Revenge Ransomware, a CryptoMix Variant, Being Distributed by RIG Exploit Kit

By Lawrence Abrams

Published: 2017-03-15 · Archived: 2026-04-05 15:40:22 UTC

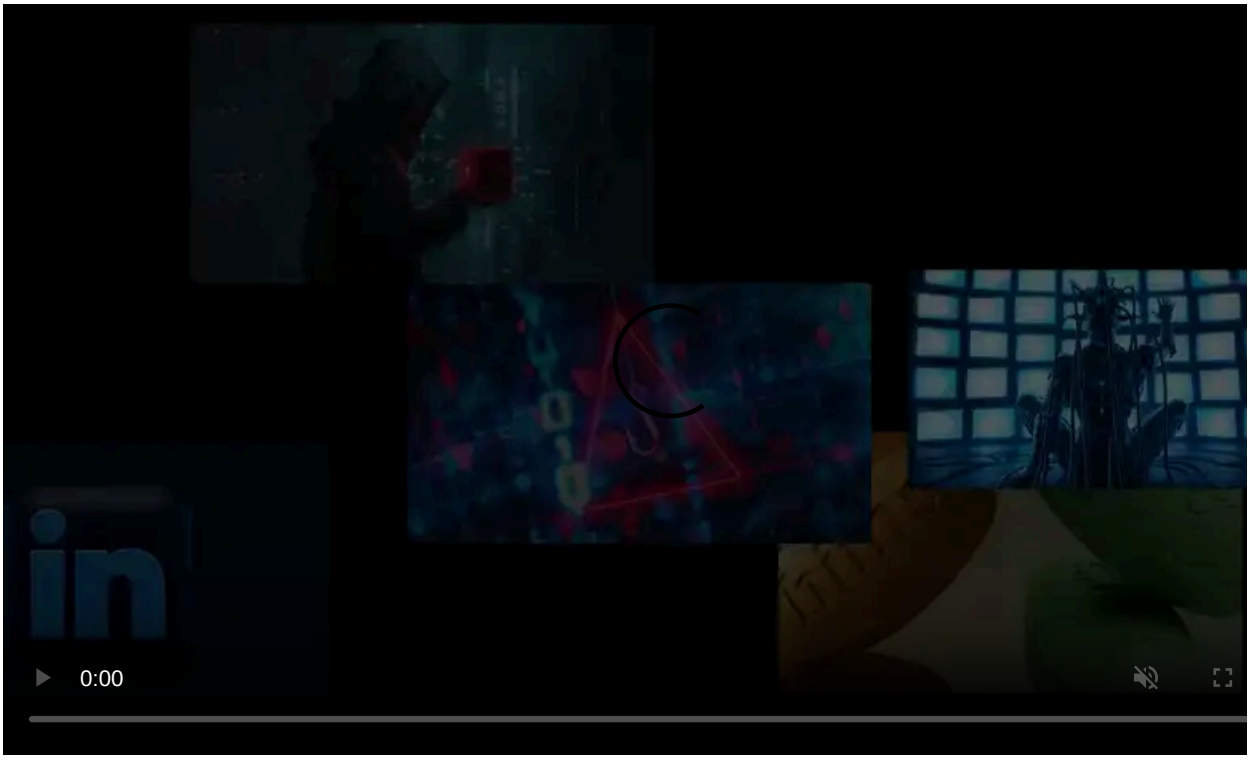
A new CryptoMix, or CryptFile2, variant called Revenge has been discovered by Broad Analysis that is being distributed via the RIG exploit kit. This variant contains many similarities to its predecessor CryptoShield, which is another CryptoMix variant, but includes some minor changes that are described below.

