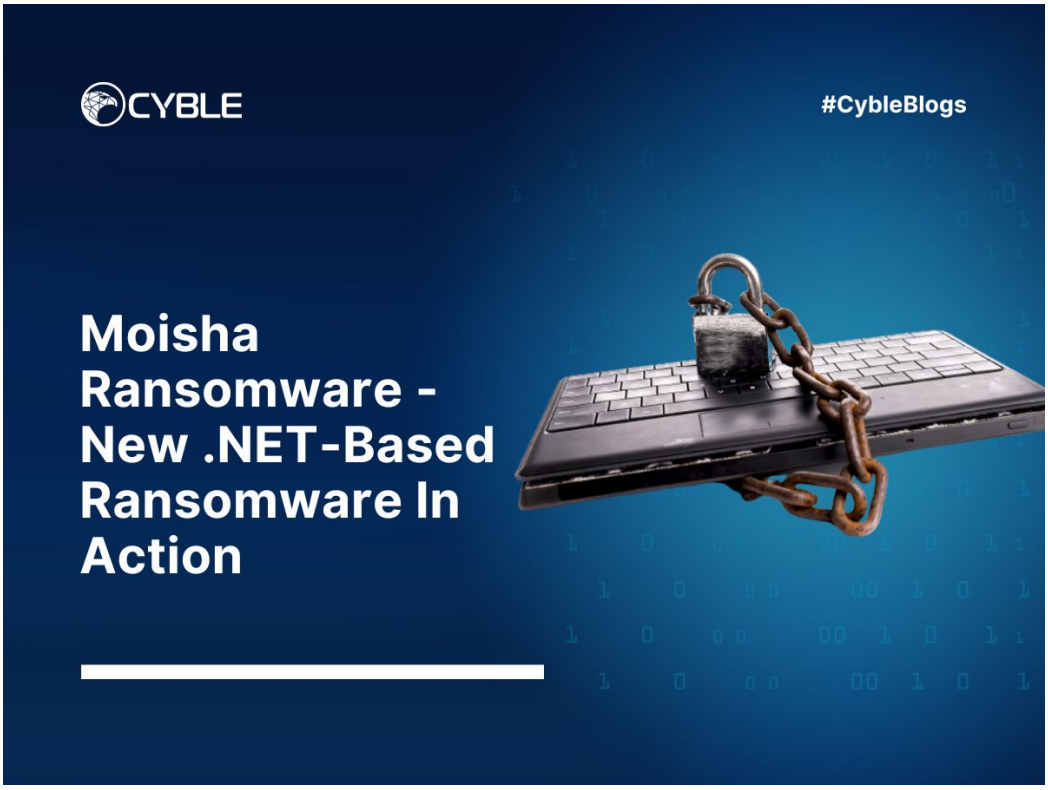
Moisha Ransomware In Action

8/25/2022



New .NET-Based Ransomware Performs Targeted Attack

Several organizations, big or small, have been facing threats from Threat Actors (TAs) at a greater frequency than ever before. An organization's primary danger remains losing access to their systems and data, which is further aggravated by the threat of TAs leaking the data if ransom requests are not fulfilled or the victim reaches out to law enforcement authorities.

Cyble Research Labs (CRL) has consistently analyzed and published information about the most prominent and active ransomware groups in the past and provided recommendations to prevent such incidents in the future. Recently, during our routine threat-hunting exercise, we came across a Twitter post about a new ransomware variant named "Moisha". A .Net-based ransomware, Moisha was first identified in mid-August 2022, and the name of the TA is PT_MOISHA team.

While executing the sample, we observed that the ransom note contains the name of an organization, indicating that the ransomware may have been developed as part of a highly targeted attack. Moisha uses double-extortion techniques to force the victims into paying the ransom. This technique enables the TAs to exfiltrate and encrypt the victim's data.

Technical Details

For our analysis, we have taken the following sample hash:

(SHA256), b3ebc327773f5f846deeb1255475644a630c4d0d3b4eda3bbf995a36599c07cf
It is a 32-bit GUI-based .NET binary targeting Windows-based operating systems.

