



SunCrypt Ransomware Gains New Capabilities in 2022

March 28, 2022 | Natalie Zargarov

SunCrypt is a RaaS (Ransomware as a Service) group that was first seen in October 2019, and was one of the first groups to apply triple extortion* tactics to their attacks. Unlike other RaaS groups, SunCrypt runs a small and closed affiliate program. The first version of this ransomware was written in GO, but after C and C++ versions were released in mid-2020, the group became much more active. SunCrypt mostly affects the Services, Technology, and Retail industries. Our researchers recently identified an updated version of this ransomware which includes additional capabilities.

SunCrypt often uses the PowerShell loader for delivery and deployment. Our sample was dropped by .zip file. This is not a very sophisticated or fast ransomware, but differs from others with its unique encryption routine which barely makes any use of the system API. Almost all of the API functions used by SunCrypt are statically imported, with a small number that are dynamically imported.

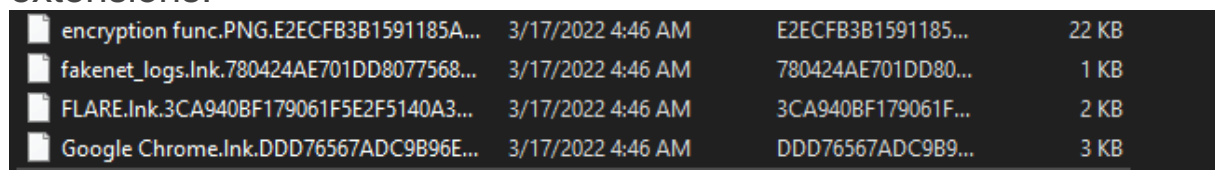
As in most ransomware cases, the encryption routine runs in several threads. It uses an I/O Completion Ports model to achieve faster encryption. According to Microsoft: “I/O completion ports provide an efficient threading model for processing multiple asynchronous I/O requests on a multiprocessor system. When a process creates an I/O completion port, the system creates an associated queue object for requests whose sole purpose is to service these requests. Processes that handle many concurrent asynchronous I/O requests can do so more quickly and efficiently by

using I/O completion ports in conjunction with a pre-allocated thread pool than by creating threads at the time they receive an I/O request.”

There are several files and directories that are whitelisted by SunCrypt:

1. Windows directory
2. \$Recycle.bin directory
3. System Volume Information directory
4. ntdetect.com
5. ntlldr
6. bootfont.bin
7. boot.ini
8. .exe extension files
9. .dll extension files
10. .ocx extension files
11. .sys extension files
12. AppData directory
13. Application Data directory
14. YOUR_FILES_ARE_ENCRYPTED.HTML – ransom note
15. Bootmgr directory
16. ..\Efi\microsoft\boot\bootmgr.efi file

Encrypted files are renamed to add random 64-byte hex string extensions:



encryption func.PNG.E2ECFB3B1591185A...	3/17/2022 4:46 AM	E2ECFB3B1591185...	22 KB
fakenet_logs.Ink.780424AE701DD8077568...	3/17/2022 4:46 AM	780424AE701DD80...	1 KB
FLARE.Ink.3CA940BF179061F5E2F5140A3...	3/17/2022 4:46 AM	3CA940BF179061F...	2 KB
Google Chrome.Ink.DDD76567ADC9B96E...	3/17/2022 4:46 AM	DDD76567ADC9B9...	3 KB

Figure 1 - Encrypted files

As its previous versions, SunCrypt encrypts the local volumes as well as found network shares. It also creates a “\Sessions\2\BaseNamedObjects\0c91c96fd7124f21a0193cf842e3495f6daf84a394f44013e92a87ad9d2ef4a0ceec9dd2e2eca22e” mutex on the infected machine.

New Capabilities

While the 2022 SunCrypt version has gained new capabilities, it seems like the ransomware is still under development. New capabilities allow the ransomware to terminate processes, stop services and clean the machine from any evidence of the ransomware execution. The ransomware also uses a winlogon.exe access token and sets it to its main thread by using **SetThreadToken** API call.

