Financial Services — Hostile Takeover Attempts

Table of Contents

Letter From the Editor

Martin McKeay
Editorial Director

Welcome to Volume 6 of the State of the Internet/ Security report. It's a new year. We've made our resolutions. In too many cases, we've already broken those resolutions and gone back to doing the same things we were doing before.

The staff who creates the SOTI really only has one resolution, and it's the same one we've had for years: evolve. Do better than we've done before, learn from our mistakes, find new challenges to explore and overcome. What we did last year was our best effort for that time, but we strive to continue to produce a better report every time we go to publication.

We don't always succeed. Even when we don't, we learn from our mistakes and we try to make sure we don't repeat the same mistakes again. In many ways, this is what any good business, any good security team, should be striving for – to be better today than we were yesterday.

The SOTI is not the report it was three years ago, two years ago, or even at the beginning of 2019. Akamai isn't the same company it was at the beginning of 2019, and your business probably isn't either. Hopefully your security practice has evolved in the past year, as well, because we're certain that criminals and other advanced agents of disruption have evolved to better overcome your defenses.

We draw the data we use to create the analysis in this report from a wide variety of products and sensors across our organization. As we introduce new products and refine the capabilities of existing ones, we gain new insights into the attacks and attackers we are defending against. Because if we don't grow, evolve, and innovate, we become irrelevant as a security company.

We looked at credential abuse several times in the past year, and it's still an important topic to cover. In this report, we're introducing two new data sets from our Identity Cloud and Enterprise Application Access products. Both provide insight into different aspects of user accounts and remote network access, and both fit broadly into the category of Zero Trust.

While New Year's resolutions are a staple for many people, our commitment to growth and change is a more integral part of what this report is. We might look at the same types of data several times over the course of a year, but we'll always try to bring something new to the report – something that will give you more intelligence about what we see happening on the Internet.

Change is the only constant we adhere to. We hope our changing approach to each report is helpful to our readers.

Overview / TL;DR

- Between November 2017 and October 2019, more than **40%** of the unique DDoS targets were in the financial services industry
- From May to October 2019, credential stuffing attacks targeting the financial services industry have targeted APIs, often accounting for **75%** or more of the total login attacks against financial services
- Traditional logins (username and password) still account for the majority **(74%)** of access methods to applications and services

Do No Harm

Jennifer Leggio
CMO, Claroty

Another year, another security conference season, and another round of security vendors doing everything they can to capture buyers' attention. This is why marketing exists and why marketing teams spend so much time, effort, and money to support conferences. Where some teams fail is in the "how" of grabbing your attention.

As a marketer, I know firsthand that vendors must be creative to stand out in the crowd. That's what we do. It's our job to support sales organizations, help them develop business relationships, and, well, make sales. But marketing organizations in the security industry have one additional responsibility: ensure that our campaigns cause no harm in their attempt to support the business.

More so than many industries, the security industry is sensitive to any marketing effort that is misleading, less than truthful, or simply wrong. This is counter to the pressure marketing teams can face from senior leadership to get buyers' attention at any cost. This is not unique to marketing; I see questionable behaviors on social media from non-marketing executives, technical leaders, engineers, analysts, and even researchers all too frequently. While marketing teams generally have a bigger megaphone (and bigger budget), everyone needs to consider the harm such attention-grabbing efforts can do.

In my view, there's one trap I consider to be the most dangerous: *FUD*.

Fear, Uncertainty, and Doubt (aka FUD)

Fear, uncertainty, and doubt sell products, or at least grab attention. Security professionals often talk about reducing or removing FUD from the industry, but many fundamental marketing tactics rely on exactly that approach. It's hard to resist the Dark Side, especially because it works so well.

How many headlines read, "In today's ever-changing cybersecurity landscape, defenders *must* do X!"? This automatically gets translated in my head to, "People, the security industry is *ever-changing!* It's impossible to keep up, so instead it's imperative you read our press release!" The message implies an authority that no one else can match.

This touches on a hot-button area I've heard from many of my chief information security officer (CISO) friends: Don't assume you know what *my* problems are or how I should address them. Each organization is different and each CISO has different needs. Marketers who use the FUD approach, unfortunately, end up diminishing the weight of what might actually be an important message and something a CISO might be interested in. Rather than encouraging a CISO to read the message, FUD creates the perception a company needs scare tactics to sell, which harms the organization's reputation.

Here are some examples of other egregious FUD headlines:

- "Your organization is likely compromised, you just don't know it yet!"
- "Don't let what happened to [Company] happen to you!"
- "We know something about your organization you don't – let us tell you about it on a call!"
- Anything with an image of someone in a dark hoodie looming over a keyboard.

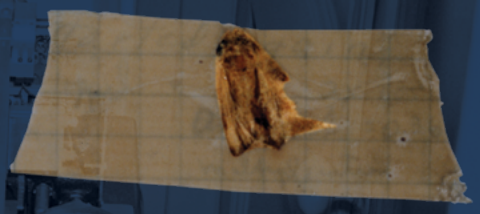
Some might defend the use of FUD, primarily because "it works." When met with that defense, I always ask for a definition of "works." Perhaps these headlines result in a lead, or even a sale, but what is the long-term impact on customer loyalty and reputation? As with any relationship, trust is the foundation, and scare tactics are corrosive to trust. In my opinion, the short-term boost of FUD-based campaigns and content is not worth the cost to our relationships with customers.

As we move into 2020, I challenge everyone in our industry and our community to consider their approach to marketing security. Is the message you send, the research your organization does, enhancing the security field or detracting from it? True, there can be a thin line between research and scare tactics, but it's generally easy to tell the difference. The best message you can send is one that educates the reader and reduces the risk in our world, rather than one that's sensational.

Jennifer Leggio is the Chief Marketing Officer for Claroty, the global leader in industrial cybersecurity. She has been a security marketer for nearly 20 years, leading teams, programs, and strategies for startups and public companies alike. A fierce advocate for truth in security marketing, ethics in market leadership, and protection of security research, she has spoken on these topics at DEF CON, Hack in the Box, RSA Conference, and myriad podcasts. She can be found on Twitter at @mediaphyter

The Moth in the Machine and the Pioneer Who Found It

On September 9, 1947, Admiral Grace Hopper is said to have pulled a two-inch moth from a shorted-out relay in the Harvard Mark II computer. In the log book, she wrote, "First actual case of bug being found."



NH 96566-KN courtesy of the Naval History & Heritage Command

01100010 01101111 01110100 01110100 01101111 01101101 00100000 01101111 01100110 00100000 01110000 01100001 01100111 01100101

Admiral Grace Hopper (1906 - 1992)

She credits her team for the discovery of the moth, but no matter who found it – this wouldn't be her last first.

In 1952, Admiral Hopper assigned call numbers to the machine-language subroutines that were recorded on snippets of magnetic tape. This was the world's first compiler.

In 1953, she replaced the call numbers with words and made the first English-like data processing language, FLOW-MATIC. This led to her leading role in the development of COBOL.

And by 1967, when one organization's COBOL wouldn't run on another's computer, she created information technology's first industry standard.

Admiral Hopper's work was so groundbreaking, in fact, she was named a distinguished *fellow* of the British Computer Society and was the Data Processing Management Association's first Computer Science *Man* of the Year.

There was no such idiom as "glass ceiling" in Admiral Hopper's day. And if there was, she would have ignored it.

She got a PhD in Mathematics from Yale in 1934, and went on to teach at Vassar, Penn, George Washington University, and the U.S. Naval Reserve.

She pushed back against a rejected application to enlist in the Navy. By the time she retired after 40 years of service (three tours of duty), she was a Rear Admiral.

Meanwhile, a Jolly Roger flew at her desk. A clock on her wall ran counterclockwise. And she's famously quoted in the U.S. Navy's *CHIPS* newsletter, "It's easier to ask forgiveness than it is to get permission."

It's no wonder that students, colleagues, superiors, and direct reports all called her "Amazing Grace."

Today, thanks to Admiral Hopper, we have industry standards that make possible everything from digital photos to 5G. We can say, "Hey, Google" instead of INHEX, HEXERTS, and CO1E 8D F0.

And the next time you debug a system, just remember, Admiral Hopper was there first.

> *"Humans are allergic to change. They love to say, 'We've always done it that way.' I try to fight that."*
>
> *– Admiral Hopper*

68 74 74 70 73 3A 2F 2F 70 61 73 74 65 62 69 6E 2E 63 6F 6D 2F 52 37 48 75 57 5A 32 39

Akamai Research

Introduction

In Volume 5, Issue 4 of the State of the Internet / Security report, we focused on the methodologies and tools that criminals use to conduct credential stuffing attacks against the financial services industry. At that time, we noted that attacks against financial services institutions were growing in both quantity and sophistication.

This still holds true today. Shortly after that report was published, Akamai witnessed a record-breaking attack against a well-known financial firm. This attack, which included 55,141,782 malicious login attempts, happened on August 7, 2019. These login attempts, commonly known as credential stuffing attacks, represented the largest spike in targeted credential abuse against financial services we've seen since we started tracking these attacks. While the attackers ultimately failed, the volume and intensity of their effort proves that financial organizations are still a prime target for criminals.