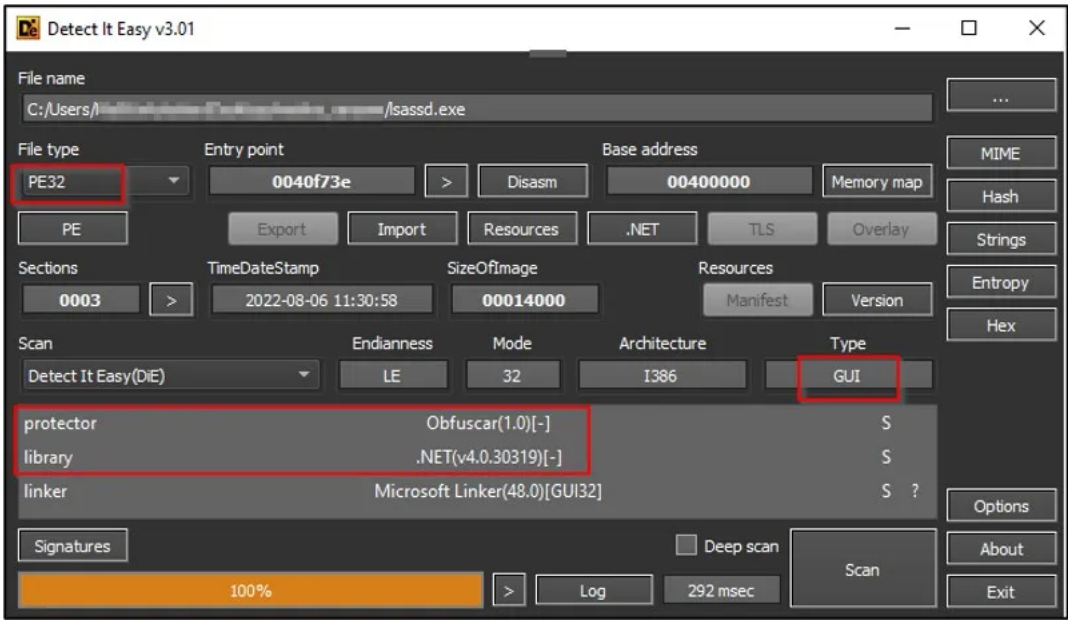


Figure 1 – Static file details of Moisha ransomware

Upon execution, the ransomware initially creates a global mutex named *"Global__w3616de3-6u4b-32fc-97b1-de928faadf50"* to ensure that only one instance of the malware is running on the victim's system at a time. The malware terminates its execution if it identifies the mutex is already present in the machine.

Next, the malware searches for the list of services such as backup services, malware-scanner services, and other services in the victim's system. If any such service is found running in the system, the malware stops the services. This step ensures that these services do not block access to the files that are going to be encrypted later. The figure below shows the *"ServiceController"* function, and a list of services targeted by the ransomware.

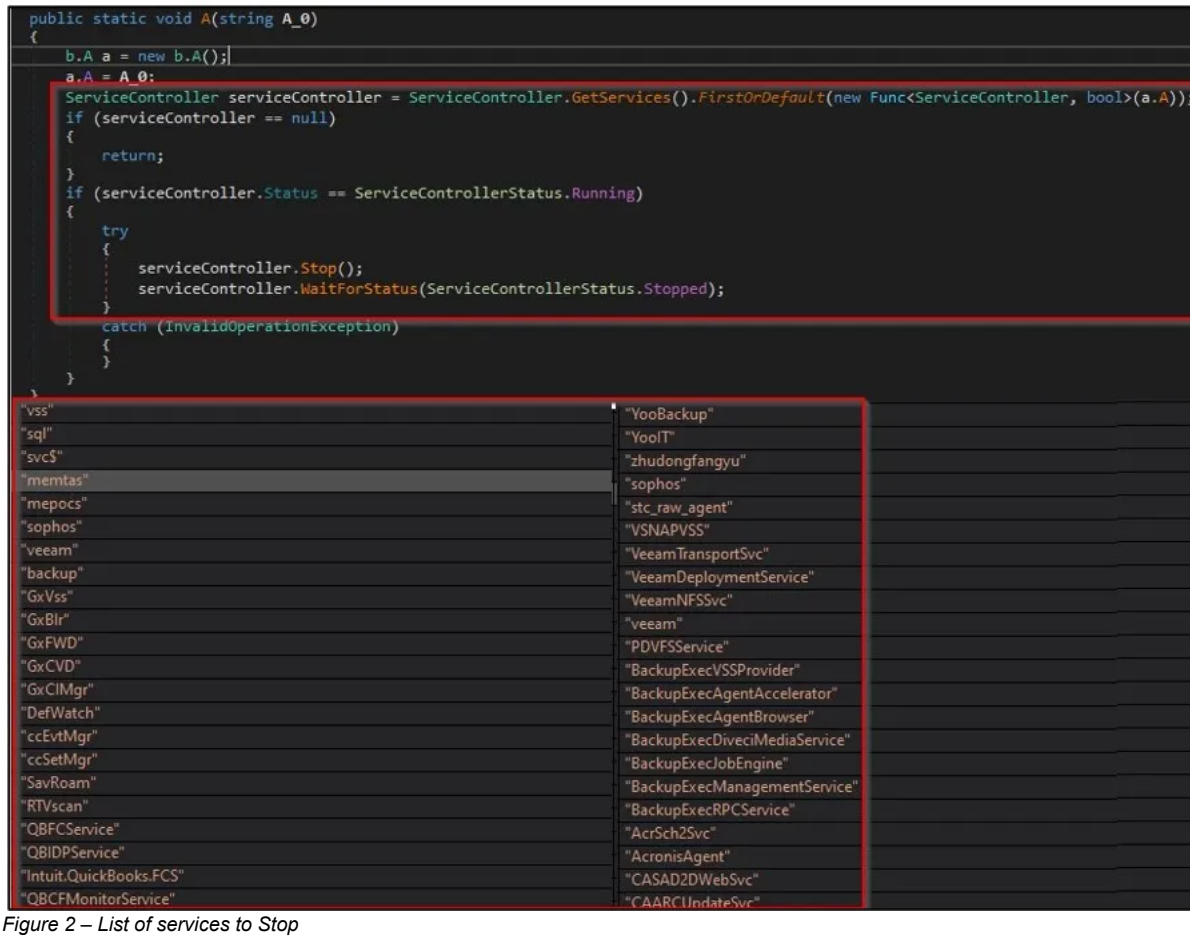


Figure 2 – List of services to Stop

After stopping the active services, the ransomware checks for the presence of a list of processes and kills them if they are actively running on the victim's machine.

