Challenge: Trigona Ransomware Lab

Platform: CyberDefenders

Category: Endpoint Forensics

Difficulty: Medium

Tools Used: EvtxECmd, Timeline Explorer, Registry Explorer, MFTECmd, PECmd, AmcacheParser

Summary: This challenge involved using a series of forensic tools to investigate multiple compromised hosts. We are provided with multiple KAPE images and are expected to form a complete attack timeline for this ransomware incident. Through forensic analysis, you can uncover the attacker's initial access via RDP all the way through to execution of the ransomware binary and encryption of files. I found it relatively challenging but really enjoyed the entire process, so I highly recommend giving it a go.

Scenario: As a forensic investigator at IResponseDash, you are tasked with examining a ransomware attack that has compromised multiple endpoints. Your primary objective is to determine the delivery method of the ransomware and to trace all activities of the attacker to understand the progression of the attack.

To accomplish this, you will analyze logs, review system and network activities, and gather evidence of the attacker's actions. This investigation will allow you to provide recommendations for addressing the current incident and enhancing defenses to prevent future attacks.

Knowing the IP address of the machine that initiated the attack helps trace the attack's origin. What is the IP address of the attacker's machine?

By analysing Event ID 4624 (successful logon) entries in the security logs, specifically filtering for logon type 10 (remote interactive, indicative of an RDP logon), we identified that at 2024-06-30 11:26:57 an unauthorised user authenticated to 'Hanii_IT'.

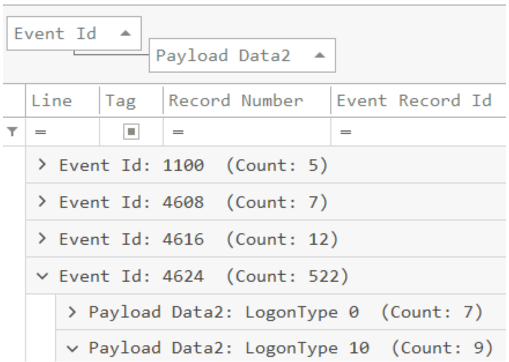
You can find the security.evtx file at:

- C:\Users\Administrator\Desktop\Start Here\Artifacts\IT-Machine\Evidence-IT\C\Windows\System32\winevt

We can parse this log file using EvtxECmd:

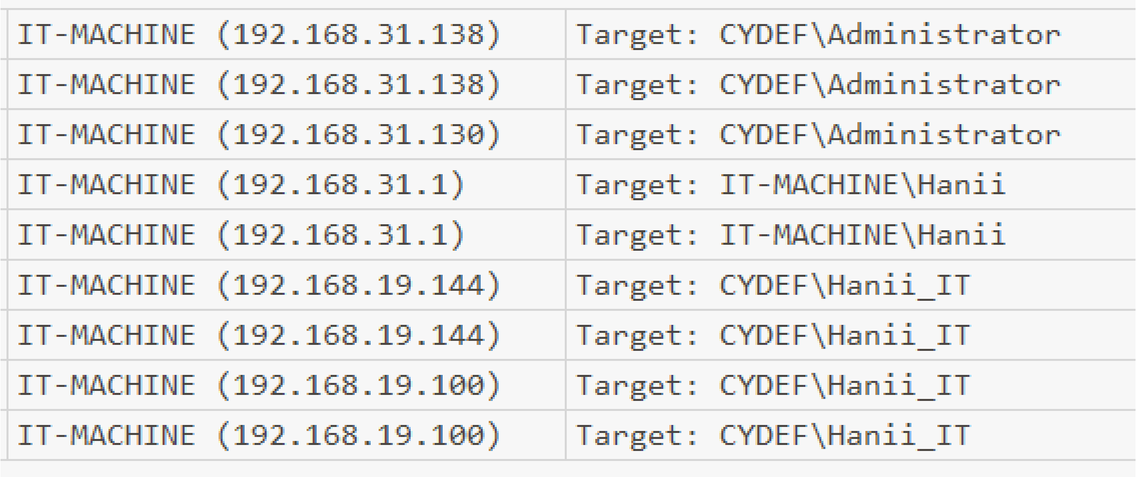
- .\EvtxECmd.exe -f ".\Security.evtx" --csv . --csvf security_out.csv

