SOTI

10 YEARS
OF SECURITY INSIGHT

V10 ISSUE 05

Navigating the Rising Tide

Attack Trends in Financial Services

Akamai

State of the Internet/Security

Table of Contents

Introduction

The financial services industry is not just a cornerstone of the global economy, it's the lifeblood of economic growth and development. Encompassing a diverse array of industries, such as commercial banks, payment processors, asset management companies, investment banks, and insurance organizations, financial services is in a constant state of evolution.

Technological advancements continue to reshape the financial services landscape, giving rise to financial technology (fintech) innovations like digital banks, robo-advisors, and cryptographic assets. The number of fintech companies has surged globally, with the United States and China leading the way. As of January 2024, 8 of the 10 largest fintech companies were based in these two countries. This technological shift is also reflected in the growth of cashless transactions, which is expected to increase significantly, particularly in places where financial access is limited. But with innovation comes vulnerability.

Cybercriminals are relentlessly targeting financial institutions, and the impact of their attacks goes far beyond financial loss. Operational disruptions, reputational damage, and crippling regulatory penalties can erode the foundation of trust on which the financial services industry is built. How can financial institutions establish effective defenses at a time when the speed of digital transformation is matched only by the sophistication of cyberthreats?

This State of the Internet report is designed specifically to help financial services professionals around the globe — Akamai clients, cybersecurity researchers, and industry leaders — navigate the increasingly complex threat landscape. As a prime target for cybercriminals, the financial services industry requires a collaborative effort to safeguard its critical infrastructure, protect businesses and customers, ensure the stability of financial markets, and prevent economic disruptions. The research presented in this report is essential reading for those who want to stay ahead of attackers, fortify the sector's critical assets, and ensure the continued trust and reliability that underpin global financial relationships.

FS-ISAC guest column

Strengthening financial services with compliance, operational resilience, and cybersecurity

One of the pivotal challenges that confronts the global financial sector today is the imperative for enhanced compliance and operational resilience. As the landscape of regulations evolves, financial institutions must proactively adapt to meet these new demands. The introduction of the Digital Operational Resilience Act (DORA), for instance, underscores the necessity for a robust framework capable of withstanding disruptions related to information and communication technology (ICT). Set to take effect in January 2025, DORA mandates comprehensive resilience strategies for financial entities and their ICT third-party providers, which is compelling firms to elevate their security and incident response capabilities.

The U.S. Securities and Exchange Commission's updated guidelines further amplify the need for a holistic cybersecurity approach. Financial institutions are now required to integrate operational resilience and disaster recovery into their strategies, placing significant emphasis on the materiality of cyber risks. This involves a deep understanding of how significant threats and incidents can impact financial stability and operations. The mandates for prompt disclosure of material cybersecurity incidents and detailed articulation of risk management strategies in annual reports signifies a paradigm shift in regulatory expectations. Navigating these regulatory landscapes requires financial institutions to partner with entities that offer state-of-the-art security solutions and visibility. As shown in this research, Akamai's expertise can help ensure that financial services organizations not only achieve compliance but also maintain operational integrity amid stringent regulatory requirements.

Considering these developments, financial institutions must adopt a comprehensive approach to address the complexities of compliance and operational resilience. This involves identifying and prioritizing material risks — those that could significantly impact an investor's decision-making process. Financial institutions must incorporate these material risks into their risk management frameworks and ensure that robust incident response plans are in place. The path to effective operational resilience is paved with the adoption of a multilayered defense-in-depth strategy. This includes reducing the attack surface through network segmentation and microsegmentation, implementing data-at-rest encryption, hardening servers, and using web application firewalls coupled with advanced threat detection systems. Continuous monitoring and regular security assessments are crucial to promptly identify and mitigate risks.

Exercises in incident response planning, based on current threat intelligence and research such as Akamai's State of the Internet (SOTI) reports are essential for financial institutions. These exercises help build plausible scenarios and ensure that institutions can adapt to new tools, techniques, and procedures as they emerge. This proactive stance is vital in ensuring operational resilience and maintaining customer trust in an increasingly volatile threat landscape. As the financial services industry evolves, the intersection of compliance, operational resilience, and cybersecurity will continue to shape its future. By adopting advanced security measures and enhancing visibility, financial institutions can navigate regulatory complexities and safeguard their operations to maintain the trust that is essential to our business.

Teresa Walsh
Global Head of Intelligence, FS-ISAC

Key insights

34%

Percentage of Layers 3 and 4 DDoS attack events experienced by financial services institutions

Financial services remains the most frequently attacked industry by distributed denial-of-service (DDoS) attack events on Layers 3 and 4. This is followed by games at 18% and high technology at 15%. This prevalent threat likely stems from ongoing geopolitical tensions, particularly the Israel-Hamas and Russia-Ukraine wars, which have fueled a surge in hacktivist activity across the globe.

API growth triggers rise in Layer 7 DDoS attacks

Although web applications have traditionally been prime targets of cyberattacks, Layer 7 DDoS attacks on APIs have notable peaks during the reporting period. This is driven largely by the growing adoption of APIs in financial services to meet evolving compliance and regulatory requirements. As organizations rely more heavily on APIs, adversaries are adapting their tactics, making API security a critical priority for modern businesses.

Traffic spikes highlight need to assess DDoS by frequency and volume

DDoS attacks in financial services reveal a critical insight: Event frequency doesn't always correlate with attack intensity. Although some months show few attacks, the corresponding Gbps data indicates significant traffic spikes, emphasizing the need to consider both attack frequency and volume when assessing DDoS attack impacts.

36%

Percentage of suspicious domains targeting financial institutions

Phishing attacks have been increasingly targeting financial services customers, elevating the risks of identity theft and account takeover. This attack trend exposes financial institutions to greater scrutiny from regulators, and breaches raise trust concerns from customers.

30%

Percentage of page visits directed to phishing and brand impersonation sites

Attackers successfully drive traffic to fraudulent sites by mimicking legitimate financial services websites and apps. They continue to target financial institutions with phishing to obtain the troves of sensitive information held by these organizations.

Financial services remains the top target for Layer 3 and 4 DDoS attacks

Layer 3 and Layer 4 distributed denial-of-service (DDoS) attacks target network and transport layers, overwhelming network infrastructure and exhausting server resources and bandwidth. These attacks send an enormous amount of traffic, aiming to consume network capacity and degrade performance for legitimate users. Among all industries, the financial services industry has been the primary target for Layer 3 and Layer 4 DDoS attacks (Figure 1). This trend is driven by several interconnected factors that have created a perfect storm of vulnerability and opportunity for attackers.

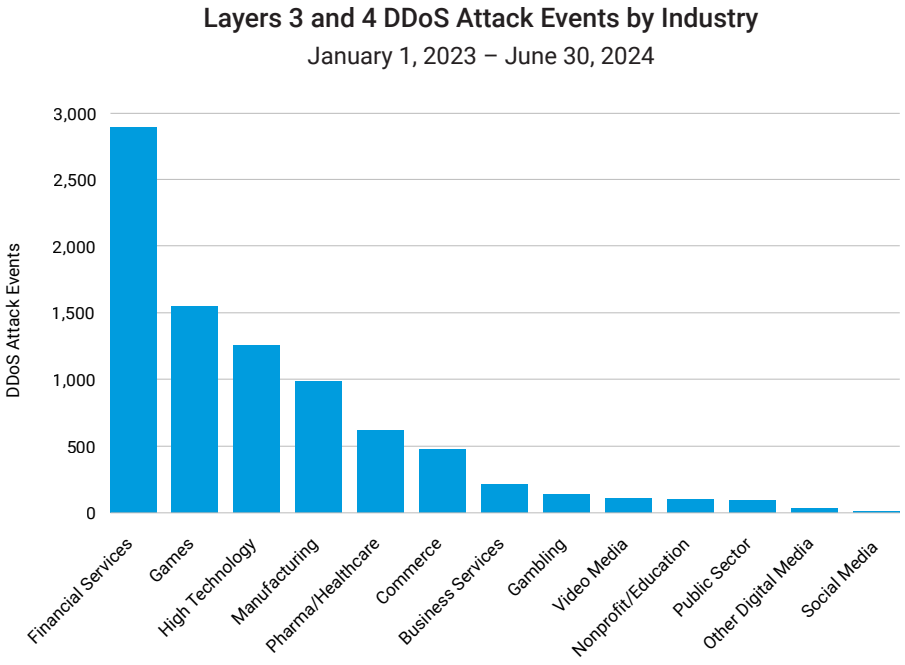


Fig. 1: The financial services industry has a towering lead over other industries in Layers 3 and 4 DDoS attack events

Geopolitical tensions have played a significant role in the rise of DDoS attacks on financial institutions. The ongoing Russia-Ukraine war and the Israel-Hamas war have coincided with notable increases in pro-Russian and pro-Palestinian hacktivism. These conflicts have fueled a surge in DDoS attacks, particularly targeting European banks with affiliations to Ukraine. The politically motivated nature of these attacks adds an additional layer of complexity to the threat landscape.

Financial institutions are especially attractive targets for DDoS attackers because of the high stakes involved. Successful disruption of operations can lead to severe financial impact, significant reputation damage, and a loss of trust in the global financial system. The potential for widespread consequences makes financial services a prime target for those seeking to cause maximum disruption or to make a political statement.

Technological advancements have dramatically increased the power and capabilities of DDoS attackers, who can now deploy virtual machine (VM) botnets to conduct attacks more efficiently by harnessing computational resources across numerous VMs and Internet of Things (IoT) devices. This approach exploits the distributed nature of cloud services, making attacks more difficult to mitigate and trace. Attackers can take advantage of high bandwidth availability and vast computational resources, enabling them to launch adaptable, powerful, and cost-effective DDoS attacks across various strategies.

Attackers can take advantage of high bandwidth availability and vast computational resources, enabling them to launch adaptable, powerful, and cost-effective DDoS attacks across various strategies.