The image below shows the kill process function and a list of processes targeted by the ransomware.

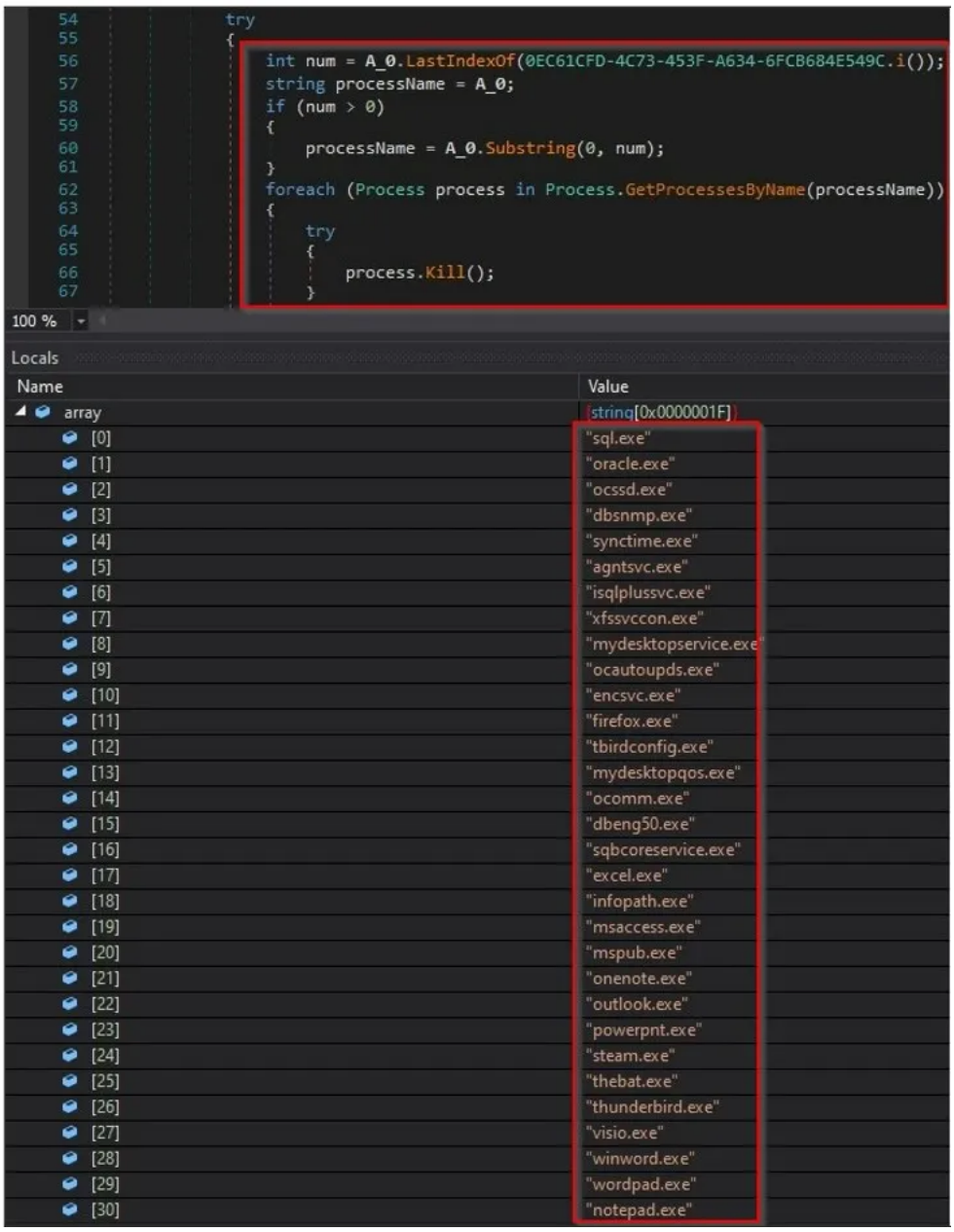


Figure 3 – List of processes to Kill

Additionally, the Moisha ransomware disables the Microsoft Defender Antivirus' real-time protection and deletes shadow copies by using the below command line:

- *powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true*
- *vssadmin.exe delete shadows /all /quiet*

Next, the malware gets the available system drives using the function *"System.IO.Directory.GetLogicalDrives()"* and adds them to the list as shown below.

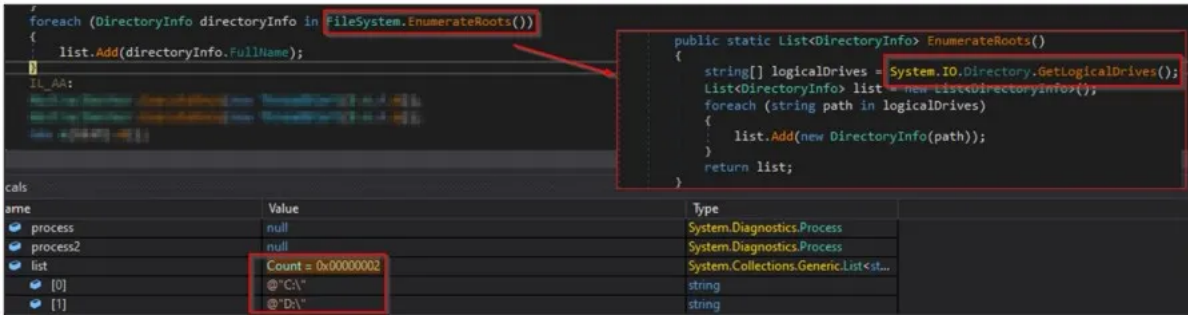


Figure 4 – Enumerate system drives

This is followed by the ransomware using the *"RecursePath()"* function to enumerate the files and folders inside the identified system drive and starts a new thread for the file encryption process, as shown in the figure below.

