Deep Dive Into Ryuk Ransomware

medium.com/ax1al/reversing-ryuk-eef8ffd55f12

astro November 18, 2020

Published in

Ax1al

astro

Nov 14, 2020

·

6 min read

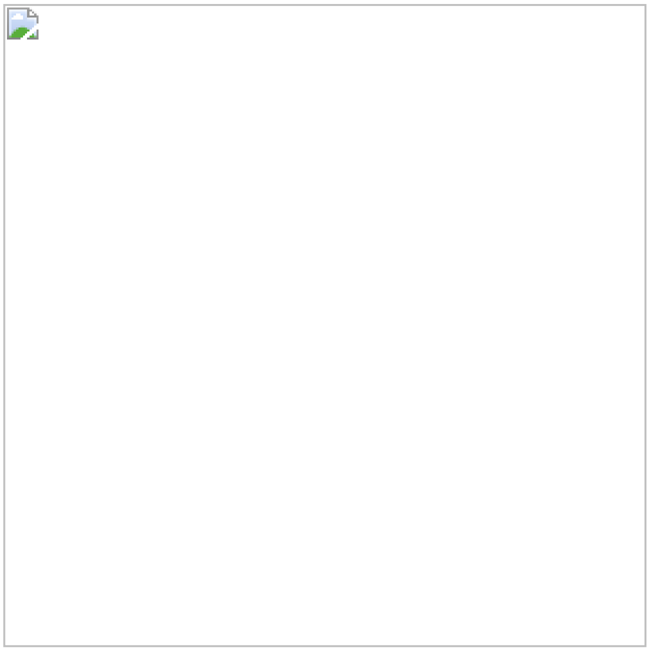
Hello World, This Will Probably be My First Malware Report Where I will Reverse Ryuk Ransomware. So Before Getting into Technical Analysis and Reverse Engineering I will Provide Some Introduction to Ryuk. So let’s First Discuss the CyberKillChain of Ryuk it goes typically like this:

1- An maldoc Contains a malicious macro that will execute PowerShell.
2- The PowerShell Command then Downloads Emotet Banking Trojan.
3- Emotet Then Downloads TrickBot
4- As A Typical Lateral Movement Activity TrickBot Downloads Ryuk
5- Ryuk Then Tries to Encrypt all the Network Hosts

However in new samples it uses BazarLoader and Cobalt Strike and it goes like this. Here I analyzed a sample not old its from 2020 but that’s because I analyzed this sample before ryuk last attack occurred.

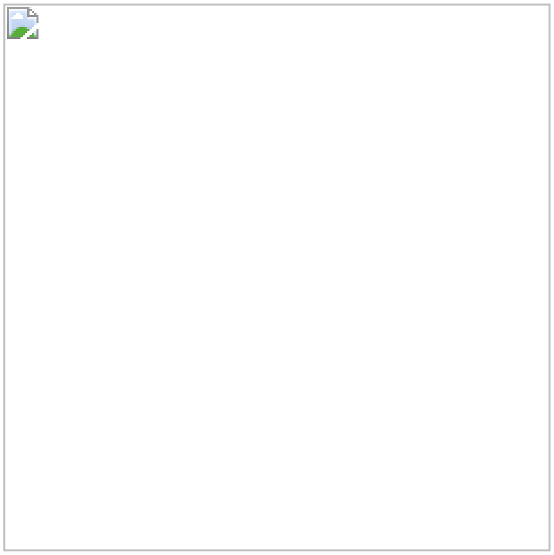
Who Created It ?

So Attribution is Hard However From What I have Read Threat Intel Researches Suggest that it belongs to the Authors of HERMES which is a Ransomware first was detected in October 2017 was then arrtributed to an APT Group Called Lazarus Group.

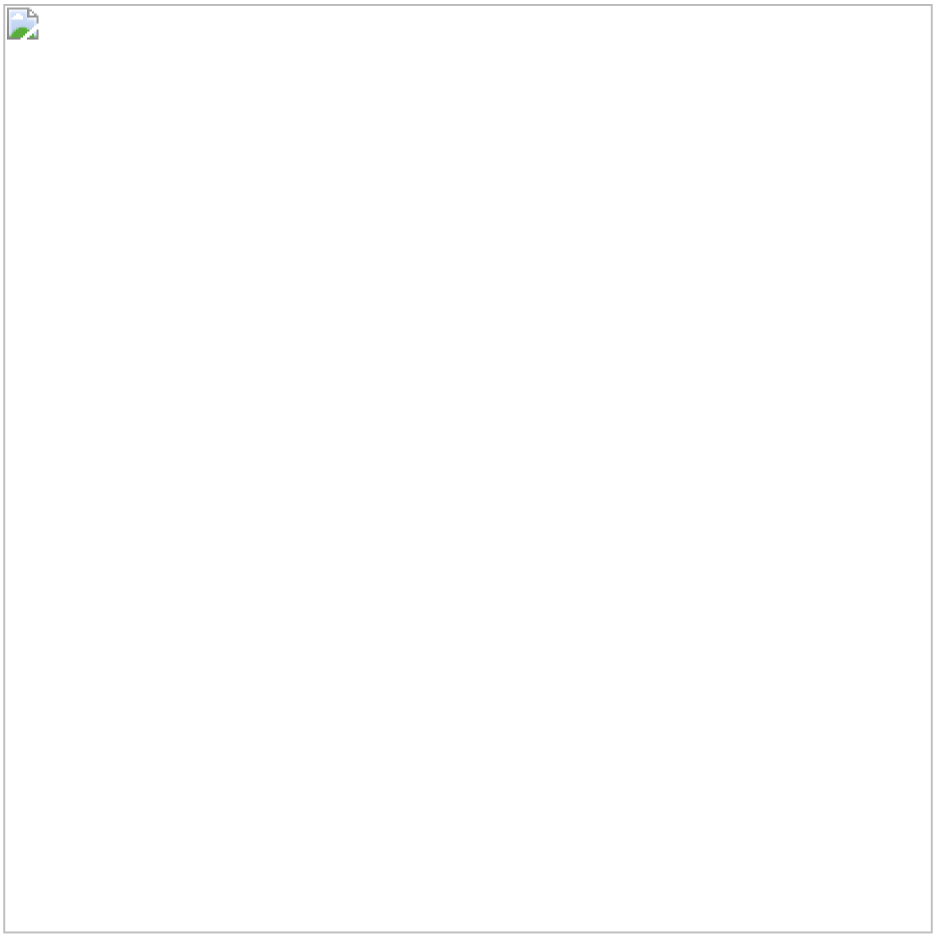


In Depth Reversing:

- I Used a Combination of Cutter, IDA and x64 dbg to reverse this malware so nvm xD
- When Executing the Sample It Drops a Copy From its Self and Execute it using “8 lan” Command.

