New Ransomware Groups on the Rise

blog.cyble.com/2022/07/12/new-ransomware-groups-on-the-rise/

July 12, 2022

"RedAlert," LILITH and 0mega leading a wave of Ransomware Campaigns

Ransomware is one of the most serious cybersecurity problems on the internet and possibly the most potent form of cybercrime plaguing organizations today. It has quickly become one of the most prominent and profitable types of malware for Threat Actors (TAs).

In a typical scenario, the ransomware infection starts with the TA gaining access to the target device. Depending on the type of ransomware, it can infect the entire operating system or encrypts individual files. The TAs will then typically demand payment from the victim for the decryption of their files.

Multiple new ransomware groups have surfaced recently, highlighting the adoption of ransomware attacks by TAs for monetary gains. A few of them include:

RedAlert Ransomware

RedAlert or N13V is a new ransomware strain that targets both Windows and Linux VMWare ESXi servers on corporate networks. The ransomware stops all running virtual machines and encrypts any file related to virtual machines, such as virtual disks. RedAlert Ransomware was named after a string with the same name in the ransom note, but threat actors named their campaign “N13V”. RedAlert only accepts ransom payments in Monero, which is rather atypical for ransomware groups.

RedAlert ransomware has manual operations, which means TAs execute the ransomware after a complete takeover of the victim system. The ransomware binary provides various options to the TAs for performing pre-encryption operations such as stopping all virtual machines running on VMware ESXi, Asymmetric cryptography performance tests, etc.

The ransomware uses NTRUEncrypt public key encryption algorithm for encryption. The ransomware only targets log files (.log), swap files(.vswp), virtual disks(.vmdk), snapshot files (.vmsn) and memory files(.vmem) of VMware ESXi virtual machines. After encryption the ransomware appends a “*.crypt[Random number]*” extension to the file.

The figure below shows the leak site of RedAlert ransomware.

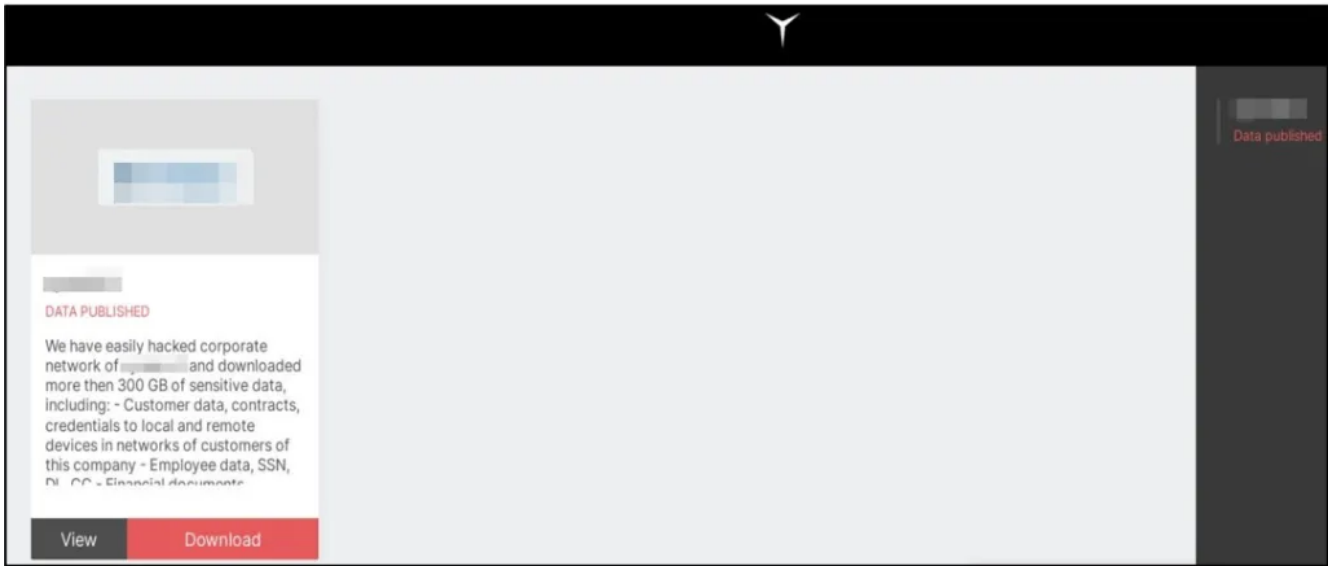


Figure 1 – RedAlert Ransomware Leak Site

0mega Ransomware

Another new ransomware gang, “0mega,” is suspected of targeting organizations using Double Extortion techniques. The indicators of compromise of this ransomware strain are unavailable in the wild.

Still, as per researchers’ comments, the ransomware appends the files with the *“.0mega”* extension and creates ransom notes named “DECRYPT-FILES.txt.”

The figure below shows the 0mega Ransomware data leak site.

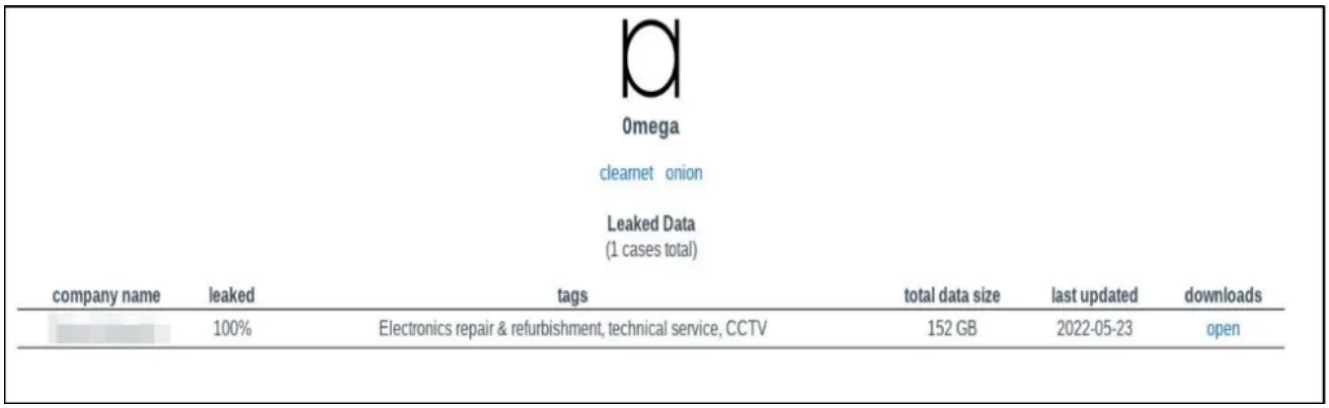


Figure 2 – 0mega Ransomware Leak Site

Lilith Ransomware

Ransomware operators now have another new tool at their disposal, named Lilith Ransomware. This threat can affect many file types and render them completely unusable.