The expanding attack surface in the financial services industry has also contributed to the rise in DDoS attacks. The growing use of digital services and APIs has opened more entry points for attackers. This shift has added complexity to financial systems and introduced numerous potential vulnerabilities for attackers to exploit. Undocumented shadow APIs are of particular concern, as they are often unprotected because information security teams are unaware of their existence. Attackers can exploit these APIs to exfiltrate data, bypass authentication controls, or perform disruptive acts.

Regulatory pressures have inadvertently increased the vulnerability of financial institutions to DDoS attacks. Requirements such as the Payment Services Directive 2 (PSD2), introduced by the European Union, have mandated that banks open their systems to third-party providers, such as fintech companies, through APIs. While this allows banks to respond to growing customer expectations through integration with fintech, mobile apps, and other platforms, it also increases security risks and expands the attack surface. The additional use of APIs among these various entities creates more potential points of failure for attackers to target.

Collectively, these factors have contributed to the financial services industry's continued title as the top target for Layer 3 and Layer 4 DDoS attacks. The combination of geopolitical motivations, high-value targets, technological advancements, an expanding digital footprint, and regulatory pressures has created an environment in which DDoS attacks on financial institutions are not only more frequent but also potentially more damaging than ever before. As the industry continues to evolve, so too must its defenses against these increasingly sophisticated and persistent threats.

Layers 3 and 4 DDoS attack events: A rollercoaster ride

Although the financial services industry experiences the highest frequency of Layer 3 and Layer 4 DDoS attack events, the rate of these attacks fluctuates throughout the year (Figure 2).

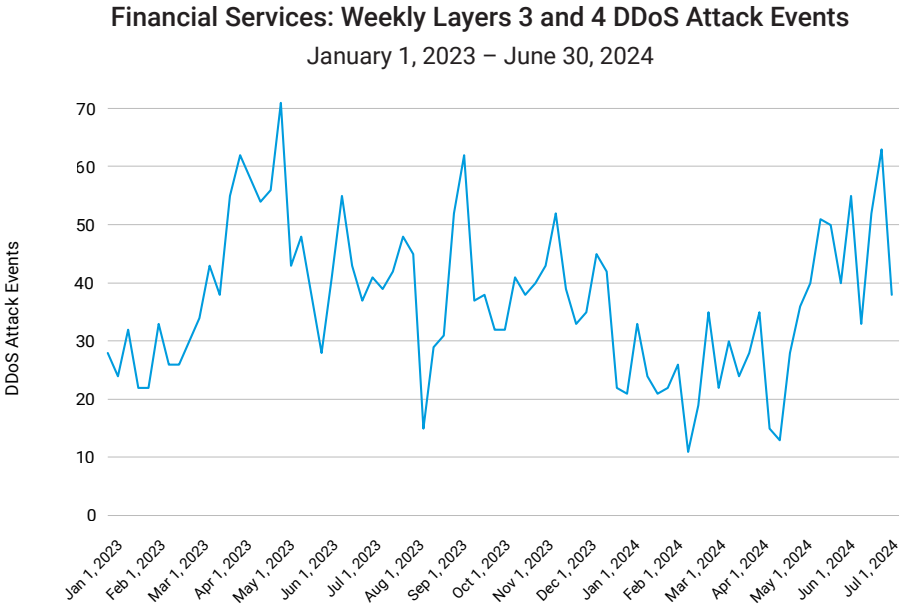


Fig. 2: A rise and fall pattern for Layers 3 and 4 DDoS attack events in the financial services industry

The Layer 3 and Layer 4 DDoS attacks on the financial services industry during March/April 2023, August/September 2023, and April/May 2024 can be attributed to several specific factors.

The spring, from March to April, marks the active U.S. income tax season, presenting an attractive opportunity for DDoS attackers. There was a noticeable rise in account abuse at national and regional banks starting on April 16, which coincides with when many banks report their first-quarter earnings. During this period, identity and access management (IAM) and network providers, such as Okta and Cisco, also reported increased and substantial credential stuffing attacks targeting online services.

In April 2023, specifically, the discovery of the Service Location Protocol (SLP) high-severity vulnerability (CVE-2023-29552) likely contributed to the surge in attack activities. This vulnerability, which can amplify DDoS attacks in both the network and application layers, reportedly affected more than 2,000 organizations worldwide and more than 54,000 SLP instances on the internet. By exploiting this vulnerability, attackers could use the compromised instances to initiate large-scale DDoS amplification attacks. With an amplification factor of up to 2,200 times, this vulnerability enabled one of the most significant amplification attacks ever documented.

We identified a key event by examining the August/September 2023 period. Akamai observed and thwarted the largest recorded DDoS attack on a U.S. financial institution on September 5, 2023. This assault combined ACK, PUSH, RESET, and SYN flood techniques, reaching peak intensities of 633.7 gigabits per second (Gbps) and 55.1 million packets per second (Mpps). Despite its high intensity, the attack was brief, lasting less than two minutes.

Security spotlight

Layers 3 and 4 DDoS attack intensity: Events vs. Gbps

To fully grasp the threat that DDoS attacks pose to the financial services industry, it's crucial to understand their sheer complexity and scale. These aren't simple, isolated incidents; each attack often involves multiple, high-volume attempts that flood networks with gigabits of data and millions of packets per second. The sophistication, intensity, and length of the attacks are increasing, and the attackers are using more varied techniques, which escalates the risk for financial institutions (Figure 3).

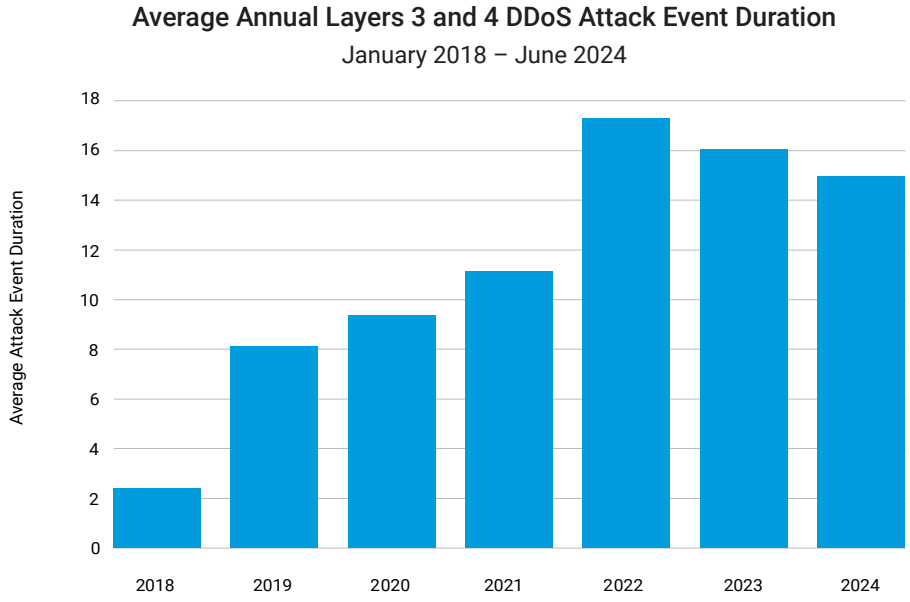


Fig. 3: The global trend for Layer 3 and 4 DDoS attack duration is increasing

Furthermore, when you compare the graph of the number of Layer 3 and 4 DDoS attack events in the financial services industry with the corresponding DDoS Gbps data, you'll notice a significant discrepancy (Figure 4). The Gbps graph shows sharp increases that are not reflected in the attack events graph. This disparity highlights an important concept: Even a month with relatively few attack events can still have an extremely high volume of DDoS traffic in terms of Gbps.

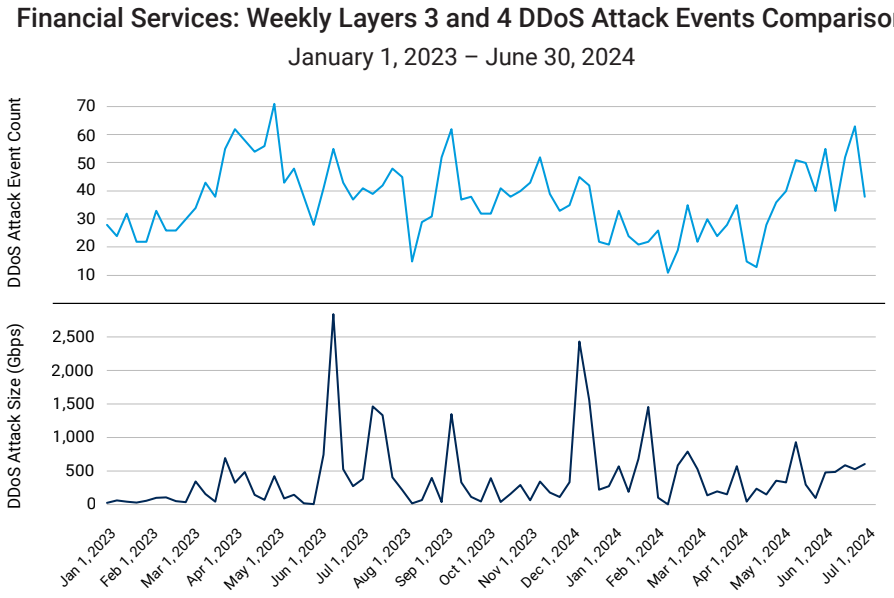


Fig. 4: The financial services industry's Layers 3 and 4 DDoS attack events compared with their measurements in Gbps

This observation highlights a critical point: relying solely on the frequency of attack events severely underestimates the true threat. It's essential to consider both the volume and intensity of traffic in each attack. A small number of highly intense DDoS attacks can cause far more damage than a larger number of smaller-scale events, making it imperative to assess the full scope of each threat.

A tendency to go solo: Single vector Layers 3 and 4 DDoS attacks in financial services

Application, or network, multi-vector attacks are a common strategy for cybercriminals who are attempting to corrupt or gain unauthorized access to a system. However, attackers focused on the financial services industry appear to attempt single vector attacks more frequently when it comes to DDoS in Layers 3 and 4 (Figure 5).

