SUBEX

Three of a kind - Solaso Ransomware

Date: 18/01/2021

Shyava Tripathi

COVID-19 introduced a whole new set of concerns for humankind, a whole new system of lifestyle, and made the past year probably the most difficult year of our lives. However, relief seems right on the horizon with mass vaccinations initiating around the world with the beginning of this year. 2020 was strenuous for global cyber frameworks as well with ransomware topping the malware leaderboards, and while 2021 brings new hope for humanity's well-being, ransomwares are far from being mitigated this coming year.
According to Cybersecurity Ventures' Cybercrime magazine's predictions, there will be a ransomware attack every 11 seconds in 2021. Moreover, the global cost associated with ransomware recovery will exceed $20 billion in 2021. The credit for this ballooning in ransomware attacks must be given where it is due, to the big game malware families and entry-level attackers alike. The fast-food approach of spamming substantial volumes of targets with cheapjack routine malware even though is duck soup to detect, it is just as unchallenging to deploy and circulate. By savaging numerous targets in one go, even a fraction of wins can still lead to an expansive number of victims and compromised entry points.

Launched at the beginning of this month, the new Solaso ransomware is one such malware, targeting and entrapping its victims with its three variants. First seen by 0x4143 (Twitter Handle), the ransomware performs offline encryption using AES & RSA standards.

Overview

The encryption and operational code of Solaso is strongly based on the previously known Encrp ransomware. A gene code analysis from Intezer (Figure 1) reveals near about 69% code similarity between Solaso and Encrp samples.

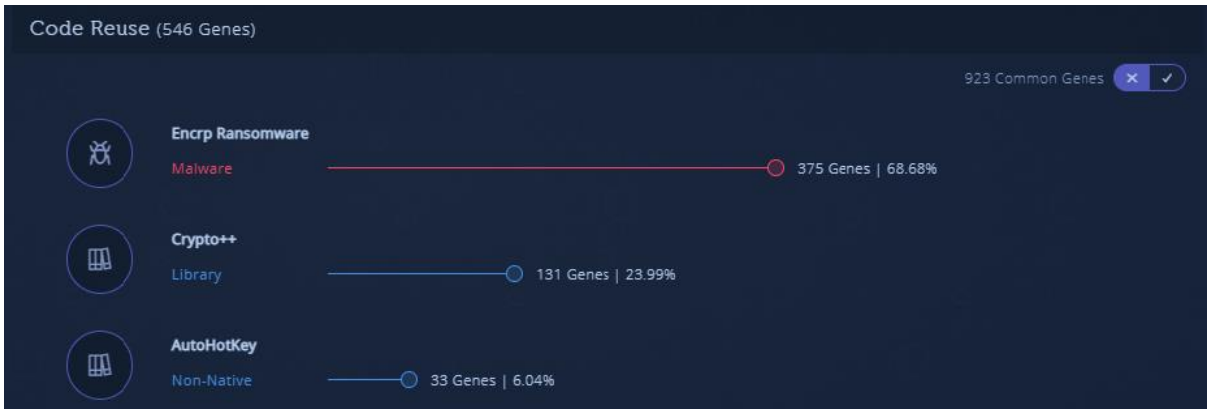

Figure 1: Code Reuse Similarity – Intezer

Variants

Although dubbed Solaso (by 0x4143), based on the extension the ransomware appends to the encrypted file, samples using two more extensions have been encountered. The extensions used by the three variants are listed below.

Variant – 1	.solaso
Variant – 2	.soli
Variant – 3	.inut

Encryption

To encrypt the target files, all Solaso variants use two encryption algorithms: AES-128 and RSA. The AES – 128-bit algorithm is used to encrypt the target files and RSA is used to encrypt the generated AES key. Solaso implements Crypto ++ library for encryption which enables AES new instruction set.

