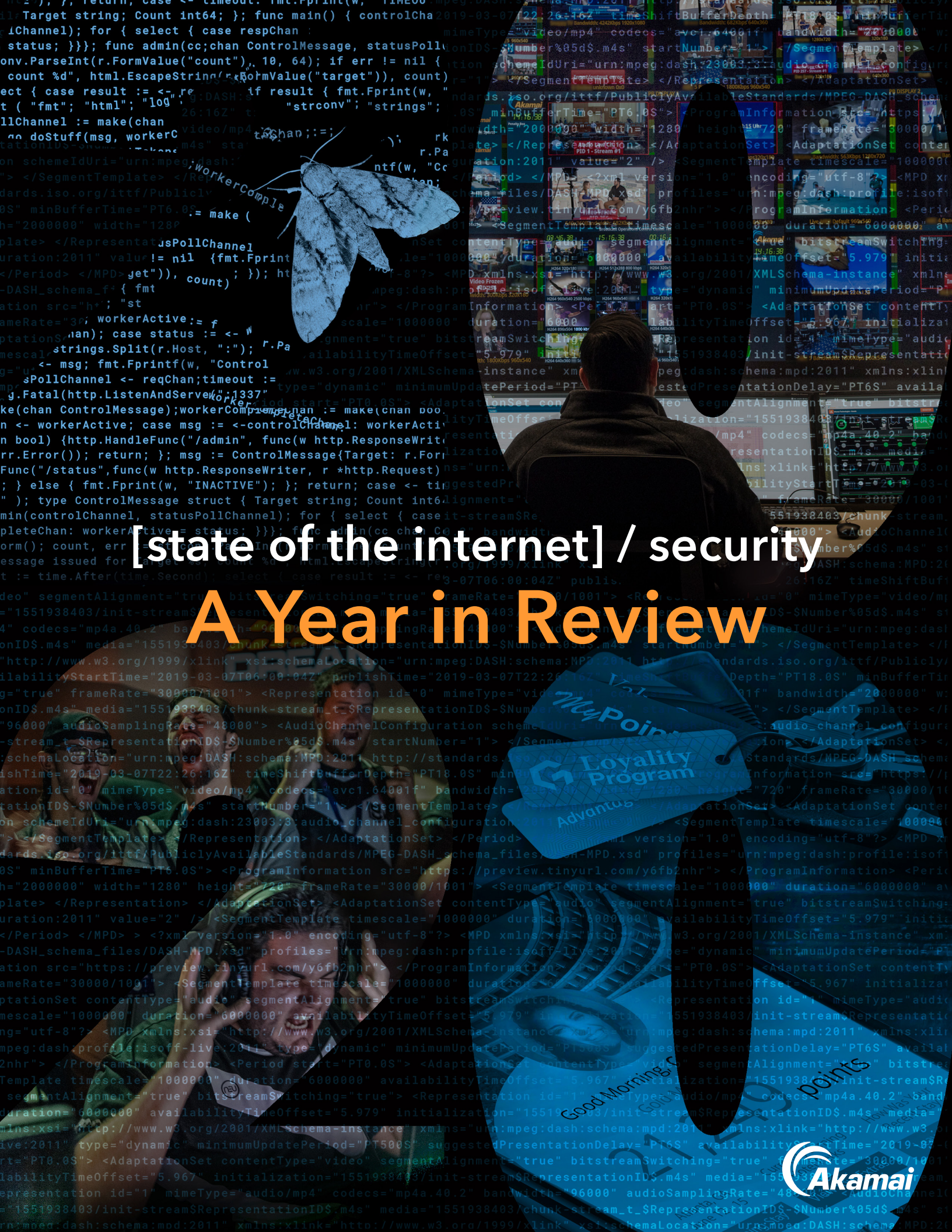
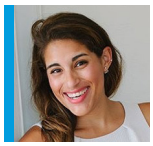

[state of the internet] / security
A Year in Review
Loyalty Program
Akamai

Table of Contents

Letter from the Editor



What a year it's been. If you are reading this – we made it to December 2020.

Just as the ink started to dry on those first pages of 2020, we opened up our first report with this:

> "As we look forward to the year ahead, the staff that produces the State of the Internet / Security report really only has one resolution – evolve. It's an interesting mandate, because we're not the only ones evolving. Criminals have started to evolve, and their attacks are getting more ambitious by the day."

No one could have predicted how much the world would "evolve" in the upcoming months.

This end-of-year report is our attempt to review a year that seems to have more chapters than your favorite book series. We look back at the reports that both were and weren't, and how COVID-19 impacted not only internet security and traffic, but the team as well.

Working with this team, through a pandemic, has really been nothing short of incredible. We did have the benefit of already working together remotely, since our team is spread out across Massachusetts, Indiana, and Florida, so we were able to transition into a "fully remote" team pretty seamlessly.

But what makes this team amazing is that we really were able to be there for each other, not just as coworkers, but as humans who were also living through a pandemic. Mental health days became something we all actively took, and asking how we were actually doing became a part of our weekly meetings.

We couldn't pretend the world wasn't changing. So, we didn't.

The silence between the releases speaks volumes. The State of the Internet / Security, Volume 6, Issue 1 (Hostile Takeovers – Financial Industry) report was published in February 2020, while the release of the State of the Internet / Security Special Media Edition got pushed to July 2020. The Special Media edition was meant to be published as part of our presence at NAB Show in April – which, like so many other events, was cancelled due to the COVID-19 lockdowns.

"You Can't Solo Security" and "Loyalty For Sale" were released about a month apart. We worked hard, we pivoted, and it's incredible to be able to see what this team was able to accomplish this year.

Thank you for continuing to read and support the State of the Internet / Security report. COVID-19 showed us that the world truly is online – and if it wasn't online before 2020, it is now. Internet security is now more vital than ever, and as we close out this year's chapter, we must continue to be vigilant as we turn the page into 2021.

Stay safe,

Amanda Goedde
Managing Editor

A Year in Review

Our year runs a little differently than the calendar. Picking up where the 2019 Year in Review left off means we are reviewing the biggest stories that we've covered, and then some, from October 2019 through October 2020.

October 2019

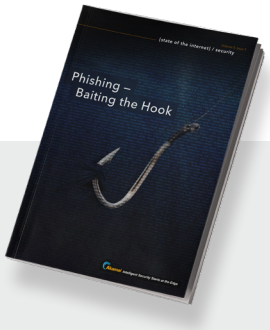
October had us on our toes, with Larry Cashdollar leading the way to help try to keep the greater internet community safe. Cashdollar's Drupalgeddon2 post reminded us that not everything is as it seems, since the attack ran code embedded inside a .gif file. While embedding code in an image file isn't a new attack method, this type of attack isn't popular or common. It was thanks to one of Cashdollar's honeypots that we were able to learn more about and witness a cryptomining SSH worm.

What's scarier than a cryptomining SSH worm? The release of State of the Internet / Security, Volume 5, Issue 5: Phishing – Baiting the Hook happened on Halloween eve.

November 2019

November ushered in a busy holiday shopping season and a fake Cozy Bear group making DDoS extortion demands. Multiple companies reported receiving an email demanding a sum of about $17,500 in bitcoin. If the payments were not made before the deadline, the email stated the price would increase by 1 BTC each day the demand isn't met, and a targeted DDoS attack will start.

While tax season was way in the rearview mirror, Or Katz did some close monitoring of a phishing campaign that impersonated the Internal Revenue Service (IRS). The campaign used at least 289 different domains and 832 URLs over 47 days. The same fake IRS login page was used in each instance, targeting over 100,000 victims worldwide.



State of the Internet / Security: Volume 5, Issue 5

Phishing: Baiting the Hook

State of the Internet / Security, Volume 5, Issue 5: Phishing – Baiting the Hook focused on the long term, socially based problem that impacts every industry. Chances are, if you do any sort of activity on the internet, you've seen a phishing attempt against one of your accounts. In this report, we dug a little deeper into the types of phishing and some trends that we saw across the Akamai platform. More than 60% of all the phishing kits monitored by Akamai were active for only 20 days or less – highlighting the quick lifecycle of phishing kits. High Tech was also the top industry targeted by phishing, followed by finance, online retail, and media. This report was also the first time we looked at how Akamai uses our own products to protect itself, specifically against phishing attacks.

