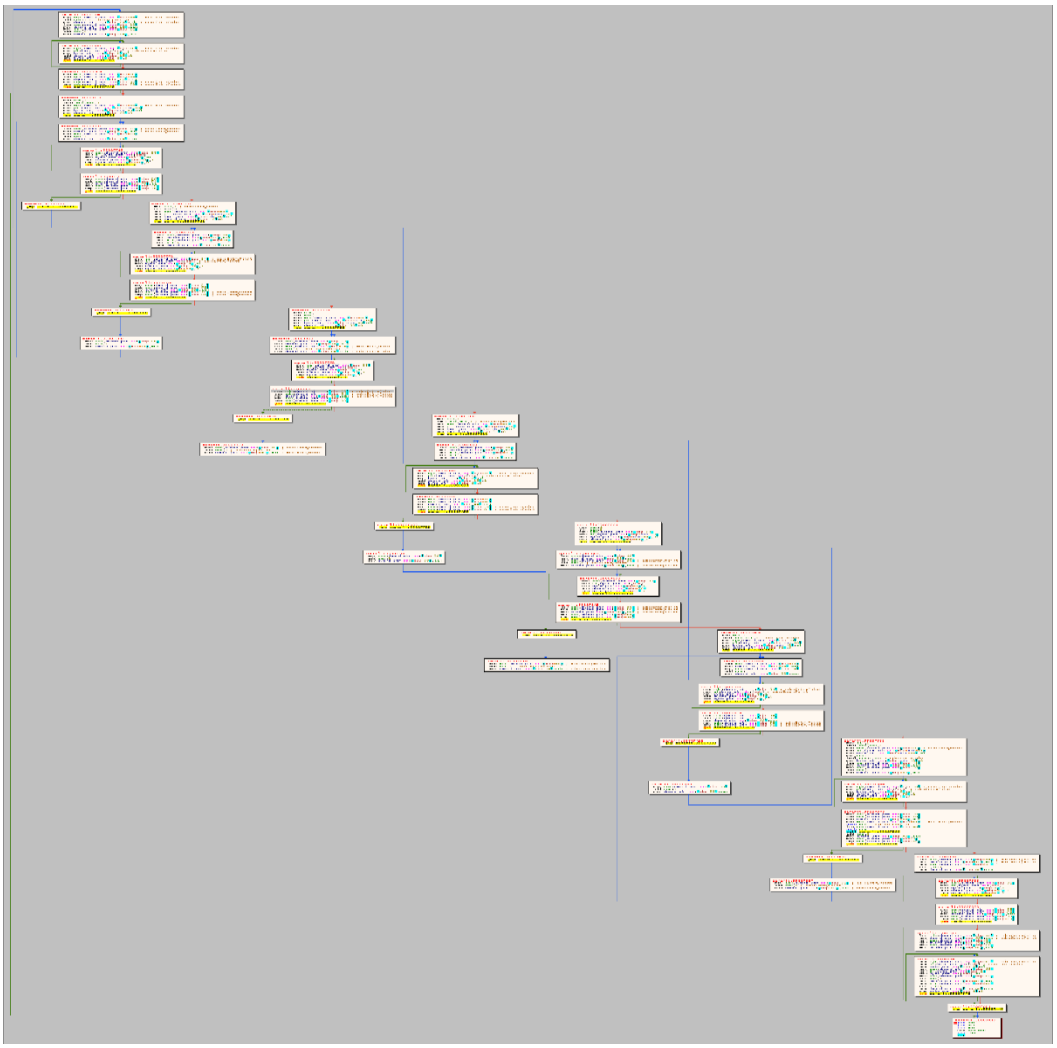
Reads the malicious system language from the register "**HKLM\System\CurrentControlSet\Control\NLS\Language**".



_frgn_info.exe Analysis

File Name	_frgn_info.exe
MD5	0a0b0ac20e9fe72753e74def1e37724f
SHA1	fd683b33ee10ba92e485f76fbad9b48a2e697358
SHA256	ec3da4ac9ec917e66ab943ab149119807922f64f2e4960ebadc36fe7520b300f

The Ryuk malicious uses certain Anti-Debug methods to block analysis. The function of the Anti-Debug method is as shown in the image below.



