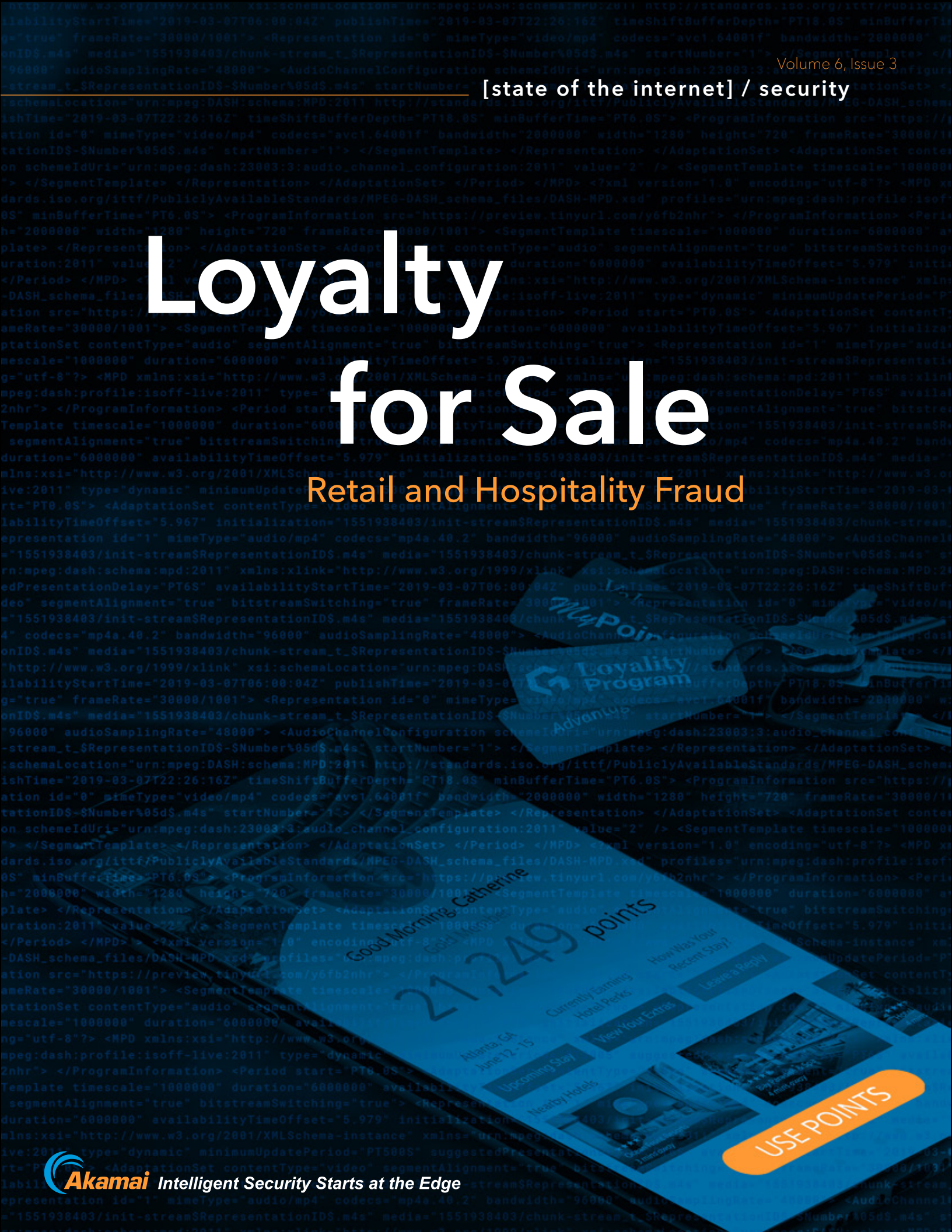
Volume 6, Issue 3

Loyalty for Sale

Retail and Hospitality Fraud



Akamai Intelligent Security Starts at the Edge

Table of Contents

Letter from the Editor

Welcome to Akamai's State of the Internet / Security report, Volume 6, Issue 3, *Loyalty for Sale: Retail and Hospitality Fraud*.

Were you prepared for 2020? To be honest, that's a rhetorical question; almost no one was prepared for this year and what it would bring. It's been a learning experience for every business, but it could easily be said that retail, travel, and hospitality organizations have been impacted the most.

Our title, *Loyalty for Sale*, has multiple possible meanings, but we mean it almost literally. While your loyalty to a merchant, airline, or hotel chain might not literally be for sale, there's a good chance the account associated with a loyalty program you use is. If we're being honest, there's also a good chance that each of us has accounts with multiple, competing companies. With each account created, we can take advantage of whichever program gives us the best discount for a specific transaction. It's not disloyal to shop around for the best deal, though it might dilute some of the power of using loyalty programs.

Criminals aren't afraid to use our loyalty against us. As we've said in previous reports, password reuse is a significant problem in all industries. Loyalty programs have the additional problem with perception, as many consumers don't think of them as high risk, and are more likely to use weak passwords or mirror accounts they're using with another organization. Even if your compromised account isn't used to book travel or your points aren't spent on products, the accounts themselves are a valuable product that can be sold to other criminals in the dark markets.

It may not be a comfortable thought, but in many ways, criminal enterprises are businesses just like any other and follow some of the same patterns we see in legitimate businesses. "As a service" is just as firmly entrenched in the underground as elsewhere – with DDoS for hire, botnet rentals, and phishing services being just a few examples. So it shouldn't be any surprise that account lists are for sale and the tools to use them are available for rent.