Lilith ransomware encrypts files on the victim's machine and appends the extension of encrypted files as *".lilith."* Afterward, a ransom note is created on the system to demand payment.

In this report, Cyble Research Labs conducts a deep analysis of Lilith ransomware to understand its behavior and infection mechanism.

Technical Analysis: Lilith Ransomware

Static analysis indicates that the Lilith ransomware file is a console-based x64 architecture executable written in C/C++, as shown below.

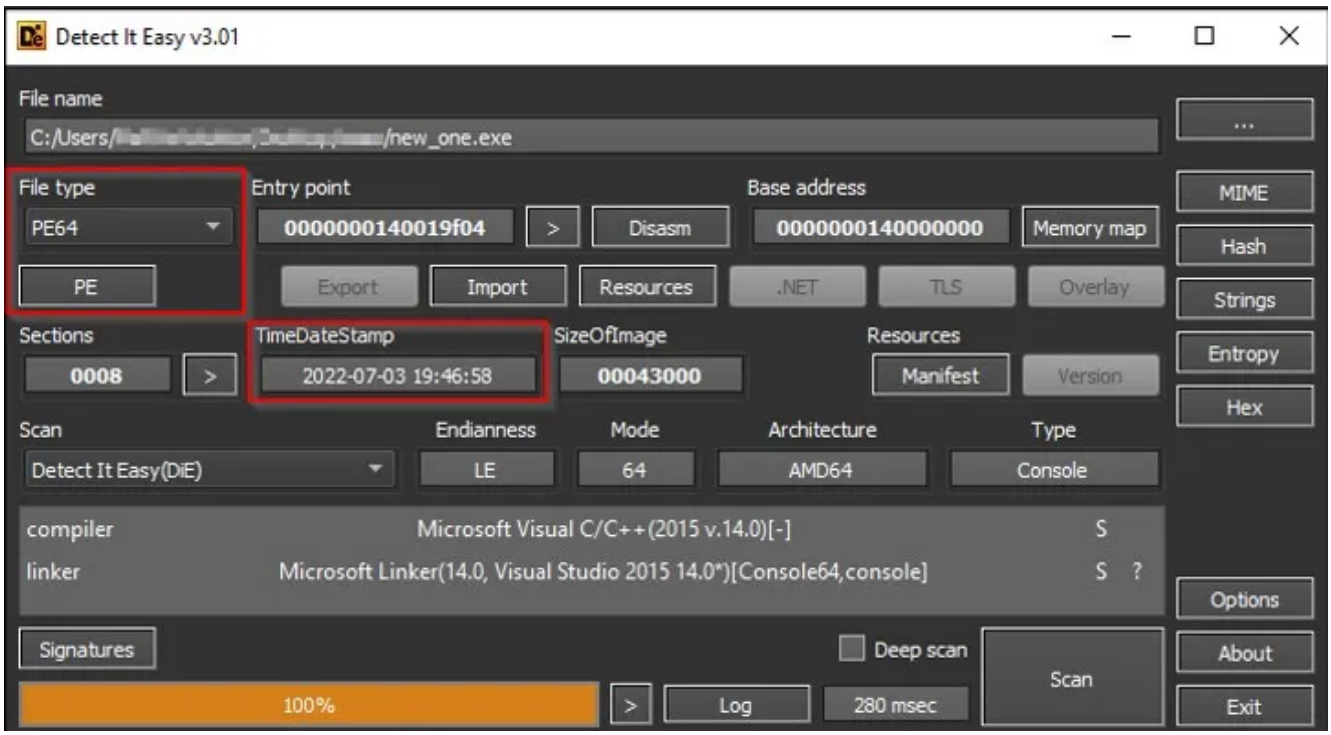


Figure 3 – Static information of LILITH Ransomware

Upon execution, Lilith ransomware initially searches for a list of hardcoded processes in the file and terminates its execution if any of them are running on the target's machine. This step ensures that these processes do not block access to the files to be encrypted.

The below figure shows the APIs used to kill the process execution by the ransomware.

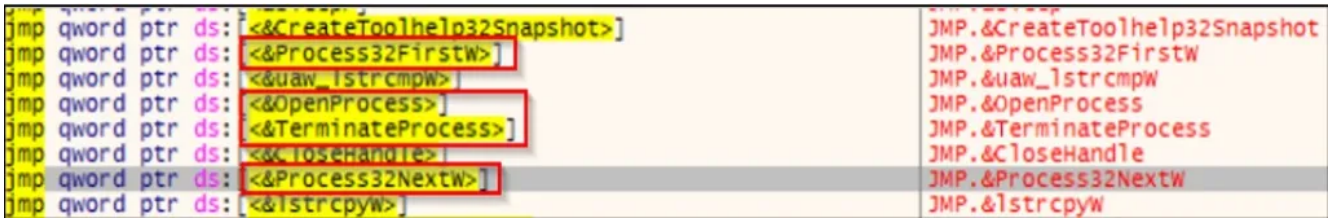


Figure 4 – APIs used to Terminate Process Execution
A full list of hardcoded process names is shown in the below figure.

