MARKET PERSPECTIVE

客户端 WAF：安全领域的下一个战场前线

Christopher Rodriguez

执行摘要

图 1

执行摘要：客户端威胁和新兴解决方案

2018 年，安全研究人员发现了一种新的网络犯罪形式 - 在线信用卡数据窃取（即 Web 数据窃取）。当时的趋势是将应用程序功能从服务器转移到客户端，而 Magecart 攻击利用了这种增长趋势。攻击者能够将恶意代码注入受信任的应用程序来源，并在远离 WAF 保护的用户浏览器中执行。最终，这些攻击将导致长期数据泄露，使得企业 Web 应用程序安全做法出现薄弱环节。

重要信息

- 客户端脚本是应用程序架构中宝贵的工具，它提供了很多好处，包括增强用户体验，提高应用程序性能，改进分析和安全性。
- 脚本无处不在。如今的网站包含几十个不同的脚本，其中，第三方脚本的占比多达三分之二。
- 客户端脚本是一个微妙而动态的功能生态系统，具有许多利益相关方。
- 在客户端安全方面，存在基准最佳做法。尽管如此，由于客户端安全方面存在的复杂性和挑战，使得企业越来越需要应对这种威胁媒介的企业安全解决方案。

建议的操作

- 市面上现有的解决方案在功能上有很大不同。对于买家而言，核心愿望是在安全性与“不造成中断”这一业务需求之间取得平衡。
- 对于许多供应商来说，客户端的监测能力和控制能力并不是一个简单或熟悉的领域。新进入市场的供应商将仔细考虑是构建自己的解决方案，还是选择通过合作或收购的方式来获得相应的功能。
- 许多 IT 企业缺乏对于客户端脚本或环境的洞察力。了解安全问题的企业更是稀少。因此，需要就市场情况对企业开展深度培训，包括提供演示、调查、概念证明和试用版本。

资料来源：IDC 2021

新的市场发展情况和动态

本期 IDC Market Perspective 分析了客户端 Web 应用程序防火墙 (WAF) 市场的威胁媒介、新兴解决方案和未来走向。

Akamai、Cymatic、PerimeterX 和 Tala Security 正在通过扩大 WAF 保护范围来应对客户端威胁，从而开拓新的市场领域。客户端脚本代表了一种新兴的威胁媒介，而安全市场也在不断发展以满足此类保护需求。

这些安全解决方案统称为 *“客户端 WAF”*、*“反脚本攻击解决方案”*或*“脚本安全解决方案”*，但该术语可能听上去令人感到困惑。请考虑以下逻辑：

- WAF 让人联想到一套适用于 Web 应用程序的特定控制措施，尽管客户端脚本在应用程序安全模式中本来就是另一个控制点。
- “客户端 WAF”是一个非常有用的术语，它可以让人联想到 WAF 中完善的安全控制措施，而相比之下，“脚本安全解决方案”则可能含义模糊，令人感到困惑。
- “反脚本攻击解决方案”将脚本概括成了一种不需要的、有缺陷的或完全恶意的技术。实际上，脚本是应用程序架构中一种非常有用的强大工具。

总的来说，IDC 之所以将这些解决方案称为“客户端 WAF”，主要是因为人们对于 WAF 更加熟悉，这种命名有助于人们理解这些解决方案。此外，术语“客户端 WAF”保持了客户端威胁类型未来扩展到脚本之外的可能性。