All businesses need to adapt to external events, whether it's a pandemic, a competitor, or an active and intelligent attacker. We've been watching credential abuse, and the markets that support it, evolve for more than two years. And nearly every time we look at it, we become more convinced it's not an issue that can be tackled without having a wide view of the problem and the actors involved.

Martin McKeay
Editorial Director

GUEST ESSAY

Cybersecurity is a Low-ROI Business Case, Until a Breach

By Jeff Borman

While tens of thousands of buildings around the world hang Marriott, Hyatt, or Hilton signs, the property is nearly always owned by a publicly traded real estate investment trust (REIT) or private owner. These major hotel companies are also 85% franchised, so the operators of a hotel are almost certainly a company that no guest ever knows. The person at the reception desk wearing a Holiday Inn name tag is very rarely employed by InterContinental (IHG), the parent company that owns the Holiday Inn brand. Major brand companies concentrate their operations efforts on only the most lucrative hotels, typically the luxury and convention type of properties. Essentially, the industry giants have evolved over the past 25 years into primarily branding companies with massive loyalty programs.

The appeal of these behemoths to a prospective property owner is that they offer better investment returns. Hedge fund managers and venture capitalists rarely have experience in hotel management, so they pay the industry's giants for their expertise. A brand management company like IHG has a corporate architecture and design team that creates a "hotel in a box" option for builders.

To deliver the higher ROI that investors seek, the major brands must bring more customers through the door than a brandless alternative. First, the brands promise travelers a consistent experience across the portfolio. Just as a Big Mac tastes the same at every McDonald's, the brands ensure that every check-in has the same "Hamptonity."

Second, their massive loyalty programs ensure that all of the world's most valuable travelers shop only within their chosen brand portfolio. With 32 brands ranging from Fairfield Inn to Ritz-Carlton, Marriott ensures that frequent travelers can find everything they need within the offerings of marriott.com. With its base of 120 million Bonvoy members, a company like Marriott can deliver 10 percentage points more in occupancy than a similar non-branded competitor, and do so in less than half of the time from opening the doors. Product reliability, combined with the perks of loyalty programs, builds a massive customer base that essentially underwrites the entire big-brand business model.

While operational cost containment and support offer significant value, for large hospitality companies, the loyalty programs are the fulcrum of their existence. Engaged customers interact directly with their preferred company. Loyal Marriott customers don't mess around with Trivago – they go straight to marriott.com. A non-branded hotel can often pay Online Travel Agencies (OTAs) like Hotels.com as much as 25% commission per booking. The same transaction under a major brand will trade at half that cost. Even still, a booking on a major hotel brand's own site can cost one-tenth as the same reservation made through an intermediary. Loyalty programs reinforce direct-booking behavior by limiting the program perks to only those who book directly.

Twenty years ago, the biggest brands managed hotels; today they manage a customer base. A downside to this "asset-light" approach is that the major hospitality companies rely on the property owners to continue investing in their hotels. Investments range from upgrading the physical property with new furniture designs to hotel management software. When Hilton launched Digital Key in 2016, the first contactless check-in process in the industry, it needed to ensure that every hotel owner installed the proper door locks and executed the proper system procedures. Enhancements like these carry large costs, so a company like Hilton must be very diligent in selecting which initiatives to mandate.

Each year, the major hospitality brand companies go through an internal prioritization process to determine which investments are the top priorities and worthy of imposing upon owners. Departments compete to make the list. Revenue Management builds a case to fund investment for better pricing algorithms. Marketing teams lobby for larger brand advertisement contributions. The Digital team argues for improved SEO funding.

Hotel operators advocate for investment in the physical plant to improve hotel quality. The winning cases are usually those with the highest probability to increase revenue – the primary proposition of a brand management company.

Each year in compliance with U.S. legal regulations, franchisors must publicly release a "Franchise Disclosure Document" outlining any new costs and rules being mandated upon franchisees. With nearly unlimited ways to spend someone else's money, it's not unusual for 90% of the "good ideas" to be cut, lest all of an owner's profits be eaten up in new projects each year. ROI beats risk mitigation every time. Non-commercial investment tends to get deprioritized, as owners always prefer projects that drive their profits over those that protect brand reputations. To hoteliers, cybersecurity is a cure for insomnia. For an industry that prides itself in helping others get a good night's rest, that may sound attractive – but falling asleep also opens an opportunity for nightmares.

Jeff Borman is the Founder and Chief of travelINNsights, a hospitality and tourism consultancy that services travel-sector investors and academics. TravelINNsights also publishes hospitality research on the economics of the travel industry for the general public. The majority of his 20 years in hospitality were leading revenue management for Marriott and Hilton, with specific expertise in analytics, pricing science, and inventory management.

When not helping the travel industry as an employee, Jeff is supporting it as a customer, having hiked, dined, and mingled with locals in over 70 countries and 45 states. When grounded at his home in Alexandria, Virginia, he can usually be found in the kitchen (preferably the outdoor one) or rummaging through the wine cellar proudly trying to recall his recently acquired sommelier skills.

Introduction

We need to address the elephant in the room. The retail, travel, and hospitality industries were deeply impacted by the COVID-19 pandemic.

These industries, known for their focus on customer service and face-to-face interaction, either augmented or created several programs to support their customers. However, these measures – including point extensions on various loyalty programs, bonus rewards, etc. – couldn't stop the drop in business during the first half of 2020. When the world came to a standstill for several months, it led to staffing and operational cuts.

Criminals seized the moment and started targeting the retail, travel, and hospitality sectors with attacks of all types and sizes. Between July 2018 and June 2020, Akamai observed more than 100 billion credential stuffing attacks, and more than 63 billion of them targeted retail, travel, and hospitality.