December 2019 – January 2020

December through January is always full of possibilities. Toward the end of December in 2019, we set our goals and a publication plan for the upcoming year. By the time we came back to start the new year, we were ready to go.

In December, Katz gave us a look back at the recent Thanksgiving holiday, and how access patterns – as they pertain to enterprise applications, such as email or other SaaS platforms – were impacted during the holiday.

Around the world, people watched as the Australian wildfires relentlessly burned over 46 million acres. Little did we know that a severe cluster of cases of what was thought to be pneumonia, on New Year's Eve in Wuhan, China, would really change the planned trajectory of 2020.

February 2020

State of the Internet / Security: Volume 6, Issue 1

Financial Services: Hostile Takeover Attempts

Our first report of 2020 focused on takeover attempts in the financial services industry. Since money is often the main thing criminals are after, this report dove deep into web application attacks, credential stuffing, and other ways that bad actors are working to try to infiltrate financial services. 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.

Daily Web Application Attacks – Financial Services

October 2019 – September 2020

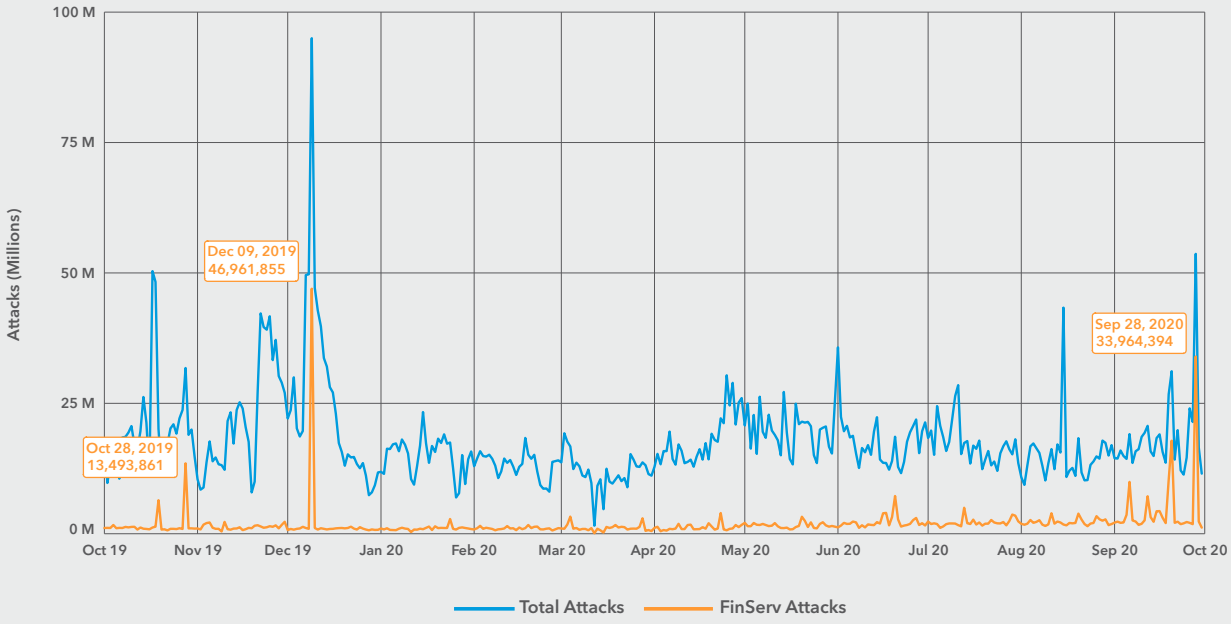


Fig. 1 – Automation is still playing a large role in the consistency of attacks against the financial services industry

October 2020 Update: *Updating the data from this report, we see that automation is still contributing to the consistency of attacks against the financial services industry. As the updated chart in Figure 1 shows, there were millions or tens of millions of attacks each day. There was a strong push in September 2020, representing more than 33 million web application attacks, as criminals focused their efforts on the common attack paths, including SQL Injection, Local File Inclusion, and Cross-Site Scripting.*

Danny Stern dove into his experience with a recruiting scam, and shares how to make sure that you don't fall victim to one. Truth be told, this post came at a time when the world was watching COVID-19 evolve from an epidemic into a pandemic, when many people's employment was placed in uncertain territory.

March 2020

Where do we start, "all you cool cats and kittens"?

On March 11, COVID-19 was officially declared a pandemic by the World Health Organization (W.H.O.), and on March 13 a national emergency was declared in the United States. Quickly, states began a lockdown that was originally planned for just two weeks. Businesses locked up, schools closed down, and toilet paper and hand sanitizer became hot commodities.

This team was almost through the final stages of the State of the Internet / Special Media Report when news came that the NAB Show in April was going to be cancelled. We decided to postpone the report, in large part because we felt that not including data from the latest quarter and the impact of COVID-19 would be disingenuous.

With many big projects and research being put on hold for a moment, the team took this opportunity to really figure out what this year might look like given the limitations of working during a global pandemic. Even more importantly, we needed to understand how we could balance research, writing, and our own physical and mental health.

> "This year caused me massive amounts of stress, and I know I'm not alone in that. Yet, working with this team was, at times, the only high point for me some days. Knowing someone had my back, or would catch me if I was to fall, was a massive boost to my mental health during the year."

Steve Ragan
Editor

April 2020

While the pandemic affected everyone worldwide, criminals took advantage of people's need for education, trusted resources, and information. Katz tracked down how some criminals were recycling phishing kits, and simply refreshing them to take advantage of the COVID-19 health crisis. He also tracked a specific phishing scam that used a three-question quiz to target people in Brazil.

"People are scared, and there is a fixation on information related to the pandemic. Fear is the key element for criminals running these scams, which are not limited to phishing alone," wrote Katz.

With more people than ever seemingly online, Martin McKeay took this moment to remind us that the internet wouldn't break under this increased traffic. Akamai Chief Executive Officer Tom Leighton said, "From our vantage point, we can see that global internet traffic increased by about 30% during the past month. That's about 10x normal, and it means we've seen an entire year's worth of growth in internet traffic in just the past few weeks. And that's without any live sports streaming, which continued to set new records prior to COVID-19."

We were able to observe a pattern of sorts – almost immediately after an isolation protocol was declared, there would be a spike in internet traffic. After a few days to a week, the traffic would normalize, still at an elevated rate, but significantly lower than the initial spike. The only place we didn't see that on a country level was the United States, since isolation protocols were decided on the state level.