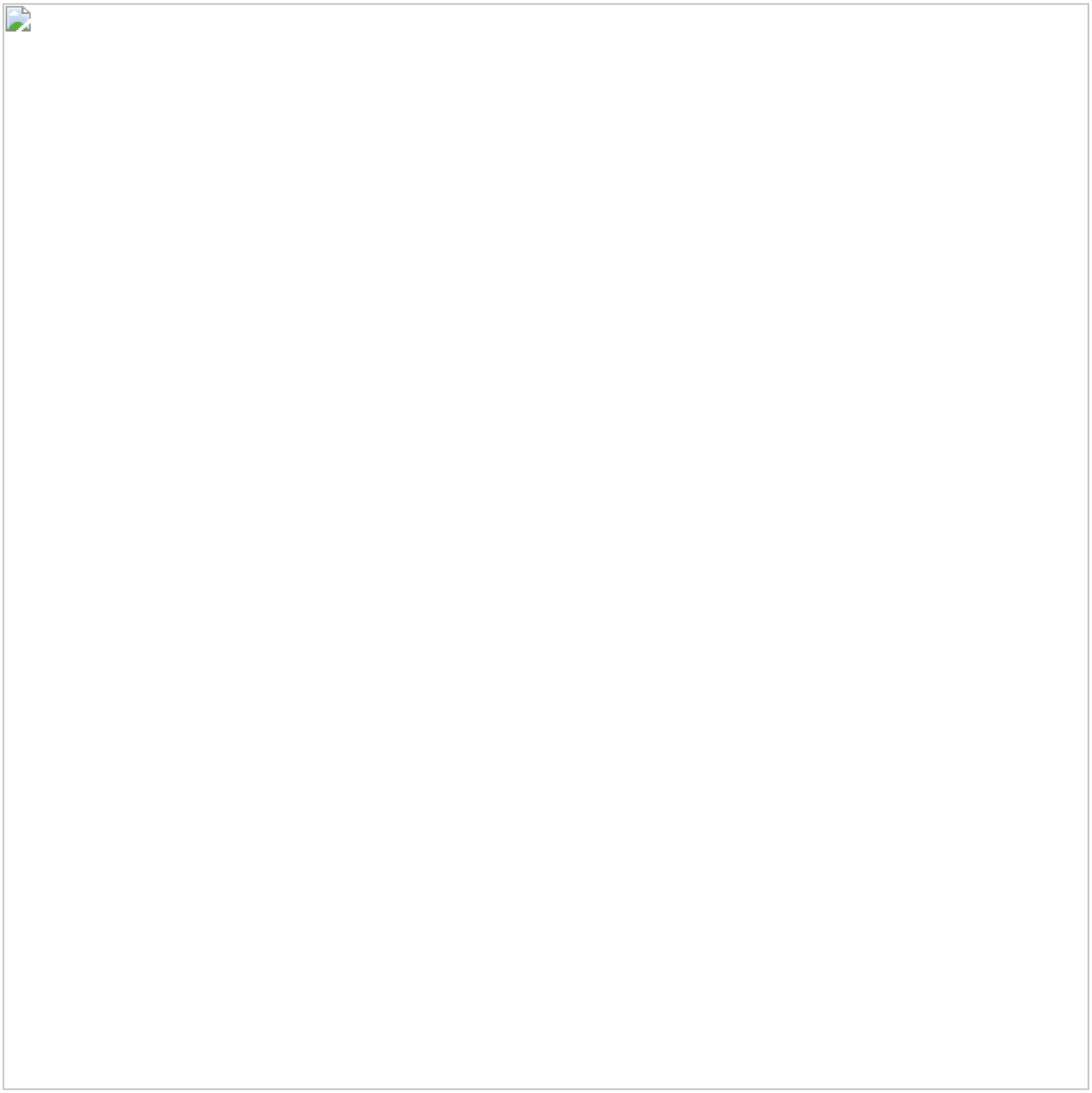


By Static Code Analysis it Concats “.exe” to the name of the dropped file and executes it using ShellExecute passing a param “8 lan” to it. this command is a hardware feauture called WoL (Wakeup On Lan) which allow a computer to turned on by a network message. it works on a lan network. the way its executed is by the program for our case its ryuk sends a message to all the devices on the same lan.



- The Name of the Dropped Exe are Seven Random Characters.
- The Malware Injects Into 4 Process taskeng.exe, host.exe, dwm.exe, ctfmon.exe
- It Encrypts the Files using “RYK” Extension
- The Malware Deletes Shadow Copies Using:

```
[+] cmd /c "WMIC.exe shadowcopy delet
[+] vssadmin.exe Delete Shadows /all /quiet
```

