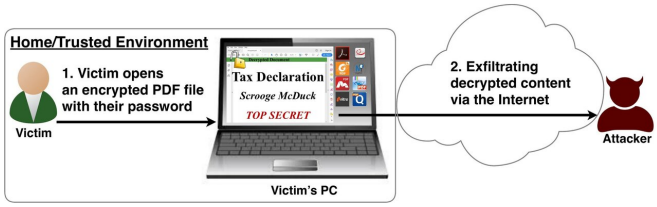
Two major security vulnerabilities found in PDF files

4 October 2019, by Bob Yirka



A combined team of researchers from Ruhr-University Bochum and Munster University has found two major security vulnerabilities in PDF files. They have documented their findings with a web-in-security blogspot posting.

PDF is a file format that includes electronic images of text and graphics. Such files are useful for documents that must be formatted in specially designed ways. They can also be sent to other people who can read them with a PDF document reader. Over the years, some users have used an encryption scheme to ensure private documents cannot be seen by anyone but an intended recipient—doctors, lawyers and even corporations have begun using the scheme to ensure privacy. But now, it appears that the encryption scheme for such documents has two major vulnerabilities—the researchers refer to them as two variations of a single PDFex vulnerability.

The first variation, which the researchers call "direct exfiltration" takes advantage of the PDF encryption specification—software that performs the encryption does not encrypt every part of the PDF file. That leaves part of the file open to hackers. An attacker can attach code to the file in the unencrypted section of the file that will run when the legitimate user opens it. Once the file is opened, the added code can send the contents of the file to a site designated by the attacker.

In the second variation, which does not have a name, an attacker uses cipher block chaining gadgets to change plaintext that exists in a PDF document to code—and just like the first variation, when the legitimate user opens the file, the embedded code executes, sending the document to a site designated by the attacker.

For either attack to work, an attacker would first have to gain access to the PDF file before it is sent. That means an attacker would have to infect the computer of the initial user with a virus that would launch code that modifies the PDF file.

The researchers plan to give a presentation outlining their findings regarding PDF vulnerabilities at this year's ACM Conference on Computer and Communications Security.

More information: "Practical Decryption exFiltration: Breaking PDF Encryption," www.pdf-insecurity.org/downloa … cryption-ccs2019.pdf

www.pdf-insecurity.org/encryption/encryption.html

web-in-security.blogspot.com/2 … ty-flaws-in-pdf.html