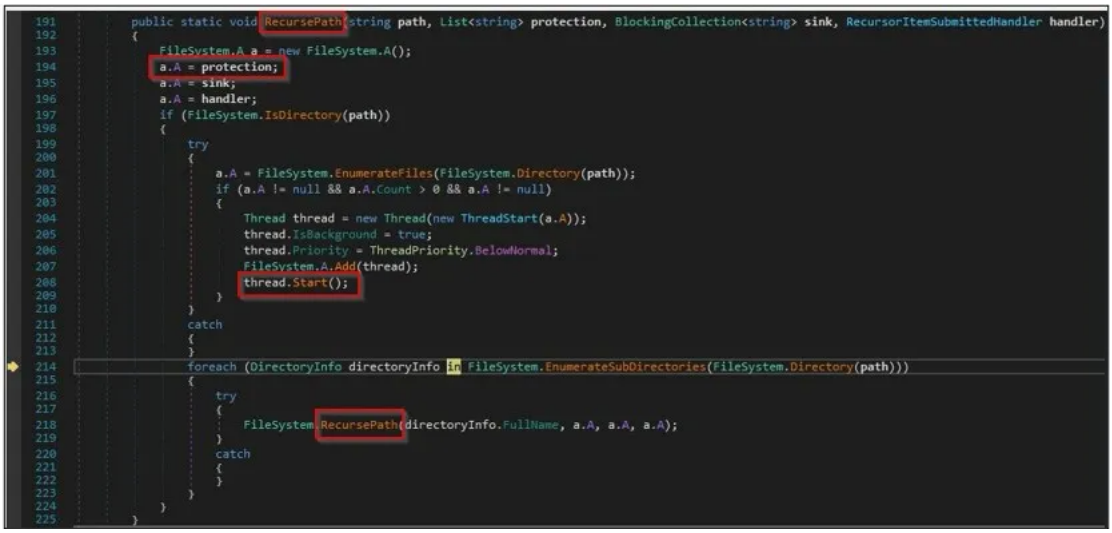


Figure 5 – Enumerate files & folders for encryption

Before initiating the encryption process, the ransomware drops the ransom note in the folder with the file name "!!!READ TO RECOVER YOUR DATA!!!.txt." The malware creates the ransom note by decoding the hardcoded Base64 content, as shown in the figure below.

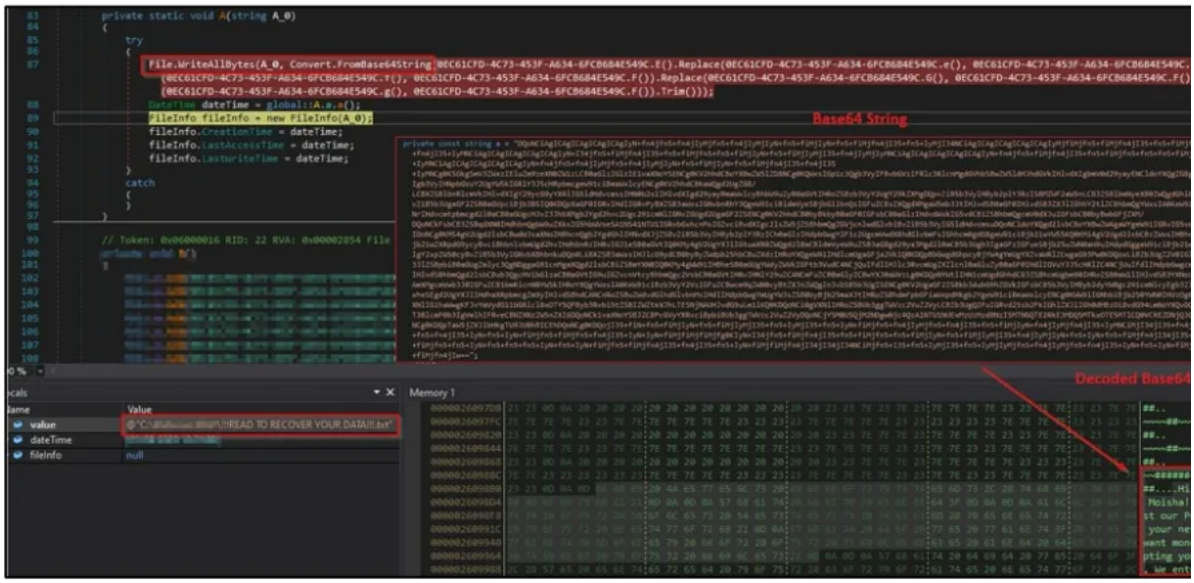


Figure 6 – Malware writing Ransom note

Figure 7 showcases the directory names, file names, and file extensions excluded by the Moisha ransomware during its encryption process.