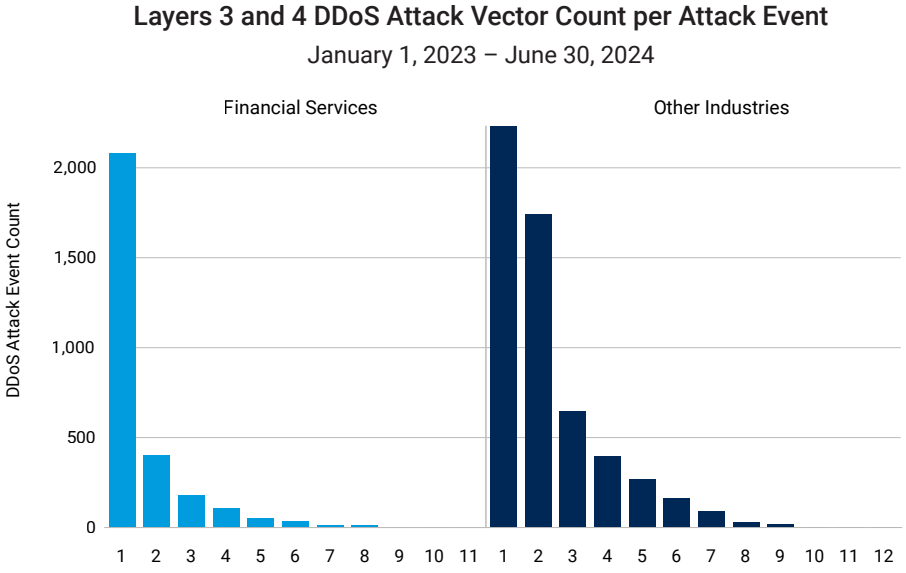


Fig. 5: Single vector attacks are more widely used for Layers 3 and 4 DDoS attacks in the financial services industry

Single vector DDoS attacks targeting Layers 3 and 4 require fewer resources and can be highly effective on their own, especially against financial institutions that may have robust defenses against more complex attacks. They are generally easier to execute and require less coordination than multi-vector attacks. There may also be some specifically known vulnerabilities that financial institutions have at Layers 3 and 4 that could be exploited effectively with a single vector attack without the risk of attempting other attack vectors that could be detected by security.

This preference for single vector attacks in the financial services industry presents a unique challenge for cybersecurity teams. While you must remain vigilant against complex, multi-vector assaults, it's crucial to ensure that any defenses can withstand focused, single vector attacks on Layers 3 and 4.

Increasing Layer 7 DDoS attacks on APIs

Application layer (Layer 7) DDoS attacks, also known as HTTP or web traffic layer attacks, have become increasingly prevalent and are now a favored method for threat actors who target the financial services industry. These attacks specifically focus on the more resource-intensive components of applications, effectively denying access to legitimate users. Unlike Layers 3 and 4 DDoS attacks, which are often mitigated by firewalls and network protection, Layer 7 attacks bypass these defenses by masquerading as legitimate requests when targeting specific application pages or search functions, with the goal of overwhelming the application server.

Although web applications in the financial services industry have generally been targeted more frequently than APIs, we've observed sharp increases in the number of Layer 7 DDoS attacks that specifically target APIs (Figure 6). These spikes are notably more significant and varied than the overall API attack pattern in other industries.

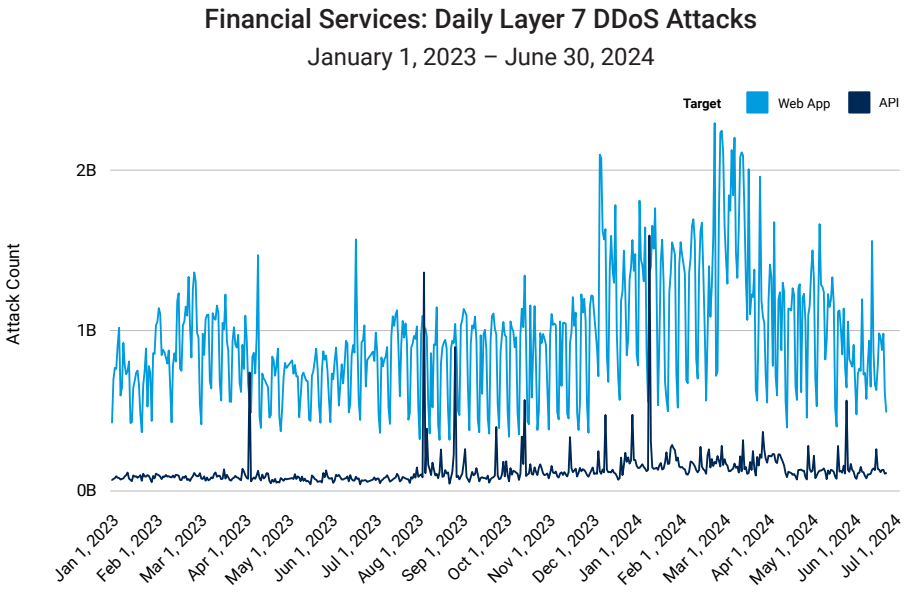
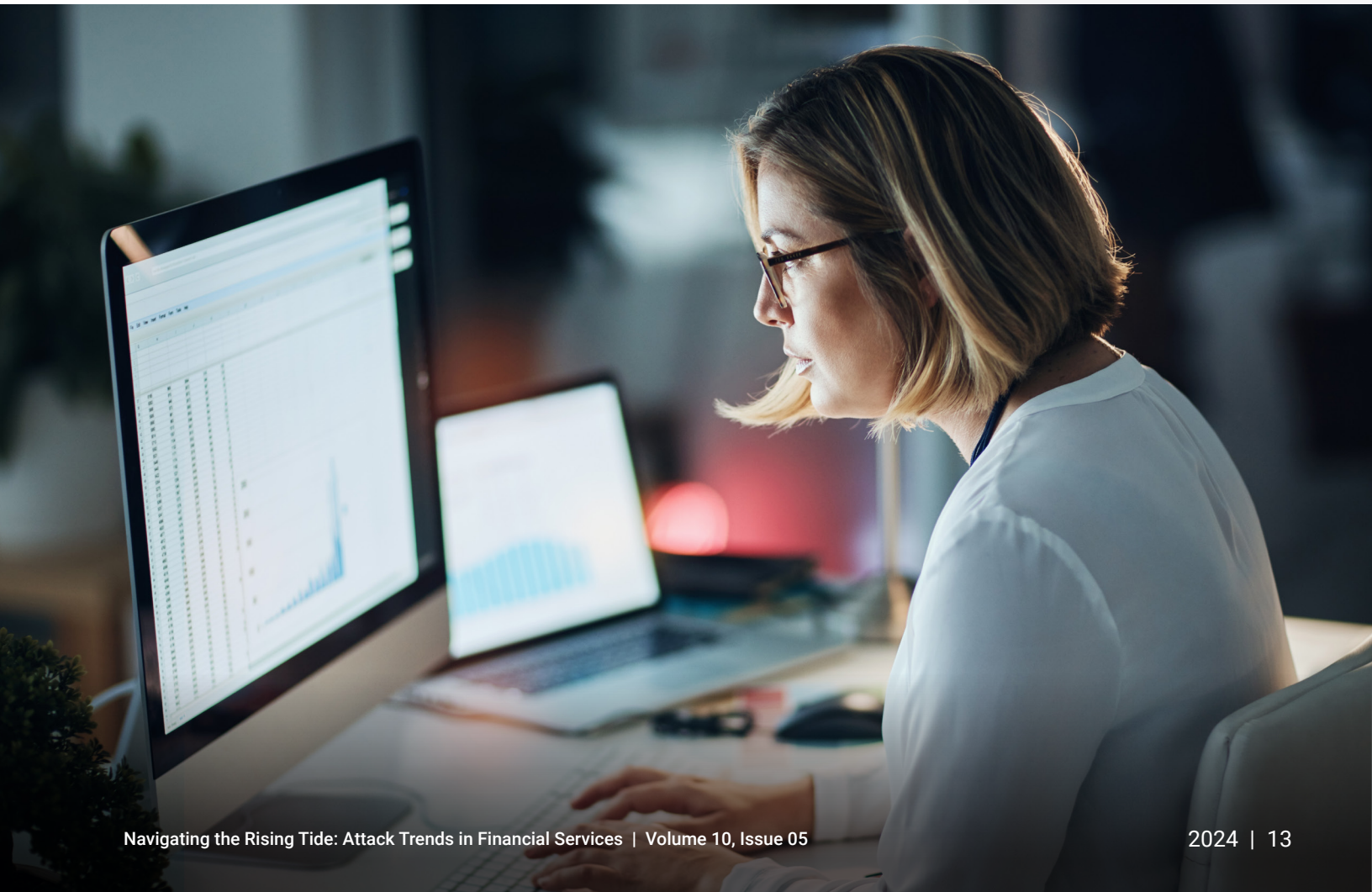


Fig. 6: Attack patterns significantly vary between targeted web applications and APIs in Layer 7 DDoS attacks on the financial services industry

These sharp increases occurred specifically in April 2023, August 2023, and January 2024. We attribute these spikes to factors similar to those that affect Layers 3 and 4 attacks, along with additional Layer 7–specific elements.

Attackers continually search for new vulnerabilities to exploit, and the discovery of such weaknesses can lead to sudden increases in attack frequency. For instance, the HTTP/2 Rapid Reset vulnerability (CVE-2023-44487), first identified in August 2023, enabled highly effective Layer 7 DDoS attacks. This vulnerability allowed attackers to exploit seemingly benign logic and to bundle multiple requests into a stream, which overwhelmed servers and applications. It resulted in the largest recorded Layer 7 DDoS attack to date.

