[趋势科技安全预警]

趋势科技安全预警：新 PE 病毒变种流行 用户需注意防范

[趋势科技中国]– [2012 年 9 月 27 日]近日，全球服务器安全、虚拟化及云计算安全的领导厂商趋势科技发布安全预警：新的 PE 病毒变种（PE _ MUSTAN.B）正在流行，这种病毒是由趋势科技 China RTL 之前公布过的“WORM_MORTO”病毒演变而来，具有感染可执行文件的能力。趋势科技建议用户需保持警惕，及时采取安装免疫工具等防范措施，以防止受到感染。

趋势科技的监测结果显示，该 PE 病毒会利用远程桌面协议（RDP）3389 端口传播，进而感染所有可执行文件。当用户感染病毒之后，系统的“C:\WINDOWS\system32\drivers\ tcpip.sys”文件会被替换，并会自动连接到恶意网站（fd1. ppiplg.com、e.ppiftns.in、59.188.25.20）上下载恶意代码，对用户系统进行进一步攻击。此外 ,这种病毒的危害还在于 ,用户系统的某些可执行文件被感染后，可能会无法运行。

趋势科技（中国区）技术总监蔡昇钦表示：“这种新的 PE 病毒变种很容易传播，特别是在网络内电脑账户有弱密码的情况下，传播会更迅速。但是，病毒却很难清除，因为其会将恶意代码写入注册表，使自己不容易被清除干净从而导致反复感染；同时，为了防止被安全软件查杀，病毒会使用修改注册表的方式禁用某些安全软件的服务，趋势科技建议用户需加强警惕并采取有效措施加强防范。”

解决方案:

1. 目前趋势科技最新发布的病毒码(9.426.60)已经可以扫描并清除被感染的文件，强烈建议用户及时更新病毒码。
2. 对于没有安装趋势桌面产品的用户，可以下载 ATTK 扫描工具，下载地址为：http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/PE_MUSTAN/ATTK_PE_MUSTAN.B.EXE
3. 趋势科技还提供了针对该工具的内存修复和免疫工具，下载地址为：

http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/PE_MUSTAN/PEImmuner_mustan.com

免疫工具启动后会自动清理被感染线程。此外，免疫工具还会添加到系统启动项中，保证在电脑重新登录或启动时自动加载，使系统不再重复感染。

注意：一些有自校验或者附加数据的文件，在被病毒感染后会损坏。即使清除了病毒，也可能会导致文件不能正常运行。