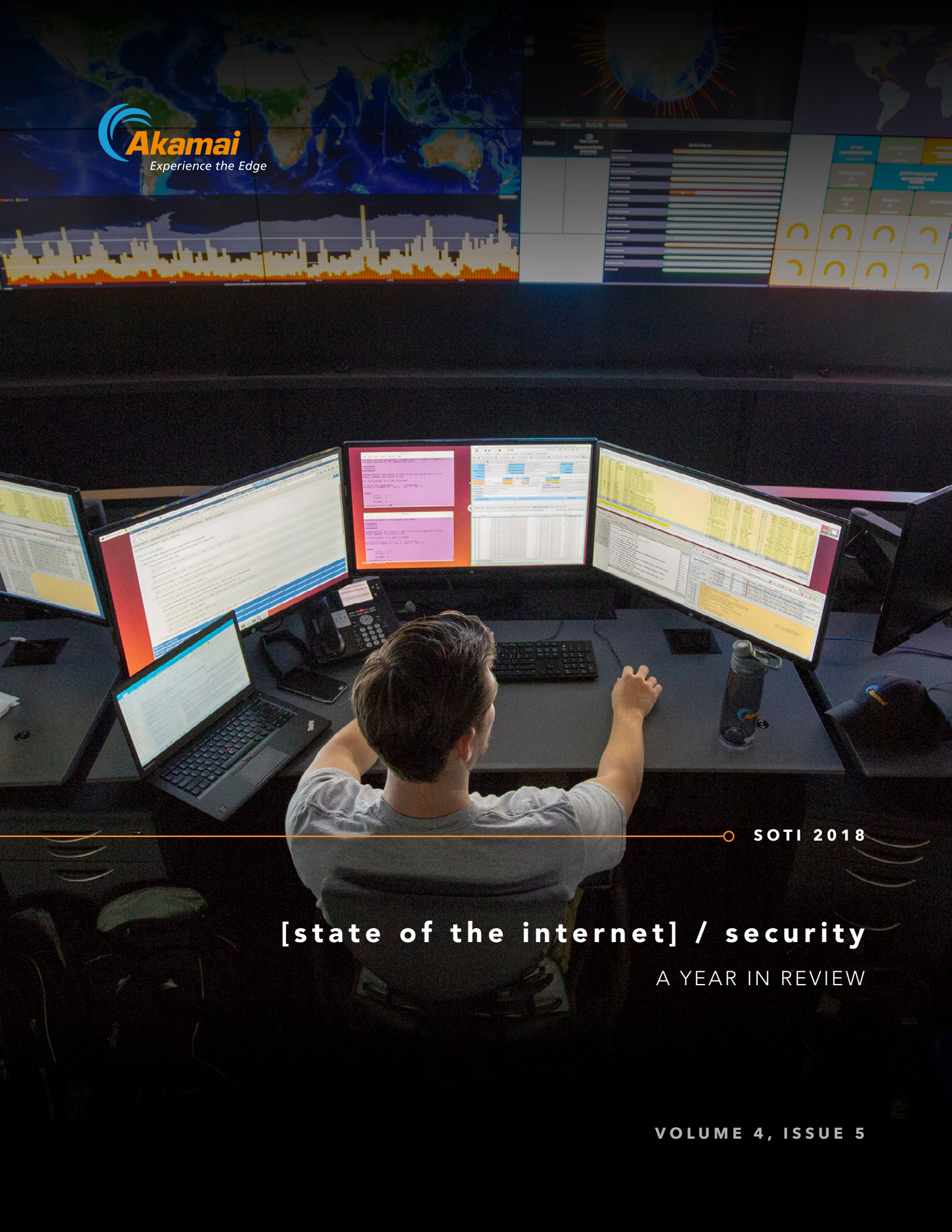


SOTI 2018

[state of the internet] / security

A YEAR IN REVIEW

VOLUME 4, ISSUE 5

TABLE OF **CONTENTS**

LETTER FROM THE **EDITOR**

Another year is quickly drawing to a close. In this issue of the State of the Internet / Security report, we decided to look back at some of the events we've been part of and the research our teams produced in the past 12 months. We're also examining a few of the stories that formed the background in security this year. It's easy to forget how much has happened.

The State of the Internet / Security report has evolved significantly in the past year, with the aim of creating a more interesting and engaging report. We're no longer just a DDoS and web attack report — we cover DNS, bots, and the whole spectrum of security topics that working at Akamai allows us to research. We've also moved from a strict quarterly cadence to a goal of releasing six (or more) reports a year.

One of the biggest changes we've made is to tell stories in place of talking about statistics. Our goal is to give readers the context and implications of the problems and challenges we see. We're still publishing information like attack types and counts, but they are being published to our blog instead. Readers have made it clear that the global numbers are important, but the details of individual attacks are key to understanding the impact to their own environment.

We've invited our Chief Security Officer (CSO), Andy Ellis, to write an analysis of the trends in the security industry and where they might impact us in the coming year. These aren't necessarily "predictions," but the insights of a veteran of the security industry with over two decades of experience. One of the many things that makes our CSO different than most is that he's been leading our security efforts for 15 years, making him one of the longest-tenured security executives in the industry. This gives him both a historical perspective and the practical experience to understand where we've come from and where it might lead us in the future.

