# [state of the internet] / security

Volume 5, Issue 1

# DDoS and Application Attacks

Akamai
Intelligent Security Starts at the Edge

# Letter from the Editor

Welcome to the first issue of the *State of the Internet / Security* report of 2019! We are already a few weeks into the new year, and the holidays are now a memory. While the first day of the year is just an arbitrary marker in time, it's a good point of demarcation to look back on the past and plan for the future.

Network security professionals are responsible for using the lessons learned from previous experiences to build controls that will protect systems in the future. This can be an easy process, but it's often complicated by the daily tasks needed to make an enterprise run. Finding time for reflection is rarely a high priority.

## TL;DR

- Sometimes an "attack" isn't exactly what it first appears to be. The experts in Akamai's SOCC saw 4 billion requests impacting a site and dug into the real cause.
- Bots are big money for attackers, and they're constantly evolving to circumvent new defenses. One attacker went so far as to offer good money for someone with experience overcoming Akamai's defenses.
- Mental health issues cost U.S. businesses more than $190 billion a year in lost earnings. Our guest author, Amanda Berlin, highlights issues you should be monitoring in your team.

Has your team set aside a time to talk through the major incidents and challenges you faced in 2018 and how they might influence your experiences in 2019? Were you fighting countless unrelated fires, or was there an overarching theme to your experiences?

There are many examples of security teams doing an excellent job of reviewing every incident in their enterprise and learning from them. But even the best teams sometimes forget to step back to look at their experiences as a whole. Global and long-term trends can only come into focus when we give ourselves a bit of distance and perspective.

An additional reminder for you as we look at the year ahead: Check on the stress levels and mental health of the people you work and socialize with in the security field. Whether it's someone who reports to you, your boss, or simply a friend at another organization, take a few minutes to reach out and see how people are doing.

Multiple conferences have added tracks on stress and burnout part of their content in recent years, most notably the BSides and RSA conferences. A short call or email can make a big difference in a peer's day. Ours is a stressful career no matter how you look at it, and we need to make a point of reaching out from time to time.

There are a wealth of opportunities to make change in 2019. What do you want to accomplish?

# Table of Contents

LETTER FROM THE EDITOR 2

MENTAL HEALTH: AWARENESS TRAINING FOR HACKERS 5

RECENT RESEARCH 11

jQuery File Upload 11

UPnProxy 11

AKAMAI RESEARCH 11

The DDoS Attack That Wasn’t 11

More Bots, More Problems 15

LOOKING FORWARD 22

APPENDIX A: METHODOLOGIES 23

CREDITS 24

## MENTAL HEALTH:

# Awareness Training for Hackers

The information security community is composed of intelligent, driven, passionate, opinionated individuals, and is difficult to compare to any other industry. When you combine the pressure and stress we put on ourselves (from research, learning, teaching, etc.), things can quickly come to a head. But not only do we put pressure on ourselves, we also take in additional pressures from our bosses, co-workers, and family in many different forms.

The majority of roles we fill cater to our drive and willingness to be behind a keyboard for hours on end. The result is that many of us are broken. We're broken in different ways, at different times, and for different reasons – but we're broken all the same.

*Amanda Berlin, the guest author for this edition of the State of the Internet / Security report, offers a different viewpoint than our usual external contribution. The SOTI / Security series focuses on immersing itself – and you, our reader – deep in the stories of bad days on the Internet. There is increasing anecdotal evidence that the levels of stress and burnout in the information security industry are on the rise, from an already high state. This often leads to fair questions about how to address wellness for security staff, not only physically, but emotionally and mentally as well. I am fortunate to work in an organization that focuses on staff wellness, which is one of Akamai's core values, but not all of our readers have the same support strucature. While the issue cannot be solved with a few pages of commentary, as members of the security community, I and the rest of the SOTI team felt Ms. Berlin's perspective could shine light on issues that aren't typically discussed openly at this level. We want to encourage and inspire more efforts at improving staff wellness, so we can all focus on making the Internet a better place.*

*This essay should not be construed as medical advice or professional counseling. Please seek professional help if you feel you or someone you know exhibits the symptoms highlighted in this essay.*

*– Martin McKeay, Editorial Director*

The World Health Organization states that over 800,000 people die due to suicide every year and suicide is the second-leading cause of death in 15–29-year-olds. There are indications that for each adult who died of suicide there may have been more than 20 others attempting suicide. Early identification and effective management are key to ensuring that people receive the care they need.

## MENTAL HEALTH AS A BUSINESS OBJECTIVE:

Serious mental illness costs America $193.2 billion in lost earnings per year; and approximately 1 in 25 adults in the U.S.—9.8 million or 4%—experience a serious mental illness in a given year that substantially interferes with or limits one or more major life activities.

Many businesses are now incorporating mental health treatments and awareness into everyday activity. They have seen that a happy, well-balanced employee produces better results, stays around longer, and in general helps provide a greater working environment.

## MENTAL HEALTH HACKERS (MHH):

Everyone has mental health needs at different levels. Whether or not you have a condition that makes it harder to maintain good mental health can also be a factor. Keeping it in the forefront of your decision making, just as if you were to go to the gym every day for physical health, can make incredible differences in your day-to-day life.

Whether you're attempting to do some self-reflection, or help out a friend or family member, trying to tell the difference between what expected behaviors are and what might be the signs of a mental health condition isn't always easy. There's no simple test that can let someone know if there is a mental health condition, or if actions and thoughts might be typical behaviors or the result of a physical illness.

Each condition has its own set of symptoms, but some common signs of mental health conditions can include the following.

