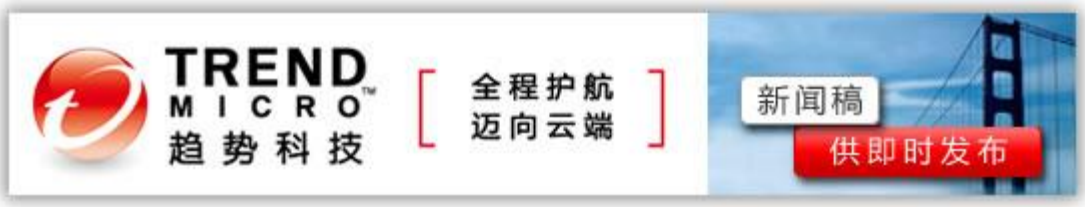

［趋势科技预警新闻］

FBI 关闭被感染 DNS 服务器倒计时

趋势科技建议网民对电脑进行健康体检

[趋势科技中国]– [2012 年 7 月 6 日] FBI 宣布将在 7 月 9 日关闭被感染的 DNS 服务器，执行“Operation Ghost Click”（幽灵点击行动）收官战役。全球服务器安全、虚拟化及云计算安全领导厂商趋势科技提醒网民： **抢救您电脑上网功能的黄金时间，正在一点点流失。当 Rove Digital 服务器被关闭时，您可能无法正常上网！**趋势科技今天表示，一旦 FBI 关闭 DNS 服务器，遭受感染的计算机很可能将无法连上互联网。根据 DNS Changer Working Group 信息，目前仍有 300,000 用户受到感染，中国是遭受此感染影响的 7 大国家和地区之一。

为此，趋势科技建议广大网民除了需要及时掌握上述信息可能造成的影响之外，如果不能确定在 2012 年 7 月 9 日之后能否继续上网，**趋势科技特别提供以下步骤让您对电脑进行健康体检：**

	如果您的计算机已感染了 Rove Digital 的 DNS 窜改木马程序	**如果您不确定自己的计算机是否已感染 Rove Digital 的 DNS 窜改木马程序**
Windows	1. 将您所有重要的文件备份至移动硬盘。	如果您使用的是 Windows 7，请单击[开始]按钮或屏幕左下方的 Windows 图标打开[开始]菜单。
	2. 利用趋势科技的 PC-cillin 2012 来扫描系统。清除您计算机上感染的 DNS 窜改木马程序。	在[搜索程序和文件]选项中输入“cmd”，然后按 Enter 键。
	3. 若要手动恢复 Windows 7 计算机的 DNS 设置，请按 [开始]按钮，或是屏幕左下角的 Windows 图标。在 [搜索程序和	

	文件]中输入“cmd”，然后按 Enter 键。	
	如果您使用的是 Windows XP ,请按[开始]→[执行] 然后输入“cmd”,再按 Enter 键。接下来，请按照下列步骤进行。	
	1. 在命令提示字符窗口（黑底白字的窗口）当中，输入“ipconfig/flushdns”，用于刷新 DNS 缓存，然后按 Enter 键。	1. 在命令提示字符窗口（黑底白字的窗口）当中，输入“ipconfig/all”，用于刷新 DNS 缓存，然后按 Enter 键。
	2. 您将会看到“已成功刷新 DNS 解析缓存”的信息。	2. 找到“DNS 服务器”这项设定，记下它列出的 IP 地址。
	3. 检查您的 DNS 设定是否重设成功，您可利用这个 FBI 提供的在线工具查询你计算机目前使用的 DNS 是否仍是 Rove Digital 的服务器 IP 地址。	3. 使用 FBI 提供的在线工具来查看是否有对应至 Rove Digital 服务器的 IP 地址。
	4. 在您的计算机得到修复之后，查看一下您的家用路由器，确定它使用的是 ISP 提供的 DNS 设定。您可能需要 ISP 的协助来重设路由器上的 DNS 设定。	使用这项工具时，您只需逐一输入 IP 地址，然后点击“Check Your DNS”(检查您的 DNS)按钮即可。
	窜改 DNS 地址设定只是 DNS 窜改木马程序的能力之一。您最好也检查一下您的银行对账单和信用卡账单，此外也更换一下网络账号密码，尤其是已被应用程序或网页浏览器所存储过的密码。	
Mac OS X	1. 将您所有重要的文件备份至移动硬盘。	1. 单击屏幕左上角的苹果图标，然后选择[系统偏好设定]。
	2. 使用您的恶意软件防护软件扫描您的系统。清除您计算机上感染的 DNS 窜改木马程序。	2. 在[系统偏好设定]面板中，选择[网络]图标。
	3. 若要手动复原您计算机的 DNS 设定 ,请按屏幕左上角的苹果图标，然后选择[系统偏好设定]。	3. 当[网络]窗口开启时，从左方选择目前使用中的网络联机。
	4. 在[系统偏好设定]面板中 ,选择[网络]图标。	4. 看一下窗口的右侧的[DNS]标签。

