[趋势科技新闻稿]

趋势科技 TDA 成功协助韩国客户抵抗黑客多重攻击

韩国黑客攻击事件　趋势科技再次呼吁企业应正视定制防御策略重要性

[趋势科技中国]– [2013 年 3 月 26 日] -上周爆发的韩国遭受黑客攻击事件引起全球瞩目，也引发了企业经营者及 IT 从业人员对于企业自身防御方案是否周全的热烈讨论。全球服务器安全、虚拟化及云计算安全领导厂商趋势科技在事前通过定制防御策略(Custom Defense Strategy)，帮助趋势科技的韩国客户事先发觉并采取防护措施，成功抵挡了此次黑客攻击，并且没有遭受任何损失。通过趋势科技的 TDA 搭配定制的防御方案，全球 6 大银行当中就有三家采用 TDA ,更有超过 80 多个政府机构也采用这套解决方案免于此类攻击。根据过往经验，不排除黑客会再发动另一波攻击，趋势科技再次呼吁企业应正视定制防御策略的重要性，才能确保企业免于成为黑客下一波攻击的牺牲者。

当地时间 2013 年 3 月 20 日星期三，韩国多家大型银行及三家大型电视公司相继出现多台电脑丢失画面的情况，有些电脑的显示屏上甚至出现骷髅头的图像以及来自名为“WhoIs”团体的警告信息。此攻击是韩国同一时间遭受的多起攻击之一。趋势科技研究显示，这是一次恶意程序攻击的结果，黑客一开始假冒银行发送主题为“三月份信用卡交易明细”的钓鱼邮件，内含会清除硬盘主引导记录（Master Boot Record，简称 MBR）的恶意程序。黑客设定该恶意程序在 2013 年 3 月 20 日同步爆发。一旦爆发，即使银行电脑系统完全瘫痪，必须逐一重装系统才能恢复。

清除硬盘主引导记录的手法通常是黑客攻击最后的一个步骤，目的是要让调查与系统还原工作更加困难。趋势科技的研究发现，黑客想要摧毁的目标不仅只有 Windows 操作系统的电脑，Linux、IBM AIX、Oracle Solaris 以及 Hewlett-Packard HP-UX 等使用 UNIX 系统的电脑也是其目标。

纵深信息安全防护　对抗黑客入侵

趋势科技威胁发现设备（Threat Discovery Appliance-简称 TDA）成功协助客户抵御了本次黑客入侵。TDA 提供了完整的攻击分析，从“侦测 – 分析 – 加固 – 响应”四个阶段进行攻击生命周期研究及提供解决信息，可强化现有的信息安全防护措施并与其整合，形成一套完整且针对客户环境量身定制的个性化防御方案。TDA 可与网络、网关与终端安全防护整合并分享安全更新信息，进而提升所有端点的防护能力，可保护客户免于锁定目标攻击与高级持续性渗透攻击（APT)。其检测引擎与个性化沙盒技术可监测及分析一般信息安全产品所无法检测的恶意程序、恶意通信以及黑客行为，具备迅速回应能力，可成功防范黑客攻击，协助企业避免重要端点瘫痪的风险。

如需更多 TDA 如何成功防范此次韩国攻击事件的相关信息，请访问：
http://cn.trendmicro.com/cn/products/enterprise/TDS/index.html?WT.mc_id=0910_tds_right_HOME_CN