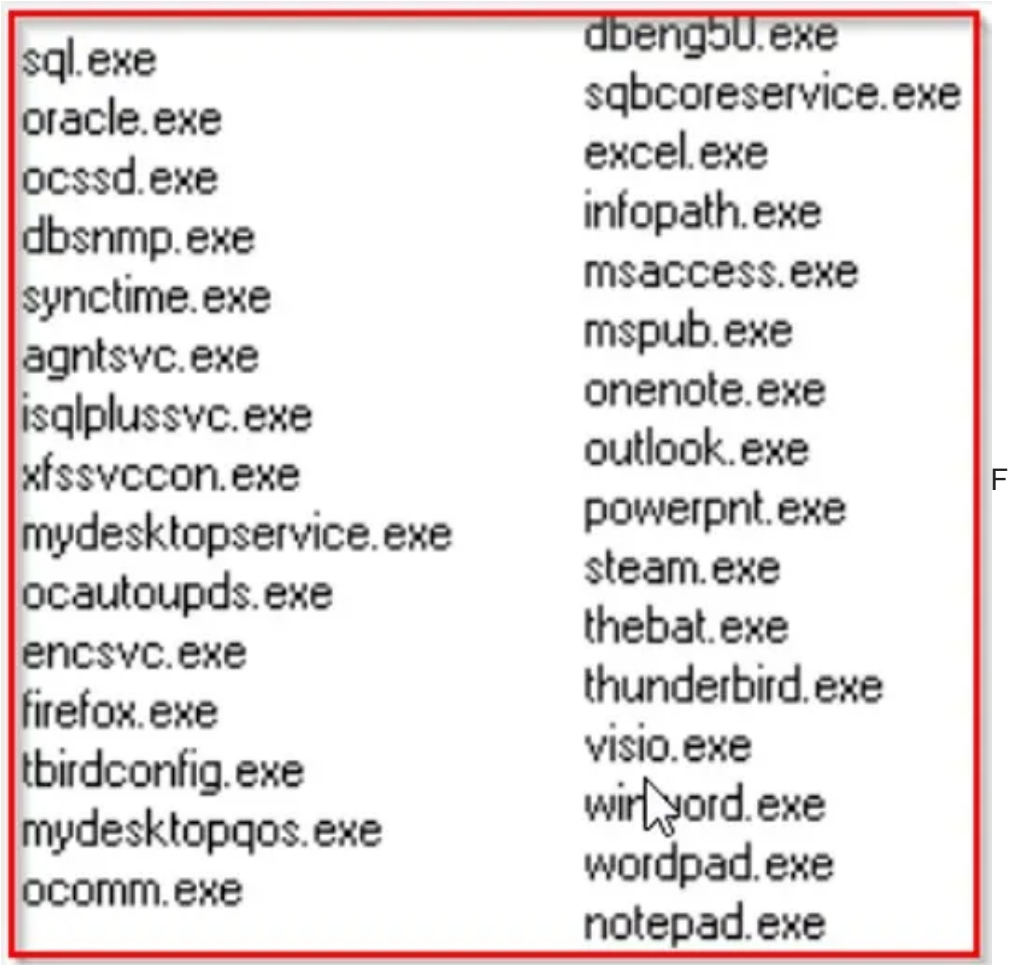


Figure 5 – List of Processes for Termination

To identify the services running in the machine, the ransomware first calls *"OpenSCManagerA()"* API, which establishes a connection to the service control manager that gives the TAs access to the service control manager database.

Upon gaining access to this database, the following APIs() will be called:

- *OpenServiceA()* – Opens the specified service.
- *QueryServiceStatusEx()* – Gets the status of the service.

- *EnumDependentServiceA()* – Retrieves the dependent services.
- *ControlService()* – takes control of the service for stopping.

If the *"OpenSCManagerA()"* API fails to get the handle to Service Control Manager (SCM), then the ransomware skips calling the below service-related APIs.

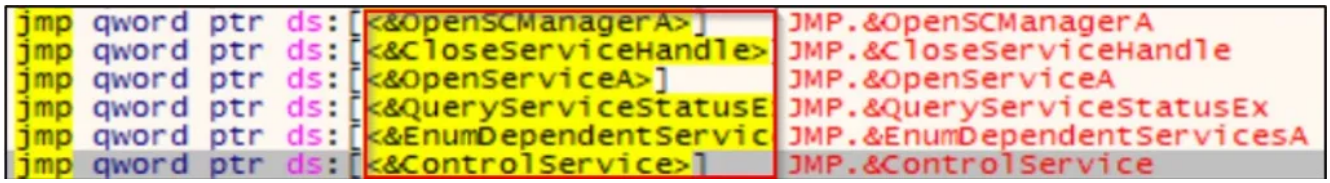


Figure 6 – Service-Related APIs

After that, the ransomware enumerates and gets the system drive information of the victim's machine by using the below APIs such as *GetDriveTypeW(), FindFirstVolumeW(),* and *FindNextVolumeW()*.

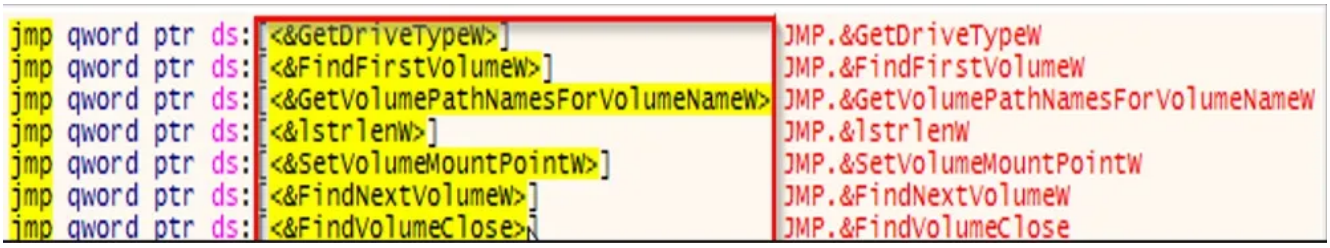


Figure 7 – System Drive Related APIs

Before initiating the encryption process, the ransomware drops the ransom note in multiple folders with the file name *"Restore_Your_Files.txt."* The ransomware creates a ransom note with the content shown in the figure below.