There also appears to be an Anti-VM feature that is not present in our sample but might be added in future versions. We noticed that 2022 version lacks C&C connection capabilities, while there is still an option to pass an argument that will stop the reporting to C&C. SunCrypt uses an undocumented "ProcessIOPriority" (0x21) information class to increase an I/O priority of the process to "High", which will to speed up its

```
execution: push 4
           push dword ptr [esi+14Ch]
           push 21h ; '!'
           push 0FFFFFFFFh
           call NtSetInformationProcess
```

Figure 2 - I/O priority setting

Process Termination:

SunCrypt terminates the following processes before initiating the encryption routine:

- Ocspd.exe
- Dbsnmp.exe
- Synctime.exe
- Agntsvc.exe
- Isqlplussvc.exe
- Xfssvcon.exe

- Mydesktopservice.exe
- Ocautoupds.exe
- Encsvc.exe
- Firefox.exe

- Tbirdconfig.exe
- Mydesktopqos.exe
- Ocomm.exe
- dbeng50.exe
- sqbcoreservice.exe
- excel.exe
- infopath.exe
- msaccess.exe
- mspub.exe
- onenote.exe
- outlook.exe
- powerpnt.exe
- steam.exe
- thebat.exe
- thunderbird.exe
- visio.exe
- winword.exe
- wordpad.exe
- ssms.exe
- notepad/notepad++.exe
- fdhost.exe
- fdlauncher.exe
- launchpad.exe
- sqlceip.exe
- sqlwriter.exe

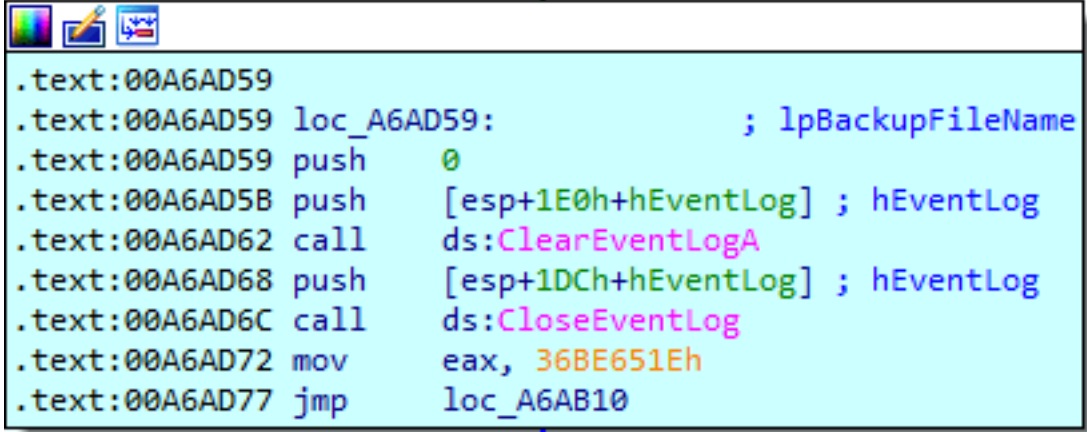
Service Stop:

While the service stopping code is present in our sample, it doesn't appear to be used. In addition, there is no service list to be stopped that is present in the sample.

Clean:

At the end of the encryption routine, SunCrypt clears the event log using **ClearEventLogA** and a combination

of **EvtOpenChannelEnum/EvtNextChannelPath/EvtClearLog** API calls. Just using one of these techniques is usually enough, as each of them works for different OS versions, but in our sample, the author decide to use both techniques irrespective of the OS version. After clearing the event log, the ransomware deletes itself from disk by executing cmd.exe with the following command: "cmd.exe /C ping 127.0.0.1 -n 10 > nul & del /f /q "path to the currently running process" >



```
.text:00A6AD59  
.text:00A6AD59 loc_A6AD59: ; lpBackupFileName  
.text:00A6AD59 push 0  
.text:00A6AD5B push [esp+1E0h+hEventLog] ; hEventLog  
.text:00A6AD62 call ds:ClearEventLogA  
.text:00A6AD68 push [esp+1DCh+hEventLog] ; hEventLog  
.text:00A6AD6C call ds:CloseEventLog  
.text:00A6AD72 mov eax, 36BE651Eh  
.text:00A6AD77 jmp loc_A6AB10
```

nul"

Figure 3 - Event Log Clear

Upon initial execution, the ransomware checks the command line arguments that were passes to the process. There are eight arguments that were defined by the ransomware authors in our version:

1. -noshares – if this argument is passed, the ransomware only encrypts local volumes.
2. -nomutex – in older versions, passing this parameter skips the mutex check, but in our version, it does not seem to affect the execution flow at all.
3. -noreport – based on older versions, if this argument is passed, the ransomware stops reporting to the C&C.
4. -noservices – apparenrly, if this argument passed, the ransomware does not stop services.
5. -vm – we do not know yet if this argument is supposed to activate or deactivate VM checks as we did not find any VM detection capabilities in our sample.
6. -path - if this argument is passed, the ransomware will only encrypt the files under a passed path.