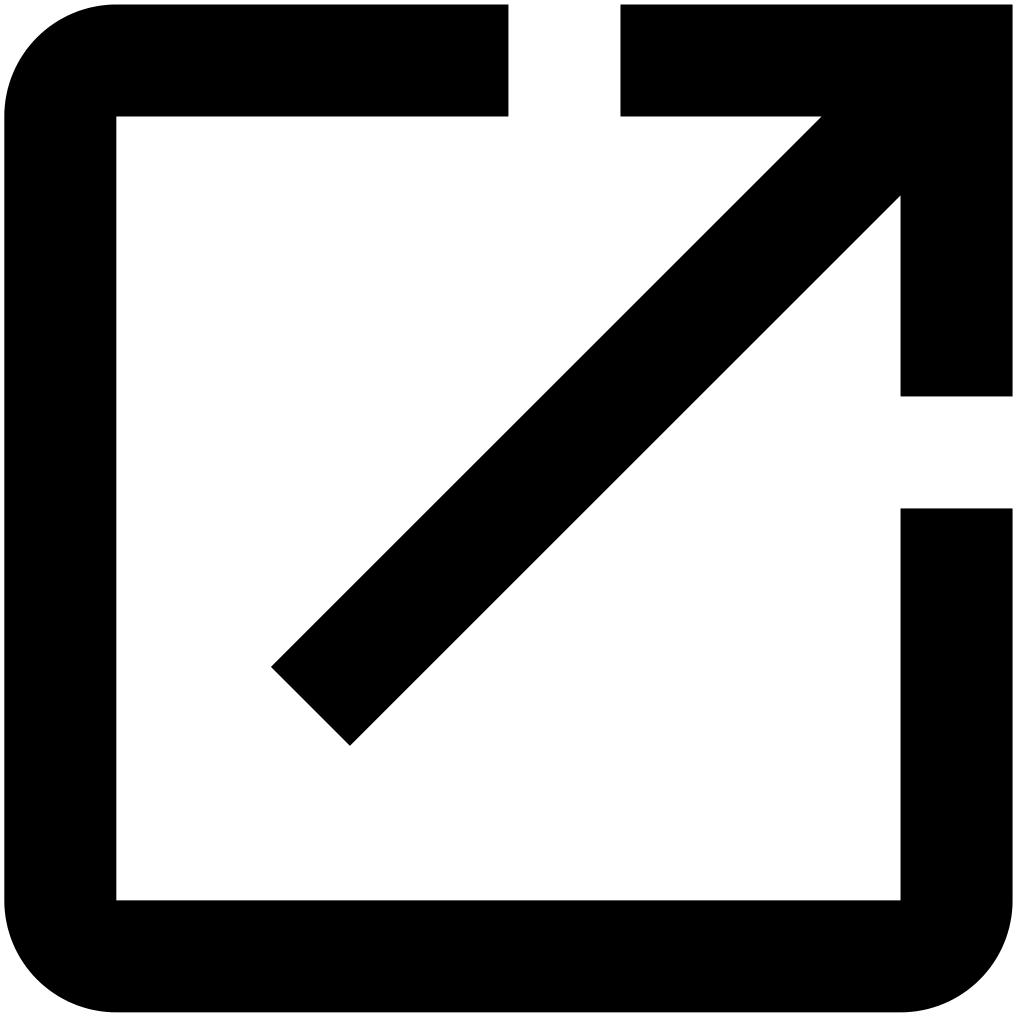
As a note, in this article I will be referring to this infection as the **Revenge Ransomware** as that will most likely be how the victim's refer to it. It is important to remember, though, that this ransomware is not a brand new infection, but rather a new version of the CryptoMix ransomware family.

How Victim's Become Infected with the Revenge Ransomware

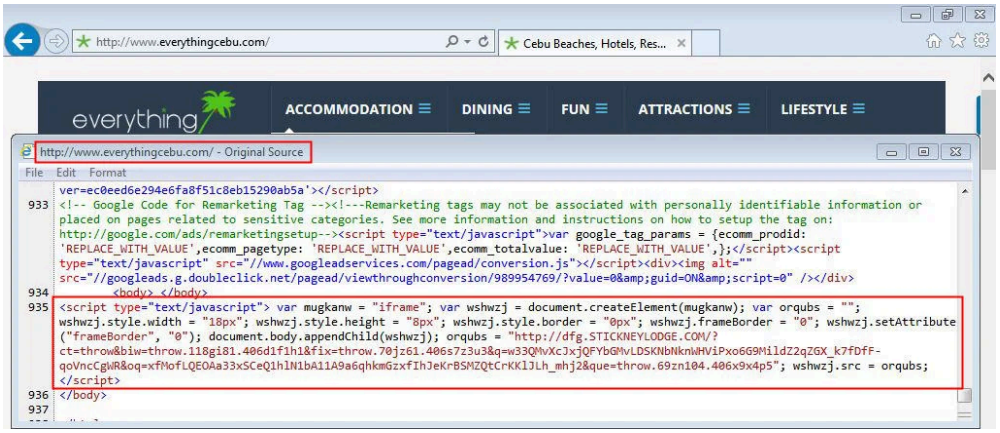
Both BroadAnalysis.com and Brad Duncan, of Malware-Traffic-Analysis.net, have seen Revenge being distributed through web sites that have been hacked so that the RIG Exploit Kit javascript is added pages on the site. When someone visits one of these hacked sites, they will encounter the exploit kit, which will then try to exploit vulnerabilities in their computer in order to install the Revenge Ransomware without their knowledge or permission.

