From the Front Lines | Another Rebrand? Mindware and SFile Ransomware Technical Breakdown

sentinelone.com/blog/from-the-front-lines-another-rebrand-mindware-and-sfile-ransomware-technical-breakdown/

June 6, 2022

Researchers have recently noted the emergence of a new ransomware operator calling itself 'Mindware'. The gang is thought to be responsible for a number of attacks beginning around March to April 2022, with suggestions that the malware was used to attack a not-for-profit mental health provider. Aside from targeting organizations in the Healthcare sector, Mindware has posted data on its leaks site belonging to organizations in sectors such as Finance, Engineering and Manufacturing. Mindware has a number of overlaps with an earlier ransomware strain known as SFile (*aka* SFile2, Escal). In this post, we review how Mindware differs from other ransomware families, note its similarities to SFile, and provide technical indicators to aid threat hunters and detection teams.

Overview

According to one source, the Mindware gang first became active in March 2022. By April, the group was practicing double extortion and operating its own leaks site. Mindware received further attention in April when it was noted by a different researcher to have attacked a mental health provider.

Mindware samples use a distinctive Reflective DLL injection technique. This, along with other indicators described below, show strong overlaps with SFile ransomware samples. Although we do not yet have specifics as to how Mindware attacks are initiated, SFile is known to use RDP bruteforce as an entry vector into an organization.

Each Mindware payload is configured for a specific target. Upon infection and successful execution, the payload drops a hardcoded ransomware note containing a combination of instructions and threats.

```
'-Mindware-',0Dh,0Ah
0Dh,0Ah
'What happened?',0Dh,0Ah
'Your network was ATTACKED, your computers and servers were LOCKED'
'. ',0Dh,0Ah
'Your private data was DOWNLOADED.',0Dh,0Ah
'It cannot be recovered by any means without contacting our team d'
'irectly. ',0Dh,0Ah
0Dh,0Ah
'What does it mean?',0Dh,0Ah
'It means that soon mass media, your partners and clients WILL KNO'
'W about your PROBLEM.',0Dh,0Ah
0Dh,0Ah
0Dh,0Ah
'DON',27h,'T TRY TO RECOVER your data by yourselves. Any attempt to r'
'ecover your data (including the usage of the additional recovery '
'software) can damage your files.',0Dh,0Ah
0Dh,0Ah
0Dh,0Ah
'DON',27h,'T TRY TO IGNORE us. We',27h,'ve downloaded a pack of your int'
'ernal data and are ready to publish it on our news website if you'
' do not respond. ',0Dh,0Ah
0Dh,0Ah
0Dh,0Ah
'So it will be better for both sides if you contact us as soon as '
'possible. ',0Dh,0Ah
0Dh,0Ah
'DON',27h,'T TRY TO CONTACT feds or any recovery companies. ',0Dh,0Ah
0Dh,0Ah
'So if you will hire any recovery company for negotiations or send'
' requests to the police/FBI/investigators, we will consider this '
'as a hostile intent and initiate the publication of whole comprom'
'ised data immediately. ',0Dh,0Ah
0Dh,0Ah
'To prove that we REALLY CAN get your data back - we offer you to '
'decrypt two random files completely free of charge. ',0Dh,0Ah
0Dh,0Ah
'You can contact our team directly for further instructions throug'
'h our website : ',0Dh,0Ah
0Dh,0Ah
0Dh,0Ah
'TOR VERSION : ',0Dh,0Ah
0Dh,0Ah
'(you should download and install TOR browser first https://torpro'
'ject.org ) ',0Dh,0Ah
0Dh,0Ah
'https://dfpc7yvle5kxmgg6sbcp5ytggy3oeob676bjgwcwhyr2pwcrmbvoilqd.'
'onion/chat/99a41fc7c382c073e52dcfba376158bc',0Dh,0Ah
0Dh,0Ah
```

Mindware ransom note

In common with a move made by other ransomware groups recently, Mindware attempts to discourage victims from contacting ‘recovery companies’, negotiators or authorities, threatening to immediately leak data should they do so. Victims are provided with a .onion URL as a means to make contact with the attackers and to decrypt two “random files” as proof that the operators possess a decryption key. Victims that refuse to pay are listed on the Mindware ransomware public leaks site.