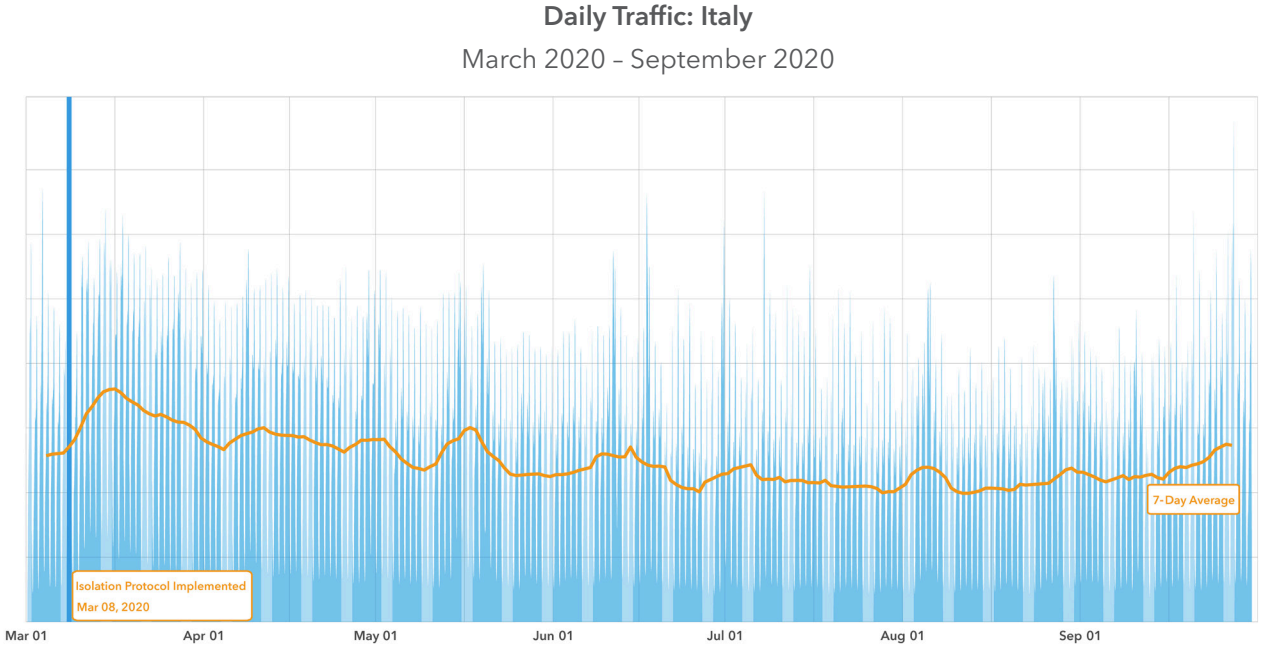


Fig. 2 – Updated data from McKeay's blog post, running through the end of September 2020

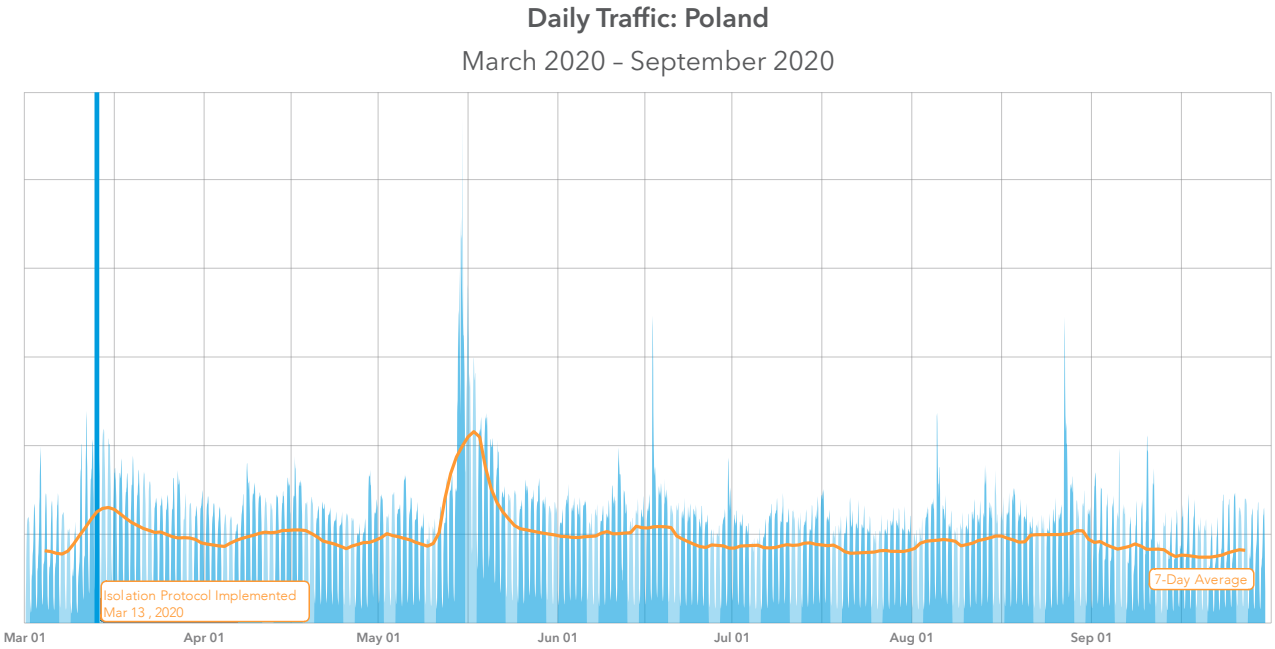


Fig. 3 – Updated data from McKeay's blog post, running through September 2020

October 2020 Update: *As shown in Figures 2 and 3, the new normal for traffic volume remained throughout the year, as organizations across the globe moved to remote access and availability. There were a few peaks, but mostly the traffic stayed exactly where we expected it to.*

On other fronts, Larry Cashdollar walked us through a brief history of rootable docker images, and Elisa Gangemi reminded us that in research, there is no such thing as failure – just learning opportunities.

> I had plans. You had plans. We all had plans for 2020. Being able to adapt to changing circumstances is an important quality no matter what you do, but this year we had to turn the adaption knob to 10. Then find out if we could squeak out just a little more. Turns out, the knob really does go to 11."

Martin McKeay
Editorial Director

May 2020

What was one of the first things to arrive on the scene in May? Murder hornets. Luckily, that's not a topic we had to cover.

A few days after the murder hornets took over the news, Steve Ragan dug deep into how criminals used their spare time during isolation to refresh their credential stuffing attacks.

> "...remote work became the norm. With that, remote access to applications and services started to gain momentum – as more and more people turned to the internet to get things done. Yet, many of those turning to their favorite application, game, or web-based service chose to trade security for ease of use and access. This created an attack surface that criminals wasted no time taking advantage of."

Credential stuffing has been one of our main focuses for over a year because it's a problem that affects every organization, regardless of size. The best defense? Using a password manager and unique passwords. It's one of the few instances where recycling is not encouraged.

McKeay also wrote about the 13th iteration of the Verizon Data Breach Investigation Report that Akamai had the opportunity to contribute to for the past five years. Being able to collaborate and contribute data allows everyone to "win," by broadening our scope of view and being able to see if the trends we see are also seen across other providers.

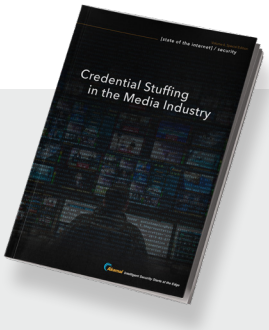
June 2020

As the world trepidatiously started to reopen its doors, the team came up with an executable plan for the rest of the year.

Cashdollar also discovered that malware called Stealthworker, which can target both Windows and Linux systems, had been installed in one of his honeypots. "Written in Golang, once a system is successfully infected, the attackers will use it to probe other targets in an attempt to spread and continue the brute force operations. Stealthworker is capable of running brute force attacks against a number of popular web services and platforms, including cPanel / WHM, WordPress, Drupal, Joomla, OpenCart, Magento, MySQL, PostgreSQL, Brixt, SSH, and FTP," Cashdollar wrote, before diving deep into his research findings.

> "Joining a new team during a global pandemic could have meant added stress, but joining THIS team thankfully resulted in the opposite. I was warmly welcomed, was given the opportunity to take care of myself and my family, and have already learned a lot in just a few short months. I look forward to seeing what next year brings!"

Chelsea Tuttle
Data Scientist



July 2020

State of the Internet / Security: Volume 6, Issue 1

Credential Stuffing in the Media Industry

After a three-month publication delay and a rewrite, the State of the Internet / Special Media Report: Credential Stuffing in the Media Industry finally saw the light of day. This report acts like a time capsule, with the majority of the original report still intact. However, we went through and added in relevant updates to the data to reflect the current state of how the internet is being used and threats that are being seen.