前言

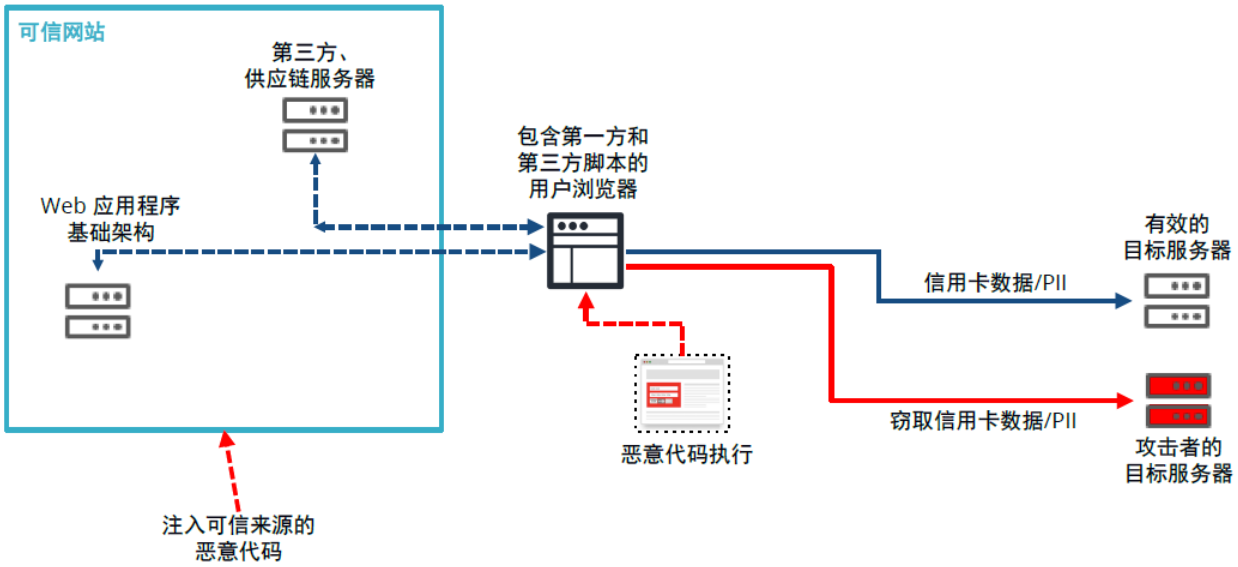
2018 年出现了一种窃取支付卡数据的新技术，此技术源自 Magecart 黑客组织。Magecart 攻击利用了一种新的威胁媒介 - 在客户端浏览器中执行的脚本。在检测到该攻击活动后，调查显示，Magecart 组织已经入侵大型在线企业的网站有数月之久，其中包括 Ticketmaster、NewEgg 和 British Airways。

Magecart 入侵活动使用客户端攻击来执行 Web 数据窃取（也可称为“在线信用卡数据窃取”或“表单劫持”）。在利用该威胁媒介的攻击中，Web 数据窃取是可见性很高的一种，而该威胁媒介还能实现其他攻击，比如水坑式攻击和加密劫持。这些攻击的目标可能各不相同，但总的来说，客户端安全解决方案有可能遭遇数据盗窃活动（可导致大规模、长时间的数据泄露）。

图 2 概述了客户端攻击的生命周期。请注意，恶意代码在浏览器中执行，这远离了 WAF 提供的保护措施。此外，恶意代码可能注入到第三方和第一方来源中。

图 2

Web 数据窃取攻击（浏览器内）剖析



资料来源：Akamai 2021

行业动态

客户端 WAF 是一个新兴市场，具有强大的增长潜力。此技术可应对一种因应用程序开发做法转变而出现的新兴威胁媒介。近年来，应用程序功能一直在从服务器向客户端转移，而且这一趋势放缓的可能性不大。通过将功能从服务器转移到客户端，可以从服务器上分流性能需求，从而使最终用户能够获得更出色的性能和互动程度更高的体验。因此，脚本成了越来越受欢迎的工具，可为互动在线体验提供支持。脚本可用于各种各样的合法用途，包括跟踪、分析、用户体验和安全性。脚本在如今的网站中普遍存在，据估计，网站包含的脚本多达 15 种甚至更多。

此外，JavaScript 的简单性也推动了非 IT 专业人士对于脚本的采用。脚本允许 IT 部门以外的业务部门出于各种目的而创建代码，并将其插入到 Web 资产中。脚本还使企业可以更轻松地集成和插入第三方服务。但是，脚本的安全性仍然在很大程度上遭到忽视，在那些仍侧重于使用 WAF 等基本工具的企业中，尤为如此。

