New Ransomware Available for Targeted Attacks

malware ransomware xftas iris advisory

Recopilación pública | 9 Seguidores | TLP: BLANCO

Seguir ¿Esto me afecta?

Summary

In September, IBM X-Force IRIS identified a new ransomware variant designed for targeted attacks against enterprise databases. IRIS analysts assess that this new ransomware variant, which we have dubbed "PureLocker", is developed by the same Malware-as-a-Service (MaaS) provider responsible for creating and selling the More_eggs JScript backdoor and its related components. The research behind this new ransomware stems from a collaborative effort with Intezer.

Threat Type

- Ransomware

Overview

IBM X-Force IRIS reverse engineers analyzed a little-known ransomware variant we have named PureLocker together with Intezer. Although this ransomware is designed for targeted attacks against enterprise databases, it will also encrypt non-database files. PureLocker is written in PureBasic and has a very low antivirus (AV) detection rate. The ransomware encrypts files on the system using AES encryption and appends the file extension .CR1 to the encrypted files. As typically seen with ransomware, this variant also drops a ransom note demanding the victim contact cr1-silvergold1@protonmail[.]com in order to decrypt their data.

After analyzing the ransomware's structure and execution, IRIS analysts identified clear similarities with other DLL files that install the More_eggs JScript backdoor, which IRIS encountered and analyzed earlier this year (See https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/). These similarities lead to our assessment that the same Malware-as-a-Service (MaaS) vendor that develops and sells More_eggs and related components also is responsible for creating this new ransomware variant. For additional information on the MaaS provider, please see the following research from QuoScient: https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648 We do not have any additional information at this time on which threat actors are purchasing or using this ransomware. We also do not know how the ransomware is delivered into the intended victim's environment. However, we note that More_eggs has typically been delivered through phishing emails carrying malicious documents or URLs to initiate the infection.

The following file was analyzed to produce this report:

File	Category	SHA256
cryptopp.dll	Ransomware	c592c52381d43a6604b3fc657c5dc6bee61aa288bfa37e8fc54140841267338d

Malware Analysis

PureLocker is a dynamic link library (DLL) that masquerades as a Crypto++

DETALLES DE LA RECOPILACIÓN | COMENTARIOS (0)

Esquema de recopilación

Informes (2)

MAL 527468a4053dc142dd479659cf2fc94c
Informe capturado el 11 nov. 2019 13:40:37 por Megan Roddie

MAL 84d4902be41e2ffa8ce720a4e5406158
Informe capturado el 11 nov. 2019 13:40:36 por Megan Roddie

Ver todos los informes

Archivos adjuntos (6)

decrypted_strings.csv
Adjuntado el 11 nov. 2019 13:38:22 por Megan Roddie
Tamaño 4.29 kB

Screen Shot 2019-11-11 at 10.33.46 AM.png
Adjuntado el 11 nov. 2019 13:33:56 por Megan Roddie
Tamaño 88.36 kB

event_log.png
Adjuntado el 11 nov. 2019 13:32:56 por Megan Roddie
Tamaño 79.84 kB

encrypted_strings.png
Adjuntado el 11 nov. 2019 13:26:30 por Megan Roddie
Tamaño 208.38 kB

api_library_hashes
Adjuntado el 11 nov. 2019 13:25:45 por Megan Roddie
Tamaño 1.48 kB

Screen Shot 2019-11-11 at 10.23.32 AM.png
Adjuntado el 11 nov. 2019 13:23:54 por Megan Roddie
Tamaño 46.65 kB

Library component with the original filename of cryptopp.dll. It expects to be executed with the Windows regsvr32 utility using the command-line arguments /s /i. This command will execute the *DllRegisterServer()* export function. Once executed, a key generation algorithm is utilized to generate a key where the last 4 bytes are brute forced and that will be used in a XOR-algorithm to decrypt embedded strings. These encrypted strings are formatted like hex-encoded Unicode strings.