Additionally, seasonally based DDoS attacks remain a popular tactic for cybercriminals targeting financial institutions, with notable spikes during the tax season and holiday periods. The significant increase in January 2024, following the busy holiday shopping season, suggests that attackers were preparing to strike during periods of heightened online transaction activity.



Ransomware and hacktivism in financial services

The financial services industry is often targeted by highly sophisticated threat actors such as ransomware groups. These groups employ a vast range of techniques to infiltrate financial institutions, steal sensitive information, and demand large ransoms. Although the operations mainly focus on financial motivations, they can also intersect with geopolitical contexts by targeting financial institutions that may have political ties. This was the case with the Russia-based ransomware group known as REvil (aka Sodinokibi). BlackCat (ALPHV) has also been involved in this way, as seen by its attack on a prominent bank.

One of the most active ransomware groups known for its attacks on large organizations, including financial institutions, continues to be LockBit. This is despite recent law enforcement actions against the group. Operation Cronos, which included a Europol and Eurojust collaboration to coordinate a first-of-its-kind international task force, has been overcome by new infrastructure established by LockBit. The ransomware group reemerged with new infrastructure and a dark web leak site just days after the law enforcement operation seized its servers in February 2024. And LockBit stated it would fight back by increasing attacks on government networks in response to Operation Cronos.

The ransomware group CL0P also continues to be active and has been especially known for exploiting vulnerabilities in file transfer software widely used in organizations including financial institutions. One notable example was with the zero-day vulnerability CVE-2023-34362 that affected MOVEit Transfer software and began with a SQL injection to infiltrate the MOVEit Transfer web application. At least 15 banks and credit unions confirmed data breaches as a result of the MOVEit vulnerability. CL0P has also gained initial access by other techniques, including phishing, and continues to run as a ransomware as a service (RaaS) model. Recently, the group has evolved its tactics to employ quadruple extortion on targets such as financial institutions. In addition to the techniques involved in triple extortion, quadruple extortion includes sending messages to harass business partners, employees, customers, high-level executives, and media to inform them that the organization has been hacked. And this tactic has led to a rise in average ransomware payments.

Other hacktivist threat actors who target financial institutions but are not classified as ransomware groups include Anonymous Sudan, KillNet, and NoName057(16). They are all notable for their activities related to the Russia-Ukraine war, and Anonymous Sudan has additionally claimed to have been involved with cyberattacks in response to the Israel-Hamas war. Last year, these groups, in addition to numerous other threat actor groups, leveraged the chaos brought on by the Russia-Ukraine war and turned their attention to critical banking infrastructure.

There are many other prolific threat actors that are not classified as ransomware groups but are known for targeting the financial services industry, such as the Lazarus Group, MoneyTaker, Carbanak/FIN7, Cobalt, and APT41.

Given the ongoing threats posed by these actors, it is critical for financial institutions to be aware of the current threat landscape and better understand attackers' motivations and techniques in order to develop more effective defense strategies. See our mitigation section later in this report for recommended safeguarding measures.

Recent outbreak of DDoS hacktivism in the Middle East among financial institutions

The financial services industry in the Middle East has recently experienced a surge in sophisticated and sustained DDoS attacks driven by geopolitical tensions. This trend is particularly prevalent in the Europe, Middle East, and Africa (EMEA) region and exemplifies the rising threat of politically motivated DDoS attacks on financial institutions.

A notable example of this trend occurred earlier this year when BlackMeta (also known as DarkMeta), a pro-Palestinian hacktivist group, launched a six-day Layer 7 DDoS attack against a financial institution in the United Arab Emirates (UAE). The attack was facilitated by InfraShutdown, a DDoS-for-hire service, highlighting the increasing accessibility of these attack tools. BlackMeta, which has been active since November 2023, has a history of targeting organizations in Israel, the UAE, and the United States.

The attack on the UAE financial institution was significant in both duration and intensity. It spanned approximately 100 hours, with web request waves lasting between 4 to 20 hours, and averaged 4.5 million requests per second. The assault placed the bank under attack 70% of the time, substantially impacting its services. BlackMeta's campaign against the bank was part of a broader effort to protest perceived injustices against Palestinians and Muslims, and demonstrated tactics similar to those employed by Anonymous Sudan.

Fortunately, the financial institution's mitigation efforts prevented more significant disruption, but this incident underscores the growing trend of politically motivated cyberattacks. It also highlights the increasing availability of DDoS-for-hire services, which lower the barrier for hacktivist groups to launch large-scale attacks. This development emphasizes the need for robust cybersecurity measures to protect against high-volume and persistent threats.

Another recent and suspected politically motivated DDoS attack occurred on July 15, 2024, and targeted a major financial services company in Israel. This massive attack, which originated from a globally distributed botnet, lasted nearly 24 hours and peaked at 798 Gbps. Akamai successfully mitigated this DDoS attack on Layers 3 and 4 that included various vectors, such as DNS reflection and UDP flood.

During this attack, Akamai blocked approximately 389 terabytes of malicious traffic in an intensive three-hour phase, with the total blocked traffic reaching approximately 419 terabytes for the entire duration. The occurrence of other outages faced by Israeli financial institutions on the same day suggests a coordinated assault, further highlighting the increasing threat posed by advanced DDoS attacks.

It's worth noting that this well-resourced aggressor had previously targeted the same financial services customer 27 times in the preceding 90 days. The customer has been repeatedly targeted with DDoS attacks since the fourth quarter of 2023, coinciding with the Israel-Hamas war. Akamai's internal DDoS threat intelligence group reports that institutions and businesses in Israel have experienced an unprecedented number of DDoS attacks in 2024. This sustained, aggressive campaign highlights the increasing scale and intensity of these threats, making it clear that attackers are becoming more persistent and resourceful.

Banking on familiarity: Brand abuse in financial services

As financial services adopt digital-first approaches to enhance customer experience, operational efficiency, innovation, overall revenue, and visibility, cyber adversaries are exploiting the inherent trust between organizations and their customers through brand impersonation schemes. Figure 7 shows examples of fraudulent sites that mimic known financial institutions. While phishing and brand impersonation are common methods, the alarming number of fraudulent websites and the rapid pace at which attackers can create new domains after their original sites are taken offline are particularly concerning. This rapid proliferation poses a growing, relentless threat to the financial services sector.

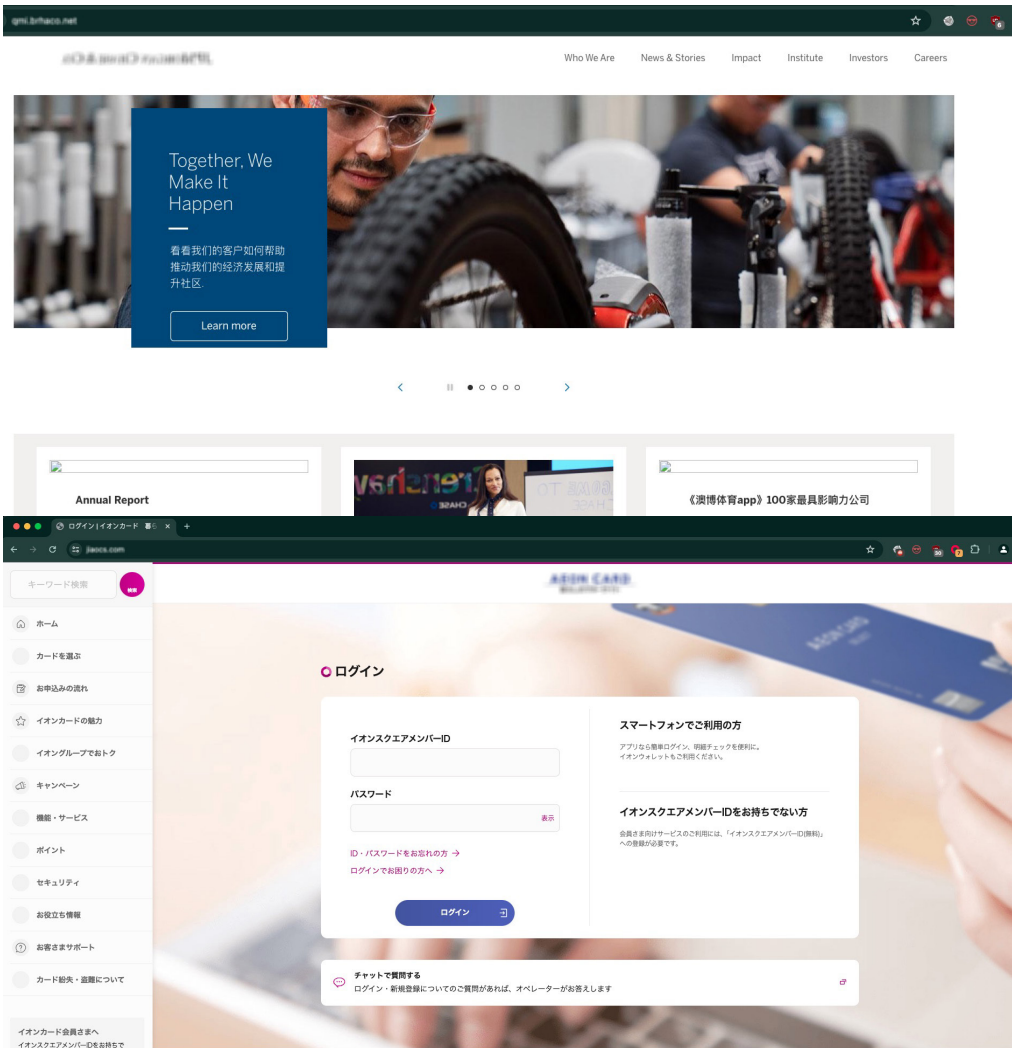


Fig. 7: Samples of fraudulent phishing sites that mimic known financial institutions

The landscape of brand abuse has been significantly altered by the emergence of phishing as a service platforms and toolkits. These resources have lowered the barrier to entry for cybercriminals, dramatically impacting the scale and magnitude of phishing attacks against financial services and their customers. To put this in perspective, the Anti-Phishing Working Group recorded nearly five million phishing attacks in 2023, designating it as the "the worst year for phishing on record."

