# New crypto-ransomware hits macOS

welivesecurity.com/2017/02/22/new-crypto-ransomware-hits-macos/

February 22, 2017

This last month we have seen a new ransomware for Mac. Written in Swift, it is distributed on BitTorrent distribution site as “Patcher” for pirating popular software.

Marc-Etienne M.Léveillé
22 Feb 2017 - 02:00PM

This last month we have seen a new ransomware for Mac. Written in Swift, it is distributed on BitTorrent distribution site as “Patcher” for pirating popular software.

Crypto-ransomware has been very popular lately amongst cybercriminals. While most of it targets the Windows desktop, we’ve also seen machines running Linux or macOS being compromised by ransomware in 2016 with, for example, KillDisk affecting Linux and KeRanger attacking OS X.

Early last week, we have seen a new ransomware campaign for Mac. This new ransomware, written in Swift, is distributed via BitTorrent distribution sites and calls itself “Patcher”, ostensibly an application for pirating popular software.

## Distribution

Figure 1 – BitTorrent site distributing Torrent files containing OSX/Filecoder.E

The Torrent contains a single ZIP file – an application bundle. We saw two different fake application “Patchers”: one for Adobe Premiere Pro and one for Microsoft Office for Mac. Mind you, our search was not exhaustive; there might be more out there.

Figure 2 - Icons of the "Patchers" as seen in Finder

Figure 2 – Icons of the “Patchers” as seen in Finder

The application is generally poorly coded. The window has a transparent background, which can be quite distracting or confusing (see Figure3), and it’s impossible to reopen the window if it is closed.

The application has the bundle identifier NULL.prova and is signed with a key that has not been signed by Apple.

```
$ codesign -dv "Office 2016 Patcher.app"
Executable=Office 2016 Patcher.app/Contents/MacOS/Office 2016 Patcher
Identifier=NULL.prova
Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20100 size=507 flags=0x2(adhoc) hashes=11+3 location=embedded
Signature=adhoc
Info.plist entries=22
TeamIdentifier=not set
Sealed Resources version=2 rules=12 files=14
Internal requirements count=0 size=12
```

Figure 3 - The main window of the ransomware

Figure 3 – The main window of the ransomware

## File encryption process

Clicking the start button – shown in Figure 3 – launches the encryption process. It copies a file called README!.txt all around the user's directories such as “Documents” and “Photos”. Its content is shown later in the article.

Then the ransomware generates a random 25-character string to use as the key to encrypt the files. The same key is used for all the files, which are enumerated with the find command line tool; the zip tool is then used to store the file in an encrypted archive.

Finally, the original file is deleted with rm and the encrypted file's modified time is set to midnight, February 13th 2010 with the touch command. The reason for changing the file's modified time is unclear. After the /Users directory is taken care of, it does the same thing to all mounted external and network storage found under /Volumes.

Once all the files are encrypted there is code to try to null all free space on the root partition with diskutil, but the path to the tool in the malware is wrong. It tries to execute /usr/bin/diskutil, however the path to diskutil in macOS is /usr/**s**bin/diskutil.

Figure 4 - Encrypted document and README!.txt as they appear in Finder

Figure 4 – Encrypted document and README!.txt as they appear in Finder

The instructions left for the victims in the README!.txt files are hardcoded inside the Filecoder, which means that the Bitcoin address and email address are always the same for every victim running the same sample. The message and contact details were the same in both samples we analyzed.

```
NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files ?
All of your files were protected by a strong encryption method.

What do I do ?

So , there are two ways you can choose: wait for a miracle or start obtaining BITCOIN NOW! , and restore YOUR DATA the easy way
If You have really valuable DATA, you better NOT WASTE YOUR TIME, because there is NO other way to get your files, except make a PAYMENT

FOLLOW THESE STEPS:
1) learn how to buy bitcoin https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
2)send 0.25 BTC to 1EZrvz1kL7SqfemkH3P1VMtomYZbfhznkb
3)send your btc address and your ip (you can get your ip here https://www.whatismyip.com) via mail to rihofoj@mailinator.com
4)leave your computer on and connected to the internet for the next 24 hours after payment, your files will be unlocked. (If you can not wait 24 hours make a payment of 0.45 BTC your files will be unlocked in max 10 minutes)


KEEP IN MIND THAT YOUR DECRYPTION KEY WILL NOT BE STORED ON MY SERVER FOR MORE THAN 1 WEEK SINCE YOUR FILE GET CRYPTED,THEN THERE WON'T BE ANY METHOD TO RECOVER YOUR FILES, DON'T WASTE YOUR TIME!
```

So far, there is no transaction related to the Bitcoin wallet. Which mean the authors have not made a dime from this ransomware. Hopefully this post will raise awareness and keep the wallet's balance at zero.

## No decryption possible, even from the author

There is one big problem with this ransomware: it doesn't have any code to communicate with any C&C server. This means that there is no way the key that was used to encrypt the files can be sent to the malware operators.

This also means that there is no way for them to provide a way to decrypt a victim's files. Paying the ransom in this case will not bring you back your files. That's one of the reasons we advise that victims **never** pay the ransom when hit by ransomware.

Alas, the random ZIP password is generated with arc4random_uniform which is considered a secure random number generator. The key is also too long to brute force in a reasonable amount of time.

## Public inbox

Interestingly, the email address is an address provided by Mailinator. Mailinator provides a free inbox to anyone without requiring them to register or authenticate. This means it is possible to see the inbox used to communicate with the malware author. We've been monitoring this inbox for the last week and didn't see any messages. However, it's possible the messages get deleted really fast and we simply missed them.

## Conclusion

This new crypto-ransomware, designed specifically for macOS, is surely not a masterpiece. Unfortunately, it's still effective enough to prevent the victims accessing their own files and could cause serious damage.

There is an increased risk when downloading pirated software that someone is using a dubious channel for acquiring software in order to make you execute malware. ESET recommends that you have a security product installed but the most important precaution in case you encounter crypto-ransomware is to have a current, **offline**, backup of all your important data.

ESET products detect this threat as OSX/Filecoder.E.

## Samples

| **SHA-1** | **Filename** | **Type** | **ESET detection name** |
|---|---|---|---|
| 1b7380d283ceebcabb683464ba0bb6dd73d6e886 | Office 2016 Patcher.zip | ZIP of App bundle | OSX/Filecoder.E |
| a91a529f89b1ab8792c345f823e101b55d656a08 | Adobe Premiere Pro CC 2017 Patcher.zip | ZIP of App bundle | OSX/Filecoder.E |
| e55fe159e6e3a8459e9363401fcc864335fee321 | Office 2016 Patcher | Mach-O | OSX/Filecoder.E |
| 3820b23c1057f8c3522c47737f25183a3c15e4db | Adobe Premiere Pro CC 2017 Patcher | Mach-O | OSX/Filecoder.E |

22 Feb 2017 - 02:00PM

## Newsletter

## Discussion