MARKET PERSPECTIVE

Client-Side WAF: The Next Security Frontier

Christopher Rodriguez

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Client-Side Threats and Emerging Solutions

In 2018, security researchers identified a new form of cybercrime called online card skimming or web skimming. The Magecart attacks exploited a growing trend to shift application functionality from the server to the client. Threat actors were able to inject malicious code into trusted application sources, which executed in users' browsers far from the protection of a WAF. Ultimately, the attacks represented a long-running data breach that exposed a weak link in enterprise web application security practices.

Key Takeaways

- Client-side scripts are a valuable tool in application architecture, offering the benefits of enhanced user experience, application performance, analytics, and security.
- Scripts are ubiquitous. Websites today have dozens of different scripts, with third-party scripts representing as many as two out of every three scripts.
- Client-side scripts represent a delicate but dynamic ecosystem of functionality, with many stakeholders.
- There are baseline best practices for client-side security. However, the complexities and challenges of client-side security will drive demand for enterprise security solutions for this threat vector.

Recommended Actions

- Available solutions in the market vary drastically by functionality. For buyers, the core desire is to balance security versus the business requirement of "not breaking things."
- Client-side visibility and control are not an easy or familiar area for many vendors. New market entrants will carefully consider whether to build their own solutions or choose existing capabilities to partner with or acquire.
- Many IT organizations lack any insights into client-side scripts or environments. Fewer understand the security issues. A high degree of market education including demos, research, proofs of concepts, and trial versions are required.

Source: IDC, 2021

April 2021, IDC #US47623221

NEW MARKET DEVELOPMENTS AND DYNAMICS

This IDC Market Perspective provides an analysis of the threat vector, emerging solutions, and future of the client-side web application firewall (WAF) market.

Akamai, Cymatic, PerimeterX, and Tala Security are blazing new trails by extending WAF protection to address client-side threats. Client-side scripts represent an emerging threat vector, and the security market is evolving to address the need.

These security solutions are roundly referred to as *"client-side WAF," anti-scripting,* or *script security,* but the terminology may be confusing. Consider the following options:

- WAF conjures to mind a specific set of controls that apply to web applications, although client-side scripts are inherently a different control point in the application security paradigm.
- Client-side WAF is a useful term in drawing a connection to a well-established security control in WAF, while "script security" can be nebulous and confusing by comparison.
- Anti-scripting generalizes scripts as an unwanted, flawed, or outright malicious technology. In reality, scripts represent a valuable, powerful tool in application architecture.

Overall, IDC refers to these solutions as client-side WAF primarily for the benefits of familiarity associated with WAF. In addition, the term client-side WAF maintains the possibility for future expansion of client-side threat types beyond scripts.

Introduction

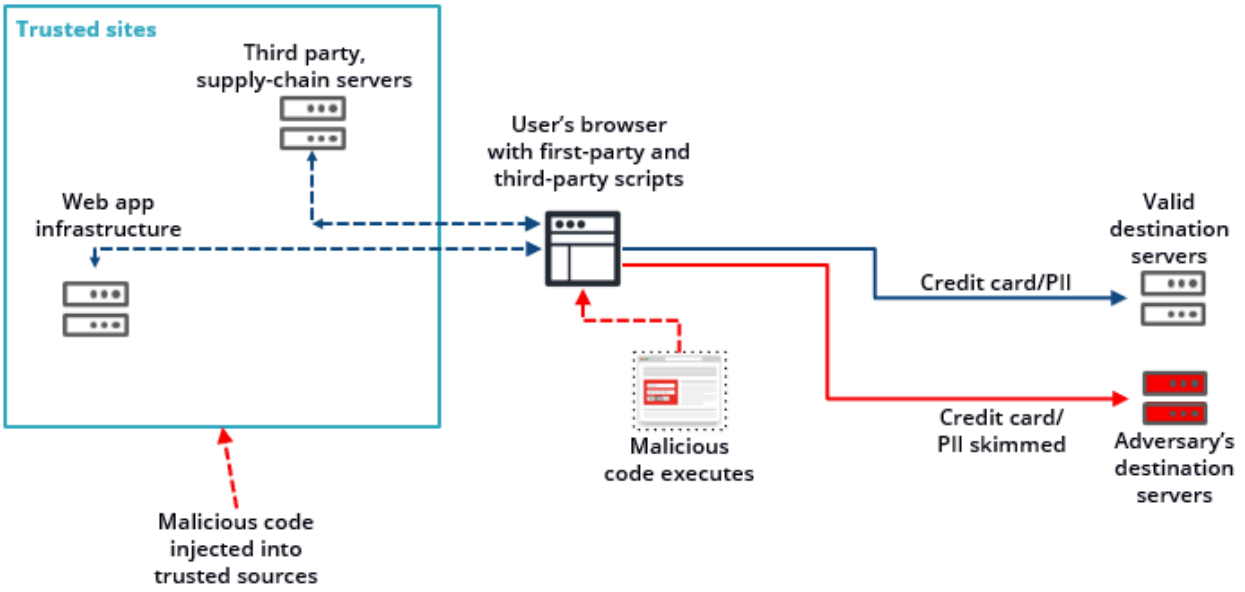
A new technique for skimming payment card data emerged in 2018 that was attributed to the Magecart hacker group. The Magecart attacks exploited a novel threat vector — scripts that execute in client browsers. Once the attack campaign was detected, investigations showed that the Magecart group had compromised the websites of large online enterprises for months, including Ticketmaster, NewEgg, and British Airways.