- Excessive worrying or fear
- Feeling excessively sad or low

- Confused thinking or problems concentrating and learning
- Extreme mood changes, including uncontrollable "highs" or feelings of euphoria
- Prolonged or strong feelings of irritability or anger
- Avoiding friends and social activities
- Difficulties understanding or relating to other people
- Changes in sleeping habits or feeling tired and low energy
- Changes in eating habits such as increased hunger or lack of appetite
- Changes in sex drive
- Difficulty perceiving reality (delusions/hallucinations)
- Inability to perceive changes in one's own feelings, behavior, or personality
- Abuse of substances like alcohol or drugs
- Multiple physical ailments without obvious causes
- Thoughts of suicide, or suicidal planning
- Inability to carry out daily activities or handle daily problems and stress

Don't be afraid to reach out if you or someone you know needs help. Learning all you can about mental health is an important first step. Reach out to your health insurance, primary care doctor, or state/country mental health authority for more resources.

I highly recommend finding a Mental Health First Aid class near you, regardless of whether you are personally struggling with an issue. Chances are high that you are close to someone who is, whether you realize it or not. Directly or indirectly, mental health conditions affect all of us. In fact, one in four people have some sort of mental health condition. We are not as alone as we think, and we can make a huge contribution to society just by staying alive.

Support systems are vital to recovery. The support helps minimize damage posed by mental illness on an individual. It also can save a loved one's life. There are many steps you can take to help yourself or others, including:

- Inform yourself as much as possible about the illness being faced.
- Start dialogues, not debates, with family and friends.
- In cases of acute psychiatric distress (experiencing psychosis or feeling suicidal, for instance), getting to the hospital is the wisest choice.
- Instead of guessing what helps: Communicate about it, or ask.
- Seek out support groups.
- Reassure your friends or family members that you care about them.
- Offer to help them with everyday tasks if they are unable.
- Include them in your plans and continue to invite them without being overbearing, even if they resist your invitations.
- Keep yourself well and pace yourself. Overextending yourself will only cause further problems in the long run.
- Avoid falling into the role of "fixer" and "savior." No matter how much you love someone, it cannot save them.
- Offering objectivity, compassion, and acceptance is valuable beyond measure.
- Know that even if your actions and love may seem to have little impact, they are making a difference.
- Have realistic expectations. The recovery process is not a straight line, nor is it one that happens quickly.

## COMMUNITY OUTREACH:

For those of you that haven't heard my *Hackers, Hugs & Drugs* talk, a little background is called for first.

I've been struggling with anxiety and depression since my mid-teens in one way or another. Poor relationships did nothing but fuel the issues I was already having. When I started interacting with the InfoSec community about six years ago, I started feeling a sense of belonging. Through my trials with different medications and coping mechanisms I've started to get a little more of a handle on (or at least a better awareness) of my own mental health.

After a year and a half giving this talk at various conferences and meetups, I continued to be awestruck at the overwhelmingly positive responses. Each time I would think "*Okay, maybe I've given this speech enough,*" another person come up to me to talk about how it led them to go get some counseling, or changed their minds about self-harm or suicide.

After hearing story after story, I thought it would be good to continue these efforts at a larger scale. While I love speaking, it only reaches a certain number of people.

We—the security community as a whole—needed more. That is when the idea of the Mental Health & Wellness workshop at DerbyCon came about, and honestly it did turn out to be more of a village with smaller workshops inside of it.

This room turned into something more than I could have ever envisioned. We had a community of passionate information security professionals come together to create this amazing thing to provide group self-care. We haven't stopped from there. We've now started up Mental Health Hackers, to bring this education and relaxed environment to more conferences.

We're all in this together and are passionate about learning new things, it's time to start the change from within our communities and families so we can start talking about our mental health almost as much as we do about vulnerabilities, protocols, and patches.

*– Amanda Berlin, Mental Health Hackers*
November, 2018

# Recent Research

In the fourth quarter of 2018, Akamai researchers released new research detailing vulnerabilities in jQuery File Upload, and fresh attacks against UPnP.

### JQUERY FILE UPLOAD:

In October, Larry Cashdollar reported a file upload vulnerability in Blueimp's jQuery File Upload project, which resulted in a quick fix. The problem didn't stop there, as other projects were using Blueimp's base code, so he attempted to reach out to those projects as well. In the end, several projects were updated, but there were several thousand that could not be reached due to visibility and contact issues on GitHub.

### UPNPROXY:

In November, Chad Seaman updated his original UPnP research and discovered new attacks using Eternal Blue and Eternal Red. He discovered 277,000 devices running vulnerable implementation of UPnP, and more than 45,000 active injection attacks. At the time his research was released, the 45,113 routers with confirmed injections exposed 1.7 million machines to the attackers.

# Akamai Research

## THE DDOS ATTACK THAT WASN'T

Early in 2018, Akamai noticed a customer in Asia was receiving an abnormal amount of traffic to one of its URLs. The customer was seeing so much traffic that, at its peak, it almost overflowed the database Akamai uses to log such activity.

When another department flagged this traffic as something to investigate, the initial report and associated data showed all the hallmarks of a major DDoS attack. Traffic volume reached 875,000 requests per second at one point. Notes from early in the incident record the flood of traffic as highly distributed, with early log grabs recording 5.5 Gbps.

## A MASSIVE AMOUNT OF TRAFFIC:

When the incident first came to the attention of the Security Operations Command Center (SOCC), it didn't come to them through normal channels. Instead, it was reported by another department within Akamai. Something was seriously wrong.