总的来说，人们对这种威胁并不十分了解。此类别中讨论最广泛的泄露事件主要源于第三方脚本。Magecart 攻击活动就是一个很好的例子。在该案例中，Magecart 黑客可以访问目标企业的一家供应商合作伙伴的代码，并能够将恶意代码插入到受信任的脚本中。对于一些企业来说，该威胁媒介可能给人一种“犯规”的感觉。帮助网站抵御大型在线企业面临的众多不同威胁已经十分困难，在此基础上，还要求处理合作伙伴系统中的漏洞，这似乎有点强人所难。第三方脚本的问题最为棘手，因为 IT 企业对合作伙伴的代码、更新或变化缺乏监测能力或控制措施。

不幸的是，Web 数据窃取只是其中的一部分问题，因为第三方脚本只是大多数网页上存在的脚本中的一种。作为参考，Akamai 的研究人员估计，大约 67% 的脚本来自第三方。归根结底，大多数网页是一个由内部利益相关方和第三方的脚本组成的生态系统。如果服务器遭到劫持，这些内部系统也可能会传送恶意代码。

一些最佳做法可能有助于减少风险。对第三方脚本采取更严格的控制措施是一个明智的开端。定期代码审查和应用程序测试也是可靠的做法。此外，IT 企业可以利用子资源完整性 (SRI) 等技术来对脚本进行哈希处理并检测脚本的变化。虽然这些方案可以提供必要的基准保护措施，但以往的数据表明，复杂的攻击者始终会采用先进、巧妙的策略来规避检测。因此，SRI 和其他做法是有用的初始保护手段，但对于高级攻击而言效果有限。

此外，除非迫不得已，否则攻击者不太可能暂停攻击。自从发生引人关注的 Magecart 攻击以来，黑客们的攻击手段花样翻新。例如，黑客可能将广告商网络作为目标，通过横幅广告注入恶意代码。其他手段包括将 GitHub 等代码库当作攻击目标。这些代码库包含开源库和代码段，许多企业通常会将它们重复用于其 Web 应用程序并予以信任。因此，这些受信任的来源成了向本来安全的网站注入恶意脚本的潜在工具。

每家供应商处理此问题的方式略有不同。市面上流行的解决方案主要通过 JavaScript 标记进行部署，因此可以先添加安全功能，然后才允许执行脚本。从这里开始，解决方案就大不相同了。核心功能往往包括对脚本和通信（例如，源和目标）的监测和映射。其他功能包括漏洞管理、策略执行以及对恶意活动和可疑事件的检测。可以实现更高级的功能，比如对密钥和嵌入数据的加密、代码混淆、沙盒和其他防御措施。目前，采用的方法似乎是为了提供核心安全功能中足够的监测能力和自动化功能。虽然随着时间推移，更复杂的检测措施可能会受到追捧，但重点仍然是：在不中断最终用户体验或以其他方式“破坏”网站功能的情况下提供足够的安全防护。

供应商示例

目前，存在一些客户端 WAF 商业产品，它们的范围和功能各不相同。市场中存在少数几家专业公司，包括 Digital.ai（原名 Arxan）、Source Defense、Cymatic、Tala Security 和 ChameleonX（于 2019 年被 Akamai 收购）。还有一些公司拥有广泛的 Web 应用程序安全产品组合。例如，Akamai 在 2020 年推出了 Page Integrity Manager，作为其通过整体 Web 应用程序和 API 安全产品组合来防范多媒介攻击的方法的一部分。同样，PerimeterX 在 2019 年推出了自己的产品，作为对其企业爬虫程序管理解决方案的补充。最新加入该市场的供应商是 Cloudflare，该公司于 2021 年 3 月推出了新的解决方案。IDC 指出，这些公司具备爬虫程序管理领域的背景，这可能有助于他们在一定程度上熟悉客户端的安全信号。爬虫程序管理是一个很难取得成效的过程，最好的解决方案往往采用了多种技术（包括 JavaScript）来对爬虫程序的行为进行检测和分类。