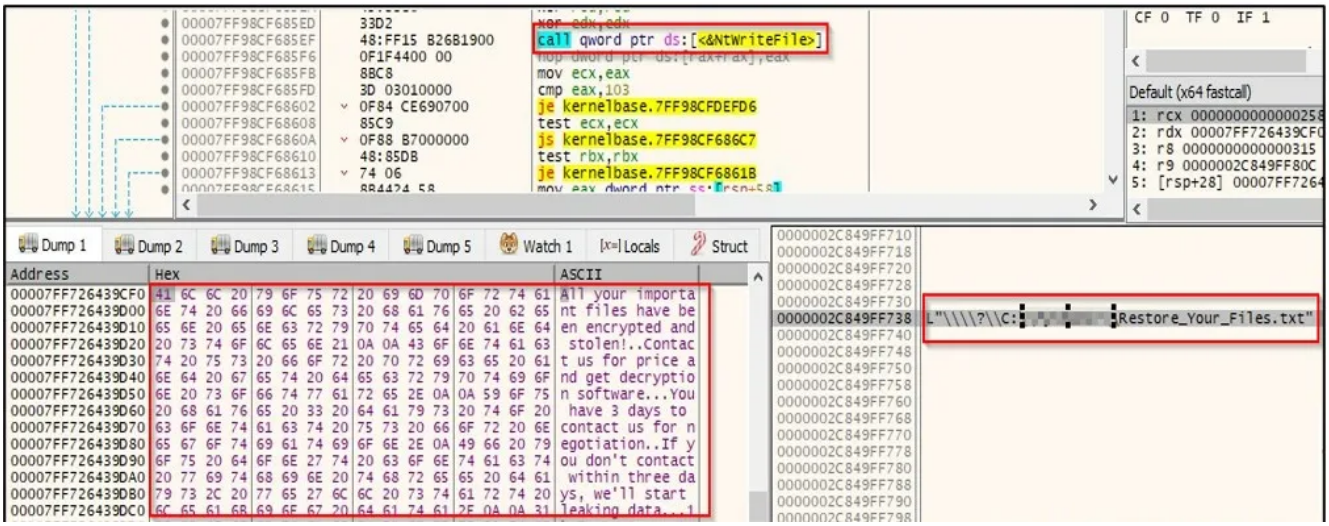


Figure 8 – Malware Writes Ransom Notes

The ransomware searches for files to encrypt on the local system by enumerating the file directories using *FindFirstFileW()* and *FindNextFileW()* API functions. It ignores the file extensions such as EXE, DLL, and SYS and excludes a list of directory and file names from the encryption process (Figure 9).

Interestingly, the exclusion list contains the filename *"ecdh_pub_k.bin,"* which stores the local public key of BABUK ransomware for file decryption.