An example of a RIG javascript can be seen in the image below.


0:00



Visit Advertiser website[GO TO PAGE]



Rig Exploit Kit Traffic
Source: BroadAnalysis.com

How the Revenge Ransomware Encrypts a Victim's Files

Once the ransomware executable is downloaded and executed on the victim's computer, it will generate a unique 16 hexadecimal character ID for the victim. It will then terminate the following database related processes so it has full access to the databases in order to encrypt them:

```
msftesql.exe, sqlagent.exe, sqlbrowser.exe, sqlservr.exe, sqlwriter.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe,
```

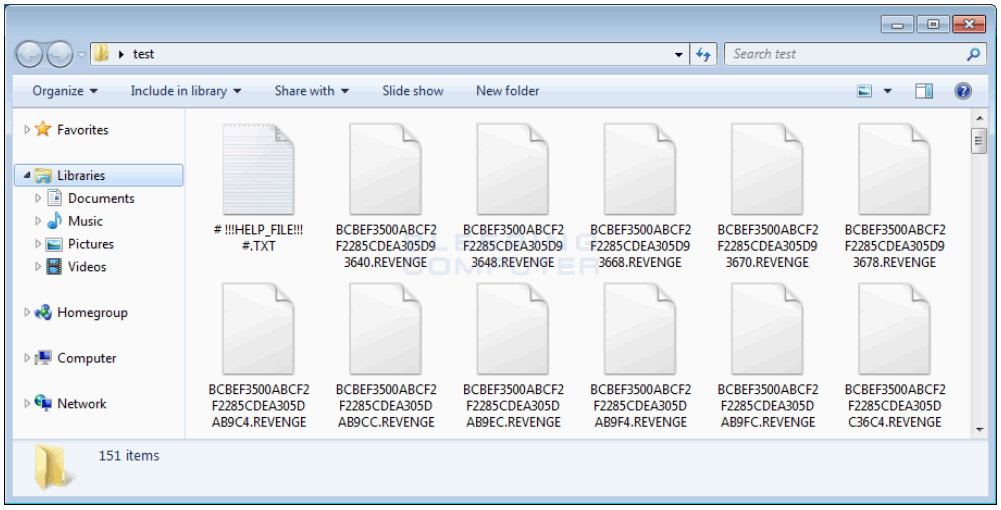
Revenge will then proceed to scan the computer for targeted files and encrypt them. While Revenge's predecessor targeted 454 extensions for encryption, Revenge targets 1,237 extensions, which can be seen at the end of the article.

When Revenge encounters a targeted file it will encrypt it using AES-256 encryption, encrypt the filename, and then append the **.REVENGE** extension to the encrypted file. The format for a renamed file is [16_hex_char_vicimt_id] [16_hex_char_encrypted_filename][unknown_8_hex_char_string][8_char_encrypted_filename].REVENGE. For example, a file called **test.jpg** would be encrypted and renamed as something like **ABCDEF0123456789B7BC7311B474CAFD.REVENGE**.

The AES encryption key used to encrypt the victim's files is then encrypted using a embedded RSA-1024 public key that only the ransomware developer has the ability to decrypt. The current public RSA key is:

```
 -----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCQrO3EuFElsq2cyX+mgWJ4lnK5 xE/YNZru2WpwEvEG2kTIcYthRInXveRJKnUzvtWJ0RCymL3mVbBQXF9J
-----END PUBLIC KEY-----
```

In each folder that Revenge encrypts a file, it will also create a ransom note named **# !!!HELP_FILE!!! #.txt**. Unlike previous versions of CryptoMix, this variant does not create a HTML version of the ransom note as well.



