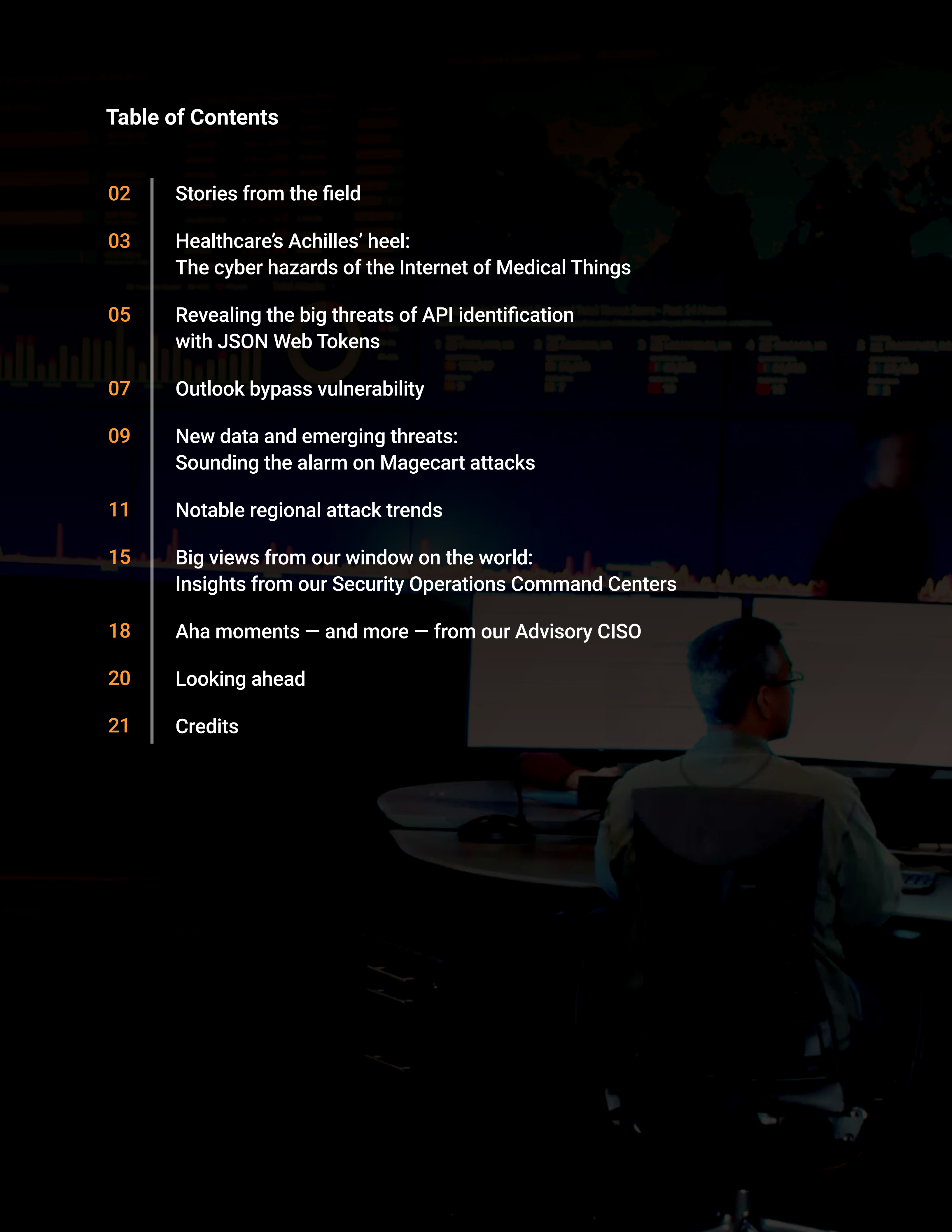
State of the Internet

Volume 9 | Issue 6

A Year in Review

A Look at 2023’s Cyber Trends and What’s to Come

Table of Contents



Stories from the field

For this State of the Internet (SOTI) report, we move away from the typical end-of-year review in which we discuss each of the previous reports we published this year, and instead focus on this central theme: What is your favorite security story of the year? We asked the writers and a data scientist in Akamai's Security Intelligence Group (SIG) to do a year-end evaluation of any story that we covered in the last 10 months. It must have been challenging for them to choose only one of the many notable stories and new discoveries that we released on our security research blog and in the SOTI reports in 2023. We also asked our Advisory CISO and a Vice President of our Security Operations Command Centers (SOCCs) to weigh in on this year's attack trends and the key learnings we can take into 2024.

A lot has happened this year in the world of security and within Akamai security research. The research contributions of our security experts are undeniably invaluable to the community. Through our dedicated hub, security professionals can easily access trusted resources containing insights, mitigation strategies, and attack trends that can aid them in defending their organizations. They can also access free tools, like our RPC Toolkit, as well as our free and open source adversary emulation platform, the Infection Monkey. Acting just like malware, the Infection Monkey propagates and "encrypts" files that it can access by flipping the bits — giving a practitioner a realistic view of how an attacker could (or couldn't) move around in that environment. The speed in which threats are evolving makes continuous testing necessary. Practitioners need to know where their network stands today, not just where it stood during the last pen test.

If a word can capture what the landscape looked like in 2023, that word would be *pivot*. Attackers shifted their tactics to circumvent security measures, looking for novel attack surfaces and untapped targets to wreak havoc on organizations of all sizes and industries. The same could be said for security defenders who continue to recalibrate and learn new ways to mitigate attacks and protect organizations better. We pivot through solutions, research, and tools with this goal: Provide actionable insights and mitigation strategies to security practitioners who fight the same security threats as we do.

Happy reading!

Favorite security stories

2023 Attack trends

2024 Looking ahead

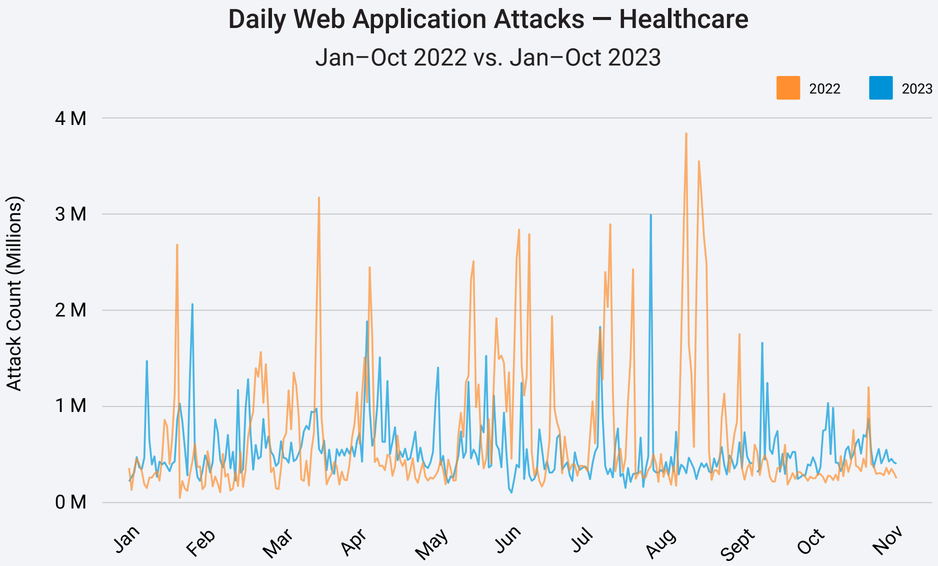
Healthcare's Achilles' heel: The cyber hazards of the Internet of Medical Things

I'm Badette Tribbey, one of the storytellers behind the SOTI reports, and I collaborate with security experts and data scientists to transform the technical findings and data into meaningful insights. I hate math, but I love how numbers can reveal compelling attack trends.

