WORK Cryptomix Ransomware Variant Released

bleepingcomputer.com/news/security/work-cryptomix-ransomware-variant-released

By
Lawrence Abrams

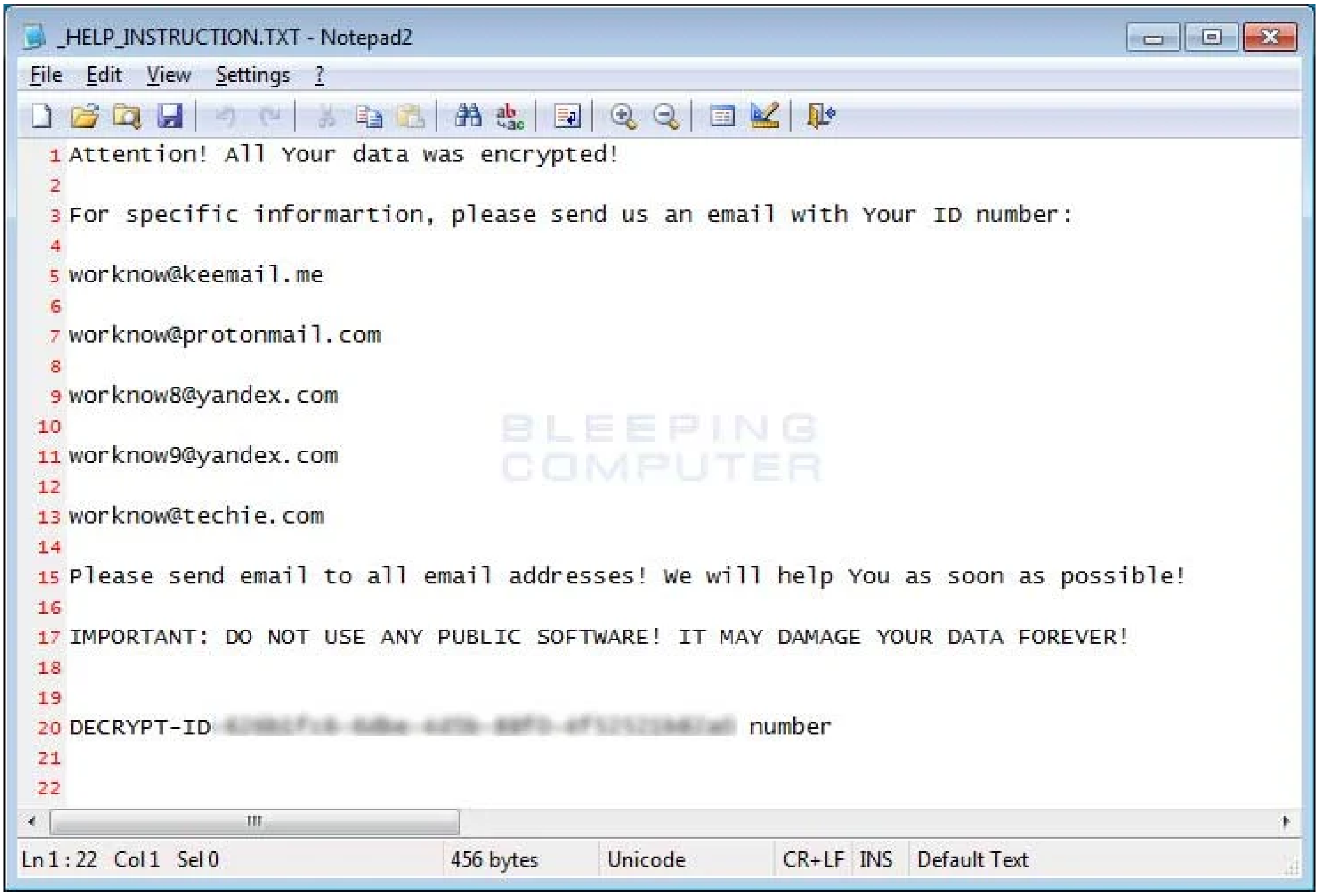
- December 13, 2017
- 11:58 AM
- 0

Today, BleepingComputer discovered a new variant of the CryptoMix ransomware that appends the **.WORK** extension to encrypted files and changes the contact emails used by the ransomware.