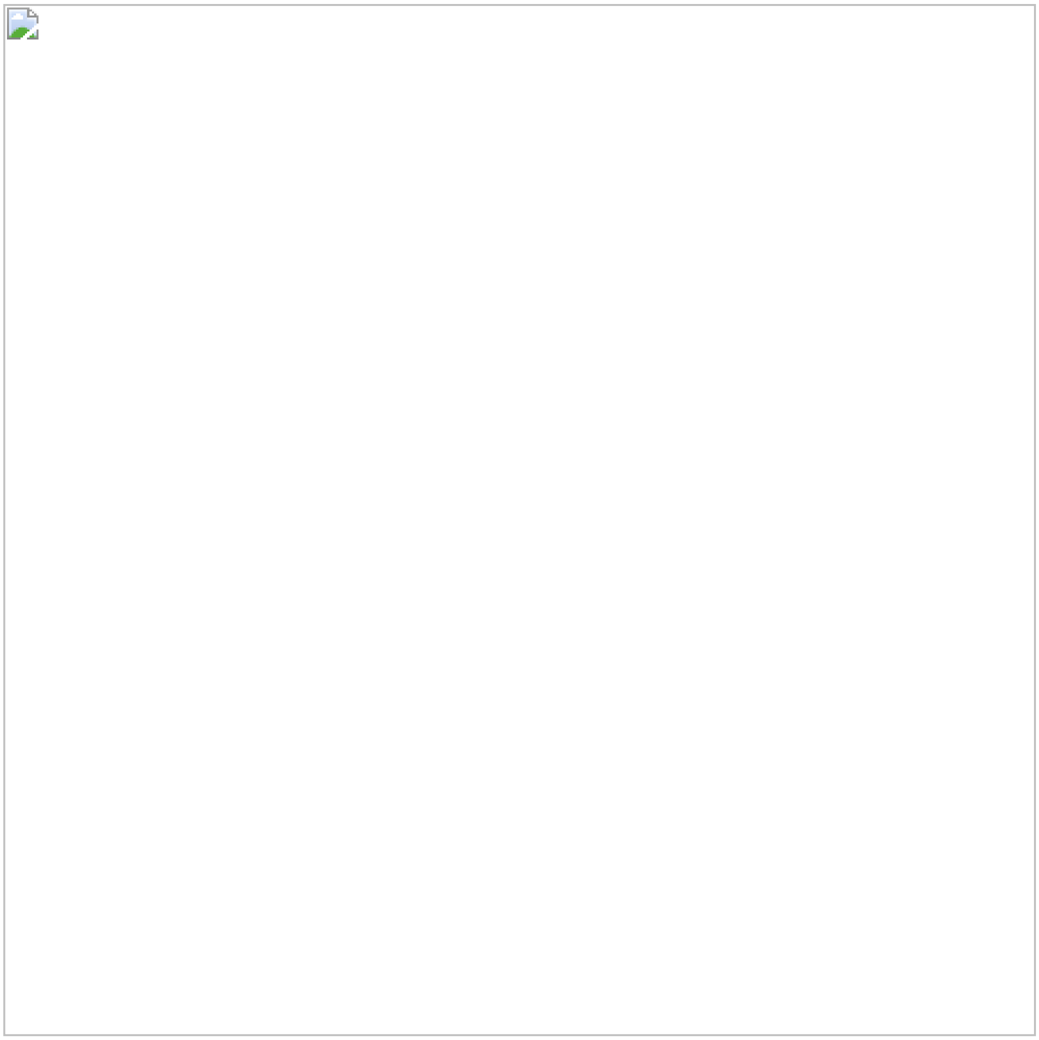


As You Can See a Typo Found in the First Command The Author Missed ‘e’ in delete.

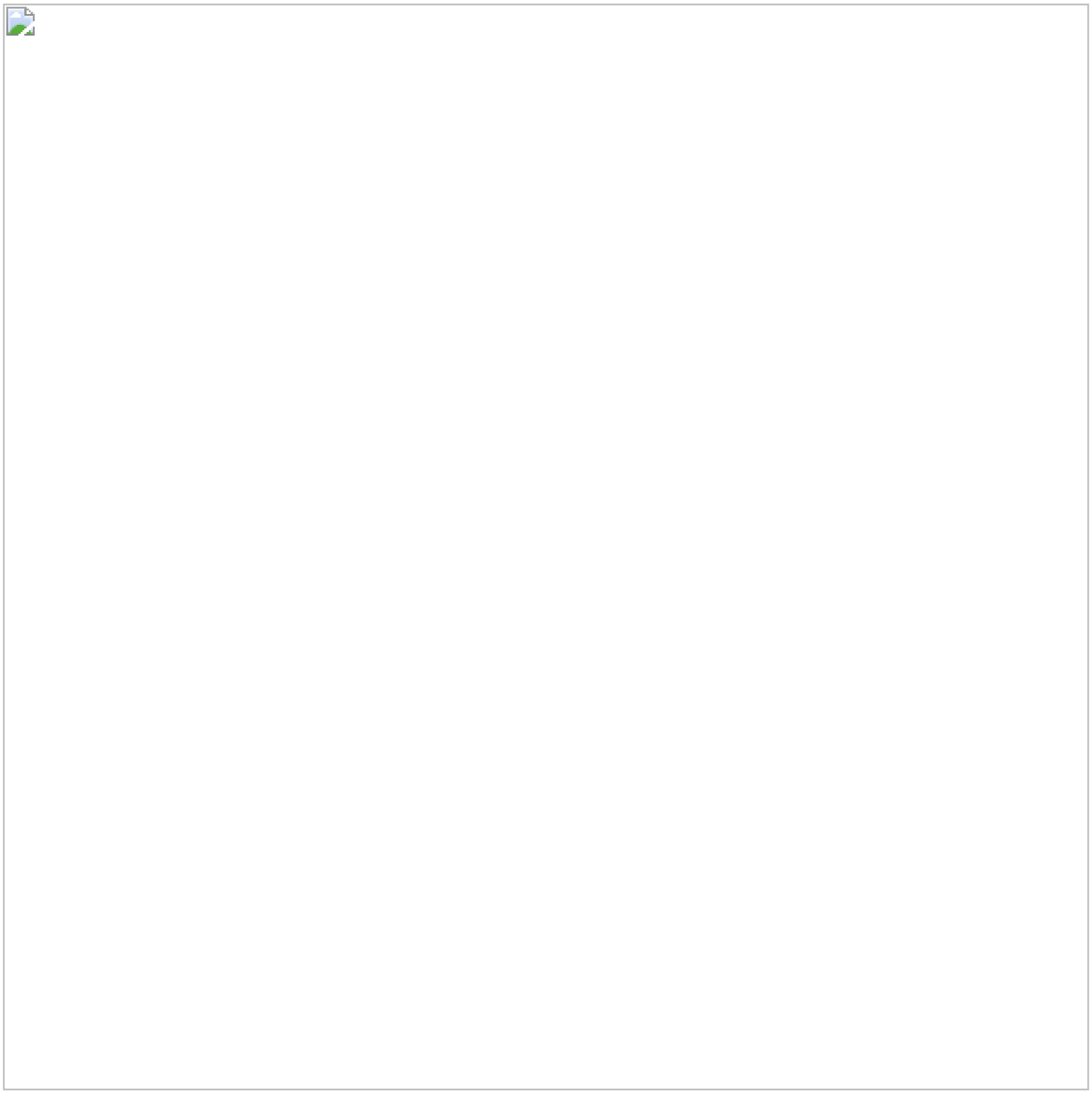
API Resolving:

Ryuk Uses GetProcAddress and LoadLibraryA to Resolve Its APIs

And By Using the Debugger:

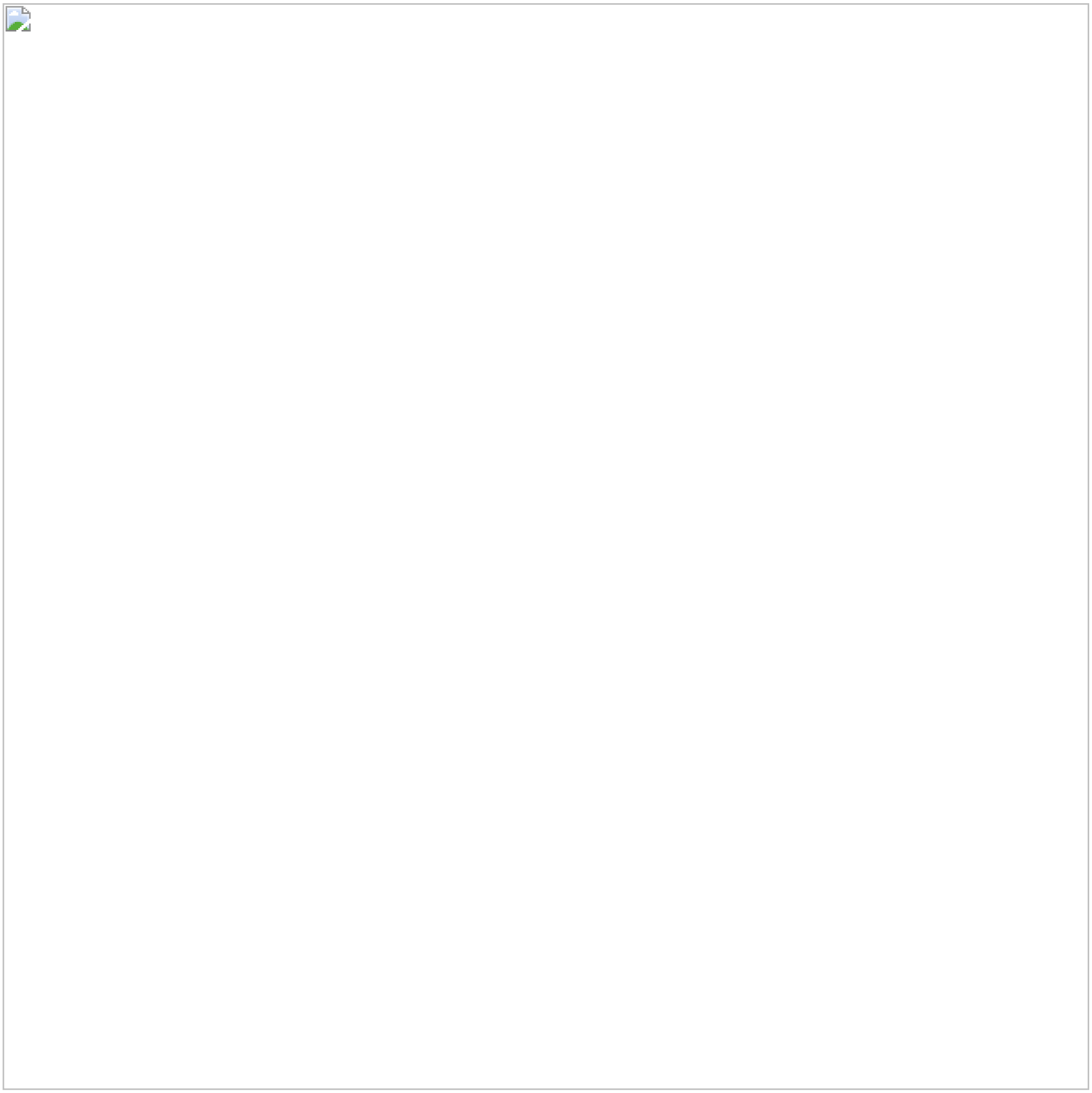


Due to That I don’t Know Emulation or Scripting + Scylla Didn’t Dump the process correctly I managed to rename them manually :) here is the result:



Privilege Escalation:

Ryuk Escalates Privilege by Modifying the Access Token



According to MSDN The LookupPrivilegeValue function retrieves the locally unique identifier (LUID) used on a specified system to locally represent the specified privilege name. It Takes 3 Parameters lpSystemName, lpName, lpLuid. What We Care About is the Second Here the Second Param is The Name of The Privilege Looked up In this Case its “ “SeDebugPrivilege” this is used to inspect and Modify the memory of other process. This Will Be Used For Process Injection.

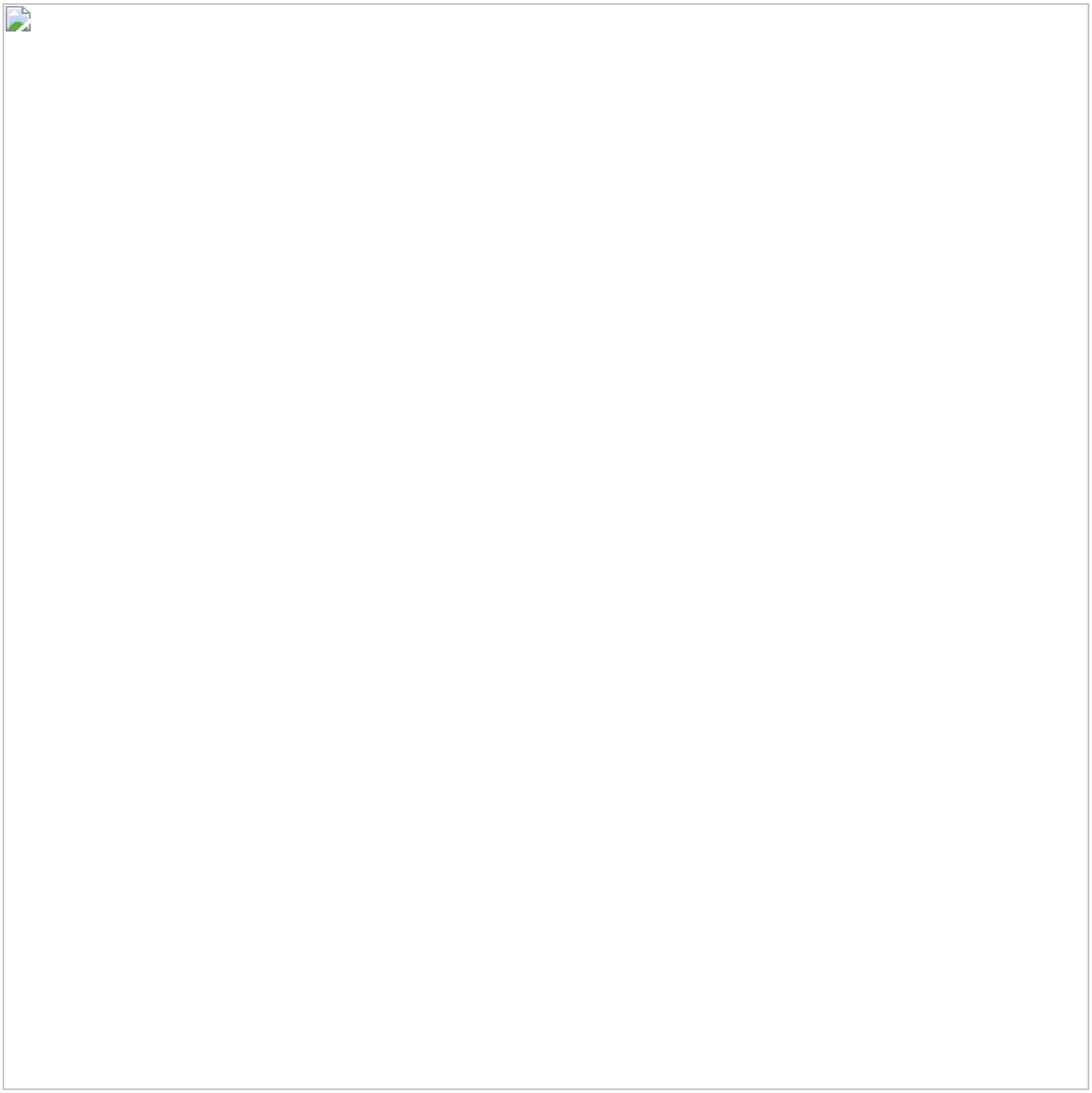
Persistence:

Ryuk Acheives Persistence by Adding the Path of the malware under /Run Key In the Registry Makes it Run Every Time the User logs In It uses this Command

```
[+] "C:\Windows\System32\cmd.exe" REG ADD
"HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos" /t REG_SZ
/d "C:\Users\admin\AppData\Local\Temp\860e50.exe" /f
```

