

HildaCrypt Ransomware Developer Releases Decryption Keys

bleepingcomputer.com/news/security/hildacrypt-ransomware-developer-releases-decryption-keys/

Lawrence Abrams

By

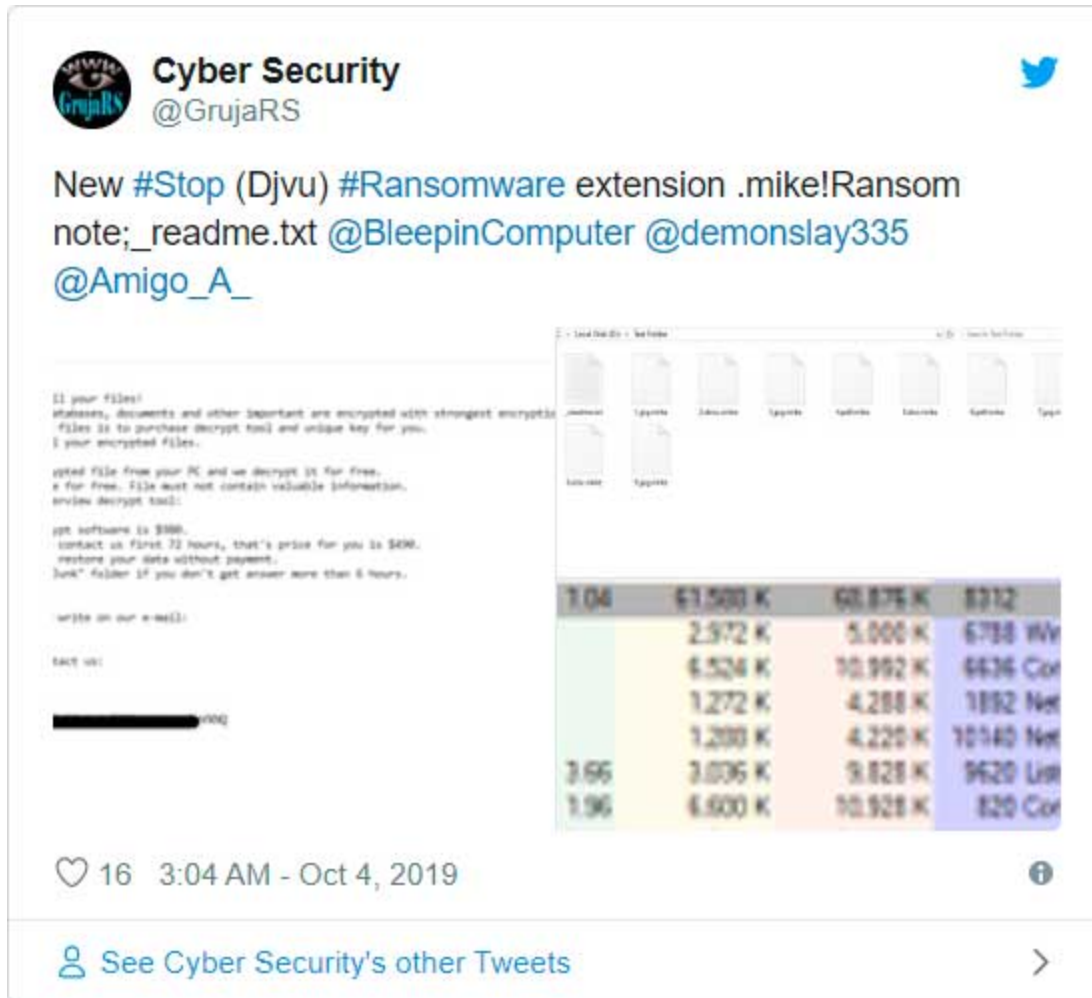
Lawrence Abrams

- October 5, 2019
- 04:47 PM
- 4



The developer behind the HildaCrypt Ransomware has decided to release the ransomware's private decryption keys. With these keys a decryptor can be made that would allow any potential victims to recover their files for free.

When a new ransomware or a variant is discovered, it is very common for researchers to post about them on Twitter. This week, researcher GrujaRS discovered a new ransomware variant and identified it as a STOP variant.



Last night, the developer contacted the researcher to tell him that it was an incorrect identification and that it was actually a variant of the HildaCrypt Ransomware.

As part of this communication, the developer decided to also release the master private decryption keys for the ransomware.

