Issued 2/23/17

Swift-based Ransomware Targets MacOS Pirates

New ransomware for the Mac has been discovered by security researchers, with the "poorly coded" malware created in Swift encrypting the user's files and demanding a payment, without any possibility of decrypting the files even if the ransom is paid.

Circulating via BitTorrent sites and called "Patcher," the malware poses as a crack for pirates to get around copy protection and licensing systems used in popular software suites. Researcher Marc-Etienne M.Léveillé found two different fake patchers that used the same code, posing as ways to unlock Microsoft Office for Mac 2016 and Adobe Premiere Pro CC 2017, but suggests there may be more instances of the malware circulating around under different names.

When extracted from the archive and executed, the malware opens up a window advising users to press the start button to patch the pirated software. If clicked, the ransomware then spreads around a "readme" file to various user directories, before encrypting all other user files using a randomly-generated 25-character key in an archive, and deleting the original files.

The Readme file explains to the user the files are encrypted, and to pay 0.25 bitcoin to a specific wallet address to unlock them within seven days.

While it is claimed files will be decrypted within 24 hours of the random's payment, another option to pay 0.45 bitcoin is also offered, touting decryption within ten minutes.

The researcher notes the malware is "generally poorly coded" in a number of ways. Produced using Swift, the application's window is impossible to open if it is closed, while code to try and use Disk Utility to null the free space on the root partition uses the wrong path to the tool.

The details within the Readme file are hard coded, meaning all victims are presented with the same bitcoin wallet and email address instead of information unique to each infection. An inspection of the Bitcoin wallet at the time of reporting reveals there have yet to be any transactions, which means no-one has so far paid the creator's ransom.

Unlike many other examples of cryptographic ransomware, it is noted victims will not be able to get their files back by decryption, even if the ransom is paid. There is no code in the malware that sends the key to the operator, so there is no possibility of providing the "service" of decrypting the files for the user, while the length of the key also suggests a brute force attack would take too long to accomplish.

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

Léveillé recommends having a current offline backup of all important data, as well as security software, to help protect against similar threats.