New Ransomware Groups on the Rise

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

NEW RANSOMWARE CROUPS ON THE RISE "REDALERT," LILITH AND OMEGA LEADING A WAVE OF RANSOMWARE CAMPAIGNS

"RedAlert," LILITH and Omega 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:

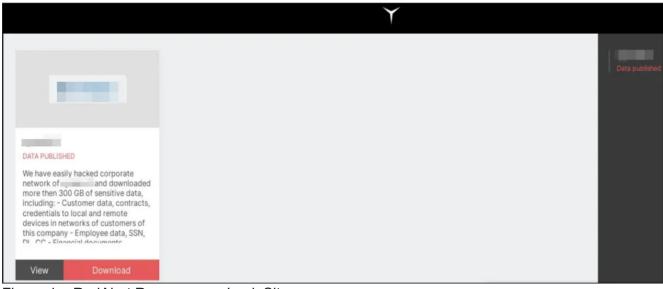
RedAlert Ransomware

July 12, 2022

<u>RedAlert</u> 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 ".Omega" extension and creates ransom notes named "DECRYPT-FILES.txt."

The figure below shows the Omega Ransomware data leak site.

| | | D | | | |
|--------------|--------|---|-----------------|--------------|-----------|
| | | 0mega | | | |
| | | clearnet onion | | | |
| | | Leaked Data (1 cases total) | | | |
| company name | leaked | tags | total data size | last updated | downloads |
| | 100% | Electronics repair & refurbishment, technical service, CCTV | 152 GB | 2022-05-23 | open |

Figure 2 – Omega 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.

| Detect It Easy v3.01 | | | | 1 | |
|------------------------|--------------------------|-------------------------|----------------------|--------------|---------|
| File name C:/Users/ | ,/new_one.exe | | | | |
| File type | Entry point | | Base address | | MIME |
| PE64 👻 | 000000140019f04 | > Disasm | 00000014000000 | 0 Memory map | Hash |
| PE | Export | rt Resources | .NET TLS | Overlay | Strings |
| Sections | TimeDateStamp | SizeOfImage | Resources | | Entropy |
| 0008 > | 2022-07-03 19:46:58 | 00043000 | Manifes | t Version | |
| Scan | Endianne | ess Mode | Architecture | Туре | Hex |
| Detect It Easy(DiE) | ▼ LE | 64 | AMD64 | Console | |
| compiler | Microsoft | : Visual C/C++(2015 v. | 14.0)[-] | S | |
| linker | Microsoft Linker(14.0, V | isual Studio 2015 14.0* |)[Console64,console] | S ? | |
| | | | _ | | Options |
| Signatures | | | Deep scan | Scan | About |
| | 100% | | Log 280 msec | Jun | Exit |

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.

| | | <pre><&CreateToolhelp32Snapshot>]</pre> | JMP.&CreateToolhelp32Snapshot |
|-----|---------------|---|-------------------------------|
| jmp | qword ptr ds: | <&Process32FirstW>] | JMP.&Process32FirstW |
| jmp | qword ptr ds: | <&uaw_lstrcmpW> | JMP.&uaw_lstrcmpW |
| | | <&OpenProcess>] | JMP. &OpenProcess |
| jmp | gword ptr ds: | <&TerminateProcess>] | JMP.&TerminateProcess |
| jmp | qword ptr ds: | <ac seriand="" te="" to="">1</ac> | JMP.&CloseHandle |
| jmp | qword ptr ds: | <&Process32NextW>] | JMP.&Process32NextW |
| jmp | qword ptr ds: | <&lstrcpyw>] | JMP.&lstrcpyW |

Figure 4 – APIs used to Terminate Process Execution

A full list of hardcoded process names is shown in the below figure.

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.