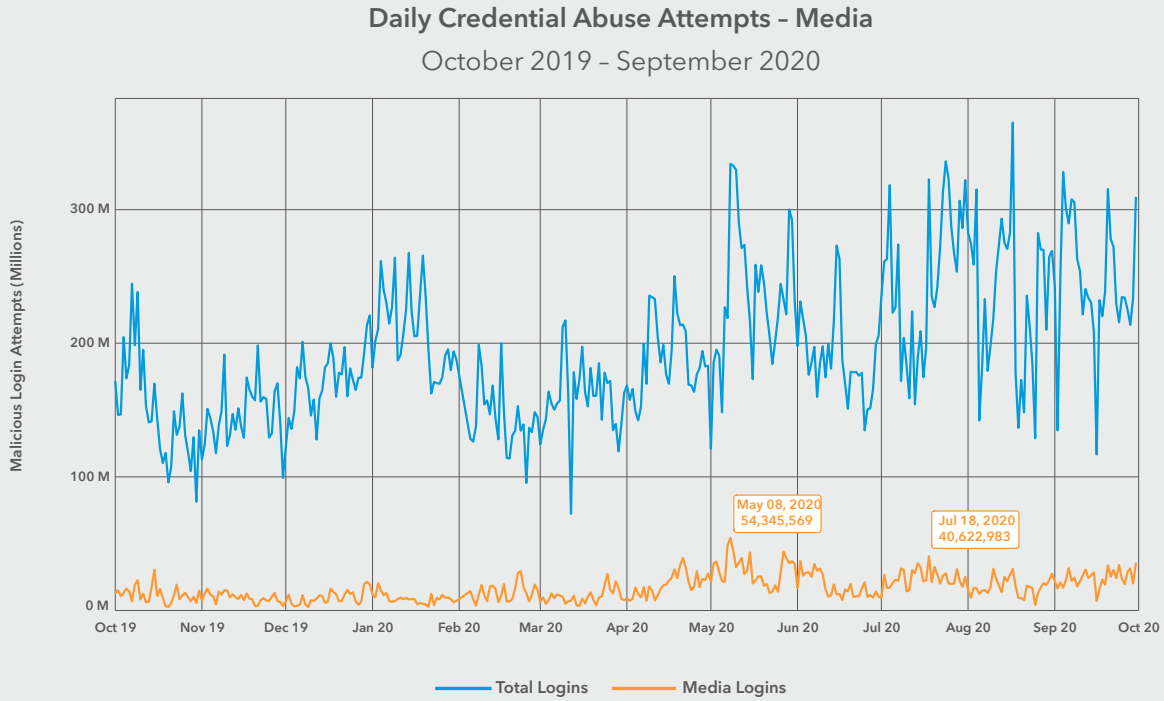


Fig. 4 – Updated credential stuffing attacks against the media vertical through September 2020

October 2020 Update: *Technically, Figure 4 represents the second set of updates for this report. Like before, we can see a steady stream of attacks against the video media industry, ramping up toward the end of Q2 and continuing on through the end of Q3. The peaks and dips are expected, as criminals still continued to churn their credential lists.*

Toward the end of August 2020, one of the largest darknet marketplaces (Empire) went offline. The cause of the shutdown remains unknown, but the sellers scattered to other marketplaces, resulting in a dip in credential stuffing in the early days of September. The resurgence of attacks can be linked to the flood of freebie credential lists, which were used to establish reputation and legitimacy among criminal clients. At the time this report was written, credential stuffing against the media industry, with a focus on account takeovers, remained steady with tens of millions of attacks per day.

Credential stuffing, as mentioned before, is an issue for all businesses, no matter which industry. However, take this as just another reminder to make sure all your passwords are unique!

Recycled passwords are not the only threat that we looked at in July. Katz revisited the "forgotten" three-question quiz phishing attacks. These attacks rely on users filling out these quizzes in exchange for a "prize," which often results in stolen personal information.

As part of this research, Katz tracked 1,161 websites hosting phishing toolkits between July 2019 and May 2020 that targeted 130 brands and had more than 5 million victims.

August 2020

Throughout August, the Akamai Security Intelligence Response Team (SIRT) was tracking ransom demand DDoS attacks from criminals claiming to be part of the Armada Collective and Fancy Bear.

Sound familiar? It should, because it is a remake of an old script with new actors. The initial contact starts with a threatening email, warning of an impending DDoS attack against their company unless a ransom is paid in bitcoin. The wording of the extortion letters is very similar to the letters published in the media during past campaigns and similar to the last DDoS extortion campaign Akamai documented in November 2019.

> This year really showed me that the team you are on really matters. Being on a team that works really hard, and is really, really smart, is great. But being on a team that works really hard, is really, really smart, AND cares about each other's mental and physical well-being, really, really makes a difference."

Amanda Goedde
Managing Editor

State of the Internet / Security: Volume 6, Issue 2

Gaming – You Can't Solo Security

It was a long time coming, but September marked the release of the State of the Internet / Security, Issue 6, Volume 2: Gaming – You Can't Solo Security. This report was different from every single report that came before it, because we decided to write this report for gamers and for those who were outside of the security realm. We collaborated with digital event company DreamHack to create a survey that would allow us to get some insight into how gamers feel about the current state of security in gaming. While surveys aren't the type of data we typically deal with in reporting, we wanted to understand how gamers picture security and how that relates to the type of attacks that game companies see on a daily basis.

At its core, the most vulnerable and most targeted element of the gaming industry is its players. The human element is always the hardest to control and secure, so this revelation isn't a surprise. More than half of the frequent players said they've had their accounts compromised, but only one-fifth of them were worried about such things.

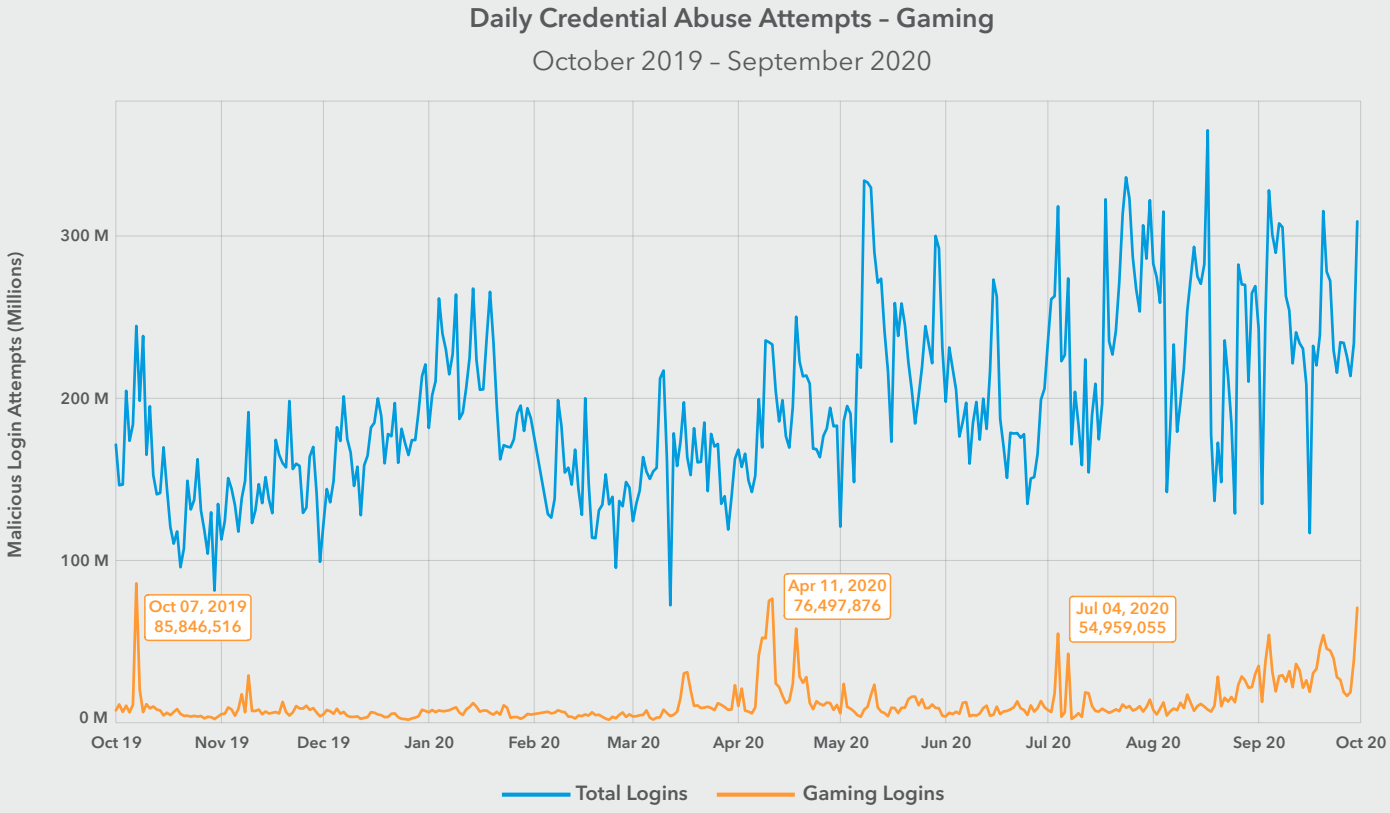


Fig. 5 – Update to the daily credential abuse attempts against the gaming industry, through September 2020