With these keys a decryptor can be made that allows a victim to get their files back for free.

```
RELEASE-2019.TXT (Read Only) - Notepad2
File Edit View Settings ?
1 Greetings from j0hanna!
2
3 These are my private RSA-2048 keys, have fun!
4
5 HILDACRYPT 1.1:
6 <RSAKeyVal><Modulus>28guEbzkzciK3N/EXUq8jGcshuMSCmoFsh/3LoMywzPrnfHGhrgotuY/cs+eSgABQ+rS1B+MMW0wvqwdvp8xUgzgsgogcJt7P+r4b
whfCCyEKDi7PGRTZuTV+xpmG+m+u/JgerBM1F149+0vUMeW5a1sZ408CVFapoJdKMT0P5cJGyLS1VFud8rEv7Ztwccagf88rt8DAut2iSzQix0aw8PpnCH5/74W
E8dAHLKf3sYmR7yFwAdcRjovzdX8/qfjMtZ41sIIIeyajvKfA180T72/UBME2gsAM/BGi2hGLXP5ZGKPGQEF72pic1fRezcpJohNZXZtGCSLfa/jQ==</Modu
lus><Exponent>AQAB</Exponent><P>+etE0HFgvrNj8QPZ/lwETFNHRk+tmshndN/bznik8z3wMu/J3Y1E1E80uxRP3UJ0df2yTLRO5m8tji+nu+rPUBoMGdy
J1tor5E7cI/wLq+JTBw7Uo97afGu/uaofJb+Jc1191HNARaTjqt/9rcVPJYRRDJUDNNDJksUR5kD+gs=</P><Q>4SEwaQZpgChiU9iQ+QQLoJy1ML8+eLY1wX1u
jRgdfE2gh17y/g2yP/qPeZzTKwzOf2tagySVDVfn1MkXpmx9iDWHI1Izwanbygi3r7U9gopiMAIKuD4Mhtxt1eLpuozBbmWJvuEe/BBZ16zIk2bis7Mf3NSG80y
NTFvQfBw8c=</Q><DP>FZdr5I7wzELzem0BAV1zn48JcJyGLNDroCOD5YEb/PJ6trX0ZTLHUDW5QAA/c31JHMhKwnL2sxhnc7f5advs3ScdfiHdvo2+isQdeg
uONFLg0b9eRk/+bXm3E8a6h2kHXW0K+nJG2EpszcVJ/nQAnegzPUBthcdqwxZHK50=</DP><DQ>ogZH0fGBo3Rb1InUS9ZC3rObuqWAF0u0XB1Gycat5ve4krSa
vdxZzUauwncU/4SkzjSMAT3HV0Jh3H0gyD1cbbdkDFkZDa16c0omLu0Z8ChIb12ieRwe+s7TIHhNapoUTX8AQpZ5Tv/6+pt9KkYJubRe3dLDK6cSrUko2CU=
</DQ><InverseQ>9JirTVM8ma+ykxb08BEHLdiouNA3XFg0BdrfKctRY5Az4yy2AG6TzjQjvWvfitcJfUmrRTZ4e/QuFL1Tbc8rbbVc28Zw3cN3RPMHF00uY5w
J5VN1etGxwb9cN7i36S5omx2qijsPoywRb2chXVGiImi082rghq+/1JfwdwbXk=</InverseQ><D>Y1iBopNF+YUE15AFgmK3HVM+GWRkbpQnfUtypxuSXBpL1n
OLgaoM/v/mnkrDRwyd1L6p+4Bzs1EMhb7p0sHCKmDtGE3GhrVGDGvJq8krTpuq99/aNXU1VDB4/ua5XAS32Xn8Cu5m/qPj8KNFwGfMT/j095jL+8cjqv6+1BU
hd687PwBtkk6VRDgPzupML708SwcN8cmoJ2Bwje8wah0iRzH0TPjwLXPM7LTPueYA1KHuxrjBNGIZYRonN0G6ujgTgTorLkTkQunrExHS15RonNdr9ZrDm43s8r
A4nNhuL7hvfvmheomquho75bz9Q7LXyVibv7CQ0DvCy+zIQ==</D></RSAKeyVal>
7 HILDACRYPT 1.2:
8 <RSAKeyVal><Modulus>0DFRVFCwfbLeL/2mm0fbx985TmG9cRiwl1u3YNNXmpZM9ZieY11p9NmjmcaN82Xpx1Z5ak/Pv558szc8zoyqwmSxwe9p06vbsrCPAP
+At81avXa6XnN1AcMdd7SRJjKqUp14S3FSY14FC7hyGpXotr9J4unmyH84Z3dyppy+m0kfkHoYknkRNWINGL63IvRHX/Z4Aezp9cPXTk2qThpTK0u14NH969Tx
p9uwbAwvzHJAWvTAHwm16+8H96knPqcm0ggiwvRhiVvJou3ofT8d8hbkgYfE0kdY1p5eL4DNzWEA2M/mLgX8q1fVYFSpawAvBBoP6sJmMtIGc761F2w==</Modu
lus><Exponent>AQAB</Exponent><P>+21gMRGcwvymFt9sWBZ9GshfypwI3GeeazjKfjN3sdr/HZVo/IU2oohmEw84JNTS9fx9NwcbmB3c9z7I0ivvtwsrha
+9AktCPX2eSvHMLZzcbN0kkb99r53HGZLQKE9LHQVTlWfNELZwukPFBkZuk4j83SHS2NgkAr+xwXbQC=</P><Q>0KwX2BwrRxF1fjnfV5H7Qqj0EcrhvoBkACVf2
SYrvvt7Xpq01jKkpx9wssDVGyvpGNLh01JYoN8660grEdpStiN90IuDdMVGfKBECK/pXcSBwkoFah/v6A79VIEPerBD/k2nurzYkd2NrO+YTQF6C9Aq4Q/zRQDY
C1jfbchN40=</Q><DP>xwiVr2Zak7bckCYRGauXLNmn417lyfHK1uc3r1wFZ1hgHnRmWc62BaxotzrTkXgf2Sulcr78irFIQTLQpcr9R9iQw32bpTvdMx63T1
QEVs3q6VJE1x+7RZAiGRXiflQqSF43S81yykm/fyptbnWxeLtu/DAHEDAI4FQWugIc=</DP><DQ>SijW8IuLfk2hJ8oFv7XVbu3hKvqQydmOunshynPFxw6BUHVS
sr/d8jDqYUYGJIDFXd5k2Yz8ePaas24tucP2Bi9GFh+qzP55Zuo98rEpFzMFm591Mx8hg9Xxy4Vkv8Xzr1pkqldLdFt5Bh9AS/dihycr51A3D9LkwtHa8KXk=
</DQ><InverseQ>Mk/rMTC82RGSv0F6GxdvurAxpjoo1i9K6j6wr076C1nit8qyp8b3y/erThX1os11p18FJIWHR1lftEueK2K0atqf1m7/Q7ip1M/b0ene/IB
```