There's no doubt that 2018 has been an interesting year for security professionals around the globe, and 2019 is likely to accelerate the changes we're already seeing. Five years ago, our industry was still struggling to garner attention from business units we support. Today, information security is a major topic of conversation at nearly every organization. That change hasn't been without a few growing pains. Sometimes a lot of pain.

Looking back at the path we've traveled over the past year is a vital step in planning for the year ahead. What lessons are you taking from 2017 and 2018 as we move into the future?

Office of the CSO

plus ça change, plus c'est la même chose

— Jean-Baptiste Alphonse Karr

If there is a single truth about trends in the Internet security space, it's that every year brings more of the same. In 1998, during Operation Desert Fox, adversaries used a distributed denial of service attack, which also leveraged the teardrop vulnerability, to attempt to bring down USCENTAF networks (I was the defensive engineer on duty at the time, so I remember the excitement of identifying the attack, testing a config, and pushing it out to our perimeter security systems). This isn't strategically different from actions taking place in our, and other, Security Operations Centers every day — only the scale and automation have changed.

So as we look forward into 2019, it is easier to note ongoing patterns from the past few years, suggest they'll continue, and surmise that they'll likely continue to evolve mostly in the ways that they have been advancing.

Brute-Force DDoS

DDoS is always a great place to start, mostly because the trends in DDoS are remarkably stable. It might be easiest to think about attacks along two different axes: leverage and bandwidth. Bandwidth is simply the measurement of traffic an adversary can generate at any given time. Historically, we've seen the size of the largest attack grow by about 9% per quarter, which nets out to doubling every two years. But, fascinatingly, that isn't a continuous growth. A new peak gets set — along that 9% QoQ curve — whenever an adversary discovers a new way to build a botnet or reflection, as in the case of Mirai or memcached reflection attacks.

Between new peaks, two things happen. First, affected parties, like systems administrators and ISP operators, take action to reduce the number of systems available for use in attacks. Second, adversaries begin to fight for control of these resources, and we see botnets begin to fragment, causing individual attacks to become smaller.

From an effectiveness standpoint, this isn't actually detrimental to the attacker. DDoS defense styles don't generally scale linearly in size. The largest attacks occur at the edge of the network, where services like Akamai's Kona Site Defender or Prolexic Routed live. Mid-tier defenses live in the core of ISPs, providing "clean-pipe" services to site owners. The smallest defenses, on-prem solutions, live solely inside target data centers. For an adversary whose botnet isn't large enough to target an edge-based defense, an attack on someone using only data center-based defenses can still be effective — even at a hundredth of the size.

Given that bandwidth-based DDoS attacks come in many shapes, it's interesting that the maximum size of the attacks appears to be constrained by a 9% quarterly growth curve. Interesting, but not inexplicable. Rather than being caused by some naturally occurring limit, the most likely explanation is that the underlying growth of the Internet limits the aggregate capacity of botnets. The Internet's capacity attenuates the total throw weight a DDoS attack can generate; the farther a target is from components of a network, the less traffic that will make it across any congested links between the target and the attack source.

Application-Level Attacks

While bandwidth is the axis of DDoS most people think about, leverage is as critical in many ways. Leverage is simply a measure of how effective an individual attack is compared to the amount of traffic generated. The higher the leverage of an attack, the more "damage" that can be done with the same amount of traffic. A pure-bandwidth flood generally has very low leverage, as an attacker

is, at best, simply trading resources with defenders: Each network card used in the attack suppresses one network card in defense. Worse (from the adversary's perspective), many bandwidth floods are cheap to defend against, with filtration happening upstream in commodity routers. High-leverage attacks are much more interesting, and are often called "low and slow" attacks in the taxonomy of defense. The Slowloris attack is a perfect example: An adversary with a handful of systems can effectively shut down massive web server farms.

From an attacker perspective, high-leverage attacks are amazingly powerful but don't tend to have the useful life of high-bandwidth attacks. Rarely do high-leverage attacks exploit fundamental architectural flaws; instead they target engineering defects or oversights in places where resource management was missed. These oversights are generally correctable. But, like any arms race, as new techniques are discovered, they are put into the field, work for a while, and are then discarded once corrective action is taken. "Discarded" means small botnets still use these techniques a decade after they've been officially "patched," targeting the long tail of ill-maintained systems.

Credential Stuffing

But DDoS isn't the only tool that attackers use, even if it's the one everyone notices when it works (like the Dyn outage a few years ago). Attackers also want to gain access to systems in ways that aren't just about outages. Take the latest high-profile attacks in the world of account takeover, which often begin with credential stuffing. This attack relies on the greatest weakness of the web: passwords. Users, faced with the challenge of managing accounts on dozens of websites, often reuse a few passwords across multiple accounts.