October 2020 Update: *The gaming industry saw attack patterns that mirrored those in the video media industry, as attacks peaked in July (55 million), but bottomed out when Empire fell offline. The attacks are tracked in Figure 5.*

The collapse of the darknet marketplace hit criminals focusing on gaming credentials hard, as they needed to scramble to find a new place to offload their collections. However, when they reestablished themselves toward the start of September, they shifted their collection offerings from game titles and game platforms to both – offering them as general collections and targeted collections. This change led to a spike in attacks, which continued to climb in October as criminals focused on the holiday season, which will see an influx of new gaming platforms and titles.

Since many on the State of the Internet team are gamers, this report was a meaningful dive into a world that many of us were close with. Especially when we, and others around the world, turned to gaming as a way to re-create that sense of camaraderie and community that seemed very distant during the height of COVID-19 isolation protocols.

October 2020

Guess what? Murder hornets are back, and researchers were able to capture a bunch of them out in Washington state.

It also was National Cybersecurity Awareness Month, and our researchers and team members on the Information Security Team took the time to dive into some of the many aspects of security that impact all of us.

Cashdollar took us back 20 years, and recounted his very first CVE for us, while describing what has changed and what has stayed the same. Another team member wrote an open letter to their parents, talking about why it's so important to use complex passwords and keep them in a safe place (remember, recycling passwords is not a great idea). Nick Caron outlined how to keep the security at home safe, in just three steps. Hieu Vuong shared with us how her brother almost fell for a COVID-19 phishing scam, and reminds us of where the best places to get information are. Eric Kobrin also reminded us that zombies aren't just limited to horror movies, but they can also be your IoT devices once they are past their prime.

State of the Internet / Security: Volume 6, Issue 3

Loyalty for Sale: Retail and Hospitality Fraud

also launched. Continuing the theme of credential stuffing and exploiting personal information, this report dives a little deeper into how these industries' rich loyalty programs became targets for criminals looking to make a quick and easy buck.

> You never know what you can do until you try, or so the saying goes. No one knew we could publish dozens of blog posts and multiple issues of our report, all during a global pandemic."

Martin McKeay
Editorial Director

Looking Forward

It's been one heck of a year, for everyone, in every single industry.

If this year has taught us anything, it's that we all can dance with uncertainty for a little bit. However, it's the teams and the people who you interact with daily that can help bring back a smidge of certainty.

So, as we start to see 2020 in the rearview mirror, let's take a moment to appreciate where we are. This year was full of learnings, not just about how attackers are leveraging fear and uncertainty to create more havoc, but about how a remote and digital world could and can function.

There was a pretty big learning curve as schools, businesses, and people started to transition from face-to-face time to face-to-screen time. There was also a big learning curve in boundary setting, since homes are now also offices, schools, activity centers, and more.

We're all learning together.

But there are a couple of big takeaways from this year: Wash your hands and don't reuse your passwords.

Methodologies

General Notes

The data used for all sections was limited to the same 12-month period – October 1, 2019, to September 30, 2020. The majority of this report was drawn directly from previous reports this year, so feel free to visit the individual reports to get detailed information on how each report was compiled.

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.

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.

DDoS

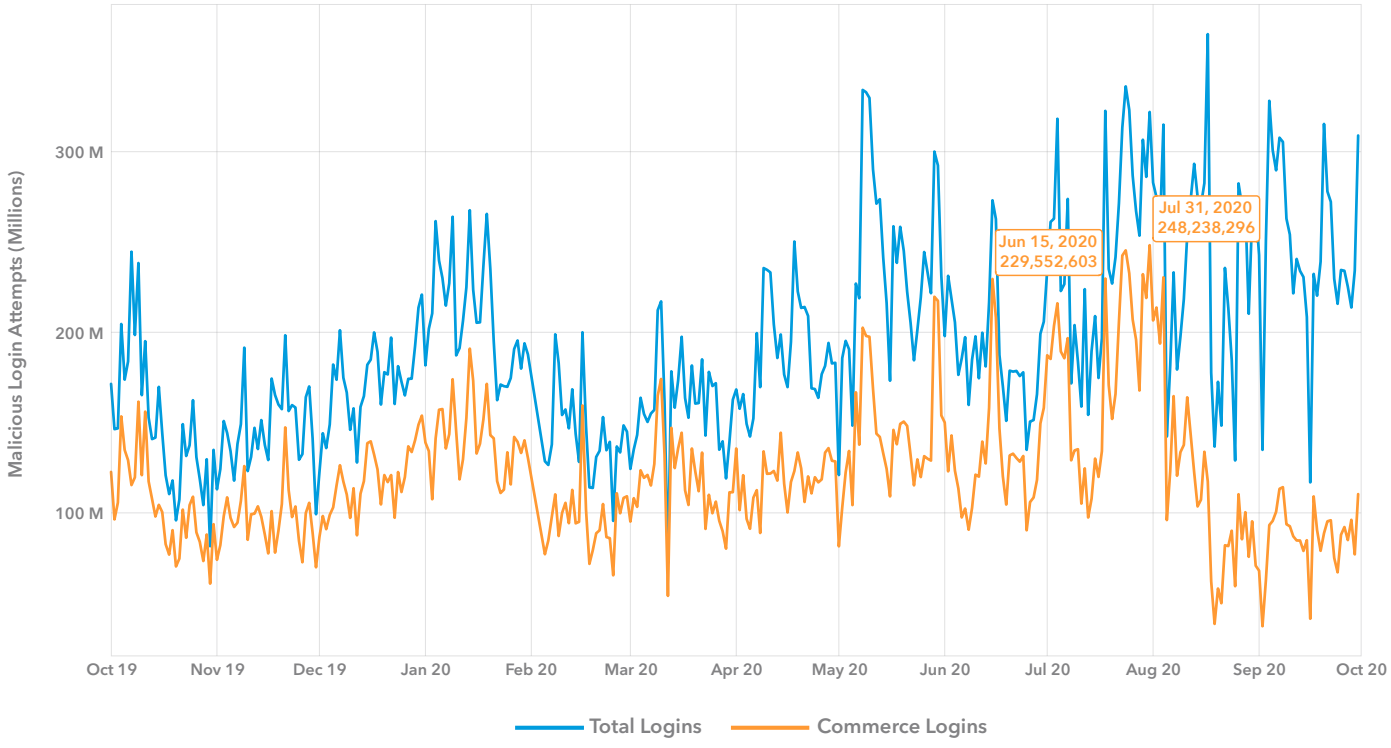
Prolexic Routed defends organizations against DDoS attacks by redirecting network traffic through Akamai scrubbing centers, and only allowing the clean traffic forward. Experts in the Akamai security operations center (SOC) tailor proactive mitigation controls to detect and stop attacks instantly, and 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.