Encrypted Files

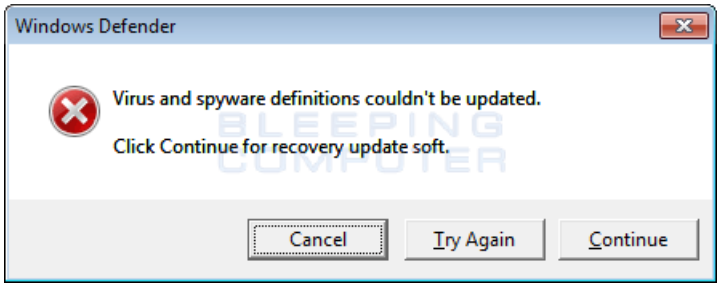
During the infection process, Revenge will issue the following commands to disable the Windows startup recovery and to clear the Windows Shadow Volume Copies as shown below.

```
 cmd.exe /C bcdedit /set {default} recoveryenabled No
cmd.exe /C bcdedit /set {default} bootstatuspolicy ignoreallfailures
C:\Windows\System32\cmd.exe" /C vssadmin.exe Delete Shadows /All /Quiet
"C:\Windows\System32\cmd.exe" /C net stop vss
```

Revenge will also display a fake alert that states:

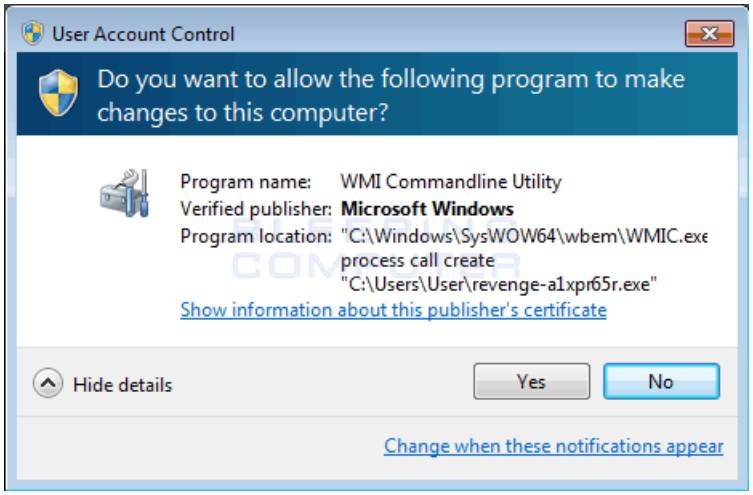
```
Windows Defender Virus and spyware definitions couldn't be updated. Click Continue for recovery update soft.
```

Like the fake alert in CryptoShield, the broken English in the Revenge alert should give victim's a hint that this alert is not legitimate.