One of the most notable topics we covered this year hits close to home — the heightened risks of the Internet of Medical Things (IoMT). In both Slipping Through the Security Gaps and Ransomware on the Move, we examined the risk landscape of healthcare and life sciences and what makes that industry susceptible to attacks. One of the things that struck me the most is how IoMT assets such as MRI machines, insulin pumps, and wearables, though highly beneficial to patients, have significantly elevated the risks of healthcare providers. These organizations were already facing challenges to secure their perimeter because of complexity across the healthcare ecosystem, vulnerable legacy technology, and IT and cybersecurity staffing issues. Additionally, timely patching in this environment can be a Herculean task, with updates coming from various vendors for multiple systems or applications, making it challenging to track.

Unpatched IoMT devices are some of the most vulnerable assets across all industries, and they can introduce more nefarious threats like ransomware. As the IoMT grows exponentially — and with it, the use of APIs — its vulnerabilities also grow, and they can potentially become pathways for attackers to gain a foothold in their targets or be abused and result in data leakage (Figure 1). A joint report by Cynerio and Ponemon Institute of a study conducted across several hospitals and healthcare systems in the United States indicated that more than half experienced cyberattacks as a result of security gaps in IoMT devices.

> “Timely patching in [the healthcare] environment can be a Herculean task, with updates coming from various vendors for multiple systems or applications, making it challenging to track.
>
> **– Badette Tribbey,**
> **Senior Technical Writer,**
> **Akamai**


Daily Web Application Attacks — Healthcare

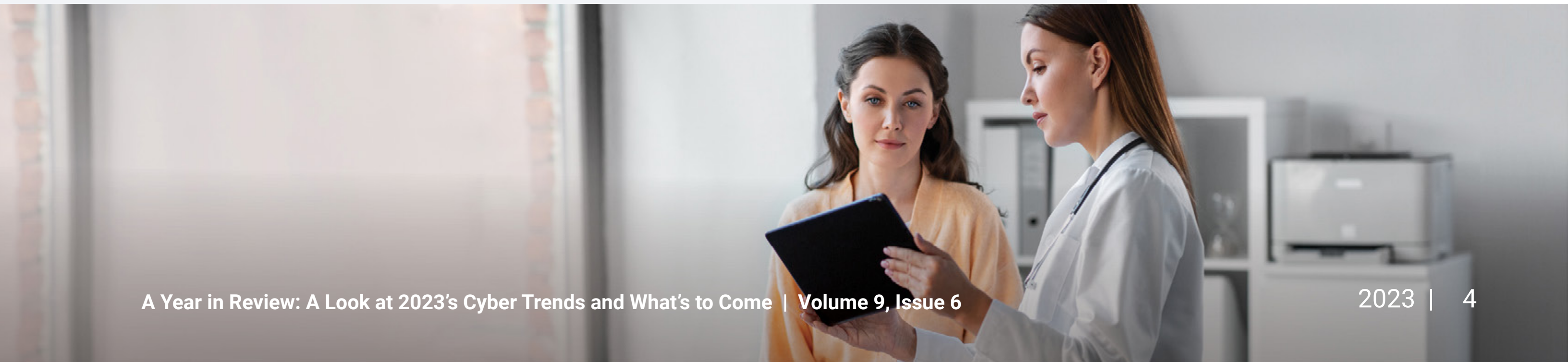
Jan–Oct 2022 vs. Jan–Oct 2023

Fig. 1: Web application and API attacks on the healthcare/pharmaceutical industry shows a steady activity with sporadic spikes between 2022 and 2023. Although attacks decreased by 21% year over year, the median number of attacks per day in 2023 is higher than in 2022.

What's next for healthcare?

As the healthcare industry expands its IoMT, APIs will continue to play a critical role in the accessibility of medical services (e.g., telehealth and remote patient monitoring), leading to better clinical and financial outcomes. And attacks against healthcare will not likely slow down, due to the high value of health records and patient data on the dark web.

As we shift our view from what has been going on to what to expect, it is clear that attackers will continue to innovate and increase the scope and complexity of their attacks. We are likely to see a continued push toward more technical attacks that take advantage of zero-day vulnerabilities. Additionally, the regulatory landscape (including, but not limited to, the Protecting and Transforming Cyber Health Care [PATCH] Act of 2022) is changing, so we need to ensure our solutions can help comply with a high volume of impending privacy, reporting, payment, data sovereignty, and resilience laws. Finally, we expect to see more disruptions in attacks for those CISOs who shift budgets to consolidate to fewer vendors and to use solutions that minimize dwell time for hackers who have gotten inside.



Revealing the big threats of API identification with JSON Web Tokens

I'm Lance Rhodes, and I've been enjoying working as a Cybersecurity Writer on the Akamai SIG team since March 2023! A lot of my job serves as "connective tissue" between our reports and blogs, as I've been working on both the publishing and writing aspects for the blog posts and sectional research and writing both content and marketing materials for the SOTI reports. And this is all tied together in my collaboration with the team on our monthly internal and external newsletters and security conference submissions.

I'd have to say that one of the more exciting blog posts I worked on this year was the JSON Web Token (JWT) post. This post had a direct connection to the app and API SOTI report (Slipping Through the Security Gaps) in that it expanded on broken authentication in JWTs, one of the standard methods of identification for APIs. So, it was fun to get a more in-depth understanding of JWTs.

After working on the app and API SOTI report earlier this year, I began working with Nitzan Namer on the JWT post, which focused on JWT as an attack vector for broken user authentication, an Open Web Application Security Project (OWASP) API Security Top 10. The SOTI report had a specific section dedicated to this, but the blog post took a deeper dive into the JWT structure and the best practices to protect against the biggest threats, including privilege escalation, data leakage, and account takeover.

I remember speaking with Nitzan about how we hoped the post would be used as an ongoing resource for security researchers, technical practitioners, and JWT users and administrators. The post fulfills this hope through its structural style — the JWT basics are listed first, then followed by six case scenarios, which include illustrations that exemplify some common threats and note best practices for each. The basics provide information on how JWTs secure APIs by issuing tokens that contain information to be shared as JSON objects. Each token is encoded, though not encrypted, and consists of a header, payload, and verification signature (authorizing that the data hasn't been altered since the server forged the token).