Once the SOCC started digging into the report, they observed a large amount of HTTP requests going to a customer's URL – leading to an immediate presumption of attack, as seen in Figure 1. At the time, there simply wasn't any other way to explain the sudden unexpected flood of traffic.

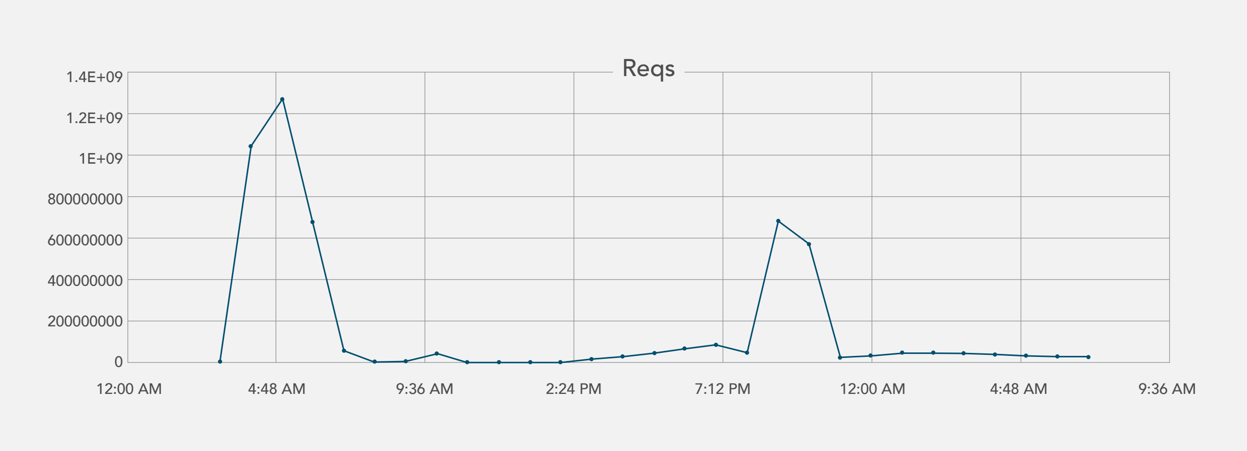


**Figure 1:** The initial spike in traffic was so large – more than 4 billion requests – it almost crashed the logging system

The SOCC's mission is to stop and mitigate problems, but they have to do so in a way that results in little to no downtime for a customer. So, while the Security Incident Response Team (SIRT) worked on determining the root cause of this surge in traffic to the customer's URL, the SOCC focused on returning the customer's operations back to normal.

## SORTING THE DETAILS:

To determine the real cause of this traffic flood, the SIRT examined traffic to the URL in question a few days prior to this incident and noticed something interesting.

There were 139 IP addresses approaching the customer's URL a few days before the peak, with the exact same "attack" features. This URL went from 643 requests, to well over 4 billion, in less than a week. The data in Figure 2 gives you an idea of how distributed these requests were.

Initial analysis showed that half of the IPs were flagged by Akamai as NAT gateways. Additional packet and header analysis confirmed the traffic in question was generated by a Windows COM Object (WinhttpRequest).

Originally, the traffic from the earlier visits to the customer's URL contained GET and POST request methods. Now, thousands of IP addresses were shredding the URL with an unrelenting stream of POST requests.

Examining all the POST requests hitting the customer's URL showed that the User-Agent fields were not being forged or otherwise altered once blocked, boosting the confidence SIRT researchers had for their conclusion that a Windows-oriented tool was responsible for this massive flood of requests.

| COUNTRY | IP ADDRESSES | REQUESTS |
|---|---|---|
| United States | 13,996 | 4,558,664,071 |
| Canada | 659 | 261,733,710 |
| Great Britain | 538 | 25,930,858 |
| Australia | 93 | 11,042,026 |
| Denmark | 49 | 21,818,410 |
| Ireland | 37 | 3,133,283 |
| India | 17 | 2,589,683 |
| China | 12 | 243,448 |
| Germany | 12 | 997,701 |
| South Africa | 11 | 2,121,635 |

**Figure 2:** This breakdown shows the top IP sources during the incident by location, including the number of requests logged by location

Over the next 28 hours, the SOCC would mitigate more than 4 billion requests from 15,582 IP addresses. It was determined that the base platform used by the customer mitigated 98% of the problematic traffic without intervention, all thanks to rate controls alone.

Akamai's platform uses adaptive rate controls to protect customers from DDoS attacks. These controls use behavior-based rules to monitor and control the rate of requests against a given application.

In this case, the rate controls were focused on stopping POST requests against the customer's URL. The other 2% of the traffic was mitigated by the development of a new ruleset to trigger the controls.

It’s important to note, like other anti-DDoS products in the market, Akamai’s rate controls work best when they’re tuned and configured properly. In this case, the customer in question worked with Akamai, before something happened, to develop rules that matched their unique requirements.

## DENIAL OF SERVICE VIA DISTRIBUTED BUGGY CODE:

By the time SIRT had finished their work, and the SOCC had things under control, everyone involved realized the incident wasn’t an attack at all.

Earlier analysis, backed by additional SIRT research, concluded the high volume of traffic hammering this customer’s URL was the result of a warranty tool gone haywire.

Once the SOCC started filtering traffic, the warranty tool kept visiting the URL. However, the subsequent visits didn’t alter anything in the headers (such as the User-Agent) that could’ve assisted in bypassing mitigations, proving that this incident wasn’t a malicious attack.

This conclusion was later confirmed by the customer, as well as the vendor responsible for the tool. A fix was pushed within hours to all of the affected systems.

