WORK Cryptomix Ransomware Variant Released

By Lawrence Abrams

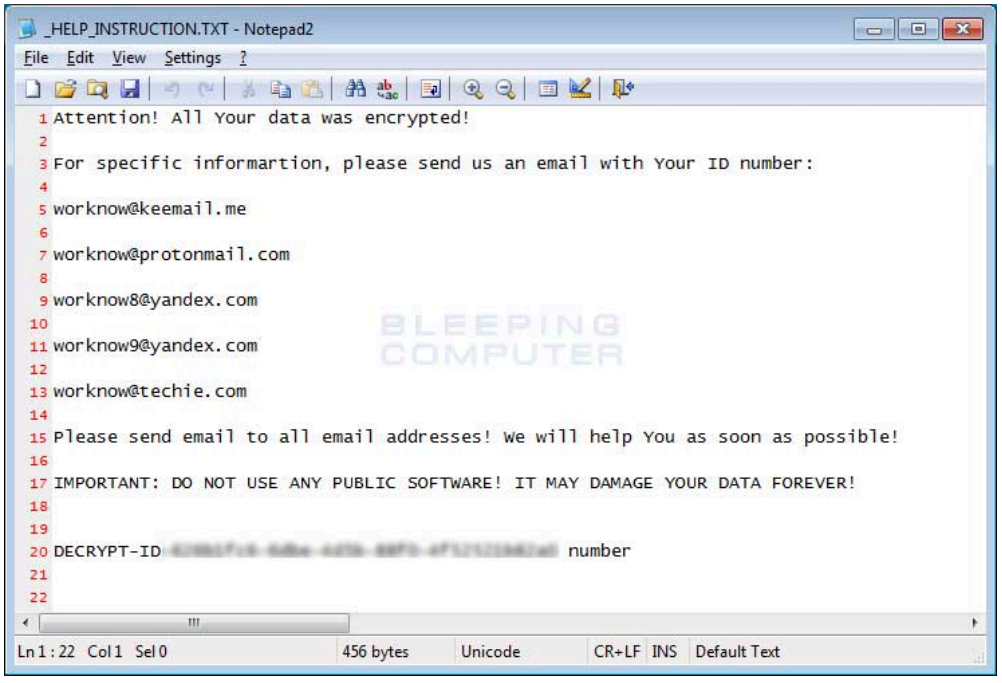
Published: 2017-12-13 · Archived: 2026-04-05 18:24:36 UTC

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.

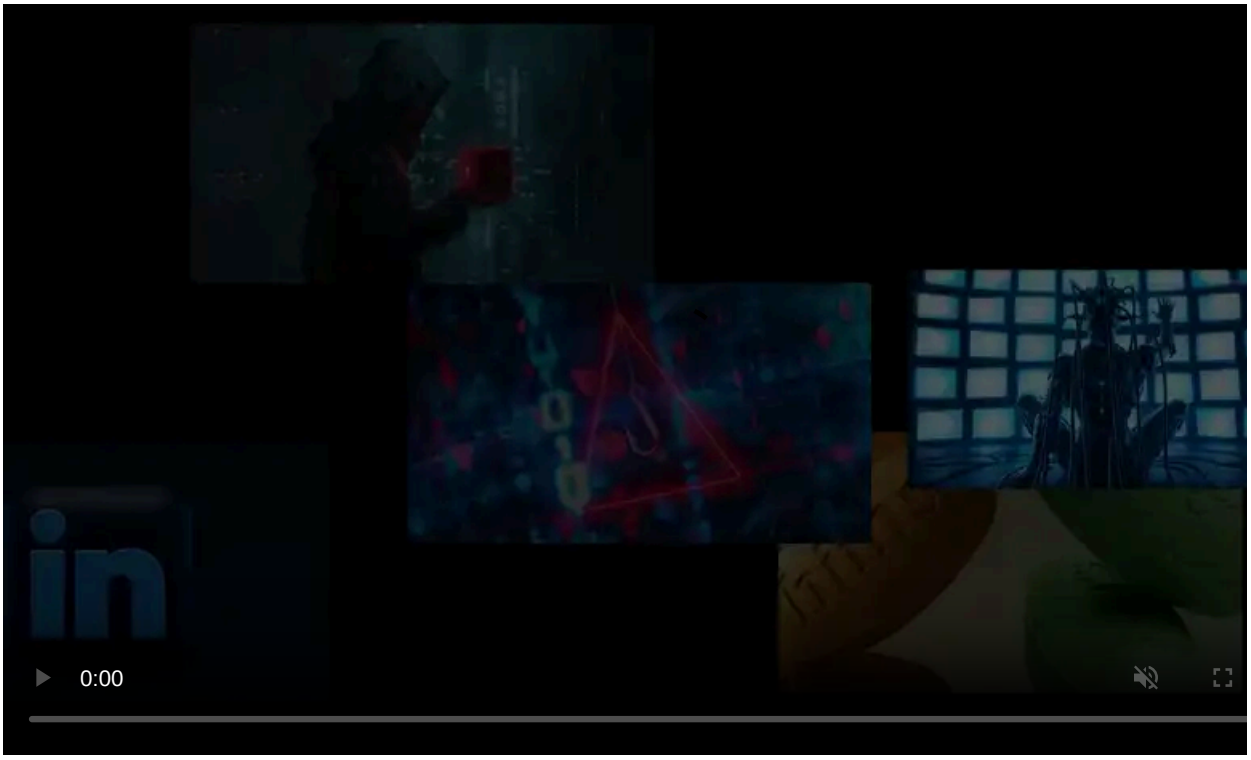
Changes in the WORK Cryptomix Ransomware Variant