The Magecart campaign used client-side attacks to perform web skimming (which may also be referred to as online card skimming or form jacking). Web skimming is one highly visible aspect of this threat vector, but the threat vector enables other attacks such as watering hole attacks and cryptojacking. The goal of these attacks may vary, but overall, client-side security holds potential for data theft campaigns that result in massive, long-running data breaches.

Figure 2 provides an overview of the life cycle of a client-side attack. Note that the malicious code executes in the browser, far from the protections afforded by a WAF. In addition, malicious code may be injected into both third-party and first-party sources.

FIGURE 2

Anatomy of a Web Skimming Attack (in the Browser)



Source: Akamai, 2021

Industry Dynamics

Client-side WAF is a nascent market with strong potential for growth. This technology addresses an emerging threat vector that is the result of a shift in application development practices. Application functionality has been shifting from servers to clients in recent years and the trend is unlikely to slow. The shift in functionality from server to client offloads performance demands from the server, thus enabling better performance and a more interactive experience for end users. As a result, scripts are increasingly popular tools for powering interactive online experiences. Scripts are used for a wide and varied array of legitimate purposes, including tracking, analytics, user experience, and security. Scripts are ubiquitous with websites today, as they contain 15 or more different scripts, by some estimates.

Furthermore, the simplicity of JavaScript has driven the adoption of scripting by non-IT professionals. Scripts allow business units outside of the IT department to create and insert code into web assets for various purposes. Scripts also allow easier integration and insertion of third-party services. However, the security aspect of scripts remains largely overlooked, especially among organizations that continue to focus on essential tools such as WAF.

Overall, the threat is not well understood. The most widely discussed breaches in this category focus on third-party scripts. The Magecart campaign provides a germane example. In that case, Magecart hackers had access to the code of a supplier partner of the targeted organization and were able to insert malicious code into trusted scripts. For some organizations, the threat vector may feel like a practice in "moving the goalposts." Already, it's a nontrivial task to secure a website against the many varied threats facing large online enterprises, and the requirement to account for vulnerabilities in partner systems seems practically unfair. Third-party scripts are the most problematic, as IT organizations lack visibility or control over partners' code, updates, or changes.

Unfortunately, web skimming is only part of the problem, as third-party scripts represent only one demographic of the scripts present on most web pages. For reference, researchers from Akamai have estimated that about 67% of scripts come from third parties. Ultimately, most web pages are an ecosystem of scripts from internal stakeholders and third parties. These internal systems can also serve malicious code if the servers are hijacked.

There are some best practices that are likely to help reduce risk. Tighter control over third-party scripts is a smart start. Regular code reviews and application testing are reliable practices as well. In addition, IT organizations can leverage technologies such as Subresource Integrity (SRI) to hash and detect changes to scripts. While these options can provide a necessary baseline of protection, history has shown that sophisticated threat actors consistently employ advanced, clever tactics to avoid detection. As a result, SRI and other practices are useful starts but will be limited against advanced attacks.