AES encryption is implemented using AESENC, AESENCLAST & AESKEYGENASSIST instructions (Figure 2). The opcode instruction AESKEYGENASSIST is used for AES round key generation (Figure 2.A). Each round of encryption for target files is carried out by AESENC instruction (Figure 2.B) followed by AESENCLAST instruction performing the last round of encryption (Figure 2.C).

```
                        ; CODE XREF: sub_14001A1E0+DD↑j
mov     rsi, rbp
mov     rcx, rdi
cmp     cs:byte_140073F8E, 0
jz      loc_14001A4BA
movdqu  xmm6, xmmword ptr [r11+rbp-10h]
mov     r8, rbp
mov     rdx, r11
call    sub_140024840
aeskeygenassist xmm0, xmm6, 0
pextrd  eax, xmm0, 3
xor     eax, [rdi]
xor     eax, 1
shr     rsi, 2
lea     rsi, ds:0[rsi*4]
lea     r9, [rsi+rdi]
mov     [r9], eax
lea     r10, unk_1400629D4
mov     edx, [rdi+4]
xor     edx, eax
lea     eax, [r15+1]
lea     r11, ds:0[rax*4]
mov     [r11+rdi], edx
mov     r8d, [rdi+8]
xor     r8d, edx
lea     eax, [r15+2]
lea     r14, ds:0[rax*4]
mov     [r14+rdi], r8d
lea     eax, [r15+3]
lea     r15, ds:0[rax*4]
mov     eax, [rdi+0Ch]
xor     eax, r8d
mov     [r15+rdi], eax
mov     rcx, [rbx+128h]
mov     rax, [rbx+130h]
lea     rdx, [rax+rcx*4]
```

```
CODE XREF: sub_14001B520+A6↓j
movdqu  xmm2, xmmword ptr [rcx]
lea     rcx, [rcx+10h]
movdqu  xmm0, xmmword ptr [r10]
aesenc  xmm0, xmm2
movdqu  xmmword ptr [r10], xmm0
movdqu  xmm1, xmmword ptr [rdx]
aesenc  xmm1, xmm2
movdqu  xmmword ptr [rdx], xmm1
movdqu  xmm0, xmmword ptr [r8]
aesenc  xmm0, xmm2
movdqu  xmmword ptr [r8], xmm0
movdqu  xmm1, xmmword ptr [r9]
aesenc  xmm1, xmm2
movdqu  xmmword ptr [r9], xmm1
sub     r11, 1
jnz     short loc_14001B580
```

```
CODE XREF: sub_14001B520+51↑j
movdqu  xmm0, xmmword ptr [r10]
mov     rax, rdi
mov     rdi, [rsp+arg_8]
add     rax, rax
movdqu  xmm2, xmmword ptr [rbx+rax*8]
mov     rbx, [rsp+arg_0]
aesenclast xmm0, xmm2
movdqu  xmmword ptr [r10], xmm0
movdqu  xmm1, xmmword ptr [rdx]
aesenclast xmm1, xmm2
movdqu  xmmword ptr [rdx], xmm1
movdqu  xmm0, xmmword ptr [r8]
aesenclast xmm0, xmm2
movdqu  xmmword ptr [r8], xmm0
movdqu  xmm1, xmmword ptr [r9]
aesenclast xmm1, xmm2
movdqu  xmmword ptr [r9], xmm1
```

Figure 2: (A) AESKEYGENASSIST Function, (B) AESENC Function, (C) AESENCLAST Function

The generated AES key is further encrypted with a hardcoded RSA key (Figure 3).

```
nop
lea     r8d, [r12+16h]
lea     rdx, aTRkeTlrke65409 ; "t;rke;tlrke65409654ytr"
lea     rcx, [rbp+1C0h+var_200]
call    sub_140002140
lea     rax, [rbp+1C0h+var_200]
mov     rdx, [rbp+1C0h+var_200]
cmp     [rbp+1C0h+var_1E8], 10h
cmovnb  rax, rdx
movzx   eax, byte ptr [rax]
mov     [rbp+1C0h+var_40], al
lea     rax, [rbp+1C0h+var_200]
cmovnb  rax, rdx
movzx   eax, byte ptr [rax+1]
mov     [rbp+1C0h+var_3F], al
lea     rax, [rbp+1C0h+var_200]
cmovnb  rax, rdx
movzx   eax, byte ptr [rax+2]
mov     [rbp+1C0h+var_3E], al
lea     rax, [rbp+1C0h+var_200]
cmovnb  rax, rdx
movzx   eax, byte ptr [rax+3]
mov     [rbp+1C0h+var_3D], al
lea     rax, [rbp+1C0h+var_200]
cmovnb  rax, rdx
movzx   eax, byte ptr [rax+4]
mov     [rbp+1C0h+var_3C], al
lea     rax, [rbp+1C0h+var_200]
cmovnb  rax, rdx
movzx   eax, byte ptr [rax+5]
mov     [rbp+1C0h+var_3B], al
lea     rax, [rbp+1C0h+var_200]
```