## LESSONS LEARNED:

On one hand, anything that comes into the SOCC is a big deal for the teams who staff it 24/7. On the other hand, not every incident poses the same challenges to understand and respond to that this one did.

In this case, while the incident was flagged from another department within Akamai, that didn’t mean it wasn’t an immediate priority for the SOCC staff. In fact, by working hand-in-hand with SIRT researchers, the SOCC was able to mitigate the issue quickly.

If there’s a lesson to be learned by this incident, it’s the importance of developing a strong defensive posture. It’s best to do this before something happens — which in this case involved the customer configuring and fine-tuning controls to match them to the organization’s needs.

## MORE BOTS, MORE PROBLEMS

Distributed computing has made life a little easier for businesses and consumers, but these advances have also opened up new attack vectors. One of the most common threats against networks and applications is bots. Akamai's research reveals that not only are these malicious bots constantly evolving, the people developing them are actively looking for evasion techniques, going so far as to hire developers with unique brand- and vendor-specific expertise.

Understanding how bots work and how to defend against them is a critical element in your security model. A key aspect is understanding how typical bot defenses and evasions function, and how this information applies to your organization's unique business and risk model.

When a majority of the traffic to your online business presence comes from bots, there is a profound ripple effect.

| VERTICAL | TOTAL BOT TRAFFIC | TOTAL REQUESTS (BOTS AND HTTP) | REQUEST PERCENTAGE (BOTS / HTTP) |
|---|---|---|---|
| Media & Entertainment | 6,385,268,181 | 94,607,069,792 | 6.75% |
| Education | 126,485,194 | 2,920,230,414 | 4.33% |
| Hotel & Travel | 17,213,912,273 | 403,734,977,420 | 4.26% |
| Miscellaneous | 1,070,980,172 | 25,252,564,668 | 4.24% |
| Retail | 107,301,948,091 | 2,768,895,396,390 | 3.88% |
| Manufacturing | 1,398,829,764 | 41,430,063,364 | 3.38% |
| Real Estate | 130,157,772 | 4,006,237,916 | 3.25% |
| Consumer Goods | 2,737,855,414 | 103,710,648,491 | 2.64% |
| Public Sector | 3,185,738,438 | 138,246,823,219 | 2.30% |
| Software as a Service | 1,624,107,871 | 77,066,649,310 | 2.11% |
| Pharma/ Health Care | 307,249,702 | 15,373,210,108 | 2.00% |

**Figure 3:** A breakdown by industry of bot traffic on the Akamai network sorted by request percentage, that includes both known-good and known bad bots

This ripple effect spreads across multiple risks associated with bot traffic, including performance issues (e.g., slow websites and frustrated customers) and increases in IT expenses. Additionally, there are brand-related risks such as bots that scrape your website for inventory assets, pricing data, or content. If that's not enough, you've also got to deal with the bots responsible for DDoS attacks, ad fraud, SEO spam, and credential stuffing, to name a few.

Known-good bots scan publicly available content, are operated by legitimate companies, and would usually identify themselves in the User-Agent header, including a URL to their web page.

We refer to the following main categories when considering known-good bots:

- **SEARCH ENGINE CRAWLERS** – web search engines operate for a wide variety of purposes, going from global search engines (e.g., Google, Bing) to more targeted ones such as job search engines, media and entertainment, commerce-focused search engines, or academic and research (publications, citation search, semantic analysis).
- **WEB ARCHIVES** – scanning the web periodically and recording its content to searchable indexed databases.
- **SEARCH ENGINE OPTIMIZATION, AUDIENCE ANALYTICS, AND MARKETING SERVICE** – scraping websites and social media for content that might provide customers with market insights such as positioning, mentions, and other references.
- **SITE MONITORING SERVICES** – automated tools that monitor a site's health, availability, and performance under load.
- **CONTENT AGGREGATORS** – bots operated in this category would scan multiple sources on the web such as news, trends, product updates, price changes, stock quotes, etc.

Many businesses have partners that utilize bots to scrape their website for recent changes to product offerings or dynamic ad listings. This is often seen in the hospitality and travel industries. However, these "good" bots can be heavy handed, causing spikes in usage loads on the business' website.

Most bot defense systems aim to accomplish a single goal: block bad bot traffic while allowing both humans and good bots to access the website. Going further, bot defenses need to separate known-good bots from bad, and make sure the known-good bots adhere to established rules and other restrictions.

