趋势科技监测发现无文件恶意软件　或导致传统安全软件陷入失效风险

[趋势科技中国]– [2015 年 5 月 29 日] 在发生病毒感染事件之后，常见的安全修复策略常是删除特定位置里面的病毒文件，并使用防毒软件进行全盘查杀。但如今，这个策略正在面临失效的风险，趋势科技发现了一种无文件载体的恶意软件，该软件摆脱了传统恶意软件的安装行为，使防毒软件的文件监测功能无法侦测到它们的存在。已经有迹象表明越来越多的病毒采用这种方式来躲避查杀，趋势科技建议企业与个人消费者务必要关注此类防毒软件的蔓延迹象，并采用行为监控的方式来防范病毒威胁。

无文件恶意软件肆虐 传统防毒软件丧失用武之地

如果将安全攻防当做一场“见招拆招”的剑术比赛，那么无文件恶意软件显然已经达到了“无招胜有招”的极高境界。与大多数恶意软件不同，无文件恶意软件并不会在目标电脑的硬盘中留下蛛丝马迹，而是针对传统防毒软件在扫描机制上的特点，直接将恶意代码写入内存或注册表中。由于没有病毒文件，文件扫描程序很难扫描或侦测到它们的存在。“POWELIKS”即是一个无文件恶意软件的例子，它可以利用另一个传统恶意软件将恶意程序代码加入注册表内，从而将自己隐藏在防毒软件的视线之外。

无文件恶意软件的攻击技术正在不断精进，在趋势科技监测到的另一个无文件恶意软件“Phasebot”中，软件除了会将恶意代码写入内存以避免监测之外，还加入了虚拟机侦测、外部模组载入等新功能。前者有利于恶意软件更快速的在企业虚拟机中传播，后者则支持黑客随时在受感染电脑上新增或移除功能。而且，该恶意软件更加强调隐蔽和躲避监测的机制，每次连接 C&C 服务器时，它都会通过随机密码来加密其通讯链路。

趋势科技（中国区）技术总监蔡昇钦指出：“Phasebot 之所以能够躲避安全软件的侦测，一个重要原因是它利用了 Windows 7 及更新版本所自带的 Windows PowerShell

工具，这本是正常的系统管理工具，但是 Phasebot 成功的利用该工具来执行它隐藏在 Windows 注册表内的组件 ,很容易让安全软件误以为这是一个正常的系统操作行为。”

当无文件恶意软件感染电脑之后，会执行黑客的后续指令，如窃取用户信息、绑架用户电脑以执行拒绝服务攻击（DDoS）攻击、自我更新、下载并执行其它恶意程序等。而且，黑客还试图在地下黑色市场销售这些攻击工具，这将导致更多的企业与个人用户处于安全风险之中。

趋势科技建议用户通过行为监控来防范威胁

无文件恶意软件的出现对于不熟悉此类病毒感染事件的用户来说会造成严重的威胁。当病毒感染事件发生之后，用户往往被建议去寻找可疑的文件或文件夹，而非 Windows 注册表这样被无文件恶意软件感染的地方。趋势科技预计会有更多黑客会使用无文件攻击技术，而且很有可能并不会局限在只用 Windows 注册表隐藏恶意软件。

无文件恶意软件的发展让那些严重依赖于恶意文件侦测的厂商面临严峻的挑战，安全厂商将不得不加紧脚步，跳出传统基于文件的侦测模式，采用新的安全防护手段。蔡昇钦表示：“要想成功防范无文件恶意软件的安全威胁 ,关键之处在于通过行为监控的方式，检查整个文件结构、寻找篡改和恶意代码注入的迹象，实现有效地侦测和阻断。”

个人消费者可以使用趋势科技 PC-cillin 2015 云安全版来防范无文件恶意软件的威胁，PC-cillin 2015 云安全版具备行为监控功能，可以持续侦测软件的恶意行为，并在恶意行为执行前就先封锁恶意软件，甚至可以在病毒码更新之前就提供充足的防护能力。

对于企业用户来说，趋势科技建议部署 OfficeScan 、Worry-Free Business Security 等终端安全防护软件或本地支持 SPN 的深度威胁发现平台（Deep Discovery，DD），这些产品可以在利用沙盒模拟、事件关联等功能发掘隐秘的攻击行动，在对系统的实时监控中发现恶意行为，阻止恶意软件进入到企业网络。

当然，在采取安全防护措施的同时，用户还需要关注网络环境的安全性，并养成良好的安全习惯。例如，用户在处理电子邮件、打开文件或网址时都要保持谨慎，必须再三确认这些文件或链接是否安全，以免被不法分子找到可乘之机。

###

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。