During the lockdowns in Q1 2020, criminals circulated dozens of password combination lists, and targeted each of the commerce industries. It was during this time that criminals started recirculating old credential lists in an effort to identify new vulnerable accounts, leading to an uptick in sales related to loyalty programs.

Akamai uses the term "commerce" when categorizing customers that fall into the retail, travel, and hospitality industries. There is a subcategory called "commerce-other" when discussing wholesalers and distributors without a direct-to-consumer channel. In this report, we use "commerce" and "other" in the graphs, but refer to the industry directly when discussing attacks and providing context.

Credential stuffing wasn't the only type of attack. Criminals also targeted the retail, travel, and hospitality industries online at the source, using SQL Injection (SQLi) and Local File Inclusion (LFI) attacks. In fact, between July 2018 and June 2020, Akamai observed more than 4 billion web attacks against retail, travel, and hospitality, accounting for 41% of the overall attack volume. Within this data set, 83% of those web attacks targeted the retail sector.

These industries are top targets for criminals because they offer several commodities, from personal information to entire accounts flush with reward and loyalty points that can be cashed out or traded.

> "Between July 2018 and June 2020, Akamai observed more than 100 billion credential stuffing attacks, and more than 63 billion of them targeted retail, travel, and hospitality."

Credential Abuse

Credential abuse, or credential stuffing attacks, have a single root problem: passwords. Recycled passwords, shared passwords, easily guessed passwords – all of these things can lead to a successful credential stuffing attack.

Over the years, criminals have adapted to changes online and started targeting APIs directly to perform these attacks, but they'll still target basic login portals. Moreover, some criminals augment their credential collections by testing variations of a given password. Doing so increases their odds of success.

For example, if an old data breach contained the password Patriots05, a criminal who knows American football might augment this to Patriots17, Patriots283, or other easily guessed variations. This is why using dictionary words or patterns is a bad idea, and why password managers are essential these days.

In fact, the number one way to stop credential stuffing attacks is to use a password manager, and generate long, random passwords that are unique to each website. This, when combined with multi-factor authentication, will render passive credential stuffing attacks useless.

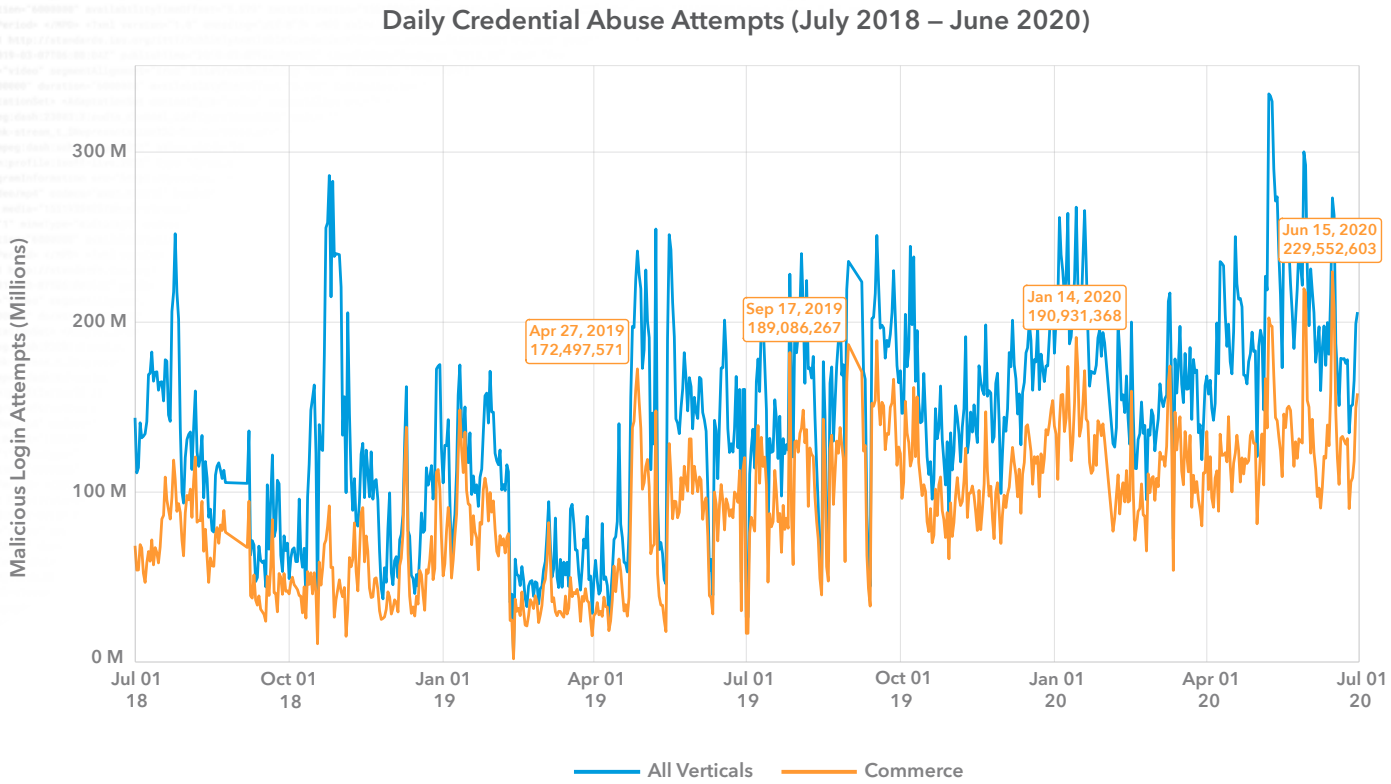


Fig. 1 – Credential stuffing attacks have remained steady over time, including a noticeable peak toward the end of Q2 2020

In Figure 1, you can see the logged credential stuffing attacks between July 2018 and June 2020, but we've removed one non-commerce customer from the data set because its attack volume generated significant traffic, and only six months of data were available at the time this report was being developed. The first thing to notice is how consistent the attacks are, no matter what line you follow. In the retail, travel, and hospitality industries combined, there were 63,828,642,449 credential stuffing attacks recorded, and more than 100 billion overall. More than 90% of the attacks in the commerce category targeted the retail industry.