Additional Data

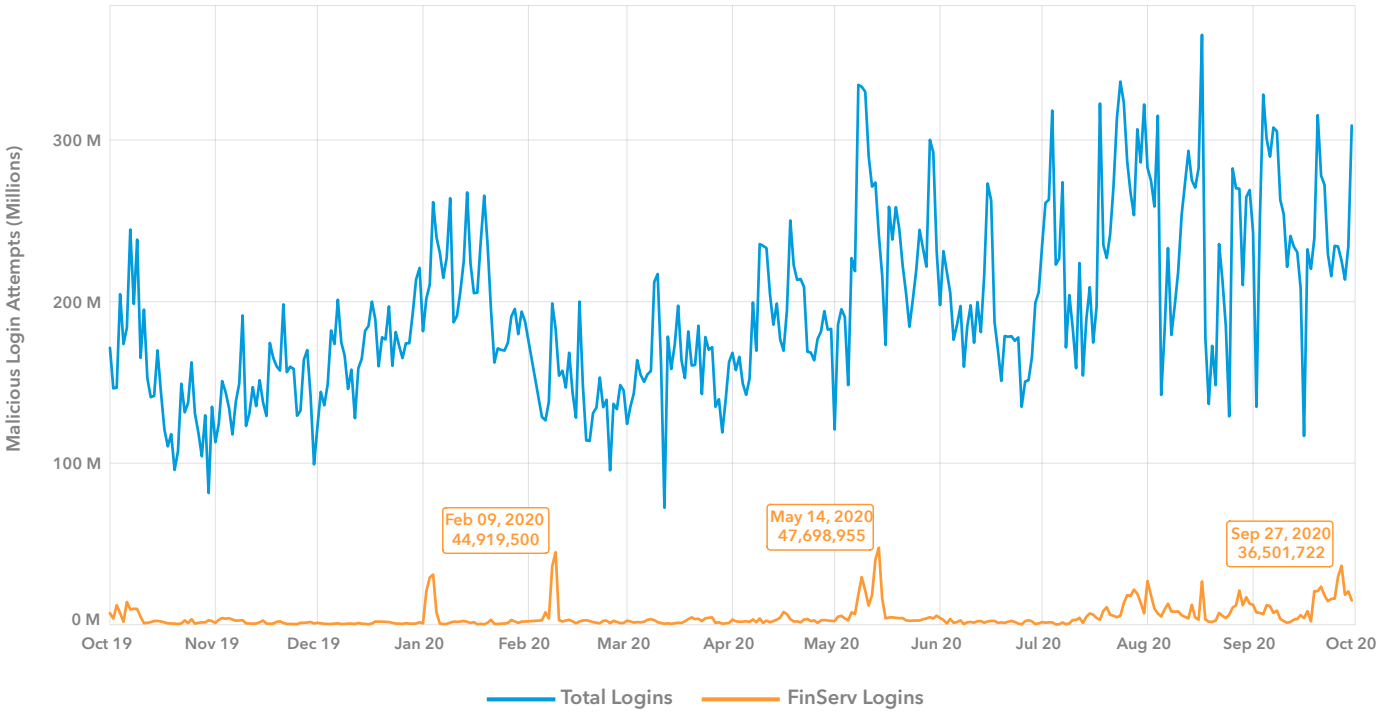
Daily Credential Abuse Attempts – Commerce

October 2019 – September 2020



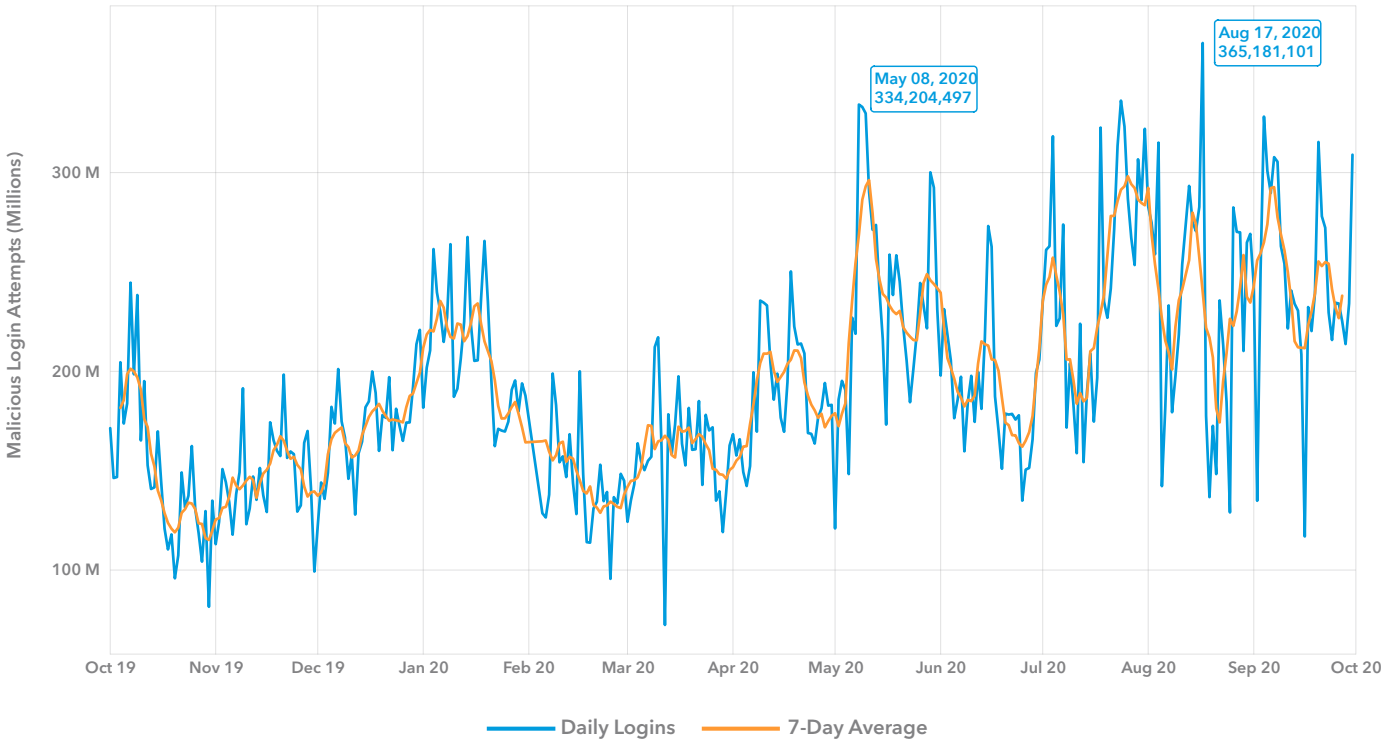
Daily Credential Abuse Attempts – Financial Services