Adversaries take aim at these reused passwords. They begin with a collection of known usernames and passwords, often released as part of a data breach. The system that was originally breached is irrelevant; whether it was a social network or a retailer, sam.gamgee@shiremail.middleearth (password: R0s!3Cotton) still represents a set of known good credentials. Credentials from multiple sites are often combined into larger data sets openly traded between attackers.

This database of credentials is fed into a botnet, where various machines in the botnet will try to log in using each of these credentials. The majority of credentials don't work — that's expected. But if a username and password do work? Now the adversary can either attack the target directly, or, more likely, add the credential to a list for sale to another adversary. Some of these credential stuffing botnets try the logins very quickly, creating a noticeable spike in failed logins. This makes it relatively easy for a website to identify the attacker's botnet and filter it out. But many adversaries program their botnet to engage in "low and slow" scanning, to fly under the radar of velocity-based detection engines.

The Gig Adversary

A particularly interesting development over the past few years is the "selling the good credentials to another adversary" part. Historically, most adversarial groups acted with steep vertical integration, doing tasks from building botnets to compromising systems. For various reasons, the adversarial market has moved further and further to something akin to a "gig" economy. Many adversaries specialize in one component of the hostile ecosystem, and "buy" access to lower-level data (like data breaches), and then, after conducting a round of credential stuffing, can sell a list of accounts ready to be taken over. While this isn't a new model, the increasing use of it — to create booter networks or validate stolen credentials — heralds an increasing marketization of the adversary landscape. And marketization tends to bring even greater economies of scale, as specialists drive efficiencies into their components of the market to defeat their competitors. So we should expect to see further specialization and monetization.

Cryptocurrencies and Exchanges

No 2019 lookahead would be complete without considering blockchain (or really, cryptocurrencies). While blockchain has yet to make serious inroads outside cryptocurrencies, the increasing value of cryptocurrencies has also brought adversaries. While some adversaries aim high — attacking cryptoexchanges or making 51% attacks — others aim small. The rise of cryptojacking, the insertion of adware-based cryptocurrency mining software, is an example of adversaries targeting the lower end of the continuum. By buying ads directly, inserting them through adware, or injecting them into unsecured HTTP connections, attackers can monetize your processing power for themselves. But doing it at a scale makes it worthwhile.

In a sense, this was the logical next step, moving from running long-term cryptominers on compromised servers, and converting to a gig-based attack economy.

Protecting Forward

These attack techniques — and the myriad of techniques I skimmed past in the interest of reducing word count to something tolerable [you didn't succeed. --Ed.]— will continue, and spread, evolving into yet more attacks that look similar from a casual glance. In many ways, that's a good thing. Robust security and safety programs might be looking at revolutionary security changes, like moving to a zero trust security system. Others might be considering small evolutionary changes, like an increased focus on bot management. But the fundamental safety philosophies that have been effective in the past will serve us as good guides into 2019 and beyond. The philosophies that haven't yet worked? Those are likely to continue not working.

12 Months of Stories

Looking at a year's worth of news and research is never an easy task. Deciding which topics were important and impactful is highly dependent upon the point of view of the person doing the evaluation. Our efforts focus primarily on the stories we were telling at Akamai, but we also wanted to look at a few of the stories that you might have missed or forgotten. Looking back, there have been some amazing changes since last November. There have also been more than a few stories that could have been from any year in the past decade.

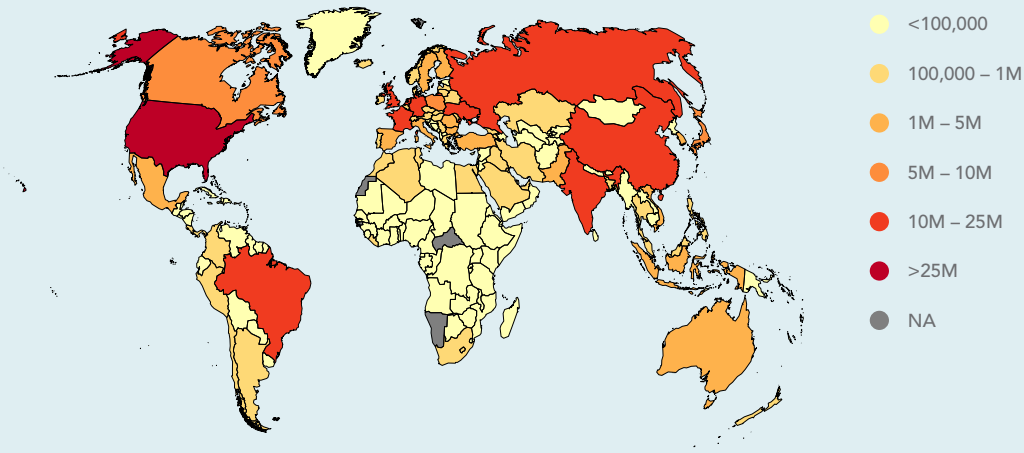
November

In November 2017, Akamai added a new organization to our enterprise, Nominum. As an organization specializing in protecting users at the enterprise and carrier level, Nominum had a different view on security than Akamai's current tools. Instead of blocking attacks at the core, Nominum examines DNS requests and blocks traffic to botnet command and control (CnC) structures by blackholing the domains they use.