We've highlighted various peaks on the timeline. On April 27, 2019, 39% of the recorded attacks were against a well-known online retailer (which has been around since the earliest days of the internet), but that day also included attacks against retailers that focus on music, as well as apparel. On September 17, 2019, the attacks were split among apparel companies (34%), the previously mentioned well-known retailer (14%), travel (5%), and office supply retailers (9%).

In January 2020, the effect of global lockdowns was noticeable as criminals targeted one of the world's largest online retailers (18%), as well as a popular home improvement retailer (4%). In addition, criminals split their time across office supplies (6%), fast food (3%), and apparel companies (17%) on this day too. Finally, on June 15, 2020, the attacks focused heavily on apparel and cosmetics (43%), followed by online retail (17%), office supplies (4%), and fast food (3%).

Top Source Areas for Credential Abuse – Commerce

July 2018 – June 2020

SOURCE AREA	MALICIOUS LOGIN ATTEMPTS	GLOBAL RANK
United States	23,160,331,758	1
China	3,416,134,923	2
Thailand	2,885,486,429	5
Brazil	2,844,012,210	4
Indonesia	2,333,147,171	7

Fig. 2 – The United States and China are the top two sources for credential stuffing attacks

The majority of these attacks, as seen in Figure 2, came from the United States, followed by China, Thailand, Brazil, and Indonesia to round out the top five. Akamai can only see the last hop in the attack chain, but proxy and bot services are in demand and popular in these areas – particularly China, where bots can be rented for pennies a minute.

When it comes to the destination of the attacks, which is determined by where the customer is located, as seen in Figure 3, the United States is still the top target, followed by China, India, Brazil, and Canada.

Top Target Areas for Credential Abuse – Commerce

July 2018 – June 2020

TARGET AREA	MALICIOUS LOGIN ATTEMPTS	GLOBAL RANK
United States	46,515,587,176	1
China	5,129,941,553	3
India	3,801,260,736	2
Brazil	1,950,460,737	6
Canada	1,276,859,184	5

Fig. 3 – The United States and China are also the top targets when it comes to credential stuffing attacks

Credential Abuse Case Study

Criminals are not picky. Anything that can be accessed can be used in some way. This is why credential stuffing has become so popular over the past few years. These days, retail and loyalty profiles contain a wealth of personal information (which can be collected, compiled, and sold) as well as financial access (stored credit/debit cards or reward balances, which can be traded or sold in pieces). Some examples are fuel points and hotel reward balances.

One criminal has been running sales since 2019 centered on fuel points, as highlighted in Figure 4. It might seem odd, and completely outside the norm when it comes to the items being sold by criminals as a result of credential stuffing, but this is a perfect example of how nothing is off limits. The ad promoting this product centers on the financial trade-off: a theoretical $30 in fuel savings, for just $13.

Fig. 4 – Criminals offer up rewards accounts good for fuel discounts

In Figure 5, the same criminal is also offering accounts with credit cards attached, which include not only the ability to spend existing reward points on fuel, but also order groceries for pickup. This isn't without risk, but the seller of the account doesn't need to worry about these things.

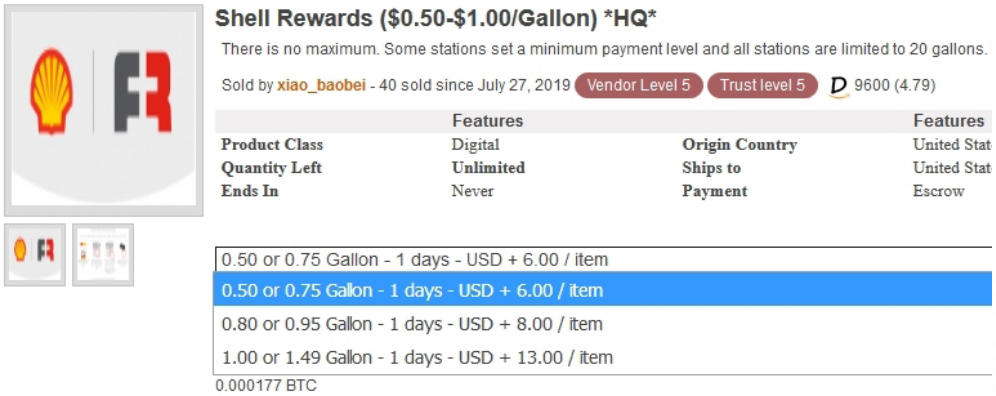


Fig. 5 – Criminals will sell anything, including reward accounts maintained by gas stations and grocery stores

Hotel rewards are also popular, including those from major chains like Hilton. Accounts are sorted and sold based on their point value. In Figure 6, one ad promotes accounts with at least 10,000 points for $3 each, while accounts with 40,000 points sell for $30. This seller also offers accounts with 100,000–550,000-point balances, as well as 600,000–1,000,000-point balances, the most expensive of which sells for $850.

