趋势科技发布最新网络安全报告： 七月中旬网络安全威胁集中爆发

Flash 漏洞导致全球十几亿用户受影响　网络威胁几年内增长率超 1000%

[趋势科技中国]– [2015 年 7 月 24 日] 尽管网络防御技术不断进步，但依然难以阻挡网络威胁的持续发生。趋势科技监测发现，七月中旬的一周之内网络安全威胁集中爆发：UEFI BIOS Rootkit 远端遥控代理程序，新的 GamaPoS 恶意软件有不断蔓延的趋势，北约国防机构还遭遇了两年来的第一个 Java 零时差攻击 ,Flash 由于安全漏洞被 Firefox 和 Chrome 浏览器暂时“封杀”。而美国政府数年内网络安全威胁增长率 1000%的研究，更加证明了网络安全威胁的爆发式增加。

新恶意软件不断蔓延 传统安全防护措施面临失效危险

上周，趋势科技的安全研究人员发现，Hacking Team 使用了 UEFI BIOS Rootkit 来确保他们远端控制系统（RCS）代理程序安装在目标系统上，即使重新安装操作系统、重新格式化或使用新硬盘，都会在微软 Windows 系统启动后再度被植入。

此外，趋势科技还发现一个新的销售终端（PoS）威胁——GamaPoS 现在正通过 Andromeda 僵尸网路来进行广泛传播。搜索 POS 系统中的信用卡数据，并且对信用卡账号进行搜集，进而导致受害者的资金或信用卡信息被窃取。

趋势科技中国区技术总监蔡昇钦表示：“与传统的恶意软件相比，新发现的恶意软件具备更强的抗查杀功能。例如利用 BIOS 启动功能、定制化攻击代码等方式来躲避杀毒软件的查杀，Getmypass 等新型恶意程序已经能逃过市面上 55 种杀毒软件的查杀，这让用户更难监测到它们的存在。”

安全漏洞吸引更多关注　全球十几亿用户受到影响

利用知名应用程序的漏洞来进行网络攻击是向来是黑客最常见的做法之一 ,受害者甚至包括网络安全防护措施严密的政府与军事目标。监测显示，最新的 Pawn Storm 活动正在利用未经修补的新 Oracle Jave 漏洞来展开攻击，这是 2013 年以来针对 Java 的第一个已知零时差攻击。该攻击活动集中在高知名度的敏感目标，包括一北约成员国和一美国国防机构。

而 Adobe Flash Player 的漏洞则让更多的个人用户感受到了安全漏洞的风险性。由于有消息指出黑客利用 Flash 的安全漏洞来控制人们的电脑，Firefox 和 Chrome 浏览器封锁了旧版本的 Flash Player，这导致全球十多亿用户在使用浏览器时接收到 Flash 被阻止的信息，如果不更新 Flash 或解除浏览器的阻止，用户将难以浏览网页上的 Flash 视频。

为了修补最近被发现的多个漏洞，7 月 14 日的“周二”更新日不仅包含微软的 Windows 系统，Adobe 也发布了一个 Flash Player 更新来修补两个已经被放到网络上的漏洞。同期，Oracle 也释出了重要修补更新，修补了二十多个 Java 安全漏洞。

防弹主机托管服务支撑网络攻击 趋势科技新报告揭示其运作方式

据估算，每年网络犯罪造成全球损失预估在数千亿美元左右。在研究网络犯罪手法时，很容易忽略主机托管服务这一关键部分，该服务已经成为网络攻击行动的基础平台，确保恶意程序能够躲过和击退安全防护软件的抵御。趋势科技的前瞻性威胁研究（FTR）团队刚刚完成了一份详细的报告，揭示了不法分子如何利用主机托管服务进行犯罪行为。

这类服务一般被称为“防弹主机托管服务（Bulletproof Hosting Services）”，在网络黑市上，无论你想要找人来托管你的恶意软件，或服务器远程命令与控制（C&C）服务器，甚至是儿童色情图片。只要价格合适，就会有人帮你将这些恶意的网络内容放到网络上，而且还会确保它持续出现在网络中。

有趣的是，防弹主机托管服务并非没有规则和准则，大多数防弹主机托管服务对孩子保持一条界线：他们通常不会让客户发布攻击儿童的内容。防弹主机托管服务通常也会禁止客户攻击自己国内的个人用户或组织：这是个“聪明”的策略，因为受害者与当地用户无关，当地执法单位不太可能花时间和精力来关闭它们。

此外，趋势科技监测到的网络安全事件还包括：

联合航空以百万飞行里程奖励黑客发现安全漏洞

联合大陆控股公司提供数百万飞里程奖励黑客，感谢他们发现了该航空公司网站的安全漏洞，为美国航空业创下了首例。

FBI 一举获破全球最大黑客黑市论坛 Darkode

FBI 最近发动了一个逮捕行动，一举获破规模庞大、防卫森严的黑客黑市 Darkode。该黑市是全球黑客交易危险恶意软件的所在，为网络攻击提供了源源不绝的“弹药“。

智能摄影头疑出现被入侵事件

在用户在购买智能摄影机监控家中状况时，发现摄像头自动追踪，并且 APP 显示同时间有两位用户登录浏览画面，怀疑摄像头遭他人入侵。在物联网的趋势下，许多电子产品都具有联网功能，如果程序出现漏洞易导致个人隐私外泄，用户最好定期检查更新，并采取及时关闭网络、使用更复杂的密码等防范措施。

###

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。