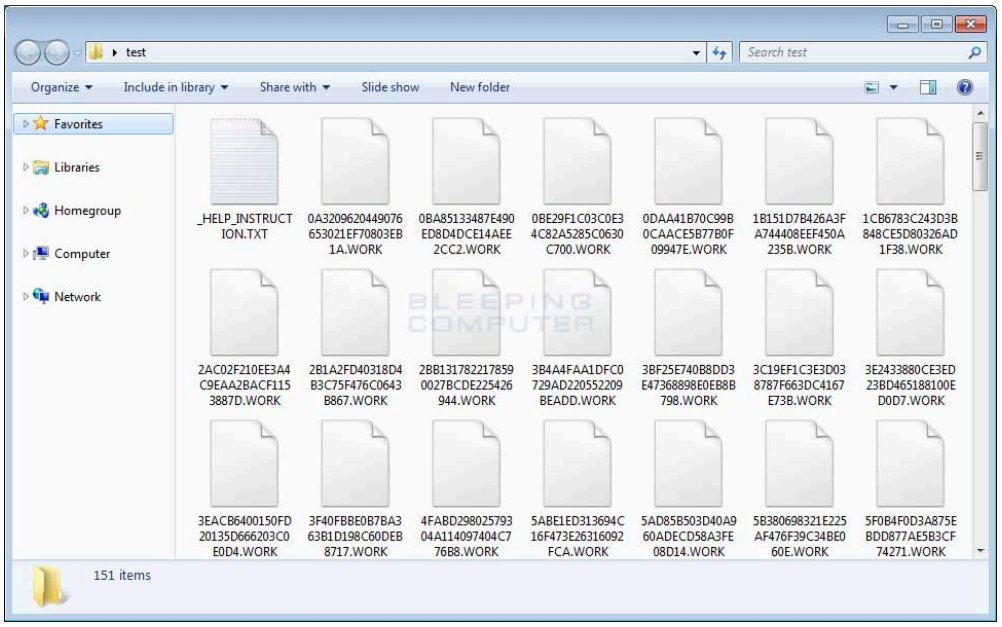
While the encryption methods stay the same in this variant, there have been some slight differences. The ransom note is still named **_HELP_INSTRUCTION.TXT**, but now uses the **worknow@keemail.me, worknow@protonmail.com, worknow8@yandex.com, worknow9@yandex.com,** and **worknow@techie.com** emails for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



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 .WORK extension to encrypted file's name. For example, a test file encrypted by this variant has an encrypted file name of **0D0A516824060636C21EC8BC280FEA12.WORK.**


0:00



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.

IOCs

File Hashes:

```
SHA256: 69fa88c5b353f55edbb7187c090bee377e54900e1c78c580d7b3b3084c9d7d0b
```

Filenames associated with the WORK Cryptomix Variant:

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

WORK Ransom Note Text:

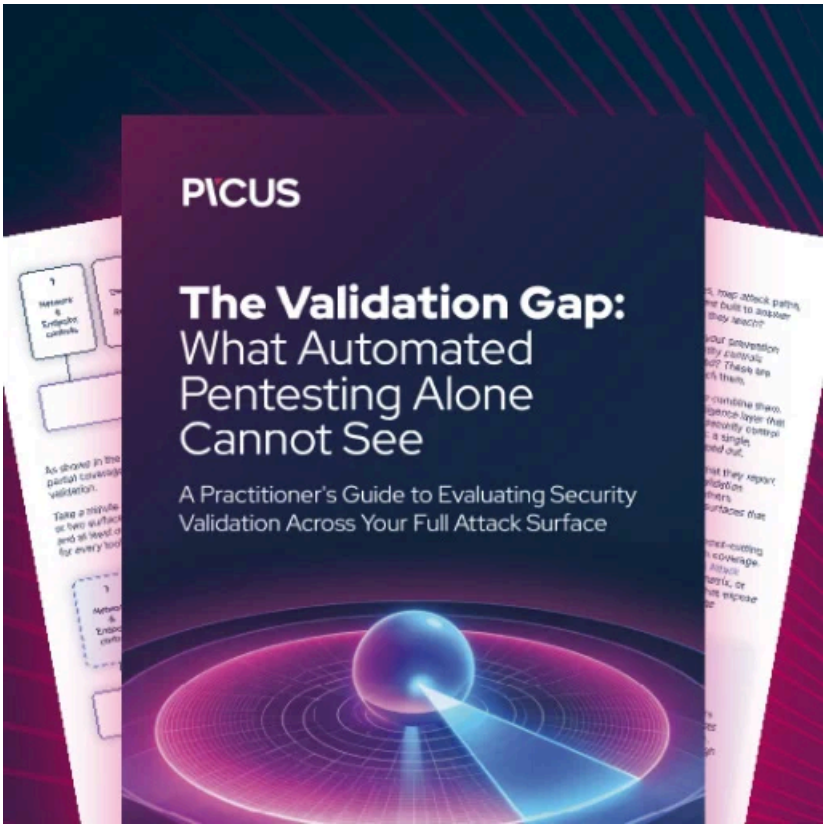
```
 Attention! All Your data was encrypted!

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
```



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/work-cryptomix-ransomware-variant-released/