> "The blog post took a deeper dive into the JWT structure and the best practices to protect against the biggest threats, including privilege escalation, data leakage, and account takeover.
>
> **– Lance Rhodes, Cybersecurity Writer, Akamai**

The six case scenarios are:

1. Allowing the server to use a token without validation
2. Using the same private key for different applications
3. Using a weak signing algorithm
4. Choosing a short and/or low-entropy private key
5. Keeping sensitive data in a JWT's payload
6. Confusing the keys

JWTs are one of the most common verification formats; proper security measures are crucial since the format provides a large attack surface with lots of room for mistakes. Although these scenarios showcase some of the most common threats to JWTs, there are still many more out there and attack techniques are continuously evolving.

JWTs are neither encrypted nor implemented with security in mind

One of my biggest takeaways from the blog post is that JWTs are neither encrypted nor implemented with security in mind. It's hard to believe that such a popular authentication token can be so vulnerable. Part of the appeal of JWTs is that they enable the usage of many web applications and APIs without having to frequently sign in. Both the SOTI report and JWT blog post analyzed the JWT algorithms in Akamai traffic and determined that symmetric algorithms are the most common, even though they are theoretically less secure and not as protective as asymmetric algorithms. For example, both publications show that 54.8% of Akamai's customers use the HS256 algorithm, which is symmetric.

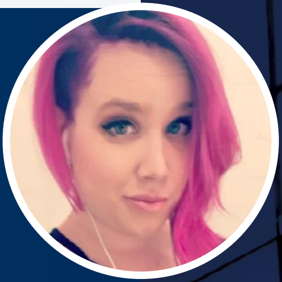
> "
>
> It's hard to believe that such a popular authentication token can be so vulnerable.
>
> – Lance Rhodes,
> Cybersecurity Writer,
> Akamai

It is likely that symmetric algorithms are chosen more often because the user only needs one key, and asymmetric algorithms require a higher amount of computational resources. JSON Web Encryption, the encrypted version of JWT, is also not commonly used. Most companies go with JWT and choose to save on power from computation.

The bottom line: Convenience, cost, and speed are often prioritized above security. This is a valuable reminder of the importance of our job as security researchers and writers. Good security research and practices are necessary for a satisfying balance between efficiency and safety.

Outlook bypass vulnerability

Hi! I hope you've smiled today! My name is Tricia Howard and I work on the blog side of the SIG. I live in the nitty-gritty world of technical write-ups and I work with our researchers, our corporate communications team, and our legal department (among others) to get the pieces out in a timely and effective manner. The best part of my job is that I get to brag on our researchers' behalf because they do some really cool stuff!



Of all the things I've been asked to write this year, this might be the most difficult. Of all the massively cool things our team has done in the past 12 months, how could I possibly choose a favorite? But since I have to choose only one, I pick Ben Barnea's work on the (in)famous Outlook bypass vulnerability. Ben is one of the most brilliant researchers I know and he managed to find a way to break an entire patch… with just one slash. I know it sounds absurd, even impossible — but it was possible, and he did it.

The original vulnerability allowed for an unauthorized attacker to send an Outlook invite with a custom notification sound. This sound doubled as an attack path that allowed a connection to the attacker's server, providing NTLM credentials. This is big bad stuff — from there, the attacker can brute force the credentials or run a relay attack. All these things can, of course, lead to privilege escalation, and we all know what can happen from there. The worst part of all is that this vulnerability was zero-click, meaning no action was required by the user to execute this attack. That takes something powerful and makes it downright dangerous — especially when you learn that it originated in Russia and was used in the wild, infiltrating various European government agencies.

The patch was issued in March. It took out the ability to use *PidLidReminderFileParameter*, which is what was allowing the attacker to specify the custom path (that is, connect to the malicious person's server). The patch instead utilized the *MapURLtoZone* feature, which checked to see whether the path was attempting to connect to the internet. If a connection was attempted, the traditional notification sound would play, eliminating the file path option for the custom notification. This would, theoretically, remove the option for a remote attacker to take advantage of this vulnerability — it would have to call out to the internet eventually if a connection between the attacker and victim was to be established.

> "Defenders have so much on their plate every day without new zero-click privilege escalation vulnerabilities to worry about.
>
> **– Tricia Howard,**
> **Senior Technical Writer,**
> **Akamai**

Thwarting the patch

Here's where it gets interesting — and, if I may say so, actually quite funny. Like any great researcher, Ben wanted to verify that the vulnerability truly wasn't exploitable anymore. This is an offensively simplistic way of putting it, but there are essentially two options for *MapURLtoZone*: allow or deny. Does it call out to the internet or not? For the most part the patch served as intended. Even when the path appeared to be local, *MapURLtoZone* recognized that the path had intended to reach the internet and blocked it from doing so.

Ben decided to play around with the path name by adding "/" to the end of it. When you provide something that *MapURLtoZone* wasn't expecting, it still has to decide whether to allow or deny. The additional slash wasn't recognized, which in turn gave back a 0, which the function read as local and trusted. After that, the rest of the vulnerability was able to execute the exact way it was intended by leveraging *CreateFile* for the custom path.

That was it! One tiny slash was added and an entire patch for a **critical** vulnerability was suddenly no longer an effective solution. That patch was likely created after days, possibly weeks or months, of cybersecurity professionals' time and energy to eliminate this threat … all to be thwarted by one single little slash.

The sheer sophistication of the original attack is pretty mind-bending when you break it down. The attacker is playing a Magnus Carlsen–level long game here. Considering it only took a slash to effectively render the patch useless, it stands to reason the attackers would have eventually figured out a bypass on their own. It's really great that it was Ben who discovered it instead by thinking outside the box.

This is why researchers who find these bugs truly are the lifeblood of the security community. Defenders have so much on their plate every day without new zero-click privilege escalation vulnerabilities to worry about. Security researchers are making a real difference in the world, especially as we become more and more dependent on technology and the internet for our daily lives.

I am so proud to be a part of this incredible team and to work with some of the most brilliant minds on this planet. To anyone who has read our blogs, our tweets, our SOTIs: Thank you. And to the researchers, both inside and outside of the Akamai SIG: Thank you for everything you do, break, and find. Let's see what next year has in store for us, shall we?

New data and emerging threats: Sounding the alarm on Magecart attacks

I'm Chelsea Tuttle and I've been with Akamai for almost eight years. As the data scientist responsible for the data represented in the SOTI over the past four years, I spend the majority of my time cleaning, exploring, analyzing, and visualizing our data. When I'm not staring at data, I am engaged in close collaboration with the SOTI writers to help communicate the stories our data is telling us. Because of the complexities of big data and the benefits of reporting on historical data, we don't often add a new dataset, but this year we did! When I look back on 2023, the stories we published around this new dataset come to mind as some of my favorites because I loved the learning opportunities that accompanied this endeavor.