After the pass of the malicious Anti-Debug method, it is the decode process of encoded strings. some of the strings obtained at the end of this process, which use two different decode functions, are as follows;

- SCHTASKS /CREATE /NP /SC DAILY /TN \ “Print”
- SYSVOL
- RyukReadMe.html
- \\Documents and Settings\\Default User\\sys
- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)
- DEL /F
- SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\
- Crss.exe
- .RYK
- Boot
- Lan.exe
- SYSTEM\\CurrentControlSet\\Control\\Nls\\Language\\
- /C REG ADD \”HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run” /v \”EV\” /t REG_SZ /d \””
- \\Documents and Settings\\Default User\\
- “\” /TR \“C:\\Windows\\System32\\cmd.exe /c for /l %x in (1,1,50) do start wordpad.exe /p”
- 10.
- Boot
- Microsoft Base Cryptographic Provider v1.0
- NTDS
- Cmd.exe /c \”bootstatuspolicy ignoreallfailures\”
- Lan.exe
- \\users\\public\\sys
- Mozilla
- HERMES
- \\users\\public\\
- Sysvol
- lsaas.exe
- /grant Everyone:F /T /C /Q
- cmd.exe /c \ “WMIC.exe shadowcopy delete\”
- 192.
- /C REG DELETE ”HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\” /v \”EV\” /f
- cmd.exe /c \”bcdedit /set {default} recoveryenabled No & bcdedit /set {defalult}\”
- explorer.exe
- 172.
- Chrome
- cmd.exe /c \”vssadmin.exe Delete Shadows /all /quiet\”
- crss.exe

API functions needed to perform malicious operations are also resolved here. The functions to be used for malicious processes are then installed in the memory area. The functions needed by the malware are listed below.

WSAStartup	Socket	Setsockopt
Sendto	Closesocket	WSACleanup
InetNtopW	İnet_ntop	GetTempPathW
CreateToolhelp32Snapshot	Process32FirstW	Process32NextW
VirtualFree	CryptExportKey	DeleteFileW
GetLastError	GetDriveTypeW	GetCommandLineW
GetStartupInfoW	FindNextFileW	VirtualAlloc
GetUserNameA	ExitProcess	Wow64evertWow64FsRedirection
CreateProcessA	GetIpNetTable	GetVersionExW
GetSystemDefaultLangID	GetUserNameW	Wow64DisableWow64FsRedirection
ReadFile	RegQueryValueEXA	CloseHandle
RegSetValueEXW	RegCloseKey	CopyFileA
SetFileAttiributesW	WinExec	CyptDeriveKey
CryptGenKey	Sleep	GetCurrentProcess
ShellExecuteW	GetFileSize	GlobalAlloc
FindClose	WaitForMultipleObjects	GetModuleFileNameA
ShellExecuteA	GetModuleHandleA	GetModuleFileNameW
CreateFileA	GetFileSizeEx	WriteFile
GetLogicalDrivers	WnetEnumResourceA	WnetEnumResourceW
RegOpenKeyExW	WnetCloseEnum	GetWindowsDirectoryW
SetFileAttiributesA	RegOpenKeyExA	SetFilePointer
GetTickCount	GetFileAttiributesW	FindFirstFileW
CryptAcquireContextW	MoveFileExW	WnetOpenEnumA
WnetOpenEnumW	CoInitialize	CryptDecrypt
CryptImportKey	SetFilePointerEx	CopyFileW
FreeLibrary	CreateProcessW	CreateDirectoryW
Create Thread	CryptDestroyKey	CoCreateInstance
CreateFileW	GetFileAttributesA	RegDeleteValueW
EnumServicesStatusW	GetTokenInformation	ImpersonateSelf
LookupPrivilegeValueW	OpenProcessToken	OpenSCManagerW
OpenThreadToken	AdjustTokenPrivileges	VirtualAllocEx
LookupAccountsidW	CommandLineToArgvW	WriteProcessMemory
VirtualFreeEx	CreateRemoteThread	GetAdaptersAddresses
IcmpCloseHandle	IcmpCreateFile	IcmpSendEcho

