阻止攻击者使用 DNS 对您发起攻击

无论什么行业，位于何地，规模如何或使用哪些产品，所有现代企业都需要使用域名系统 (DNS) 运营业务。DNS 是一种协议，可将用户友好的域名（例如 www.paloaltonetworks.com）转换为机器可使用的 IP 地址 - 本例中为 199.167.52.137。如果没有 DNS，我们就需要记住随机的数字字符串，但人类大脑并不擅长记忆大量信息。因此，对全世界每一家现代企业来说，DNS 都必不可少。网络运营商无法阻截 DNS 流量，防火墙必须允许该流量通过。网络需要 DNS 才能正常运行。

虽然许多企业理应投入大量时间和资源来保护 Web 和电子邮件攻击媒介，但许多安全专业人员并未意识到攻击者滥用 DNS 的简便性和普遍性。事实上，许多安全团队不会检查 DNS 流量是否存在威胁，因为他们假设通过 DNS 协议和端口 53 发送的查询是良性的。其他企业也不会检查 DNS 流量，因为该流量过于庞大，寻找该流量中的恶意迹象无异于大海捞针。这需要花费大量时间和资源 - 对于企业而言往往需要投入巨资，尤其是对于假设 DNS 不会构成重大威胁的企业而言更是如此。

DNS 是一个容易被忽略的巨大攻击面，企业需要对 Web 和电子邮件执行相同的审查和保护。攻击者会利用它传播恶意软件，执行命令和控制 (C2) 或造成数据泄露。攻击者可以在多个攻击点随意滥用无处不在的 DNS。根据 Palo Alto Networks Unit 42 威胁研究团队的研究结果，近 80% 的恶意软件使用 DNS 来启动命令和控制程序。DNS 被视为维持与 DNS 服务器连接的可靠方式，因此，由攻击者建立的可靠的命令渠道很难被阻止或识别。随着攻击者的攻击日渐自动化，几乎无法识别和阻止这些威胁。

80%

的恶意软件使用 DNS 启动可用于窃取数据和传播恶意软件的命令和控制程序

图 1： Unit 42 关于 DNS 流量的研究

与此同时，许多安全团队缺乏对 DNS 流量的可视性，也无法了解威胁如何使用 DNS 来维持对受感染设备的控制。安全团队面临着诸多压力，例如，需要对数百万新恶意域实施一致的保护，同时制定出应对 DNS 隧道等高级攻击策略的措施。除了 DNS 应用的普遍性及易于被滥用的特点，新恶意域的速度之快及数量之庞大也不容小觑，通过创建静态签名的方式加以应对已经远远无法应对这一问题。如果系统受到感染，网络和安全团队就会面临快速识别哪些系统被感染并解决感染问题的挑战。到那时，恶意软件可能已经传播开，数据也可能已经遭到窃取。

使用 DNS 进行的三种主要攻击

了解攻击者如何滥用 DNS 是阻止网络攻击并最大限度降低网络安全风险的第一步。以下是网络犯罪分子滥用 DNS 掩盖其命令和控制活动，以便传递更多恶意软件或窃取数据的三种首选方式。

使用 DNS 执行命令和控制的恶意软件

这是攻击者利用 DNS 发起攻击的最典型方式之一。攻击者使用常见的网络协议（包括 DNS）传播恶意代码。可以通过在线广告、电子邮件中的恶意 URL 或其他方式将恶意软件发送给用户。一旦用户的计算机遭到感染，系统就会将 DNS 请求发送回攻击者的控制服务器。通过这种方式，受感染的计算机便成为攻击者可以控制的僵尸程序。然后，恶意软件可以窃取个人或财务数据，并通过发出指令扫描网络以查找其他计算机进行快速传播。

最近，黑客组织 WINDSHIFT 发起了一场使用 DNS 执行命令和控制的网络攻击，攻击位于中东地区的政府部门和关键基础架构。要了解技术细节和时间表，请参阅 Unit 42 关于 WINDSHIFT 攻击的研究。

