# 五个 DNS 必问问题

几乎每次针对互联网的恶意攻击，均源于域名系统 (DNS) 请求将域名转换成 IP 地址。尽管 DNS 令互联网快速且高效，并为大家带来更多便捷，但由于其开放性和广泛应用，因此易于受到攻击。DNS 本身并不具备智能性，因此会同时解析善意域和恶意域提出的请求。

网络犯罪分子利用递归 DNS 的漏洞，发动具有破坏性的恶意软件和勒索软件活动、网络钓鱼攻击，以及针对公司数据的窃取。随着您的用户、设备、应用程序和数据继续向传统企业边界和控制区域之外迁移，攻击面只会不断扩大。

那么，如何主动保护您的网络不受这些定向威胁的侵害？许多企业开始采用 Zero Trust 安全策略，“验证，且从不信任”所有用户和设备。在检查用户和设备通过出站 DNS 请求构成的固有风险时，此方法就显得尤为重要。要确定是否需要 DNS 安全策略，有五件事要问自己。

## 1 您的递归 DNS 每天解析多少请求？

一台设备每天提出数千条查询；而如今，考虑到网络上的每个用户和每台设备，数量会成倍增加。由于数据量庞大，通常无法向安全信息和事件管理 (SIEM) 系统输入，因此难以汇总这些数据。由于善意流量过多，恶意流量过少，因而无法保证向 SIEM 添加 DNS 日志。此外，要导出日志并解析多个来源的数据并不容易。即使您克服这些汇总的问题，您将看到数千个（或百万个）毫无上下文的主机名。虽然数据太多会出现问题，但数据过少则更糟，您根本无法获取见解。

## 2 不规则 DNS 流量是什么样的？

那么，您是否具有相关基准来衡量规则、健康的 DNS 流量？鉴于您网络中 DNS 请求的数量和种类，这些请求通常源自笔记本电脑、手机、台式机、平板电脑、打印机和访客 Wi-Fi，更不必说所有“智能”互联设备，因此想要了解普通一天中双向流量的构成，并非易事。另外，通过挖掘数据来确定网络上的哪些设备正在发出请求往往非常耗时费力。

然而，这也是一项重要信息，因为设备类型可以是已出现问题的关键指标。尽管笔记本每天进行数千次递归 DNS 查询不应引发警报，但对于建筑物的暖通空调系统发出过多请求的情况，当然要进一步调查。但是，只有首先确定暖通空调是多余请求的来源才可以继续进行。随着互联设备（物联网）数量（预测 2020 年将达到 204 亿[1]）的攀升，风险只会不断增加。

即使您分配资源持续监控和分析 DNS 日志或十分不正常的现象，而到那时可能为时太晚，根本不可能在遭受损害前，就明确并缓解入侵。这是因为贵司的样本尺寸过小，无法识别整个互联网的趋势和威胁，因此许多企业部署了云服务。您总体了解的流量和情报越多，就越容易识别不规则 DNS 流量；您必须了解全球趋势和形式，才能持续有效识别威胁。

## 3 您知道递归 DNS 可用于窃取您企业中的数据吗?

随着公司和个人对攻击采取措施，定向威胁也在不断发展。网络犯罪分子日趋使用递归 DNS 入侵安全边界，利用基础设施的固有漏洞。您网络中的一台设备受感染后，大多数恶意软件将请求发回命令和控制 (CnC) 服务器，等待后续指令。鉴于 DNS 流量未经筛选且开放，这些恶意查询可以躲过审查，绕开所有网络级别的安全屏障。

通过该 DNS 隧道，恶意攻击者能窃取财务记录、身份证号、信用卡信息、知识产权及其他敏感数据。这些数据包经加密、压缩、缩减，然后使用各种技术传输，避开缓慢滴注、IP 欺骗、域名生成算法 (DGA) 及快速通量等检测。如果您仅依赖网络级别的安全措施，您会对这种入侵一无所知。

如果考虑到当今劳动力的流动性日益增加这一情况，了解此固有漏洞就变得更加重要。随着员工、提供商、合作伙伴和供应商迁移到网络边界之外，从而造成在家、咖啡店、机场、酒店和会场等地点办公的情况越来越多，但他们的设备很可能连接到不安全的网络。只需将一台遭受攻击的设备重新连接到企业网络，就能发起导致整个企业数据外泄的恶意软件攻击。

## 4 您能否在数秒内采取政策，拦截整家公司的恶意活动?

识别恶意域名或 IP 地址难度很大，这只是缓解定向威胁的部分措施。查明攻击或漏洞后，IT 团队就得疲于在整个公司范围内快速实施防御计划。如果没有云基解决方案，可能就要反复实施大量繁冗的软件更新和硬件安装。这些指令还需要与总部及时有效沟通，并要看网络中的所有分支机构、员工和设备是否 100% 合规。

很多地方都有可能出错，而且漏洞的暴露时间即便没有数天，也有数小时。而云基解决方案可在几分钟内完成配置和部署，无需硬件或软件。能在任何地方管理，能推送到各处，几乎瞬间完成单边实施。

## 5 DNS 是否属于分层安全系统?

如果不属于，您承担不起其造成的损失。70% 的组织在 2016 年发生过对业务造成负面影响的安全事件，[2] 并且 2017 年数据泄露的数量增长了 30%。[3] 从入侵到发现的平均时间超过六个月[4] 而且平均代价为 1,800 万美元，包括品牌声誉损失。[5]

企业发出的每个网络请求始于 DNS，这使它成为确保对网络请求的整个企业级可见性和应用安全政策的完美控制点。由于验证发生在 IP 连接之前，威胁在安全击杀链前端遭拦截，离企业边界还很远。大家通常遗忘递归 DNS 能作为攻击向量，但鉴于恶意软件不断更迭，黑客要价增加，您必须增强易受攻击的后门防御。

## 主动云端定向威胁防御

主动防御递归 DNS 不受定向威胁侵害势在必行，并且将 Akamai 的 Enterprise Threat Protector 等云基解决方案融入安全堆栈从未如此容易。可快速配置，易于扩容，轻松部署，无需硬件或软件，且停机时间为零。云门户实现灵敏中央管理并在数分钟内实施统一策略，可让用户通过仪表板详细了解 DNS 流量、威胁事件、可接受使用策略 (AUP) 活动。

Enterprise Threat Protector 易于将其他安全产品与报告工具整合，充分发挥公司对深度防御战略所有层的投资效益。依托于 Akamai Cloud Security Intelligence 的实时情报，及通过 Akamai Intelligent Platform 管理 30% 全球 Web 流量所积累的见解，Enterprise Threat Protector 向公司及其员工提供几近实时的防护。

有关 Enterprise Threat Protector 的更多信息，请阅读“*采用 DNS 最佳实践以主动抵御恶意软件的攻击*”并访问产品页面。

## 资料来源


1. http://www.gartner.com/newsroom/id/3598917
2. **《2016 RSA 网络安全贫困指数》，**https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016
3. http://247wallst.com/technology-3/2017/06/22/2017-data-breaches-nearly-30-higher-than-2016s-record-pace
4. **《波耐蒙研究所：2016 数据泄露代价研究》，** https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
5. **《波耐蒙研究所：高级持续性威胁的经济影响》**