Welcome to Dataleak blog

* Welcome to data leak blog. Below on the page are the data of companies that did not agree to the terms
* Bienvenue sur le blog data leak. Ci-dessous sur la page sont les données des entreprises qui n'ont pas accepté les conditions
* Willkommen auf dem Datenleck-Blog. Unten auf der Seite finden Sie die Daten von Unternehmen, die den Bedingungen nicht zugestimmt haben
* Benvenuti nel blog di perdita di dati. Di seguito nella pagina sono riportati i dati delle aziende che non hanno accettato i termini

acorentacar

URL	https://www.acorentacar.com
Data size	200gb
Date	11 Apr 2022
Time left	00:00:00:00
Files	[browse]

Move at your own pace behind the steering wheel, without restrictions, without schedules, in Miami, Miami Beach, Orlando, Fort Lauderdale, Los Angeles California, Dallas-Fort Worth, Detroit, Canada, Aruba, Curacao, Chile, Mexico or Venezuela it is necessary to contact us. You have reached the right place. With ACO Rent A Car you will enjoy the best car rental services. Business trips or vacation trips, we have the car you need. At ACO Rent A Car you will find the best car rental service located in the major airports of Miami, Orlando, Fort Lauderdale,Los Angeles California, Aruba, Curacao, Chile, Mexico and Venezuela. You won't have to wait in long and tedious lines to book a car because you can book online, anytime , anywhere. Also, you can prepay the total or a partial amount and save even more time.

allwell

URL	https://allwell.org
Data size	200GB
Date	4 Apr 2022
Time left	00:00:00:00
Files	[browse]

Healing and hope for every age and diagnosis.
Allwell Behavioral Health Services is a private, not-for-profit provider of comprehensive community mental health services in Coshocton, Guernsey, Morgan, Muskingum, Noble and Perry counties.

Allwell was created in 2016 as a merger of Six County Inc. and Thompkins Treatment Inc. While Six County offered services to all ages, Thompkins Treatment specialized in youth aged 2 to 18. After conducting an analysis of our services, we determined that we could better serve our communities as a single entity. We integrate mental and physical care to offer the hope of wellbeing for you and every member of your family

Since the 1950□s, our services have expanded to meet the changing needs of our diverse communities. Because every client comes to us with unique values and problems, we mold our services to their needs to help them reach their full potential.

Mindware public leaks site

Mindware Technical Analysis

As noted above, Mindware uses Reflective DLL Injection, a technique in which the shellcode dynamically retrieves handles to key API functions like LoadLibraryA() and GetProcAddress() by locating function addresses through the Export Address Table loaded by the host process.

This allows the shellcode to be position-independent by building its own import table and parsing through when executed in memory. This means a PE file could be loaded in the form of shellcode or a DLL entirely from memory.

The technique, which has also been noted in other ransomware families such as BlackMatter, avoids searching for module names directly and instead checks for hashes precalculated with a ROT13 algorithm.

Mindware and SFile samples require kernel32.dll and ntdll.dll. The APIs are searched for using a combination of the PEB (Process Environment Block) of the module and the EAT (Export Address Table) and enumerating all function names.

```
mov     edx, [ebp-24h]
add     edx, [ebp-1Ch]
mov     [ebp-24h], edx
```

```
mov     eax, [ebp-24h]
cmp     dword ptr [eax], 4550h
jnz     short loc_432BD1
```

```
jmp     short loc_432BDC
```

```
loc_432BD1:
mov     ecx, [ebp-1Ch]
sub     ecx, 1
mov     [ebp-1Ch], ecx
jmp     short loc_432B8C
```

```
loc_432BDC:
mov     edx, large fs:30h
mov     [ebp-8], edx
mov     eax, [ebp-8]
mov     ecx, [eax+0Ch]
mov     [ebp-8], ecx
mov     edx, [ebp-8]
mov     eax, [edx+14h]
mov     [ebp-0Ch], eax
```

```
loc_432BF8:
cmp     dword ptr [ebp-0Ch], 0
jz      loc_432E8B
```

```
mov     ecx, [ebp-0Ch]
mov     edx, [ecx+28h]
mov     [ebp-18h], edx
mov     eax, [ebp-0Ch]
mov     cx, [eax+24h]
mov     [ebp-4], cx
mov     dword ptr [ebp-10h], 0
```

```
loc_432C1D:
mov     edx, [ebp-10h]
push    edx
call    ROT13
add     esp, 4
mov     [ebp-10h], eax
```

```
mov     eax, [ebp-18h]
movzx   ecx, byte ptr [eax]
cmp     ecx, 61h
jl      short loc_432C49
```

```
(2540,1255) (659,1401) 00032021 00432C21: ReflectiveLoader(x)+C1
```