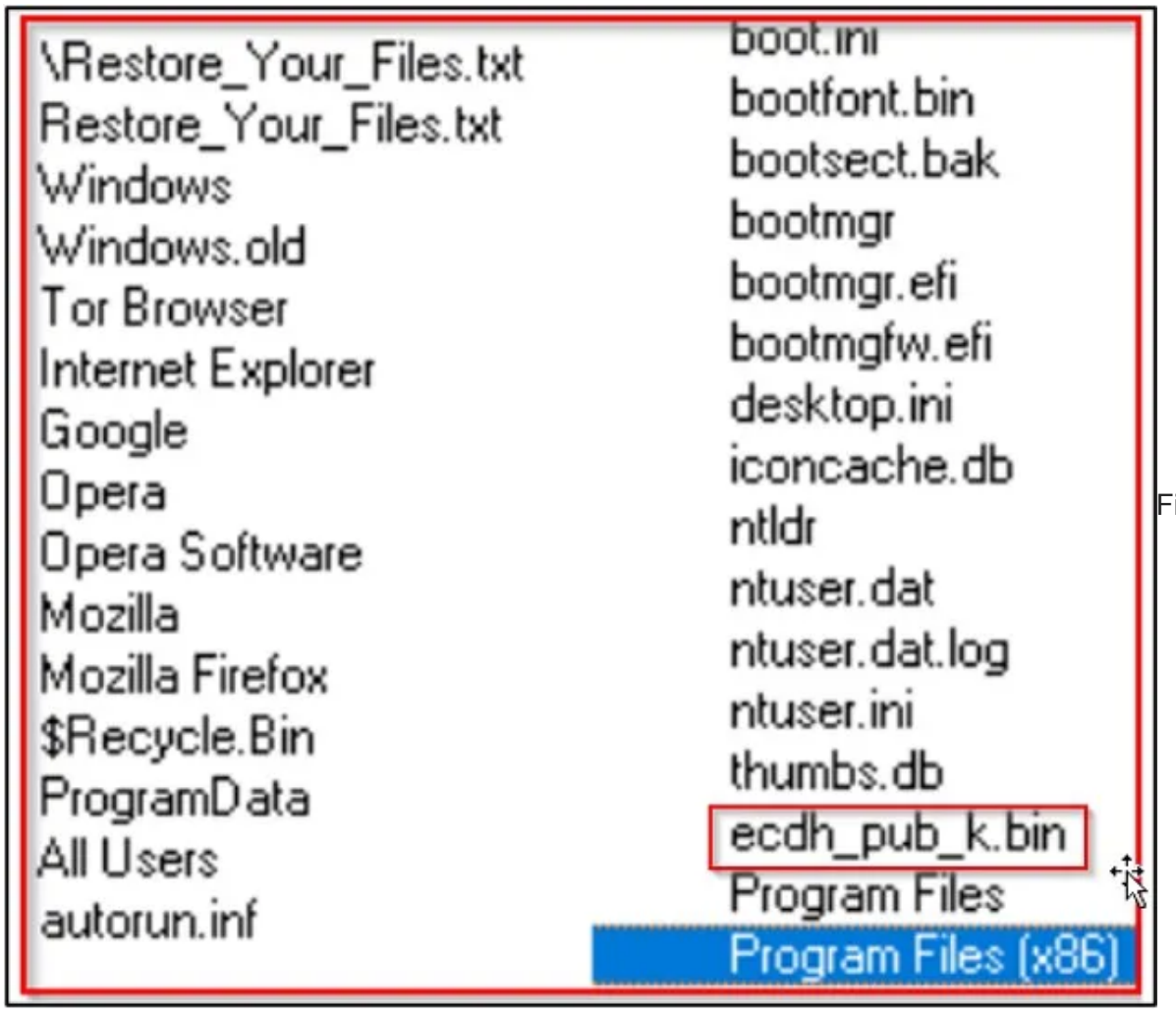


Figure 9 – Exclusion List of Folder and File names

The malware uses cryptographic APIs such as *CryptAcquireContextW()* and *CryptGenRandom()* from ADVAPI32.dll to encrypt victims' files. The ransomware generates a random key with the function *"CryptGenRandom()"* and then encrypts the files using an encryption routine as shown below.

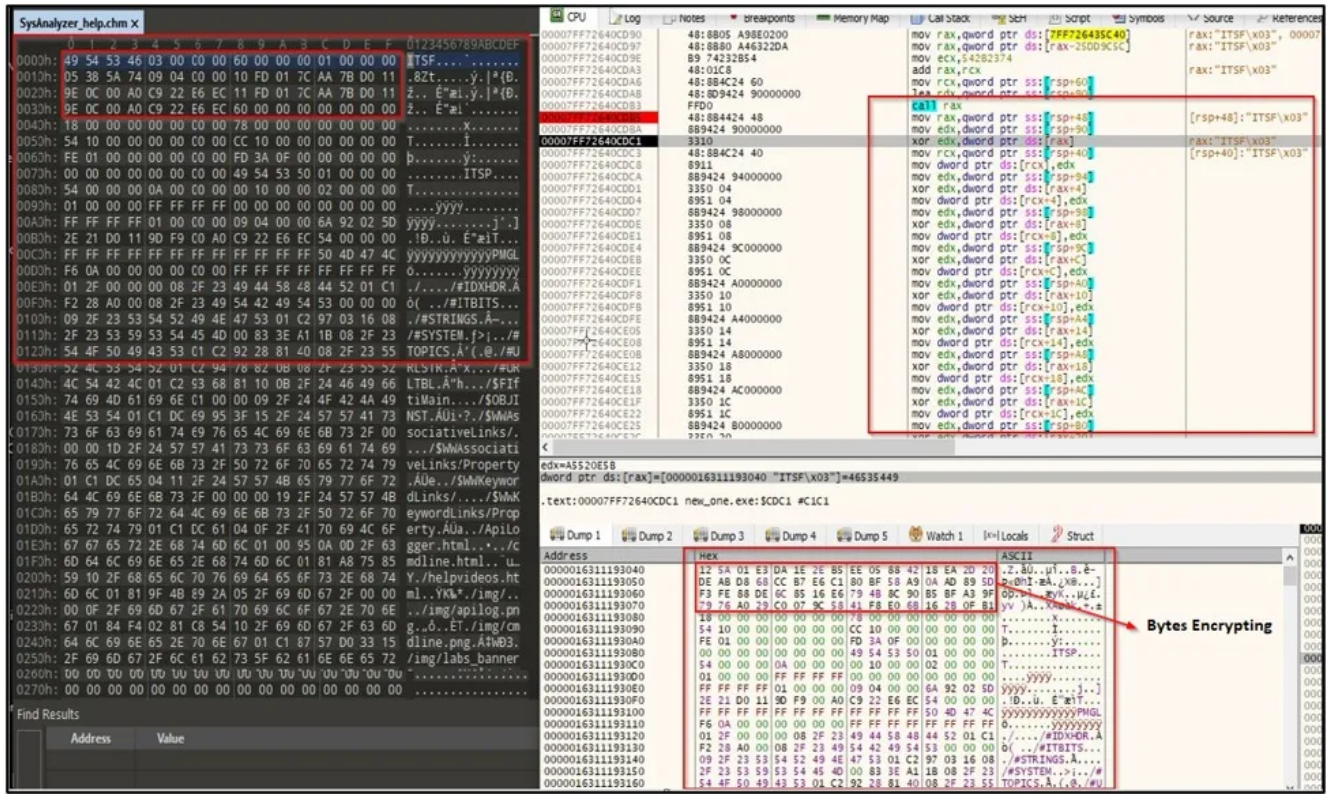


Figure 10 – Encryption Routine

The figure below shows the WriteFile operation and the original/infected file content before and after encryption.