Following the decode operation of strings, the Ryuk malicious copies itself to the directory where it is located to run with the parameter "**8 LAN**". The name of the copied executable file is also used by using the **GetTickCount** API, adding the string "**lan.exe**" to the end, with nine letters randomly.

```
lea eax,dword ptr ss:[ebp-B90]          eax:L"C:\\Users\\ceku\\Desktop\\SDcuPjXytlan.exe"
push eax
lea ecx,dword ptr ss:[ebp-F78]          ecx:L"C:\\Users\\ceku\\Desktop\\zararli.exe"
push ecx
call dword ptr ds:[<&CopyFileW>]
```

The malicious uses the **SetFileAttributesW** API to hide the new file after copying itself to the directory where it started.

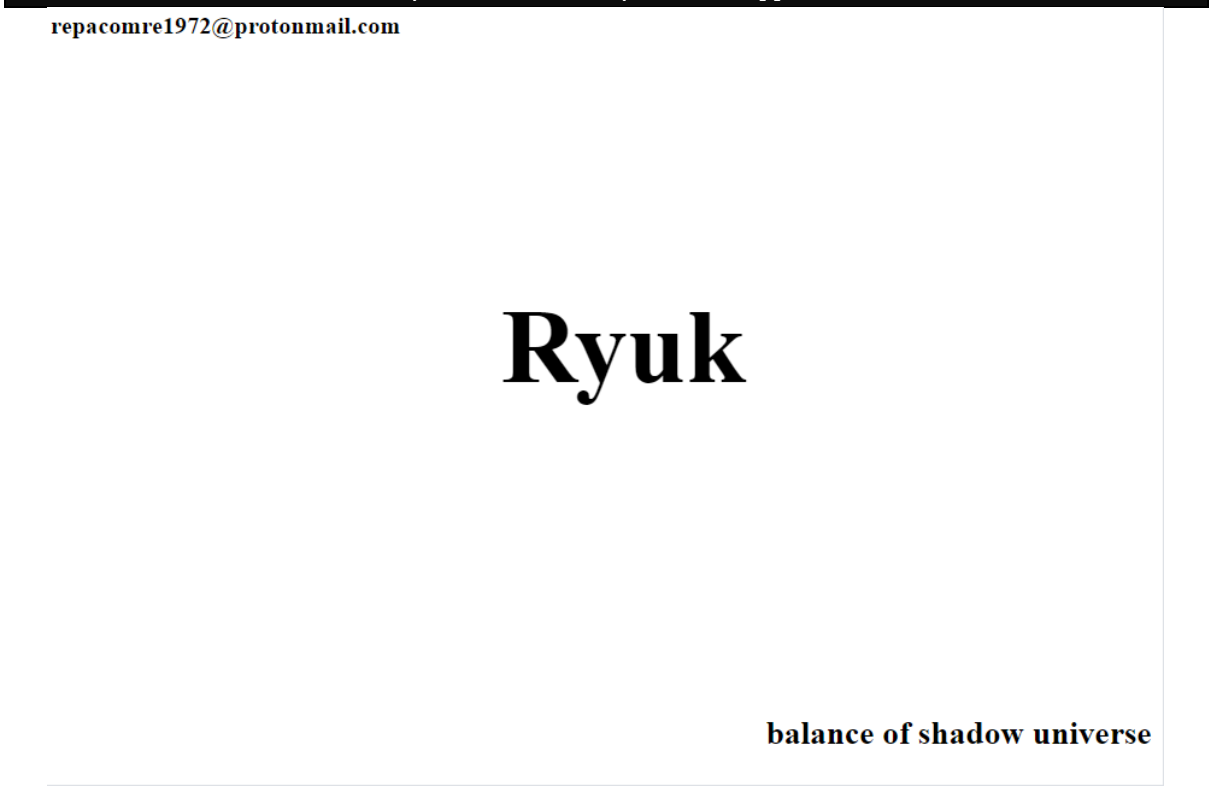
```
push 2
lea edx,dword ptr ss:[ebp-B90]          edx:L"C:\\Users\\ceku\\Desktop\\SDcuPjXytlan.exe"
push edx
call dword ptr ds:[<&SetFileAttributesW>]
```