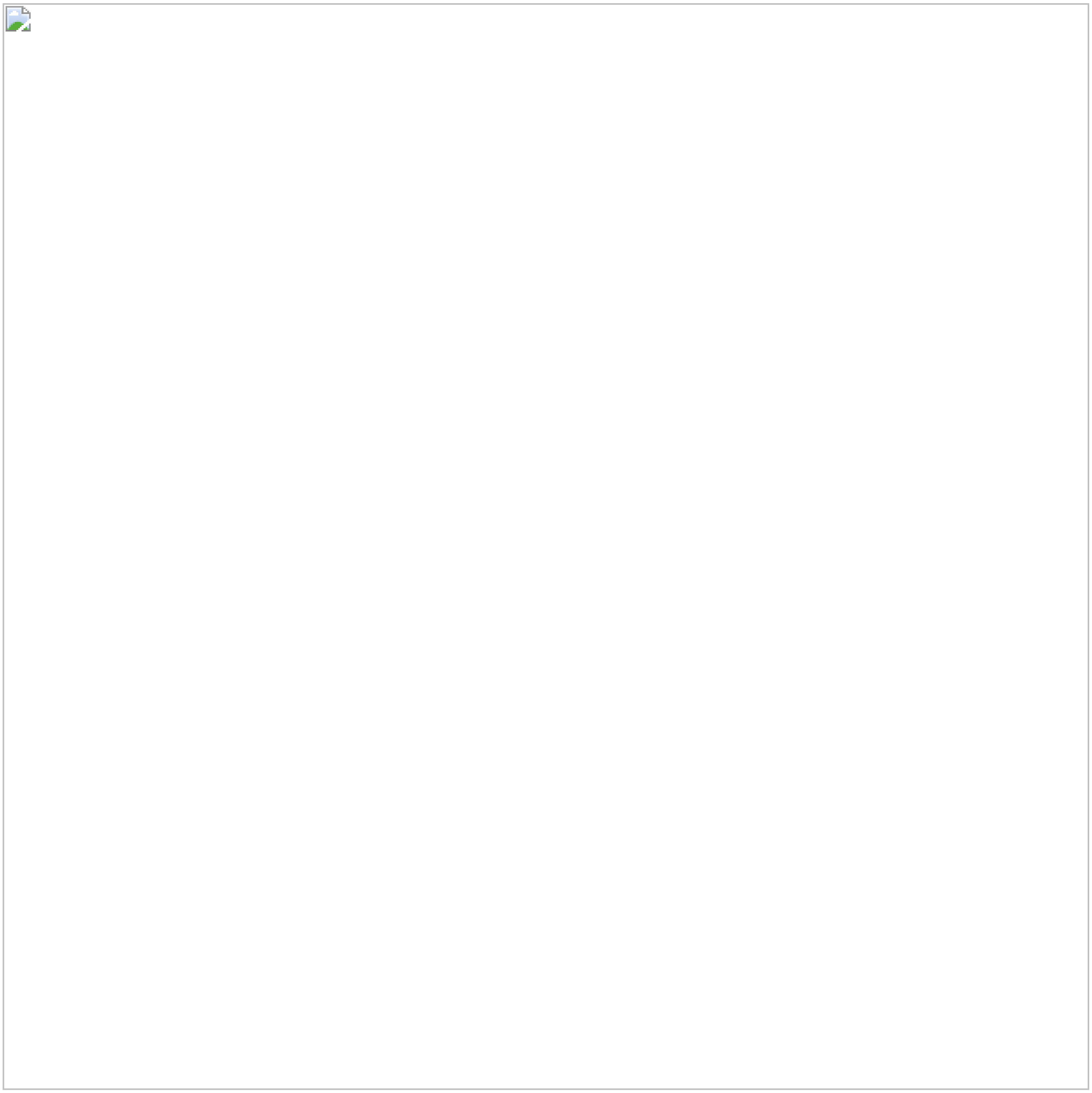
Process Injection:

First It Opens a Process



Then It Allocates Memory in the Target Process

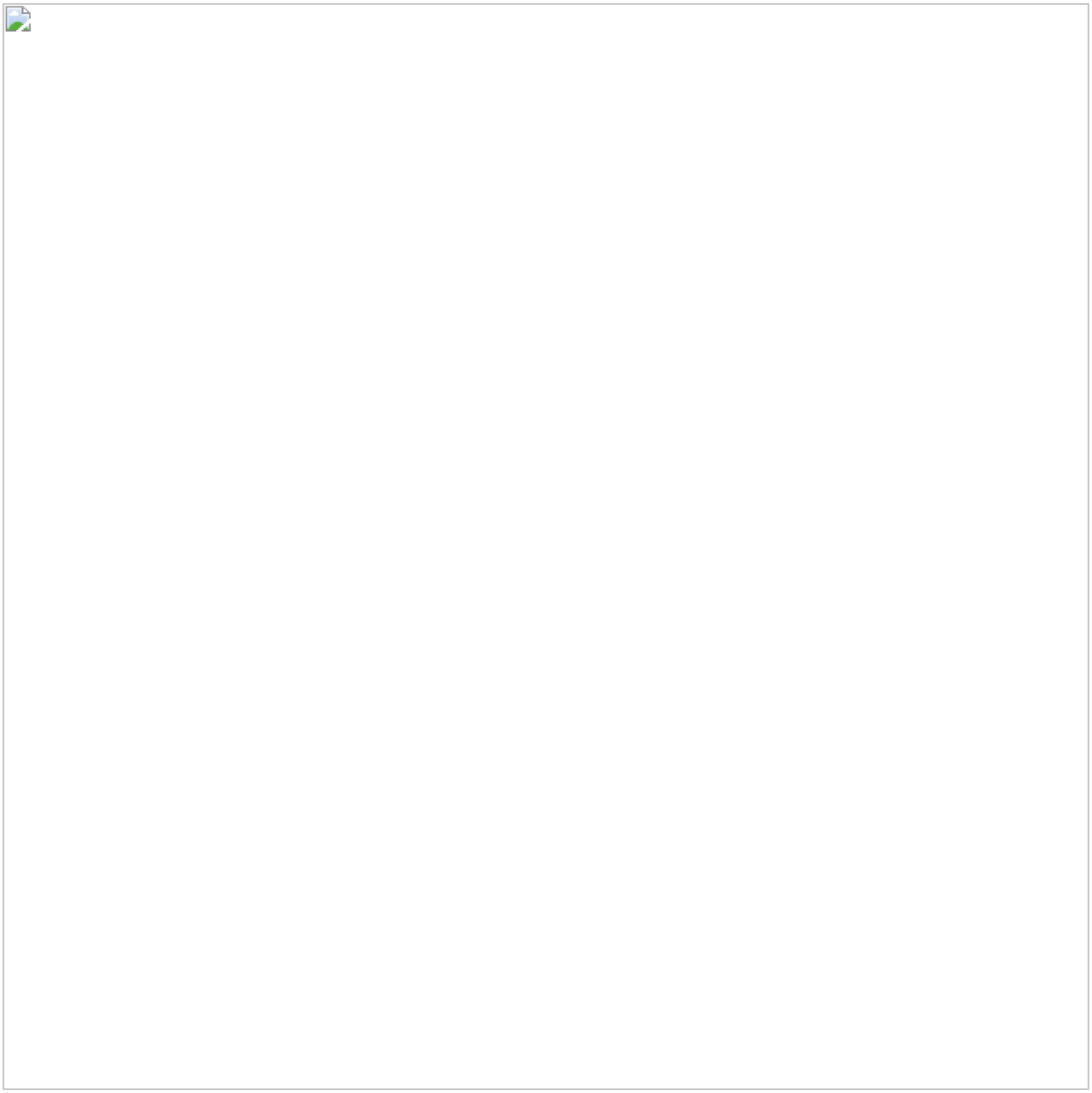
Next it Writes injects its Self using WriteProcessMemory and Creates a Thread to run the injected code