In this report, we examine application programming interfaces, or APIs, that criminals target with credential stuffing attacks.

When it comes to credential stuffing, the APIs we're examining use REST and SOAP to access resources. This includes account summary pages with personal information, account records, and balances, as well as other tools or services within the platform.

While they're not directly comparable, both REST and SOAP are essentially methods of communication between applications. REST can be implemented in different ways, depending on the project. SOAP is a standard for data exchange.

APIs are everywhere. Employees and customers in the financial services sector are exposed to them constantly, especially REST, since it is frequently used in website and mobile application development. However, SOAP is another popular option in the enterprise space – particularly in banking. SOAP offers a higher degree of flexibility when dealing with client and server relationships that require precision and accuracy when it comes to database transactions.

As far as criminals are concerned, REST and SOAP architectures are just targets. They're things to be bypassed in order to obtain sensitive data or financial assets.

The inconsistency in development methods using APIs has led to many of the problems we've seen over the past few years. For example, some APIs allow as many password guesses as needed to successfully authenticate, while others throttle attempts. Criminals take advantage of the lack of limitation and process tens of thousands of credentials in minutes. For APIs that are throttled, criminals use threading, taking a low and slow approach to achieve their goals.

Another API development practice that leads to problems is related to error checking. Criminals leverage APIs to validate their lists and confirm that a username actually exists on a service. Depending on how the application or platform was developed, the error responses can be used to sort and validate lists, which enables a higher degree of targeting.

Finally, API usage and widespread adoption have enabled criminals to automate their attacks. This is why the volume of credential stuffing incidents has continued to grow year over year, and why such attacks remain a steady and constant risk across all market segments.

Staging Attacks Against Financial Services

Criminals need three things to start staging credential stuffing campaigns. First, they'll need credential lists (also known as combo lists), which contain usernames and passwords. From there, criminals need a known target with accessible authentication mechanisms. In many cases, these authentication mechanisms are API endpoints. Finally, they need a tool to leverage those lists, as well as configuration files, to properly communicate with the victim's authentication mechanism.

API Attacks

From December 2017 through November 2019, Akamai observed 85,422,079,109 credential abuse attacks across our customer base. Nearly 20%, or 16,557,875,875, were against hostnames that were clearly identified as API endpoints. Of these, 473,518,955 attacked organizations in the financial services industry. Some organizations use less obvious paths and names for their APIs, but for our purposes, there were clearly identifiable endpoints we deemed sufficient.

Figure 1 shows daily malicious logins, with the obvious API endpoints highlighted. The top graph shows all verticals, while the bottom graph is focused solely on financial services. The rate of malicious logins against APIs in the financial services sector increased significantly starting in May of 2019. Also highlighted are the single largest spikes in our data for non-API and API credential abuse, both overall and for the financial services industry.

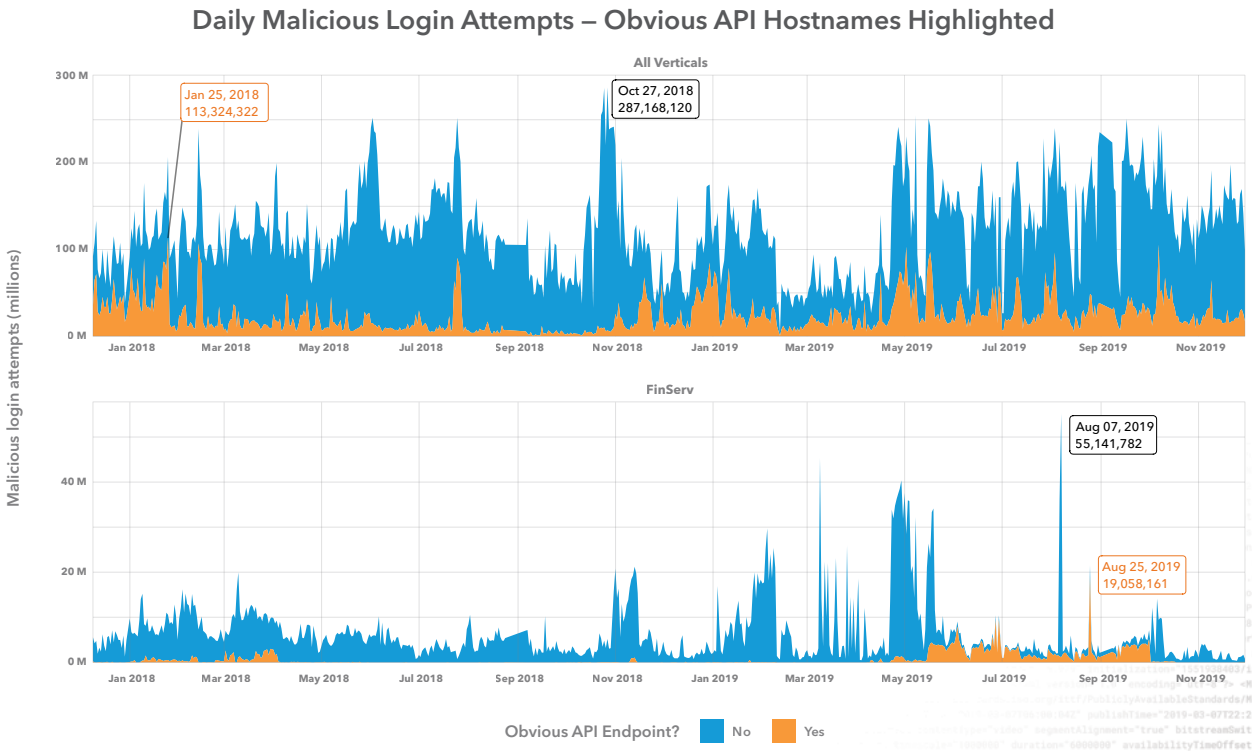


Fig. 1 – The rate of malicious logins against APIs in the financial services sector increased significantly in May of 2019

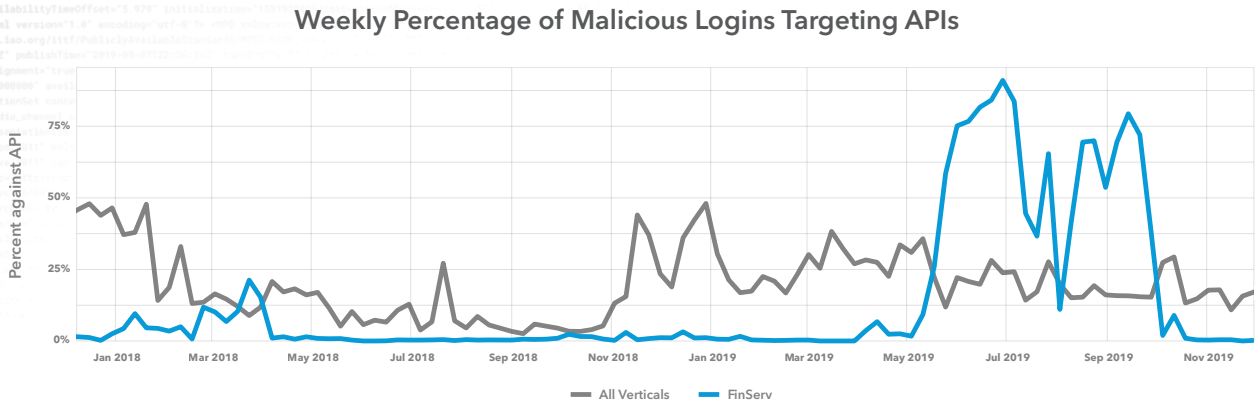


Fig. 2 – In May of 2019, malicious logins against API endpoints rose sharply in financial services targets as a percentage of the overall attacks

Figure 2 displays API credential stuffing attacks as a portion of all such attacks and highlights how attacks against APIs have grown in recent months, at times accounting for 75% of attacks. This indicates a drastic shift away from general login pages to API logins by criminals.

Looking at an additional six months of data in this report allowed us to make several interesting observations about credential stuffing attacks against the financial services industry. Figure 3 shows the weekly credential abuse attempts for the same weeks in 2018 vs. 2019 and the change in attempts each month.

The breakaway month is May, where the number of malicious logins against financial services almost tripled from 2018 to 2019. The cause of this growth can likely be attributed to the flood of credential lists on the criminal market, and the fact that data from the financial services industry is worth a considerable amount to criminals, who use it for outright financial theft, money laundering, and identity fraud. This also aligns with the shift in credential abuse to API pages, signaling significant targeting of those API logins.