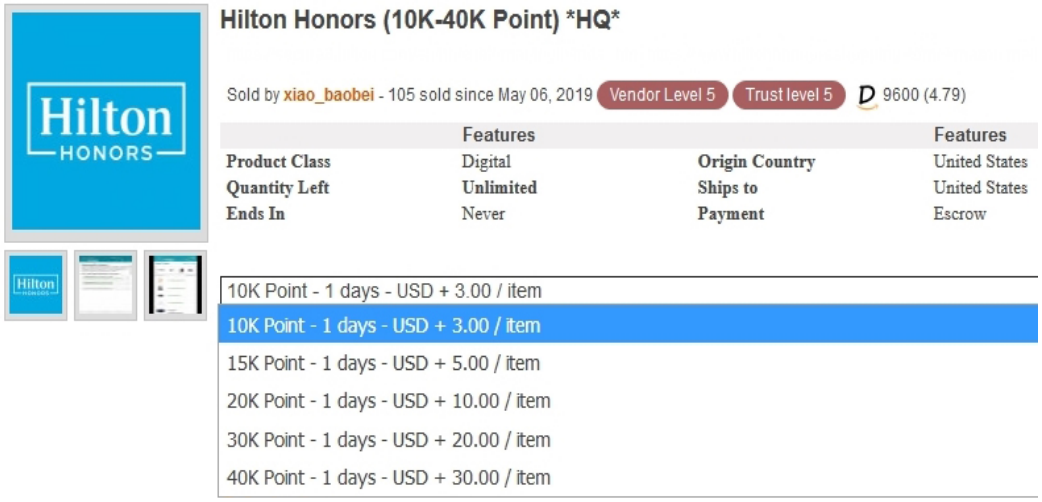
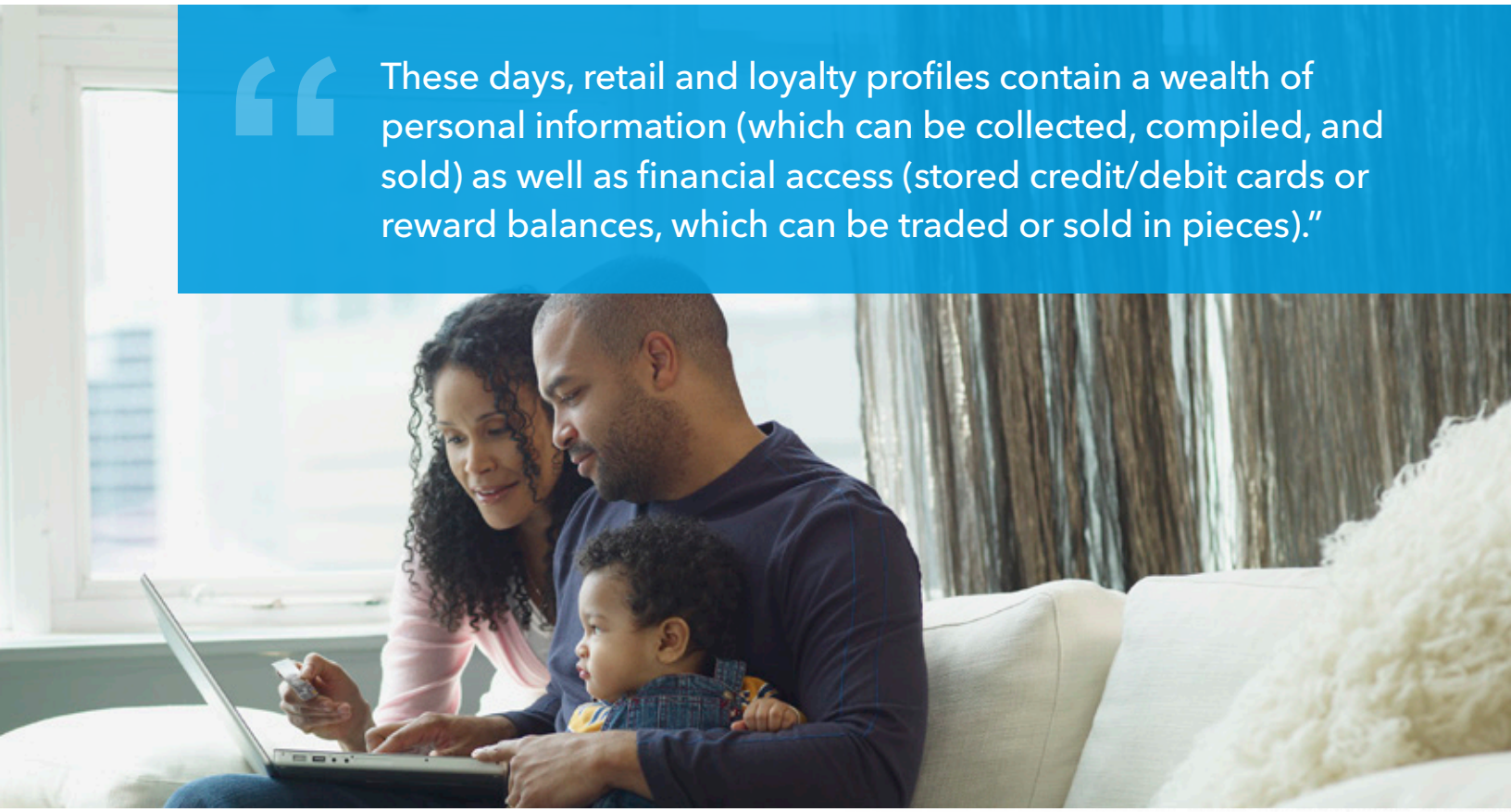


Fig. 6 – Hotel rewards are frequently traded and sold on darknet markets



> "These days, retail and loyalty profiles contain a wealth of personal information (which can be collected, compiled, and sold) as well as financial access (stored credit/debit cards or reward balances, which can be traded or sold in pieces)."