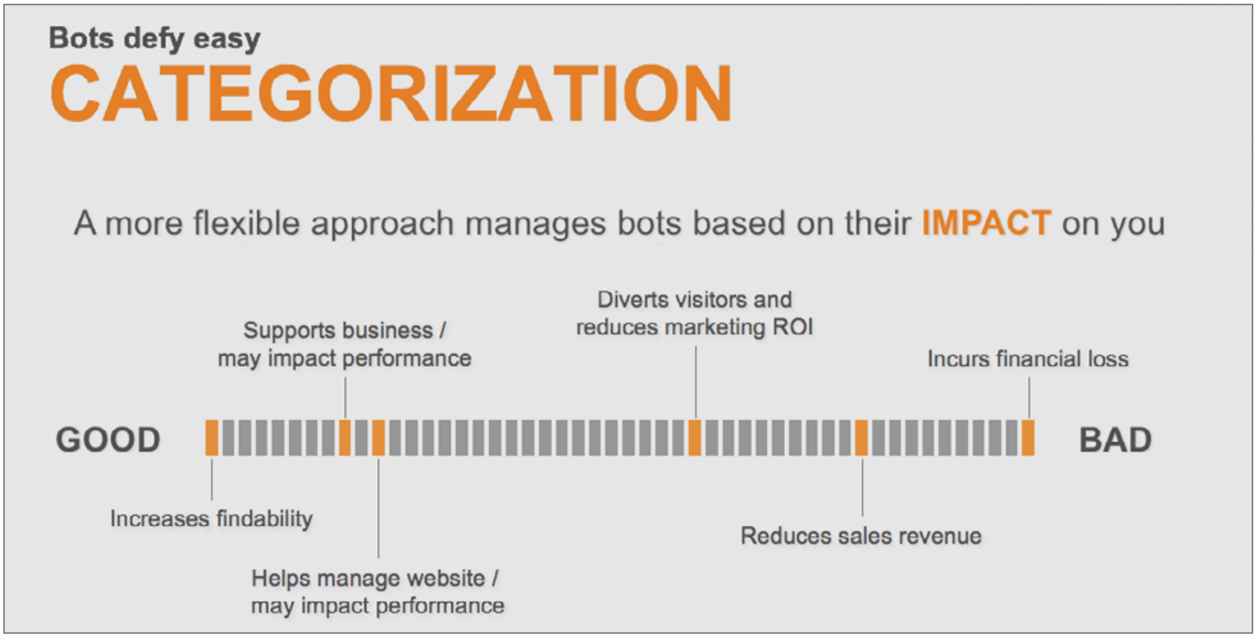

Bots defy easy
CATEGORIZATION
A more flexible approach manages bots based on their IMPACT on you
Supports business / may impact performance
Diverts visitors and reduces marketing ROI
Incurs financial loss
GOOD
BAD
Increases findability
Reduces sales revenue
Helps manage website / may impact performance

**Figure 4:** The impact of bots varies significantly by organization and each business needs to evaluate them differently

Dealing with bots isn't easy. In addition to possible visibility issues, standard defenses like blacklists have a difficult time keeping up.

## EVASION TACTICS:

To avoid detection, the bots visiting your website will employ various tricks and tactics. The most basic evasion technique is altering the User Agent, or other HTTP header values, allowing the bot to impersonate widely used browsers, mobile applications, or even known-good bots.

Bots will also change the IP addresses used in order to mask their origin, or use multiple IP addresses. The IP address change-out is also used to bypass rate limitations, as the bot will use a "low and slow" method where multiple IP addresses send a low number of requests each hour.

Other rate limitation evasion methods include using mobile and API endpoints, as well as morphing IP addresses via proxies, VPNs, and Tor.

Some bots will tamper with browser properties, spoofing known fingerprint characteristics that are often whitelisted. Bots may also do cookie tampering in the hopes of evading detection, such as dropping cookies, or harvesting good cookies and playing them back.

## AN ATTACK WITH MULTIPLE LAYERS:

Recently, several Akamai customers experienced a bot attack from an adversary targeting multiple industries. The attacker leveraged thousands of IP addresses and multiple evasion techniques across several customers. One standout evasion technique was brand new and leveraged at scale, posing a minor challenge until engineers quickly sorted it out.

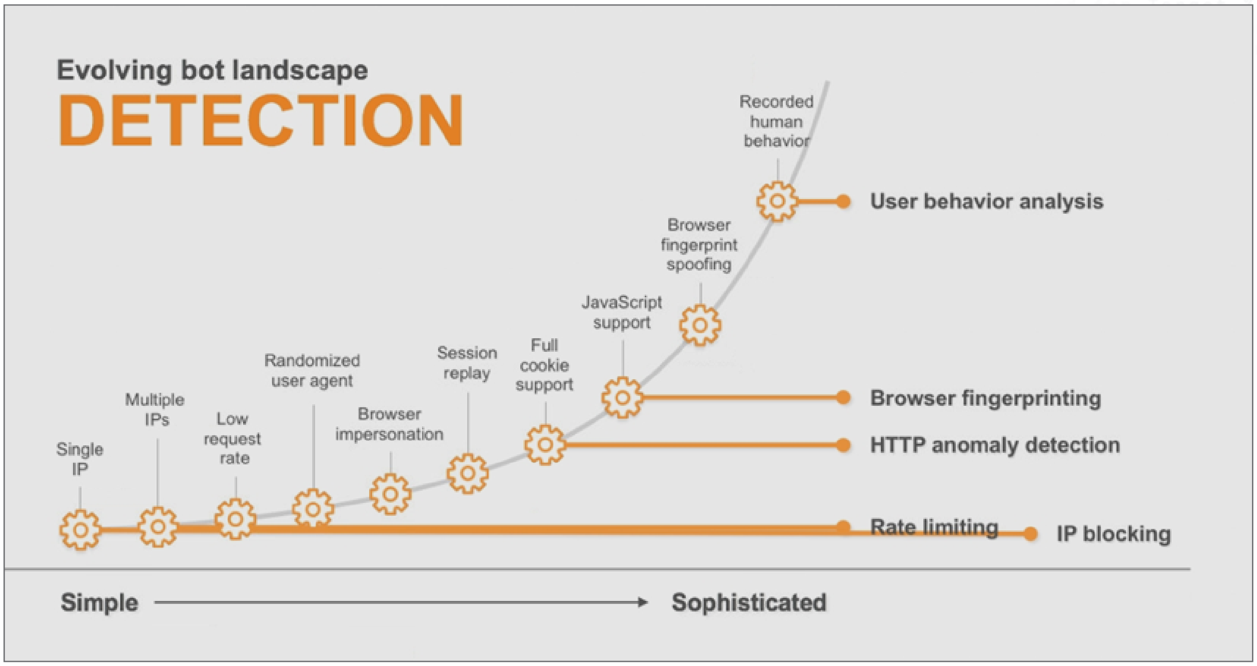


**Figure 5:** Common evasion tactics mapped to their logical defense mechanism, scaled by level of difficulty for the adversarial bot