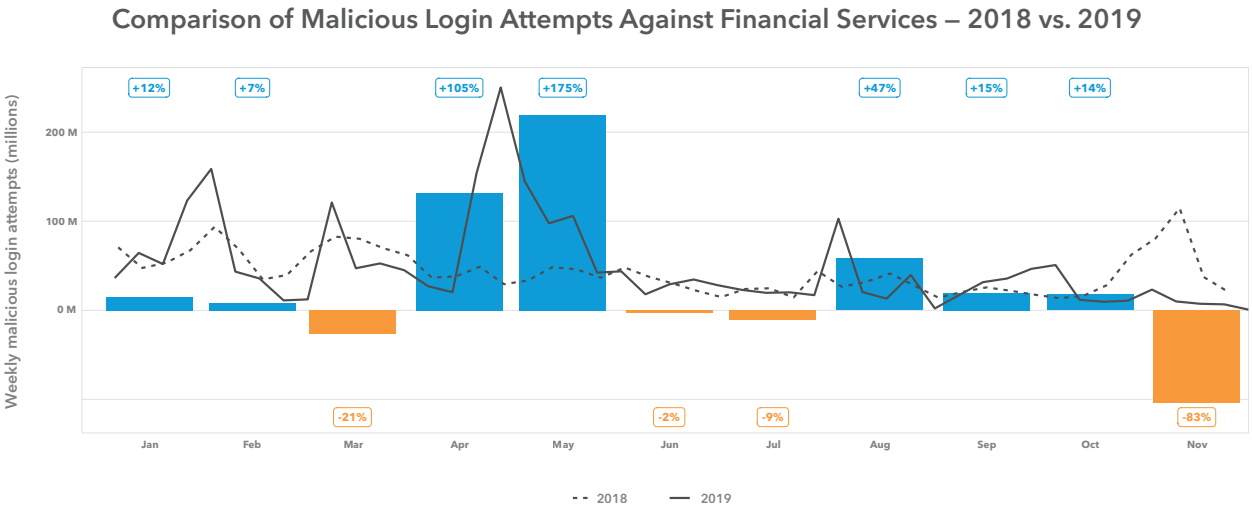


Fig. 3 – May showed the largest spike of credential stuffing attacks in financial services, with almost triple the number logins from 2018 to 2019

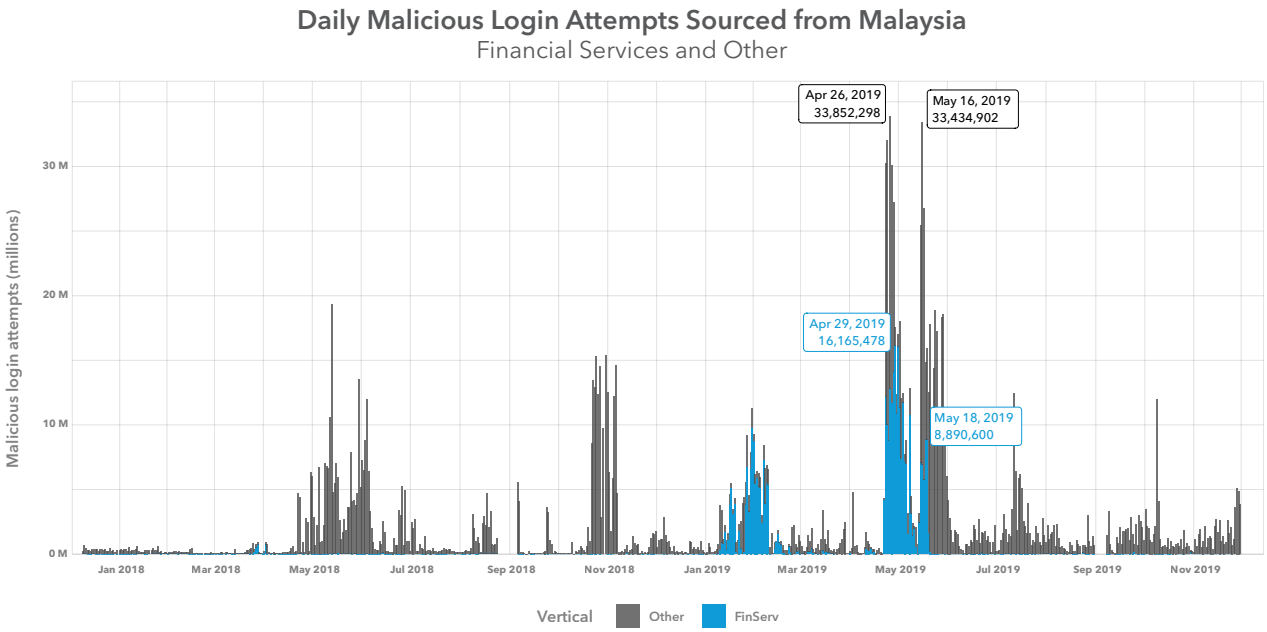


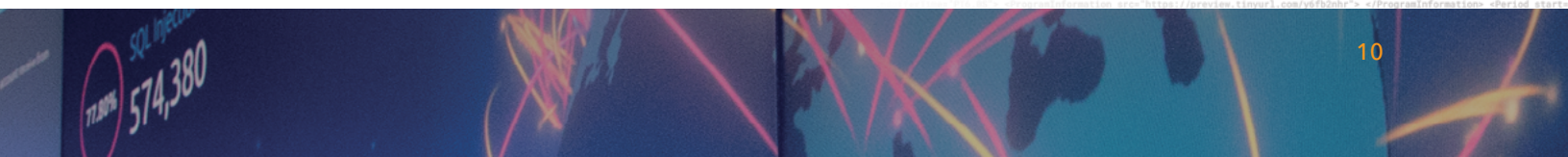
Fig. 4 – The bulk of the Malaysian-sourced malicious logins against financial services happened in Q1 and Q2, 2019

Criminals are still buying, selling, and trading bank cards, financial credentials, compromised gift card balances, and online banking accounts at a rapid clip, because demand for such things remains high. Some compromised assets are being exchanged for cash, while others are being exchanged for more product in a direct swap between criminals, such as someone who trades valid banking accounts with balances for credit card accounts in Europe.

Another credential stuffing data point concerns source countries. In our last report on financial services, Malaysia was the third-largest source of attacks, behind China and the United States. At the time, Malaysia accounted for 227,443,763 (23.15%) of the malicious logins against financial services. In our most recent data set, Malaysia accounts for 351,107,813 of the malicious logins against financial services, or 21.49% (a drop of 1.66%, despite the 100-million-plus increase in total malicious login count).

Virtually all of the Malaysian-sourced malicious logins against financial services took place during the first six months of 2019. A total of 99.6% of the attempts during that time frame – close to 351 million – targeted a well-known payment service online.

The buying and selling of compromised bank cards and financial credentials is still common among criminals today.



Web Attacks

Credential stuffing is just one attack type that the financial service industry faces. Criminals aren't choosy when it comes to methodologies, and for the most part, they'll try different attack types until they're successful. This is why a solid, multilayered approach to defense is key to stopping them.

Within the same 24-month period used to examine credential abuse traffic, Akamai observed 662,556,776 web application attacks against the financial services sector and 7,957,307,672 across all verticals. The peak attack dates in 2018 and 2019 are highlighted in Figure 5.

Figure 6 shows a breakdown of web attack types during the 24-month observation period. Overall, SQL Injection (SQLi) accounted for more than 72% of all attacks when looking at all verticals during this period. That rate is halved to 36% when looking at financial services attacks alone. The top attack type against the financial services sector was Local File Inclusion (LFI), with 47% of observed traffic.

LFI attacks exploit various scripts running on servers, usually PHP, but LFI flaws have also been known to exist in ASP, JSP, and other web technologies. The consequence of these attacks is usually the disclosure of sensitive information. However, LFI attacks can also be leveraged for client-side command execution (such as a vulnerable JavaScript file), which could lead to Cross-Site Scripting (XSS) and denial-of-service (DoS) attacks.

Taking all of this into account, criminals conducting the LFI attacks are looking to expose data that could enable a stronger foothold on the server, such as exposing a configuration file with database credentials. If the database user has write permissions, the criminal could use the data exposed via LFI to remotely connect to the database and compromise the server itself by command execution.

Between 2018 and 2019, the most common attack type against the financial sector was Local File Inclusion (LFI).

XSS was the third-most common type of attack against financial services, with a recorded 50.7 million attacks, or 7.7% of the observed attack traffic. XSS accounted for 3.3% of the attacks in all verticals. After that, PHP Injection (PHPi) came in at just shy of 16 million attempts against financial services. Finally, Command Injection (CMDi), Remote File Inclusion (RFI), OGNL Injection, and malicious file uploads rounded out the final 5.7% of recorded attacks against financial services.