Figure 3: Generated AES key is encrypted using a hardcoded RSA Key

Target Files

The ransomware contains capability to target multiple file types including Microsoft Office files, image files, database files, archive files, etc (Figure 4).

```
mov     rax, cs:__security_cookie
xor     rax, rsp
mov     [rbp+4Fh+var_10], rax
mov     rdi, rcx
xorps   xmm0, xmm0
xor     eax, eax
movups  [rbp+4Fh+var_A0], xmm0
movups  [rbp+4Fh+var_90], xmm0
movups  [rbp+4Fh+var_70], xmm0
movups  [rbp+4Fh+var_60], xmm0
movups  [rbp+4Fh+var_50], xmm0
movups  [rbp+4Fh+var_40], xmm0
movups  [rbp+4Fh+var_30], xmm0
mov     [rbp+4Fh+var_20], rax
lea     rbx, [rcx+8]
lea     rax, aExeMsiDocDocxX ; "\\.(?:exe|msi|doc|docx|xls|xlsx|xlsm|pp"...
mov     qword ptr [rbp+4Fh+var_A0], rax
mov     qword ptr [rbp+4Fh+var_A0+8], rax
mov     qword ptr [rbp+4Fh+var_90], r8
xor     esi, esi
mov     qword ptr [rbp+4Fh+var_90+8], rsi
lea     rax, [rbp+4Fh+var_80]
mov     [rbp+4Fh+var_B0], rax
movdqa  [rbp+4Fh+var_80], xmm0
mov     qword ptr [rbp+4Fh+var_70], rsi
mov     qword ptr [rbp+4Fh+var_70+8], rsi
xor     edx, edx
lea     rcx, [rbp+4Fh+var_80]
call    sub_14000FC70
nop
lea     ecx, [rsi+30h]  ; unsigned __int64

aExeMsiDocDocxX db '\.(?:exe|msi|doc|docx|xls|xlsx|xlsm|ppt|pdf|jpg|jpeg|png|rar|7z|z'
                                        ; DATA XREF: sub_14000E3D0+56↑o
                db 'ip|bdf|fmp12|db|mdb|itdb|dbf|pdb|wdb|edb|mdb|db3|ddl|frm|sql|sqli'
                db 'te|dbc|dbs|bkf|mp3|mp4|mkv|avi|wave|iso|pptx|ppt|pptm|EXE|MSI|DOC'
                db '|DOCX|XLS|XLSX|XLSM|PPT|PDF|JPG|JPEG|PNG|RAR|ZIP|BDF|FMP12|DB|MDB'
                db '|ITDB|DBF|PDB|WDB|EDB|MDB|DB3|DDL|FRM|SQL|SQLITE|DBC|DBS|BKF|MP3|'
                db 'MP4|MKV|AVI|WAVE|ISO|PPTX|PPT|PPTM|html|htm|js|jse|php|xml|xsl|bi'
                db 'n|vbs|max|psd|aep|sln|cpp|h|vhd|VHD|bak|BAK|vmdk|VMDK|vmsn|VMSN|T'
                db 'IB|MDF|mdf|tib)',0
```