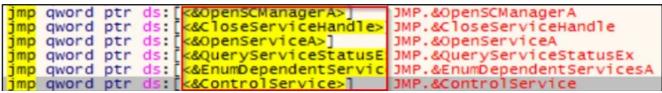


Figure 6 – Service-Related APIs

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()*.

| jmp | qword ptr ds: | | JMP.&GetDriveTypeW |
|-----|---------------|---|---------------------------------------|
| jmp | qword ptr ds: | <pre><&FindFirstVolumeW>]</pre> | JMP.&FindFirstVolumeW |
| | | | JMP.&GetVolumePathNamesForVolumeNameW |
| jmp | gword ptr ds: | <pre>[<&lstrlenW>]</pre> | JMP.&lstrlenW |
| jmp | gword ptr ds: | | JMP.&SetVolumeMountPointW |
| | | | JMP.&FindNextVolumeW |
| | | | JMP.&FindVolumeClose |

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.

| 00007FF98CF685ED 00007FF98CF685EF 00007FF98CF685EF 00007FF98CF685EF 00007FF98CF685E0 00007FF98CF68608 00007FF98CF68608 00007FF98CF68608 | 48:FF15 82681900 0F1F4400 00 88C8 3D 03010000 ~ 0F84 CE690700 88C9 ~ 0F88 87000000 48:85D8 ~ 74 06 | wor day, edw call qword ptr ds:[<&MtWrit hop dword ptr ds:[*Arrax], mov ecx, eax cmp eax,103 je kernelbase.7FF98CF08F06 test ecx,ecx js kernelbase.7FF98CF68618 mov eax dword ntr ss:[rspt] | eax | , , | CF 0 TF 0 IF 1 CF 0 TF 0 IF 1 Default (x64 fastcall) 1: rcx 0000000000000258 2: rdx 00007FF726439CF0 3: r8 00000026849F80C 5: [rsp+28] 00007FF7264 C |
|--|---|---|--|-------------|---|
| Ump 1 Ump 2 Ump 3 Ump 3 | 🗒 Dump 4 🛛 💭 Dump 5 💮 1 | Watch 1 [x=] Locals 2 Struct | 0000002C849FF710 0000002C849FF718 0000002C849FF720 | | |
| Noncost Noncost <t< th=""><th>5 73 20 68 61 76 65 20 62 27 70 74 65 64 20 61 6E 2 79 70 74 65 64 20 61 6E 2 10 70 74 65 64 20 61 6E 2 20 70 72 69 63 65 20 0 64 61 79 70 74 69 63 64 51 73 20 74 67 32 0 64 61 79 73 20 74 67 32 0 64 62 20 73 20 66 67 72 20 73 73 20 66 67 72 20 73 74 62 62 20 74 68 22 62 64 64 20 65 20 64</th><th>61 All your importa 65 nt files have be 64 en encrypted and 63 stolen!Contac 61 t us for price a 67 nd get decryptio 75 n softwareYou 20 have 3 days to 68 contact us for n 79 egotiationIf y 74 ou don't contact 61 within three da 20 vs. we'll start</th><th>0000002C849FF728</th><th>L"\\\\?\\C:</th><th>Restore_Your_Files.txt"</th></t<> | 5 73 20 68 61 76 65 20 62 27 70 74 65 64 20 61 6E 2 79 70 74 65 64 20 61 6E 2 10 70 74 65 64 20 61 6E 2 20 70 72 69 63 65 20 0 64 61 79 70 74 69 63 64 51 73 20 74 67 32 0 64 61 79 73 20 74 67 32 0 64 62 20 73 20 66 67 72 20 73 73 20 66 67 72 20 73 74 62 62 20 74 68 22 62 64 64 20 65 20 64 | 61 All your importa 65 nt files have be 64 en encrypted and 63 stolen!Contac 61 t us for price a 67 nd get decryptio 75 n softwareYou 20 have 3 days to 68 contact us for n 79 egotiationIf y 74 ou don't contact 61 within three da 20 vs. we'll start | 0000002C849FF728 | L"\\\\?\\C: | Restore_Your_Files.txt" |

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.

| \Restore_Your_Files.txt Restore_Your_Files.txt Windows Windows.old Tor Browser Internet Explorer Google Opera Opera Software Mozilla Mozilla Firefox \$Recycle.Bin ProgramData All Users autorun.inf | boot.ini bootfont.bin bootsect.bak bootmgr bootmgr.efi bootmgfw.efi desktop.ini iconcache.db ntldr ntuser.dat ntuser.dat ntuser.dat.log ntuser.ini thumbs.db ecdh_pub_k.bin Program Files (x86) | 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.