In this article I will provide a brief summary of any changes that have occurred in this new variant. As we are always looking for weaknesses, if you are a victim of this variant and decide to pay the ransom, please send us the decryptor so we can take a look at it. You can also discuss or receive support for Cryptomix ransomware infections in our dedicated Cryptomix Help & Support Topic.

Changes in the WORK Cryptomix Ransomware Variant

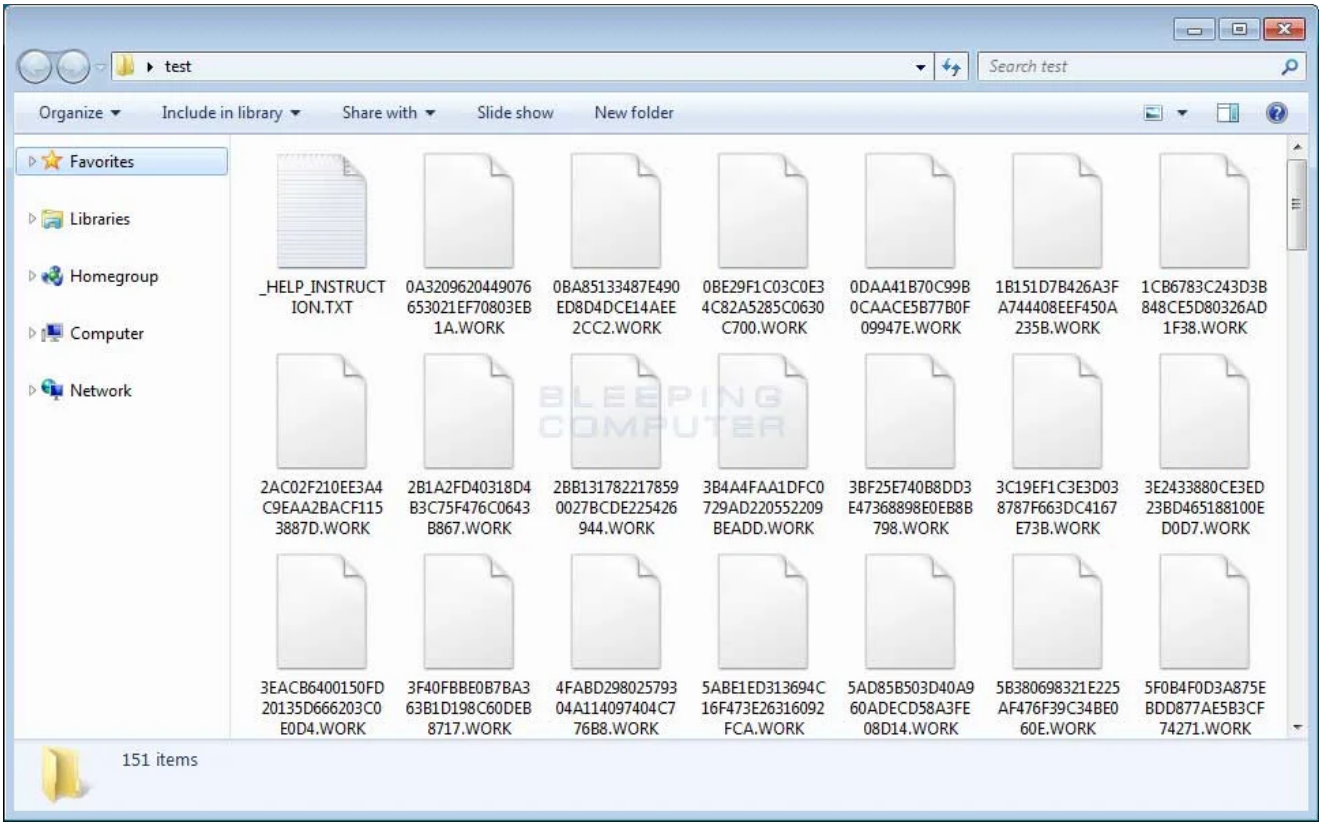
While the encryption methods stay the same in this variant, there have been some slight differences. The ransom note is still named **_HELP_INSTRUCTION.TXT**, but now uses the **worknow@keemail.me, worknow@protonmail.com, worknow8@yandex.com, worknow9@yandex.com,** and **worknow@techie.com** emails for a victim to contact for payment information.



```
Attention! All Your data was encrypted!

For specific informartion, please send us an email with Your ID number:

worknow@keemail.me

worknow@protonmail.com

worknow8@yandex.com

worknow9@yandex.com

worknow@techie.com

Please send email to all email addresses! We will help You as soon as possible!

IMPORTANT: DO NOT USE ANY PUBLIC SOFTWARE! IT MAY DAMAGE YOUR DATA FOREVER!


DECRYPT-ID [redacted] number