ROT13 Algorithm

As noted, the same technique is characteristic of SFile ransomware samples, first seen in 2020 and active through 2021. Interestingly, SFile attacks seem to have been on hiatus over the last 9 months or so, and the emergence of Mindware samples with strong overlaps is indicative, as other researchers have noted, of a possible rebrand.

Both SFile and Mindware ransomware payloads accept the following parameters:

```
--enable-shares -> encrypt network shares
--kill-susp -> Triggers process termination
```

The ransomware checks for and then encrypts internal, removable and remote drive types.

```
00436890
00436890
00436890
00436890        Check_Drive_Type proc near
00436890        db      66h
00436890 000 nop
00436892 000 push    ebp
00436893 004 mov     ebp, esp
00436895 004 cmp     dword ptr [ebp+8], 3
00436899 004 jz      short loc_4368A7

0043689B 004 cmp     dword ptr [ebp+8], 4
0043689F 004 jz      short loc_4368A7

004368A1 004 cmp     dword ptr [ebp+8], 2
004368A5 004 jnz     short loc_4368AE

004368A7
004368A7        loc_4368A7:
004368A7 004 mov     eax, 1
004368AC 004 jmp     short loc_4368B0

004368AE
004368AE        loc_4368AE:
004368AE 004 xor     eax, eax

004368B0
004368B0        loc_4368B0:
004368B0 004 pop     ebp
004368B1 000 retn    4
004368B1        Check_Drive_Type endp
004368B1
```

Mindware and SFile payloads check for different drive types

Over 200 file types are targeted for encryption, denoted by a hardcoded list of file extensions. However, the following files are specifically excluded from encryption:

- autorun.inf
- desktop.ini
- ntuser.ini
- boot.ini
- iconcache.db
- thumbs.db
- bootfont.bin
- ntuser.dat
- bootmgr
- bootsect.bak
- ntuser.dat.log
- message_to_<<redacted>>.txt
- ! cynet ransom protection(don't delete)

Similarly, files in the following locations are also excluded from encryption:

%windir%	\all users\microsoft\	\cache2\
\google\	\All Users\Microsoft\	:\$RECYCLE.BIN\
\Program Files\Internet Explorer\	\far manager\	\mozilla\
\Roaming\Microsoft\	\windows\system32\	:\system volume information\
\ida 7.0\	\tor browser\	\Local\Microsoft\
\windows\syswow64\	\Program Files\Microsoft Games\	\ida 6.8\
\windows.old\	\Local Settings\Microsoft\	\windows\system\
\inetpub\logs\	\Default\Extensions\	\intel\
\LocalLow\Microsoft\	\windows\winsxs\	:\boot\
\Temporary Internet Files\	\msocache\	\Common\Microsoft\
\System\msadc\	:\drivers\	\Temp\
\perflogs\	\Sophos\	\Common Files\
:\wsus\	$windows.~bt	\ProgramData\Microsoft\
\Symantec\	\WindowsPowerShell\	\cache\
$windows.~ws	\Application Data\Microsoft\	\Leaked\