Following with the debugger we can see the exectuable in the memory dump

Encryption:

Ryuk Uses AES-256 Encryption it utilizes the CryptoAPI by Microsoft. It Encrypts the Files using “.RYK” Extension. The AES Key is Encrypted using a Public RSA Key.

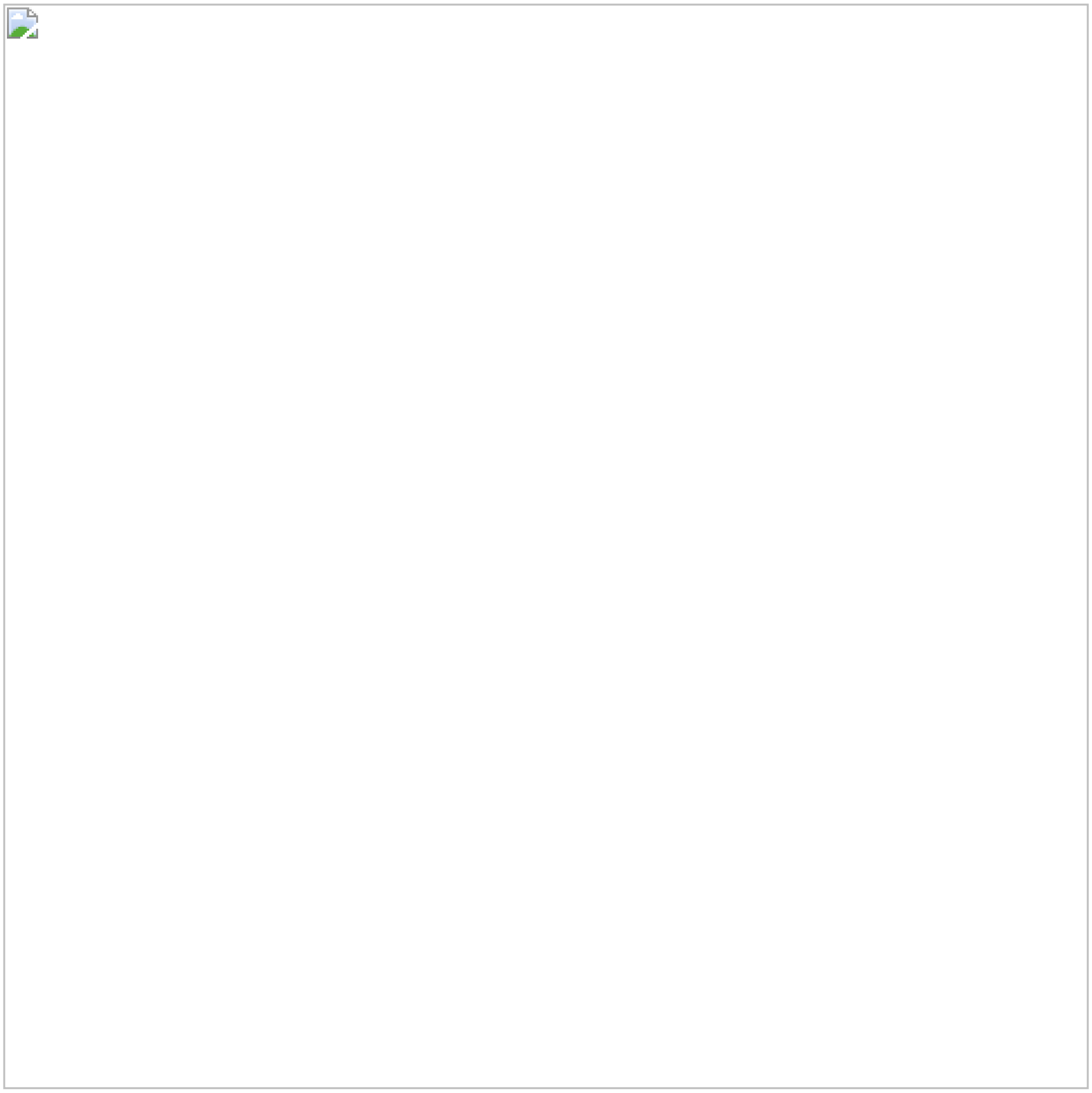


It uses a Marker “HERMES” to identify if the file is encrypted or not.

Its Uses:

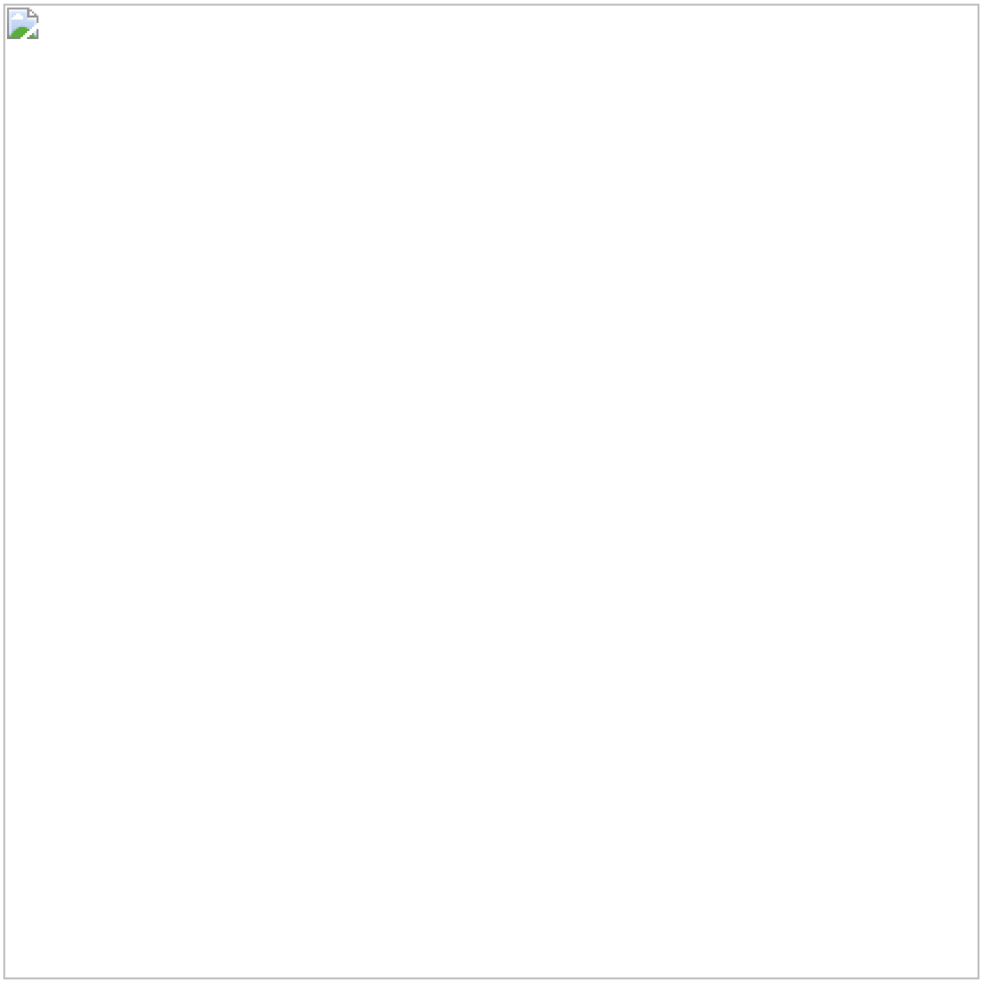
```
[+] CryptEncrypt
[+] CryptGenKey
[+] CryptDecrypt
[+] CryptAquireContextW
[+] CryptDestroyKey
[+] CryptDeriveKey
[+] CryptImportKey
```

