

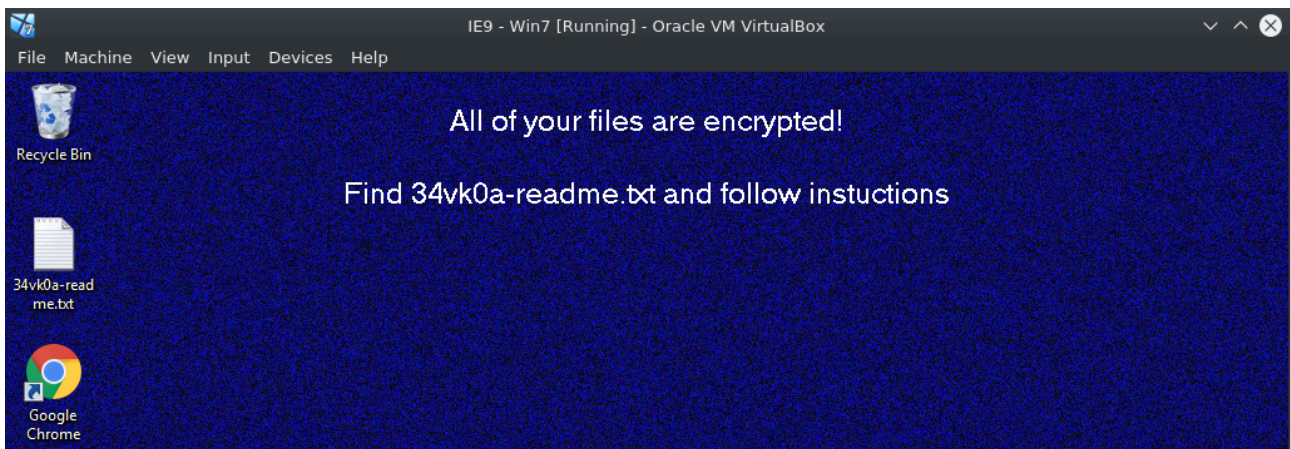
Germanwiper's big brother? gandgrab's kid ? sodinokibi!

By f0wL

Published: 2019-08-10 · Archived: 2026-04-05 23:36:52 UTC

Sat 10 August 2019 in [Ransomware](#)

After last week's analysis on GermanWiper I thought it would be about time to have a Look at Sodinokibi aka REvil, the new weird kid on the block.



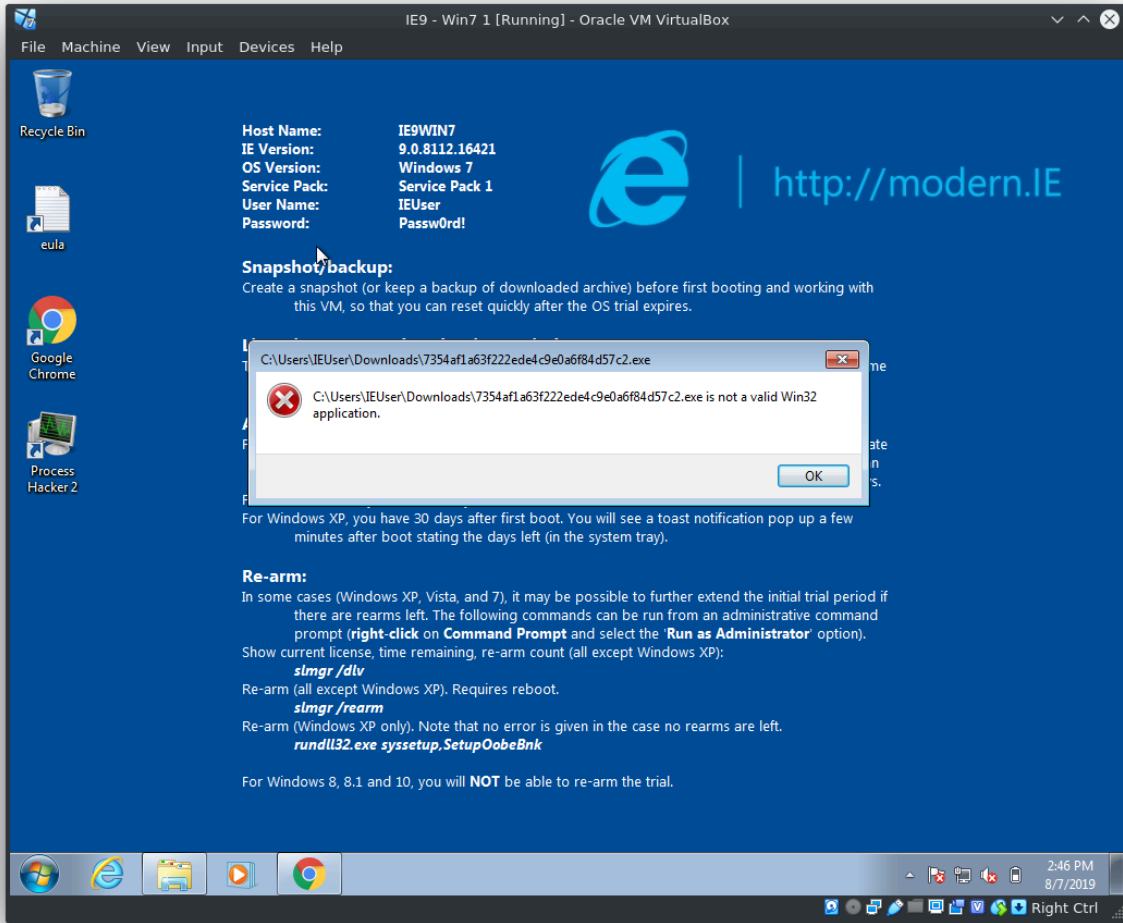
According to [Cybereason](#) the Sodinokibi Ransomware was written by the same guys who created GandCrab, which is a pretty big deal after GandCrab retired recently. The samples that I'll be looking at today were first dropped in Asia, but it did not take long to reach other continents as well.