October 2019 – September 2020



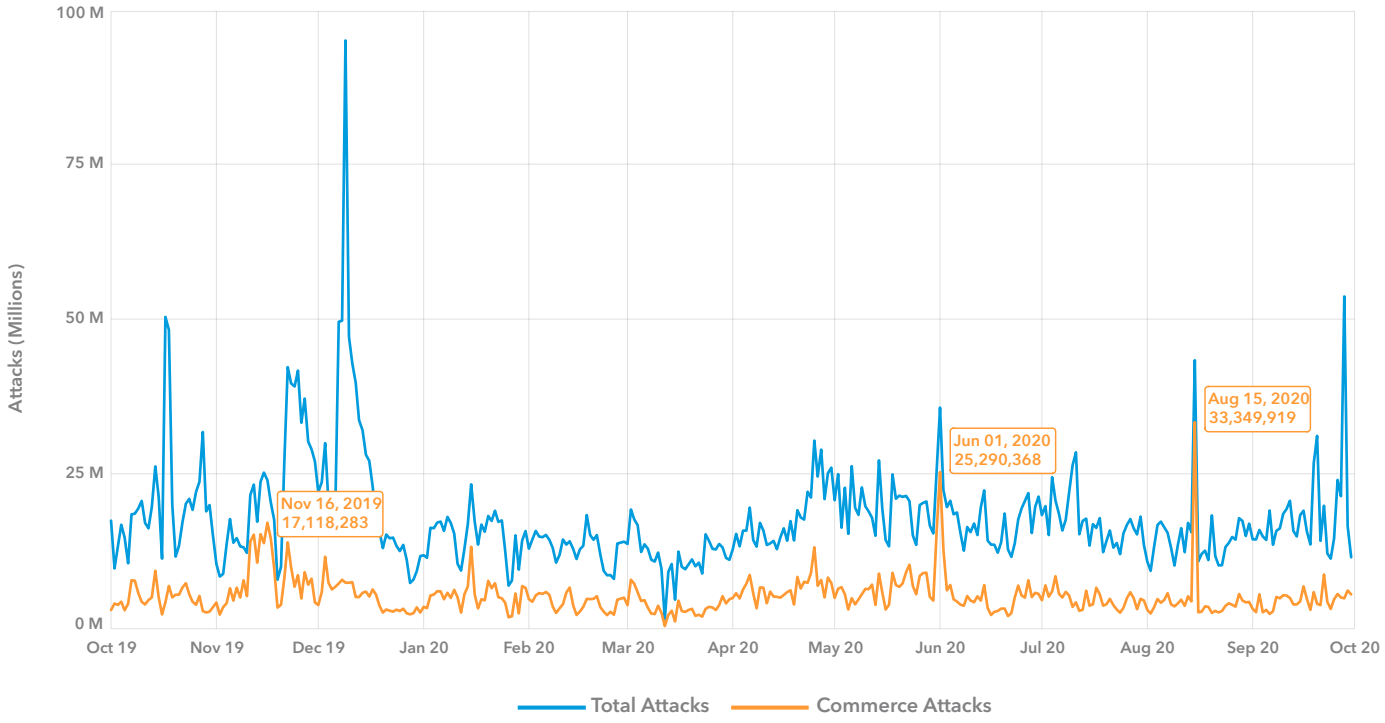
Daily Credential Abuse Attempts

October 2019 – September 2020



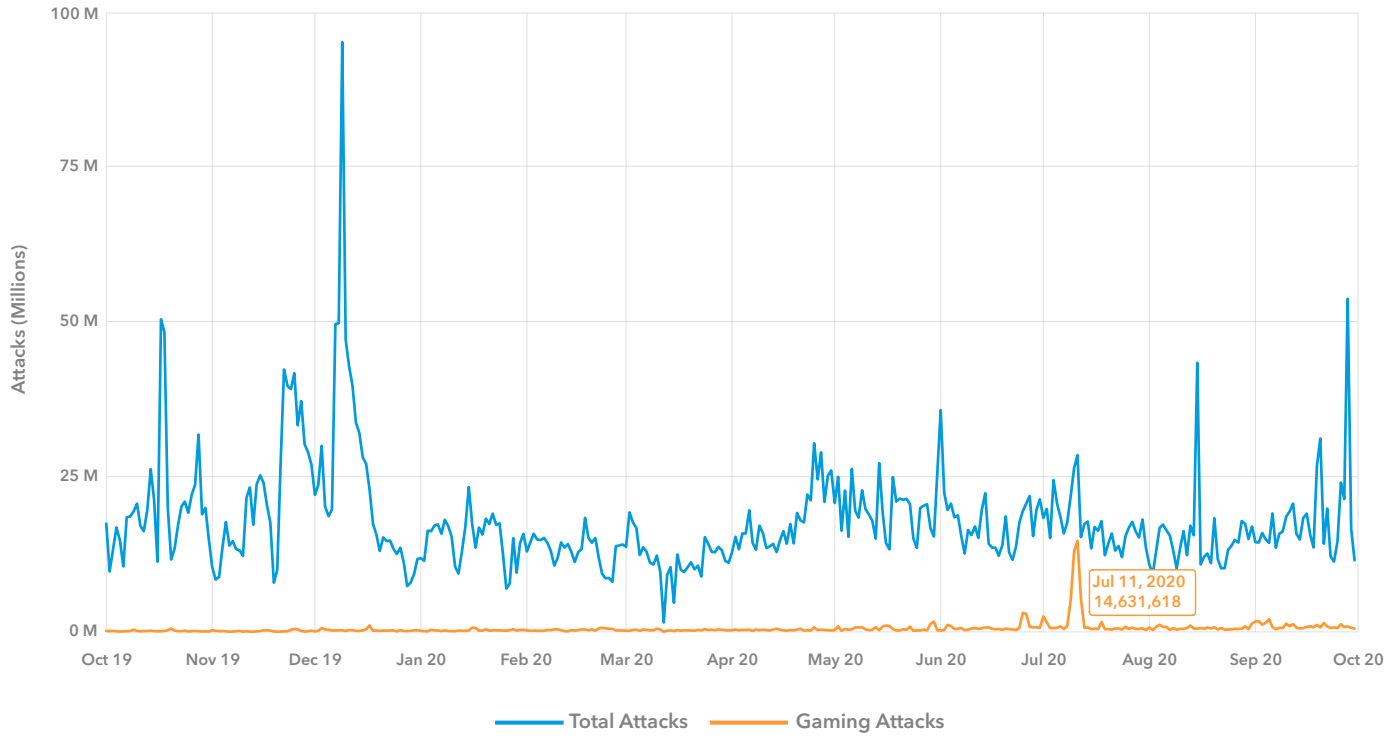
Daily Web Application Attacks – Commerce