使用域生成算法的恶意软件

域生成算法 (DGA) 可以随机生成大量略有不同的域名，这种有效的方法发展十分迅速。例如，域生成算法可以在一天之内创建数千个域，每个域名与 www[.]bigbadguys[.]com 相比都有些许不同。攻击者开发出了域生成算法，这样，恶意软件便可生成类似上述域并将其用于执行命令和控制。Unit 42 观察到，18% 的恶意软件每天使用域生成算法自动创建数千个命令和控制域，而攻击者可以任选其一使用，这样防御人员就无法阻截攻击。在攻击者控制的恶意域中，可以将命令和控制渠道在不同点之间快速移动，从而绕过传统的安全控制措施，例如黑名单或 Web 信誉过滤。受感染的计算机会联系其中一些新域名以接收命令和更新。域生成算法的一个关键方面在于，尽管可以在短时间内生成数千个域，但并非所有域都需要注册。

使用 DNS 进行攻击的有效方法迅速发展起来。使用域生成算法 (DGA) 的恶意软件同比增长了

124%

图 2： Unit 42 关于域生成算法的研究

域生成算法为攻击者隐藏其命令和控制中心的位置提供了有效手段，攻击者利用这些命令和控制中心进行财务欺诈、身份窃取和其他恶意活动。要进一步了解域生成算法，请参阅 Unit 42 的域生成算法威胁简报。

DNS 隧道

高级持续性威胁 (APT) 执行者逐渐开始使用这项技术，方便攻击者在 DNS 请求中以小块编码其有效负载，从而绕过安全控制。高级攻击者使用 DNS 隧道在标准 DNS 流量中隐藏数据窃取或命令和控制行为。受害者的设备遭到入侵后，受感染的设备会在 DNS 流量中发送请求。DNS 服务器遵循指示连接到网络犯罪分子的服务器，这就建立了一个用于窃取和传输数据的渠道。借助 DNS 隧道，DNS 请求可以通过公司防火墙内外的普通 DNS 服务器。但是，隐藏在 DNS 请求中的隧道数据不会被发现。包括威胁组织 OilRig 在内的攻击者近年来已广泛使用 DNS 隧道。

为什么当前的安全方法会失败

出于某些原因，当前阻截使用 DNS 执行恶意软件攻击的方法不适用。首先，难以根除攻击者使用 DNS 入侵企业的多种方式。许多企业只专注于保护他们的 DNS 基础架构，这是理所应当的。如果 DNS 发生故障，则无法再访问互联网。但他们并不关注隐藏的威胁：攻击者会利用 DNS 本身传播恶意软件或窃取数据。有些企业并未采取任何措施保护 DNS，而是向攻击者敞开大门。许多企业不进行 DNS 监控，他们只会阻截恶意域，实质上无法消灭滥用 DNS 的恶意软件。

其他安全团队采用黑名单方法阻截使用 DNS 的攻击，这种方法依赖于相对静态的威胁源，而威胁源可以清除已知的恶意域。但是，随着恶意软件越来越多地使用域生成算法，仅阻截已知恶意域的有效性越发有限。使用随机生成的域列表进行命令和控制，将会让旧有工具和传统安全方法的签名功能不堪重负。一组有限的签名根本无法扩展以应对不断增长的基于 DNS 的攻击威胁。

此外，对静态列表的依赖限制了防御者可以访问的情境数量，这有碍于全面了解网络攻击的情况。虽然威胁情报源会定期更新来自企业外部来源的指标或工件，但每日甚至每小时的更新速度太慢，无法与生成的大量 DNS 数据保持同步。巨大的 DNS 流量通常意味着防御者缺乏相应的可视性或资源，无法对这些流量执行普遍检查以查找威胁。使用传统方法，安全团队没有相应资源可以采取主动措施或扩展其 DNS 安全性。