A general disclaimer as always: downloading and running the samples linked below will lead to the encryption of your personal data, so be f\$cking careful. Also check with your local laws as owning malware binaries/sources might be illegal depending on where you live.

Where I dug up the samples this time:

Sodinokibi #1 available @ <https://malshare.com/sample.php?action=detail&hash=6cb6fda0b353d411a30c5b945e53ea52> sha256
bace25c1ec587d099b4c566b1a07978dd9cb3bd67c2acaa55d2e4644a7877070

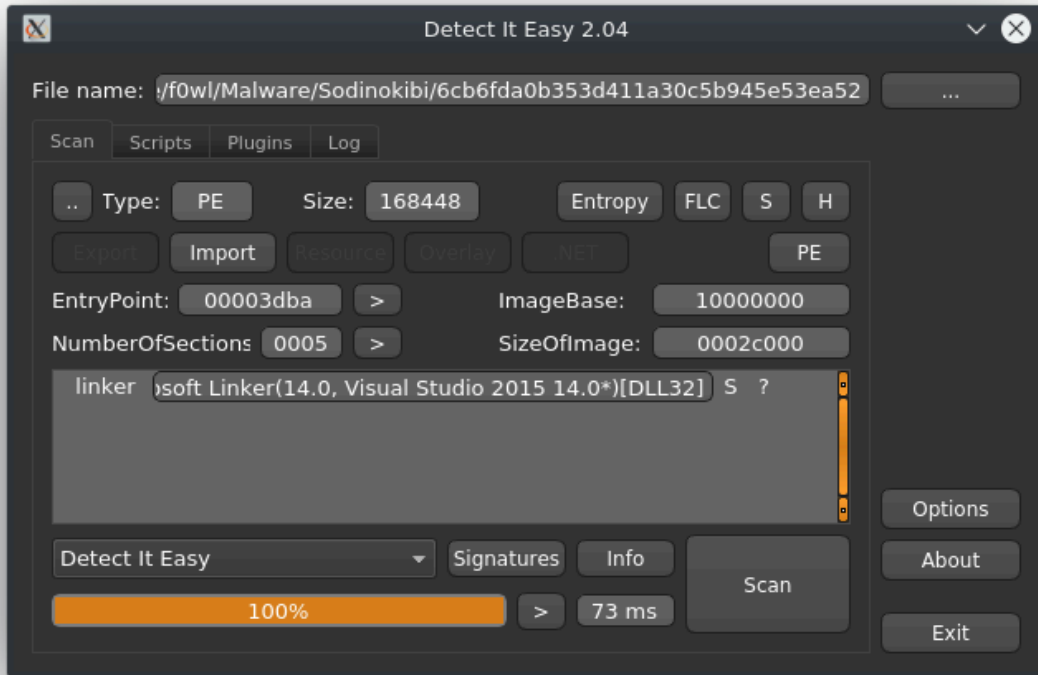
Sodinokibi #2 available @ <https://malshare.com/sample.php?action=detail&hash=7354af1a63f222ede4c9e0a6f84d57c2> sha256
2fea45f7be7c7313ee6e4fe7ad9ef64d9966a2391003a00dcbbd6214e9c522ef