Travel Case Study

Did you know criminals have travel agents? They've been around for years, and their business isn't so much exploiting the hospitality and travel industries, but taking advantage of the existing workflows and supply chain.

In some cases, the criminal travel agents will book using stolen credit cards, or compromised airline miles or hotel reward points, but in reality, they don't have to. Loyalty points can be shared between accounts, so transfers are a common method of operation. There are also discount programs, insider access, and third-party service abuses.

Many of the travel listings on the darknet charge a percentage of the overall trip cost, anywhere from 25% to 35% – meaning a $2,000 booking on a well-known travel comparison/booking website would cost about $700 on the darknet, as shown in Figure 7.

Yet the criminals running the travel businesses see themselves as being in the service industry. In their ads, customer support is stressed, as is the hassle, worry-free process of booking.

"We have completed 8,500+ transactions over the years with nothing more than positive response to the services we provide. Although we charge more than the average 'travel vendor' you can trust our name and history, there will be no cancellations, security issues or headaches during your travel when booking with us [*sic*]," explains one travel vendor on the darknet.

Another claims, "We've used the same method for all these years and we put more effort into ensuring your safety than the competition. We do not use credit card fraud or points fraud, our method involves fraud but the company (provider) will always keep their funds, and there will be no such thing as chargeback which means there will be no one investigating the service you've ordered. [*sic*]"

As mentioned, some criminals book travel for their customers by using compromised cards, compromised reward accounts, or a mix of both. The risk is assumed entirely by the person taking the trip.

But many of the more successful sellers – who are ranked by cancellations and problems (the fewer, the better) – target third-party agencies or have boasted about someone on the inside who can slip in bookings.

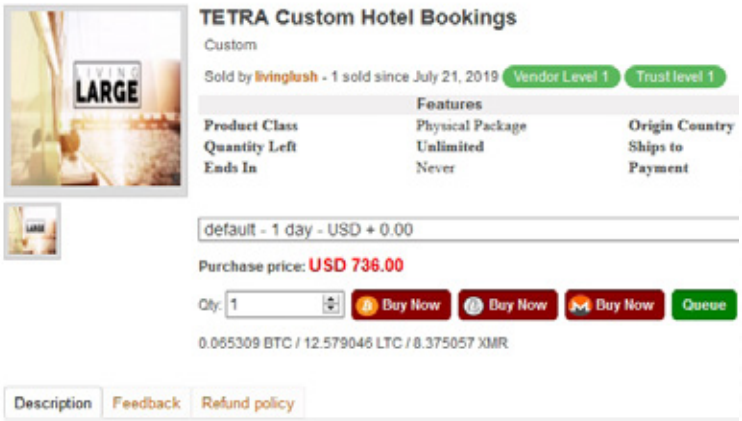


Fig. 7 – A custom booking offered up to an unknown buyer on the darknet

WAF

Credential stuffing isn't the only way that criminals target the retail, travel, and hospitality industries. They target organizations in these industries at the source using SQL Injection (SQLi) and Local File Inclusion (LFI) attacks. Between July 2018 and June 2020, Akamai observed 4,375,711,860 web attacks against retail, travel, and hospitality, accounting for 41% of the overall attack volume across all industries. Within this data set, 83% of those web attacks targeted the retail sector.

In Figure 8, you see the breakdown of web attacks in the commerce category. There were more than 3.4 billion SQLi attacks during the recording period, and more than 610 million LFI attacks. Clearly there is a difference between attacks, and SQLi stands out as the clear method of choice for criminals, but why?

Access.

Criminals are targeting databases to access personal information, financial records, password hashes, and anything else that's stored. SQLi attacks can result in complete account takeovers, but most attacks are focused on dumping information for quick processing.

The targets of the web attacks we've recorded are the usual locations, with the United States taking the top spot, followed by the United Kingdom, Germany, China, and Italy (Figure 9). We call them the usual locations because these places are where several popular retailers and hospitality organizations reside, so it isn't shocking to see them ranked in this order.