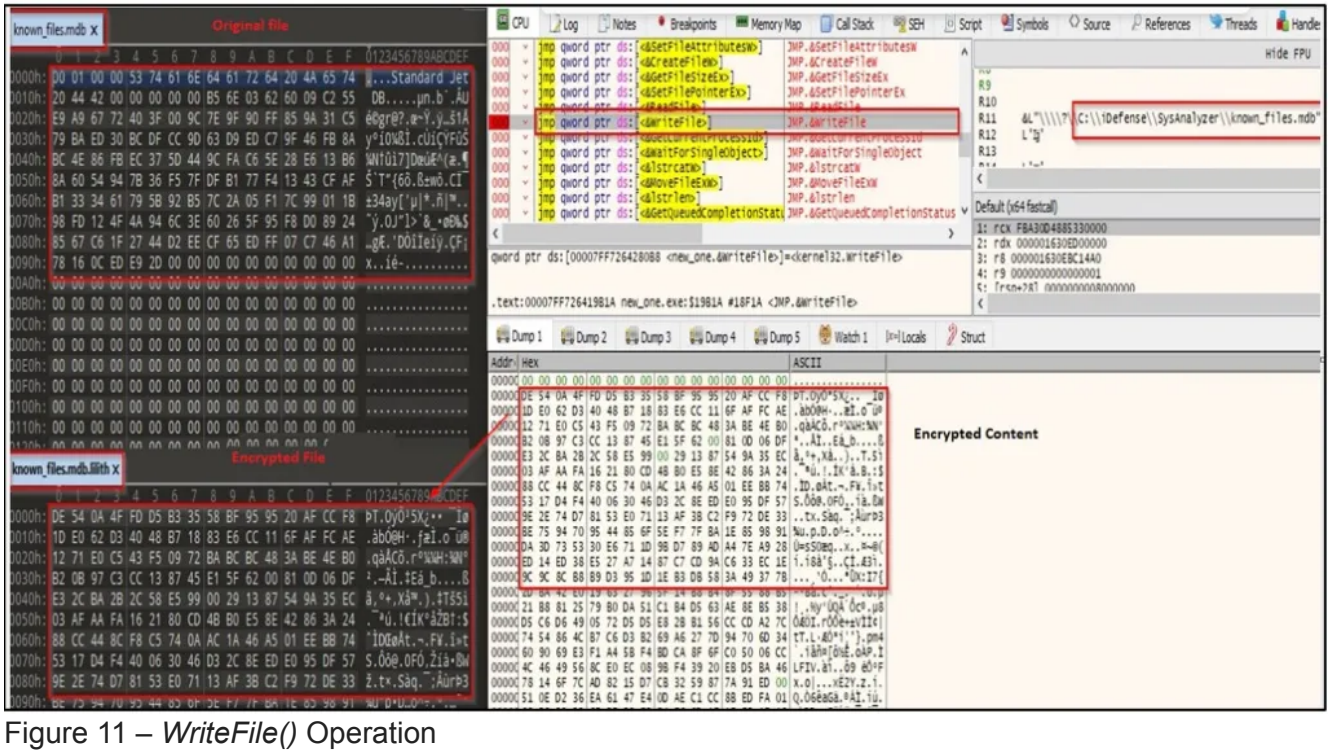


Figure 11 – *WriteFile()* Operation

Finally, the malware renames the encrypted file with the *".lilith"* extension and replaces it with the original file by using the *"MoveFileExW()"* API, as shown below.

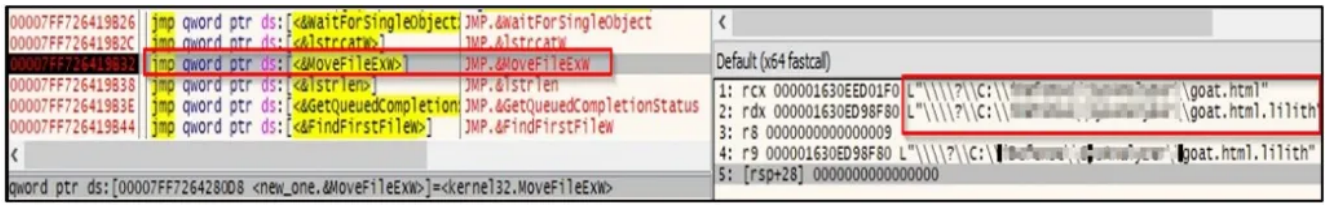
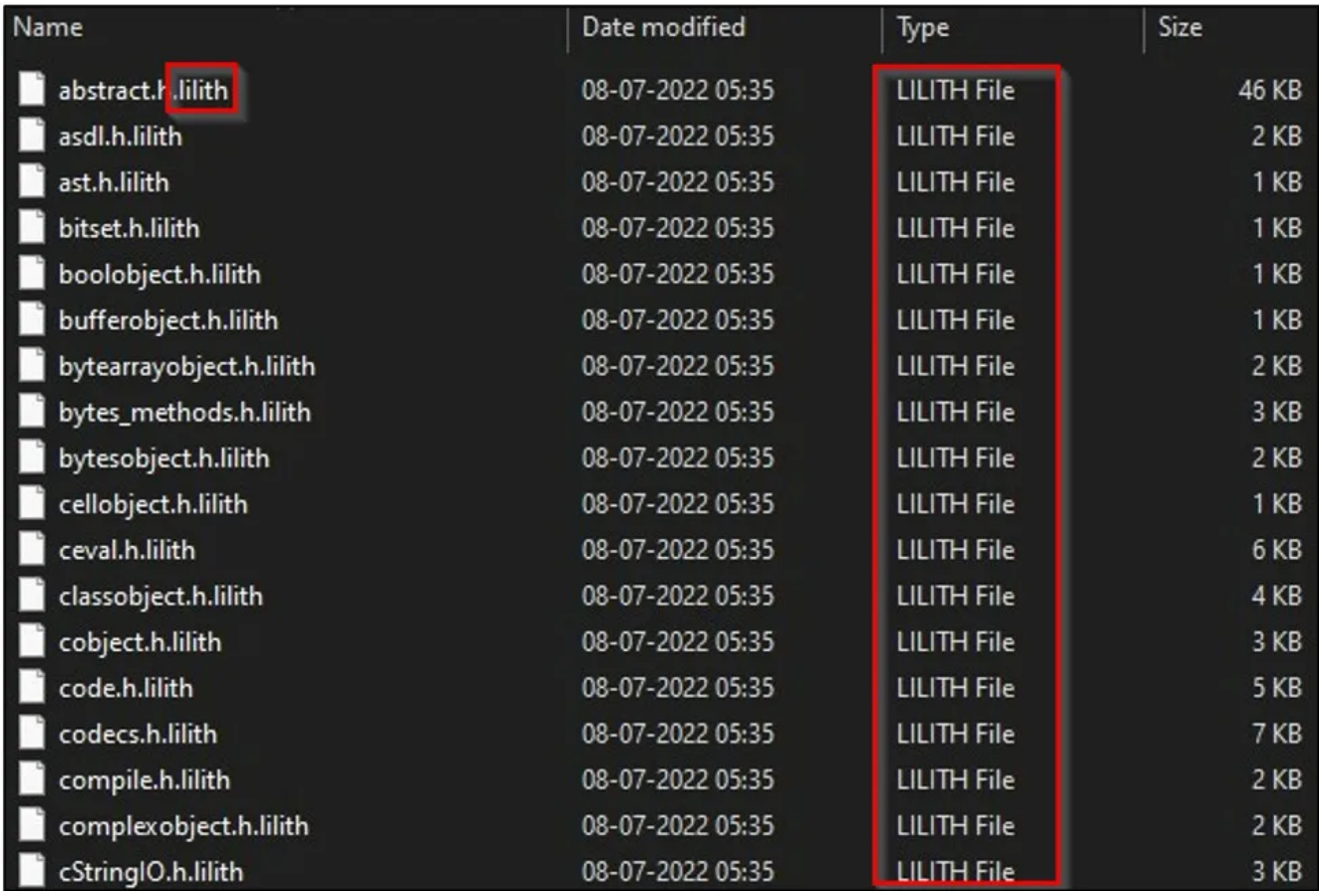