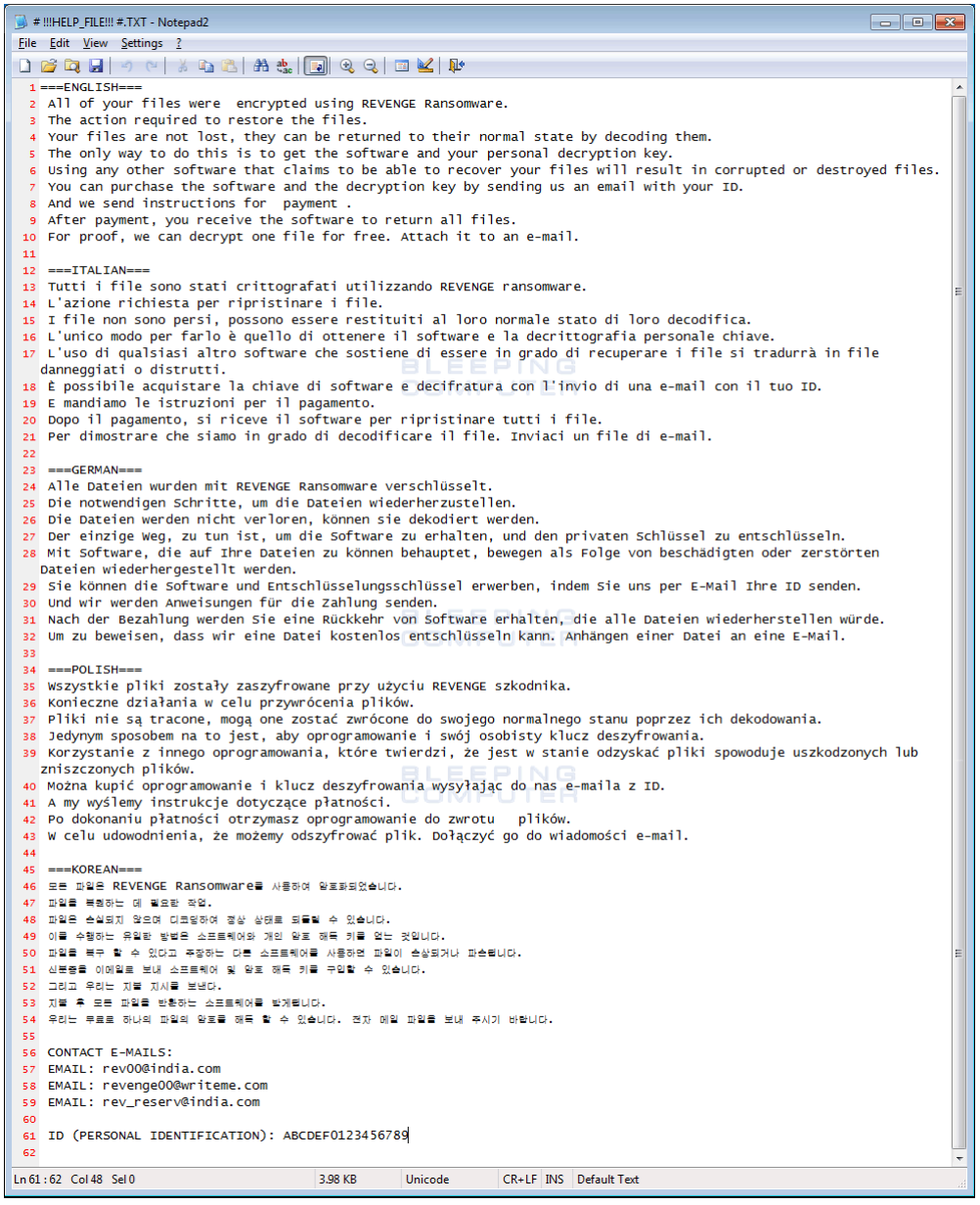
Fake Explorer.exe Alert

Once you press Continue in the above prompt, you will be presented with a User Account Control prompt, which asks if you wish to allow the command **"C:\Windows\SysWOW64\wbem\WMIC.exe" process call create "%UserProfile%\a1x[r65r.exe"** to execute. This explains why the previous alert was being shown; to convince a victim that they should click on the **Yes** button in the below UAC prompt so that ransomware is executed with administrative privileges.



UAC Prompt for the Launch of the SmartScreen.exe Executable

Finally, the Revenge Ransomware will display a ransom note called **# !!!HELP_FILE!!! #.txt**.



Text Ransom Note

This ransom note contains information regarding what happened to your files, a personal identification ID, and three email addresses that can be used to contact the ransom developer for payment instructions. The current email addresses are **rev00@india.com**, **revenge00@writeme.com**, **rev_reserv@india.com**

Unfortunately, at this time there is no way to currently decrypt files encrypted by Revenge for free. For those who wish to discuss this ransomware or receive support, you can always use our CryptoMix or CrypMix Ransomware Help Topic.

File Associated with the Revenge Ransomware Variant:

```
C:\ProgramData\Microsofts\Windows NT\svchost.exe
# !!!HELP_FILE!!! #.txt
```

Revenge Ransomware Hashes:

```
SHA256: f5bceebaecb329380385509d263f55e3d7bddde02377636a0e15f8bfd77a84a6
```

Revenge Ransomware Network Communication:

```
109.236.87.201/js/other_scripts/get.php
```