After setting the visibility of the file written to the desktop, it is run with the parameter "**8 LAN**".

```
push eax                                eax:L"8 LAN"
lea ecx,dword ptr ss:[ebp-B90]          ecx:L"C:\\Users\\ceku\\Desktop\\SDcuPjXytlan.exe"
push ecx
push 0
push 0
call dword ptr ds:[<&ShellExecuteW>]
```

After repeating this process at least 3 times, a file named "RyukReadMe.html" is created in the scanned directories. The file contains a ProtonMail account.

Repacomre1972@protonmail[.]com



Ryuk ransomware, starts operations with the parameters specified in the process "**icacls**". Two different icacls processes begin for the "**C**" and "**D**" directories.

```
push 0
lea eax,dword ptr ss:[ebp-33C]
push eax                                  eax:"icacls \"C:\\*\" /grant Everyone:F /T /C /Q"
call dword ptr ds:[<&WinExec>]
push 0
lea eax,dword ptr ss:[ebp-33C]
push eax                                  eax:"icacls \"D:\\*\" /grant Everyone:F /T /C /Q"
call dword ptr ds:[<&WinExec>]
```

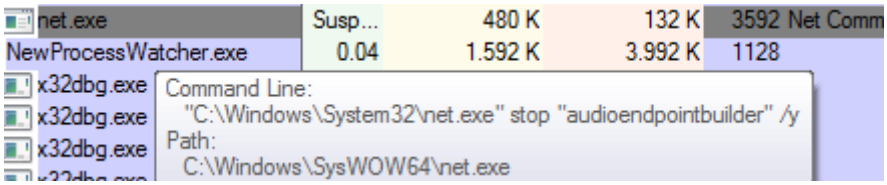
This process is a Microsoft Windows local command-line utility that can display and modify security descripters on folders and files. Allows all users to access files and folders on the specified drive.
The" **F**" parameter has full access. The " **/Q /C /T**" parameter allows permissions to be applied to all subfolders.

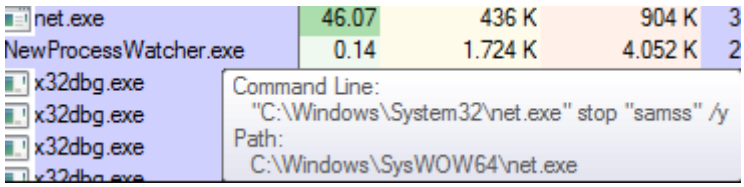
Likewise, it disables Windows startup repair using the **bcdedit** command via the **WinExec** API.

cmd.exe /c "bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures"

Ransomware stops the following services the "**net.exe**" legal process;

- C: \ Windows \ System32 \ net.exe audioendpointbuilder /y
- C: \ Windows \ System32 \ net.exe samss /y



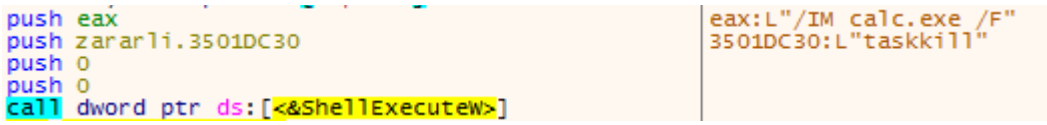


The Ryuk malicious stops the **Windows Audio Endpoint Builder** audio service. As a second step, **Security Accounts Manager** stops the service. Disabling this service will prevent other services on the system from being notified. These techniques can be used to prevent alerts generated by suspicious activities on the affected system from being sent to the SIEM system.

It also does control processes running on the system while the malicious encryption process is in process. The checked process names are listed below.