Brand abuse can be an impetus for escalating risks like identity theft and account abuse. Attackers often peddle customer information on the dark web or use it in account takeover. From a security standpoint, early intervention in brand attacks is crucial. By thwarting the attack lifecycle early on, you can prevent attackers from harvesting credentials for nefarious purposes.

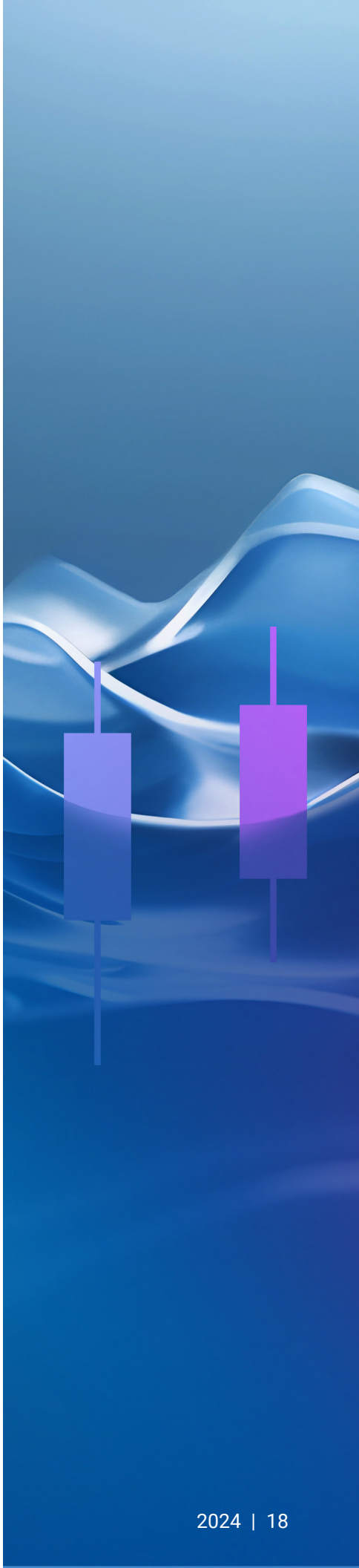
The ramifications of brand abuse extend beyond immediate security concerns. An organization can suffer substantial financial losses due to reputational damages, compliance and legal issues, and even sales lost to counterfeit products. In today's digital landscape, early detection of brand impersonation attacks is paramount in maintaining customer trust and business continuity.

Deception point: A closer look at impersonation attacks

Security teams face the daunting challenge of defending against brand abuse that can occur across various online platforms — this makes digital assets arduous to safeguard as both legitimate users and attackers can access them. Attackers often scrape the content of public-facing assets like online banking portals to create their own spoofed site and register a misspelled domain to trick unsuspecting users. Additionally, cyber adversaries launch campaigns involving phishing emails, social media posts, and other digital channels to lure potential victims to their malicious sites or fake apps.

For this report, we analyzed brand impersonation and phishing activities observed on active domains over the past 12 months to provide insights into the prevalence of brand impersonation across industries, with a particular focus on financial services. Akamai's comprehensive visibility and proprietary solution enable us to:

- Track traffic through phishing and brand impersonation sites, including marketplaces
- Identify the number of active malicious domains
- Assess the malicious domains' severity scores



Financial services was the most impersonated industry (36.25%) among all the suspicious sites monitored by Akamai (Figure 8). This finding particularly underscores the financial services industry's vulnerability to brand impersonation and abuse. Organizations in the commerce (26.41%) and business services (18.90%) industries followed in second and third places, respectively.

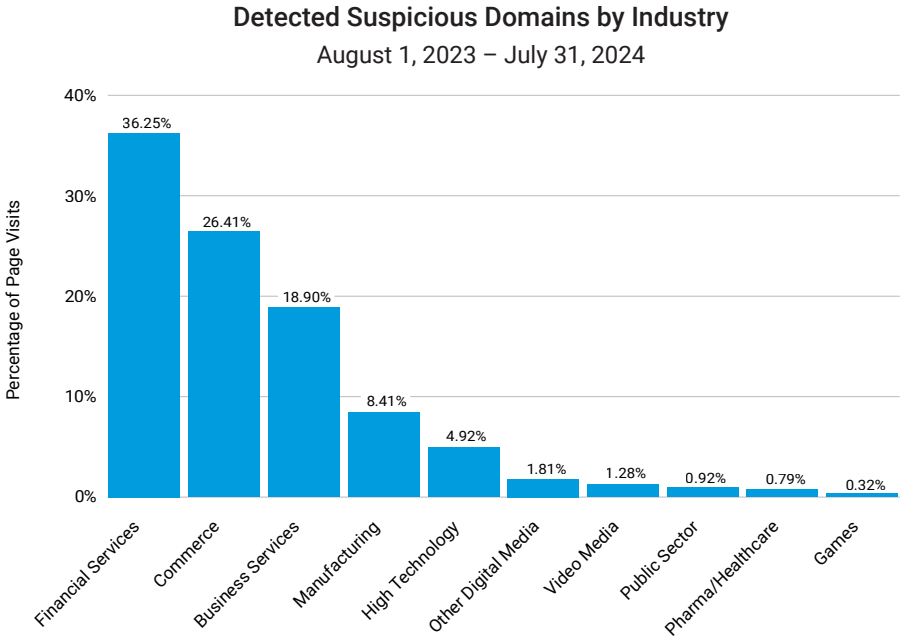


Fig. 8: Financial services accounted for 36.3% of phishing and/or brand impersonation domains

The financial services industry is a prime target for brand impersonation attacks due to the vast amounts of sensitive, highly valuable data it holds, such as banking credentials and personally identifiable information (PII). Information obtained from counterfeit banking sites allows cybercriminals to easily access and subsequently drain accounts. Similarly, other high-value financial details like credentials for e-wallets and cryptocurrency accounts (prices range from US$120 to US$400 on the dark web) can be obtained, enabling attackers to transfer what's in the account or sell the information in dark marketplaces. The high payoff of such schemes makes financial services prime targets of brand abuse and phishing attacks.

Similarly, commerce organizations have become lucrative targets of brand abuse since the rise of ecommerce and online shopping, which presents opportunities to siphon credentials and other personal information. Manufacturing companies and third-party vendors that provide services are equally vulnerable to brand abuse. Although digitalization enhances overall business growth, it has become a vulnerable soft spot for many organizations, leading to the proliferation of brand impersonation attacks and increased phishing attempts.

The high payoff of [brand impersonation] schemes makes financial services prime targets of brand abuse and phishing attacks.

Organizations must remain vigilant and implement security measures to protect both brands and customers in this evolving digital landscape. This includes continuous monitoring for brand misuse, rapid takedown procedures for fraudulent sites, and educating customers to recognize potential impersonation attempts. By prioritizing these efforts, organizations can better safeguard their reputation and their customers' trust in an increasingly complex threat environment.

Financial services in the crosshairs of brand abuse

To gain a holistic view of the impact of brand impersonation and phishing, we also analyzed the number of page visits to suspicious websites. Our findings reveal that sites masquerading as financial institutions received 30% of visits while those mimicking commerce companies follow with 20% of visits (Figure 9). These results consistently place financial services and commerce at the top spots, whether we measure by requests or domains. This consistency highlights their status as prime targets for brand abuse and impersonation — and for good reason.

Financial services encompass a wide range of targets from well-established banks to smaller institutions with fewer security resources, all of which are at high risk. Commerce, another industry under similar scrutiny by compliance forums (e.g., the Payment Card Industry Security Standards Council) as services, also faces significant risks because of the wealth of customer information they possess.

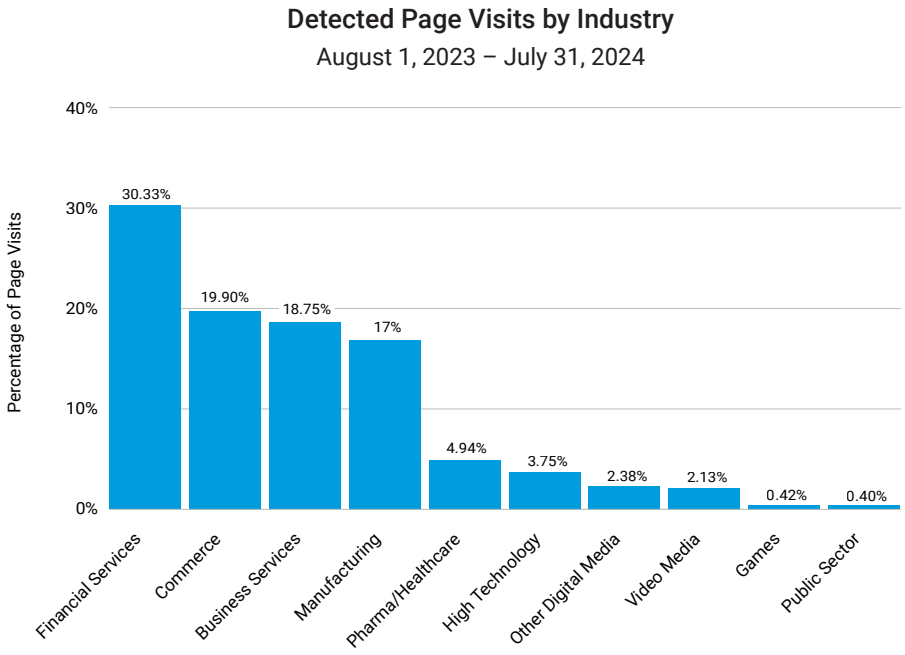


Fig. 9: More than 30% of page visits during the reporting period (August 2023–July 2024) went to suspicious sites that were masquerading as legitimate financial services sites

Interestingly, we observed some disparities between domain impersonation rankings and actual visit numbers across industries. For instance, high technology ranks in the top five for impersonated domains, but it falls to sixth place in terms of actual visits. Similarly, there are fewer domains posing as pharma/healthcare but the visits to these domains are higher.