You can take the output and open it using Timeline Explorer. If we group it by Event ID and Payload Data2 (Long type field), we can see 9 successful remote interactive authentication attempts:



```
Event Id ▲
        Payload Data2 ▲
Line | Tag | Record Number | Event Record Id
 =   |  ■  |  =            |  =
> Event Id: 1100  (Count: 5)
> Event Id: 4608  (Count: 7)
> Event Id: 4616  (Count: 12)
v Event Id: 4624  (Count: 522)
    > Payload Data2: LogonType 0  (Count: 7)
    v Payload Data2: LogonType 10  (Count: 9)
```

At 2024-06-30 11:26:57 someone authenticated to Hanii_IT over RDP with the source IP address being 192.168.100.19, this falls outside of the organisation's subnet, raising concerns about unauthorised access.



IT-MACHINE (192.168.31.138)	Target: CYDEF\Administrator
IT-MACHINE (192.168.31.138)	Target: CYDEF\Administrator
IT-MACHINE (192.168.31.130)	Target: CYDEF\Administrator
IT-MACHINE (192.168.31.1)	Target: IT-MACHINE\Hanii
IT-MACHINE (192.168.31.1)	Target: IT-MACHINE\Hanii
IT-MACHINE (192.168.19.144)	Target: CYDEF\Hanii_IT
IT-MACHINE (192.168.19.144)	Target: CYDEF\Hanii_IT
IT-MACHINE (192.168.19.100)	Target: CYDEF\Hanii_IT
IT-MACHINE (192.168.19.100)	Target: CYDEF\Hanii_IT

Answer: 192.168.19.100

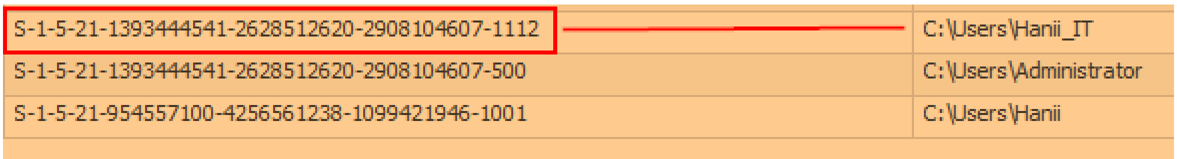
Knowing the account used by the attacker helps track activities and identify compromised accounts. What is the SID of the account the attacker used to gain initial access on the victim machine?

We are able to identify the SID associated with the compromised account 'Hanii_IT' by inspecting the SOFTWARE registry hive, specifically the ProfileList key located at:

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

First, we need to load the registry hive, we can do so by using Registry Explorer. You can find the SOFTWARE hive at:

- C:\Users\Administrator\Desktop\Start Here\Artifacts\IT-Machine\Evidence-IT\C\Windows\System32\config



S-1-5-21-1393444541-2628512620-2908104607-1112	C:\Users\Hanii_IT
S-1-5-21-1393444541-2628512620-2908104607-500	C:\Users\Administrator
S-1-5-21-954557100-4256561238-1099421946-1001	C:\Users\Hanii

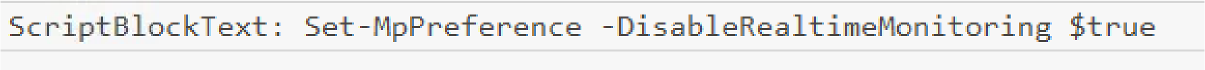
Answer: S-1-5-21-1393444541-2628512620-2908104607-1112

Identifying PowerShell commands reveals attackers' activities such as avoiding detection. What was the first PowerShell command the attacker used for defense evasion?