HildaCrypt Ransomware Decryption Keys

After giving the keys to Michael Gillespie, he confirmed they were legitimate [released a decryptor](#) using them.

For those who wish to view the keys or create a decryptor based on them, they can be [accessed here](#).

HildaCrypt was created for fun

BleepingComputer had a conversation with the ransomware developer last night and was told that HildaCrypt was only made for fun and "it was mainly an educational thing really".

They further told us "hildacrypt never was used on anyone" and that they released the keys in case "some kid gets a hold of these binaries I hope the keys would be of some use".

After further discussion, the developer intimated that they were probably going to stop development of the ransomware and instead focus on getting involved in more legitimate efforts of the cybersecurity community.

Related Articles:

[HelloKitty ransomware source code leaked on hacking forum](#)

[TransForm says ransomware data breach affects 267,000 patients](#)

[Critical Atlassian Confluence bug exploited in Cerber ransomware attacks](#)

[US sanctions Russian who laundered money for Ryuk ransomware affiliate](#)

[TellYouThePass ransomware joins Apache ActiveMQ RCE attacks](#)




- [Decryptor](#)
- [HildaCrypt](#)
- [Ransomware](#)


[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- [Previous Article](#)
- [Next Article](#)

Comments

-  nkdev Photo
-  GT500 Photo
-  cybercynic Photo

-  matutn Photo
[matutn](#) - 4 years ago

-
-

Hi, do you have any information about ".coot".

I tried with many decryptors like rannohdecryptor, trend micro (cause I read it could be "CryptXXX V...", then I read that could be "hildacrypt" and used emsisoft decryptor, but nothing is working.

The note says:

ATTENTION!

Don't worry, you can return all your files!

All your files like photos, databases, documents and other important are encrypted with strongest encryption and unique key.

The only method of recovering files is to purchase decrypt tool and unique key for you.

This software will decrypt all your encrypted files.

What guarantees you have?

You can send one of your encrypted file from your PC and we decrypt it for free.

But we can decrypt only 1 file for free. File must not contain valuable information.

You can get and look video overview decrypt tool:

<https://we.tl/t-lbdGyCKhdr>

Price of private key and decrypt software is \$980.

Discount 50% available if you contact us first 72 hours, that's price for you is \$490.

Please note that you'll never restore your data without payment.

Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.

thx

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