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000020   00 00 90 90 00 00 36 00  30 00 33 00 32 00 35 00   ......6.0.3.2.5.
00000030   32 00 33 00 31 00 33 00  31 00 32 00 37 00 32 00   2.3.1.3.1.2.7.2.
00000040   36 00 31 00 39 00 34 00  30 00 35 00 42 00 34 00   6.1.9.4.0.5.B.4.
00000050   44 00 35 00 45 00 31 00  35 00 00 00 36 00 46 00   D.5.E.1.5...6.F.
00000060   30 00 34 00 35 00 43 00  32 00 43 00 33 00 31 00   0.4.5.C.2.C.3.1.
00000070   00 00 31 00 44 00 32 00  41 00 35 00 44 00 32 00   ..1.D.2.A.5.D.2.
00000080   38 00 00 00 41 00 3A 00  00 00 35 00 37 00 32 00   8...A.:...5.7.2.
00000090   34 00 35 00 34 00 36 00  44 00 33 00 31 00 33 00   4.5.4.6.D.3.1.3.
000000A0   41 00 33 00 36 00 00 00  21 00 00 00 31 00 44 00   A.3.6...!...1.D.
000000B0   32 00 42 00 34 00 30 00  32 00 34 00 00 00 22 00   2.B.4.0.2.4...".
000000C0   00 00 35 00 30 00 32 00  37 00 35 00 44 00 36 00   ..5.0.2.7.5.D.6.
000000D0   34 00 33 00 31 00 31 00  44 00 32 00 36 00 35 00   4.3.1.1.D.2.6.5.
000000E0   43 00 35 00 42 00 35 00  37 00 34 00 44 00 35 00   C.5.B.5.7.4.D.5.
```

The key used by the analyzed sample was determined to be D3F3CEBB972965. Once the key is generated, the sample will perform the following:

- Checks that it was executed with the /s /i arguments.
- Reads the BeingDebugged field in the Process Environment Block (PEB) to determine if it is being debugged.
- Checks the NtGlobal flag to determine if it is being debugged.
- Maps ntdll from "\KnownDlls32\". This is a form of hook evasion where the sample loads the version of the library that's loaded at system startup.

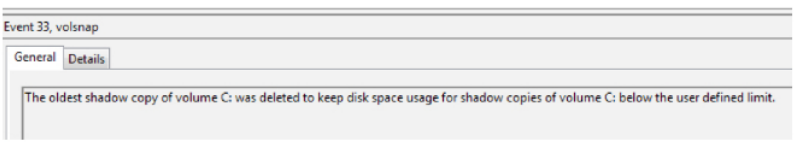
During execution, PureLocker calculates a hash for the API library name "ntdll.dll". The hash was observed to be 0x84C05E40. Additional computed hashes can be found in the "api_library_hashes" file in the "Attachments" section to the right.

Once these hashes are resolved, the ransomware checks the system date and ensures that it is 2019. Then it will check that its file extension is either .ocx or .dll. Finally, it will determine if the user has administrator privileges using the *CheckTokenMemberShip()* API function.

If any of the above checks fail, the malware will terminate.

Using the decoded string "CR1" and the victim's computer name, a named mutex is generated that is formatted like the following: 04780006780E6407.

During analysis, PureLocker attempted to execute the command C:\Windows\Sysnative\wbem\WMIC.exe. The Sysnative folder doesn't exist; it is used as a redirect to the %WinDir%\System32\ directory. This is likely an evasion technique to hide program execution from the System32 directory. The commandline argument to WMIC.exe is 41 spaces (0x20). Then PureLocker adjusts the amount of space allocated to store volume shadow copies using the command: *wmic shadowstorage SET MaxSpace=337000000.* This decreases the allocated space to 321.39 MB. During analysis, the following System event log entry was logged in association with this activity:



Filesystem Encryption

During the encryption process, the ransomware creates a logfile named “dbg.txt” and a ransom note named “YOUR_FILES.txt”. The logfile lists the files that could not be deleted and the number of threads the malware is utilizing during execution. The ransom note indicates that the files are encrypted with AES-256-CBC + RSA-4096 and to contact the actor at cr1-silvergold1@protonmail[.]com.

The sample does not appear to encrypt files with the following file extensions.

.lnk	.msg	.msi	.hxh	.log	.hxw	.com	.txt
.wpl	.ico	.chm	.appref-ms	.mui	.lib	.qm	.cr1
.oca	.bak	.bat	.sys	.exe	.readme	.manifest	.searchconnector-ms
.dmp	.old	.search-ms	.library-ms	.inf	.db	.ini	.hlp
.cmd	.cpl	.etl	.tmp	.url			

When analyzed in a virtual machine, PureLocker was observed to generate a 32-byte random AES key and a 16-byte random initialization vector (IV) per encrypted file using the *SystemFunction036()* API. Analysis is still on-going to understand the full extent of the encryption functionality of the ransomware.

Sample Ransom Note Content

The date in the note is the date that the system was encrypted.

