



SOTI 2018

[state of the internet] / security

CREDENTIAL STUFFING ATTACKS

VOLUME 4, ISSUE 4

AT A GLANCE

8.3 Billion

malicious login attempts detected by Akamai from bots in May and June.

Low & Slow

botnets attack across multiple domains, hiding their activity.

300,000

malicious login attempts per hour created by one botnet.

The U.S., Russia, and Vietnam were the largest sources of credential stuffing attacks.

TABLE OF CONTENTS

LETTER FROM THE EDITOR	4
OVERVIEW	5
BACKGROUND NOISE	6
AN OVERWHELMING ROAR	10
WORLDWIDE CREDENTIAL STUFFING	13
LESSON LEARNED	16

LETTER FROM THE EDITOR

MARTIN MCKEAY,
SENIOR SECURITY ADVOCATE,
AKAMAI

“Change
is the only
constant.”

– Heraclitus of Ephesus

Welcome to the fourth issue of the State of the Internet / Security report for 2018. Our focus with this report is the effect of botnets on the Financial Services industry and the continuation of our research into credential stuffing. We are taking a new direction and focusing on a topic other than DDoS, but never fear, we'll cover that topic again soon. If this is your first time reading the State of the Internet / Security report, welcome — and we hope you find the knowledge contained herein valuable.

The term “botnet” covers a lot of ground, from web crawlers to site scrapers to account takeover tools or even DDoS tools. Given that many businesses live and die by their search engine rankings, the bots that organizations like Google and Baidu use to organize the Internet for users are vitally important. But there's a wide range of bots and botnets responsible for things like news aggregation and site scraping where the value to the target organizations is highly dependent upon business models and a host of other factors. We're not talking about any of those in this report.

One type of botnet focuses on a tactic considered malicious by every business: credential stuffing. These botnets attempt to log into a target site in order to assume an identity, gather information, or steal money and goods. They use lists of usernames and passwords gathered from the breaches you hear about nearly every day on the news. They're also one of the main reasons you should be using a password manager to create unique and random strings for your passwords. Yes, remembering that “*.77H8hi9~8&” is your password is difficult, but having your login at the bank compromised is a much bigger hassle.

We see a significant amount of credential stuffing traffic at Akamai — over 30 billion malicious login attempts from the beginning of November 2017 until the end of June 2018. Our stories in this issue cover attacks against two financial institutions that have experienced tens and hundreds of thousands of attempts to log into their sites from credential stuffing botnets. We also continue our efforts to better understand the overall trends in botnet traffic, examining activity in May and June.

Every business is impacted by credential stuffing botnets. Many businesses just see the traffic because of scatter shot scans, but financial services and retail sites are prime targets. Account takeover is profitable for attackers, guaranteeing that it will be a threat for the foreseeable future.

Overview

We chose to highlight two attacks on financial services sites, because they represent high-value targets that are constantly under pressure from credential stuffing botnets. A successful compromise of a bank account or stock portfolio could easily net an attacker thousands, if not hundreds of thousands, of dollars. Given the low risk attackers face for performing credential stuffing attempts, it's no surprise this type of attack is so popular. Luckily, there is an extremely low success rate for most credential stuffing campaigns.

Each of these attacks highlights a number of common themes in credential stuffing attacks. All too often, failed login attempts are viewed as a low-risk threat until a major change in traffic patterns causes administrators to look deeper into logs and network traffic. When a credit union saw a large spike in malicious login attempts, a trio of botnets targeting its site was discovered. While it was the noisy botnet that caught their attention, the discovery of a botnet that had been very slowly and methodically trying to break in was a bigger concern, because of its ability to stay below the radar for long periods of time.

The second example shows a type of botnet that couldn't be ignored. A sudden tripling in account logins was created by a single botnet. Rather than trying to be quiet, this botnet's owner decided to try as many attempts as possible before defensive actions kicked in. Another possibility is that the botnet owner did not understand how to configure its tool and accidentally created a DDoS-like condition. The resultant traffic is functionally identical to a defender.

The data used to create this report comes from two primary sources. The first is Bot Manager Premier — our product designed to use intelligence gathered from across Akamai's many tools to classify bots and help customers combat malicious botnets based on their specific needs. The second source of data is our Cloud Security Intelligence (CSI) platform, which collects data from multiple products across Akamai to help feed intelligence to other Akamai products. Both attack highlights are drawn from the Bot Manager reports and data, while the worldwide trends rely on CSI data. Akamai would like to acknowledge that customer base and location of servers and services influences the trends we are reporting. All graphics were originally created in Excel or Tableau.