Moreover, threat actors are unlikely to pause their efforts unless forced to. Since the headline-grabbing Magecart attacks, hackers have modified these attacks in numerous ways. For example, hackers may target advertiser networks as a means to inject malicious code via banner ads. Other means include targeting code repositories such as GitHub. These repositories include open source libraries and code snippets that are generally reused and trusted by many organizations for use in their web applications. As a result, these trusted sources represent a potential vehicle for injecting malicious scripts into otherwise safe websites.

Each vendor approaches the problem slightly differently. The solutions in the market trend are largely deployed via JavaScript tags, which allows the security function to be inserted before scripts can execute. From there, solutions diverge drastically. Core capabilities tend to include the visibility and mapping of scripts and communications (e.g., source and destination). Additional capabilities include vulnerability management, policy enforcement, and detection of malicious activity and suspicious events. More advanced capabilities are possible, such as encryption of keys and embedded data, code obfuscation, sandboxing, and other defensive measures. For now, the approach seems to be to provide sufficient visibility and automation of core security capabilities. While more sophisticated detection measures may be welcome over time, the emphasis continues to be on providing sufficient security without disrupting the end user experience, or otherwise "breaking" website functionality.

Vendor Examples

Currently, there are a few commercial offerings for client-side WAF, which are varied in scope and capability. There are a handful of market specialists including Digital.ai (formerly named Arxan), Source Defense, Cymatic, Tala Security, and ChameleonX (acquired by Akamai in 2019). Others have broad web application security portfolios. For example, Akamai introduced Page Integrity Manager in 2020 as part of its approach to protect against multivector attacks via a holistic web application and API security portfolio. Similarly, PerimeterX introduced its offering in 2019 as a complement to its enterprise bot management solution. The newest entrant is Cloudflare, which introduced its new solution in March 2021. IDC notes that these companies have a background in bot management that may have helped to provide a level of familiarity with client-side security signals. Bot management is a challenging process to do well, and best-of-breed solutions tend to employ multiple techniques (including JavaScript) to detect and categorize bot behavior.

Client-side attacks can be difficult to detect. However, once they are detected, these threats are quite clear in terms of financial costs to affected companies and their customers. For example, these types of data breaches can often be measured in terms of the number of customer records stolen. Existing competitors in the space have demonstrated a high degree of efficacy in script-based threat detection

and mitigation. This causes threat actors to focus their efforts elsewhere, resulting in a game of whack-a-mole in the industry. For attackers, the goal is to find unsecured or undersecured websites to attack. Despite the visibility of the Magecart attacks, market awareness of the threat vector remains low, which allows threat actors to find new targets. All of these factors are likely to increase mainstream awareness of the threat vector, which will drive demand and lure additional companies into the marketplace in the coming years.

Market Strategies

Client-side threats will be a challenge for large online enterprises for as long as cybercriminals perceive the attack vector to be profitable. However, this is an attack type that is more highly targeted than mass broadcasted attacks such as ransomware. It will take time for most targeted organizations to detect and mitigate script-based attacks. Mainstream market awareness of these issues may also take time and effort to elevate. Vendors are challenged to raise awareness via ongoing education, demonstrations, and proof-of-concept testing.

More companies will likely introduce products and capabilities of their own. Akamai introduced Page Integrity Manager a year ago to address the expanding attack surface created by scripts loaded in browsers — where personally identifiable information (PII) is submitted and accessed. This is also where client-side threats have proliferated in 2020 as the use of the internet for transactions accelerated in the COVID-19 environment.

Cloudflare is the most recent addition to the market, introducing a new solution called Cloudflare Page Shield. Prior to this deal, Cloudflare addressed this threat vector via a technology partnership with Tala Security.

While Cloudflare has decided to develop its own client-side security capabilities, IDC notes that the approach may not be as easy for others to follow. For most vendors in the market, the development of client-side WAF capabilities was preceded by bot detection techniques that leverage JavaScript clients. Legacy WAF solutions do not have these capabilities or other experience with client-side code.