Figure 4:File Types targeted

The ransomware encrypts files stored in Documents (Figure 5), Pictures, Music, Downloads, Videos and Desktop folders in the specified order.

```
                        ; CODE XREF: main+279↑j
movups  xmm0, [rbp+4F0h+var_500]
movups  cs:xmmword_14006FC18, xmm0
movups  xmm1, xmmword ptr [rbp+0]
movups  cs:xmmword_14006FC28, xmm1
mov     [rbp+4F0h+var_4E8], 0Fh
mov     byte ptr [rbp+4F0h+var_500], 0
lea     r14, xmmword_14006FC18
mov     rdx, r14
movq    rcx, xmm0
movdqa  xmm0, xmm1
psrldq  xmm0, 8
movq    rax, xmm0
cmp     rax, 10h
cmovnb  rdx, rcx
movq    r8, xmm1
lea     rcx, off_14006F010
call    sub_140003070
mov     rcx, rax
call    sub_14000D720
call    cs:GetConsoleWindow
mov     rcx, rax        ; hWnd
xor     edx, edx        ; nCmdShow
call    cs:ShowWindow
lea     rcx, aUserprofile ; "USERPROFILE"
call    sub_1400334F0
mov     cs:qword_140073D80, rax
mov     r8d, 0Bh
lea     rdx, aDocuments ; "/Documents/"
lea     rsi, qword_14006FC38
mov     rcx, rsi
call    sub_140001FC0
mov     [rbp+4F0h+var_250], r12
mov     [rbp+4F0h+var_248], 0Fh
mov     [rbp+4F0h+var_260], 0
mov     rbx, cs:qword_140073D80
```

Figure 5: Function encrypting files stored in Documents Folder

The extensions .solaso (Figure 6.A), .soli (Figure 6.B) and .inut (Figure 6.C) are appended by the respective variants to the encrypted target files.

```
                        ; CODE XREF: main+9DD↑j
mov     edx, 80h ; '€'  ; dwFileAttributes
call    cs:SetFileAttributesW
mov     r8d, 7
lea     rdx, aSolaso    ; ".solaso"
lea     rcx, [rbp+4F0h+var_3D0]
call    sub_140002140
lea     rax, [rbp+4F0h+var_520]
mov     [rbp+4F0h+var_4A8], rax
mov     [rbp+4F0h+var_510], r12
mov     [rbp+4F0h+var_508], r12
mov     rsi, [rbp+4F0h+var_3C0]
lea     r14, [rbp+4F0h+var_3D0]
cmp     [rbp+4F0h+var_3B8], 10h
cmovnb  r14, [rbp+4F0h+var_3D0]
cmp     rsi, 10h
jnb     short loc_1400095AC
movups  xmm0, xmmword ptr [r14]
movups  [rbp+4F0h+var_520], xmm0
mov     [rbp+4F0h+var_508], 0Fh
jmp     short loc_140009622
```

```
                        ; CODE XREF: main+88D↑j
mov     edx, 80h ; '€'  ; dwFileAttributes
call    cs:SetFileAttributesW
mov     r8d, 5
lea     rdx, aSoli      ; ".soli"
lea     rcx, [rbp+10E0h+var_500]
call    sub_1400021D0
lea     rax, [rbp+10E0h+var_FD0]
mov     [rsp+11E0h+var_1178], rax
mov     [rbp+10E0h+var_FC0], r13
mov     [rbp+10E0h+var_FB8], r13
mov     rsi, [rbp+10E0h+var_4F0]
lea     r14, [rbp+10E0h+var_500]
cmp     [rbp+10E0h+var_4E8], 10h
cmovnb  r14, [rbp+10E0h+var_500]
cmp     rsi, 10h
jnb     short loc_1400098CF
movups  xmm0, xmmword ptr [r14]
movups  [rbp+10E0h+var_FD0], xmm0
mov     [rbp+10E0h+var_FB8], 0Fh
jmp     loc_140009955
```