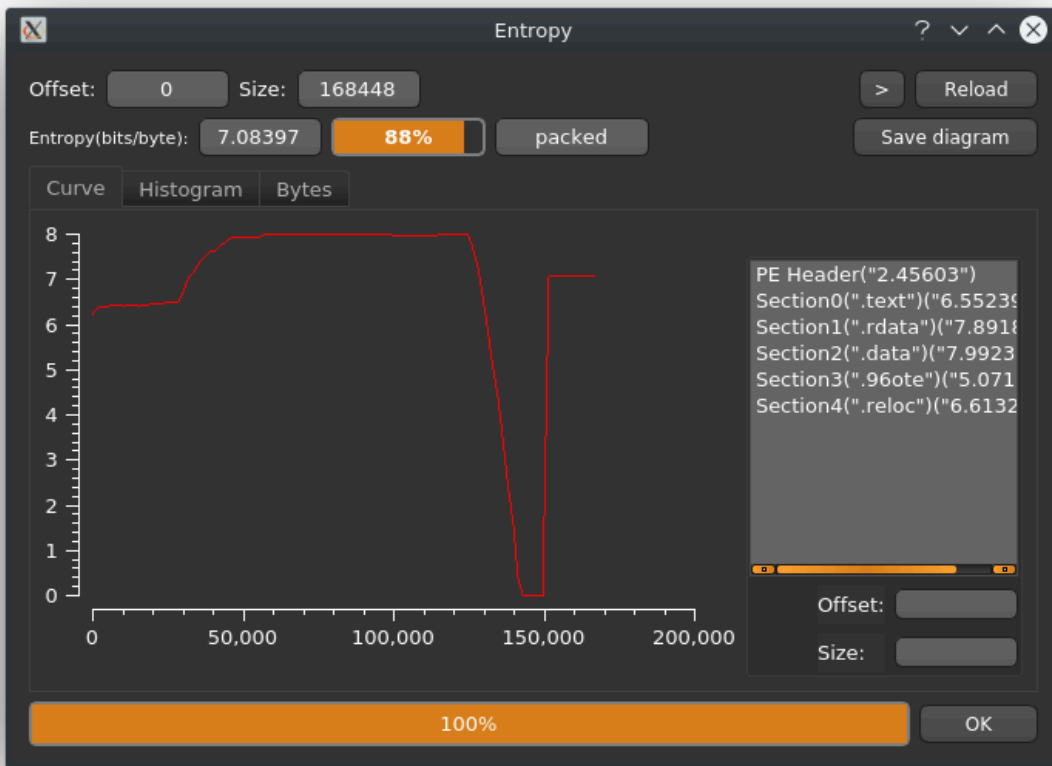
Running it through VirusTotal we get a pretty good detection rate, but that is to be expected since REvil is around for a few days already. Here's a direct Link to the [VT Analysis](#).

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis	Suspicious	Ad-Aware	DeepScan:Generic.Ransom.Sodinokibi.7...
AegisLab	Trojan.Win32.Sodinokibi.4lc	Alibaba	Ransom:Win32/Sodinokibi.30d530e9
ALYac	Trojan.Ransom.Sodinokibi	Antiy-AVL	Trojan[Ransom]/Win32.Sodinokibi
SecureAge APEX	Malicious	Arcabit	DeepScan:Generic.Ransom.Sodinokibi.7...
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Crypt.XPACK.Gen	BitDefender	DeepScan:Generic.Ransom.Sodinokibi.7...
CAT-QuickHeal	Ransom.Sodinokibi	ClamAV	Win.Ransomware.Sodinokibi-7013612-0
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cylance	Unsafe

Looking at Detect it easy we don't see anything special either. The PE seems to be built with MS Visual Studio 2015 (Linker Version 14).



Entropy-wise we can observe a huge drop near the end of the binary.