一些企业使用独立的单点产品解决其 DNS 面临的威胁。这些工具可以充分解决 DNS 安全某些具体方面的问题，但即使是“最佳”技术也存在局限性。例如，如果要让这些工具能够有效地工作，通常需要更改其 DNS 基础架构。不同产品所带来的孤立的威胁情报和数据也可能不适用于企业安全结构中的其他区域。结果，等待团队处理的是来自各个独立工具的大量不协调数据，使其不堪重负。这些工具带来了更多需要兼顾和管理的内容，不仅增加了复杂性，也消耗了本已有限的人力资源。

Unit 42 关于 OilRig 的威胁研究

OilRig 是一个由 Unit 42 首次发现的有组织的活跃威胁组织。OilRig 主要在中东地区发展，精心选择将要攻击的企业，以便跨多个行业进一步实现其区域战略目标（包括基于供应链的攻击）。该组织采用复杂的自定义 DNS 隧道执行命令和控制并泄露数据，这也是它攻击策略中的部分内容。隧道的使用包括：

- **ALMA Communicator 特洛伊木马**，它使用 DNS 隧道接收来自攻击者的命令并泄露数据。恶意软件使用特制的子域向命令和控制服务器发送数据，并使用特定的 IPv4 地址，通过 DNS 请求将数据从命令和控制传输到特洛伊木马。
- **Helminth 基于 PowerShell 的特洛伊木马**，它可以使用一系列 DNS 文本查询从命令和控制服务器获取文件，每隔 50 毫秒重复一次，实际上则是通过 DNS 发送的难以检测的增量在受害者的系统上构建恶意软件。

OilRig 使用 DNS 隧道技术使该组织建立起可靠的命令和控制，从而规避现有防御措施以执行更多的攻击阶段。从 Unit 42 的博文系列或交互式 Playbook Viewer 获取有关 OilRig 的全部详细信息。

阻止攻击者使用 DNS 对您发起攻击

如何重新夺回对 DNS 流量的控制权并阻止攻击者使用 DNS 攻击您的企业?

大量的安全数据

需要大量真实的安全数据，既可以是您自己收集的数据，也可以是通过威胁情报或网络威胁联盟收集的数据。利用庞大且不断扩展的情报共享社区所分享的数据，您所能提供的保护将不断完善。

分析和机器学习

您的安全团队需要能够对该数据运行分析。若要应对域或 DNS 隧道的动态特性，您的团队必须使用机器学习动态识别未知的恶意域。如果不执行分析，就无法预测高度动态的恶意域名。行为分析还有助于确定活动的基准情况，了解一般模式，并找出哪些是正常的活动。当防御者接收到需要采取行动的信号时，分析可帮助确定该行动所需的手动或自动化程度。分析还有助于了解需要对哪些信号采取行动，帮助您的团队合理划分时间和资源的优先级。

与新一代防火墙集成以实现自动化操作

由于许多基于 DNS 的攻击在瞬间发生，因此，安全团队必须以更短的时间手动响应这些攻击。为了抢夺先机，防御者需要自动化的响应。自动化可以快速确定受感染的计算机、采取自动响应，并在威胁扩散到网络其他区域之前进行有效控制。安全团队需要通过集成的创新工具来提升现有安全投资的价值，同时不会使操作复杂化。

基于云的保护

通过使用云，您的 DNS 防护可以得到无限扩展并始终保持最新状态，您可以利用这一关键的全新控制点阻止使用 DNS 的攻击。防御者可以通过基于云的创新来开发和部署新的检测技术，您的企业可以立即运用这些技术。基于云的保护无需请求您执行更新或更改软件即可立即更新，这意味着您的安全运营中心 (SOC) 团队的工作量将大大减少。