".pem"	"Tox"	"ntuser.ini"
".der"	"Admin"	".reg"
".rsa"	"local"	"iconcache.db"
".exe"	"$Recycle.Bin"	"thumbs.db"
".dll"	"autorun.inf"	"#recycle"
".ocx"	"boot.ini"	"!!!READ TO RECOVER YOUR DATA!!!.txt"
".drv"	"bootfont.bin"	".list"
".sys"	"bootsect.bak"	"/boot"
".ttf"	"bootmgr"	"/bin"
".otf"	"bootmgr.efi"	"/usr"
".log"	"bootmgfw.efi"	"/lib"
"Boot"	"desktop.ini"	"/snap"
"Windows"	"ntldr"	"/run"
"Windows.old"	"ntuser.dat"	"/tmp"
"Tor Browser"	"ntuser.dat.log"	

Figure 7 – Exclusion list of file extensions and file/folder names from encryption

Our analysis indicates that the Moisha ransomware uses the RSA and AES encryption algorithms, and it comes with a fixed hardcoded Base64 encoded RSA Public Key, as shown below.

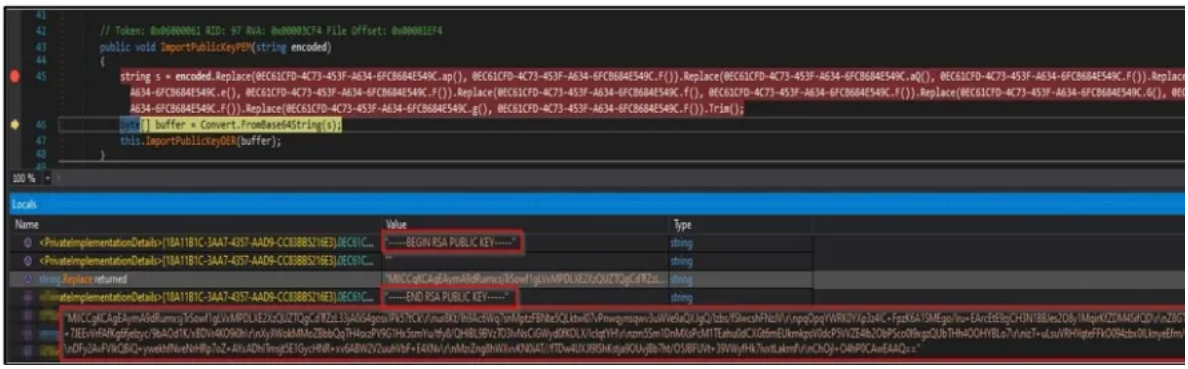


Figure 8 – RSA Public key

The malware also checks whether the file size is less than 2 GB using the *"OnItemArrived()"* function. Based on the file size, it calls the encryptor function to perform faster file encryption, as shown in Figure 9.