The team of data scientists at Nominum were no strangers to research, and several days after they joined Akamai released their Data Revelations Nominum Data Science Security report. The report leaned heavily on the research the team was doing to provide protection to customers and examined multiple aspects of how DNS is being used in phishing, botnets, and malware.

At nearly the same time as the Nominum team was releasing their report, we released the Q3 2017 State of the Internet / Security report. In this report, we examined the WireX botnet and the collaborative efforts between half a dozen security companies, including Akamai. This botnet highlighted why cooperation between companies is so vital to the health of the Internet. We also mirrored Nominum's research by discussing Fast Flux botnets, which use rapidly changing DNS information to evade defenders.

Source Countries for Web Application Attacks – Worldwide, Q3 2017



In other research, Google also released a study that estimates there were over 1.9 billion usernames available on the black market. If anything, Google's estimates might have been conservative and were a harbinger of things to come. The Open Web Application Security Project (OWASP) released their annual Top 10 application security flaws list, which remained largely unchanged. While not research, another important story from November was the release of the White House guidelines on the disclosure of security flaws. The conversation about how governments should handle software vulnerabilities they discover is far from over, but these rules give a foundation to start from.

December

The end of the year didn't bring any respite to the security field. In fact, if your organization is directly or indirectly involved in retail, December is one of the most stressful months of the year as attacks often ramp up in order to take advantage of overloaded systems and personnel. However, there is evidence that even bad guys take a few days away from the Internet for Christmas. That being said, our research team didn't rest long and published a blog post on Domain Generation Algorithms just a few days before the beginning of the new year.

Not all the research and publications we generate at Akamai are prompted by internal projects. We are regularly engaged to research and respond to threats found by external researchers. In December, a nearly two-decade-old vulnerability resurfaced, designated ROBOT or the Return Of Bleichenbacher's Oracle Threat. Understanding the nature of potential vulnerabilities like ROBOT, and how they affect our customers, is one of the largest responsibilities of the Security team at Akamai.

Another area of responsibility for our team is interfacing with our customers and law enforcement. Where appropriate, we share data with organizations to support efforts to track and arrest criminals. The FBI made a public announcement of the arrests of the people behind the Mirai botnet in December. Akamai was the first major enterprise Mirai targeted. This was another incident that highlights the need for cross-organizational cooperation, even amongst competitors.

Globally, the efforts by the Anonymous collective were typified by the annual events dubbed OpUSA and OpIsrael. Every year, this "protest" is announced with various amounts of fanfare and is touted as retaliation against the U.S. and Israel. Targets are treated to DDoS attacks and web defacements of varying effectiveness, but often the announcement itself is what gains the most notice.

After Google's research posited the existence of 1.9 billion sets of credentials in November, it shouldn't have been a surprise that researchers from security company 4iQ found a stash of 1.4 billion credentials in a single file available in the dark corners of the Internet. Evidence suggested that most of the accounts were pulled from previously known compromises, but this file has been used by both researchers and criminals to fuel their tools since the event.

2018

January

It would be hard to find a start to a year that was more explosive than the revelation of the pair of vulnerabilities, Meltdown and Spectre, on January 3. All modern CPUs were affected by these bugs in the "speculative execution" feature of modern chips, and Akamai's systems were no exception. Because these vulnerabilities affect the basic functioning of modern chips, much of this year was spent dealing with the fallout. New ways to exploit this feature have been discovered every few months since the initial discovery, though no widespread usage has been discovered to date.

Blog posts aren't the only way we spread our knowledge to the world. Several of our researchers attended Botconf in Montpellier, France. It's not uncommon to see one or more Akamai employees presenting at events ranging from RSA to Black Hat and Defcon to local events like Derbycon or specialized events like Botconf. As an organization, we have long supported such presentations as a vital part of contributing to the security industry.

While attackers might have taken a few days off for Christmas, the weeks leading up to it were just as busy for attackers as they were for defenders. In "Gone Phishing for the Holidays," our Enterprise Threat Protector team demonstrated how domains are abused to gain the trust of users. Think twice before clicking on any link that promises a chance to win a new phone or gaming system.

January's security news was dominated by Meltdown and Spectre, to almost no one's surprise. Major vulnerabilities that affect large sections of the Internet seem to happen with more frequency every year. The good news is that our ability as an industry to respond to these events seems to be maturing as well.

February

We released our first major publication of the year with the Q4 2017 State of the Internet Report. This edition of the report included guest author Christina Kubecka, CEO of HypaSec, examining her research on servers still open for use as DNS reflectors. The number of vulnerable servers was more than it should be then, and it still is now.

The Mirai botnet was (and still is) a concern to Akamai, and the report looked at several different aspects of the botnet and its evolution. We also followed up the December arrest announcements with a post on how important community cooperation is to fighting malware like Mirai.

