Issued 8/18/17

SyncCrypt Ransomware Able To Sneak Past Most Antivirus Defenses

A new ransomware called SyncCrypt is using a unique method of downloading the malicious files that makes it very hard for an antivirus program to detect.

SyncCrypt was detected by Emisoft researcher xXToffeeXx, reported Bleeping Computer, and is spread via spam emails containing an attachment with .wsf (Windows Script File) files. What is unusual about this, other than a .wsf file being used – which is rare – said Bleeping Computer founder Lawrence Abrams, is the .wsf will download an image with embedded .zip files containing the ransomware.

Once the email is opened and the target decides to open the attachment, the social engineering plan being used has the document being listed as a court order, a JavaScript script activates that downloads the image