The Microsoft-Windows-PowerShell%4Operational.evtx file captures executed PowerShell commands and scripts. We can utilise EvtxECmd to parse this file and look at the output in Timeline Explorer:

- .\EvtxECmd.exe -f ".\Microsoft-Windows-PowerShell%4Operational.evtx" --csv . --csvf powershell_out.csv

At 2024-06-30 11:31:44 a PowerShell command was executed to disable Windows Defender real time monitoring:



```
ScriptBlockText: Set-MpPreference -DisableRealtimeMonitoring $true
```

Answer: Set-MpPreference -DisableRealtimeMonitoring $true

We need to find the enumeration output file revealing the network information gathered by the attacker. What is the TXT filename output of one of the network enumeration activities performed by the attacker?

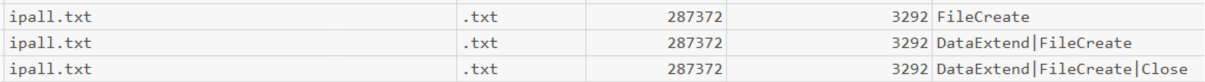
The USN Journal is a forensics artifact that maintains a record of changes made to the NTFS file system. The creation, deletion, or modification of files or directories are journalised/stored here. We can parse this file using MFTECmd and look for file creation events after the initial compromise (i.e., after 2024-06-30 11:26:57). The USN Journal is located at:

- C:\Users\Administrator\Desktop\Start Here\Artifacts\IT-Machine\Evidence-IT\C\$Extend\$J

We can parse this using MFTECmd:

- .\MFTECmd.exe -f ".\` $J" --csv . --csvf usn_journal_out.csv

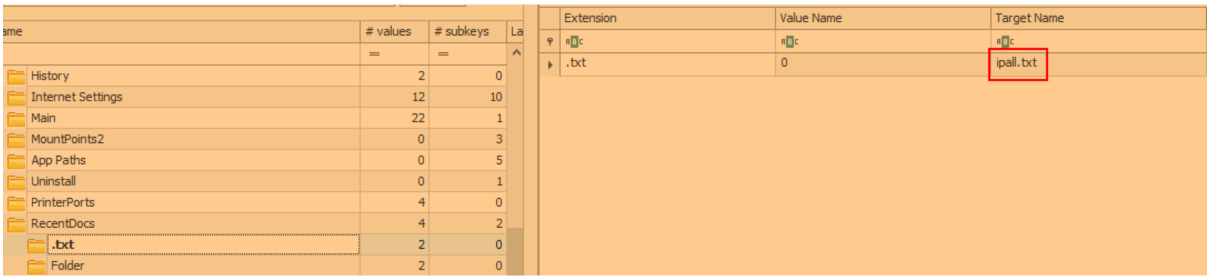
At 2024-06-30 11:34:59 a file called ipall.txt was created:



ipall.txt	.txt	287372	3292	FileCreate
ipall.txt	.txt	287372	3292	DataExtend|FileCreate
ipall.txt	.txt	287372	3292	DataExtend|FileCreate|Close

You can corroborate this by investigating the RecentDocs registry key. You can find the RecentDocs key with the users NTUSER.dat hive. The key is located at:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



ame	# values	# subkeys	La
History	2	0	
Internet Settings	12	10	
Main	22	1	
MountPoints2	0	3	
App Paths	0	5	
Uninstall	0	1	
PrinterPorts	4	0	
RecentDocs	4	2	
.txt	2	0	
Folder	2	0	

Extension	Value Name	Target Name
.txt	0	ipall.txt

As you can see, ipall.txt is found within this key, indicating that this file was opened by the threat actor.

Answer: ipall.txt

Identifying the tools used reveals the methods and scope of network enumeration. After gathering basic information about the network, what third-party tool did the attacker use to identify the file share and perform network enumeration?