避免使用独立的单点产品

您的安全团队需要避免部署难以集成或需要更改 DNS 路由的独立工具。这些工具往往未针对自动化而设计，在执行操作之前需要分析人员手动将诸多来自互不相关来源的资讯整合在一起。这些产品也不会自动共享数据或资讯，您无法在整个安全堆栈中协调警报。因此，您的团队无法从整体上实施保护，导致对威胁的响应速度减慢。

DNS 流量的全面可视性和情境

为防御 DNS 上的威胁，您需要出色的检测功能以及分析，以便为安全人员提供快速有效地制定策略和响应威胁所需的情境。了解 DNS 流量有助于识别恶意和良性流量及趋势。根据安全事件情境，可以了解域被阻截的原因以及该域的历史记录。可以参照该信息优化策略和安全环境，并了解任何恶意活动的性质和范围，从而快速采取措施，解决所有问题。

基于类别采取防御措施

DNS 上的所有威胁并非都相同，每种威胁的应对方法也需要有所不同。比如，恶意软件可能只需要阻截和发出警报即可，而 C2 则需要瓦解以及识别、隔离和检查可能受感染的端点。此外，动态 DNS 或新注册的域（不明确会出现威胁）也可以被视为高风险，应避免其接触网络上的某些系统。基于 DNS 流量类别的自动响应使您能够精细控制 DNS 流量，从而更快、更有效地缓解威胁，并降低风险。

DNS 安全最佳实践

除了部署合适的技术之外，您的企业还可以遵循其他最佳实践来保护网络免受基于 DNS 的威胁。

培训员工，提高员工的安全意识

实施安全教育和意识计划，培养员工在可疑电子邮件中发现威胁的意识和习惯。鼓励他们在点击链接时要多加注意，避免安装恶意软件。网络钓鱼培训可以帮助他们了解如何识别、规避和报告基于电子邮件的攻击。

实施威胁情报计划

了解威胁形势并建立威胁情报计划，明确存在哪些威胁和相关技术。有了这些知识，就可以确保您已掌握相应的技术堆栈，从而保障您的网络安全。

了解日志内容

不要只关注 DNS 流量。除非您了解查看的内容、相关数据说明的问题以及可以采取哪些措施保护网络免受基于 DNS 的攻击，否则收集 DNS 日志几乎没有任何价值。

不要盲目依赖 DNS 解析器

如果 DNS 服务器遭到入侵，它可能会向您提供错误的响应，以便将您的流量引入其他被入侵的系统或启动中间人攻击。

制定移动员工风险管理计划

制定移动员工策略，因为他们可能使公司数据面临风险。警告他们不要使用不安全、免费或公共 Wi-Fi，因为攻击者可以轻松利用这种连接来攻击员工。集成多重身份验证。假设设备丢失或被盗的风险很高，并制定应对计划。

全面管理网络安全

不要依赖承诺可以解决所有安全问题的单一产品。相反，应采取整体方法保障网络安全，确保您拥有应对现代威胁的所有适用工具。查看安全工具的功能并确认它们是否可以有效地配合使用。您需要使用具有多种功能的工具应对各类威胁途径，包括入侵防御、URL 过滤和文件阻截。

在评估供应商解决方案时，重要的是要在概念证明中进行直接比较。各个环境不尽相同，而针对 DNS 层安全目前尚无独立于供应商的独立测试。

自动响应，而不仅仅是发出警报

需要实现自动响应，而不只是发出信号。威胁移动得很快，仅是发出警报或信号基本上不起作用。等到分析师确定警报优先级，确认威胁并识别威胁及其来源后，可能已经为时已晚。您的安全系统必须能够自动确定威胁并隔离可能受感染的系统，防止遭到更严重的损害。

您的企业是否在 DNS 安全策略中实施最佳实践？执行最佳实践评估加以确定。

paloalto NETWORKS

免费咨询热线：400 9911 194
网址：www.paloaltonetworks.cn
邮箱：contact_salesAPAC@paloaltonetworks.com