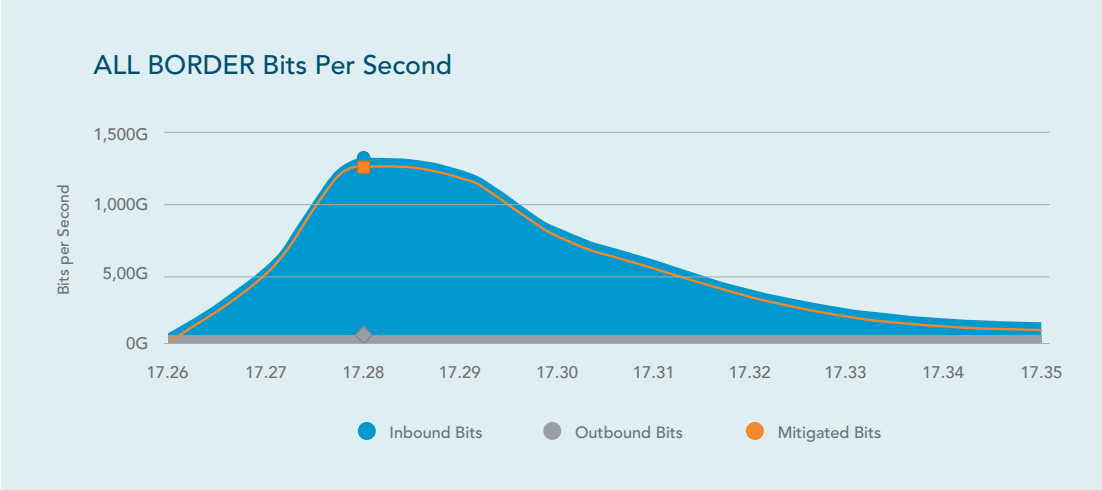
We also highlighted two efforts by our researchers. The first gave a glimpse into how Akamai plans for connectivity at a global scale, while the second examined a pair of vulnerabilities that came to light at the end of 2017 and why they needed to be watched. Drawing from research in this and previous reports, we published one of our first Syn City posts, "The Borg ate my login." It's good to have a little fun with titles from time to time.

While not the traditional type of denial of service we normally think of at Akamai, a vulnerability in WordPress opened up a potential application layer DoS in unpatched systems. While this one doesn't affect Akamai directly, when we see a widespread application vulnerability we can help defend against, we believe it's our duty to make the public aware.

As if the initial issues with the Meltdown and Spectre vulnerabilities weren't bad enough, we saw a series of alternative exploit methods crop up as the year progressed. Meltdown/Spectre was further complicated because changes made at the operating system level were not completely effective for an issue at the architecture level.

The end of February marked a major event for the Internet. Akamai's Security Intelligence and Research Team (SIRT), and similar teams at other organizations, started noticing and researching a new DDoS reflection vector being used in attacks. It turned out that a Unix service with known vulnerabilities, memcached, had been exposed to the Internet thanks to changes in the default configurations of several Linux distributions. This research gave Akamai and others a few days' warning before the biggest DDoS attack the Internet has seen so far happened.

The last day of February was definitely exciting, with a 1.3 Tbps attack hitting an Akamai customer. The harbinger attacks seen earlier in the month were just tests of memcached as a reflector. When the big attack hit, it instantly became the highest-traffic attack ever seen on the Internet — a record it still holds. Thanks to quick action by network administrators around the globe, memcached servers were quickly being taken out of the pool of potential reflectors. But at the same time, botnet owners seized on this new vector — and as more attackers used memcached, the amount a single attack could muster shrank.



March

That is not to say memcached immediately stopped being a threat. The way this reflector was used evolved quickly, with attackers including a Monero wallet address in their attack traffic that targets needed to send coins to if they wanted the attacks to stop. At the same time, defenders started discussing a "kill switch" in memcached that allowed them to flush the cache being used to fuel attacks. The problem for organizations was that the tool bordered on being an attack on its own and never saw a significant uptake as a valid defense.

Credential stuffing, the use of automated tools to make multiple login attempts against target sites, has been a growing problem. With this in mind, our researchers looked at one of the more popular tools, SNIPR. The fact that account-checking tools like SNIPR are relatively powerful and easy to use makes it likely this problem isn't going away any time soon.

April

It was a nice change of pace to have the RSA Conference happen in April this year. RSA is where businesses need to be to get in front of customers, partners, and competitors. Because of its importance, many companies see the conference as the cornerstone of the security calendar.

We released the Spring 2018 State of the Internet / Security: Carrier Insights report during the week of RSA. This report opened with guest writer Megan Stifel, CEO of Silicon Harbor Consultants, examining the importance of cooperation and data sharing, once again highlighting one of our themes for 2018. The report included in-depth research into vulnerabilities in the Web Proxy Auto-Discovery Protocol, zero-day domains, and the evolution of several botnets.

In a series of blog posts titled "The Dark Side of APIs" (1, 2), our researcher started raising concerns about how little many organizations know about the traffic hitting the interfaces used for computer-to-computer interaction. Considering that API traffic now constitutes more than 25% of all web traffic Akamai sees, we believe this is something organizations should be concerned with as well.

While Universal Plug and Play (UPnP) wasn't a new DDoS vector by any metric, an uptick in its use prompted our researchers to publish a white paper. Similar to the problems that caused memcached issues, UPNP is a protocol that was never meant to be exposed to the Internet, but all too often is.