| SysAnalyzer_help.chm × | CPU Log | Notes 🔹 breakpoints 🚥 Memory Maj | p 📑 Call Stack 👒 SEH 🕑 Script 😕 Symbols | V Source Keterences |
|--|--------------------------------------|--|--|-----------------------|
| 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF | 00007FF72640CD90 | 48:8805 A98E0200 | mov rax, gword ptr ds: [7FF726435C40] | rax:"ITSF\x03", 00007 |
| 0000h: 49 54 53 46 03 00 C0 00 60 00 00 00 00 00 00 00 ITSF | 00007FF72640CD97 00007FF72640CD9E | 48:8880 A46322DA 89 74232854 | mov rax, qword ptr ds: [rax-2SDD9CSC] mov ecx, 54282374 | rax:"ITSF\x03" |
| 0010h: 05 38 5A 74 09 04 C0 00 10 FD 01 7C AA 7B D0 11 .8Ztý. *{B. | 00007FF72640CDA3 | 48:01C8 | add rax,rcx | rax:"ITSF\x03" |
| 0020h: 9E OC 00 A0 C9 22 E6 EC 11 FD 01 7C AA 7B D0 11 ž., É"æi.ý. *{B. | 00007FF72640CDA6 00007FF72640CDA8 | 48:884C24 60 48:8D9424 90000000 | mov rcx, gword ptr ss: rsp+60 | |
| 0030h: 9E OC 00 A0 C9 22 E6 EC 60 00 00 00 00 00 00 00 Ž., É*æ1' | 00007FF72640CD83 | FFDO | call rax | |
| 0040h: 18 00 00 00 00 00 00 78 00 00 00 00 00 00 00x | 0000777726400085 | 48:884424 48 889424 90000000 | mov rax, qword ptr ss: rsp+48 | [rsp+48]:"ITSF\x03" |
| 0050h: 54 10 00 00 00 00 00 CC 10 00 00 00 00 00 00 TÌ | 00007FF72640CDBA 00007FF72640CDC1 | 3310 | mov edx, dword ptr ss: rsp+90 xor edx, dword ptr ds: [rax] | rax: "ITSF\x03" |
| 20060h: FE 01 00 00 00 00 00 FD 3A OF 00 00 00 00 0 pý: | 00007FF72640CDC3 | 48:884C24 40 | mov rcx.gword ptr ss: rsp+40 | [rsp+40]:"ITSF\x03" |
| 0070h: 00 00 00 00 00 00 00 00 49 54 53 50 01 00 00 00 | 00007FF72640CDC8 00007FF72640CDCA | 8911 889424 94000000 | mov dword ptr ds:[rcx],edx mov edx,dword ptr ss:[rsp+94] | |
| 0080h: 54 00 00 00 0A 00 CO 00 00 10 00 00 02 00 00 00 T | 00007FF72640CDD1 | 3350 04 | <pre>xor edx, dword ptr ds:[rax+4]</pre> | |
| 0090h: 01 00 00 00 FF FF FF FF 00 00 00 00 00 00 | 00007FF72640CDD4 00007FF72640CDD7 | 8951 04 889424 98000000 | mov dword ptr ds:[rcx+4],edx | |
| 00ADh: FF FF FF FF 01 00 C0 00 09 04 00 00 6A 92 02 5D yyyyj'.] | 00007FF72640CDD2 | 3350 08 | <pre>mov edx,dword ptr ss:[rsp+98] xor edx,dword ptr ds:[rax+8]</pre> | |
| 0080h: 2E 21 DO 11 9D F9 CO AO C9 22 E6 EC 54 00 00 00 .10u. E"#iT | 00007FF72640CDE1 | 8951 08 | mov dword ptr ds:[rcx+8],edx | |
| DOCDH: FF 50 4D 47 4C 99999999999999990 | 00007FF72640CDE4 00007FF72640CDEB | 889424 9C000000 3350 0C | <pre>mov edx,dword ptr ss:[rsp+9C] xor edx,dword ptr ds:[rax+C]</pre> | |
