CYBERSECURITY ADVISORY

16 August 2017

(U) SyncCrypt Ransomware Hides Inside JPG Files

(U//FOUO) ***On 16 August, a new sophisticated ransomware dubbed SyncCrypt, was reportedly detected. This malware is delivered as an email attachment. The email topic and attachment both appear to target persons associated with legal activities; according to open source reports citing a typical naming convention such as CourtOrder_845493809.wsf.***

- (U) When executed, these WSF files contain a JScript script that will download an image from one of three sites as shown below.
    - (U) https:[//]image.ibb.co/mxRqXF/arrival[.]jpg
      http:[//]sm.uploads.im/X8IO1[.]jpg
      http:[//]185.10.202.115/images/arrival[.]jpg
- (U) Once the Sync.exe executable is extracted from the zip file as described above, the WSF file will create a Windows scheduled task called Sync that is configured to go off in one minute after the WSF file is executed. Once the sync.exe file is executed it will scan the computer for certain file types and encrypts them using AES encryption. Once encrypted, the file will have the .kk extension appended to the filename.
- (U) When SyncCrypt has finished encrypting a computer, a folder called README will appear on the desktop. This folder contains the AMMOUNT.txt, key, readme.html, and readme.png files. The ammount.txt file is the ransom amount, the key is the encrypted decryption key, and the other two files are the ransom notes. SyncCrypt will then automatically open and display the readme.html ransom note in the victim's default browser.
- (U) After a payment has been made, the victim is told to send an email containing the key file to one of the getmyfiles@keemail.me, getmyfiles@scryptmail.com, or getmyfiles@mail2tor.com emails to get a decrypter.
- (U) Listed below are the SHA256 File Hashes:
  877488d8f43548c6e3016abd33e2d593a44d450f1910084733b3f369cbdcae85 (sync.exe)
  3049a568c1c1cd4d225f8f333bf05e4560c8f9de5f167201253fedf35142fe3e (CourtOrder_845493809.wsf)
  c6565d22146045e52110fd0a13eba3b6b63fbf6583c444d7a5b4e3a368cc4b0d (image files)

(U//FOUO) ***The Cal-CSIC recommends information security personnel carefully scan their networks for the presence of this new ransomware, and apply the following basic mitigation procedures:***

- (U) Ensure antivirus systems have the most up-to-date patterns. VirusTotal's current analysis suggests only 28 of 63 major Anti-Virus software companies can detect this latest variant.

(U) ***Information security professionals should notify the Cal-CSIC immediately at*** CalCSIC@CalOES.CA.Gov ***or (833)REPORT1 if they believe their networks or systems have been infected with this new strain of ransomware.***