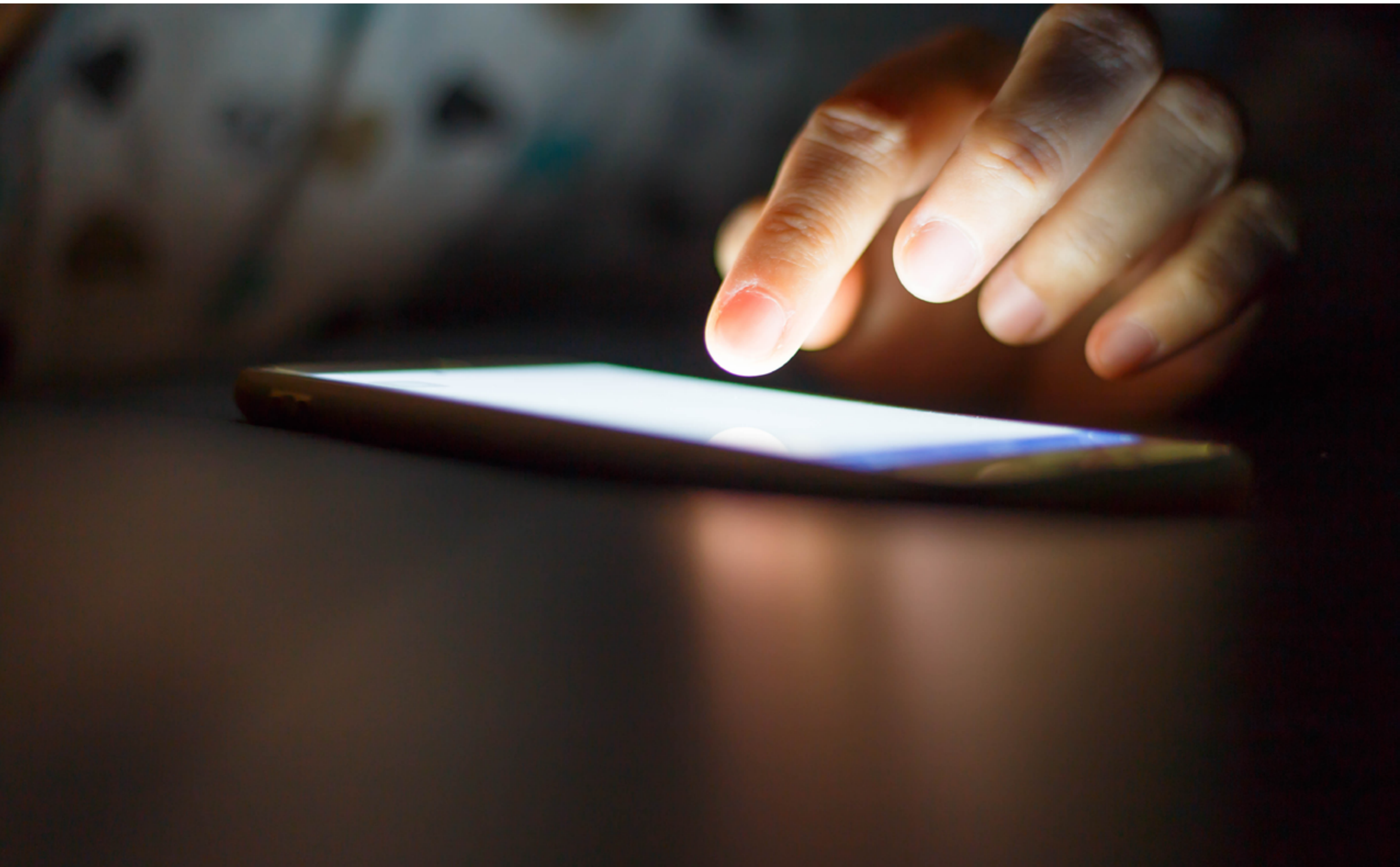
From a research point of view, this multiple-industry attack was interesting because it demonstrated the power of Akamai's visibility into the Internet when dealing with such things. This enabled a solution that won't cause any problems in the future with fingerprint collisions or false identifications towards non-malicious entities.

## A RETAIL EXAMPLE:

In the retail sector, bots are used to purchase items automatically, often taking advantage of sales, limited-edition items, and promotional events. The bot owner will then resell those purchased items at a substantial markup, because their own purchases have increased the rarity of these items in many cases.