- Vmcomp
- Vmwp
- Veeam
- Backup
- Xchange
- Sql
- Dbeng
- Sofos
- Calc
- Ekrn
- Zoolz
- Encsvc
- Excel
- Firefoxconfig
- İnfopath
- Msaccess
- Mspub
- Mydesktop
- Ocautoupds
- Ocomm
- Ocssd
- Onenote
- Oracle
- Outlook
- Powerpnt
- Sqbcoreservice
- Steam
- Synctime
- Tbirdconfig
- Thebat
- Thunderbird
- Visio
- Word
- Xfssvccon
- Tmlisten
- PccNtMon
- CNTAoSMgr
- Ntrtscan
- mbabtray

If one of the processes listed is running, it is terminated by the malware. For example, when we run “**calc.exe**" process, it terminates the process with the "**taskkill**" command.



The Ryuk malicious continues the process of encrypting files by checking directory names. Directories that the malicious does not encrypt are observed to be as shown in the following image.

```
35002AA4   68 CCE30135          push zararli.3501E3CC                    3501E3CC:L"\\Windows\\
35002AA9   8D8D D4FCFFFF        lea ecx,dword ptr ss:[ebp-32C]
35002AAF   51                   push ecx
35002AB0   E8 6B710000          call zararli.35009C20
35002AB5   83C4 08              add esp,8
35002AB8   85C0                 test eax,eax
35002ABA   0F85 E8000000        jne zararli.35002BA8
35002AC0   68 14C80135          push zararli.3501C814                    3501C814:L"Windows"
35002AC5   8D95 D4FCFFFF        lea edx,dword ptr ss:[ebp-32C]
35002ACB   52                   push edx                                 edx:L"ini"
35002ACC   E8 4F710000          call zararli.35009C20
35002AD1   83C4 08              add esp,8
35002AD4   85C0                 test eax,eax
35002AD6   0F85 CC000000        jne zararli.35002BA8
35002ADC   68 74E40135          push zararli.3501E474                    3501E474:L"boot"
35002AE1   8D85 D4FCFFFF        lea eax,dword ptr ss:[ebp-32C]
35002AE7   50                   push eax
35002AE8   E8 33710000          call zararli.35009C20
35002AED   83C4 08              add esp,8
35002AF0   85C0                 test eax,eax
35002AF2   0F85 B0000000        jne zararli.35002BA8
35002AF8   68 54E90135          push zararli.3501E954                    3501E954:L"WINDOWS"
35002AFD   8D8D D4FCFFFF        lea ecx,dword ptr ss:[ebp-32C]
35002B03   51                   push ecx
35002B04   E8 17710000          call zararli.35009C20
35002B09   83C4 08              add esp,8
35002B0C   85C0                 test eax,eax
35002B0E   0F85 94000000        jne zararli.35002BA8
35002B14   68 4CE50135          push zararli.3501E54C                    3501E54C:L"Chrome"
35002B19   8D95 D4FCFFFF        lea edx,dword ptr ss:[ebp-32C]
35002B1F   52                   push edx                                 edx:L"ini"
35002B20   E8 FB700000          call zararli.35009C20
35002B25   83C4 08              add esp,8
35002B28   85C0                 test eax,eax
35002B2A   75 7C                jne zararli.35002BA8
35002B2C   68 F8EA0135          push zararli.3501EAF8                    3501EAF8:L"Mozilla"
35002B31   8D85 D4FCFFFF        lea eax,dword ptr ss:[ebp-32C]
35002B37   50                   push eax
35002B38   E8 E3700000          call zararli.35009C20
35002B3D   83C4 08              add esp,8
35002B40   85C0                 test eax,eax
35002B42   75 64                jne zararli.35002BA8
35002B44   68 54D70135          push zararli.3501D754                    3501D754:L"SYSVOL"
35002B49   8D8D D4FCFFFF        lea ecx,dword ptr ss:[ebp-32C]
35002B4F   51                   push ecx
35002B50   E8 CB700000          call zararli.35009C20
35002B55   83C4 08              add esp,8
35002B58   85C0                 test eax,eax
35002B5A   75 4C                jne zararli.35002BA8
35002B5C   68 ECE40135          push zararli.3501E4EC                    3501E4EC:L"NTDS"
35002B61   8D95 D4FCFFFF        lea edx,dword ptr ss:[ebp-32C]
35002B67   52                   push edx                                 edx:L"ini"
35002B68   E8 B3700000          call zararli.35009C20
35002B6D   83C4 08              add esp,8
35002B70   85C0                 test eax,eax
35002B72   75 34                jne zararli.35002BA8
35002B74   68 0CDC0135          push zararli.3501DC0C                    3501DC0C:L"netlogon"
35002B79   8D85 D4FCFFFF        lea eax,dword ptr ss:[ebp-32C]
```

