Issued 12/14/17

New Spider Ransomware Threatens to Delete your Files if you don't Pay within 96 Hours

A new form of ransomware has emerged and is being distributed through malicious Office documents, infecting victims with file-encrypting malware. Uncovered by researchers at Netskope, the 'Spider Virus' ransomware campaign was first detected on December 10 and is ongoing.

The malicious Microsoft Office attachment contains obfuscated macro code which -- if macros are enabled -- allows a PowerShell to download the first stage of the ransomware payload from a host website. Following this, the PowerShell script decodes the Base64 string and performs operations to decode the final payloads in an .exe file -- which contains the Spider ransomware encryptor. PowerShell then launches the encryptor, encrypting the user's files, adding a '.spider' extension to them and then displaying a ransom note. The note tells the victim they've been infected with the Spider Virus and that they need to make a bitcoin payment for "the right key" in order to get their files back. The attackers also issue a threat that if the payment isn't received within 96 hours, their files will be deleted permanently. They add victims shouldn't "try anything stupid" as the ransomware has "security measures" which delete the files if the victim tries to retrieve them without paying the ransom. An additional note provides the victim with instructions on how to download the Tor browser required to access the payment site, how to generate a decryption tool, and how to purchase bitcoin. "This may seem complicated to you, actually it's really easy", the note says -- adding that there's also a video tutorial inside a 'help section'.

It's common for ransomware distributors to provide this sort of 'service' to victims, because if the victims can't pay the ransom, the criminals won't make money from their campaign. "In addition to disabling macros by default, users must also be cautious of documents that only contain a message to enable macros to view the contents and also not to execute unsigned macros and macros from untrusted sources," said Netscope's Amit Malik. Because Spider is a brand new form of ransomware, there's currently no free decryption tool available for victims to retrieve files.