Background Noise

Many organizations prefer not to think about credential stuffing unless they see a spike in traffic. Administrators view them as just part of the price of being on the Internet, until the number of malicious logins impacts performance, at which point they deal with the problem. Then it's back to business as usual, because the attacks have gone away. But they really don't stop just because you've dealt with a single attacker. Credential stuffing is part of an expanding ecosystem of attackers coming to your site every day, increasingly using methods that you can't detect without specialized tools.

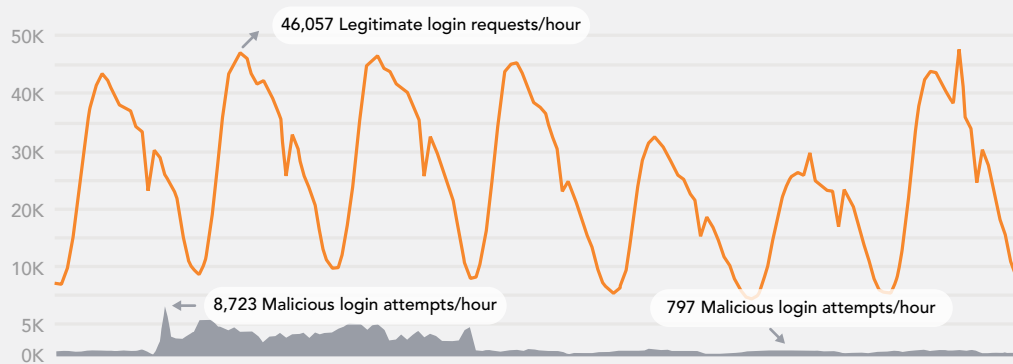
The first example highlights the traffic that a large credit union in North America sees on a daily basis. Because U.S. traffic patterns commonly peak around lunchtime on the East Coast, it is not surprising to see a cycle that peaks in the midafternoon every day and is a little lighter during the weekends. It's also not unusual for this organization to see in excess of 45,000 legitimate logins per hour. Over the seven-day period we examined, there were 4.2 million legitimate login requests by the credit union's customers. At the same time, there was also a steady cadence of credential stuffing attempts, with an attempt rate hovering at 1.5% of legitimate logins. However, one botnet generated enough traffic to get itself noticed and alerted the organization to two other botnets in the process.

Under normal conditions, this site experiences approximately 800 malicious login attempts per hour. Over the course of a week, the site would see more than 100,000 attempts from a diverse set of IP addresses. The assumption was that this traffic level was not targeted and part of the noise all sites experience from the Internet.

The first sign of trouble was a greater than 10x increase in credential stuffing attempts. A spike to 8,723 attempts per hour immediately caught the attention of the site's defenders. This was only the start of the attacks. Over the week, there were 315,178 malicious login attempts from 19,992 IP addresses containing 4,382 different user agents from nearly 1,750 Autonomous System Numbers (ASNs).




fig 1 **Even under normal traffic conditions, low and slow malicious logins are a concern**




For an organization that generally sees a much lower rate of malicious traffic, this was a wake-up call. Many organizations would treat this situation like a DDoS attack: Deal with the symptoms and hope the attack stops soon. However, in the process of defending against this spike, the organization realized there were two additional botnets targeting its site it hadn't noticed before.




The first botnet involved in this series was unsophisticated — a dumb botnet that had a number of easily identified characteristics. This botnet was responsible for 94,296 requests — nearly a third of the malicious login attempts seen over seven days — approximately nine per minute. Similar to normal traffic, this botnet hit peaks at regular times, as shown by this sparkline . This botnet is an example of the “background radiation” that sites constantly experience, 24 hours a day, 365 days a year.

We call this a “dumb” botnet because it’s very simplistic, with all the traffic coming from two IP addresses based on a cloud platform, and every request contained the exact same user agent. Any organization mining its failure logs would be able to detect this botnet as a top talker and create simple rules to either block the IP addresses at the edge of its network or block the user agents closer to the login page of the site. The botnet owner could move to a new set of IPs or change the user agents, but the simplicity of the attack suggests that might be beyond the technical capability of the “bot herder.”

The second botnet is what actually caused the alarm to ring. We would also classify this as a somewhat “dumb” botnet, but for different reasons. The size of this botnet was much more significant, generating traffic from over 10,000 different IP addresses with 695 different user agents contained in the traffic.

This bot herder was impatient and attacked at such a high rate it couldn't escape notice. Over three days, the botnet averaged 59 requests per second and was responsible for 190,487 malicious login attempts, shown in this sparkline . The defenses required to mitigate the botnet used in this attack require deeper examination of the characteristics of the traffic and tools specifically created to defend against botnet attacks. Even though a defender will be able to see the spike in overall traffic, the number of IP addresses the login attempts were coming from makes attempts to block traffic based on the source difficult. Blocking a specific IP address isn't very effective when the attacker is constantly shifting between thousands of them.