7. -justcrypt – if this argument is passed, the ransomware does not terminate processes, duplicate winlogon.exe token, prioritize the running process and as we assume, stop services.
8. -keep_exe – if this argument is passed, the ransomware executable is not be deleted at the end of the flow.

```
aNoshares: ; DATA XREF: som
text "UTF-16LE", '-noshares',0
aNomutex: ; DATA XREF: som
text "UTF-16LE", '-nomutex',0
asc_F50032 db '-',0 ; DATA XREF: som
aNoreport:
text "UTF-16LE", 'noreport',0
asc_F50046 db '-',0 ; DATA XREF: som
aNoservices:
text "UTF-16LE", 'noservices',0
asc_F5005E db '-',0 ; DATA XREF: som
aVm:
text "UTF-16LE", 'vm',0
asc_F50066 db '-',0 ; DATA XREF: som
aPath:
text "UTF-16LE", 'path',0
asc_F50072 db '-',0 ; DATA XREF: som
aJustcrypt:
text "UTF-16LE", 'justcrypt',0
aKeepExe: ; DATA XREF: som
text "UTF-16LE", '-keep_exe',0
```

Figure 4 - Arguments that might be passed to the ransomware

SunCrypt, much like most ransomware groups nowadays, claims to exfiltrate victim data before encrypting it and offer the victim the option of uploading an encrypted file to prove decryption capabilities:

If you get this message, your network was hacked!

After we gained full access to your servers, we first downloaded a large amount of sensitive data and then encrypted all the data stored on them.

That includes personal information on your clients, partners, your personnel, accounting documents, and other crucial files that are necessary for your company to work normally.

We used modern complicated algorithms, so you or any recovery service will not be able to decrypt files without our help, wasting time on these attempts instead of negotiations can be fatal for your company.

Make sure to act within 72 hours or the negotiations will be considered failed!

Inform your superior management about what's going on, invite someone who is authorized to solve financial issues to our private chat. To get there you should download and install [TOR browser](#) and follow the link below:

<http://sttzxdr7uofos6f5koi644dv2xash7ope5x2yrat6fmhyvywigzc3eqd.onion/chat.html?2e1252bfd6-839caee5d3-d5d0502efec2a4b27b62-24dce843c8-017ebce84f-c873e9958a-f2a5b7619e>

If you and us succeed the negotiations we will grant you:

- complete confidentiality, we will keep in secret any information regarding to attack, your company will act as if nothing had happened.
- comprehensive information about vulnerabilities of your network and security report.
- software and instructions to decrypt all the data that was encrypted.
- all sensitive downloaded data will be permanently deleted from our cloud storage and we will provide an erasure log.

Our options if you act like nothing's happening, refuse to make a deal or fail the negotiations:

- inform the media and independent journalists about what happened to your servers. To prove it we'll publish a chunk of private data that you should have ciphered if you care about potential breaches. Moreover, your company will inevitably take decent reputational loss which is hard to assess precisely.
- inform your clients, employees, partners by phone, e-mail, sms and social networks that you haven't prevent their data leakage.

Figure 5 - Ransom Note

One of the most recent victims is Migros, Switzerland's largest retail company and largest supermarket chain with over 100K employees. While our sample looks like a “work in progress” it might indicate the threat actor’s intent to significantly increase their victims list and catch up with already familiar capabilities of other competing ransomware groups.

* Triple extortion is a relatively new practice among ransomware operators where the first two extortions of file encryption and publication to the world are not enough. In this case, if the victim still fails to comply and pay the ransom, the ransomware operator will DDOS the victim, making it even more difficult for them to return to operation.

Resources:

<https://docs.microsoft.com/en-us/windows/win32/fileio/i-o-completion-ports>

IOC's:

Mutex:

- “Sessions\2\BaseNamedObjects\0c91c96fd7124f21a0193cf842e3495f6daf84a394f44013e92a87ad9d2ef4a0ceec9dd2e2eca22e “