鳄鱼还是木头？
亚信安全提醒：APT 攻击防范要当心“水坑”

【亚信安全】-【2016 年 3 月 3 日】就像是“鳄鱼还是木头”的寓言一样，大多数 APT 攻击并不会直接暴露真实面目，而是会很好的在用户经常访问的可信网站上或是分支机构中伪装起来，等待粗心的企业用户，这类的攻击也被叫做 “水坑攻击”（Water hole attack）。为了防范此类攻击，亚信安全建议用户改变“单点作战”的传统做法，更加重视威胁情报共享和定制化解决方案。

瞄准企业网络弱点 “水坑攻击”让人防不胜防

水坑攻击是 APT 攻击的一种常用手段，黑客通过分析被攻击者的网络活动规律，寻找被攻击者经常访问的网站弱点，入侵这些防御措施相对薄弱的服务器并植入恶意程序，当用户访问了这些网站，就会遭受感染。就像是鳄鱼捕食的惯用伎俩一样，捕食者埋伏在水里，等待角马喝水时发动攻击。

狡猾的黑客会绕过层层设防的主要入口，选择企业的合作伙伴，或者是分支机构，在必经之路上设置一个“水坑（陷阱）”，这让普通用户甚至是管理员都很难防范。这其中的典型案例就是美国连锁超市 TARGET 的信息泄露事件。

在 TARGET 的泄露事件中，黑客通过研究其供应链的各个环节，选定了 TARGET 的一家第三方供应商为跳板，使用社交工程钓鱼邮件窃取了该供应商的用户凭证，从而获得进入 TARGET 网络系统的权限。随后，黑客通过在

POS 系统中植入软件，感染了所有刷卡机，截取了刷卡机上的信用卡信息，最后成功入侵数据中心，窃走了所有的用户信息。

单点防御产品无力鉴别 APT 风险

针对“水坑攻击”日渐猖獗的情况，亚信安全 APT 安全专家白日表示：” 随着互联网+在各行各业的加速融合，许多企业网络的边界已经模糊化，黑客利用“水坑攻击”手段，以中小企业或合作伙伴为跳板，最终对大型企业发动 APT 攻击，增加了核心数据的保全难度。这种攻击方式超越了单点防护产品的功能范畴，用户需要在侦测能力上部署更先进、更全面的防护手段。”

“水坑攻击”和“路过式下载攻击”有着很大区别，后者属于一般性攻击，很容易被发现，而利用“水坑”发动的 APT 攻击则更加隐蔽。攻击者还会利用网络钓鱼电子邮件、包含恶意代码的下载包、零日漏洞来发动攻击，而传统的防火墙、入侵检测、安全网关、杀毒软件和反垃圾邮件系统等主要是采用特征码匹配检测技术对网络边界和主机边界进行已知威胁检测,它们均缺乏对未知攻击的检测能力和对流量的深度分析能力。

有别于传统设备的“单兵作战”，亚信安全提供了深度威胁发现设备（TDA）、深度威胁安全网关（DE）、深度威胁邮件网关（DDEI）、深度威胁分析设备（DDAN）、深度威胁终端取证及行为分析系统（DDES ）等产品构成的深度威胁发现平台（Deep Discovery，DD），该平台可以与亚信安全其它的网关、虚拟化、服务器以及终端安全防护产品整合。另外，亚信安全还与趋势科技全球 15 个恶意软件实验室、云安全智能保护网络（Smart Protection Network）共享威胁信息 ，形成全覆盖的侦测平台。不论是传统安全威胁，还是“水坑攻击”都能从这里侦测并得到分析，同时还能清晰的描述攻击路径、定位到终端或个人，最终形成威胁的预警信息。

针对“水坑攻击”重点对象，白日还表示：中小企业本身防护意识和能力比较薄弱，被攻击的成功率也就很高，黑客往往会选择这些对象进行“挖坑”。另外，国内大部分的企业对 APT 攻击都停留在简单认知的层面，只有很少的一部分用户非常了解 APT 攻击的危害。因此，威胁情报共享和定制化解决方案对于防止和识别针对性攻击而言越来越重要，亚信安全将全力协助企业用户远离此类风险。

##

关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式 ,助力客户构建“立体化主动防御体系” ，为国家提供网络安全与云产业安全保障 ,推动实施自主可控战略。更多关于亚信安全公司及最新产品信息 ,请访问: http://www.asiainfo-sec.com