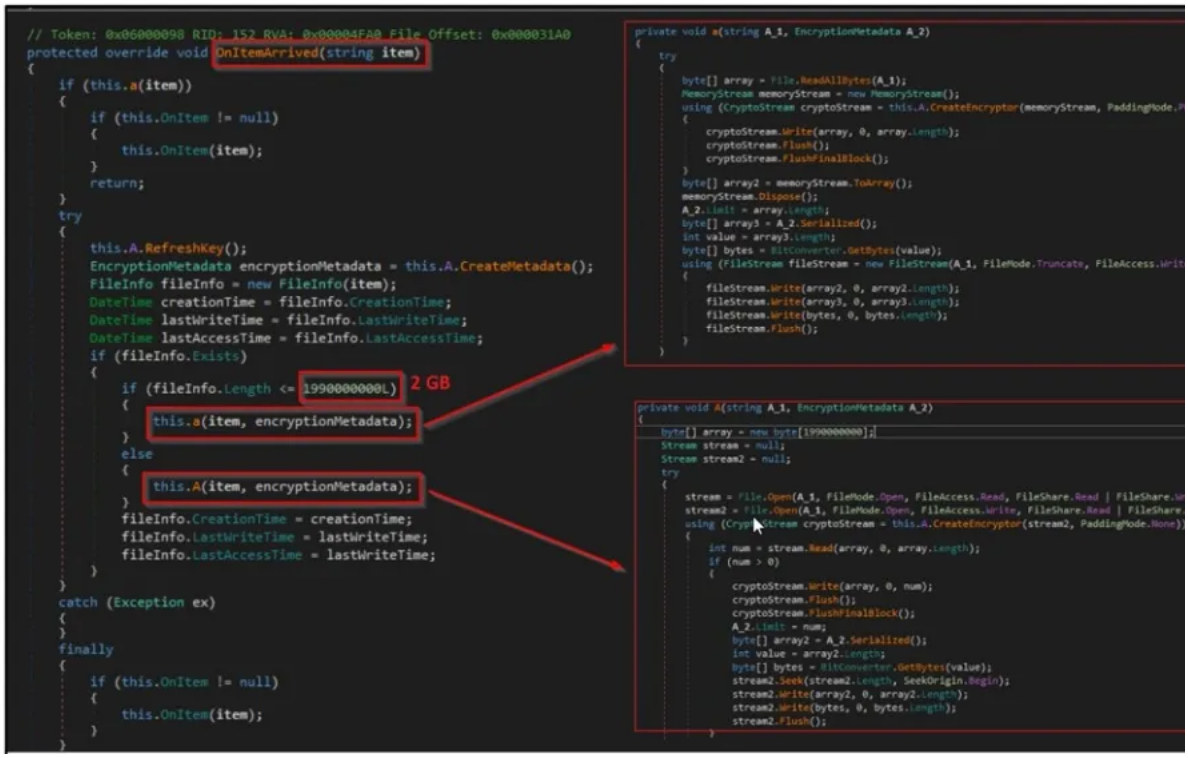


Figure 9 – File size check for encryption

The image below shows the code snippet of the encryption function and the original and infected file content before and after encryption.

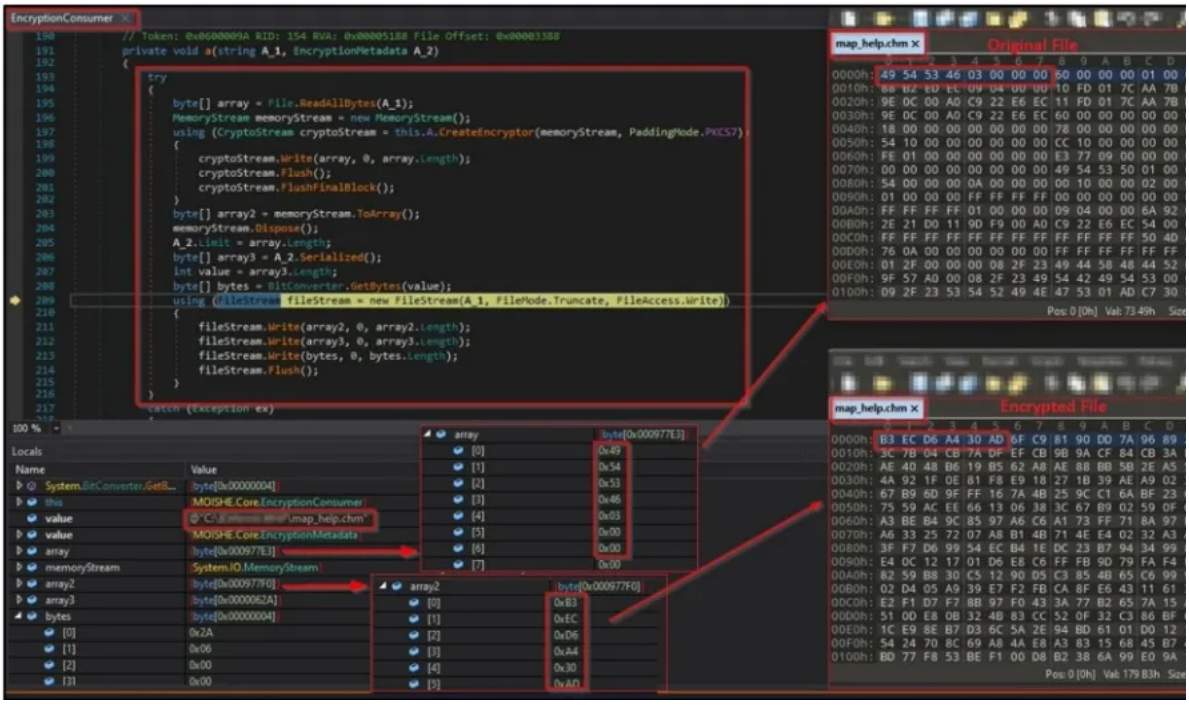


Figure 10 – Code snippet of the encryption function

We observed that the Moisha ransomware does not change the file name or extension after file encryption. The image below shows the encrypted files and ransom note text file of the Moisha ransomware after the successful infection of the victim's machine.