Phishing for credentials

Brand abuse takes many forms, including lookalike sites that replicate the legitimate company's exact logo and design, fraudulent apps, and fake social media profiles mimicking official corporate accounts. To understand the extent of this issue, we analyzed counterfeit pages and classified them into types: brand impersonation, phishing, rogue apps, fake stores, paywall bypassers, and fake social profiles and stores. It's important to note that a single organization's domain can fall into multiple classifications based on the pages we monitor.

Our analysis revealed that phishing dominates the counterfeit domains that are targeting financial services institutions, accounting for a staggering 68% of all recorded instances (Figure 10). Brand impersonation follows in second place, representing 24% of all recorded domains. Among user-frequented sites, phishing and brand impersonation again rank first and second, respectively. Other forms of brand abuse, like fake social media profiles and stores, are less significant within financial institutions than in other industries. Despite fewer attacks targeting rogue apps, it's important to note that attackers are adopting increasingly creative methods to broaden their reach.

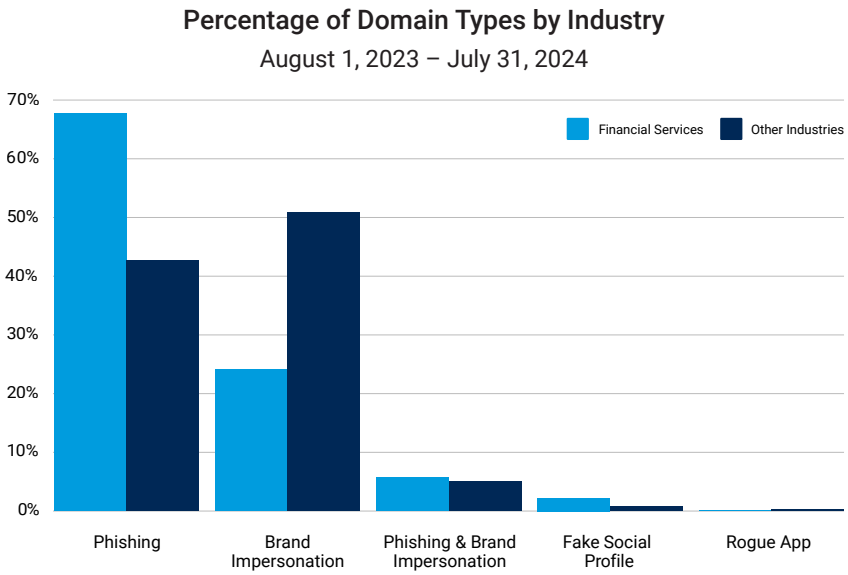


Fig. 10: The majority of the domains we recorded for financial services are phishing websites, even exceeding the total of all other industries combined

Financial institutions are seen as highly trusted entities, making them prime targets for fraudsters who exploit that trust.

Despite increased awareness of the risks posed by phishing, the human element remains a significant security gap. This gap is exacerbated by sophisticated techniques used by attackers (read The anatomy of brand abuse section for more details), making it difficult for the untrained eye to spot a bogus page. Financial institutions are seen as highly trusted entities, making them prime targets for fraudsters who exploit that trust. By impersonating these institutions, attackers deceive users into willingly handing over their credentials, leveraging the institution's reputation to make their scams more convincing and effective.

To safeguard both an organization and its customers, it is crucial to use security technologies with brand monitoring capabilities that can proactively monitor for any unauthorized use of the brand — whether it's a domain name, mobile app, or email communication. Once these are identified, the next step is to conduct takedowns to thwart traffic, which could potentially expose customers to the dangers (such as data theft) posed by brand abuse and phishing.

Case study: The increasing sophistication of credential stuffing attacks against financial institutions

A US fintech company endured relentless credential stuffing attacks throughout 2023 and 2024 that targeted one of its customer-facing applications. The magnitude of these attacks is staggering — during a 24-hour period, Akamai detected more than 3,000 alerts from different IP addresses that were attempting to infiltrate accounts using stolen credentials. We observed a single IP address trying at least 115 username and password combinations. In total, we recorded more than 100,000 alerts in July 2024.

Fraudulent financial services sites at critical risk level

The exclusive intelligence from our global edge, combined with additional data feeds from third-party threat intelligence, gives us a distinct advantage in detecting brand impersonations. We use this comprehensive system to meticulously examine and classify each domain based on its threat score.

We compute the threat score using three key factors:

1. **The confidence score** — our certainty that an event is a phishing attempt
2. **The severity level** — the degree of risk (critical, high, medium, or low) that is associated with an event
3. **The frequency factor** — the number of events/sessions associated with the site within a given time frame

Our scoring system balances the three key factors: confidence, severity, and frequency. We combine these scores to generate a comprehensive threat score for each suspicious domain, capped at 99, to ensure a holistic assessment of potential threats.

Our latest analysis reveals that the financial services sector holds an alarming median threat score of 85, highlighting the significant risks the industry continues to face (Figure 11). This score places financial institutions squarely in the sights of cybercriminals, who are relentlessly targeting their vast stores of sensitive data.

Threat Scores by Industry

Industry	Median Threat Score	Industry	Median Threat Score
Public Sector	**95**	Gaming	**65**
Financial Services	**85**	Manufacturing	**64**
Business Services	**85**	Other Digital Media	**62**
Pharma/Healthcare	**85**	Commerce	**61**
Video Media	**71**	High Technology	**60**

Fig. 11: Our computation of median threat scores shows financial services with an alarmingly high score

While the public sector recorded the highest median threat score, likely due to its wealth of sensitive information and limited security resources, financial services remain an equally attractive target, with attackers drawn by the potential for enormous financial gain. Sectors like business services and pharma/healthcare also score similarly, indicating that cybercriminals are diversifying their targets — but financial institutions remain a primary focus due to the critical nature of their data.

This high threat level demands immediate action to strengthen defenses and mitigate evolving threats before they lead to significant financial and reputational damage.

The anatomy of brand abuse

The magnitude of phishing and impersonation campaigns is worsened by the existence of phishing toolkits.

The success of fraud and brand abuse relies heavily on the brand's power as a social engineering lure. Attackers capitalize on the sense of familiarity and inherent trust that consumers have toward known brands, designing fake websites that closely mimic legitimate ones. In some cases, fraudsters even copy the exact code, making these illegitimate sites look almost identical to the real ones. With the rise of generative AI tools, which help fraudsters eliminate telltale spelling and grammar mistakes, it has become even more difficult for consumers to distinguish between authentic and fake sites.

The magnitude of phishing and impersonation campaigns is worsened by the existence of phishing toolkits. For as little as US$50, attackers can purchase phishing toolkits that enable them to create convincing phishing sites. The cybercriminal enterprise of developing, building, and selling phishing toolkits significantly lowers the barrier of entry for conducting phishing and impersonation campaigns. Kr3pto and 16Shop are two examples of prevalent phishing toolkits. Kr3pto targeted UK banks by bypassing two-factor authentication, while 16Shop focused on major brands like PayPal and Amazon, among others. In August 2023, an international law enforcement operation resulted in the arrest of 16Shop's creators. These cases highlight the evolving sophistication of phishing attacks and the coordinated efforts to combat cybercrime.

Underrated but effective: Combosquatting

Another important facet of brand abuse is the use of domain names that bear close resemblance to legitimate websites. Typically, attackers register their domains after purchasing or building their own phishing site. This is where tried and true techniques like cybersquatting and its many variants play a critical role. One common tactic is typosquatting, in which attackers register a domain with a slight misspelling of a company name (e.g., acamai[.]com), hoping the consumer will make a typo. Another method, combosquatting, involves adding extra keywords — such as "support," "login," or "help" — to the domain name. This tactic takes advantage of the microsites often found on legitimate company websites.

According to Akamai research, despite being an underreported tactic, comboquatting (the addition of a keyword) exceeds typosquatting (the addition, removal, or replacement of a character) in the number of active domains. Interestingly, "com" came up as one of the top keywords added in fraudulent sites.

There are other tactics observed in the wild that make it harder for consumers to identify an impersonation site and these can increase the success rate of these attacks.

Distribution mechanism

Counterfeit and phishing websites are delivered and peddled through various mechanisms — chief among them is email. These email messages look convincing via the use of a legitimate logo, and contain urgent messages, such as requests to update account information. However, brand abuse isn't limited to websites and emails — attackers also spread threats through social media, further expanding their reach and deception tactics.

Hidden (links) in plain sight

There are other tactics observed in the wild that make it harder for consumers to identify an impersonation site and these can increase the success rate of these attacks. For instance, the use of shortened URLs, QR codes, image hyperlinks, and text links in SMS obfuscate the malicious links. Unlike email with spam filters that provide protection against this abuse, text scams are likely not blocked and have a higher chance of getting read or opened.

Regional phishing and brand impersonation attacks in financial services

Brand abuse affects organizations and consumers worldwide, but some regions experience a higher vulnerability to fraud and abuse due to the concentration of traffic to brand impersonation and phishing sites. Our analysis reveals that the EMEA region experienced the highest volume of traffic to phishing and impersonation sites detected in the past 12 months, even surpassing those in North America (Figure 12). This ranking covers both financial services and other industries.