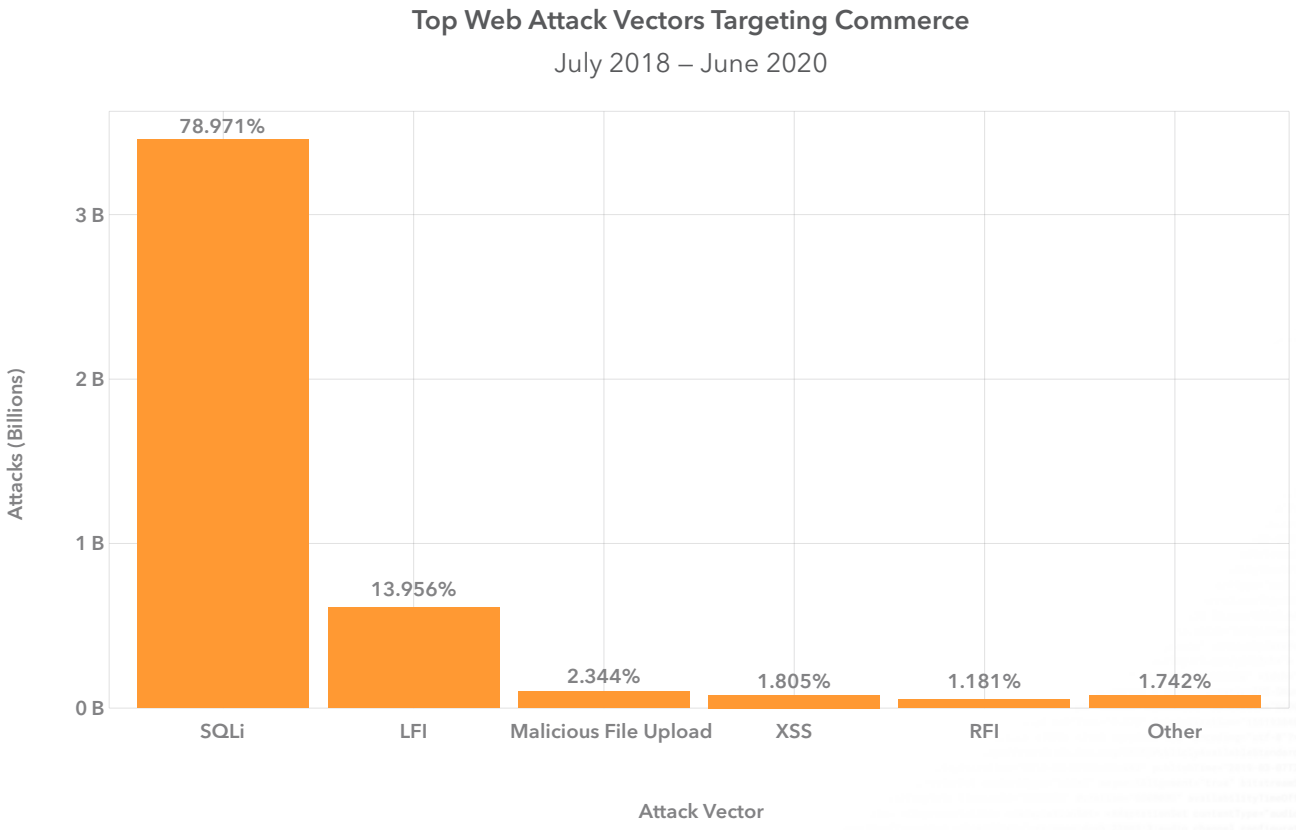


Fig. 8 – SQLi attacks are the clear favorite among criminals, accounting for 78% of the attacks against retail, travel, and hospitality

Top Target Areas for Web Application Attacks – Commerce

July 2018 – June 2020

TARGET AREA	ATTACK TOTAL	GLOBAL RANK
United States	3,254,388,815	1
United Kingdom	213,941,278	2
Germany	101,055,323	4
China	89,718,070	9
Italy	89,008,029	12
India	79,656,341	3
Japan	78,784,298	6
Brazil	72,290,365	13
Spain	58,100,405	8
France	54,359,137	5

Fig. 9 – The United States remains the top target for web attacks in the commerce category

In Figure 10, the source of the web attacks alters the list some, with Russia taking the top spot, followed by the United States, Ukraine, China, and the Netherlands rounding out the top five. These locations represent the final hop in the attack chain, but they're not indicative of the originating source, as criminals use proxy servers and VPNs to route their attacks.

Top Source Areas for Web Application Attacks – Commerce

July 2018 – June 2020

SOURCE AREA	ATTACK TOTAL	GLOBAL RANK
Russia	991,460,523	2
United States	824,268,280	1
Ukraine	226,722,689	5
China	203,910,633	4
Netherlands	192,644,127	3
Brazil	158,750,288	9
India	120,168,099	6
Thailand	117,005,532	12
Germany	85,055,475	8
France	77,354,726	14

Fig. 10 – Russia is the top source for web application attacks, followed by the United States

WAF Case Study

SQLi attacks target databases and the data within. In Figure 11, a recent addition to a darknet marketplace promotes a compromised database from a travel and hotel booking website. The database, holding roughly 17 million records, contains device information, email addresses, passwords, usernames, and other personal information.

Fig. 11 – Criminals compromise databases via SQLi to leverage the data within, and to sell the database itself

DDoS

Distributed Denial-of-Service (DDoS) attacks are something any retailer dreads, because if their online commerce portal collapses under an onslaught of packets and malicious traffic, it could cost them thousands of dollars a second.

Between July 2019 and June 2020, shown in Figure 12, the commerce category faced 125 DDoS attacks – 90% of them against organizations operating in the retail sector, with the remainder in travel and hospitality.