PE-bear v0.3.9.5 [home/fowl/Malware/Sodinokibi/6cb6fda0b353d411a30c5b945e53ea52]

File Settings Compare Info

6cb6fda0b353d411a30c5b945e53ea52

DOS Header
DOS stub
NT Headers
Signature
File Header
Optional Header
Section Headers
Sections
- .text
- .rdata
- .data
- .96ote
- .reloc

EP = 31BA

Offset	Name	Value	Meaning
0	Machine	14c	Intel 386
4	Sections Count	5	5
10	Time Date Stamp	5d437f4f	Friday, 02.08.2019 00:09:51 UTC
14	Ptr to Symbol Table	0	0
18	Num. of Symbols	0	0
22	Size of Optional Header	e0	224
26	Characteristics	2102	File is executable (i.e. no unresolved external references). 32 bit word machine.
30		100	File is a DLL.
34		2000	

Imports

BaseReloc.

Check for updates

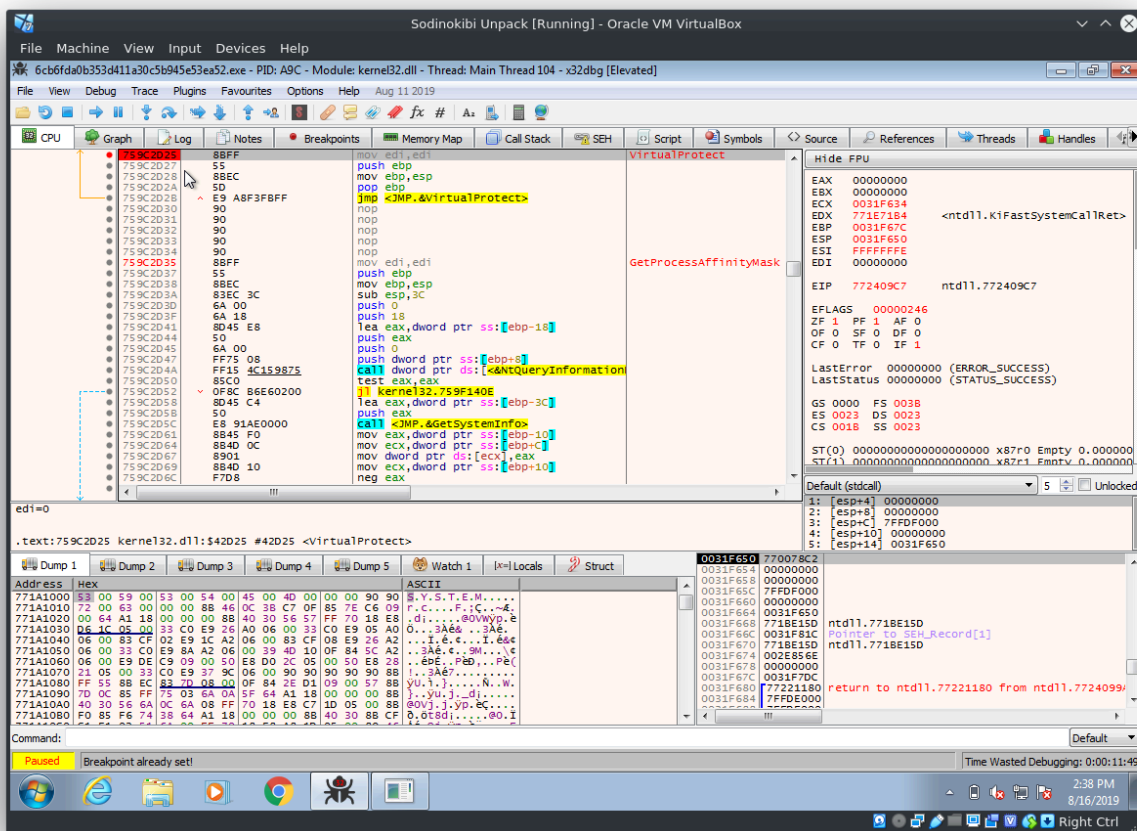
The imports definitely indicate that something is wrong here. Only loading kernel32.dll with 3 entries is a bit minimalistic for ransomware.

Offset	Name	Func. Count	Bound?	OriginalFirstTh	TimeDateStar	Forwarder	NameRVA	FirstThunk
0CE8	KERNEL32.dll	3	FALSE	EB10	0	0	EB4E	C000

KERNEL32.dll [3 entries]						
Call via	Name	Ordinal	Original Thunl	Thunk	Forwarder	Hint
C000	CloseHandle	-	EB20	EB20	-	7F
C004	SetErrorMode	-	EB2E	EB2E	-	4EF
C008	CreateThread	-	EB3E	EB3E	-	E8

For one to get his/her Hands on the actual PE with an intact/complete IAT there are a couple of possible ways. Sergei Frankoff explained a very fast, but slightly "messy" Method on OALive. I'll try to replay this technique and plan to come back to this sample soon to try and script my way out of this hole.