We closed April with additional reflection on the memcached attacks. As a reflector, the memcached service displayed the highest amplification factor ever seen. Because attackers can put whatever they like into the cache, it's theoretically possible for them to increase traffic 500,000-fold. Here's hoping we don't see another vector like it.

One positive note, an announcement by Europol of a multi-country effort to arrest the people behind the WebStresser site was also made in April. Using dubious claims that their site was meant to be used to stress test customer sites, the reality was that this was the biggest "DDoS-for-hire" site on the Internet. For just a few dollars, their customers could point the sites botnets at any target, and frequently did. Although the fall of the site didn't significantly reduce the number of attacks Akamai sees, it does send a message to those offering similar services.

May

Spring flowers are nice, but new research might be better, which is why we started the month with a long research post on domain reputations systems. We followed up with a white paper on several new phishing threats we'd recently seen. Positive messages — those offering excitement or hope to the reader — are more popular and effective in phishing attempts, it seems.

May also marked the one-year anniversary of the WannaCry ransomware attacks. You remember those, don't you? A member of our team took a look back at the primary problem that made WannaCry possible: security debt. Unluckily, this isn't an issue we've made much progress on as an industry.

June

The Summer 2018 State of the Internet / Security report marked a significant evolution in our reporting. The statistics-driven data that was the core of the report became two different blog posts, DDoS by the Numbers and Web Application Attacks, as well as a research paper on the memcached attacks. The information in these posts is important to many of our readers and we felt it would reach a wider audience through the blog.

The report itself focused on two DDoS attacks we found interesting, plus botnet attacks on the hospitality and travel industries. We drew from the research on botnet attacks to posit some theories on the attacks we might see surrounding the World Cup. It's also worth noting that this issue of the report marked the biggest visual change we've ever made to the report.

As mentioned earlier, operations by the Anonymous collective are a recurring issue, and when Operation Icarus was announced, we felt it needed to be analyzed and that readers should be made aware of its potential. Luckily, the operation was more fizzle than bang, but this is the type of work our researchers are constantly performing.

There were unexpected consequences to GDPR that started being widely discussed in June. In order to meet with the European guidelines, many organizations started to scrub the WHOIS database to prevent potential violations, which means data that researchers and law enforcement rely on is no longer available. The U.S. federal government also released a Report to the President on botnets. The full title is much longer, but this report highlights how significant the issue of botnets has become.

July

The second half of the year started with a look at a tool called DrupalGangster. This highlights a common theme: the reuse and evolution of tools to take advantage of new vulnerabilities as they are discovered. Why write a new tool when you can modify one that's already available?

While it's not a security story, we're proud to see Akamai supporting Girls Who Code for the fourth year in a row. If you're not familiar with the project, its aim is to give young women in their junior year of high school a chance to learn how to write code.

Making the most of our data is a full-time job. This summer, we tasked the team intern to give our web application attack data a look with a fresh set of eyes — and wow, did she deliver. In the first of three blog posts, she normalized attack data against population and connectivity. It made us rethink how we represent some of our data.

In "The Router of All Evil" we examined the VPNFilter malware coming out of Russia. While some people might not technically think of home routers as Internet of Things devices, they'd be wrong. We're not the only organization with these concerns, which are highlighted in a look inside how IoT devices are used in DDoS.

August

The other cornerstone of our industry's calendar is the triumvirate of Black Hat, Defcon, and BSides. Attending Security Summer Camp (as some people call it) and baking in the heat of a Las Vegas summer is one of the aspirations that hackers, researchers, and security professionals share.

While many of our peers were in Las Vegas, there was a bigger issue brewing back at home. A researcher had revealed a pair of vulnerabilities in UDP and TCP that could be used to perform a resource exhaustion attack on most modern platforms. The UDP vulnerability was patched on August 6, while its TCP twin was patched on August 14. The communication between the researcher, Finland's NCSC, and many other organizations made it possible to have patches available in a very timely manner.

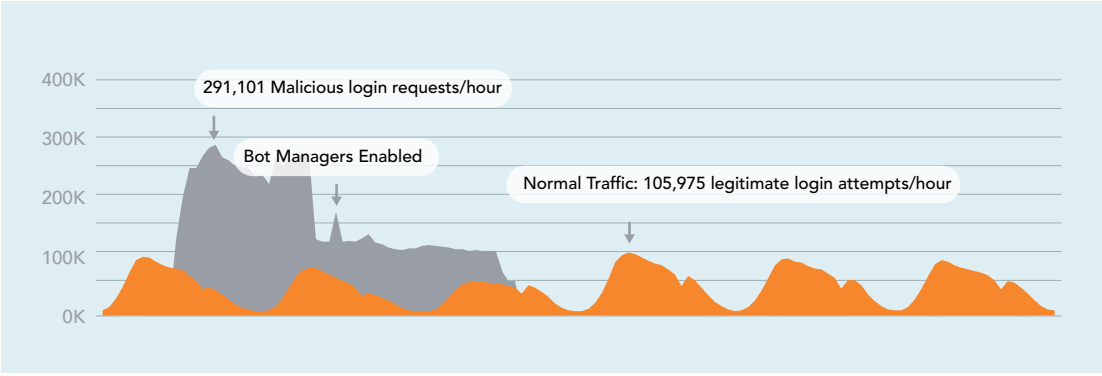
The project our summer intern started in July culminated in two more posts in August. The first, play fully titled Data Spaghetti, examines some of the ways data scientists manipulate data to see what can be revealed. The final post in the series, Diversity and Density of Web Application Attacks, discusses the most interesting points we found in the data. You'll see more of a few of those maps in the future.