Figure 12 – *MoveFileExW()* API

The below figure shows the encrypted files by Lilith ransomware after the successful infection of a victim's machine.



Name	Date modified	Type	Size
abstract.h.lilith	08-07-2022 05:35	LILITH File	46 KB
asdl.h.lilith	08-07-2022 05:35	LILITH File	2 KB
ast.h.lilith	08-07-2022 05:35	LILITH File	1 KB
bitset.h.lilith	08-07-2022 05:35	LILITH File	1 KB
boolobject.h.lilith	08-07-2022 05:35	LILITH File	1 KB
bufferobject.h.lilith	08-07-2022 05:35	LILITH File	1 KB
bytearrayobject.h.lilith	08-07-2022 05:35	LILITH File	2 KB
bytes_methods.h.lilith	08-07-2022 05:35	LILITH File	3 KB
bytesobject.h.lilith	08-07-2022 05:35	LILITH File	2 KB
cellobject.h.lilith	08-07-2022 05:35	LILITH File	1 KB
ceval.h.lilith	08-07-2022 05:35	LILITH File	6 KB
classobject.h.lilith	08-07-2022 05:35	LILITH File	4 KB
cobject.h.lilith	08-07-2022 05:35	LILITH File	3 KB
code.h.lilith	08-07-2022 05:35	LILITH File	5 KB
codecs.h.lilith	08-07-2022 05:35	LILITH File	7 KB
compile.h.lilith	08-07-2022 05:35	LILITH File	2 KB
complexobject.h.lilith	08-07-2022 05:35	LILITH File	2 KB
cStringIO.h.lilith	08-07-2022 05:35	LILITH File	3 KB

Figure 13 – Files Encrypted by Lilith Ransomware

In the dropped ransom note, victims are given three days to negotiate the price with the TAs for the decryption software. At the end of this deadline, the TAs threaten to begin leaking personal data if the ransom is not paid.

The ransom note also contains the poison ID for TOX communication and the Onion URL of the leak site page – shown in the figure below.

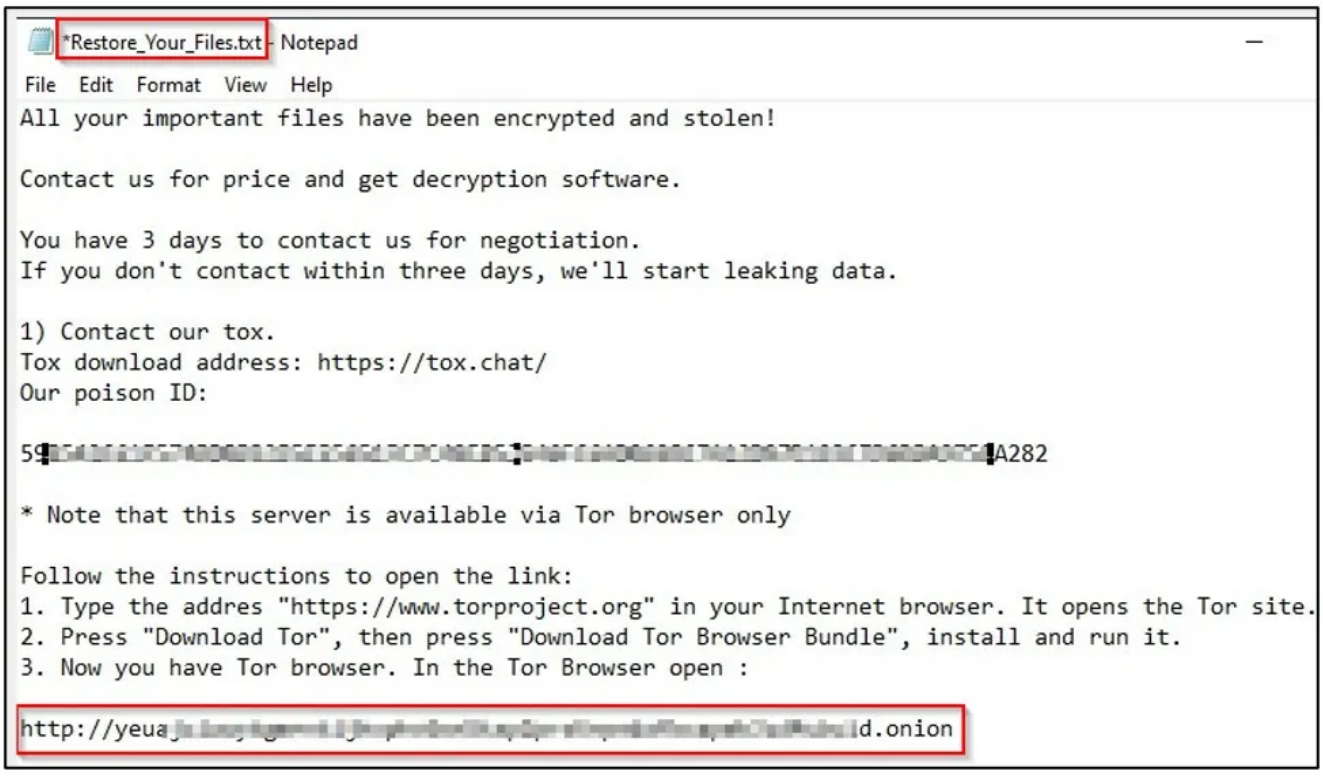


Figure 14 – Ransom Note

The figure below shows the Onion leak site home page of Lilith ransomware.