The malicious crypts directories using " **Microsoft Enhanced RSA and AES Cryptographic Provider**".

```
68 000000F0          push F0000000
6A 18                push 18
68 D8D70135          push ec3da4ac9ec917e66ab943ab14911980792 3501D7D8:L"Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)"
6A 00                push 0
68 900B0235          push ec3da4ac9ec917e66ab943ab14911980792
FF15 10110235        call dword ptr ds:[<&CryptAcquireContextW>]
```

Extension of encrypted file "**.RYK**"

```
&L"C:\\Program Files\\Cheat Engine 7.1\\autorun\\ceshare\\images\\link.png"
L"C:\\Program Files\\Cheat Engine 7.1\\autorun\\ceshare\\images\\link.png.RYK"

L".RYK"
L".RYK"
```

The "**HERMES**" keyword and public encryption key are added to the encrypted file as the final process. The contents of a sample file are as follows;

dllmain.cpp.RYK

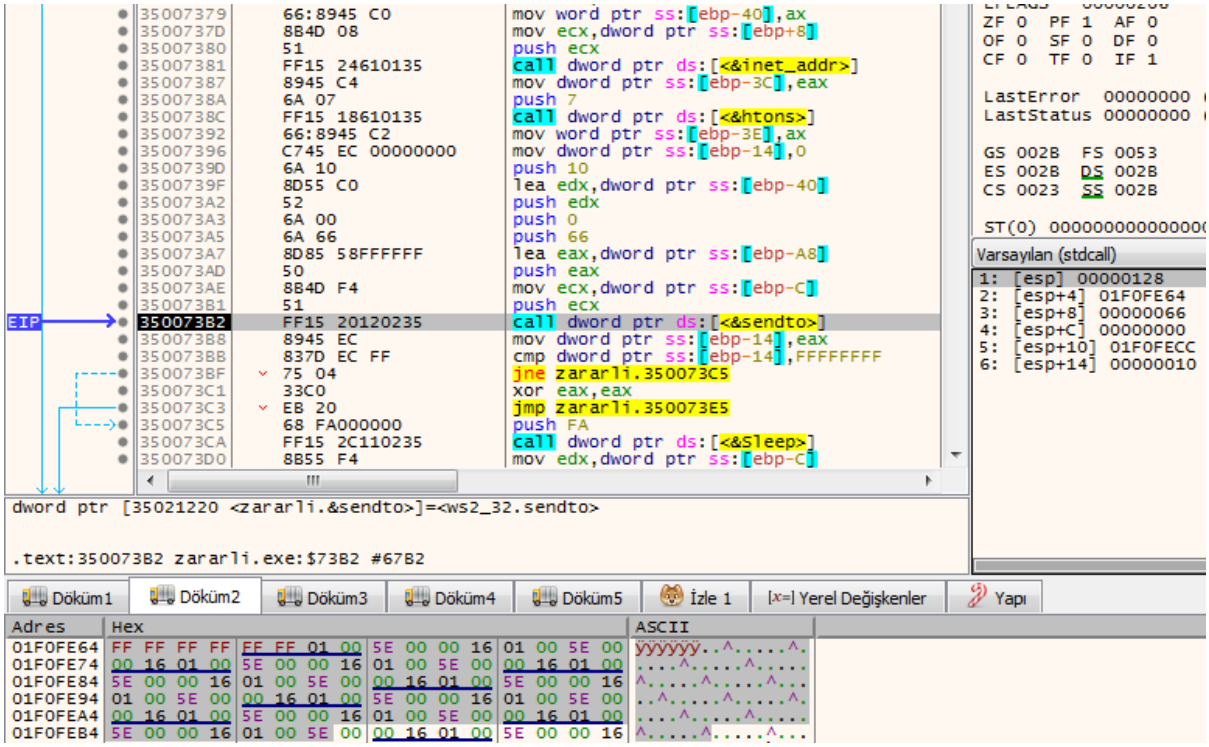
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Çözülmüş metin
00000280	32	BE	34	62	5F	65	18	B3	50	A1	BB	B7	2C	0D	55	9B	2¾4b_e.³P¡»·,.U›
00000290	80	79	D2	D2	68	A6	82	43	18	48	70	BC	6B	15	4A	A7	€yÒÒh¦‚C.Hp¼k.J§
000002A0	44	B6	7A	6F	19	C9	BC	1D	CB	F3	92	77	3C	79	D7	05	D¶zo.É¼.Ëó'w<y×.
000002B0	48	45	52	4D	45	53	01	02	00	00	10	66	00	00	00	A4	HERMES.....f...¤
000002C0	00	00	B9	52	34	7C	8A	23	9B	AD	DE	90	E7	CC	25	D1	..¹R4|Š#›.Ş.çÌ%Ñ