客户端攻击可能很难被检测到。但是，这些威胁一旦被检测到，他们对受影响的公司及其客户所造成的财务成本损失将十分明确。例如，这些类型的数据泄露往往可以用被盗的客户记录数量来进行衡量。该领域的现有竞争对手已经在基于脚本的威胁检测和抵御方面展现出了极高的成效。这导致攻击者将他们的攻击集中在了其他地方，使得该行业中在与攻击者上演类似于打地鼠的游戏。对于攻击者来说，他们的目标是找到不安全或保护不足的网站并发起攻击。尽管监测到了 Magecart 攻击，但这个市场对该威胁媒介的认识仍然不足，这使得攻击者总能找到新的目标。所有这些因素都有可能提高主流对该威胁媒介的认识，这将推动需求，并在未来几年吸引更多公司进入该市场。

市场战略

只要网络犯罪分子认为攻击媒介能够带来利益，客户端威胁就会成为大型在线企业面临的一项挑战。但是，这是一种比勒索软件等大规模广播式攻击更具针对性的攻击类型。大多数成为攻击目标的企业需要时间来检测和抵御基于脚本的攻击。同样，主流市场对这些问题的认识可能也需要投入时间和精力来提升。供应商面临的挑战是，他们需要通过持续的培训、演示和概念验证测试来提高市场对于这些问题的认识。

更多的公司可能会推出自己的产品和功能。Akamai 在一年前推出了 Page Integrity Manager，以应对浏览器（个人身份信息 (PII) 会在其中进行提交和访问）中加载的脚本所造成的不断扩大的攻击面。2020 年，随着新冠疫情环境中使用互联网进行交易的人越来越多，客户端威胁也随之激增。

Cloudflare 在最近加入了该市场，它推出了名为 Cloudflare Page Shield 的全新解决方案。在推出此解决方案之前，Cloudflare 通过与 Tala Security 开展技术合作来应对该威胁媒介。

虽然 Cloudflare 已决定开发自己的客户端安全功能，但 IDC 指出，这种策略对其他公司来说可能不那么容易效仿。对于市场上的大多数供应商来说，在开发客户端 WAF 功能之前，他们必须具有利用 JavaScript 客户端的爬虫程序检测技术。传统的 WAF 解决方案不具备这些功能或其他与客户端代码有关的经验。

对于那些正在增强自身的 Web 应用程序和 API 安全产品线的供应商来说，收购专门的解决方案可能是开展公平竞争的最佳选择。Akamai 通过收购 ChameleonX 释放了将专用技术与云规模相结合的潜力，这就是一个很好的例子。Page Integrity Manager 现在每天可分析 64 亿次脚本执行，从而每月为超过 37 亿次页面浏览提供保护。由于每周大约可观察 4000 万次可疑和恶意的最终用户互动，Akamai 能够提供实时通知、根本原因分析、即时抵御和自动化策略创建。

IDC 的观点

只要网络犯罪分子认为客户端攻击能够带来利益，该攻击媒介就会发展成一个越来越大的安全漏洞，并且可能会持续多年。造成这种情况的一个重要原因是，人们对客户端威胁媒介并不十分了解。传统上，WAF 解决方案的工作模式是分析针对 Web 服务器的 Web 应用程序流量。随着多年来 JavaScript 的普及，大量功能已经迁移到了客户端浏览器上。但许多企业忽视了这些事实，或者没有适当评估将 Web 功能迁移到客户端浏览器所带来的风险和安全影响。

与勒索软件等大规模广播式攻击相比，此类攻击的针对性更强，这进一步导致市场陷入极度混乱的境地。例如，大多数企业都很熟悉 WAF 和 DDoS 抵御解决方案所应对的攻击类型。大众逐渐了解非必要或恶意的爬虫程序所带来的安全风险。但是，API 安全性和客户端安全性等较新的领域代表了新兴的风险领域，这些领域完全不可见，因此带来了巨大的风险，就像冰山的水下部分（请参见图 3）。

图 3

Web 应用程序和 API 安全冰山

资料来源：IDC 2021

在企业了解了潜在的威胁媒介后，他们需要对在复杂的 IT 环境（包含多个域、网页和 Web 应用程序）中运行的脚本编制目录并加以了解，此过程可能是一项艰巨的任务。在 Magecart 攻击事件发生时，要检测注入的恶意脚本，就必须手动逐行审查代码以检测变更。此过程现在变得更加精简，因为研究人员了解了底层问题和最佳做法。但是，重点仍然在于，大多数遭到攻击的企业需要耗费时间来检测和抵御基于脚本的攻击，因为他们需要花时间来了解威胁媒介，以及耗费额外的时间来识别任何现有的安全漏洞或对漏洞的利用。此外，威胁媒介是一个不断移动的目标，因为每个季度都有 75% 的脚本发生改变。每一个新的变更都有可能引入新的漏洞和恶意代码。