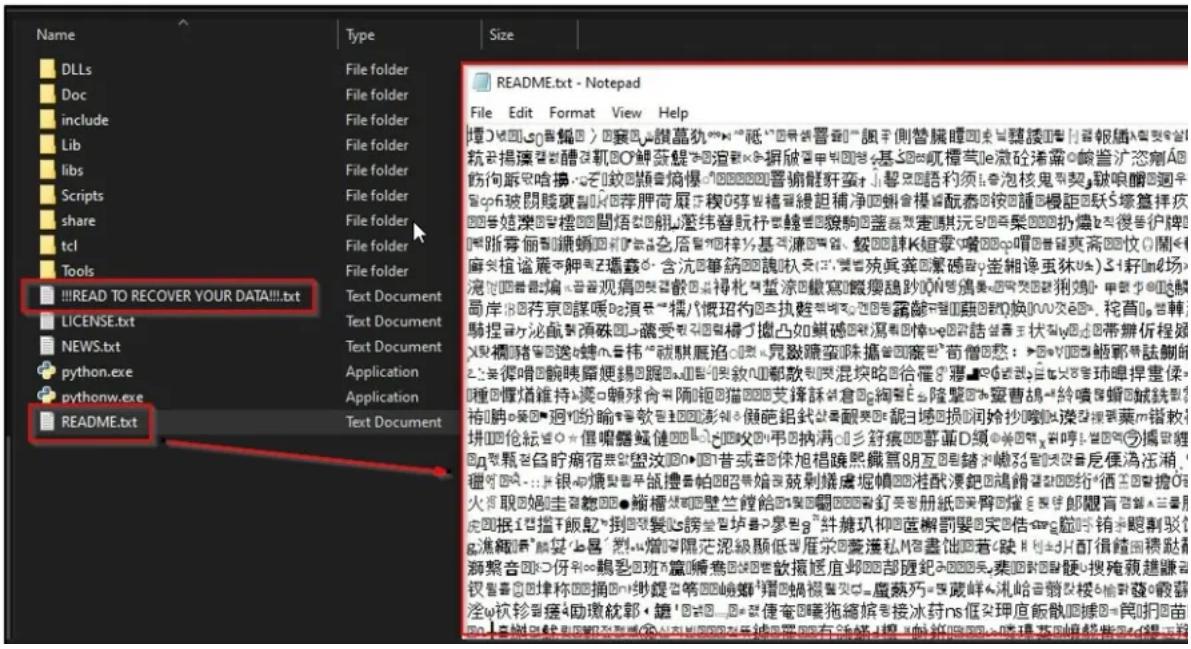


Figure 11 – Encrypted file by Moisha ransomware

Once the victim's system is infected, the malware spreads to other machines in the same network by using the following functions:

- *EnumNetShares()*
- *GetAllShares()*
- *GetComputerShares()*
- *NetWkstaGetInfo()*
- *WriteToFileThreadSafe()*

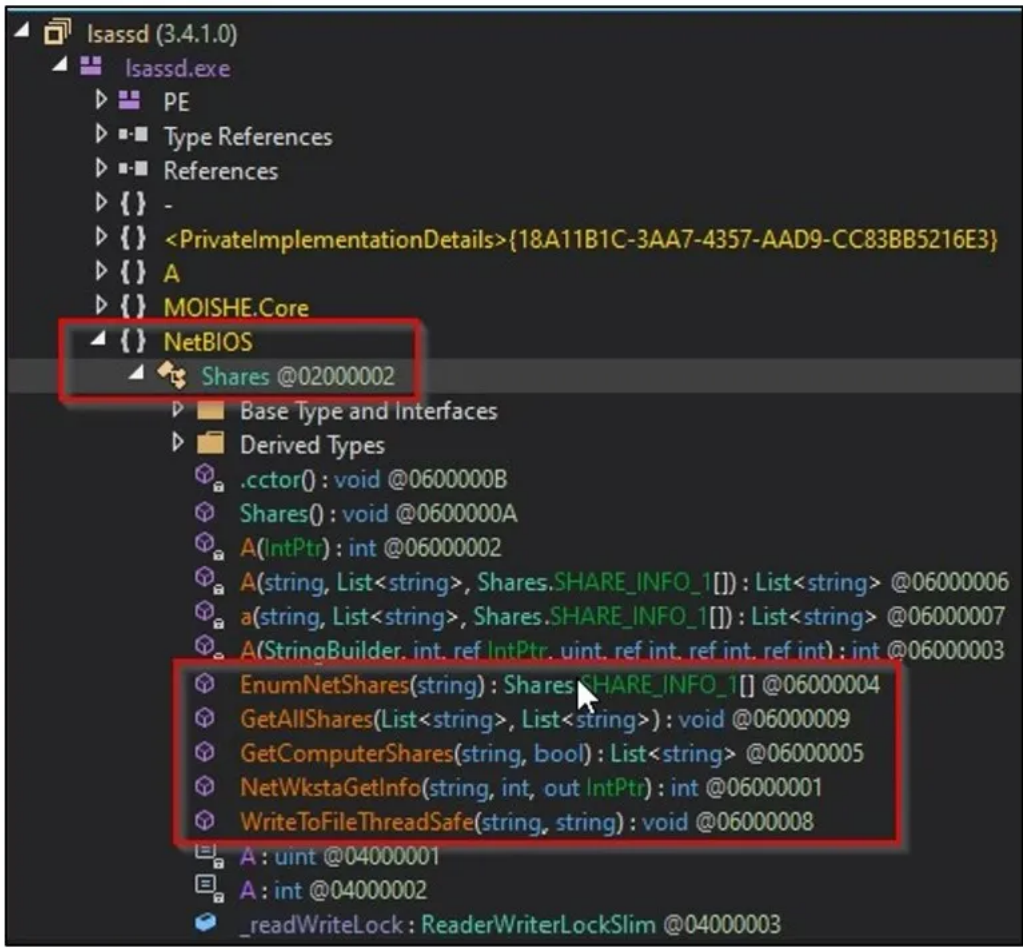


Figure 12 – Network Spreading functions

Finally, the ransomware deletes itself by using the powershell command line:

- *powershell.exe rm "<filename>"*

In the ransom note dropped by Moisha, victims are given instructions on contacting the TAs to restore their encrypted files. Additionally, the TAs behind Moisha ransomware threaten victims stating that they have entered the organization's network and downloaded all work-related files along with the source codes, compromising over 200 gigabytes of data.

The ransom note also contains the Moisha ID of TOX Messenger for ransom negotiations and a Proton mail ID for quick communication with the TAs, as showcased in the figure below.

