COMPUTERWORLD

May 4, 2010

Foxit Reader update blocks new PDF attack tactic

Adobe Reader rival adds 'safe mode' to stymie embedded-malware attacks

By Gregg Keizer

http://www.computerworld.com/s/article/9176308/Foxit_Reader_update_blocks_new_PDF_attack_tactic?taxonomyId=17

Foxit Software, the developer of a rival PDF viewer to Adobe's vulnerability-plagued Reader, released an update today that blocks some attacks with a "safe mode" that's switched on by default.

Foxit Reader 3.3 for Windows includes what Foxit dubbed "Trust Manager," which blocks all external commands that may be tucked into a PDF document. The new version is designed to stymie some common attack vectors that hackers use when they probe PCs for bugs in the PDF format, or in a viewer application.

"The Foxit Reader 3.3 enables users to allow or deny unauthorized actions and data transmission, including URL connection, attachment PDF actions, and JavaScript functions," the update's accompanying text explains.

Last week, several security companies warned of a major malware campaign that tried to dupe users into opening rigged PDFs that exploited an unpatched design flaw in the PDF format, one attackers could use to infect users of Adobe's and Foxit's software.

That flaw in the PDF specification's "/Launch" function was disclosed in late March by Belgium security researcher Didier Stevens, who demonstrated how he could abuse the feature to run malware embedded in a PDF document. He also reported he had figured out how to change Adobe Reader's warning to enhance the scam.

The attacks last week that exploited the /Launch flaw peaked on Friday, April 28, and have since dropped to nearly nothing, researchers at IBM Internet Security Systems' X-Force team said yesterday.

Foxit is alone in addressing the /Launch problem: Adobe has declined to answer questions on whether in-the-wild use of the function would prompt the company to update Reader and Acrobat. However, Brad Arkin, Adobe's head of security and privacy, has acknowledged that one possible solution would be to disable /Launch; currently, it's turned on by default.

PDF-based attacks are a major problem. According to recent tallies by antivirus vendor McAfee, PDF exploits were up more than eight-fold in 2009 compared to the year before, a trend that has continued thus far into 2010. Microsoft and Symantec have also noted a surge in exploits tucked into PDF documents.

Foxit 3.3's Trust Manager is switched on by default, said Eugene Xiong, the president of Foxit Software. But contrary to the text that accompanies the update, it does not disable all JavaScript, the scripting language that hackers have frequently used to exploit Adobe Reader vulnerabilities. "It doesn't disable JavaScript entirely," Xiong said. "It only partially disables JavaScript."

Among the JavaScript functions that Trust Manager strips away is one that lets a PDF execute another, non-PDF file, Xiong added.

Foxit 3.3 can be downloaded free-of-charge from the company's Web site.