Ryuk Uses MultiThreaded Approach to Encrypt the files which means it makes a thread per file which makes it very fast. It loops Through the Files using FindFirstFileA and FindNextFileA. It Avoid Encrypting Some Files



Here is a List of Them:

```
[+] RyukReadMe.html
[+] UNIQUE_ID_DO_NOT_REMOVE
[+] boot
[+] PUBLIC
[+] PRIVATE
[+] \Windows\
[+] sysvol
[+] netlogon
[+] bin
[+] Boot
[+] dev
[+] etc
[+] lib
[+] initrd
[+] sbin
[+] sys
[+] vmlinux
[+] run
[+] var
[+] dll
[+] lnk
[+] hrmlog
[+] ini
[+] exe
```

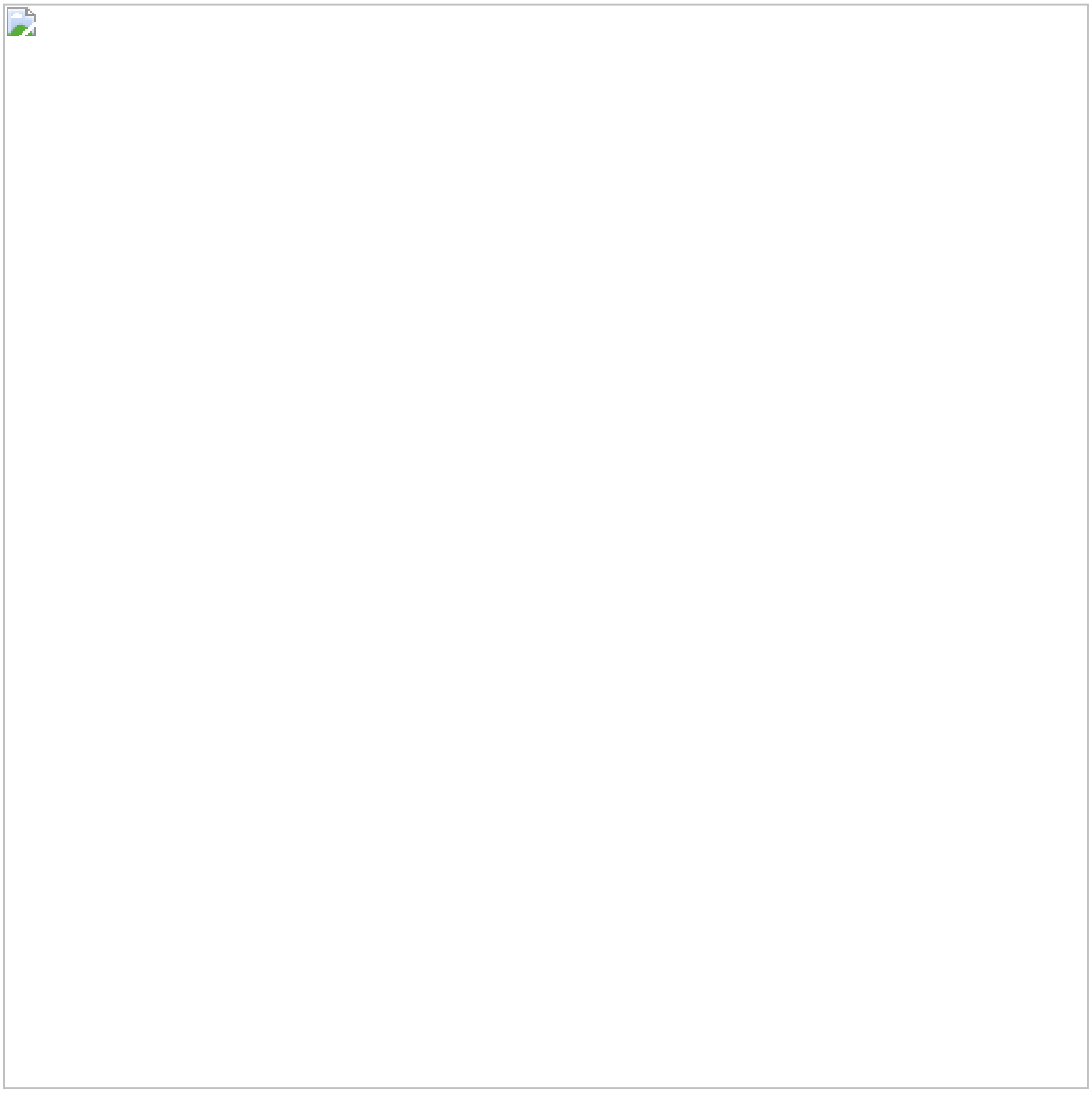


Here it builds Strings on stack for folders to avoid encrypting its files or skipping it

```
[+] Ahnlab
[+] Chrome
[+] Mozilla
[+] Windows
[+] $Recycle.bin
```

Relation to HERMES:

There is two Assumptions One is that that Who Wrote Ryuk was the same who wrote HERMES or just that Ryuk Author was having HERMES Source code. The Encryption Logic is Same as HERMES. As We Saw Ryuk Uses AES-256 and Encrypts the KEY using RSA and that is the same in HERMES. Also Checking the Code the Author Didn’t Change the marker of the encrypted files. This Marker is used to check if the file was encrypted or not. Also HERMES Uses the Same Batch Script used to delete the shadows copies. Even the files/folders that are skipped are the same.