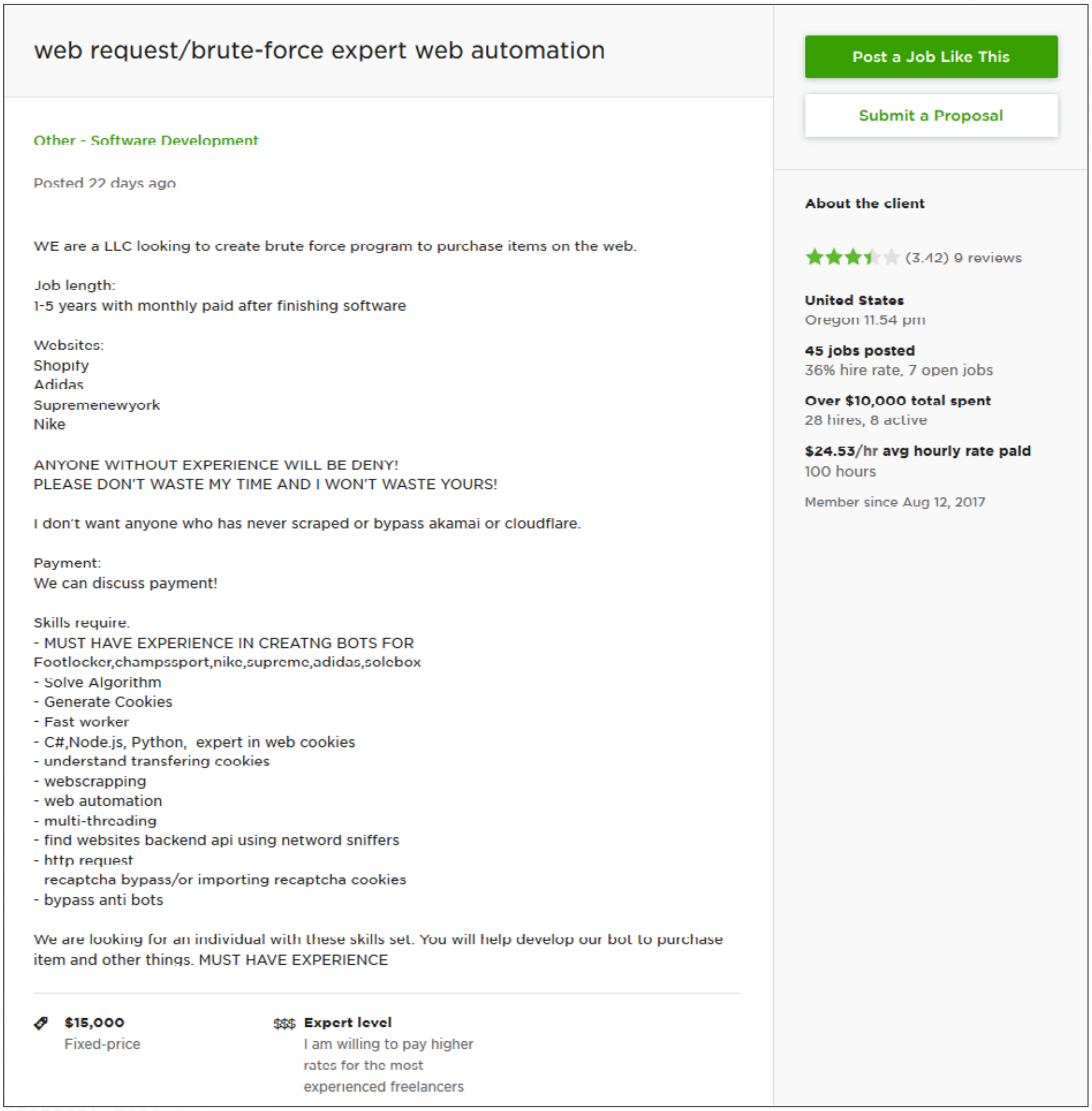
As we've shown, bot owners will leverage evasion tricks when defenses are detected. However, the race to stay ahead of defenders means the bot owners have to maintain a pool of resources. If all else fails, they're willing to spend good money to develop new evasion techniques.

We found a job posting from a bot owner willing to pay $15,000 USD for a developer to "create a brute force program to purchase items on the web." The posting is specifically looking for someone with experience with evading Akamai's defenses for this freelance gig.



The ad goes on to require that the developer be experienced in creating bots for prominent sportswear brands. The bot itself will need to have a number of evasion functions, including anti-bot bypasses, cookie generation, web scraping, API sniffing, reCAPTCHA bypasses, or reCAPTCHA cookie importing.

The person offering the development gig had posted more than three dozen related jobs at the time this screenshot was made, with more than $10,000 spent across 28 hires. Many of the jobs were coding-based, and all of them focused on avoiding bot



web request/brute-force expert web automation

Other - Software Development

Posted 22 days ago

WE are a LLC looking to create brute force program to purchase items on the web.

Job length:
1-5 years with monthly paid after finishing software

Websites:
Shopify
Adidas
Supremenewyork
Nike

ANYONE WITHOUT EXPERIENCE WILL BE DENY!
PLEASE DON'T WASTE MY TIME AND I WON'T WASTE YOURS!

I don't want anyone who has never scraped or bypass akamai or cloudflare.

Payment:
We can discuss payment!

Skills require.
- MUST HAVE EXPERIENCE IN CREATNG BOTS FOR Footlocker,champssport,nike,supreme,adidas,solebox
- Solve Algorithm
- Generate Cookies
- Fast worker
- C#,Node.js, Python,  expert in web cookies
- understand transfering cookies
- webscrapping
- web automation
- multi-threading
- find websites backend api using netword sniffers
- http request
  recaptcha bypass/or importing recaptcha cookies
- bypass anti bots

We are looking for an individual with these skills set. You will help develop our bot to purchase item and other things. MUST HAVE EXPERIENCE

$15,000
Fixed-price

$$$ Expert level
I am willing to pay higher rates for the most experienced freelancers

About the client

★★★☆☆ (3.42) 9 reviews

United States
Oregon 11.54 pm

45 jobs posted
36% hire rate, 7 open jobs

Over $10,000 total spent
28 hires, 8 active

$24.53/hr avg hourly rate paid
100 hours

Member since Aug 12, 2017

**Figure 6:** An example of a job posting for an adversary with experience with company-specific knowledge

defenses. Similar development gigs from other sources were paying just a fraction ($500, in one case) of what this gig was worth, but had little or no interest from the freelance developers on the site.