(A)Function appending .solaso extension (B)Function appending .soli extension

```
                        ; CODE XREF: main+C2B↓j
lea     rdx, [rbp+4E0h+Memory]
mov     rcx, r12
call    sub_140006720
nop
mov     [rbp+4E0h+var_3B0], r15
mov     [rbp+4E0h+var_3A8], 0Fh
mov     byte ptr [rbp+4E0h+var_3C0], 0
lea     rdx, [rbp+4E0h+Memory]
cmp     [rbp+4E0h+var_3C8], 10h
cmovnb  rdx, [rbp+4E0h+Memory]
mov     r8, [rbp+4E0h+var_3D0]
lea     rcx, [rbp+4E0h+var_3C0]
call    sub_140001FC0
mov     r8d, 5
lea     rdx, aInut      ; ".inut"
lea     rcx, [rbp+4E0h+var_3C0]
call    sub_140002140
lea     rax, [rbp+4E0h+var_530]
mov     [rbp+4E0h+var_498], rax
mov     [rbp+4E0h+var_520], r15
mov     [rbp+4E0h+var_518], r15
mov     rdi, [rbp+4E0h+var_3B0]
lea     rsi, [rbp+4E0h+var_3C0]
cmp     [rbp+4E0h+var_3A8], 10h
cmovnb  rsi, [rbp+4E0h+var_3C0]
cmp     rdi, 10h
jnb     short loc_140009061
movups  xmm0, xmmword ptr [rsi]
movups  [rbp+4E0h+var_530], xmm0
mov     [rbp+4E0h+var_518], 0Fh
jmp     short loc_1400090D7
```

Figure 6: (C)Function appending .inut extension

Upon encryption, a text file containing the ransom note is created and dropped in all six target folders. The name of the dropped ransom file varies between '__READ_ME_PLEASE.txt__' and __READ_ME_TO_RECOVER_YOUR_FILES.txt'. The attacker demands a ransom of 50 USD. Since the ransomware performs offline encryption, the ransom note contains the address of a Bitcoin wallet and the attacker's email ID. The victim is instructed to deposit the ransom amount to the mentioned Bitcoin wallet and notify the attacker with the infected computer ID on the specified email address (Figure 7).

```
_READ_ME_PLEASE.txt_
Hello, you cant open your files.
The only way to open and use your files again is using a tool that only we have.
In order for us to send you the tool, you will have to make a transfer of Bitcoins
to an electronic wallet. We leave you here the data to make the bitcoins transfer.

Bitcoin wallet: 3QtbAioBSw249J5xsGd1sCqTqhdDX4CD9L
Transfer the amount of bitcoins equivalent to 50 USD.

ID is:

Once you make the transfer of bitcoins, send us the transfer ID and your computer ID to our email: sammy70p_y61m@buxod.com
When we verify the transfer we will send you the tool.
```

Figure 7:Ransom note dropped by Solaso

The function in Figure 8 depicts the function used to create and drop the ransom note.

```
nop
mov     qword ptr [rsp+1A0h+var_168], rdi
mov     qword ptr [rsp+1A0h+var_168+8], 0Fh
mov     byte ptr [rsp+1A0h+var_178], dil
mov     [rsp+1A0h+var_180], 5
mov     rdx, qword ptr cs:xmmword_14006FC08
add     rdx, 17h
lea     rcx, [rsp+1A0h+var_178]
call    sub_14000D050
lea     rdx, xmmword_14006FBF8
cmp     qword ptr cs:xmmword_14006FC08+8, 10h
cmovnb  rdx, qword ptr cs:xmmword_14006FBF8
mov     r8, qword ptr cs:xmmword_14006FC08
lea     rcx, [rsp+1A0h+var_178]
call    sub_140002140
lea     r8d, [rdi+17h]
lea     rdx, aReadMePleaseTx ; "\\__READ_ME_PLEASE.txt__"
lea     rcx, [rsp+1A0h+var_178]
call    sub_140002140
lea     rdx, [rsp+1A0h+var_178]
cmp     qword ptr [rsp+1A0h+var_168+8], 10h
cmovnb  rdx, qword ptr [rsp+1A0h+var_178]
mov     esi, 2
mov     r8d, esi
lea     rcx, [rsp+1A0h+var_128]
call    sub_14000D1F0
lea     ebx, [rdi+6]
test    rax, rax
mov     rax, [rsp+1A0h+var_130]
movsxd  rcx, dword ptr [rax+4]
lea     rcx, [rsp+rcx+1A0h+var_130]
jz      short loc_14000880B
mov     edx, 4
cmp     [rcx+48h], rdi
cmovnz  edx, edi
jmp     short loc_140008818
```

Figure 8: Function creating and dropping the ransom note

SubexSecure Protection

SubexSecure detects the three Solaso ransomware variants as 'SS_Gen_Solaso_A', 'SS_Gen_Solaso_B' and 'SS_Gen_Solaso_C'.