Too often in our world we focus on reporting the number of attack attempts we see across our network and miss important opportunities to report data relevant to securing potential vulnerabilities and preventing attacks. One dataset we added to our SOTI reports this year stands out because it is unique in highlighting a potential area of vulnerability instead of focusing on the volume of attacks. This dataset is derived from observations provided by Akamai Client-Side Protection & Compliance from its eagle-eyed view of billions of web page scripts on a daily basis. One of the areas of potential vulnerability we keep an eye on is the number of first-party and third-party scripts utilized across websites. Although the use of a first-party script does not guarantee security and the use of a third-party script does not guarantee a vulnerability, the more trust that is put into someone else, such as trusting a third-party to host a web page script, the more risk is added to a security profile. Akamai is working to bridge the gap between convenience and security that has been created by the increasing use of third-party scripts throughout all industries.

As seen in our Entering Through the Gift Shop: Attacks on Commerce SOTI report from June 2023, one area of focus for Akamai research this year was the recent Magecart-style web skimming attacks; in particular, observing how Magecart attacks are continuing to invade the digital commerce industry. This type of attack attempts to steal sensitive user credentials, such as credit card information, from a digital commerce website's shopping cart using malicious JavaScript code injection. This type of attack tends to be easy for adversaries, yet poses big risks for consumers, while becoming increasingly hard to detect.

> “
>
> Akamai is working to bridge the gap between convenience and security that has been created by the increasing use of third-party scripts throughout all industries.
>
> **– Chelsea Tuttle,**
> **Senior Data Scientist,**
> **Akamai**

These Magecart, or web skimming, attacks often occur without the website user or owner even realizing it, and attackers will commonly choose digital commerce websites that are using vulnerable or outdated software.

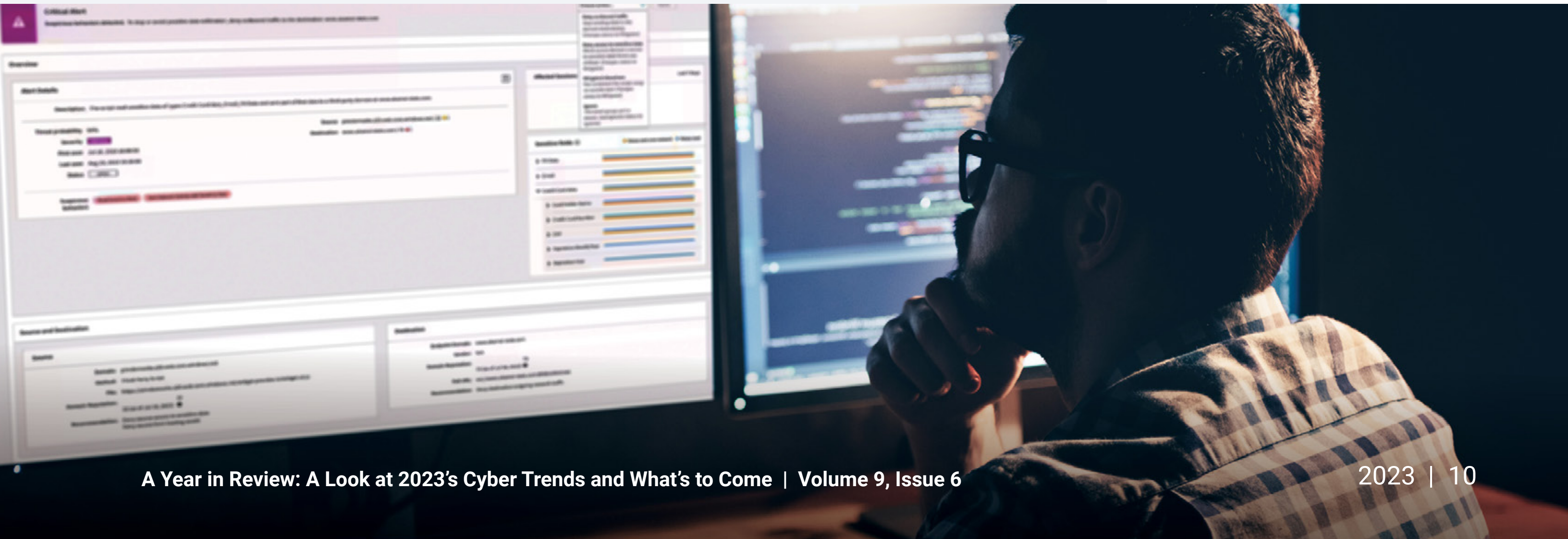
Recent Magecart variants

A number of Magecart variants can be seen in the more recent Magecart campaigns that Akamai researchers explored. Our June 2023 SOTI report focused on the Magecart client-side attacks and noted exploited vulnerabilities found in third-party scripts from open source libraries that could lead to supply chain attacks. Soon after that SOTI report was written, we published a blog post about how Akamai researchers discovered a new Magecart-style campaign that was abusing legitimate websites to attack others. In this campaign, there were essentially two sets of victim websites: The legitimate sites hijacked for the hosting, which act as attacker-controlled servers, and the vulnerable commerce sites attacked with client-side web skimming. A second blog post was published in August that described how Akamai researchers discovered another new Magento campaign with a hidden server-side template injection that was exploiting digital commerce sites to glean victim pay stats.

Akamai SIG's latest Magecart blog post uncovers a new obfuscation technique in which attackers are manipulating the website's default 404 error page to hide malicious code. Akamai researchers found this new campaign consists of two additional advanced concealment techniques, and they present the developing tactics that attackers are using to lengthen the attack chain and avoid detection.

As we close out 2023 and I look back at all of the research and reporting opportunities we had thanks to new data and emerging threats, I cannot help but also look forward to the new data and the learning opportunities that lie ahead for 2024.

Akamai researchers discovered a new Magecart-style campaign that was abusing legitimate websites to attack others



Notable regional attack trends

I'm Charlotte Pelliccia and I was added to the SOTI team in 2023 to bring to light the stories from the Asia-Pacific and Japan (APJ) and the Europe, Middle East, and Africa (EMEA) regions. Our APJ and EMEA snapshots are companion pieces to our global SOTI reports. Here, I'll revisit some of the most significant attack trends we covered in 2023, updating data from snapshots published earlier in the year.

Web application and API attacks — a tale of two verticals

Consistent with our most recent financial services and commerce SOTI reports, financial services has remained the top vertical for web application and API attacks in APJ, followed by commerce. Since our report in June 2023, attacks on financial services have topped 4.5 billion (up from 3.7 billion, an 18% increase). And since our March 2023 report, attacks on commerce climbed from 1.2 billion to 1.9 billion, a 58% increase. The splits among sub-verticals remain relatively consistent (Figure 2).