Example Revenge Ransom Note Text:

```
===ENGLISH===
All of your files were  encrypted using REVENGE Ransomware.
The action required to restore the files.
Your files are not lost, they can be returned to their normal state by decoding them.
The only way to do this is to get the software and your personal decryption key.
Using any other software that claims to be able to recover your files will result in corrupted or destroyed files.
You can purchase the software and the decryption key by sending us an email with your ID.
And we send instructions for  payment .
After payment, you receive the software to return all files.
For proof, we can decrypt one file for free. Attach it to an e-mail.

===ITALIAN===
Tutti i file sono stati crittografati utilizzando REVENGE ransomware.
L'azione richiesta per ripristinare i file.
I file non sono persi, possono essere restituiti al loro normale stato di loro decodifica.
L'unico modo per farlo è quello di ottenere il software e la decrittografia personale chiave.
L'uso di qualsiasi altro software che sostiene di essere in grado di recuperare i file si tradurrà in file danneggiati o
È possibile acquistare la chiave di software e decifratura con l'invio di una e-mail con il tuo ID.
E mandiamo le istruzioni per il pagamento.
Dopo il pagamento, si riceve il software per ripristinare tutti i file.
Per dimostrare che siamo in grado di decodificare il file. Inviaci un file di e-mail.

===GERMAN===
Alle Dateien wurden mit REVENGE Ransomware verschlüsselt.
Die notwendigen Schritte, um die Dateien wiederherzustellen.
Die Dateien werden nicht verloren, können sie dekodiert werden.
Der einzige Weg, zu tun ist, um die Software zu erhalten, und den privaten Schlüssel zu entschlüsseln.
Mit Software, die auf Ihre Dateien zu können behauptet, bewegen als Folge von beschädigten oder zerstörten Dateien wiede
Sie können die Software und Entschlüsselungsschlüssel erwerben, indem Sie uns per E-Mail Ihre ID senden.
Und wir werden Anweisungen für die Zahlung senden.
Nach der Bezahlung werden Sie eine Rückkehr von Software erhalten, die alle Dateien wiederherstellen würde.
Um zu beweisen, dass wir eine Datei kostenlos entschlüsseln kann. Anhängen einer Datei an eine E-Mail.
```

```
===POLISH===
Wszystkie pliki zostały zaszyfrowane przy użyciu REVENGE szkodnika.
Konieczne działania w celu przywrócenia plików.
Pliki nie są tracone, mogą one zostać zwrócone do swojego normalnego stanu poprzez ich dekodowania.
Jedynym sposobem na to jest, aby oprogramowanie i swój osobisty klucz deszyfrowania.
Korzystanie z innego oprogramowania, które twierdzi, że jest w stanie odzyskać pliki spowoduje uszkodzonych lub zniszczon
Można kupić oprogramowanie i klucz deszyfrowania wysyłając do nas e-maila z ID.
A my wyślemy instrukcje dotyczące płatności.
Po dokonaniu płatności otrzymasz oprogramowanie do zwrotu   plików.
W celu udowodnienia, że możemy odszyfrować plik. Dołączyć go do wiadomości e-mail.

===KOREAN===
모든 파일은 REVENGE Ransomware를 사용하여 암호화되었습니다.
파일을 복원하는 데 필요한 작업.
파일은 손실되지 않으며 디코딩하여 정상 상태로 되돌릴 수 있습니다.
이를 수행하는 유일한 방법은 소프트웨어와 개인 암호 해독 키를 얻는 것입니다.
파일을 복구 할 수 있다고 주장하는 다른 소프트웨어를 사용하면 파일이 손상되거나 파손됩니다.
신분증을 이메일로 보내 소프트웨어 및 암호 해독 키를 구입할 수 있습니다.
그리고 우리는 지불 지시를 보낸다.
지불 후 모든 파일을 반환하는 소프트웨어를 받게됩니다.
우리는 무료로 하나의 파일의 암호를 해독 할 수 있습니다. 전자 메일 파일을 보내 주시기 바랍니다.

CONTACT E-MAILS:
EMAIL: rev00@india.com
EMAIL: revenge00@writeme.com
EMAIL: rev_reserv@india.com

ID (PERSONAL IDENTIFICATION): ABCDEF0123456789
```

Revenge Ransomware Associated Emails:

```
 restoring_sup@india.com - SUPPORT;
restoring_sup@computer4u.com - SUPPORT RESERVE FIRST;
restoring_reserve@india.com - SUPPORT RESERVE SECOND;
```

Extensions Targeted by Revenge:

```
, .3G2, .3GP, .7Z, .AB4, .ACH, .ADB, .ADS, .AIT, .AL, .APJ, .ASF, .ASM, .ASP, .ASX, .BACK, .BANK, .BGT, .BIK, .BKF, .BKP,
```

Source: https://www.bleepingcomputer.com/news/security/revenge-ransomware-a-cryptomix-variant-being-distributed-by-rig-exploit-kit/