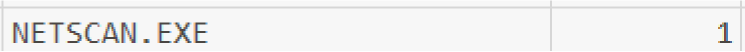
One valuable forensic artifact is the Prefetch, which provides evidence of program execution. The Prefetch files can be found at:

- C:\Users\Administrator\Desktop\Start Here\Artifacts\IT-Machine\Evidence-IT\C\Windows\prefetch

To analyse the Prefetch directory, we can use a tool called PECmd:

- .\PECmd.exe -d "C:\Users\Administrator\Desktop\Start Here\Artifacts\IT-Machine\Evidence-IT\C\Windows\prefetch" --csv . --csvf prefetch_out.csv

Analysis reveals that at 2024-06-30 11:35:08 netscan.exe was executed:



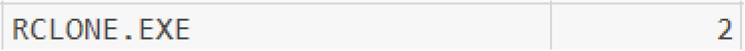
NETSCAN.EXE	1

NetScan is a tool frequently employed by threat actors for network scanning and enumeration.

Answer: netscan

Knowing the tool used for data exfiltration helps in identifying the methods and channels used by the attacker to exfiltrate sensitive data. What command-line tool did the attacker use to attempt data exfiltration?

Further examination of the Prefetch output reveals that at 2024-06-30 11:39:01, rclone.exe was executed:



RCLONE.EXE	2

Rclone is a widely used command-line tool for transferring data to cloud storage, it is often abused by threat actors for exfiltrating data to their own cloud storage.

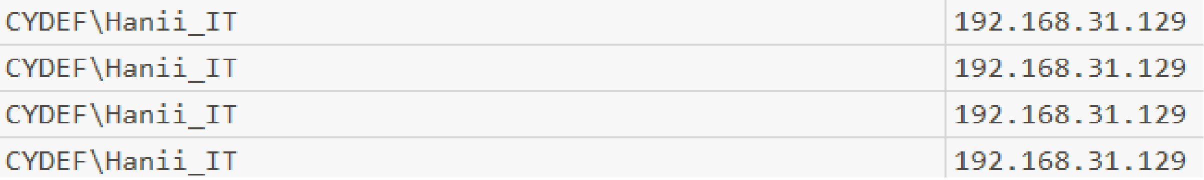
Answer: rclone

Identifying the IP addresses of the machines involved in lateral movement helps map the attacker's path and understand the attack's scope. Can you provide the IP address of the machine to which the attacker moved laterally and the IP address of the initial access machine?

Let's review Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx logs from the file server, focusing on Event ID 24 (RDP session connections). We can use EvtxECmd to parse this log file:

- .\EvtxECmd.exe -f ".\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx" --csv . --csvf local_session_manager.csv

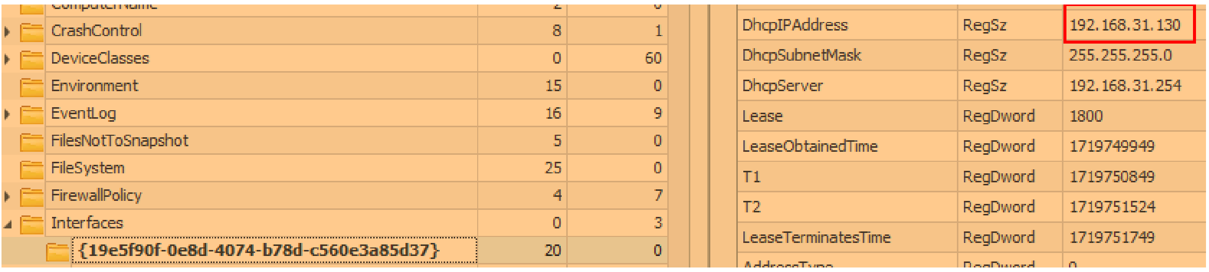
We can observe that the compromised system (IP: 192.168.31.129, username: Hanii_IT) established an RDP connection to the file server at 2024-06-29 16:33:45:



CYDEF\Hanii_IT	192.168.31.129
CYDEF\Hanii_IT	192.168.31.129
CYDEF\Hanii_IT	192.168.31.129
CYDEF\Hanii_IT	192.168.31.129

To determine the IP address of the file server, we need to load the SYSTEM hive and navigate to:

- SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces



ComputerName	2	0
CrashControl	8	1
DeviceClasses	0	60
Environment	15	0
EventLog	16	9
FilesNotToSnapshot	5	0
FileSystem	25	0
FirewallPolicy	4	7
Interfaces	0	3
{19e5f90f-0e8d-4074-b78d-c560e3a85d37}	20	0

DhcpIPAddress	RegSz	192.168.31.130
DhcpSubnetMask	RegSz	255.255.255.0
DhcpServer	RegSz	192.168.31.254
Lease	RegDword	1800
LeaseObtainedTime	RegDword	1719749949
T1	RegDword	1719750849
T2	RegDword	1719751524
LeaseTerminatesTime	RegDword	1719751749
AddressType	RegDword	0

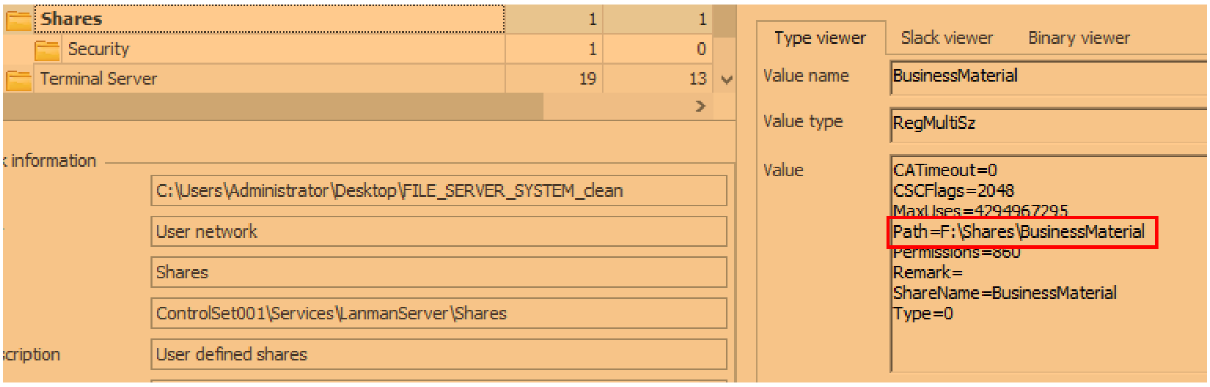
The file server has been assigned the IP 192.168.31.130 as observed in the above image.

Answer: 192.168.31.130, 192.168.31.129

Knowing the path of the file share targeted by the attacker helps in identifying compromised data and understanding the attack's impact. What is the full path of the file share on the file server that was targeted by the attacker?

To find the file shares on the file server, we can load the SYSTEM registry hive and navigate to:

- SYSTEM\CurrentControlSet\Services\LanmanServer\Shares



Shares	1	1
Security	1	0
Terminal Server	19	13

information

C:\Users\Administrator\Desktop\FILE_SERVER_SYSTEM_clean

User network

Shares

ControlSet001\Services\LanmanServer\Shares

cription: User defined shares

Value name: BusinessMaterial

Value type: RegMultiSz

Value:

```
CATimeout=0
CSCFlags=2048
MaxUses=4294967295
Path=F:\Shares\BusinessMaterial
Permissions=860
Remark=
ShareName=BusinessMaterial
Type=0
```

Answer: F:\Shares\BusinessMaterial

Identifying the SHA1 file hash of the malware helps in verifying the exact malicious file and correlating it with known malware signatures. What is the SHA1 file hash of the ransomware run on the file server and IT-machine?

The AmCache registry hive logs program execution details such as the file path, execution timestamp, SHA1 hash, and more. It is located at:

- C:\Windows\appcompat\Programs\Amcache.hve

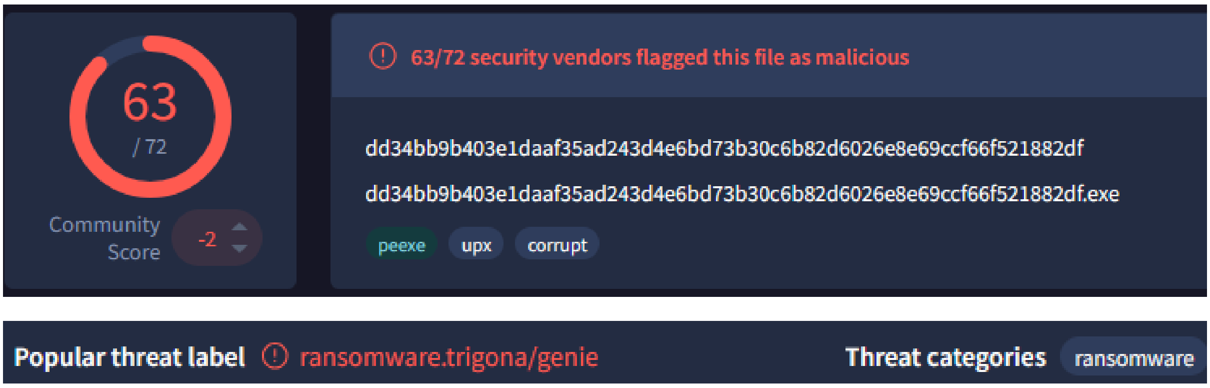
To parse this hive, we can use a tool called AmcacheParser

- .\AmcacheParser.exe -f ".\Amcache.hve" --csv amcache

Prior to rclone being executed, a suspicious binary named final.exe was executed out of the tools\execute directory:

```
c:\users\hanii_it\desktop\tools\execute\final.exe
c:\users\hanii_it\desktop\tools\out\rclone.exe
```

When the SHA1 hash of this binary was submitted to VirusTotal, it shows 63/72 detections and was flagged as ransomware:



63/72 security vendors flagged this file as malicious

dd34bb9b403e1daaf35ad243d4e6bd73b30c6b82d6026e8e69ccf66f521882df

dd34bb9b403e1daaf35ad243d4e6bd73b30c6b82d6026e8e69ccf66f521882df.exe

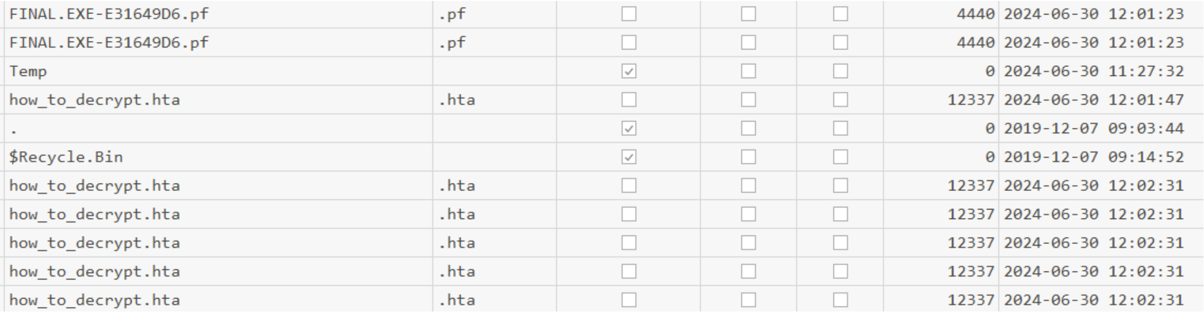
Popular threat label: ransomware.trigona/genie

Threat categories: ransomware

Answer: cfaa59dd3288387f62efbf54477d531f4d3964f3

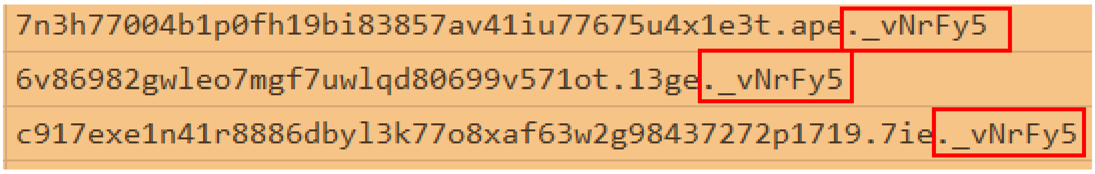
Knowing the extension of encrypted files can potentially help us with identifying the ransomware variant. What is the file extension of the encrypted files?