	5. 当[网络]窗口开启时，点选[进阶]按钮。	5. 记下您计算机设定的DNS服务器IP地址。
	6. 找到[DNS]标签。删除当中所列的全部项目，如此，您的DNS设定就会回复到默认值。	6.使用 FBI 提供的在线工具来查看是否有对应至 Rove Digital 服务器的 IP 地址。
	7. 检查您的 DNS 设定是否重设成功，您可利用这个 FBI 提供的在线工具。	使用这项工具时，您只需逐一输入 IP 地址，然后点击“Check Your DNS”(检查您的 DNS)按钮即可。
	8. 在修复您的计算机之后，查看一下您的家用路由器，确定它使用的是 ISP 提供的 DNS 设定。您可能需要 ISP 的协助来重设路由器上的 DNS 设定。	
	窜改 DNS 设定只是 DNS 窜改木马程序的能力之一。您最好也检查一下您的银行对账单和信用卡账单，此外也更换一下网络账号密码，尤其是应用程序或网页浏览器所记住的密码。	

Rove Digital 是什么？

去年秋天，FBI 发起了“Operation Ghost Click”行动，在趋势科技的协助下一举破获了 Rove Digital 网络犯罪集团。该犯罪团伙最为人所知的恶行，就是散播 DNS 窜改木马程序来从事和协助其他黑客组织进行不法行动，同时，该团伙也是史上最大的僵尸网络 DNS Changer（域名系统劫持病毒）的制造者。“

Rove Digital 是 Esthost、EstDomains、Cernel、UkrTelegroup 以及多家不知名的空壳公司在爱沙尼亚的母公司，Rove Digital 旗下这些公司从 2002 年起即开始从事网络犯罪。据了解，侦破 Rove Digital 时，全球 240 个国家共 400 多万个 IP 地址的计算机已经受感染。四年内，Rove Digital 仅利用广告诈欺获利就已超过 1400 万美元。虽然 Rove Digital 已在 2011 年 11 月 8 日遭到破获，但已遭病毒感染的计算机如果未及时清除恶意软件，也未重新设定 DNS，一旦 Rove Digital 的 DNS 服务器遭到关闭，这些受感染的计算机将无法连上因特网。

趋势科技（中国区）高级产品经理林义轩表示：“用户浏览特定网站或在线观赏影片都可能感染过 DNS 窜改木马，并且未被用户发觉。感染后，计算机内的 DNS 服务器地址设定遭到窜改，并指向 Rove Digital 建立的服务器，不法分子也利用 DNS 窜改木马程序来监视用

户通过键盘输入的信息。同时，这些被感染的计算机也可能当作代理（Proxy），将别的受害用户指向假冒的网络银行或社交网站。因此，网络犯罪分子可能已经借此窃取了您和他人的网络银行与社交网络密码。"

若要了解 Rove Digital 的网络犯罪历史，请参阅趋势科技 TrendLabs 的图文解说："The Rise and Fall of Rove Digital"。另外，如需更多有关 DNS 窜改木马程序的信息，或者要了解 Rove Digital 如何利用这些程序来牟利，请参阅趋势科技的"威胁百科"网站文章：How DNS Changer Trojans Direct Users to Threats。

###

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 1,200 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。