

黑客利用PDF功能散布Zeus僵尸网络思科认证 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/644/2021_2022__E9_BB_91_E5_AE_A2_E5_88_A9_E7_c101_644601.htm 全厂商Websense近日指出，已发现有黑客利用PDF格式的功能瑕疵，将恶意程序注入PDF中，再利用邮件散布，当使用者开启该PDF文件时，便会被植入僵尸程序以扩张Zeus僵尸网络的势力。黑客所利用的是安全研究人员在今年3月底所揭露的PDF漏洞，由于PDF文件夹格式的规格允许使用者嵌入各种可执行的内容，包括影片、声音、3D物件等，再加上PDF的Launch功能可被用来执行应用程序、开启或列印文件，使得黑客能够利用相关功能在PDF文件案中嵌入恶意内容。包括Stevens及另一名安全研究人员Jeremy Conway皆曾打造相关的概念性验证程序。其中，Conway指出黑客得以滥用PDF的/Launch及更新程序功能而打造类似蠕虫的恶意程序感染途径。严格来说这并非安全漏洞，而是PDF文件夹格式的功能。对于研究人员的发现，Adobe表示，这说明了某些功能的不当使用所带来的潜在风险，该公司会研究最佳作法并透过定期更新修补。不过，在Adobe还未来得及更新的时候，Websense就发现黑客已透过上述方法在PDF文件夹中夹带恶意程序，当使用者开启该PDF文件时，就会在使用者电脑中植入Zeus僵尸程序，Zeus光是在美国就感染逾300万台个人电脑，该僵尸网络最知名的用途是窃取使用者电脑中的机密信息，同时这也是至今为止首个利用该PDF漏洞的僵尸网络。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com