The ransomware binary final.exe was executed at 2024-06-30 12:01:12. By reviewing MFT activity after this timestamp, we can spot unusual changes in filenames:



FINAL.EXE-E31649D6.pf	.pf	□	□	□	4440	2024-06-30 12:01:23
FINAL.EXE-E31649D6.pf	.pf	□	□	□	4440	2024-06-30 12:01:23
Temp		☑	□	□	0	2024-06-30 11:27:32
how_to_decrypt.hta	.hta	□	□	□	12337	2024-06-30 12:01:47
.		☑	□	□	0	2019-12-07 09:03:44
$Recycle.Bin		☑	□	□	0	2019-12-07 09:14:52
how_to_decrypt.hta	.hta	□	□	□	12337	2024-06-30 12:02:31
how_to_decrypt.hta	.hta	□	□	□	12337	2024-06-30 12:02:31
how_to_decrypt.hta	.hta	□	□	□	12337	2024-06-30 12:02:31
how_to_decrypt.hta	.hta	□	□	□	12337	2024-06-30 12:02:31
how_to_decrypt.hta	.hta	□	□	□	12337	2024-06-30 12:02:31

In the image above, we can observe activity likely indicating that the ransomware has started to encrypt files (as evident by the existence of how_to_decrypt.hta files). Soon after, we can see files being appended with _vNrFy5:



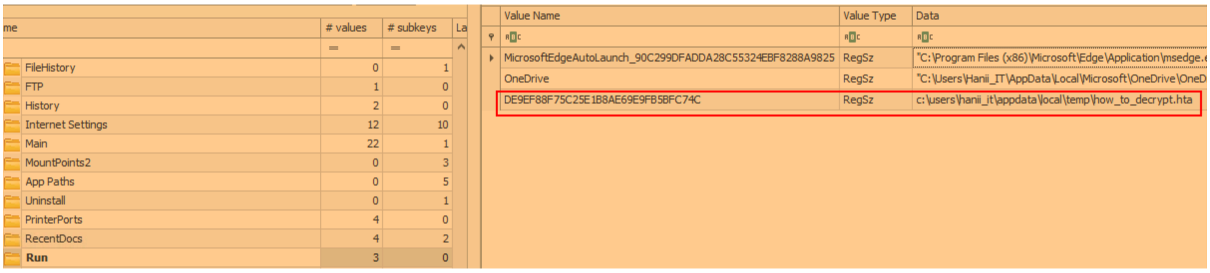
```
7n3h77004b1p0fh19bi83857av41iu77675u4x1e3t.ape._vNrFy5
6v86982gwleo7mgf7uwlqd80699v571ot.13ge._vNrFy5
c917exe1n41r8886dbyl3k77o8xaf63w2g98437272p1719.7ie._vNrFy5
```

Answer: _vNrFy5

Determining the registry modifications by the malware is crucial for identifying its malicious activities. What registry value did the malware add to display its ransom message?

A common technique for persistence is using Run keys, which automatically execute specified programs at user login. In this case, the relevant key is found at:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



me	# values	# subkeys
FileHistory	0	1
FTP	1	0
History	2	0
Internet Settings	12	10
Main	22	1
MountPoints2	0	3
App Paths	0	5
Uninstall	0	1
PrinterPorts	4	0
RecentDocs	4	2
Run	3	0

Value Name	Value Type	Data
MicrosoftEdgeAutoLaunch_90C299DFADDA28C55324EBF8288A9825	RegSz	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.
OneDrive	RegSz	"C:\Users\Hanii_IT\AppData\Local\Microsoft\OneDrive\OneD
DE9EF88F75C25E1B8AE69E9FB5BFC74C	RegSz	c:\users\hanii_it\appdata\local\temp\how_to_decrypt.hta

Answer: c:\users\hanii_it\appdata\local\temp\how_to_decrypt.hta