For vendors that are bolstering their web application and API security product lines, the acquisition of specialized solutions may present the best option to even the playing field. Akamai's acquisition of ChameleonX provides an example of the potential benefits of combining purpose-built technologies with cloud scale. Page Integrity Manager now protects over 3.7 billion page views each month by analyzing 6.4 billion script executions every day. Approximately, 40 million suspicious and malicious end-user interactions are observed weekly, which allows Akamai to provide real-time notifications, root cause analysis, immediate mitigation, and automation policy creation.

IDC'S POINT OF VIEW

Client-side attacks will be a growing security gap for as long as cybercriminals perceive the attack vector to be profitable, which could be for many years. A significant reason for this is the fact that the client-side threat vector is not well understood. Traditionally, WAF solutions function by analyzing web application traffic targeting the web server. As JavaScript has become more popular over the years, significant amounts of functionality have migrated to the client browser. But many organizations overlook these facts or have not done a proper assessment of the risks and security implications of this migration of web functionality to the client browser.

The fact that this type of attack is more highly targeted than massive-scale broadcasted attacks such as ransomware is further contributing to high levels of market confusion. For example, most organizations are well acquainted with the types of attacks addressed by WAF and DDoS mitigation solutions. The security risk presented by unwanted or malicious bots is another practice that is gaining mainstream awareness. However, newer areas such as API security and client-side security represent emerging areas of risk that are simply not visible and thus present a significant risk, much like the submerged half of an iceberg (see Figure 3).

FIGURE 3

The Web Application and API Security Iceberg

Source: IDC, 2021

Once an organization understands the potential threat vector, the process of cataloging and understanding the scripts running in a complex IT environment with several domains, web pages, and web applications may represent a herculean task. At the time of the Magecart attacks, the process of detecting injected malicious scripts represented a manual, line-by-line review of the code to detect changes. The process is more streamlined now, as researchers understand the underlying issues and best practices. However, the point remains that it will take time for most targeted organizations to detect and mitigate script-based attacks because it takes time to understand the threat vector and additional time to identify any existing security gaps or exploits. In addition, the threat vector is a moving target, as 75% of scripts are changed each quarter. Each new change opens the possibility to introduce new vulnerabilities and malicious code.

However, time is of the essence. Already, the known breaches due to client-side attacks were long lived and provided attackers with months' worth of a head start. In that time, a countless number of credit cards as well as other PII, were stolen. Once an attack is detected, attackers are free to close shop and start fresh with the next victim. Essentially, client-side attacks have a massive time to detection, and this imbalance is a tremendous advantage for cybercriminals that must be reduced.

Thus time is the biggest hurdle for the security industry to educate and improve buyer awareness of the issue. Vendors are challenged to raise awareness via ongoing education, demonstrations, and proof-of-concept testing. Akamai, for example, is offering a free trial version of its Page Integrity Manager offering. The solution provides an overview of the script ecosystem of targeted web pages, along with analysis of the various scripts, vulnerabilities, and risk factors. Other vendors offer trial versions, demonstrations, and educational resources as well.

IDC lauds these approaches. Nothing conveys the urgency of a situation or the value and efficacy of a security solution than a proof of concept. For vendors, the benefit of a potential premium subscription conversion is clear. Buyers also benefit substantially, by gaining visibility into a threat vector that has traditionally been a complete blind spot for most organizations.

Further on the horizon, IDC will be monitoring the client-side WAF market to understand its impact on established markets such as WAF, DDoS mitigation, bot management, and online fraud prevention. Once the client-side security blind spot is addressed, deeper discussions on the impact of the potential visibility and enforcement capabilities of the client side, as a security control point, will be required.

LEARN MORE

Related Research

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

Synopsis

This IDC Market Perspective provides an analysis of the threat vector, emerging solutions, and future of the client-side WAF market. Few IT organizations have a complete understanding of the threats targeting client-side scripts that run in their web environments. Cybercriminals have targeted client-side scripts as a means to execute malicious code surreptitiously for tremendous financial gain, without the risk of being caught. As this threat vector grows more pronounced in the coming years, the demand for enterprise client-side WAF solutions is set to climb steadily.

"The client-side script is the next frontier for security. Cybercriminals remain relentless in their pursuit of lucrative exploits and have found a new gap in enterprise digital security stacks," says Christopher Rodriguez, research manager, IDC Network Security Products and Strategies.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

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