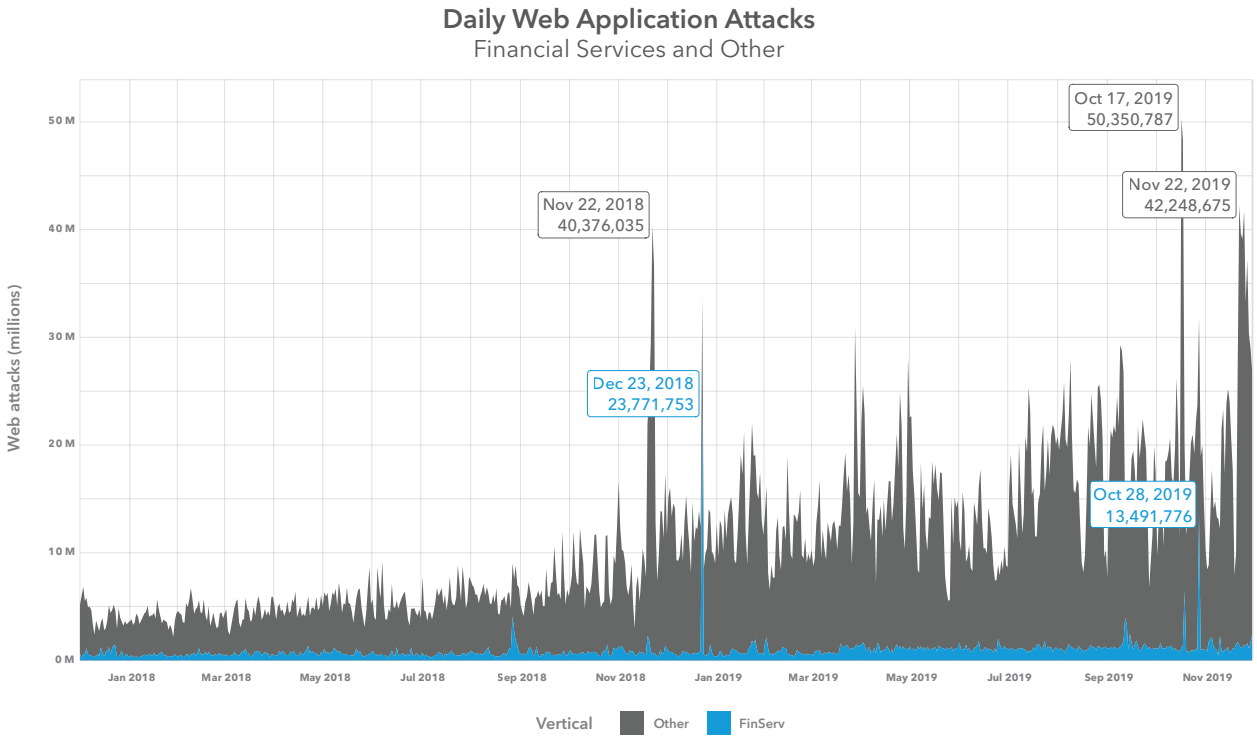


Fig. 5 – While the single-day peaks in attacks are concerning for individual organizations, the continued growth in web attacks affects all organizations

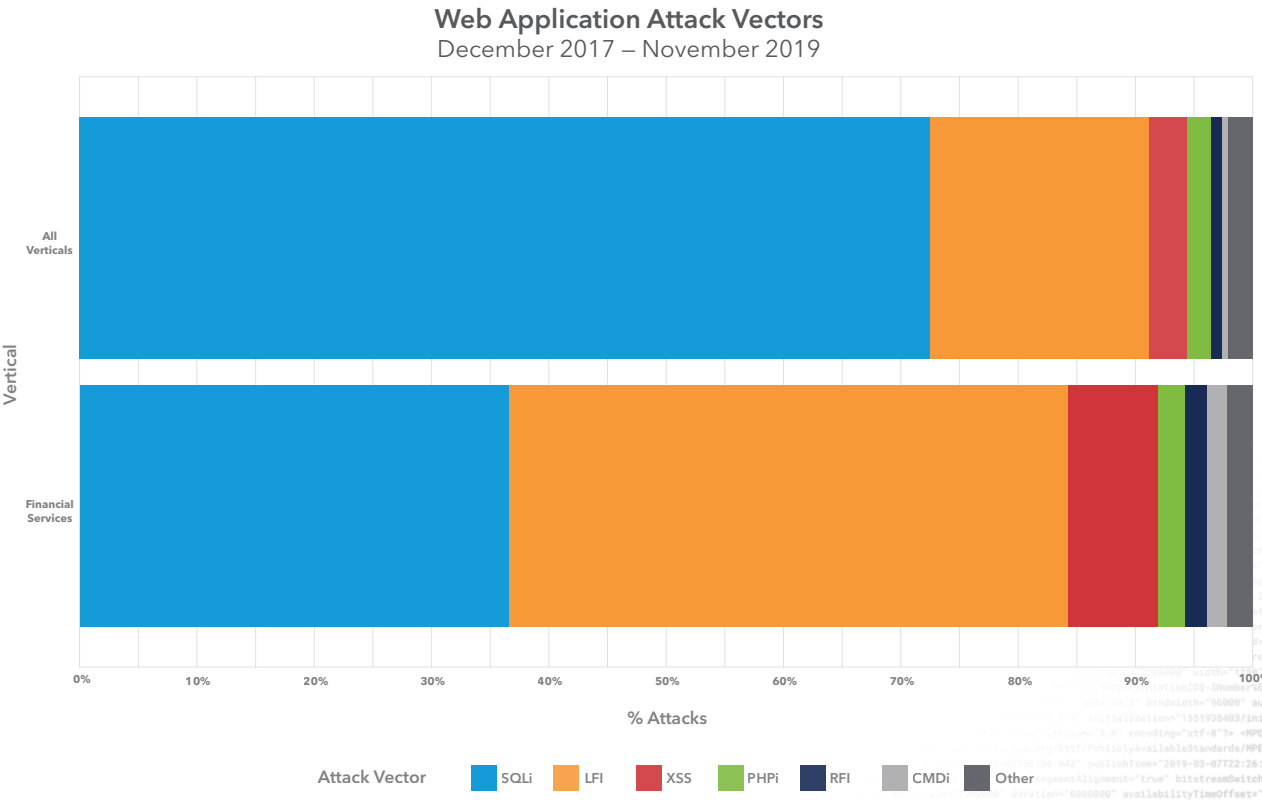
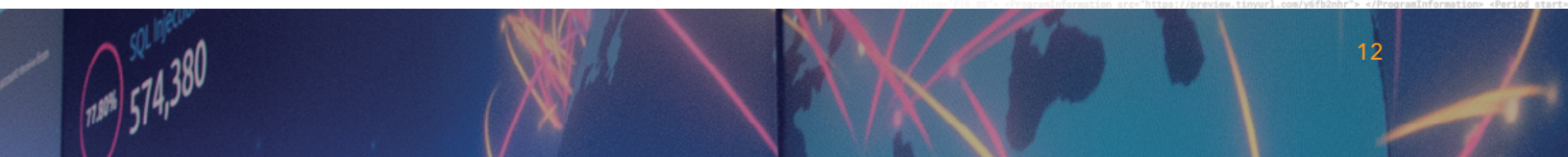


Fig. 6 – LFI was the top financial services attack type, but SQLi continues to dominate when looking at all verticals



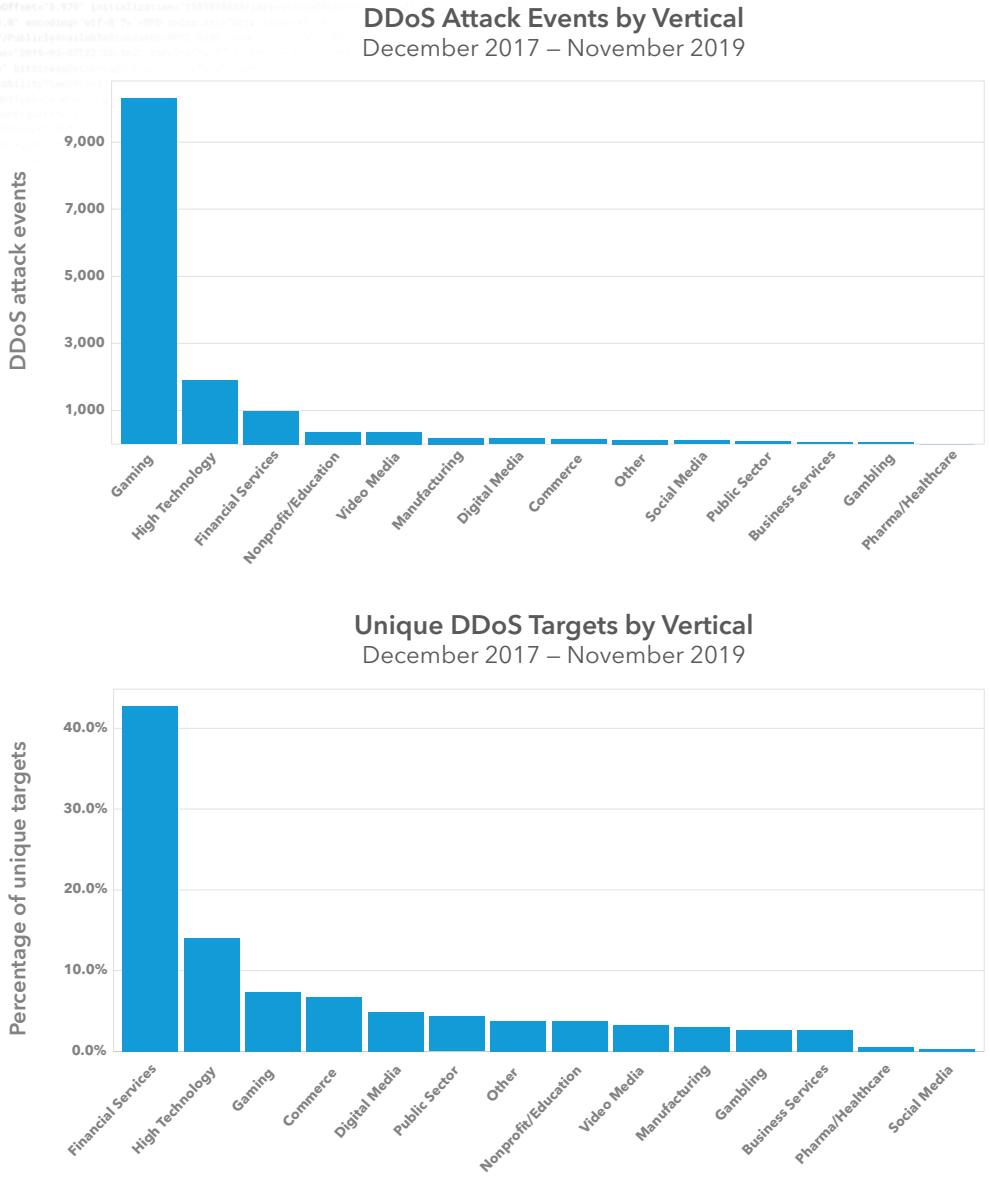


Fig. 7 – More than 40% of the organizations Akamai defended from attack were in the financial services industry

DDoS Attacks

The financial services industry was the third-most targeted industry in DDoS attacks during the reporting period, with gaming and high tech being the most common targets. However, when we look at the number of organizations attacked, financial services ranks first. Figure 7 shows that more than 40% of all organizations targeted by DDoS attacks fell within the financial services industry.