| 00DDh: F6 0A 00 00 00 00 00 00 FF FF FF FF FF FF FF | 00007FF72640CDEE | 8951 OC | mov dword ptr ds:[rcx+C],edx | |
| 00EDh: 01 2F 00 00 00 08 2F 23 49 44 58 48 44 52 01 C1 .//#IDXHDR.A | 00007FF72640CDF1 00007FF72640CDF8 | 8B9424 A0000000 3350 10 | <pre>mov edx,dword ptr ss:[rsp+A0] xor edx,dword ptr ds:[rax+10]</pre> | |
| 00F0h: F2 28 A0 00 08 2F 23 49 54 42 49 54 53 00 00 00 ô(/#ITBITS | 00007FF72640CDF8 | 8951 10 | mov dword ptr ds:[rcx+10],edx | |
| 0100h: 09 2F 23 53 54 52 49 4E 47 53 01 C2 97 03 16 08 ./#STRINGS.Â | 00007FF72640CDFE | 889424 A4000000 | mov edx, dword ptr ss: rsp+A4 | |
| 0110h: 2F 23 53 59 53 54 45 4D 00 83 3E A1 1B 08 2F 23 /#SYSTEM.j>j/# | 00007FFF2640CE05 00007F792640CE08 | 3350 14 8951 14 | <pre>xor edx,dword ptr ds:[rax+14] mov dword ptr ds:[rcx+14].edx</pre> | |
| 0120h: 54 4F 50 49 43 53 C1 C2 92 28 81 40 08 2F 23 55 TOPICS.Å'(.@./#U | 00007FF72640CE0B | 8B9424 A8000000 | mov edx, dword ptr ss: [rsp+A8] | |
| 01301: 52 4C 53 54 52 01 C2 94 78 82 08 08 2F 23 55 52 RL51K.A.X/#UK | 00007FF72640CE12 | 3350 18 8951 18 | <pre>xor edx,dword ptr ds:[rax+18]</pre> | |
| 0140h: 4C 54 42 4C 01 C2 93 68 81 10 0B 2F 24 46 49 66 LTBL.Â"h/\$FIF | 00007FF72640CE15 00007FF72640CE18 | 8951 18 889424 AC000000 | mov dword ptr ds:[rcx+18],edx mov edx,dword ptr ss:[rsp+AC] | |
| 0150h: 74 69 4D 61 69 6E C1 00 00 09 2F 24 4F 42 4A 49 tiMain/\$OBJI | 00007FF72640CE1F | 3350 1C | xor edx, dword ptr ds:[rax+1C] | |
| 0160h: 4E 53 54 01 C1 DC 69 95 3F 15 2F 24 57 57 41 73 NST.AUI.?./\$WWAs | 00007FF72640CE22 00007FF72640CE25 | 8951 1C 889424 80000000 | mov dword ptr ds:[rcx+1C],edx mov edx,dword ptr ss:[rsp+80] | |
| (0170h: 73 6F 63 69 61 74 69 76 65 4C 69 6E 6B 73 2F 00 sociativeLinks/. | 0000755736405536 | 2250 20 | I YOF BAY AGAIN ATT ATTERVING | |
| 0180h: 00 00 1D 2F 24 57 57 41 73 73 6F 63 69 61 74 69/\$WWAssociati | < | | | |
| 0190h: 76 65 4C 69 6E 6B 73 2F 50 72 6F 70 65 72 74 79 veLinks/Property | edx=A5520E58 | 00016311193040 "ITSF\x03"]=465354 | 14 | |
| 01ADh: 01 C1 DC 65 04 11 2F 24 57 57 48 65 79 77 6F 72 .AUe/SwWiKeywor | umord per ds:[rax]=[00 | 00016311133040 1138/X03]#465354 | 142 | |
| 01BDh: 64 4C 69 6E 6B 73 2F 00 00 00 19 2F 24 57 57 4B dLinks//\$WWK | .text:00007FF72640CDC1 | new_one.exe:\$CDC1 #C1C1 | | |
| 01CDh: 65 79 77 6F 72 64 4C 69 6E 6B 73 2F 50 72 6F 70 eywordLinks/Prop | | | | |