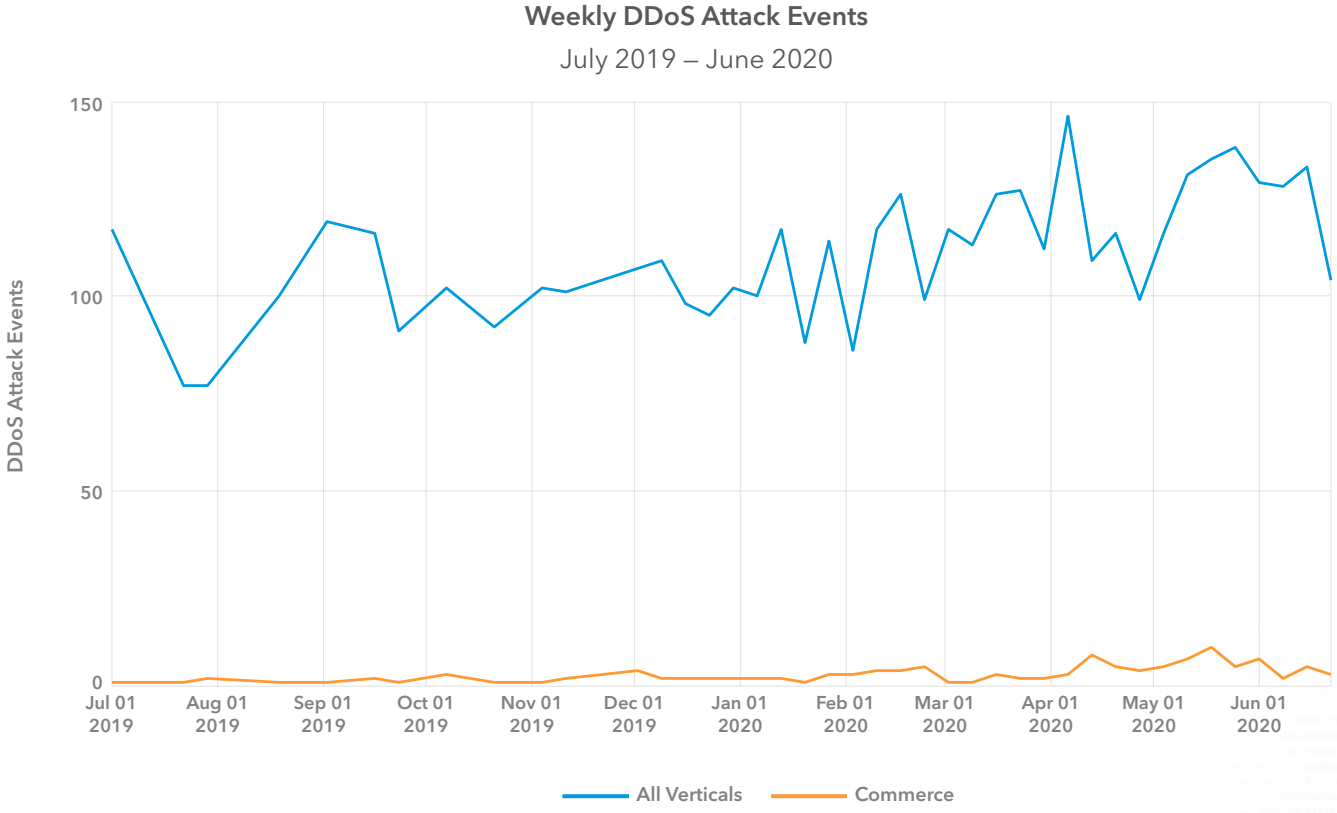


Fig. 12 – The majority of the commerce DDoS attacks observed targeted the retail sector, which stands to suffer massive financial losses if not defended

Conclusion

The retail, hospitality, and travel industries are consistently targeted by criminals, because they have access to assets that are easily turned into commodities. These assets could be personal information, financial information, brand-based loyalty programs, or all of them combined.

Defenders have developed, improved, and redeveloped defenses and defense products over the years to deal with attacks. But the criminals are just as innovative, and just as creative, so their attacks continue.

This is why it is essential to keep customers protected, by requiring strong passwords and multi-factor authentication. Some of the top loyalty programs targeted require nothing more than a mobile number and a numeric password, while others rely on easily obtained information as a means of authentication. There is an urgent need for better identity controls and countermeasures to prevent attacks against APIs and server resources.

The constant back-and-forth between defenders in the retail, travel, and hospitality industries and criminals isn't going away. It's up to the organizations themselves and their internal teams to sync up and work to stay ahead of the curve.

Security isn't a one-off purchase or control. It's a constantly evolving process that focuses on keeping the business going, or getting back to business as quickly as possible in the event that an incident has taken place, thus turning security itself into a service industry underneath the larger IT umbrella.

Methodologies

General Notes

The data used for all sections was limited to the same 24-month period – July 1, 2018, to June 30, 2020 – unless stated otherwise below.

Attack "Source" and "Target" Areas

For requests flagged as an application attack or credential abuse attempt, the source area is determined using the source IP address that connected to one of Akamai's edge servers and our in-house geolocation service, EdgeScape. Akamai leverages its massive network and high visibility to verify and maintain the geolocation data, which is 99% accurate at the country level.

The source of traffic should not be confused with attribution of attacker location. Attribution implies a determination of the location of the person or organization controlling the attack. It's relatively easy to say where the traffic came from, while it's extremely difficult to determine who caused the traffic to be generated in the first place without a dedicated team of researchers. Even then, it's nearly impossible at scale.

Given our definition for source area, one may assume that target area is determined by the IP address that received the malicious request, but that's not the case. If it were, the top target list would likely look pretty similar since Akamai edge servers are deployed in most countries. Instead, the target area of an attack is defined as the primary location of the customer that was targeted. Many organizations have a widely distributed network and services environment, and gathering data based on where data is being served from would be problematic on multiple levels.

The global ranking that is referenced for the source and target areas of these attacks is calculated by taking all verticals into consideration, as opposed to filtering it to a specific vertical such as commerce.

Web Application Attacks

This data 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.

The data 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 approximately 300,000 servers in 4,000 locations on 1,400 networks in 135 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.

DDoS

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. Similar to web application traffic, the source is determined by the source of the IP traffic prior to Akamai's network.

This data covered a 12-month period – July 1, 2019, to June 30, 2020.

Credential Abuse

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.

This data was also drawn from the CSI repository.

Credits

State of the Internet / Security Contributors

Editorial Staff

Martin McKeay
Editorial Director

Steve Ragan
Senior Technical Writer, Editor

Amanda Goedde
Senior Technical Writer, Managing Editor

Chelsea Tuttle
Data Scientist

Marketing

Georgina Morales Hampe
Project Management, Creative

Murali Venukumar
Program Management, Marketing

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/threatresearch

Access Data from This Report

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

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 10/20.