In other words, attacks against gaming and high tech targets were focused on a few organizations, while DDoS attacks against the financial services industry were spread across a larger number of organizations. DDoS attacks are not only an effective means of getting the victim's attention, but they can also obfuscate other types of attacks, including SQLi and LFI.

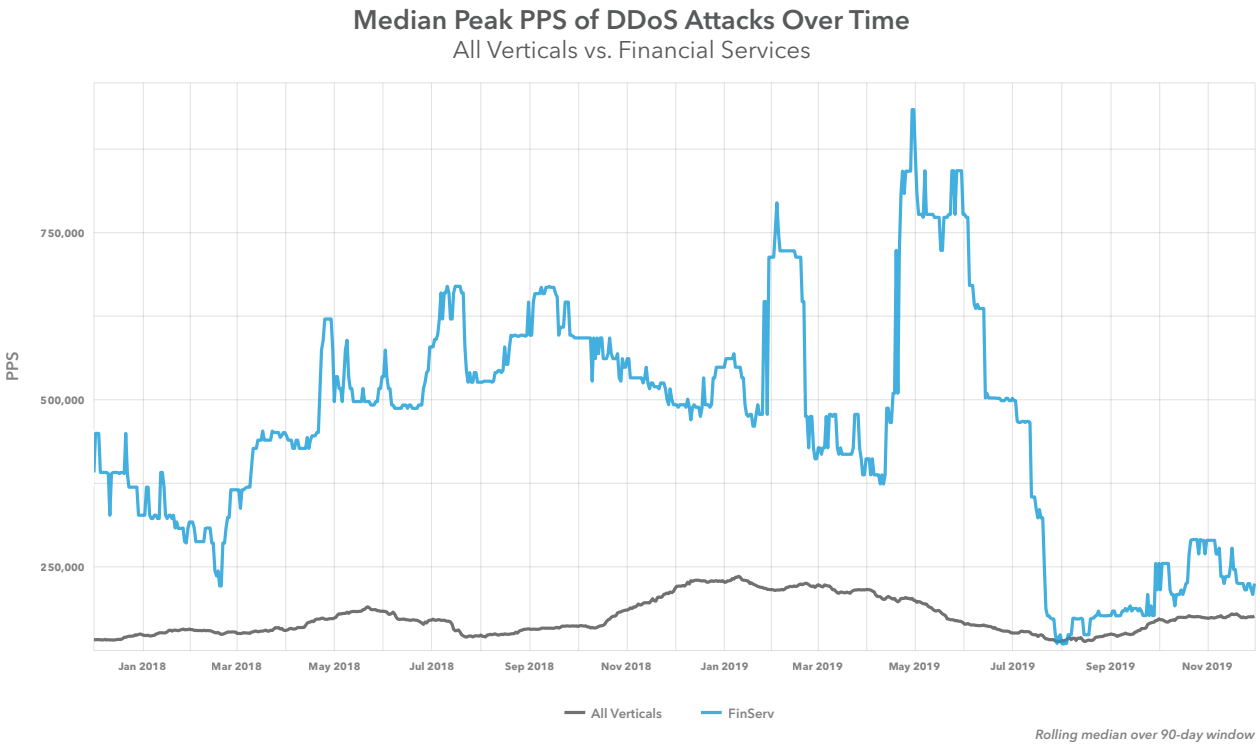
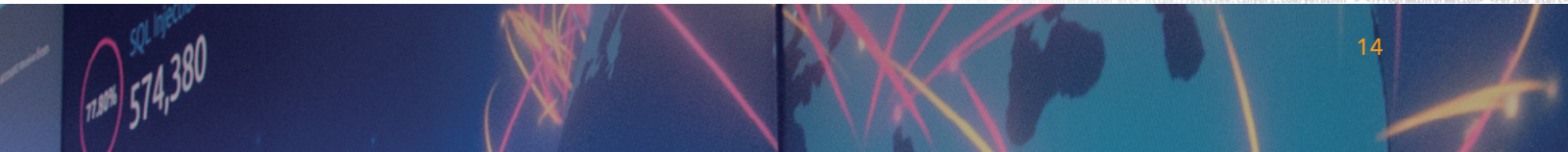


Fig. 8 – Peak pps in financial services had a sharp uptick in May 2019, followed by a sharp drop toward the end of the summer

The median packets per second (pps) has remained consistent over the past 24 months, but as shown in Figure 8, the peak pps for attacks against financial services was consistently higher when compared with attacks across all verticals. Pps is an important measure of attack traffic when DDoS is targeting application or network vulnerabilities. Given the smaller data set of financial services customers, the median is more heavily influenced by individual attacks than the overall measurement of pps.

On April 25, 2019, an incident reaching 113 million pps and 39 gigabits per second (Gbps) targeted an online bank and credit card issuer, making it the largest attack by pps across all verticals for the year. While the packet count for this attack was extremely high, individual packets were relatively small, limiting the volume of traffic created.

More than 40% of unique DDoS targets were financial services organizations.



Using the same plot style as Figure 8, Figure 9 shows median peak Gbps. Unlike pps, the median peak Gbps for all attacks has seen some significant growth in the past year or so. Similar to the peak pps, the peak Gbps for financial services attacks is typically higher than for all attacks, except for a big dip in the summer of 2019.

Volumetric attacks, which aim to overload networks with more traffic than they can handle, use Gbps as the most important measure of their impact. These are the attacks most readers will think about in conjunction with DDoS, and they're generally created by using reflectors (e.g., services like DNS) that amplify the traffic the attacker can create from the systems they control.

On April 22, 2019, a DDoS attack against a well-known and established bank used six different attack types, including SYN and UDP flooding, UDP fragmentation, RESET floods, Netbios floods, and CLDAP reflection. The attack reached a peak of 160 Gbps and 32 million pps. It is common for a single attack to use multiple attack types, with reflectors like CLDAP being responsible for amplifying the attacker's traffic.