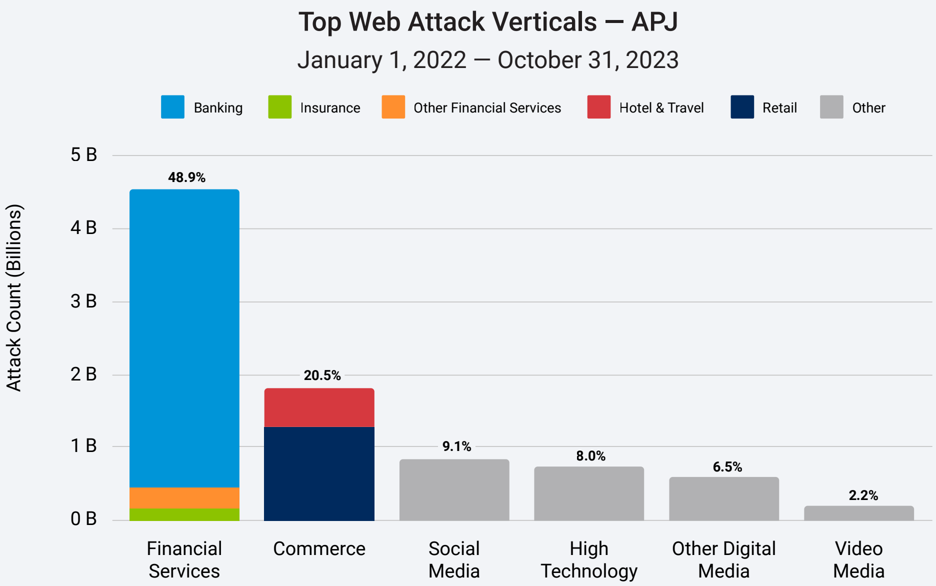


Fig. 2: Web attack verticals in APJ through October 2023

> Visibility into regional attack trends is vital to help organizations better understand their risk and fine-tune their tools and best practices.
>
> **– Charlotte Pelliccia, Cybersecurity Writer, Akamai**

Meanwhile, in EMEA, commerce remains the top vertical for web application and API attacks, with attacks now topping 6.5 billion (up from 4.6 billion, a 41% increase) since our March 2023 report. Although manufacturing has moved up from fourth to replace financial services in the third position, attacks against financial services have climbed 70% since we reported in June 2023, reaching 1.7 billion up from 1 billion. Here, too, splits among sub-verticals have remained relatively consistent (Figure 3).

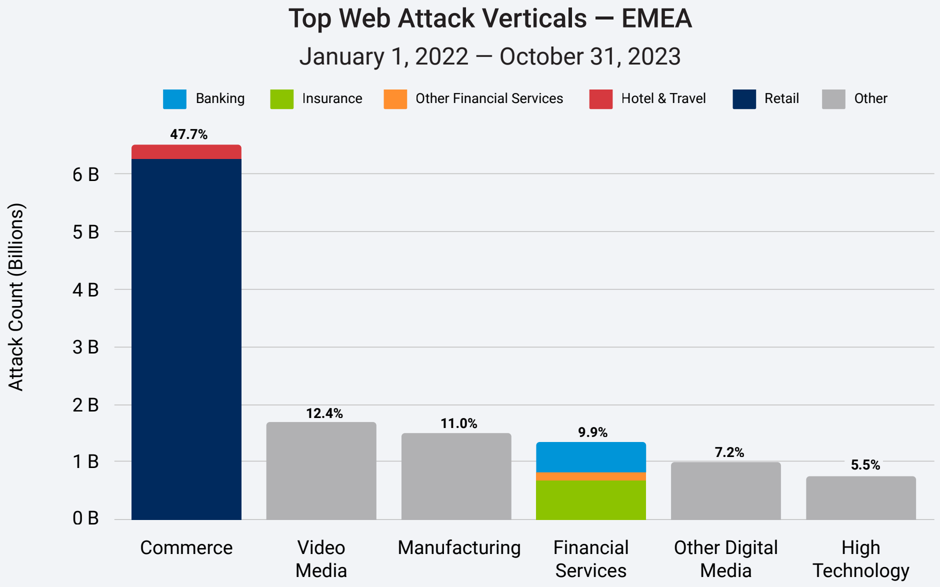
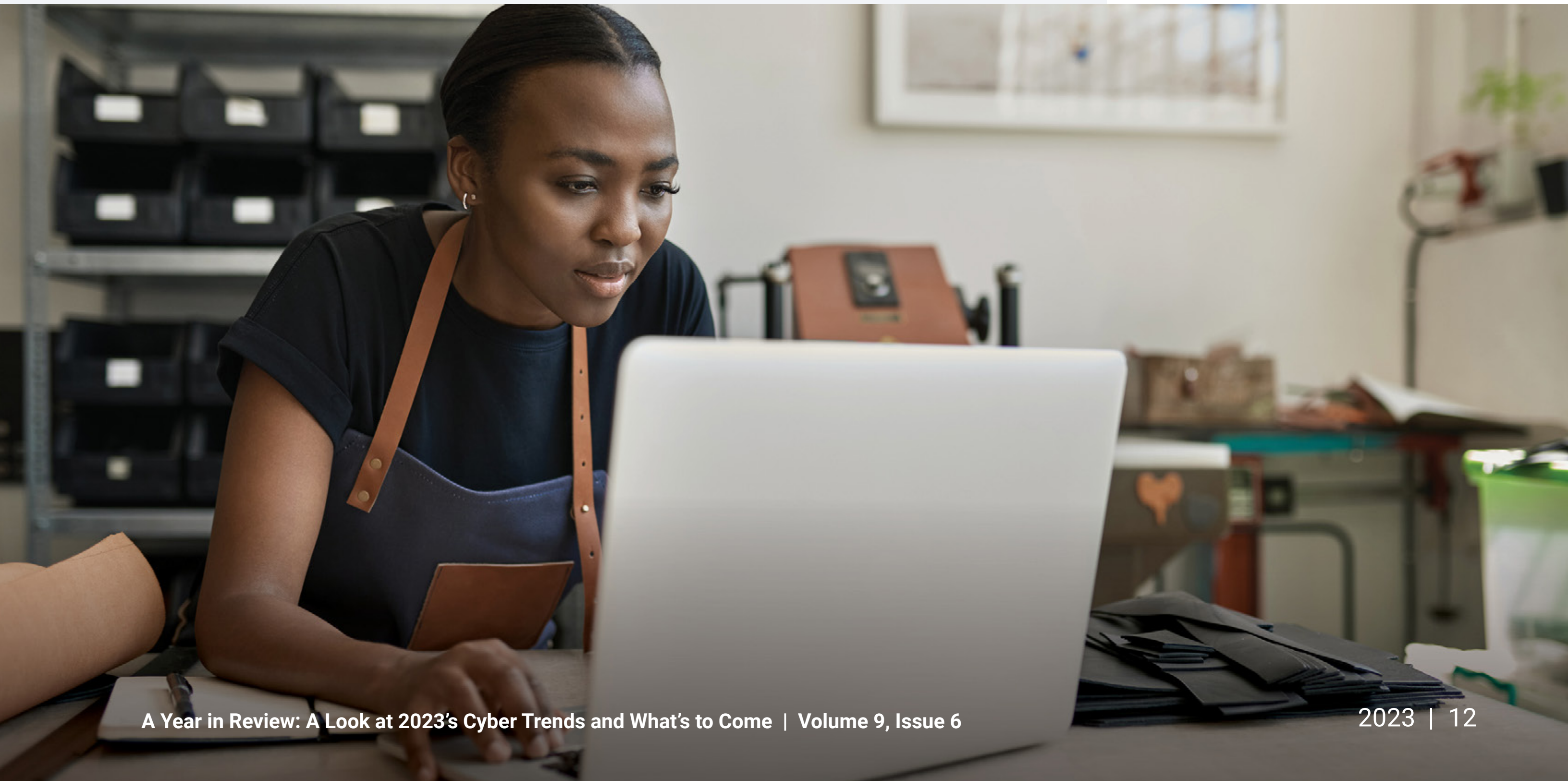