| 01DDh: 65 72 74 79 01 C1 DC 61 04 0F 2F 41 70 69 4C 6F erty.AUa/ApiLo | Dump 1 Dump 2 | Dump 3 💭 Dump 4 💭 Dump 5 | 5 👹 Watch 1 🛛 🕸 Locals 🎾 Struct | 1000 |
| 01E0h: 67 67 65 72 2E 68 74 6D 6C 01 00 95 0A 0D 2F 63 gger.html/c 01F0h: 6D 64 6C 69 6E 65 2E 68 74 6D 6C 01 81 A8 75 85 mdline.htmlu. | Address | Hex | ASCII | 000 |
| 0200h: 59 10 2F 68 65 6C 70 76 69 64 65 6F 73 2E 68 74 Y./helpvideos.ht | 0000016311193040 | 12 5A 01 E3 DA 1E 2E B5 EE 05 | 88 42 18 EA 20 20 .Z.ã0µî8.ê- | 000 |
| 0210h: 6D 6C 01 81 9F 48 89 2A 05 2F 69 6D 67 2F 00 00 ml. YKk*./img/ | 0000016311193050 0000016311193060 | DE AB D8 68 CC B7 E6 C1 80 BF | 58 A9 0A AD 89 5D D≪0h1 zA.¿X0] 8C 90 85 8F A3 9F 0D → .xyKµ¿£. | 000 |
| : 0220h: 00 0F 2F 69 6D 67 2F 61 70 69 6C 6F 67 2E 70 6E/img/apilog.pn | 0000016311193070 | 79 76 A0 29 C0 07 9C 58 41 F8 | E0 68 16 28 OF B1 VV)A XHOAK +. ± | 000 |
| 0230h: 67 01 84 F4 02 81 C8 54 10 2F 69 6D 67 2F 63 6D g., o ET./img/apilog.pm | 0000016311193080 | 18 00 00 00 00 00 00 00 78 00 | 00 00 00 00 00 00 00x | s Encrypting |
| 0240h: 64 6C 69 6E 65 2E 70 6E 67 01 C1 87 57 D0 33 15 dline.png.ŇWD3. | 0000016311193090 00000163111930A0 | FE 01 00 00 00 00 00 00 FD 3A | OF 00 00 00 00 00 bý: | 000 |
| 0250h: 2F 69 6D 67 2F 6C 61 62 73 5F 62 61 6E 6E 65 72 /img/labs banner | 0000016311193080 | 00 00 00 00 00 00 00 00 49 54 | 53 50 01 00 00 00ITSP | 000 |
| 0260h: 00 00 00 00 00 00 00 00 00 00 00 00 00 | 00000163111930C0 00000163111930D0 | | 00 00 02 00 00 00 T | 000 |
| 0270h: 00 00 00 00 00 00 00 00 00 00 00 00 00 | 00000163111930E0 | FF FF FF FF 01 00 00 00 09 04 | 00 00 6A 92 02 5D yyyyj] | 000 |
| fradhauk. | 00000163111930F0 0000016311193100 | 2E 21 D0 11 90 F9 00 A0 C9 22 | E6 EC 54 00 00 00 .10u. E"æ1T FF FF 50 4D 47 4C yyyyyyyyyyyyy | 000 |
| Find Results | 0000016311193100 | F6 0A 00 00 00 00 00 00 FF FF | FF FF FF FF FF FF FF 0 | 000 |
| Address Value | 0000016311193120 | 01 2F 00 00 00 08 2F 23 49 44 | 58 48 44 52 01 C1 .//#IDXHDR.A | 000 |
| | 0000016311193130 0000016311193140 | P2 28 A0 00 08 2F 23 49 54 42 09 2F 23 53 54 52 49 4E 47 53 | 49 54 53 00 00 00 0(/#ITBITS 01 C2 97 03 16 08 ./#STRINGS.Å | 000 |
| | 0000016311193150 | 2F 23 53 59 53 54 45 40 00 83 | 3E A1 18 08 2F 23 /#SYSTEM>j/# | 000 |
| | 0000016311193160 | 54 4F 50 49 43 53 01 C2 92 28 | 81 40 08 2F 23 55 TOPICS. A. (.@. /#U | 000 |