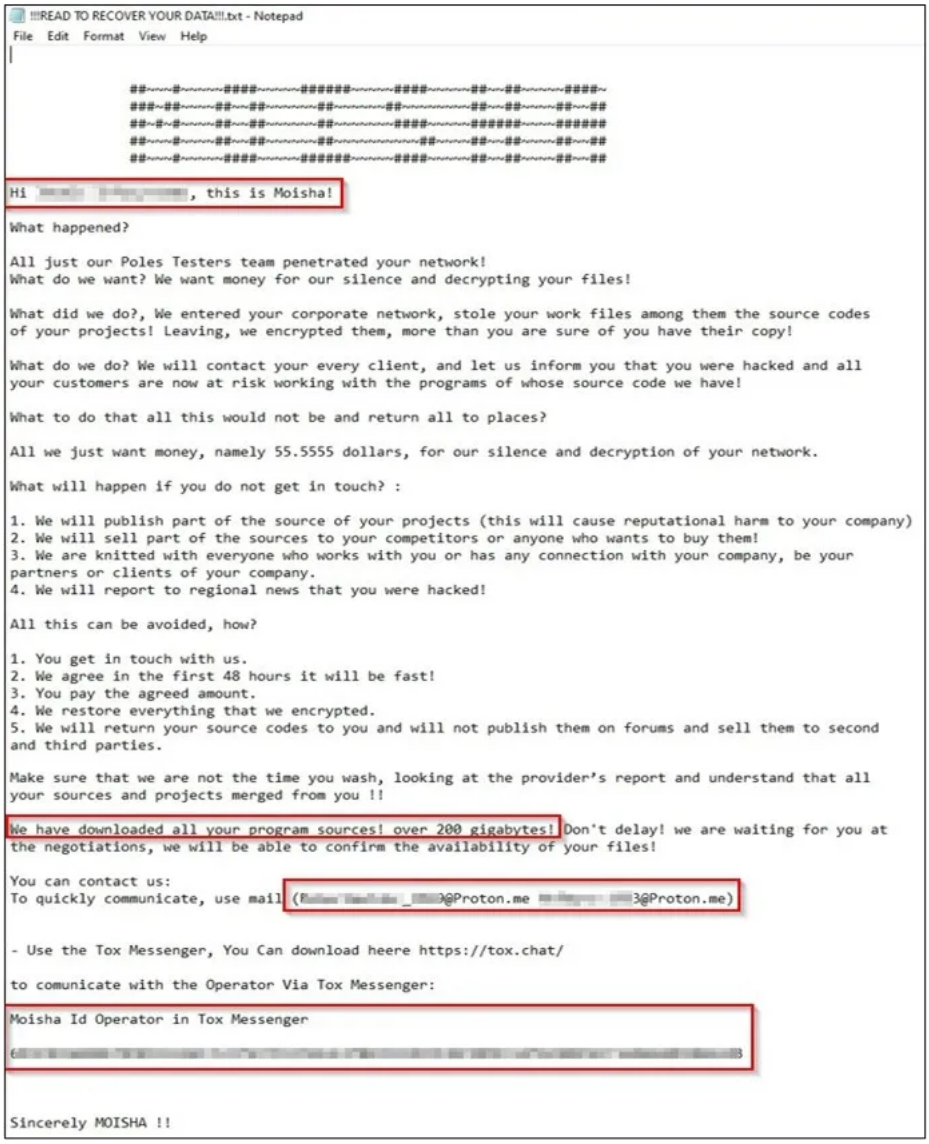


Figure 13 – Ransom note

Conclusion

Ransomware is becoming an increasingly common and effective attack method, adversely affecting organizations and their productivity. To prevent ransomware attacks, enterprises need to stay ahead of the techniques used by TAs besides implementing the requisite security best practices and security controls.

Ransomware victims are at risk of losing valuable data as a result of such attacks, in addition to significant financial loss and lost productivity. If the victim is unable or unwilling to pay the ransom, TAs often leak or sell this data online, compromising sensitive user data for businesses and individuals and resulting in severe loss of reputation for the affected organization(s).

Cyble Research Labs continuously monitors new ransomware campaigns to keep our readers updated with our latest findings.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

Safety Measures Needed to Prevent Ransomware Attacks

- Conduct regular backup practices and keep the backups offline or in a separate network.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

Steps To Take After A Ransomware Attack

- Detach infected devices on the same network.
- Disconnect external storage devices if connected.
- Inspect system logs for suspicious events.

Impacts And Cruciality of Moisha Ransomware

- Loss of Valuable data
- Loss of the organization’s reputation and integrity
- Loss of the organization’s sensitive business information
- Disruption in the organization’s operations
- Financial loss

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
	T1059	Command and Scripting Interpreter
Defence Evasion	T1027	Obfuscated Files or Information
	T1070	Indicator Removal on Host
Discovery	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1518	Security Software Discovery
	T1057	Process Discovery
	T1046	Network Service Discovery
Impact	T1486	Data Encrypted for Impact
	T1489	Service Stop
	T1490	Inhibit System Recovery

Indicators of Compromise (IoCs):

Indicators

d197883d8745a61fe25aebea85622a65 5d22d359e7b8dc70ccf5e369fb07f2e0960ef76f b3ebc327773f5f846deeb1255475644