Yara Rule:

You Can Find My YARA Rule Here Ryuk

IOCS:

```
SHA256:40b865d1c3ab1b8544bcf57c88edd30679870d40b27d62feb237a19f0c5f9cd1
SHA1: AD11ED52AB33AD05EB9B1E9ADE134CA1348ACC81
MD5: 484a2bcb1335ac97ee91194f4c0964bc
```

TTP’s:

[+] Command-Line Interface T1059

[+] Execution through API T1106

[+] Service Execution T1035

[+] Registry Run Keys / Startup Folder T1060

[+] Process Injection T1055

[+] Disabling Security Tools T1089

[+] File Permissions Modification T1222

[+] Modify Registry T1112

[+] Process Injection T1055

[+] Query Registry T1012

[+] System Service Discovery T1007

[+] Inhibit System Recovery T1490

[+] Access Token Manipulation T1134

[+] Process Discovery T1057

[+] Service Stop T1489

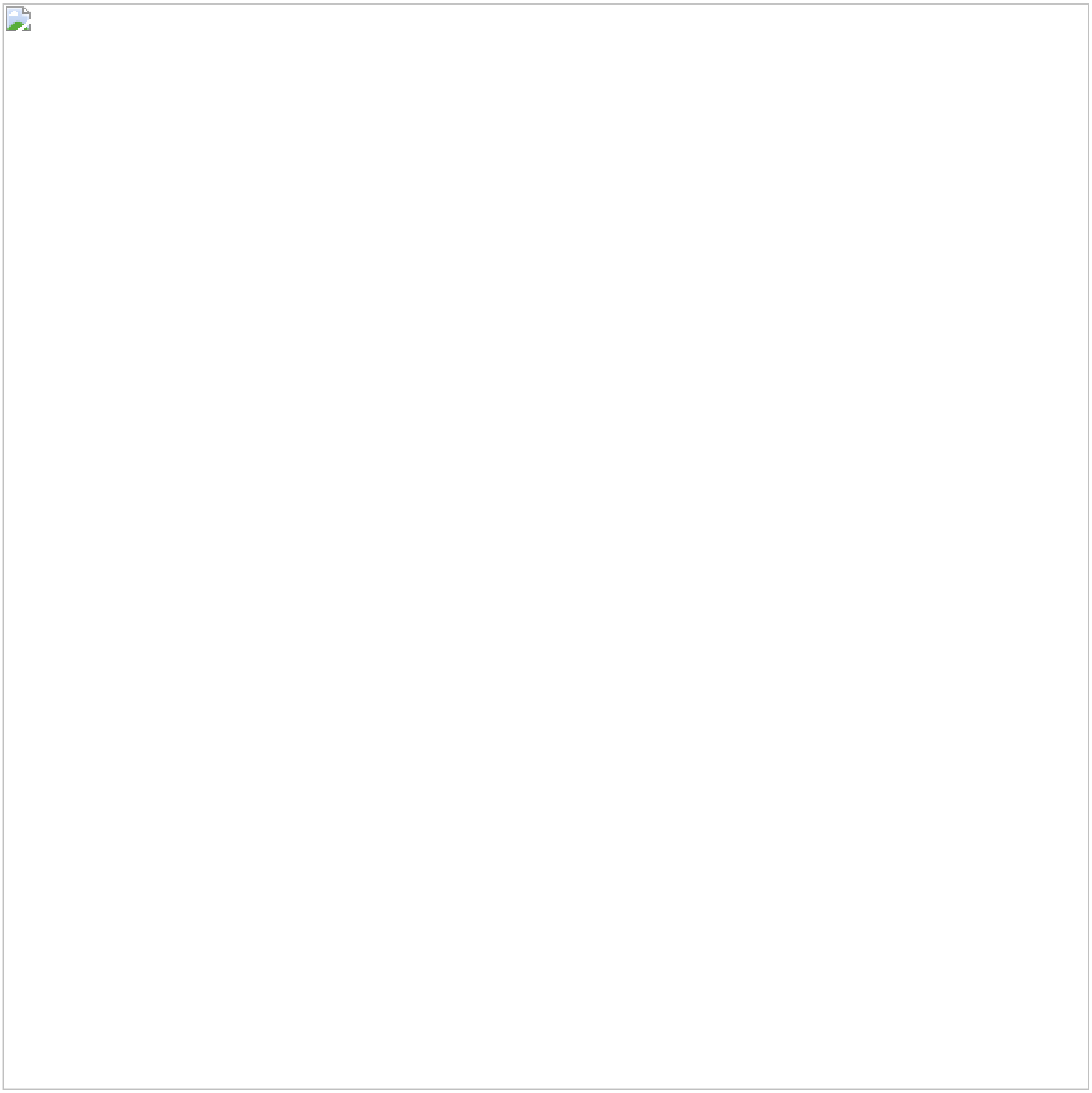
[+] Impair Defenses: Disable or Modify Tools T1562

[+] Data Encrypted for Impact T1486

List of The Commands Executed:

```
[+] cmd /c \"WMIC.exe shadowcopy delet\[+] icacls "C:\*" /grant Everyone:F /T /C /Q[+]
vssadmin.exe Delete Shadows /all /quiet[+] bcdedit /set {default} recoveryenabled No &
bcdedit /set {default}[+] bootstatuspolicy ignoreallfailures[+]
"C:\Windows\System32\net.exe" stop "audioendpointbuilder" /y[+] C:\Windows\system32\net1
stop "audioendpointbuilder" /y[+] "C:\Windows\System32\net.exe" stop "samss" /y[+]
C:\Windows\system32\net1 stop "samss" /y[+] REG  ADD
"HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos" /t REG_SZ
/d "C:\Users\admin\AppData\Local\Temp\USvoLou.exe" /f[+] "C:\Windows\System32\cmd.exe"
/C REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos"
/t REG_SZ /d
    "C:\Users\admin\AppData\Local\Temp\USvoLou.exe" /f[+] /C REG DELETE
"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run" /v "svchos" /f
```

RansomNote:



Refrences:

https://n1ght-w0lf.github.io/malware%20analysis/ryuk-ransomware/

https://www.fortinet.com/blog/threat-research/ryuk-revisited-analysis-of-recent-ryuk-attack

https://research.checkpoint.com/2018/ryuk-ransomware-targeted-campaign-break/

https://blog.malwarebytes.com/threat-analysis/2018/03/hermes-ransomware-distributed-to-south-koreans-via-recent-flash-zero-day/

https://app.any.run/tasks/152b6f3a-d6c9-418a-9d0d-3654e26d3117

GoodBye!

So That’s It Hope You Enjoy It I am a N00b so my mistakes are alot xD so if u have any suggestions for me feel free to dm on twitter @astrovax

--

More from Ax1al

A community for the nerds by the nerds related to:Reverse Engineering, Malware analysis, Web security, CTFs & various other domains of security research.

Read more from Ax1al

Recommended from Medium

Emmalynne Ankney

{UPDATE} Gin Rummy Master Hack Free Resources Generator

Lynn Joed

{UPDATE} Crossword. The smart puzzle game. Hack Free Resources Generator

Fancy McNair

{UPDATE} True or False Hack Free Resources Generator