Fig. 3: Web attack verticals in EMEA through October 2023



Malicious bots are a weapon of choice

Continuing what we saw in previous reports, APJ is second to North America in malicious bot activity. The top three attack verticals from January 2022 through October 2023 in APJ are commerce (27.4%), video media (15.0%), and financial services (14.3%). In EMEA, half (50.1%) of all malicious bot activity targeted commerce, followed by other digital media at 15.3%, and video media at 12.2% (Figure 4).

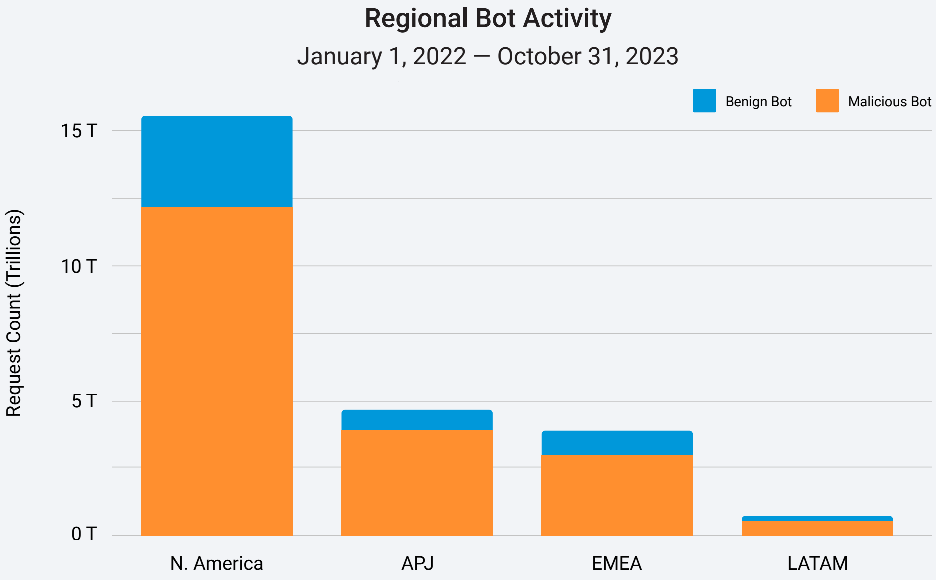


Fig. 4: The usage of malicious bots is prevalent across all regions, far exceeding the usage of benign bots

See the following essay for insights from our SOCC about how bot and DDoS attacks are changing.

EMEA in the crosshairs of the regional shift in DDoS attacks

Our 2023 report made it abundantly clear that threat actors have set their sights squarely on EMEA, attributed in part to the current geopolitical climate. A prime example: The number of Distributed Denial-of-Service (DDoS) attack events against the financial services, gambling, and manufacturing sectors in EMEA exceeded the numbers in all other regions combined (Figure 5).

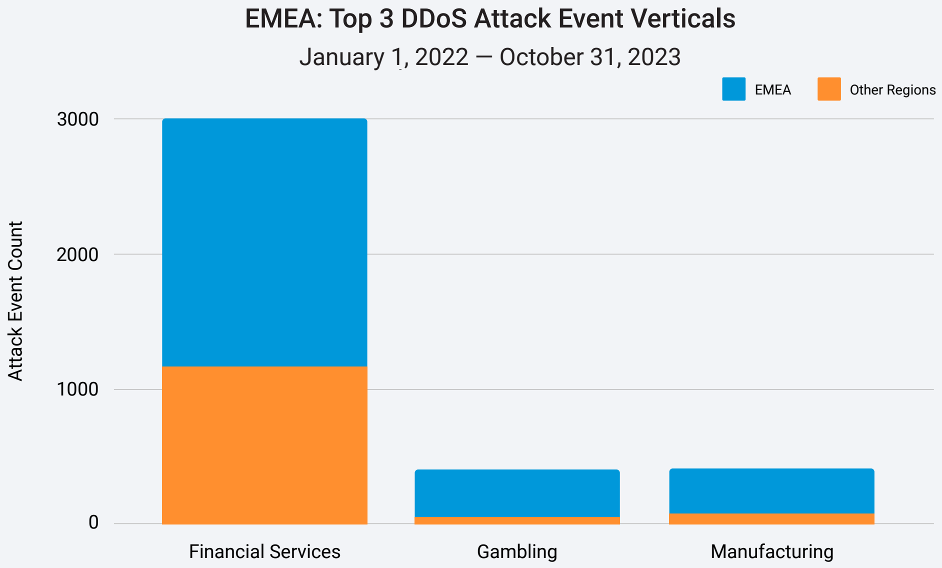


Fig. 5: EMEA experienced more DDoS attack events in these verticals than all other regions combined

Looking forward

As long as threat actors find success with web, bot, and DDoS attacks, it is reasonable to expect that these will remain their weapons of choice. In fact, these three vectors are already evolving to maintain or gather strength. Web application zero-day exploits are being intertwined with ransomware techniques (by ransomware groups such as CL0P) and are including DDoS attacks to create triple extortion tactic. Web scalping via bots has become the new normal for almost every major airline event or ticket sale. And API attacks directed at the business logic of the API are emerging.

In response, regulatory oversight and reporting obligations continue to increase around the globe and across industries, as no region or sector is safe from attack. The aim is to keep cybersecurity legislation up-to-date with the evolving threat landscape. Organizations need to remain vigilant about fulfilling reporting requirements and prepared to mitigate risk through a multilayered defense.

Big views from our window on the world: Insights from our Security Operations Command Centers

I'm Roger Barranco, Vice President of Global Security Operations. I've been with Akamai nearly a dozen years and I'm responsible for the company's managed security operations, which is serviced out of six SOCCs positioned around the globe and facilitated by a fantastic team. I started my career in cybersecurity and was drawn to the field because it's an interesting, ever-changing market — 2023 is a great example of that.

The Akamai SOCC has never been busier — by the end of 2023, we will have handled approximately 30% more security-related tickets than last year. Here are the key insights we've gleaned from working with our managed security service customers that organizations should keep in mind for 2024.