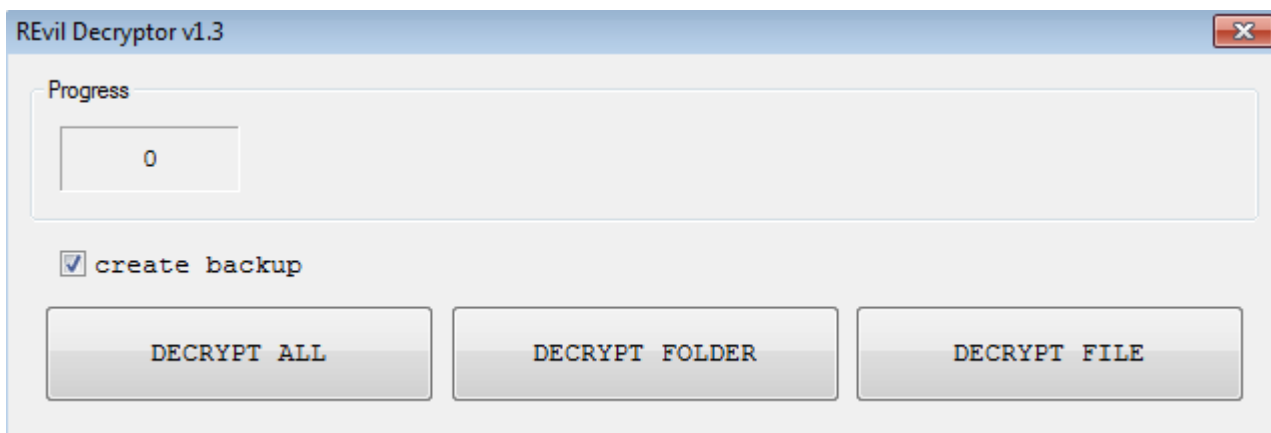


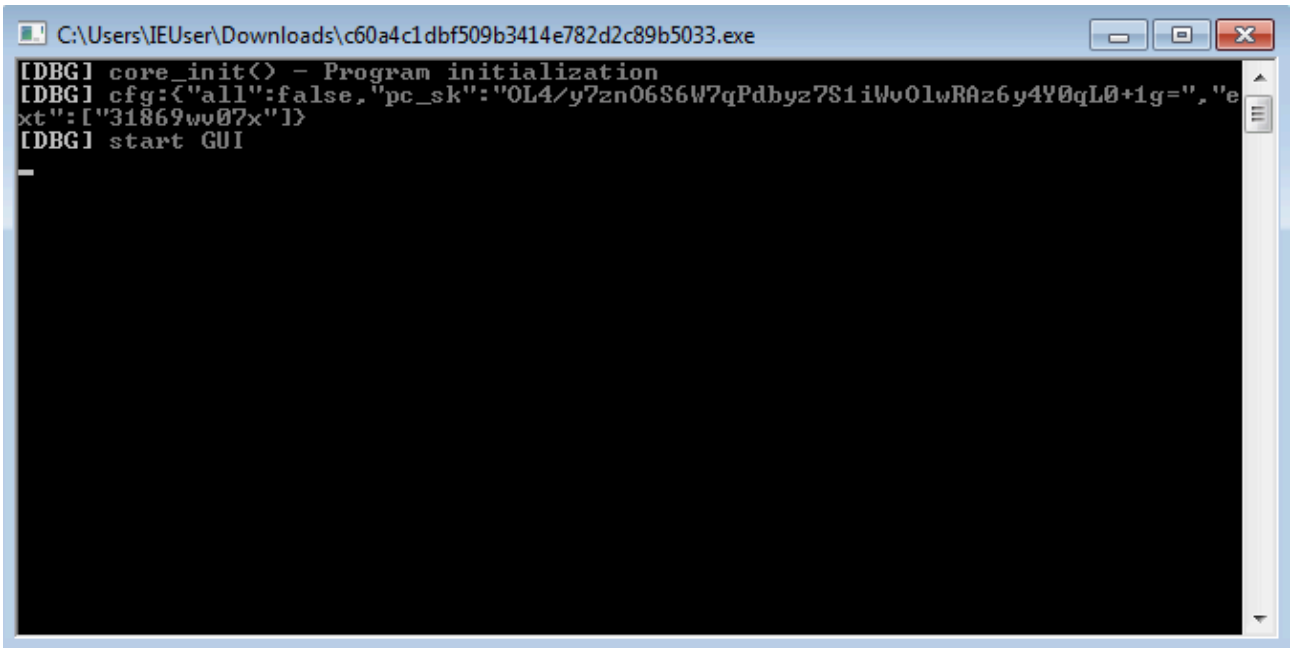


A dump of the strings in the binary file can be found [here](#). Likewise a sample of the ransomnote dropped as a textfile by the malware is available [here](#).

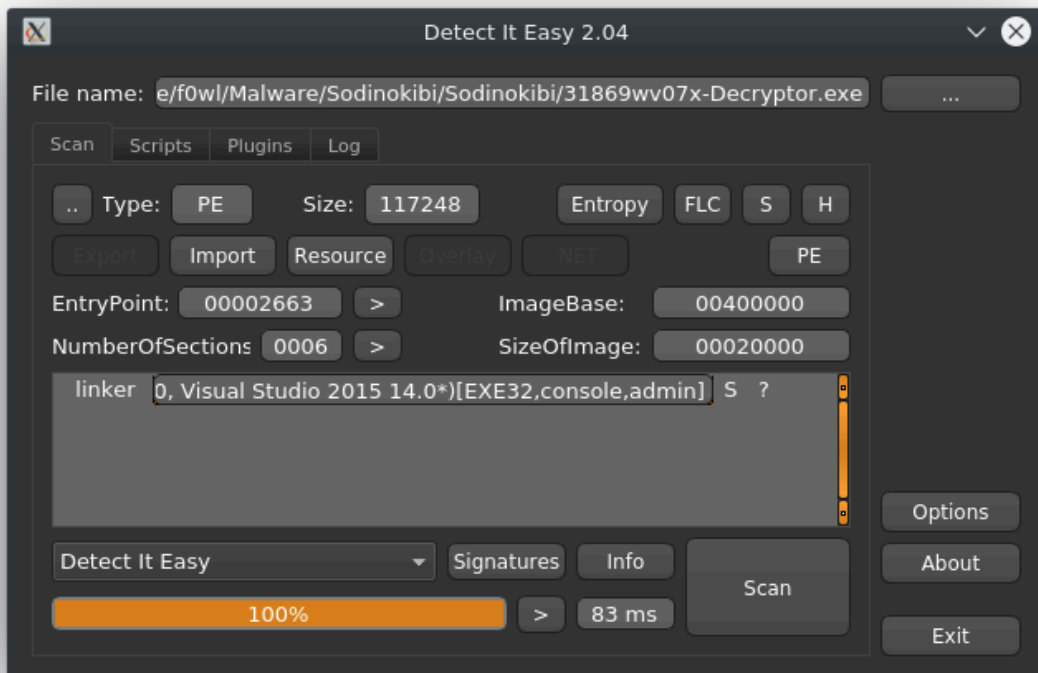
The Decryptor

Thanks to a businessman who shall remain nameless but decided to pay the ransom we can take a look at the Decryptor V1.3 as well. My feeling about this executable is, that it is being built to order rather than prepared in case a decryption is requested. The tool feels relatively unpolished because of the active debugging, no obfuscation or anti-evasion.





Running it through Detect it Easy there is nothing spectacular going on here. Consistent with the ransomware itself the decryptor was built with Visual Studio 2015 as well. Entropy-wise there are no surprises either at 4.64889.



OL4/y7znO6S6W7qPdbyz7S1iWvOlwRAz6y4Y0qL0+1g= 31869wv07x

IOCs

Sodinokibi / REvil Ransomware (SHA256)

```
bace25c1ec587d099b4c566b1a07978dd9cb3bd67c2acaa55d2e4644a7877070  
2fea45f7be7c7313ee6e4fe7ad9ef64d9966a2391003a00dcbbd6214e9c522ef  
ada9794bcc8e87af05f9982522e26f7ead3d1cb07bb76ce58fac1bf98e41cf53
```

URLs

```
httx://decryptor[.]top  
httx://aplebzu47wgazapdqks6vrcv6zcnjppkxbr6wketf56nf6aq2nmyoyd.onion
```

Source: <https://dissectingmalwa.re/germanwipers-big-brother-gandgrabs-kid-sodinokibi.html>