000002D0	76	98	F0	D1	3C	A1	A1	5A	E3	BB	60	88	32	E1	55	37	v˜ğÑ<¡¡Zã»`ˆ2áU7
000002E0	E5	92	95	59	F5	DA	9B	F5	85	6C	1C	1E	6B	E8	40	47	å'•YõÚ›õ…l..kè@G
000002F0	D4	37	D3	89	89	0C	38	35	45	2D	2C	F7	BA	37	C7	38	Ô7Ó‰‰.85E-,÷°7Ç8
00000300	24	1D	25	5A	0A	ED	61	FD	AA	C5	AF	A8	6E	43	25	49	$.%Z.íaı²Å¯¨nC%I
00000310	BE	2E	DD	33	CD	52	B9	D8	CE	80	CD	7D	55	B0	0D	EE	¾.Ì3ÍR¹ØÎ€Í}U°.î
00000320	68	3F	A6	FF	B2	CF	6A	60	D6	49	50	4E	AA	5F	73	55	h?¦ÿ²Ïj`ÖIPNª_sU
00000330	71	F5	75	EA	6F	D5	39	16	6A	DB	87	80	0F	43	02	2C	qõuêoÕ9.jÛ‡€.C.,
00000340	B5	C9	B7	2B	A9	C3	0C	5C	AC	C7	76	C5	47	F9	45	64	µÉ·+©Ã.\¬ÇvÅGùEd
00000350	41	D1	87	50	90	FC	5D	BB	BB	C5	36	D6	E2	09	06	0C	AÑ‡P.ü]»»Å6Öâ...
00000360	A7	C6	41	A8	EB	2D	A6	81	7A	37	0B	9D	47	81	BD	D8	§ÆA¨ë-¦.z7..G.½Ø
00000370	50	90	28	8F	89	0F	17	31	C0	18	5F	58	BF	98	5A	A9	P.(.‰..1À._X¿˜Z©
00000380	8C	60	A8	48	61	C3	25	B6	A8	99	3F	79	36	23	89	F1	Œ`¨HaÃ%¶¨™?y6#‰ñ
00000390	5D	B9	F6	AB	3E	96	4F	B8	CD	10	65	8D	0E	8B	62	FD	]¹ö«>–O¸Í.e..‹bı
000003A0	74	11	FB	44	19	61	FE	BF	36	0F	19	51	4D	4F	9B	05	t.ûD.aş¿6..QMO›.
000003B0	E6	7A	B7	F7	75	9A	5A	49	40	37	E4	15	4B	AD	C6	18	æz·÷ušZI@7ä.K.Æ.
000003C0	5E	B6	□														^¶

Network Analysis

Ransomware, together with processes with parameters "**8 LAN**", initiates a subnet scan on the local network and initiates a wider network scan on the subnet it finds. The subnets it scans are as follows;

