趋势科技新闻稿

[即时发布]

索尼影视遭遇重大 APT 网络攻击 大量商业机密遭泄露

APT 攻击愈演愈烈 趋势科技提醒企业领先一步部署应对措施

[趋势科技中国]– [2014 年 12 月 09 日] 近日，索尼影视娱乐公司(Sony Pictures Entertainment)遭到黑客团体发动的 APT 网络攻击，数万名员工的信息以及多部未发行的电影拷贝遭泄露，这个事件再度印证了趋势科技关于 APT 攻击将愈演愈烈的安全预测。

据悉，11 月 24 日，自称为“和平卫士”（Guardians of Peace）的黑客组织声称，已获取了索尼影业的内部数据，包括一些“秘密”数据，包括密码、员工社保号码和一些与名星、经销商签订的合同文本等。并称如果去要求得不到满足的话，将公开这些数据。黑客组织侵入索尼内部数据库后 ,窃取了索尼至少 100 TB 的内部文件和电影数据，相当于美国国会图书馆十倍的信息存储量。报告显示，在攻击发生之后，索尼影视禁用了整个企业网络，以防范黑客的进一步破坏行动。然而，对企业网络的禁用不仅严重地影响企业的日常营运，也让调查任何攻击变得更加困难。

趋势科技（中国区）业务发展总监童宁指出：“禁用网络并不是应对这种高层级攻击的典型处理措施，在遭遇到针对性目标攻击之后，企业合理的选择是尽快调查现有攻击，并及时封堵安全漏洞，清除安全威胁，将攻击对组织日常运作的影响降至最低。”

关于 APT 攻击目的，诸多线索显示黑客并非想要窃取金钱或是商业机密，而是基于政治诉求或情绪发泄。这也再度提醒了 IT 管理员防范那些以破坏组织运作为目的的攻击，保护组织的网络安全。99%的恶意软件感染小于 10 个受害者，80%的恶意软件只有 1 个受害者，这说明目前的网络攻击具有高度的针对性，IT 管理员很难对 APT 攻击的时间、范围、方式等进行精确的预测，也无法完全依赖传统安全防护系统的机械式判断。趋势科技建议，防范 APT 攻击的关键点是采取定制化智能防御，将威胁的防范融入到

一个更大的监测及预防策略中，并整合现有的网络防御，实现对整个企业 IT 架构数据动态的监测，发现那些隐藏的可疑网络行为。

在企业搭建了严密的监测网络之后，IT 运维管理人员便可以在攻击还未发生时收到相关设备的报警，从而在第一时间采取措施阻断攻击行为。在 2013 年韩国爆发的大规模 APT 攻击事件中，一部分企业用户便在事前通过趋势科技 TDA（威胁发现设备）的启发式侦测与沙盒分析提示，监测出该次攻击相关的邮件中的恶意附件，并定制防御策略(Custom Defense Strategy)，最终成功抵挡攻击。

###

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。