面对 APT，企业可以做什么？

APT 攻击凸显巨大风险 趋势科技提醒企业加强攻击侦测与控制

[趋势科技中国]– [2013 年 12 月 12 日] APT 攻击作为一种复杂且多方位的攻击，对于企业的安全保障构成了极大的风险。尽管很多全球化企业在安全控管上都投入了庞大的资源，但是 APT 攻击仍然渗透进这些企业，并使韩国金融企业、Adobe 等遭遇了重大损失。这些事件都向我们警示了 APT 攻击的复杂性与巨大破坏性，并敦促我们尽快采取相应防范措施。

APT 攻击使企业面临巨大风险

APT 攻击可能发生在任何一家公司，其中最大的一个原因就是为了窃取公司的机密信息。知识产权、金融资料、员工和客户的个人信息、财务信息等很多机密信息都具有很高的价值。一旦黑客通过 APT 攻击获取这些机密信息，将有可能给目标企业造成巨大的损失。但同时，窃取机密信息并非 APT 攻击的唯一原因，破坏系统、监视等都有可能成为黑客攻击者的原因。因此，不管企业有无敏感信息，都时刻都暴露在 APT 攻击的风险之下。

攻击者可能会利用某个组织的网络基础设施来发动对其它组织的攻击。在某些案例中，攻击者会利用受害者的电子邮件账号来增加他们鱼叉式网络钓鱼攻击邮件的可信度。在类似的攻击事件中，为了实现对大型组织网络的攻击，黑客可能会从连接到该组织网络的小企业入手，然后以其作为跳板发动攻击。对攻击者来说，通过小企业的网络会更加容易也更为隐蔽，而且不会在大型组织的网络内留下痕跡。

此外，一家公司也可能单纯的被当成跳板，用来掩盖攻击者和目标之间的攻击路径。

在韩国近期遭受的大规模 APT 攻击中，黑客就假冒银行的电子邮件账号发送主题为“三月份信用卡交易明细”的钓鱼邮件，该邮件包含了名为“您的账户交易历史”的恶意.rar 文件，它会连接数个恶意 IP 地址并下载 9 个文件，企业内部的中央更新管理服务器也会因为遭受入侵而被植入恶意程序。

面对 APT 攻击可以做什么

不管企业的防御措施有多么完善，只要一个设定错误或某个用户打开恶意文件或访问恶意网站，就可能会让公司受到影响。因此，企业所要做的不仅是在攻击发生后迅速的采取修补措施，还应该及时的对整个 IT 架构的数据动态进行检测，一旦攻击者进入公司网络，受攻击的目标必须要能尽快的加以侦测和控制。在这时间点，可以进行完整的调查来看看攻击者去过哪些地方和造成哪些损害。

在韩国此次遭受的 APT 攻击中，就有部署了趋势科技 TDA 的韩国用户成功的抵挡了此次攻击。趋势科技 TDA 具备完善的启发式侦测能力与沙盒分析提示，当恶意程序在网络中传播感染其它用户时，它们就会被打上标记，其中就包括向外界传送信息或从恶意的来源接收命令的隐藏型恶意软件。当 TDA 侦测出此次攻击相关的邮件中的恶意附件后，企业就有充足的时间来定制防御策略(Custom Defense Strategy)以抵御攻击。

对威胁进行侦测和控制的过程可能非常耗时，但是企业可以先专注在两个方面来将损害降到最低程度，同时也让事件调查可以尽可能的快速和成功。第一，企业要执行适当的纪录政策，将网络分割，并通过趋势科技 TDA 等威胁发现设备来加强安全威胁检测和对关键资料的保护。第二，企业要有已经受过训练和运作正常的威胁情报小组和事件调查小组。

为了帮助改善安全状态，渗透测试对公司来说也会很有帮助，从测试结果里可以了解很多安全隐患。如果可以的话，也要进行社交工程和实体安全测试。一旦完成，渗透测试可以用来作为事件调查小组的训练工具，并将所发现的信息提供给公司，有助于企业了解整体的安全性问题。

安全是一项投资，但由于 APT 攻击可能对企业造成的巨大损害，这种投资是值得的。企业需要随时关注 APT 攻击的防御措施，并且了解更多关于如何尽量减少成为 APT 攻击受害者风险的详细信息，以保证企业的安全性。

###

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。