```
#CR1
All your files have been encrypted using: AES-256-CBC + RSA-4096.
Shadows copies were removed, original files were overwritten, rena
med and deleted using safe methods.
Recovery is not possible without own RSA-4096 private key.
Only we can decrypt your files!
To decrypt your files contact us at: cr1-silvergold1@protonmail.co
m
Your private key will be deleted after 7 days starting from: 15/1
0/2019, after that the recovery of your files will not be possibl
e.
```

Sample logfile Content

```
Started with 1 threads
can't_delete:C:\tools\cygwin\etc\pki\ca-trust\extracted\java\cacer
ts
can't_delete:C:\tools\cygwin\etc\pki\ca-trust\extracted\openssl\ca
-bundle.trust.crt
can't_delete:C:\tools\cygwin\etc\pki\ca-trust\extracted\pem\email-
ca-bundle.pem
can't_delete:C:\tools\cygwin\etc\pki\ca-trust\extracted\pem\objsig
n-ca-bundle.pem
can't_delete:C:\tools\cygwin\etc\pki\ca-trust\extracted\pem\tls-ca
-bundle.pem
can't_delete:C:\tools\cygwin\var\cache\rebase\rebase_dyn
can't_delete:C:\tools\cygwin\var\cache\rebase\rebase_exe
can't_delete:C:\tools\cygwin\var\cache\rebase\rebase_lst
can't_delete:C:\tools\cygwin\var\cache\rebase\rebase_pkg
can't_delete:C:\tools\cygwin\var\cache\rebase\rebase_user
```

Decrypted Strings

A list of decrypted strings can be found in the "decrypted_strings.csv" file in the Attachments section to the right.

Conclusion

As noted by our partners at Intezer, this new ransomware variant appears designed for use in targeted attacks against an organization's enterprise servers and databases as opposed to indiscriminate attacks to infect as many systems as possible. It also appears that the above-mentioned MaaS provider is now expanding its product line to include ransomware, which may be sold increasingly to threat actors determined to infect specific organizations with ransomware that has a very low AV detection rate.

Indicators of Compromise

MD5

- MAL | 527468a4053dc142dd479659cf2fc94c
- MAL | 84d4902be41e2ffa8ce720a4e5406158

Filenames

- `dbg.txt`
- `YOUR_FILES.txt`

Recommendations

- Ensure anti-virus software and associated files are up to date.
- Search for existing signs of the indicated IOCs in your environment.
- Block all URL and IP based IoCs at the firewall, IDS, web gateways, routers or other perimeter-based devices.
- Keep applications and operating systems running at the current released patch level.
- Exercise caution with links and attachments in emails.

References

- X-Force IRIS Threat Research
- http://intezer.com/blog-purelocker-ransomware-being-used-in-targeted-attacks-against-servers