Figure 10 – Encryption Routine

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

| Chown_files.mdb x Crigunal File 0 - 1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - A - B - C - 0 - E - 6 (123456789A8CDEF 0000h: 00 - 00 - 00 - 53 - 74 - 61 - 6E - 64 - 61 - 72 - 64 - 20 - 4A - 65 - 74 - 0standard Jet 0010h: 20 - 44 - 42 - 00 - 00 - 00 - 00 - 00 - | CU Jtog Notes Breakponts Memory Map Cal Stack SCPt Symbols Source References Threads Memory Map 000 100 quord ptr dt: (dicretter)lest JMP.Adertilettributesw JMP.Adertilettributesw JMP.Adertilettributesw Memory Map |
|---|---|
| 0C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 | Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Weath 1 Imiliaria Products Produ |

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.

| 00007FF726419826 jmp qword ptr ds:[<cdistrcates]< td=""> JMP.&WaitForSingleObject 00007FF726419826 jmp qword ptr ds:[<cdistrcates]< td=""> JMP.&lstrcate 00007FF726419826 jmp qword ptr ds:[<cdistrcates]< td=""> JMP.&lstrcate 00007FF726419836 jmp qword ptr ds:[<cdistrcates]< td=""> JMP.&lstrcate 00007FF726419836 jmp qword ptr ds:[<cdistrlers]< td=""> JMP.&lstrlere 00007FF726419836 jmp qword ptr ds:[<cdistrlers]< td=""> JMP.&Gistrlere 00007FF7264198364 jmp qword ptr ds:[<cdistrleres]< td=""> JMP.&Gistrlere 00007FF726419844 jmp qword ptr ds:[<cdistrleres]< td=""> JMP.&Gistrlere 00007FF726419844 jmp qword ptr ds:[<cdistrleres]< td=""> JMP.&Gistrlere 00007FF726419844 jmp qword ptr ds:[<cdistrleres]< td=""> JMP.&Gistrleres] 00007FF726419844 jmp qword ptr ds:[<cdistrleres]< td=""> JMP.&Gistrleres] 00007FF726428008 science: jmP.&Single: qword ptr ds:[00007FF726428008 <new_one.&movefileexw>]=<kernel32.movefileexw></kernel32.movefileexw></new_one.&movefileexw></cdistrleres]<></cdistrleres]<></cdistrleres]<></cdistrleres]<></cdistrleres]<></cdistrlers]<></cdistrlers]<></cdistrcates]<></cdistrcates]<></cdistrcates]<></cdistrcates]<> | <pre>C Default (x64 fastcal) 1: rcx 00001630EED01F0 L"\\\\?\\C:\\ 2: rdx 000001630ED98F80 L"\\\?\\C:\\ 3: r8 00000000000000000000000000000000000</pre> |
|--|--|
|--|--|

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 | Туре | Size |
|----------------------------|------------------|-------------|-------|
| abstract.r.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.

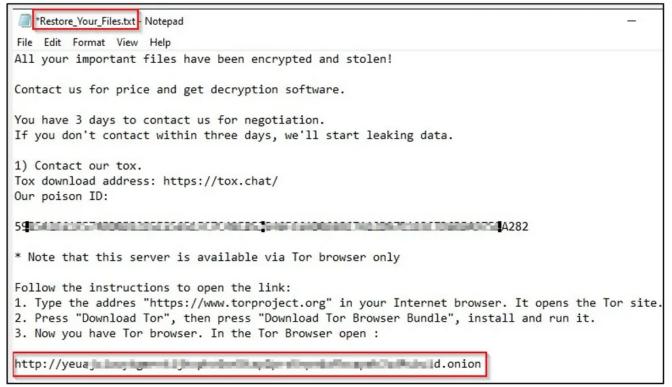


Figure 14 – Ransom Note

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

| | Lilith | × + | 7 | - | | х |
|---|-----------------|--|---|---|----|---|
| ÷ | \rightarrow C | yeu and a state of the state of | ☆ | 0 | ₩. | ≡ |
| | Г | ₩ LILITH | | | | |
| | | | | | | |
| | | CCR Group | | | | |
| | | ◎ 2022-07-04 🛛 | | | | |
| | | | | | | |

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 Omega 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

| Execution | <u>T1204</u> | User Execution |
|-----------------|--|--|
| Discovery | <u>T1012</u> <u>T1082</u> <u>T1083</u> | Query Registry System Information Discovery File and Directory Discovery |
| Defense Evasion | <u>T1027</u> | Obfuscated Files or Information |
| Impact | <u>T1486</u> | 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) |