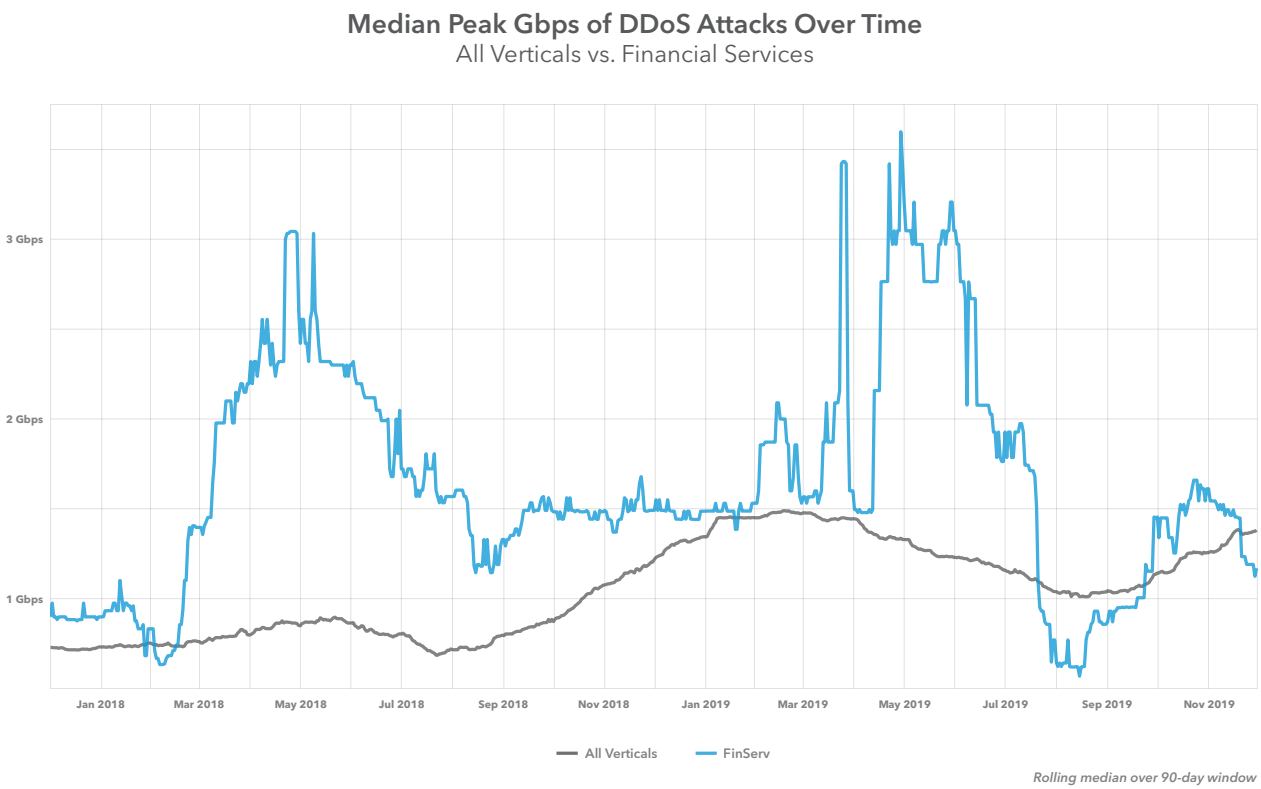


Fig.9 – During the period of rapid growth, from September 2018 to March 2019, the median peak Gbps for financial services remained relatively steady

In Figure 10, we examine the density of attack events by bps and pps for all verticals and for the financial services industry. The x-axis shows peak pps, while the y-axis is peak bits per second (bps); both are log-scaled. Lighter colors represent a higher density of attacks in a specific hexagon. Because of the different scale in number of attacks per intersection, we chose a separate color scale for financial services. These charts show a strong correlation between the pps and the amount of traffic created within a broad band.

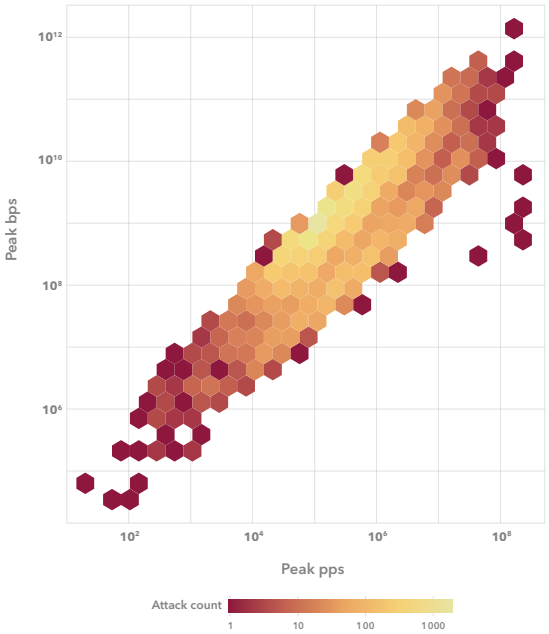
Zero Trust

We just spent a good deal of this report talking about attacks, from credential stuffing to SQLi and DDoS. Now we're going to talk about a framework designed to address each of these. The concept has been around since 2010, and it's been known by a number of names, such as microsegmentation, nano-segmentation, and BeyondCorp. But it's best known as Zero Trust.

The axiom of "trust, but verify" was sufficient when it came to networks with clearly defined boundaries. That was before the bring your own device (BYOD) revolution and the boom of remote workers, and long before cloud-based architectures became the norm for enterprises.

The Zero Trust model replaces "trust, but verify" with "trust nothing, and trust no one." Under Zero Trust, the network cuts off all access to network resources until it determines who the user is, and whether they're authorized. Nothing, absolutely nothing, inside or outside of the network is trusted. Security architectures further support this approach by applying the concept of least privilege to the user and the resources they're granted access to.

Density of Attacks Over Peak PPS and Peak BPS
All Verticals



Density of Attacks Over Peak PPS and Peak BPS
Financial Services

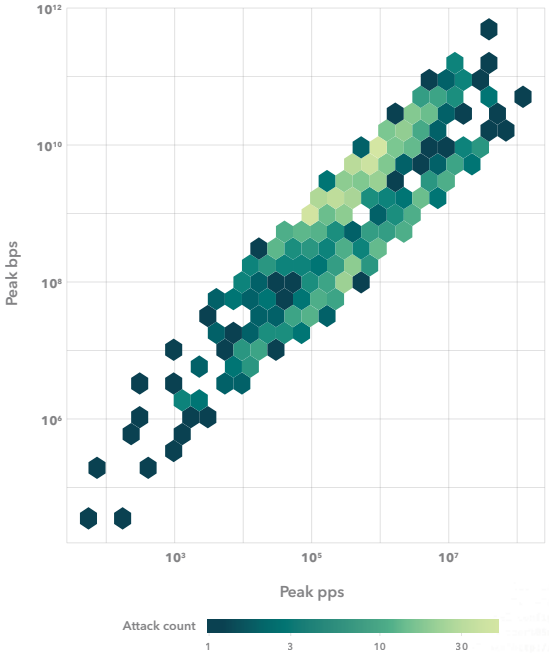


Fig.10 – Lighter hexes show the most common intersection of the number of packets and the amount of traffic in DDoS attacks

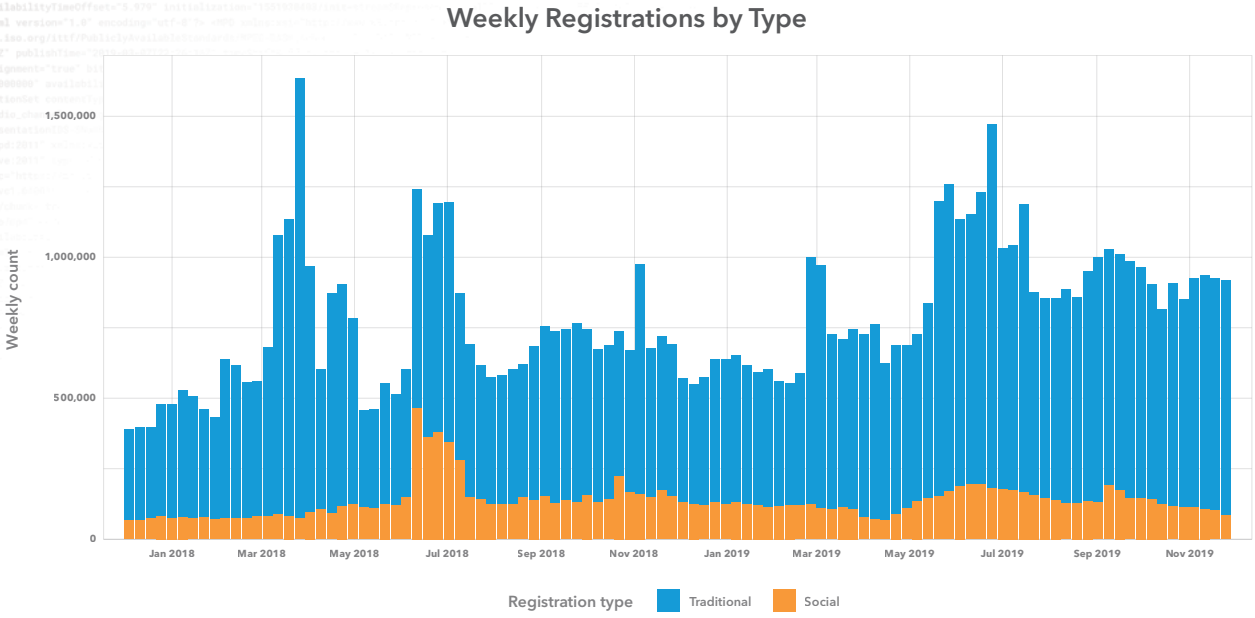


Fig.11 – During the period of rapid growth, from September 2018 to March 2019, the median peak Gbps for financial services remained relatively steady

It might seem harsh. It isn't. Consider the reality we're facing today. Organizations continue to suffer access-related problems with their users and resources, such as ransomware or compromised servers and databases. They also need to confront compromised supply chains and development channels. The concept of perimeter defense cannot keep up with the way technology is expanding and growing.

Many security programs in place today automatically trust a user or device once it is on the network. This enables criminals to pivot, exfiltrate data, or install malicious applications. Balance is another problem security programs face. Sometimes security can become an obstacle, which leads to users circumventing controls, or implanting their own solutions – also known as Shadow IT.

Organizations can leverage Zero Trust to address all of that.

Threats aside, Zero Trust is also being used to bake security into the enterprise evolution. It addresses the needs of an organization that doesn't have a centralized data center, but instead chooses to host some applications on-premise and others in the cloud. It's also used to enable controlled access to network resources for users, customers, and business partners no matter where they are in the world.

Getting to Zero – Identity

Zero Trust isn't a thing or product that you buy – it is a concept you build on. One of those building blocks is identity and access management (IAM). There are two types of identity management in play today; one of them is focused on internal operations (IAM) and the other is for external operations, called customer identity and access management (CIAM). It is possible to leverage both on a given network, and some enterprises do just that. Akamai acquired Janrain, a CIAM provider in Portland, Oregon, in January 2019. That acquisition has helped shape Akamai's Identity Cloud.