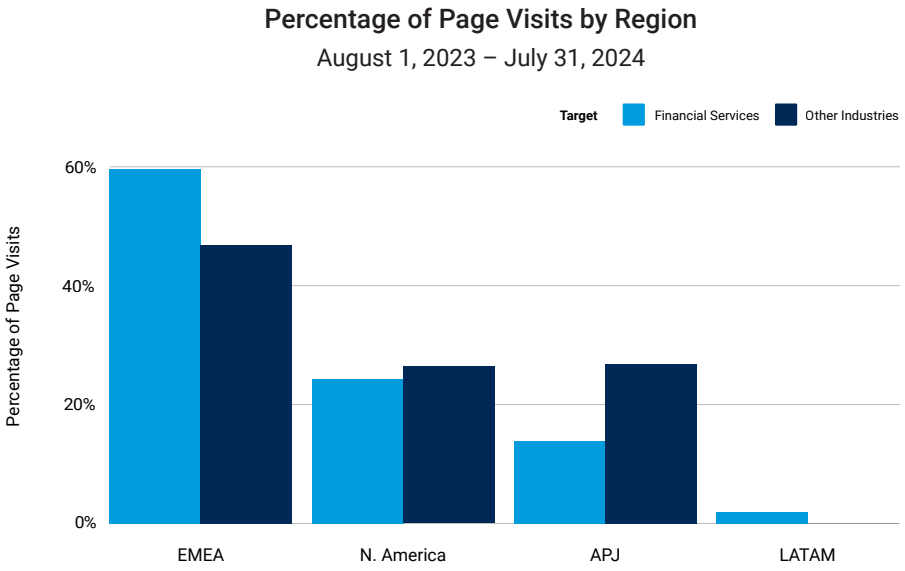
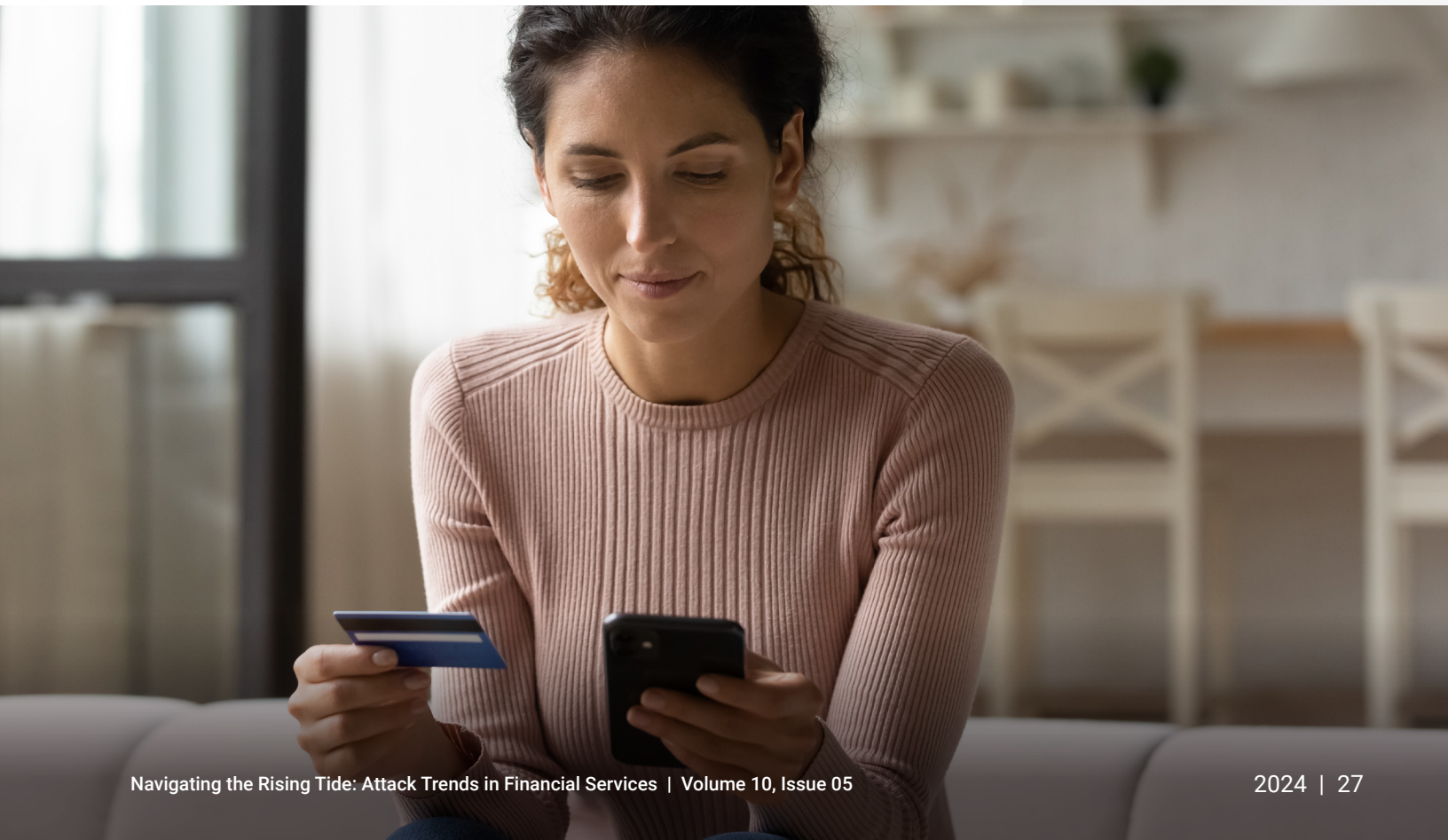


Fig. 12: EMEA surpassed North America as the region most impacted by phishing and brand abuse in financial services

Although the Latin America and the Asia-Pacific and Japan (APJ) regions recorded relatively smaller numbers of page visits, this does not indicate less targeting. Instead, these findings likely reflect the concentration of global brands with large customer bases in North America and EMEA. This creates a bigger pool of potential victims for adversaries. We can also attribute this finding to the emergence of phishing toolkits like V3B, which has specifically targeted EU banks since 2023.

Although EMEA outranks most regions in the number of suspicious domains and page visits, APJ has the highest median threat score: 97. Latin America, despite having the lowest number of site visits, receives a surprising median threat score of 94. This indicates that consumers in both Latin America and APJ are at a higher risk of having their banking information and other sensitive data stolen when visiting websites.

Several factors contribute to the rising dangers of brand abuse against financial services in APJ. First, most financial services institutions in APJ are highly digitized — almost every service offering can be done online without ever visiting a physical branch. The internet penetration and digital adoption rate in APJ is one of the highest globally, making this region an attractive target for cybercriminals to leverage. Second, this region is home to some of the most active social media countries in the world. And financial services institutions have stepped up customer engagements via these platforms to compete for market share and gain better customer loyalty. The widespread use of social media and messaging apps in the APJ region provides cybercriminals with additional vectors to deliver phishing and impersonation attacks, often by abusing the trust that people place in these platforms.



Evolving compliance: How global cybersecurity regulations are shaping financial institutions

When asked why he robbed banks, notorious bank robber Willie Sutton famously responded, "Because that's where the money is." Sutton's statement, of course, can easily be applied to cyberattacks against financial institutions today. The motivation of financial gain, however, only tells a part of the story. Financial institutions find themselves increasingly under fire from attackers who are motivated by political concerns, as well as by geopolitical strategic motives. These motivations, combined with the fact that "that's where the money is," create a perfect storm for financial institutions as they lead the pack as the most attacked industry sector.

This should not surprise us. The financial industry has always played a critical and central role in society and has been the subject of significant regulation. Although regulation of financial institutions in the past has focused on protecting consumers in their dealings with financial institutions, regulators are now seeking to apply critical infrastructure–style security and resiliency regulation to financial institutions and services companies. This newer trend includes requirements for not only the financial institution themselves, but also for their information and communication technology (ICT) suppliers.

There are numerous examples of cybersecurity and operational resilience regulations. In the European Union, the Digital Operational Resilience Act (DORA) mandates that financial entities and their suppliers have robust ICT risk management frameworks and conduct regular testing and incident reporting. In the United States, the Securities and Exchange Commission (SEC) has introduced cyber materiality regulations requiring public companies, including financial institutions, to disclose cyber incidents that could materially impact their operations. In Australia, the Australian Prudential Regulation Authority (APRA) has set standards demanding that entities maintain information security capabilities commensurate with the size and extent of threats to their information assets (regulation CPS 234). These examples illustrate the global trend toward enhancing the cybersecurity and operational resilience of financial sectors to protect against evolving risks and to ensure financial stability.

Given these regulations, it is incumbent upon financial institutions to perform due diligence when purchasing ICT and security services to make sure that the suppliers meet these developing stringent standards. They should choose suppliers that not only provide a resilient service, but also understand the relevant regulations, provide the necessary visibility to identify and mitigate evolving threats, and help to apply that intelligence to ongoing operations.

Visibility is critical because you cannot protect what you don't know you have (or what you are connecting to) and you cannot protect against a threat that you don't know is out there. Services like the Akamai Guardicore Platform provide not only protections against attacks, but also help customers understand data flows, identify anomalies, and properly segment network assets to mitigate threats. Similarly, its API security services are designed to identify API traffic to assist with shadow APIs, as well as recognize potential attacks via APIs.

Perhaps banks should add visibility to the traditional CIA triad (confidentiality, integrity, availability) to reflect this new trend — VCIA: visibility, confidentiality, integrity, and availability.

James Casey
Vice President, Chief Privacy Officer,
Akamai

Ramping up defenses with Zero Trust

Trust forms the foundation on which financial institutions build their reputation. However, when it comes to safeguarding complex environments and confidential data, trust can easily become a significant liability. Adversaries often take advantage of implicit trust in myriad ways, including:

- Phishing attacks to impersonate individuals within the organization
- Attacks that exploit security vulnerabilities in third-party suppliers to access high-value targets
- Insider threats that abuse access for nefarious purposes

The growing sophistication of attacks has rendered traditional perimeter-based security inadequate, as it deems all traffic from within as trustworthy. Given the high stakes in financial services, maintaining a resilient security posture is crucial. This is where the Zero Trust framework becomes imperative. This security approach operates on the principle that any connection request, user, or device is a potential hazard. It implements continuous verification and removes implicit trust, denying access to resources by default unless the requester is authenticated and authorized.

Zero Trust enhances compliance with evolving regulatory requirements for financial institutions by securing systems that handle regulated data, thereby allowing an organization to avoid penalties from failed audits. It provides additional controls for legacy systems, offering granular visibility to detect unauthorized users who are attempting to access critical applications.