\Mozilla Firefox\

In order to protect itself and prevent other running processes from interfering with the encryption process, Mindware kills all other processes, with the exception of the following:

explorer.exe	powershell.exe	rundll32.exe
vmnetdhcp.exe	vmware-authd.exe	vmware-hostd.exe
vmware-tray.exe	vmware-usbarbitrator.exe	vmware-usbarbitrator32.exe
vmware-usbarbitrator64.exe	webroot_updater.exe	werfault.exe
windowsupdate.exe		

```
                          ; "powershell.exe"
dd offset aRundll32_exe ; "rundll32.exe"
dd offset aWerfault_exe ; "werfault.exe"
dd offset aExplorer_exe ; "explorer.exe"
dd offset aVmnetdhcp_exe ; "vmnetdhcp.exe"
dd offset aVmwareAuthd_ex ; "vmware-authd.exe"
dd offset aVmwareHostd_ex ; "vmware-hostd.exe"
dd offset aVmwareTray_exe ; "vmware-tray.exe"
dd offset aVmwareUsbarbit ; "vmware-usbarbitrator64.exe"
dd offset aVmwareUsbarb_0 ; "vmware-usbarbitrator32.exe"
dd offset aWebroot_update ; "webroot_updater.exe"
dd offset aWindowsupdate_ ; "windowsupdate.exe"
dd offset aVmwareUsbarb_1 ; "vmware-usbarbitrator.exe"
align 10h
```

List of processes that Mindware and SFile allow to run

SFile and Mindware samples are PEs typically around 250-300KB in size.

SFile and Mindware Ransomware Targeting

Analysis of the SFile payloads shows that SFile ransomware was mostly used against U.S organizations in Manufacturing, Mechanical, and Automobile sectors.

SHA1 – SFile Samples	Targeted Sector/Industry
28f73b38ace67b48e525d165e7a16f3b51cec0c0	Automotive Engineering
bdb0c0282b303843e971fbcd6d2888d834da204c	Other Personal Services
5ffac9dff916d69cd66e91ec6228d8d92c5e6b37	Investment
6960beedbf4c927b75747ba08fe4e2fa418d4d9b	Manufacturing

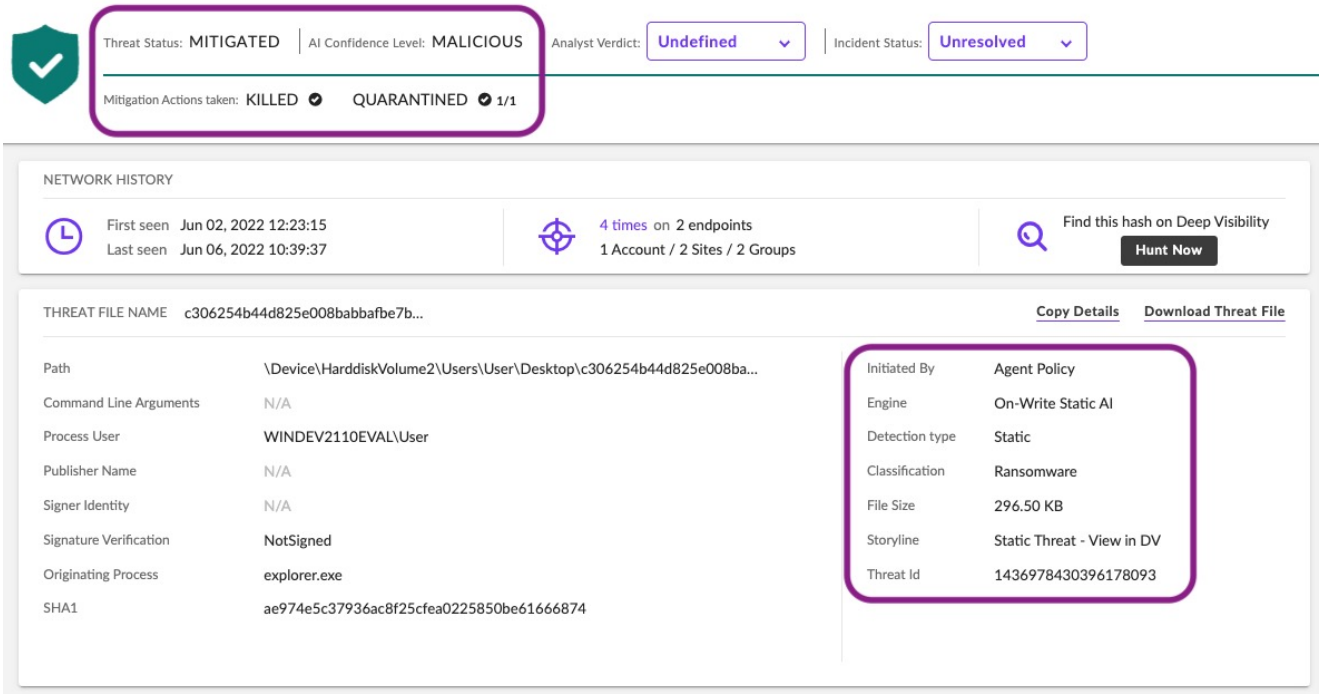
665572b84702c4c77f59868c5fe4d0b621f2e62a	Insurance
a67686b5ce1d970a7920b47097d20dee927f0a4d	Retail
14e4557ea8d69d289c2432066d860b60a6698548	Sample has hardcoded org name as CCCR [parent organization could not be determined]
0f20e5ccdbbed4cc3668577286ca66039c410f95	Engineering