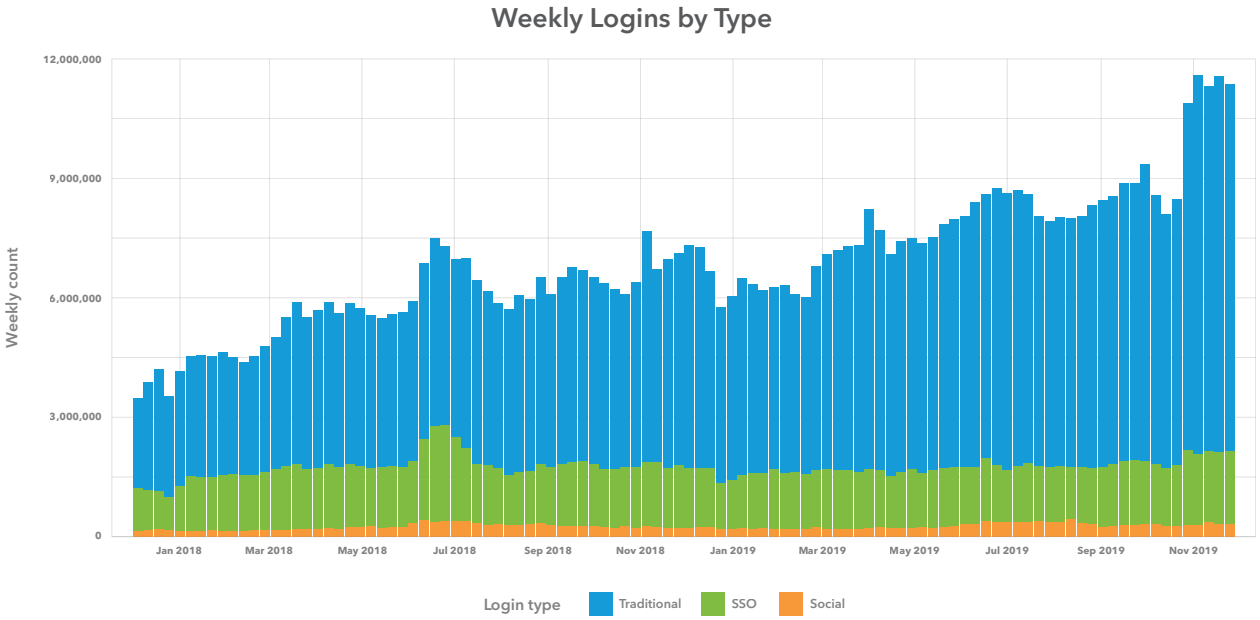


Fig.12 – SSO authentication remained steady during the observation period, with social logins accounting for only a small portion of the traffic

Looking at data from Janrain covering the time frame of December 2017 through November 2019, we can see signs that customers are increasingly starting to adopt IAM/CIAM postures. These are the foundations on which Zero Trust is built.

Consider Figure 11, which shows the weekly registrations by registration type. There are two that are tracked outside of the API account imports generated by an administrator: traditional and social. Traditional registrations happen when an account is established via registration UI, JavaScript API, mobile SDK, or OAuth API. Social registrations happen when an account is established by a user who a third-party identity provider authenticates, such as Facebook, LinkedIn, or Google.

The idea behind Zero Trust is to start building protections and security from the moment of registration onward. In some cases, the authentication of the user starts before the account can even be created, depending on the level of control needed.

Figure 11 shows that, while some organizations and users will opt to authenticate with a social method before registration, the standard practice, registering via traditional means, is still the go-to method.

When it comes to logins, traditional logins (username and password) still account for the majority of access methods (74%), but Single Sign-On (SSO) and social are also active. Social login is actually the smallest traffic set. However, within that data, Facebook, Google, and Twitter are the top OAuth mechanisms being used to authenticate people. In other words, don't expect to shut down your sign-up page any time soon.

As shown in Figure 12, SSO remains somewhat steady during the recording period, which is a good indicator that organizations are moving to multi-factor authentication for day-to-day activities.

Top 10 Verticals – EAA Customers

VERTICAL	% CUSTOMERS
High Technology	27.7%
Commerce	14.1%
Manufacturing	14.1%
Financial Services	9.3%
Business Services	7.1%
Video Media	7.1%
Nonprofit/Education	3.9%
Public Sector	3.9%
Pharma/Healthcare	3.2%
Other Digital Media	2.9%

Fig.13 – High tech is the top vertical using EAA to enable access and identity controls

Percent of Applications Behind Each Connector Type

CONNECTOR TYPE	% APPLICATIONS
VMware	60.3%
AWS EC2	*25.4%*
Microsoft Azure	*5.8%*
Microsoft Hyper-V	4.9%
OpenScrack/KVM	1.8%
Docker	0.8%
Google CGE	*0.5%*
VirtuaBox	0.4%

Connectors specific to cloud services providers

Fig.14 – VMware is top for on-premise connectors, with Amazon's EC2 as the lead cloud-based connector

Getting to Zero – Access

Identity is just one element of the Zero Trust concept, access and control are the other parts. At Akamai, we leverage the Zero Trust framework internally, using our own and external products, as we deliver the same to our customers. Enterprise Application Access (EAA) is a core component of our Zero Trust stack: the connector between the end user and the applications they're using.

EAA is designed to ensure that only authorized users and devices have access to the internal applications they need. It does this by combining data path protection, SSO, IAM, application security, management, and visibility controls into a single product.

At one point, some enterprises entertained an idea somewhat similar to Network Access Controls (NAC). As it turned out, the problem was that NAC became too difficult and expensive to implement for most organizations, so it fell by the wayside. Now, Zero Trust delivers on the promise of what could've been with NAC, but with the ease of VPN.

Looking at EAA data, nearly 28% of the user base Akamai serves is in the high tech sector, followed by commerce, manufacturing, financial services, business services, and video media. Figure 13 shows the top 10 vertical markets.

When it comes to the applications EAA users are connecting to, VMware, an on-premise solution, drives the largest number of applications and services. It is important to remember that the connector itself isn't actually hosting the application, but simply enabling access. A decade of movement to the cloud hasn't eclipsed the need for connecting to hosted services. For connectors directly related to cloud services, AWS is the leader, which shouldn't be surprising to anyone. The wide adoption of AWS reflects the fact that it is a more open platform for Software-as-a-Service (SaaS) solutions than many alternatives. There are signs that adoption is growing, not only because of SaaS enablement, but because it's focused on granular control and access – the very same qualities needed to establish a Zero Trust environment.

According to data that was available at the time this report was written, 30% of applications being protected in a Zero Trust architecture are SaaS applications (e.g., Azure, AWS). We anticipate this number to increase over time, as more and more critical enterprise applications and services move to the cloud.

As organizations move to adopt cloud-based applications and services, the Zero Trust framework becomes a vital part of the equation. AWS is viewed as the industry standard by administrators and business leaders, followed closely by Azure. Both platforms are growing with their customers, and offering more customized solutions for network and service architecture, which includes Zero Trust models.

These figures show that enterprises are becoming more agile in the way they delegate tasks and services. For now, they're more apt to keep things on-premise when possible, as it offers more visibility and control.

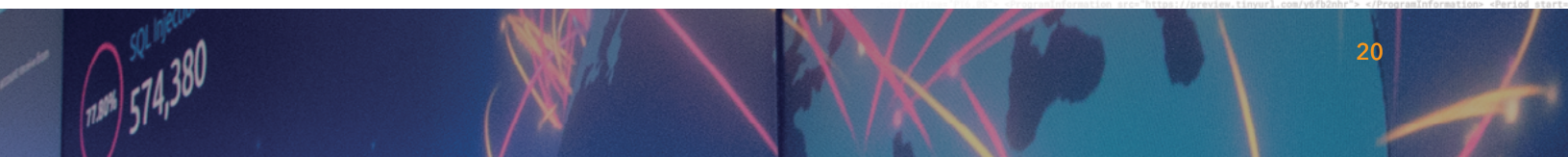
Lessons Learned

It isn't just financial services; everyone is being targeted by criminals who use and abuse stolen credentials to fuel their criminal enterprises. However, the financial services industry is a major target for criminals because of the wealth of information that those organizations possess. If nothing else, financial services organizations should be aware of the shift to credential abuse targeting their APIs. From credential stuffing to DDoS attacks, criminals are relentless in their pursuits, forcing defenders to remain ever vigilant.