DDoS attacks are changing

Although the number of customers being attacked has historically increased year over year, the "how" is different today. First, the type and volume of customer properties being attacked has changed. For example, instead of 10 attacks against the same or similar endpoints, now we're seeing 100 attacks all aimed at different IPs in the customer's network space. And those attacks do not just target Layer 3, but also Layer 7 at the same time. Additionally, attacks against DNS have increased dramatically and the bulk are valid query attacks that can easily fatigue the customer's DNS infrastructure. Just a few megabits of unwanted DNS traffic can cause significant strain on an enterprise. We are also starting to see a concerning resurgence of activity on the Mirai front, which gained notoriety for harnessing the power of the Internet of Things to cause wide-scale disruption.

In today's threat landscape, it's not enough to put strong gear on the edge to keep up with attacks. Organizations need a robust, cloud-level security service to take on that workload, maintaining state while also implementing unique protections for each of those endpoints. This is where Akamai excels from both a platform and a services perspective. We can apply multiple layers of security to defend against the full spectrum of cyberattacks. And our hands-on experts examine the nuances and trends for each customer in order to monitor and mitigate in a very specific fashion that stops the ugliness but allows expected, clean traffic to come through.

> “
>
> The Akamai SOCC has never been busier — by the end of 2023, we will have handled approximately 30% more security-related tickets than last year.
>
> **– Roger Barranco,
Vice President of
Global Security Operations,
Akamai**

Battling bots can be brutal

Credential abuse is brutal to mitigate because distinguishing unwanted from wanted traffic is difficult, and customers have fairly unique back ends that may require very different mitigations. Additionally, attackers who perform credential abuse are some of the most skilled and the most vigilant because successful credential abuse is the easiest way to profit. The dangerous and costly nature of these bot attacks makes it important to have a credential abuse prevention solution, particularly in the financial services and commerce industries where malicious bot usage continues to climb.

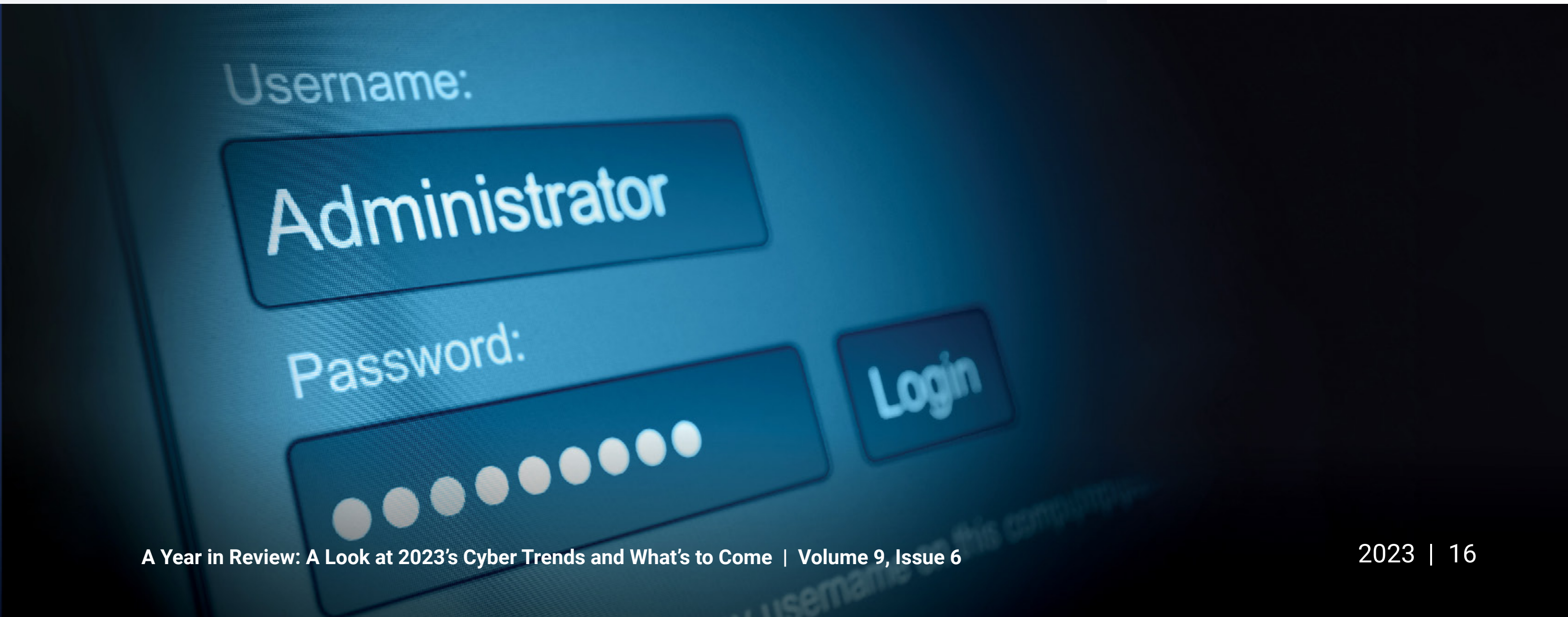
EMEA remains in attackers' sites

Ever since the Ukrainian incursion, EMEA (Europe, in particular) has displaced the United States as the top region for cyberattacks in a number of different verticals and categories of attack types, most notably DDoS. This shift highlights the fact that many aggressors are nation-states or nation-state sympathizers and their focus on Europe is not abating.

Attacker sophistication is rising

Gone are the days when script kiddies posed the main threat by leveraging generic tools to launch an attack hoping to get lucky, or by renting a DDoS botnet for $10 an hour to knock off a video game competitor. Today, attackers are more sophisticated and they appear to be focusing on specific targets in detail, planning their strategy, conducting reconnaissance sometimes a year in advance, and crafting attacks to take advantage of perceived possible weaknesses. As a result of the groundwork aggressors are putting in place, today's attacks are getting longer than the attacks of the past several years that frequently lasted just a few minutes.

> "
>
> As a result of the groundwork aggressors are putting in place, today's attacks are getting longer than the attacks of the past several years that frequently lasted just a few minutes.
>
> – Roger Barranco,
> Vice President of
> Global Security Operations,
> Akamai



Best practices for cyber and operational alignment

Despite these challenges, customers can increase the effectiveness of their efforts to protect themselves by following two best practices for cyber and operational alignment that enable Akamai to work as an extension of their cyber team. First, they should partner with the SOCC during peacetime to proactively build their defensive posture instead of attempting to do this during an attack. This way, attacks can be pre-mitigated, with no impact on production, and customers will receive a follow-up report that details the averted attack.

Second, they should proactively work on operational readiness and backup plans. For example, they should ensure that they know to route on and route off different platforms during testing. A five-minute attack can hurt a customer for an hour because of operational issues, so being operationally prepared is just as important as being prepared to respond to a pure cyber issue.

This year has underscored how cybersecurity is ever-changing, and we expect that to continue. The good news is that by applying these insights customers can get ahead of the curve and protect themselves in 2024.