Another job listing offered $2,000 to a max of three developers, with a $1,000 monthly retainer to develop retail bots with several evasion techniques. Again, the developers applying for the job were required to have experience in bypassing Akamai defenses on retail websites.

## TAKEAWAY LESSONS

Bots are here to stay. As automation is made easier, bots represent both great business opportunities and increased risk. Because there are two sides to this reality, bots should be managed instead of ignored or completely blocked. Businesses should make efforts to distinguish between bots that benefit their website (e.g., search engine crawlers, aggregators, etc.) and bots that negatively impact the business and its customers.

A key advantage when dealing with bots is having visibility into their operation and actions. In the context of known-good bots, this is helpful both in identifying their legitimate origins and characteristics, as well as for identifying impersonation trends. In the context of malicious bots, wide visibility allows for actionable threat intelligence, as well as the ability to cope with sophisticated operators running large-scale campaigns.

## Looking Forward

One of the most important rules of security is "know your environment." You can't understand when something unusual is happening if you don't have a baseline understanding of the norm on the network. This becomes more difficult almost every day as new tools, new technologies, and massive changes happen on the network to meet the needs of the enterprise — but that doesn't mean any organization can stop trying.

We looked at one example of a good tool gone bad in our first story, but it might be a theme you'd recognize from previous State of the Internet / Security reports. It's not that uncommon for a new partner to connect to your APIs, only to forget to properly throttle their requests. The site crawlers that feed search engines are occasionally a source of network outages. Not all attacks are done maliciously — sometimes they are simply a mistake. The impact on the target can still be very negative.

That stands in stark contrast to the tools that are targeting your network. Not the network of a particular type of merchant, not the network of a bank like yours, but actually targeting your environment and your systems to defeat your defenses. It's becoming more common for tools being advertised in the dark corners of the Internet to list a specific set of targets, specifically so the buyer knows they can target your business.

It causes a mixed reaction at Akamai to see attackers targeting our technology in their hiring documents. On one hand, they're targeting us! They are putting more effort into overcoming our tools, our defenses, than they are into other development efforts. On the other hand, it's an explicit verification that we're being effective in stopping the bots they're building. They wouldn't be looking for those skills if our technology wasn't frustrating them. It's kinda cool, in a very geeky way.

If you didn't read Amanda Berlin's essay on mental health early in the report, find a quiet corner to sit and read it now. No career path is without stress, but the path of a security professional seems to be more difficult than many. It's worth pausing for a few minutes to meditate on Amanda's suggestions to see if they apply to you or your team.

Thank you for reading the *State of the Internet / Security* report.

# Appendix A: Methodologies

The data used to create the State of the Internet / Security report is drawn from multiple solutions across Akamai and can be classified into two major networks. These solutions include the Kona Web Application Firewall (WAF), Prolexic DDoS protections, and Bot Manager Premier, just to name a few. These systems form a complex ecosystem designed to protect Akamai's customers. Because of the breadth of our networks, we are able to see a significant portion of all Internet traffic.

The first network is the Akamai intelligent edge security platform, a network of over 200,000 servers in thousands of networks around the globe. In November 2018, this network delivered an average daily peak in excess of 50 terabits per second (Tbps). In early December, multiple patch and gaming releases drove nearly 69 Tbps of traffic over Akamai's network. The Kona WAF is used to protect this traffic, and the information about the attacks is fed into an internal tool called Cloud Security Intelligence, or CSI. This data, measured in petabytes per month, is used to research attacks, understand trends, and feed additional intelligence into Akamai's solutions.

The second major network Akamai provides is the Prolexic platform. In contrast to the distributed nature of the intelligent edge security platform, the Prolexic solutions were created to route all traffic for a customer organization to Akamai data centers, where the good traffic can be separated from the bad. Each data center has been chosen – based on physical location, connections to high-speed interconnected networks, and a long list of other factors – to best serve customers in each region.

"The DDoS Attack That Wasn't" highlights the type and volume of traffic the team at Akamai can see and how issues can require multiple teams to understand and resolve. While the primary issues were discovered and resolved using traffic captures from the Prolexic solution, the expertise of several teams was required to fully understand the issue.

In "More Bots, More Problems," the data was primarily gathered from Akamai's Bot Manager Premier solution. But this is a tool that relies on the synthesis of multiple other data sets, such as web application firewall logs and IP reputation tools. In addition, significant traffic analysis was necessary to understand how the attacker was manipulating traffic to avoid detection. But the single most important tool in our arsenal is experience and human intelligence, as shown by the additional research on hiring practices in the space.

The *State of the Internet / Security* report represents the analysis of the teams across Akamai, and no story is told without their expertise.

# Credits

### State of the Internet / Security Team

Ben Tang, Data Scientist
Elad Shuster, Security Researcher, Senior Lead
Chad Seaman, Security Intelligence Response Team, Senior II
Larry Cashdollar, Security Intelligence Response Team, Senior II
Moshe Zioni, Threat Research, Director
Gabriel Bellas, Practice Manager, Global Services

### Editorial Staff

Martin McKeay, Editorial Director
Amanda Fakhreddine, Sr. Technical Writer, Managing Editor
Steve Ragan, Sr. Technical Writer, Editor

### Guest Author

Amanda Berlin, Mental Health Hackers*

### Creative

Benedikt Van Holt, Art Direction
Brendan John O'Hara, Graphic Design
Georgina Morales Hampe, Kylee McRae, and Murali Venukumar, Project Management

*** Amanda Berlin's views are not necessarily the views of Akamai Technologies, and the article contained herein should not be construed as Akamai providing medical advice or professional counseling.**

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 01/19.