但是，时间至关重要。由于客户端攻击造成的已知漏洞已经存在了很长时间，这为攻击者提供了几个月的先机。在这段时间里，有无数的信用卡数据以及其他 PII 被盗。检测到攻击后，攻击者可以从容结束攻击，并继续攻击下一个受害者。从本质上讲，客户端攻击需要大量的时间来检测，这种失衡状态是网络犯罪分子的一个巨大优势，因此必须减少这种失衡。

所以，安全行业在培训买家并提高买家对该问题的认识方面，时间是最大的障碍。供应商面临的挑战是，他们需要通过持续的培训、演示和概念验证测试来提高市场对于这些问题的认识。例如，Akamai 正在提供 Page Integrity Manager 产品的免费试用版。该解决方案概述了成为攻击目标的网页的脚本生态系统，并分析了各种脚本、漏洞和风险因素。其他供应商也提供了试用版、演示和培训资源。

IDC 对这些方法表示赞许。没有什么比概念验证更能介绍情况的紧迫性或安全解决方案的价值和功效。供应商有可能获得付费订阅客户，这一优势显而易见。买家也会从中受益匪浅，因为他们可以监测到以往对于大多数企业而言完全是盲点的威胁媒介。

未来，IDC 将监控客户端 WAF 市场，以了解其对 WAF、DDoS 抵御、爬虫程序管理和在线欺诈预防等成熟市场的影响。在解决客户端的安全盲点问题后，需要更深入地讨论客户端的潜在监测和执行功能所带来的影响，而这将作为一个安全控制点。

了解更多

相关研究

- *IDC FutureScape: Worldwide Future of Trust 2021 Predictions*（IDC #US46912920，2020 年 10 月）
- *Pervasive Application Edge Defense: An Application-Based Framework for Trust*（IDC #US46810219，2020 年 9 月）
- *IDC Market Glance: Software-Defined Secure Access, 2Q20*（IDC #US46291520，2020 年 5 月）
- *Worldwide Internet Defense Forecast, 2020-2023: Infrastructure and Application Security Drive Business Value*（IDC #US46022619，2020 年 2 月）
- *Security Convergence at the Edge: Emerging Pervasive Data Defense and Response Platforms*（IDC #US46075520，2020 年 2 月）

概要

本期 IDC Market Perspective 分析了客户端 WAF 市场的威胁媒介、新兴解决方案和未来走向。很少有 IT 企业能够完全了解对其 Web 环境中运行的客户端脚本发起攻击的威胁。网络犯罪分子将客户端脚本作为一种偷偷执行恶意代码的手段，以此获得巨大的经济利益，而且不会有被捕的风险。随着这种威胁媒介在未来几年内变得越来越明显，对于企业客户端 WAF 解决方案的需求也将稳步攀升。

IDC 网络安全产品和战略研究经理 Christopher Rodriguez 表示“客户端脚本是安全领域的下一个战场前线。网络犯罪分子仍在不遗余力地寻找有利可图的漏洞，并在企业数字化安全堆栈中找到了一个新的缺陷。”

关于 IDC

国际数据公司 (IDC) 是全球著名的信息技术、电信行业和消费科技咨询、顾问和活动服务专业提供商。IDC 的分析和洞察助力 IT 专业人士、业务主管和投资机构制定基于事实的技术决策，以实现关键业务目标。IDC 在全球拥有超过 1100 名分析师，为 110 多个国家或地区的技术和行业发展机遇提供全球化、区域化和本地化的专业视角及服务。50 多年来，IDC 提供的战略见解不断帮助着我们的客户实现其关键业务目标。IDC 是提供技术媒体、研究和活动的全球领先公司 IDG 的子公司。

全球总部

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter：@IDC
idc-community.com
www.idc.com/cn