The Zero Trust model restricts east-west traffic by limiting network access to critical systems and preventing lateral movement of threats like ransomware. This containment strategy protects essential data and assets by isolating infected systems. As the number of ransomware attacks on financial services has increased significantly, the importance of Zero Trust in safeguarding sensitive information cannot be overstated. With its granular visibility, Zero Trust helps you detect and neutralize threats within complex environments, which is crucial for preventing ransomware spread and protecting critical assets.

Another acute advantage of Zero Trust is its ability to secure data flows between applications, which is essential for the safe deployment of cloud-based applications. This not only facilitates modernization but also ensures the protection of confidential information in an ever-shifting threat landscape, allowing financial institutions to innovate without compromising security. Implementing a Zero Trust framework enhances security posture and future-proofs an institution against evolving threats.

Segmentation is good. Microsegmentation is better.

Segmentation is an architectural approach that divides a network into smaller segments for the purposes of enhancing performance and security. Microsegmentation is a security technique that enables you to logically divide a network into distinct security segments down to the individual workload level. Security controls and service delivery can then be defined for each unique segment.

Microsegmentation is also the backbone of Zero Trust. In a recent Akamai report, financial services cybersecurity leaders cited advancing Zero Trust as the most frequent driver of implementing a segmentation project. In fact, almost all the leaders who have segmented at all are deploying or have already deployed a Zero Trust security framework (99%), although less than half (47%) report their Zero Trust framework as being fully complete and defined, and therefore mature.

Microsegmentation works with existing systems and deploys faster than traditional methods like firewalls. This approach speeds up ransomware response by up to 13 hours and simplifies management across all IT environments. It also helps meet compliance needs through precise data control.

A real-world example shows the impact of modern microsegmentation: A project cut implementation time from 2 years to 6 weeks, used just one engineer, and reduced costs by 85%. This case illustrates how microsegmentation can save organizations time and money. IT directors should compare these outcomes with their current security costs and implementation time.

To fortify their cybersecurity posture, financial institutions must prioritize the implementation of advanced segmentation strategies. CISOs should spearhead efforts to align security measures with evolving industry standards, integrating microsegmentation as a cornerstone of a robust Zero Trust architecture. IT directors must establish a cadence of regular security audits and strategy updates to ensure that their defenses remain resilient against sophisticated cyberthreats.

This proactive approach not only helps mitigate current vulnerabilities but also positions organizations to effectively counter emerging cybersecurity challenges. By adopting these measures, financial institutions create a comprehensive security framework that addresses both immediate concerns and long-term risk management.

[Microsegmentation] not only helps mitigate current vulnerabilities but also positions organizations to effectively counter emerging cybersecurity challenges.

Mitigation

When it comes to protecting your financial institution from various cyberthreats, you need to implement a multifaceted approach. Let's explore the key mitigation strategies for phishing, brand impersonation, DDoS attacks, and ransomware.

Phishing and brand impersonation protection

To safeguard your institution against phishing and brand impersonation, consider using third-party brand protection services to detect and take down fraudulent content quickly. It's also important to educate your employees and customers. Conduct regular security awareness training for your staff on how to recognize phishing and impersonation attempts. Provide clear guidance on how to identify legitimate communications from your institution. Establish a rapid response plan for impersonation attempts, including a process for notifying partners and customers about identity scams.

Additionally, implement these safeguarding techniques:

- Register similar domain names to prevent typosquatting and use domain monitoring services to detect lookalike domains.
- Strengthen authentication protocols by using strong, unique passwords and password managers, and implement robust multi-factor authentication (MFA) for all accounts and systems.
- Deploy email authentication protocols like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) to prevent email spoofing. Use anti-phishing solutions and advanced email filtering to detect and block malicious emails.
- Secure your website and digital channels by obtaining SSL certificates, implementing HTTPS, and using anti-fraud tools to detect suspicious activities on your website and mobile apps.
- Safeguard communication channels by providing secure portals and implementing encrypted messaging for sensitive correspondence.

DDoS protection

Protecting your financial institution from DDoS attacks requires a multilayered defense strategy. Implement proactive strategies, such as using specialized DDoS detection, mitigation, and protection products; configuring rate limiting; and caching content on a CDN. Additionally, stay informed about security measures such as patch management, incident response plans, mitigation controls for DDoS-exposed IP addresses and critical subnets, access control policies, network segmentation, and firewalls. Implement proactive strategies such as configuring rate limiting; caching content on a CDN; and using specialized DDoS detection, mitigation, and protection products.

To safeguard DNS infrastructure, continuously monitor and analyze inbound DNS traffic and opt for a hybrid platform rather than a traditional DNS firewall. Understanding the tactics, techniques, and procedures used by attackers will help you better protect against DDoS attacks.

Ransomware protection

As mentioned earlier in this report, achieving Zero Trust with network segmentation, especially microsegmentation, is crucial to limiting the spread of ransomware throughout your financial institution. Implementing robust cybersecurity measures such as this will help to combat the advanced techniques ransomware attackers are employing. Also, be vigilant and use the MITRE ATT&CK framework to gain insights into prevalent tactics and techniques used by attackers and strengthen your playbooks accordingly to break the ransomware kill chain.

Continuously update your defenses and educate your staff to recognize and effectively respond to potential threats. Incorporate strong perimeter defenses, endpoint protection, email filtering, and regular patch management. Establish continuous monitoring of network traffic, system logs, and user behavior, and implement threat detection practices to proactively identify ransomware threats.

Implement regular and secure data backups, including air-gapped backups, to ensure that critical information can be restored quickly in the event of a ransomware attack. Implement MFA for all user accounts to add an extra layer of security.

By implementing these comprehensive mitigation strategies, you can significantly enhance your financial institution's ability to defend against various cyberthreats, ensure operational continuity, protect your reputation, and preserve customer trust.

Conclusion

As your financial institution embraces digital transformation to enhance customer experience, operational efficiency, and competitive positioning, the security challenges intensify, coupled with mounting pressure to navigate an evolving regulatory landscape. In this edition of the SOTI report, we've explored the persistent and emerging threats that are facing the financial services industry, underscoring the need for continuous evaluation and enhancement of security solutions. As threats become more sophisticated, it's critical to stay ahead by fortifying defenses and refining security strategies.

With DDoS attacks on financial institutions now surpassing those in the games industry — long considered the top target — this alarming trend underscores the rising risks. Factors like hacktivism and the geopolitical climate have made financial services more vulnerable than ever. In parallel, the scale and severity of traffic generated by brand impersonation and phishing sites that target financial institutions, along with the speed at which attackers can generate new domains after the initial sites are taken down, are notable. Tracking these activities can be resource-intensive for organizations, and security teams need solutions that include takedown services, threat intelligence, and the detection of brand impersonation and phishing across multiple digital channels.

Consumers and regulators often hold financial institutions accountable, even when they are not directly at fault, after falling victim to phishing and other scams. More important, phishing and brand impersonation frequently serve as precursors to more dangerous attacks, making it crucial to disrupt the attack cycle early. Taking decisive action can mean the difference between becoming tomorrow's headline because of a breach and safeguarding your institution's reputation and customer trust.

Given the relentless nature of attacks against financial institutions, safeguarding confidential information to prevent fraud and abuse remains a formidable challenge. Adopting a security framework like Zero Trust is essential to effectively defend against phishing attacks that target employees and prevent ransomware from spreading within networks to reach critical assets, all while ensuring compliance with existing and emerging global regulations.

This report provides actionable insights into the latest attack trends in the financial services industry, empowering you to fortify your defenses. By remaining vigilant and implementing the strategies outlined in this report, you can better protect your organization and your customers from the growing threat landscape.

Stay plugged into our latest research by checking out our security research hub.

Methodology

DDoS (Layer 7)

This data describes application-layer alerts on traffic seen through our web application firewall (WAF). The L7 DDoS alerts are triggered when we detect volumetric anomalies in the number of requests to a protected website, application, or API. These alerts can be triggered by both malicious and benign requests. Typically the requests themselves are benign, but the high volume of requests indicates malicious intent. 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, 2023, through June 30, 2024.

DDoS (Layers 3 and 4)

Akamai Prolexic Routed defends organizations against DDoS attacks by stopping the attacks and other unwanted or malicious traffic before they reach applications, data centers, and cloud and hybrid internet-facing infrastructure (public or private), including all ports and protocols. 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. These mitigated attacks are organized and grouped into attack events, and all the associated data is recorded by the SOCC to be analyzed.

This data in this report covered the 18-month period from January 1, 2023, to June 30, 2024, unless otherwise stated.

Brand impersonation attacks

Akamai Brand Protector is an anti-abuse solution designed to safeguard businesses and their customers against brand impersonation attacks, such as phishing, counterfeit websites, fake social accounts, and rogue applications. It uses Akamai's global edge network, analyzing more than 900 TB of data daily, to detect threats before they impact customers. This intelligence is enhanced with third-party feeds from partners to offer a broad view of potential threats across various online platforms.

Various characteristics of each detected suspicious domain are analyzed, and their determined levels of risk contribute to the domain's calculated threat score. These suspicious domains are monitored, the associated data is tracked, and the impacted customers are alerted to these malicious campaigns that attempt to exploit brand identity.

The data in this report covered suspicious domains detected in the 12-month period from August 1, 2023, to July 31, 2024.

Credits

Research director

Mitch Mayne

Editorial and writing

James Casey
Lance Rhodes
Badette Tribbey

Review and subject matter contribution

Cheryl Chiodi
Ziv Eli
Reuben Koh
Gal Meiri
Richard Meeus
Steve Winterfeld

Data analysis

Chelsea Tuttle

Promotional materials

Barney Beal

Marketing and publishing

Georgina Morales
Emily Spinks

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 that 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 for threats targeting the financial services industry, visit our **financial services page**.

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn. Published 09/24.