Unlike the UDP/TCP vulnerabilities earlier in the month, the Apache Struts vulnerability revealed on August 23 didn't affect Akamai directly, but it did affect a number of our customers. Part of our role is to communicate the impact of issues such as this, which is why we followed up with additional data on how quickly we saw an uptick in attack patterns. Hint: It didn't take long.

The month closed with another blog post in our Dark Side of APIs series, concentrating on the effects of a DDoS on your site's APIs.

September

When you're working at a global organization, it's important to remember that just because it's summer in your half of the world, it's not summer everywhere. We were reminded of this, which is why we made another minor evolution to the reports and started naming them by issue number. Issue 4 of the report focused on credential stuffing — specifically two different attacks against financial services organizations under Akamai's protection. Since the report was released, we've been hearing plenty from our peers that Akamai is not the only organization seeing an increase in these sorts of attacks.



As part of our continuing research, we exposed another evolving botnet. The Tsunami/Kaiten botnet, a "cousin" of Mirai, was actively being developed and learning from other IoT botnets. This will keep happening until security of all things IoT becomes a priority for manufacturers.

October

Imagine for a moment what would happen if the root of all trust on the Internet somehow failed. This is a real concern, and one of the measures in place to prevent that failure is changing the keys that secure everything. ICANN is responsible for the Root Key Signing Key for the Internet, and announced they were finally going to replace the keys for the entire DNSSEC infrastructure. While it held the potential for disaster, when the key change happened, it went off without fanfare. Thankfully.

What do security researchers do for fun? They participate in Capture The Flag exercises like the one put on by HackerOne. If you've never been part of one of these events, this will give you a good idea of the thought that goes into breaking these vulnerabilities down. If you're a hacker (in the good sense) who does the same type of work for fun, you'll enjoy some of the twists and turns needed to complete this CTF.

For those not familiar with security response headers, our researchers wrote a post on how and why this HTTP header should be part of your security toolset. Even better, this is the first in a series of posts, each building on how these headers can and should be used to increase the security of your site.

Another example of "what do researchers do for fun" is highlighted in the blog post "An Examination of a Phishing Kit Dubbed Luis." Our researcher was pointed at a repository for a phishing kit and took it apart to see what he'd find.

The same researcher got bored and discovered a vulnerability in a project called jQuery file upload. It turns out that when changes are made to the software underlying your project, Apache in this case, all the assumptions you made in securing your project can be laid to rest. When the vulnerability was first discovered, we made the assumption that it wasn't a big deal. But further digging into jQuery revealed that this was actually a much bigger issue than originally thought, which probably isn't too surprising when you realize the project had been forked over 7,800 times.

Sometimes it's interesting to see how the very products we make as a company hinder our own research efforts. It turns out that bot management products interfere with the research being done by security researchers. Sometimes tools cut both ways, stopping attackers from being successful, but also hampering the efforts of defenders as well.