- 10.x.x.x
- 172.x.x.x
- 192.x.x.x

In order to perform this scan, the malicious then sends an ARP packet to the IP addresses on the gateway where the computer on which it is running and waits for answers.




```
    19 169.382774    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.4? Tell 192.168.119.129
    20 169.382873    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.6? Tell 192.168.119.129
    21 169.382969    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.8? Tell 192.168.119.129
    22 169.383041    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.10? Tell 192.168.119.129
    23 169.383187    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.12? Tell 192.168.119.129
    24 169.383350    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.14? Tell 192.168.119.129
    25 169.383634    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.1? Tell 192.168.119.129
    26 169.384714    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.16? Tell 192.168.119.129
    27 169.384786    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.18? Tell 192.168.119.129
    28 169.385138    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.20? Tell 192.168.119.129
    29 169.385206    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.22? Tell 192.168.119.129
    30 169.385271    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.24? Tell 192.168.119.129
    31 169.385333    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.26? Tell 192.168.119.129
    32 169.385400    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.28? Tell 192.168.119.129
    33 169.385461    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.30? Tell 192.168.119.129
    34 169.385522    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.32? Tell 192.168.119.129
    35 169.385592    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.34? Tell 192.168.119.129
    36 169.385832    PharosNZ_3e:72:f0    Broadcast           ARP      42 Who has 192.168.119.36? Tell 192.168.119.129
```

When a computer on the local network responds, ransomware is trying to add disks belonging to that computer as network drives and encrypt data on those disks.

MITRE ATT&CK Table

Looking at the dynamically called API and processes, the following MITRE ATT&CK tactics and techniques were detected.

Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Command and Control
T1106	T1574.010	T1055	T1497	T1518.001	T1573
		T1574.010	T1055	T1497	
		T1497	T1564.001	T1057	
		T1564.001	T1027	T1083	
		T1574.010	T1574.010	T1082	

Solution Proposals

- Use of up-to-date, reliable antivirus software in systems,
- Careful reading of incoming mails does not open without scanning the
- attachments in it,
- Spam mails were ignored,
- paying attention to phishing sites while browsing the internet,
- Installing the latest updates available in the operating system
- Monitoring the processes and network movements performed by the running processes on the system

Ryuk malware of ransomware type can be prevented from infecting and damaging the system.

YARA Rule

```
import "hash"

rule Ryuk_Detected
{
    meta:
      author = "MALWATION"
      site = "https://malwation.com"
      description = "Ryuk Ransomware Analysis"

    strings:
            $tes1 = "TES LOGISTIKA d.o.o.1" fullword
            $tes2 = "TES LOGISTIKA d.o.o.0" fullword
            $str1 = "14537679:;decfeh" fullword
            $str2 =
"zcbcjfrivYMnraUQZFkpvMZkaZLAFTfIxUprkulMZnVPRsItEEcHvPHqrPcsVlPilkAGoTdFByXxb
xmXHkhZIRzCTWVcwIdTq" fullword
            $str3 = "Bgyasj440foo"
            $str4 = "RyukReadMe.html"
            $lan = "lan.exe"
            $enc = "encrypt"
            $task = "taskkill"
            $hermes = "HERMES"
            $ryk = ".RYK"
            $extlan =  { ?? ?? ?? ?? ?? ?? ?? ?? ?? 6c 61 6e 2e 65 78 65 }
            $com1 = "cmd.exe /c \"bcdedit /set {default} recoveryenabled No & bcdedit /set
{default}\"" fullword ascii
            $com2 = "\" /TR \"C:\\Windows\\System32\\cmd.exe /c for /l %x in (1,1,50) do start
wordpad.exe /p " fullword ascii
            $com3 = "cmd.exe /c \"vssadmin.exe Delete Shadows /all /quiet\"" fullword ascii
            $com4 = "cmd.exe /c \"WMIC.exe shadowcopy delete\"" fullword ascii
            $com5 = "/grant Everyone:F /T /C /Q"
            $com6 = "Cmd.exe /c \"bootstatuspolicy ignoreallfailures\""
            $path = "\\users\\Public\\"
            $path2= "\\users\\Public\\sys"
            $network_package = {FF FF FF FF FF FF [0-96] 00 00}

    condition:
        hash.md5(0, filesize) == "0a0b0ac20e9fe72753e74def1e37724f" or all of them

}
```