Aha moments — and more — from our Advisory CISO

My name is Steve Winterfeld and I am Akamai's Advisory CISO. I served as CISO for Nordstrom Bank and as Director of Incident Response and Threat Intelligence at Charles Schwab. My role is to ensure that our partners are successful in defending their customers, and to determine where we should be focusing our capabilities.

This year saw a few trends that surprised me and a few that were confirmed by data that can be used to update our strategy. My top nine stories this year included some aha moments, some expected news, and some things that never seem to change.

Aha moments

- A total 10% to 16% of organizations have encountered command and control (C2) traffic in their network at least once per quarter. Additionally, 26% of infected devices reached out to domains related to an initial access broker.
- The ransomware threat landscape saw a concerning shift in attack techniques with the rampant abuse of zero-day and one-day vulnerabilities in the past six months.
- Akamai research found that victims of multiple ransomware groups are almost 6x more likely to experience a subsequent attack within the first three months of the initial attack.

Expected news

- API attacks directed at the business logic of the API are complicated to detect and mitigate. Consequently, they are challenging to determine at the individual request.
- Organizations need to ensure compliance with the new Payment Card Industry Data Security Standard (PCI DSS) v4.0 requirements and the Digital Operational Resilience Act (DORA) regulations.

> These insights are great guides to help you war-game your security program and see where you have redundant tools or gaps.
>
> **– Steve Winterfeld, Advisory CISO, Akamai**

Things that never seem to change

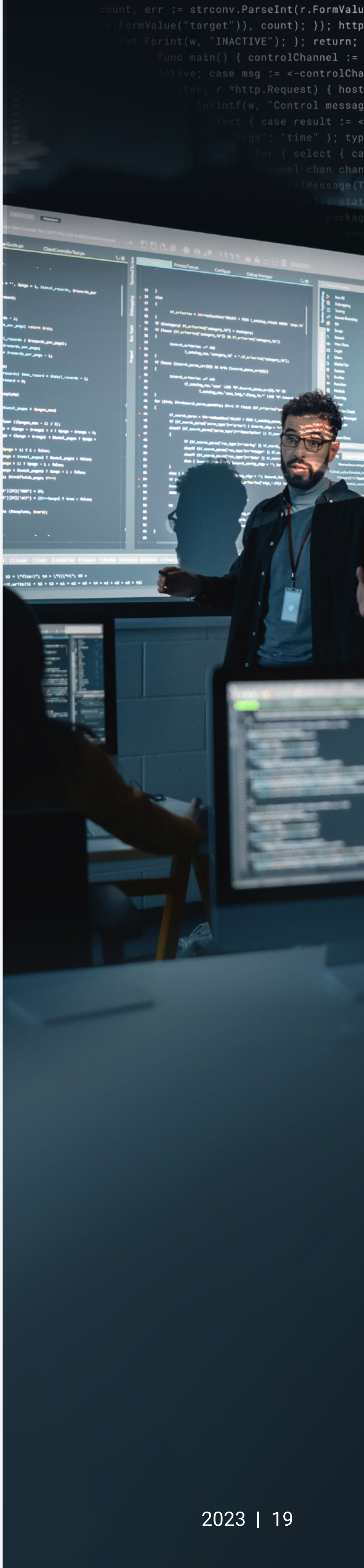
- The number of bots and API attacks continues to grow, and new records are being set for DDoS attacks.
- The most attacked industries tend to be financial services, high tech, and commerce.
- Local File Inclusion (LFI) is the most leveraged attack technique.
- There is an ongoing shift from North America to Europe as the region with the most DDoS attacks.

One pivotal discovery that gave me pause was the validated indicators of compromise from C2 communication. What was particularly unsettling was the high frequency of first-time detection occurring after malware had already successfully compromised systems and was establishing communication. This emphasizes the critical balance needed between preventive measures and rapid detection to minimize impact.

The story that surprised me the most was the shift from attacking people through social engineering to using zero-days. For the last few years, I've felt like our technical defenses were getting stronger and I needed to reinforce the staff with training and monitoring. But after this year's shift to zero-days, I need to take a hard look at where I deploy resources next year.

The attacks that seem the most unfair are the ones that hit while your organization is already dealing with or recovering from a ransomware attack. It is easy to get hyperfocused on the crisis and pull resources from ongoing defensive monitoring. This research was a powerful reminder that you can NOT afford to let your defenses down!

These insights are great guides to help you war-game your security program and see where you have redundant tools or gaps. They can drive exercises to update playbooks/processes, steer training, enhance pen test plans, or support risk portfolio reviews. Cybersecurity is a team sport, so these insights also are useful to drive discussions with internal partners (such as your legal or IT teams) and vendors. As always, references/tools like the National Institute of Standards and Technology (NIST), the MITRE ATT&CK knowledge base, and the OWASP Top 10 are great resources.



Looking ahead

It is impossible to predict the future, but we can anticipate that DDoS and API attacks will dominate 2024. The continued efforts to build larger botnet armies and develop new techniques, combined with influence of nation-states, will cause DDoS to grow. This factor, together with the evolution of ransomware, will be the genesis of legislation and resiliency.

Transformation continues to be the driving force for the implementation of APIs in most industries. This rapid growth will inadvertently lead to larger attack surfaces and more vulnerabilities, shadow APIs, zombie APIs, and API abuse. We expect to see significant growth in attacks on web applications and APIs. This will come from both standard attacks like LFI, and from emerging techniques like Server-Side Request Forgery (SSRF) and Server-Side Template Injections (SSTI), which will necessitate tools that can detect lateral movement and mitigate impacts.

Finally, with the exception of some industry- and region-specific trends, we expect to see an overall shortage of skilled cybersecurity professionals. There will be some relief from machine learning and large language model artificial intelligence, but overall it will be extremely difficult to find and retain the talent we need. This will lead to partnering with vendors for on-demand staffing or managed services for nonessential functions.

As for the Akamai SIG, we will continue to sound the alarm for prevalent threats and emerging security risks on the horizon. We will engage with the security community through our platforms and channels to bolster threat intelligence efforts. And in 2024, we will celebrate the 10th anniversary of our SOTI reports! We are excited to continue to improve our reports by introducing new datasets, visual aids, and key insights that can support security professionals in their quest to keep their organizations protected.

We look forward to sharing more research insights next year. In the meantime, stay safe!

Credits

Editorial and writing

Roger Barranco
Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Chelsea Tuttle
Steve Winterfeld

Review and subject matter contribution

Kimberly Gomez
Reuben Koh
Emily Lyons
Richard Meeus
Carley Thornell

Data analysis

Chelsea Tuttle

Marketing and publishing

Georgina Morales Hampe
Emily Spinks

More State of the Internet/Security

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

More Akamai threat research

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

Access data from this report

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

More on Akamai solutions

To learn more information on Akamai solutions against threats, visit our **Security Solutions page**.

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn.
Published 11/23.