IOCs

.solaso	5b9f7b8e99b1b5e79c3e12e6e326c968d8ba8370a607ca6e4c3fc7c566c02c95
	bd136b3fde933505cf3740c3800a5007e3a94a2d31f28416b04c212dcb0669b6
	3ff97721c26cc0b6f86f657ce63408ffa1cba6c99341b415648ca083a2888936
	39969192ff49975ebb38270c2f7abe4e2c512f3f045516c59e32336ea9ddf806
	eda2f2134bb8e3f9f8d6c634e472add222bff3ea3c655614d6732698ae1a8253
	2fe67494cf7595642b653e5e3440fd9f452b76c7159f925e0396d802405e8d86
	7b21d113e8ec02d640c4658f4865d4d3b45589290101562fa8977c7b7965b772
	69671f1478a22c839a6b0bed748be451ae60f78dd611860fcd2db2bee3706e01
	567ce33e7edc21568b400ddef4d0a367303175f85e4b77f781124ceb8174d206
	dc4cc89f03b3cdc1e694fede12d7b283f032da14c9cbc99cf4c5d7571a2cc0ac

.soli	881e22e5edee6732171de878b1ac89107fec3433e7b8b2de8b5ddc37bd9a6208

.inut	378ae4d290d37aaefa326893d9d3760437a1e6a807cce6f2e7448b3fefc7b699
	09375cc2becc3ccd6b3526e26f169953a23beddc4a4f62d3b603fd6e6eb9df76
	1478f2ee347359da9289122e768f4da5e214b5bd6b71020e2ee60e6f0bec4300
	d098c1907a154afce87d80b94fdf707b743cff96b69dbb45cbf703bbf1597c2c
	ce7ba3c41de77a0c4013f198f0aceb6f29f7a0c51a13023b4caa6504d3e6f8cf
	4138d076b2cc74351c62f5c643f9d4d55805f5bdfd8aaa81e7d2553fe8e7e7c8
	e5c1fc6c0ae625d8c20afcbe362a62ab14a30975b0b46fb467b54fc7cdbc72a3
	c676e7aa4c327234eefe5b06ccefea558ee9f1896e4e90e7f65f9c080d6d0216
	2a2e4eac37ff9216eff4e094f340b612e46adca8b35b17f66a4c1962490bad71
	da8100e396bc4b01aa0d6070af00a737f04bdc98254528e8ef08962c36ab7381
	3530ea48e6c38118fb6bb7ededcd1c4403ac01f6af85596bca405ea961bae774

Artefacts

File Name	ENCRIPTAR.exe
Compilation Date	2021-01-06
PDB Path	C:\Users\MARIO\source\repos\ENCRIPTAR\x64\Release\ENCRIPTAR.pdb
RSA Key	t;rke;tlrke65409654ytr
Email - ID	sammy70p_y61m@buxod.com
Bitcoin Wallet Address	3QtbAioBSw249J5xsGd1sCqTqhdDX4CD9L
Contained Sections	7
Section Names	.pdata
	_RDATA

Mitre Techniques

TACTIC	ID	TECHNIQUE
Execution	T1059.003	Command & Scripting Interpreter: Windows Command Shell
Execution	T1035	Service Execution
Execution	T1129	Shared Module
Persistence	T1060	Registry Run Keys / Start-up Folder
Persistence	T1179	Hooking
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1027.002	Obfuscated Files or Information: Software Packing
Defence Evasion	T1107	File Deletion
Defence Evasion	T1112	Modify Registry
Discovery	T1083	File and Directory Discovery
Discovery	T1012	Query Registry
Discovery	T1497	Virtualization/Sandbox Evasion
Impact	T1486	Data Encrypted for Impact
Impact	T1490	Inhibit System Recovery

OUR HONEYPOT NETWORK

This report has been prepared from threat intelligence gathered by our honeypot network that 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 are 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.