```

WORK CryptoMix Ransom Note

The next noticeable change is the extension appended to encrypted files. With this version, when a file is encrypted by the ransomware, it will modify the filename and then append the .WORKextension to encrypted file's name. For example, a test file encrypted by this variant has an encrypted file name of **0D0A516824060636C21EC8BC280FEA12.WORK.**


test
Search test
Organize
Include in library
Share with
Slide show
New folder
Favorites
Libraries
Homegroup
Computer
Network
_HELP_INSTRUCTION.TXT
0A3209620449076653021EF70803EB1A.WORK
0BA85133487E490ED8D4DCE14AEE2CC2.WORK
0BE29F1C03C0E34C82A5285C0630C700.WORK
0DAA41B70C99B0CAACE5B77B0F09947E.WORK
1B151D7B426A3FA744408EEF450A235B.WORK
1CB6783C243D3B848CE5D80326AD1F38.WORK
2AC02F210EE3A4C9EAA2BACF1153887D.WORK
2B1A2FD40318D4B3C75F476C0643B867.WORK
2BB1317822178590027BCDE225426944.WORK
3B4A4FAA1DFC0729AD220552209BEADD.WORK
3BF25E740B8DD3E47368898E0EB8B798.WORK
3C19EF1C3E3D038787F663DC4167E73B.WORK
3E2433880CE3ED23BD465188100ED0D7.WORK
3EACB6400150FD20135D666203C0E0D4.WORK
3F40FBBE0B7BA363B1D198C60DEB8717.WORK
4FABD29802579304A114097404C776B8.WORK
5ABE1ED313694C16F473E26316092FCA.WORK
5AD85B503D40A960ADECD58A3FE08D14.WORK
5B380698321E225AF476F39C34BE060E.WORK
5F0B4F0D3A875EBDD877AE5B3CF74271.WORK
151 items
BLEEPING COMPUTER

Folder of Encrypted WORK Files

As this is just a cursory analysis of this new variant, if anything else is discovered, we will be sure to update this article.

How to protect yourself from the WORK CryptoMix Ransomware

In order to protect yourself from ransomware, it is important that you use good computing habits and security software. First and foremost, you should always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack.

You should also have security software that incorporates behavioral detections to combat ransomware and not just signature detections or heuristics. For example, Emsisoft Anti-Malware and Malwarebytes Anti-Malware both contain behavioral detection that can prevent many, if not most, ransomware infections from encrypting a computer.

Last, but not least, make sure you practice the following security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them,
- Scan attachments with tools like VirusTotal.

- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore it is important to keep them updated.
- Make sure you use have some sort of security software installed that uses behavioral detections or white list technology. White listing can be a pain to train, but if your willing to stock with it, could have the biggest payoffs.
- Use hard passwords and never reuse the same password at multiple sites.

For a complete guide on ransomware protection, you visit our How to Protect and Harden a Computer against Ransomware article.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

IOCs

File Hashes:

```
SHA256: 69fa88c5b353f55edbb7187c090bee377e54900e1c78c580d7b3b3084c9d7d0b
```

Filenames associated with the WORK Cryptomix Variant:

```
_HELP_INSTRUCTION.TXT
C:\ProgramData\[random].exe
```

WORK Ransom Note Text:

```
Attention! All Your data was encrypted!

For specific informartion, please send us an email with Your ID number:

worknow@keemail.me

worknow@protonmail.com

worknow8@yandex.com

worknow9@yandex.com

worknow@techie.com

Please send email to all email addresses! We will help You as soon as possible!

IMPORTANT: DO NOT USE ANY PUBLIC SOFTWARE! IT MAY DAMAGE YOUR DATA FOREVER!


DECRYPT-ID-[id] number
```

Emails Associated with the WORK Ransomware:

```
worknow@keemail.me
worknow@protonmail.com
worknow8@yandex.com
worknow9@yandex.com
worknow@techie.com
```

Executed Commands:

```
sc stop VVS
sc stop wscsvc
sc stop WinDefend
sc stop wuauserv
sc stop BITS
sc stop ERSvc
sc stop WerSvc
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
```

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.