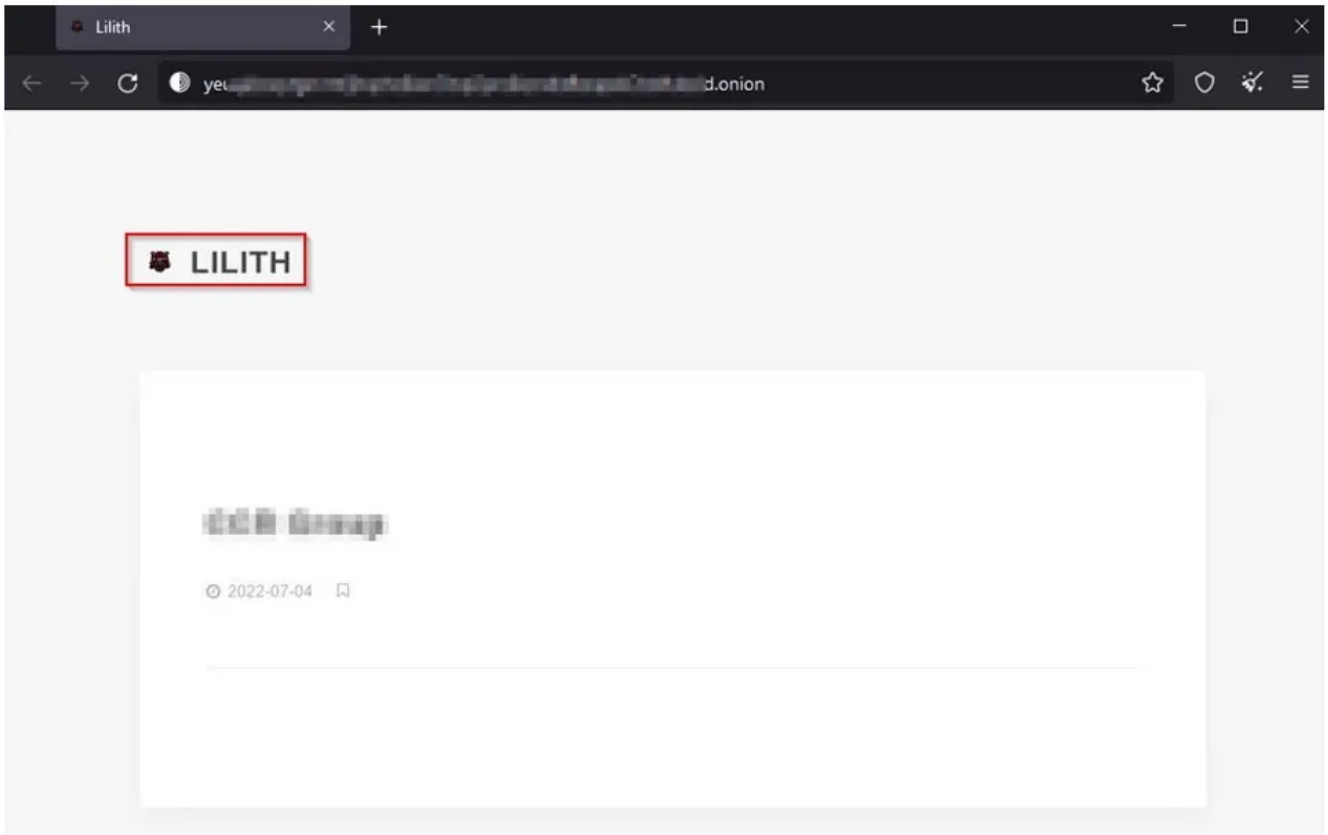


Figure 15 – Onion Leak Site

Conclusion

Ransomware groups continue to pose a severe threat to firms and individuals. Organizations 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, resulting in financial loss and lost productivity. If the victim is unable or unwilling to pay the ransom, the TAs may leak or sell this data online, compromising sensitive user data for businesses and individuals and resulting in a loss of reputation for the affected organization(s).

Throughout 2021 and 2022, we have observed record levels of ransomware activity. While notable examples of this are rebrands of existing groups, newer groups like LILITH, RedAlert, and 0mega are also proving to be potent threats.

Cyble Research Labs continuously monitors new ransomware campaigns and will keep our readers updated.

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 those 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.

Users Should Take the Following Steps After the 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 Ransomware

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

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name

Execution	T1204	User Execution
Discovery	T1012 T1082 T1083	Query Registry System Information Discovery File and Directory Discovery
Defense Evasion	T1027	Obfuscated Files or Information
Impact	T1486	Data Encrypted for Impact

Indicator Of Compromise (IOCs)

Indicators	Indicator Type	Description
b7a182db3ba75e737f75bda1bc76331a cf0fe28214ad4106c48ec5867327319eaa82b3c3 f3caa040efb298878b99f883a898f76d92554e07a8958e90ff70e7ff3cfabdf5	MD5 SHA1 Sha256	LILITH Ransomware x64 EXE file
f2fa9a3ce883a7f5b43ba5c9ff7bdf75 da6a7e9d39f6a9c802bbd1ce60909de2b6e2a2aa 039e1765de1cdec65ad5e49266ab794f8e5642adb 0bdeb78d8c0b77e8b34ae09	MD5 SHA1 Sha256	RedAlert Ransomware Linux file (elf)