Mindware samples also show a strong preference for businesses in similar industries.

SHA1 – Mindware Samples	Targeted Sector/Industry
ae974e5c37936ac8f25cfea0225850be61666874	Engineering
e9b52a4934b4a7194bcbbe27ddc5b723113f11fe	Healthcare
9bc1972a75bb88501d92901efc9970824e6ee3f5	Manufacturing
f91d3c1c2b85727bd4d1b249cd93a30897c44caa	Finance
46ca0c5ad4911d125a245adb059dc0103f93019d	Engineering

How To Protect Against Mindware and SFile Ransomware

The SentinelOne Singularity platform detects and prevents execution of Mindware and SFile ransomware strains.



For organizations not currently protected by SentinelOne, please see the list of Indicators of Compromise at the end of this post and the technical indicators described above.

Conclusion

Indications suggest Mindware is likely a rebrand of SFile, or at least that the same source code or builder for SFile is available to Mindware operators. While neither strain has achieved the notoriety of some of the more well-known ransomware strains that have been circulating recently, it may be that flying under the radar and hitting selective targets without attracting too much public attention is exactly what the gang are aiming for.

We hope that the information in this post serves to enable security teams to ensure that they have adequate resources to detect and prevent this threat. The SentinelOne Singularity platform detects and protects against SFile, Mindware and all other known ransomware threats. For more information about ransomware protection, see here. To learn more about how SentinelOne can help protect your organization from ransomware and other threats, contact us or request a free demo.

Indicators of Compromise

Mindware Onion Address

https[:]//dfpc7yvle5kxmgg6sbcp5ytggy3oeob676bjgwcwhyr2pwcrmbvoilqd[.]onion/

Mindware Samples, SHA1
ae974e5c37936ac8f25cfea0225850be61666874
e9b52a4934b4a7194bcbbe27ddc5b723113f11fe
9bc1972a75bb88501d92901efc9970824e6ee3f5
f91d3c1c2b85727bd4d1b249cd93a30897c44caa
46ca0c5ad4911d125a245adb059dc0103f93019d

Mindware Samples, SHA256
c306254b44d825e008babbafbe7b07e20de638045f1089f2405bf24e7ce9c0dc
00309d22ab53011bd74f4b20e144aa00bf8bb243799a2b48f9f515971c3c5a92
32c818f61944d9f44605c17ca8ba3ff4bd3b2799ed31222975b3c812f9d1126c
81828762ebe7ea99b672c8ac07dc3c311487a5a246db494c7643915f6c673562
d1a0a2dc26603b2e764ee9ab90f3f55a2f11a43e402dd72f4a32a19b0ac414b5

MITRE ATT&CK
TA0005 – Defense Evasion
T1485 – Data Destruction
T1486 – Data Encrypted for Impact
T1027.002 – Obfuscated Files or Information: Software Packing
T1007 – System Service Discovery

T1059 – Command and Scripting Interpreter
T1112 – Modify Registry
TA0010 – Exfiltration
T1018 – Remote System Discovery
T1082 – System Information Discovery