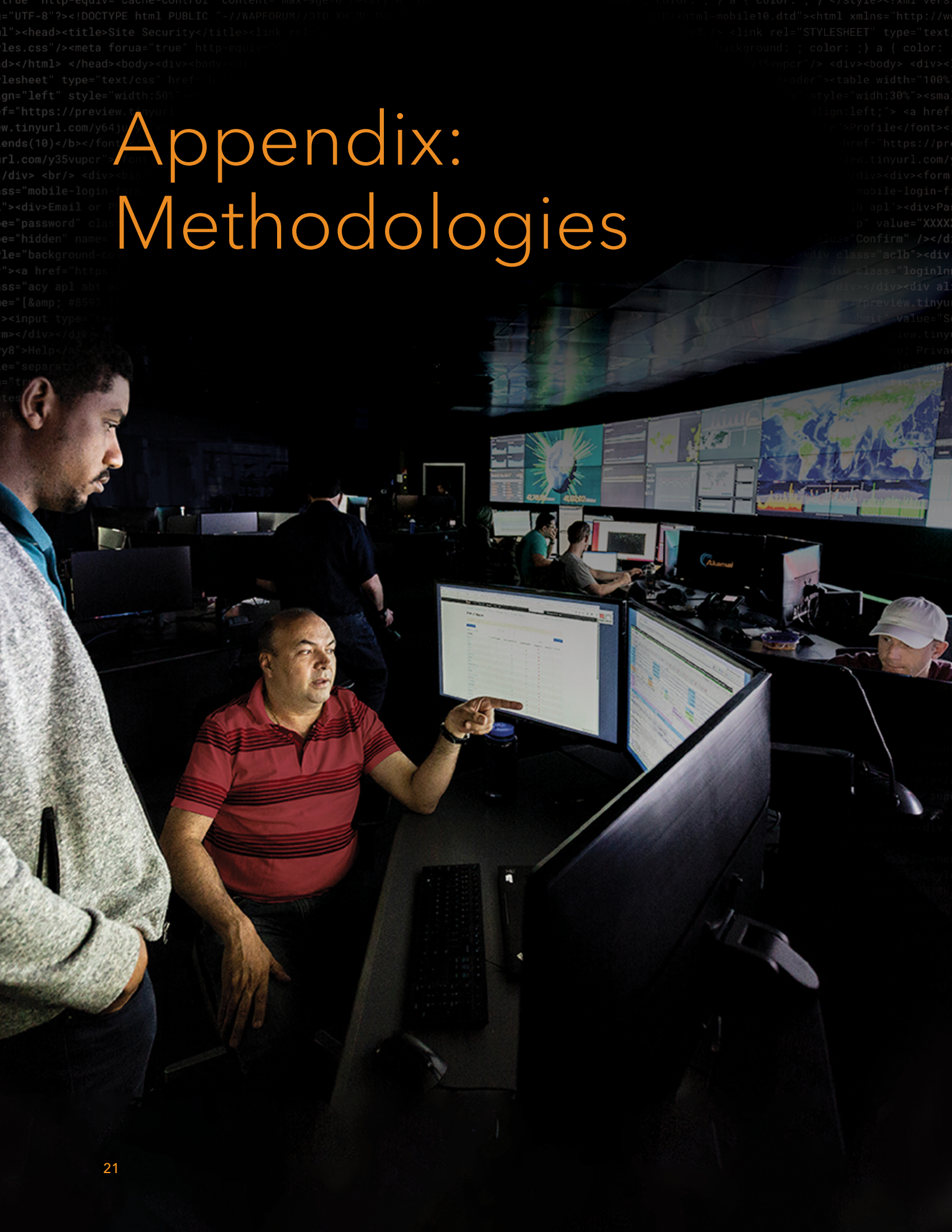
One of the tools to fight this continued assault is Zero Trust. As adoption of this framework spreads, it will become more difficult for criminals to use passive attacks, like credential stuffing, to gain a foothold on a given network. It will be harder for them to leverage phishing or custom command and control servers, since DNS can be blocked at the source.

That doesn't mean Zero Trust is a silver bullet. You can't throw money at a problem, adopt lots of different technologies, and expect things to happen like magic – security doesn't work that way. The most success with Zero Trust comes from embracing the concept, and building your operations around it, which will include investments as needed.

Zero Trust isn't an easy thing to adapt to. It can take time, and legacy systems could cause some headaches at first. But evolving away from the notion of a perimeter defense is where the future is heading, because the world as we know it is quickly expanding and connecting everyone.



Appendix: Methodologies



General Notes

The data used for all sections was limited to the same 24-month period — December 1, 2017, to November 30, 2019.

API Attacks

The data for this section was drawn from Cloud Security Intelligence (CSI), an internal tool for storage and analysis of security events detected on the Akamai Intelligent Edge Platform. This is a network of more than 230,000 servers in thousands of networks around the globe. 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.

Credential abuse attempts were identified as unsuccessful login attempts for accounts using an email address as a username. We use two algorithms to distinguish between abuse attempts and real users who can't type. The first is a simple volumetric rule that counts the number of login errors to a specific address. This differs from what a single organization might be able to detect because Akamai is correlating data across hundreds of organizations.

The second algorithm uses data from our bot detection services to identify credential abuse from known botnets and tools. A well-configured botnet can avoid volumetric detection by distributing its traffic among many targets, using a large number of systems in its scan, or spreading out the traffic over time, just to name a few evasion examples.

To identify obvious API endpoints, we matched hostnames against a regular expression pattern, checking for the inclusion of *api*, *soap*, or *rest*.

Web Attacks

The data for this section, also drawn from the CSI repository, describes application layer alerts generated by Kona Site Defender and Web Application Protector. The products trigger these alerts when they detect a malicious payload within a request to a protected website or application. The alerts do not indicate a successful compromise. While 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.

DDoS Research

Prolexic Routed defends organizations against DDoS attacks by redirecting network traffic through Akamai scrubbing centers, and only allowing the clean traffic forward. Experts in the Akamai Security Operations Center (SOC) 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 SOC or the targeted organization itself, depending on the chosen deployment model — always-on or on-demand — but the SOC records data for all attacks mitigated. Peak pps and bps reflect the highest recorded values during the attack event and may occur at different times.

Top Source Areas – Malicious Logins Against APIs

SOURCE AREA	API TARGETS	ALL TARGETS	GLOBAL RANK ALL TARGETS
United States	4,125,096,694	27,720,941,969	1
Canada	1,201,645,251	2,755,050,121	7
Germany	824,565,170	2,248,968,240	11
Russia	750,697,426	5,971,495,742	2
Brazil	728,124,509	3,946,259,977	3
France	711,910,138	2,419,030,977	9
China	707,860,559	2,934,117,887	5
India	587,264,282	3,101,634,280	4
Vietnam	577,668,010	2,350,650,696	10
Netherlands	553,657,601	1,704,898,799	12

Top Source Areas – Malicious Logins Against Financial Services

SOURCE AREA	FINSERV	ALL VERTICALS	GLOBAL RANK ALL VERTICALS
United States	1,510,868,522	27,720,941,969	1
Malaysia	351,107,813	1,633,449,986	15
China	248,220,277	2,934,117,887	5
France	201,122,825	2,419,030,977	9
Indonesia	187,890,980	2,587,071,754	8
India	177,518,111	3,101,634,280	4
Vietnam	166,682,300	2,350,650,696	10
Brazil	166,370,637	3,946,259,977	3
Russia	140,434,207	5,971,495,742	2
Germany	125,437,147	2,248,968,240	11

Top Target Areas – Malicious Logins Against APIs

TARGET AREA	API TARGETS	ALL TARGETS	GLOBAL RANK ALL TARGETS
United States	10,664,573,225	63,989,127,852	1
India	3,989,751,301	6,541,253,765	2
China	513,042,265	5,368,482,247	3
Canada	294,066,912	2,117,361,682	4
Brazil	289,952,527	745,960,037	9
United Kingdom	281,425,519	1,097,838,460	6
United Arab Emirates	270,209,848	391,643,895	10
Switzerland	81,399,628	182,758,977	16
Italy	66,819,193	220,843,398	13
Australia	58,692,014	238,803,544	12

Top Target Areas – Malicious Logins Against Financial Services

TARGET AREA	FINSERV	ALL VERTICALS	GLOBAL RANK ALL VERTICALS
United States	4,154,212,999	63,989,127,852	1
Canada	184,382,462	2,117,361,682	4
France	87,871,337	242,255,513	11
Malaysia	30,064,767	199,700,300	15
Germany	29,726,664	1,555,016,496	5
India	12,246,297	6,541,253,765	2
Israel	11,693,350	11,693,350	27
Brazil	11,596,822	745,960,037	9
Australia	3,482,832	238,803,544	12
United Kingdom	3,104,323	1,097,838,460	6

Credits

State of the Internet / Security Contributors

Omri Hering
Senior Lead Data Analyst – *API Attacks* and *Web Attacks*

Sean Calhoon
Product Line Director – *Zero Trust*

Lydia LaSeur
Data Scientist – *DDoS Attacks* and *Zero Trust*

Bill Poulos
Engineering Manager – *Zero Trust*

Or Katz
Principle Lead Security Researcher – *Zero Trust*

Robert Towne
Architect – *Zero Trust*

Editorial Staff

Martin McKeay
Editorial Director

Amanda Fakhreddine
Senior Technical Writer, Managing Editor

Steve Ragan
Senior Technical Writer, Editor

Lydia LaSeur
Data Scientist

Marketing

Georgina Morales Hampe
Project Management, Creative

Murali Venukumar
Program Management, Marketing

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 02/20.

Akamai

Intelligent Security Starts at the Edge

More State of the Internet / Security

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

More Akamai Threat Research

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


Akamai
Intelligent Security
Starts at the Edge