法国最大的全球性电视网遭袭击　11 个频道全部断线：4 小时改变了世界

趋势科技发现针对基础设施网络攻击进入新阶段　警示企业管理者加强 APT 防护投资

[趋势科技中国]– [2015 年 4 月 21 日] 近日，法国最大的全球性电视网遭到重大网络攻击，造成电视转播信号中断数小时，电视台的网站和社交网络同时被黑客控制，并出现了大量“圣战”标语、视频和图片。尽管完整的细节尚未明朗，不过从 Arid Viper 和 Sony 等公司之前遭到的攻击 ,以及趋势科技针对关键基础设施攻击的调查显示,这很有可能是以网络钓鱼为入侵手段的进阶性持续攻击(Advanced Persistent Threat, APT)。趋势科技发现，此次事件凸显针对关键基础设施，并以影响社会秩序和服务为目的的网络攻击不再是小说中的情节，警示企业管理者认真看待 APT 攻击带来的重大影响。

在此次攻击事件中，这家法国最大的全球性电视网因为网络攻击而导致完全断线。由于攻击整合了以社交网络、电视台、网站为目标的多种攻击，使针对关键基础设施的攻击威胁上升到新的层次。攻击的范围前所未见，攻击者能够：

1. 完全中断该电视台所有 11 个频道的播出。
2. 完全中断电视台的内部网络。
3. 取得对电视台网站和社交媒体帐号的控制。
4. 变更网站内容成为亲 ISIS 的声明。
5. 在社交媒体账号贴出对 ISIS 行动的法国士兵亲属名字和个人信息。

趋势科技提醒企业应从这起事件中吸取充足的教训。企业管理者应该认识到，针对关键基础设施的网络攻击不再仅仅是国家行为，而是成为恐怖组织播撒恐慌、制造舆论的工具。管理者需要和政策制定者协调一致，认真看待此情况并迅速采取行动，现在就加大对 APT 攻击防御措施的投资，以在下一波更大的攻击到来前更好地保护网络。

趋势科技威胁研究响应团队也密切关注此事件发展，以确保提供用户完整的防护。趋势科技（中国区）技术总监蔡昇钦表示：“对于企业的管理者来说，我们无时无刻都处于精密规划的 APT 攻击威胁之中，攻击者往往采取网络钓鱼的方式，从组织防御最薄弱

的地方入手，以到达破坏企业网络或者窃取重要数据的目的。因此，组织管理者必须打起精神坚定我们的防御措施。”

针对面临 APT 攻击威胁的用户，趋势科技提供了分层式内容安全防护解决方案，涵盖移动设备、终端电脑、服务器、云服务等端点的安全保护。凭借分层式防护解决方案，趋势科技可保护用户信息、数据中心（Data Center）、云资源免于信息外泄及目标式攻击。

APT 与其它目标式攻击的一个关键点在于他们会寻找企业的系统、软件弱点与安全防护漏洞，并抢先在漏洞修补前发动攻击。在渗透进入企业内部网路后，攻击者随即开始使用各种恶意程序、黑客工具、恶意程序代码上传到远程的命令与控制服务器(Command & Control Server, C&C）。有鉴于此，趋势科技持续将新发现的 C&CIP 位址加入趋势科技主动式云端截毒技术（Smart Protection Network, APN）资料库中，协助阻挡此类攻击事件中的上传行为，大幅降低可能带来的损害。

*趋势科技持续关注网络攻击事件的发展，并会将新信息或是防护措施（病毒特征或新防御规则等）公布于以下知识库 http://esupport.trendmicro.com/solution/en-us/1109423.aspx

###

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。