Looking Ahead

the more things change, the more they stay the same

— Some French Guy

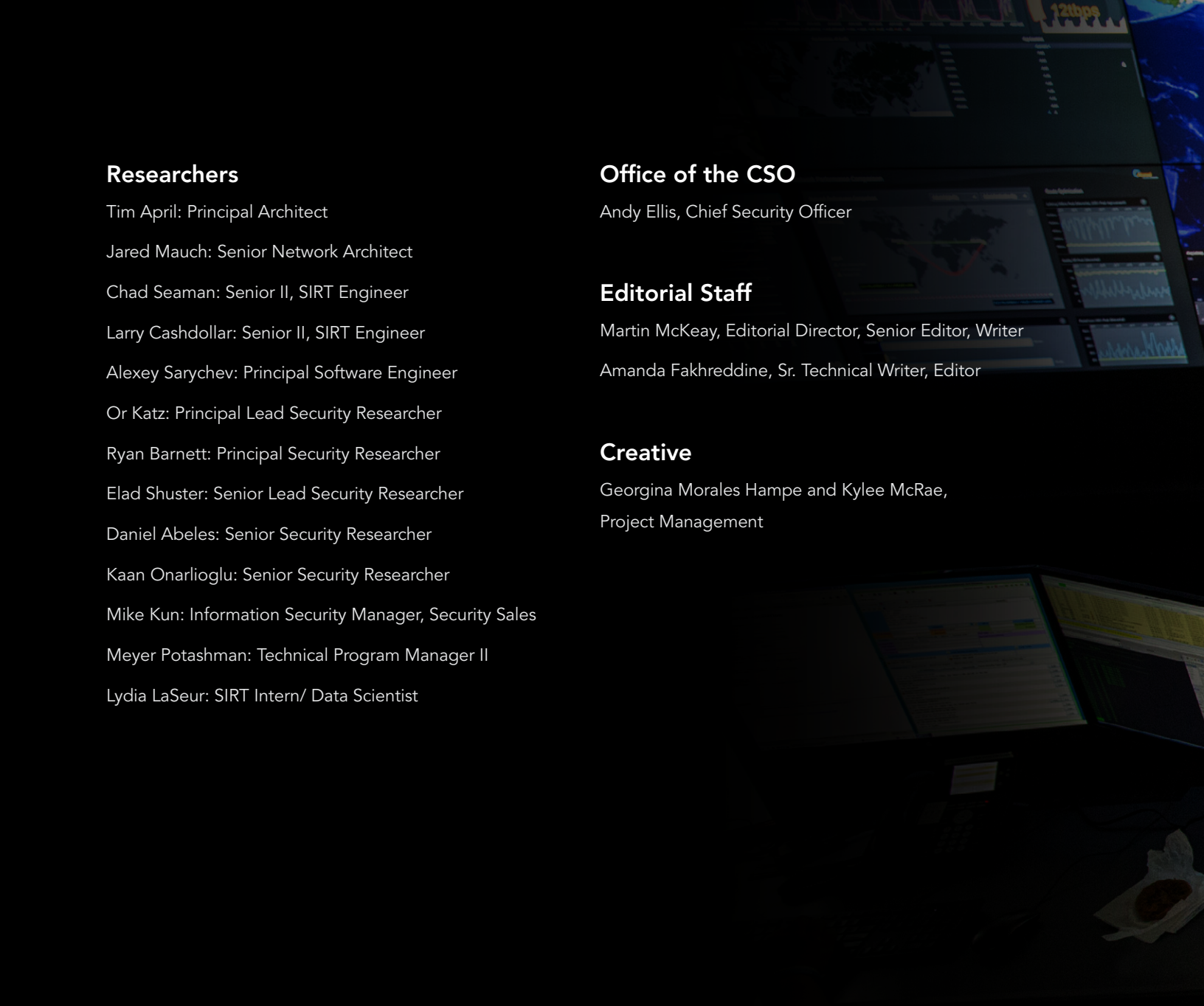
Security is a constantly evolving field; whether we're talking about the attacks coming at our networks, the tools we use to defend those same networks, or the information we're gathering to inhibit the former (attacks) and enable the latter (defense). One of the things you learn the longer you've been in this industry is that the rate of evolution is always increasing. It's probably one of the things that draw many practitioners to this field.

When we released the State of the Internet / Security report in November 2017, it focused on two aspects of Akamai's business: DDoS attacks and web application attacks. This had been the focus of the report since its inception. However, when the Nominum team joined Akamai with their own report and own data sets, it was plain to see that we could move beyond these topics and explore the wider world of Akamai's data.

We've been listening to the feedback we're getting from readers and progressing from statistics-driven reports to more story-driven writing. While statistical data about how many attacks we've seen and which protocols are the most popular targets are important, we've heard your requests to report on specific attacks, regions, and industries. We're still publishing the statistical analysis as blog posts, but future reports will be looking deeper into specific events rather than global trends. Unless something interesting and exciting is happening at the global level, that is.

Our goal in 2019 is to continue the narrative of specific industry trends. We'll be publishing new information on DDoS and application attacks in January, following up in February with a report on several aspects of the DNS traffic Akamai is tracking. Malicious bots, botnets, and credential abuse will continue to be a big part of our reporting early in the year. Zero Trust and everything it means are another big area of research for us in 2019.

Security is a field that is constantly evolving and every year brings new surprises. The impact of the memcached and Meltdown/Spectre vulnerabilities were huge in 2018. Despite any predictions you might see as the year comes to a close, no one knows what 2019 will bring — which is why Akamai will continue to evolve our research and what we bring to you in the State of the Internet / Security report.



Researchers

Tim April: Principal Architect

Jared Mauch: Senior Network Architect

Chad Seaman: Senior II, SIRT Engineer

Larry Cashdollar: Senior II, SIRT Engineer

Alexey Sarychev: Principal Software Engineer

Or Katz: Principal Lead Security Researcher

Ryan Barnett: Principal Security Researcher

Elad Shuster: Senior Lead Security Researcher

Daniel Abeles: Senior Security Researcher

Kaan Onarlioglu: Senior Security Researcher

Mike Kun: Information Security Manager, Security Sales

Meyer Potashman: Technical Program Manager II

Lydia LaSeur: SIRT Intern/ Data Scientist

Office of the CSO

Andy Ellis, Chief Security Officer

Editorial Staff

Martin McKeay, Editorial Director, Senior Editor, Writer

Amanda Fakhreddine, Sr. Technical Writer, Editor

Creative

Georgina Morales Hampe and Kylee McRae,
Project Management

About 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 or call 877-425-2624. Published 12/18.

Questions? Email us at research@akamai.com