October 2019 – September 2020



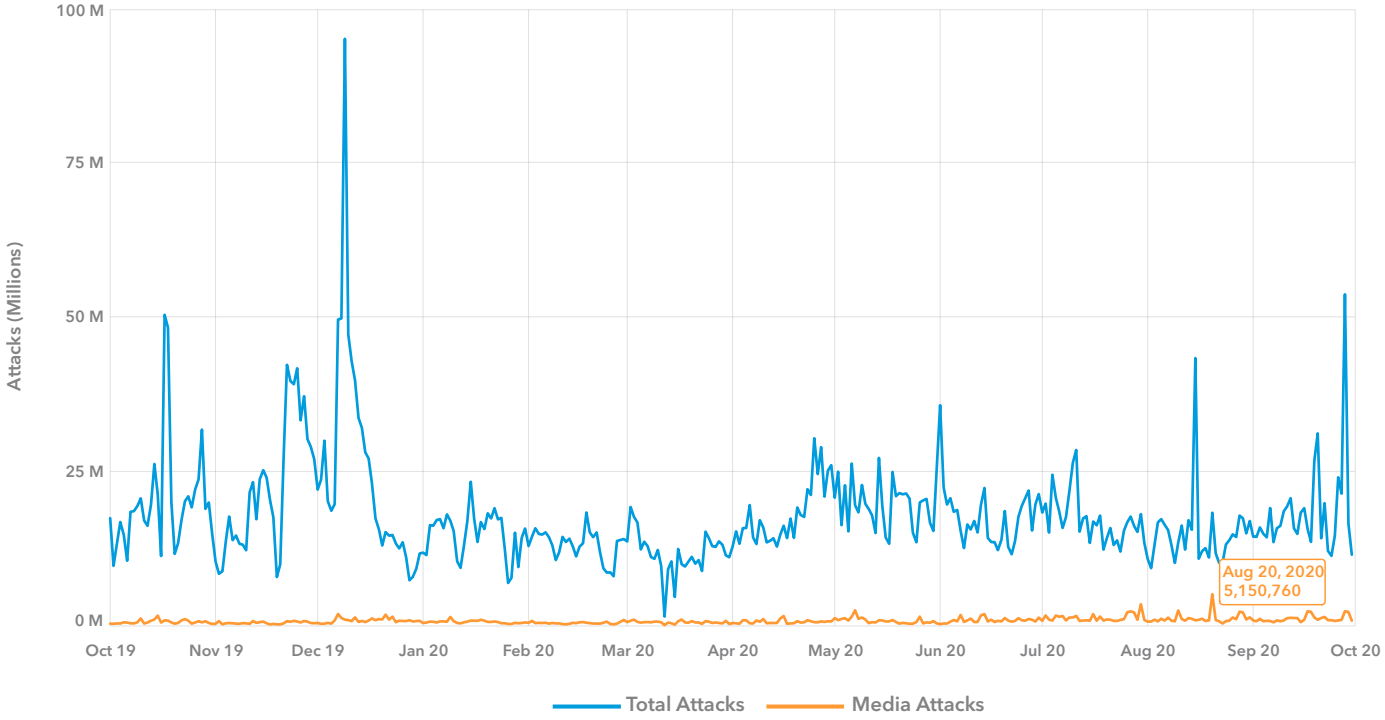
Daily Web Application Attacks – Gaming

October 2019 – September 2020



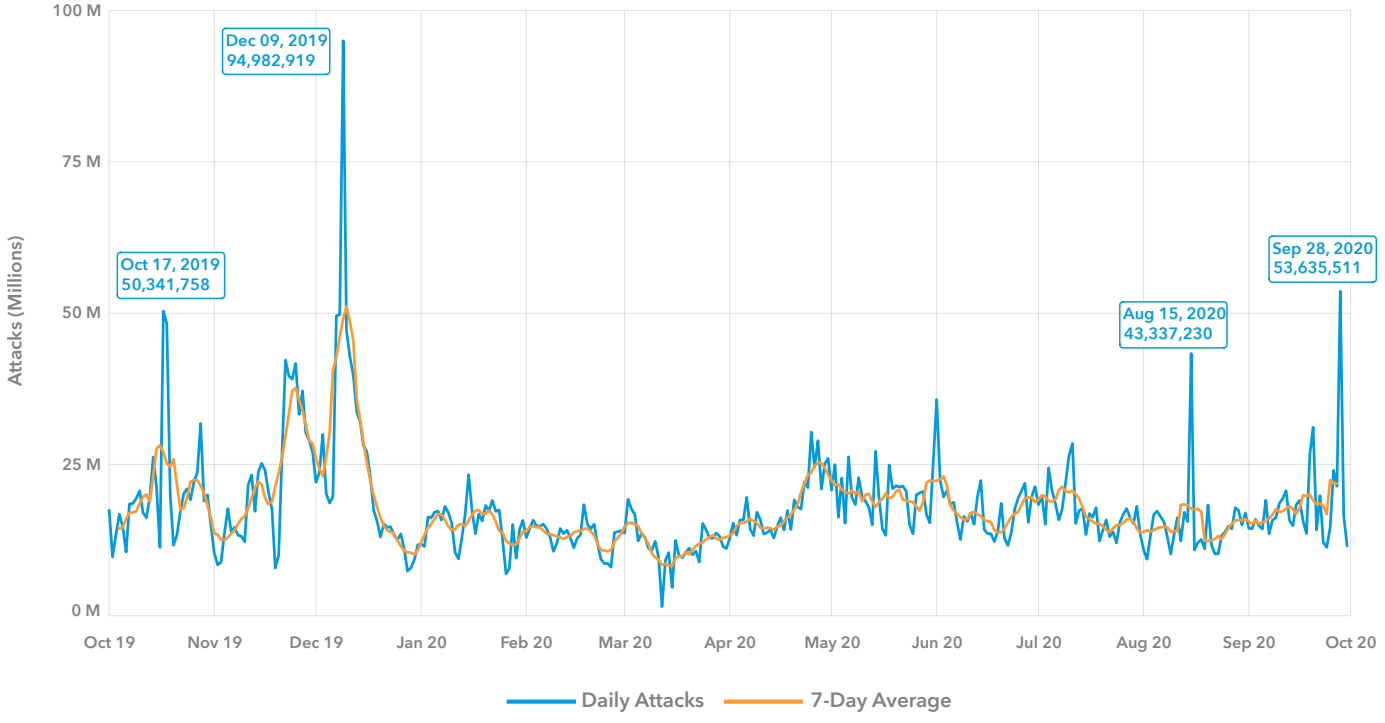
Daily Web Application Attacks – Media

October 2019 – September 2020



Daily Web Application Attacks

October 2019 – September 2020



Credits

State of the Internet / Security Contributors

Editorial Staff

Martin McKeay
Editorial Director

Steve Ragan
Senior Technical Writer, Editor

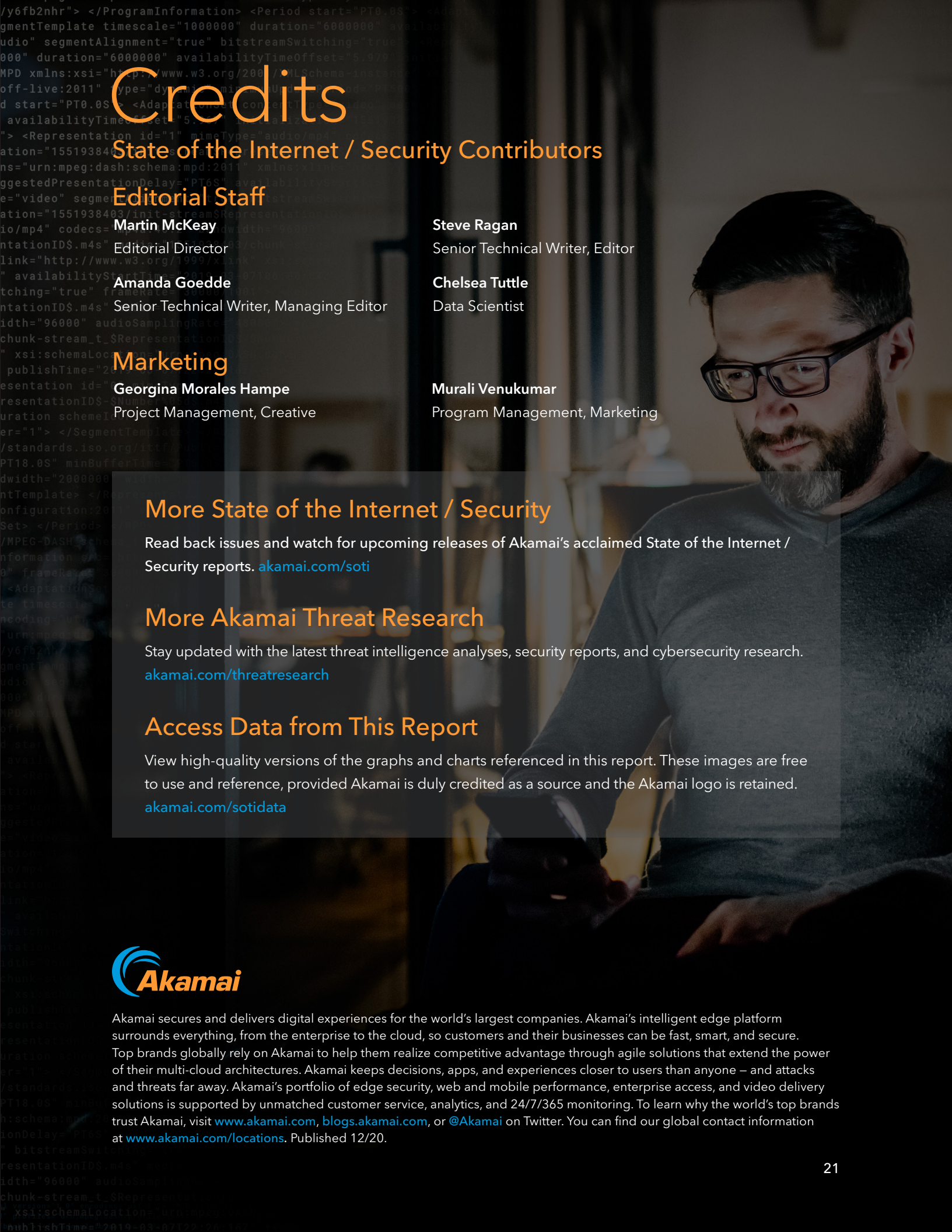
Amanda Goedde
Senior Technical Writer, Managing Editor

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

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 12/20.