A third botnet was also detected during this time. This one was actually the most dangerous and difficult to detect of all three bots. This bot used a "low and slow" approach to attacking the site, averaging one malicious login attempt every other minute. This sparkline shows a high of just over three login attempts per minute . There were 188 unique user agents being used by this botnet, and with a population of 1,500 IPs in use, the average number of requests per IP address was .00035 requests per second. Even though the botnet sent 5,286 malicious login attempts over the week we monitored, the slow rate of the traffic made it difficult to spot and allowed the attacker to remain undetected for long periods of time.

The real danger of low and slow botnets is not how effective they are against a single target, it's how much of an impact they can have on the larger ecosystem. In many cases, the botnet is only using each IP address against a specific defender's site once or twice each day. But the botnet isn't leaving that node idle when it's not attacking your site. Instead, each node is making malicious login attempts against other sites in a rotation. This allows the botnet owner to make the best use of resources and evade detection at the same time. This tactic allows a credential stuffing botnet to remain active and undetected for long periods of time and gives it a better chance of finding vulnerable accounts.

For more information on this type of bot threat, read the following blog posts:

["Improving Credential Abuse Threat Mitigation"](#) by Or Katz and

["What You Need to Know: 'SNIPR' Credential Stuffing Tool"](#) by Daniel Abeles

An Overwhelming Roar

In some cases, credential stuffing isn't background noise; it comes as an avalanche of traffic that looks a lot like a DDoS attack. It might be that the attacker doesn't care about being detected and doesn't care if the botnet it's using will get reported and potentially shut down. Or it might be that the bot herder doesn't understand its tools and forgot to enable throttling to keep the botnet quiet. A third option is that the attack really is an attempt at DDoS — but if that was the goal, there are better ways to use a botnet to achieve it. Even if the real reason is one, all, or none of these explanations, any time login attempts more than triple to a site, the administrators are almost certain to notice and take action!

Our second case study looks at a Fortune 500 financial services institution that saw the number of login attempts jump from an average of approximately 50,000 an hour to over 350,000 in one afternoon. Like many organizations, it was accustomed to having time-related peaks and valleys, but the difference between a daily peak of 100,000 logins per hour and tripling that when traffic should be declining was hard to miss. It was quickly discovered the cause was a credential stuffing botnet sending hundreds of requests a minute.

Looking at normal traffic, this organization saw 7 million legitimate logins over six days. In contrast, the botnet generated in excess of 8.5 million malicious login attempts, with the vast majority of these attempts coming over the span of 48 hours. Between them, nearly a third of the traffic was generated from Vietnam and the United States, but as Figure 3 shows, the traffic came from a wide variety of countries. In total, this botnet consisted of over 20,000 endpoints on 4,923 different ASNs.

fig 2 This is what a botnet that's as subtle as a sledgehammer between the eyes looks like.

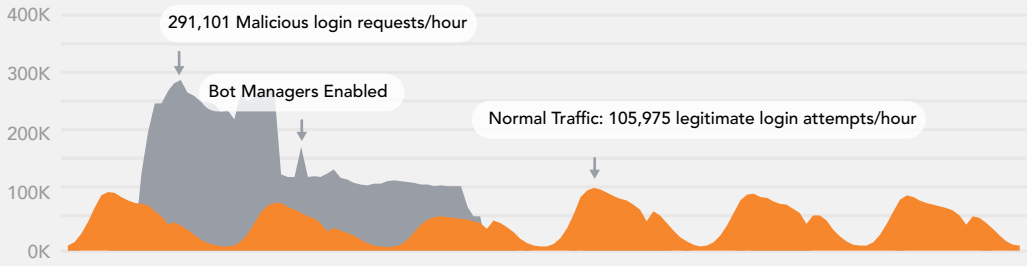
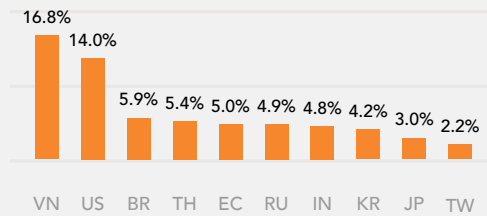


fig 3 Malicious login attempts over the 48-hour period came from many countries; however, nearly a third of the traffic was generated from Vietnam and the U.S.



One of the main identifying characteristics of this botnet was the principal user agent contained in its requests. In total, the botnet used over 10,000 different user agents, which suggests that the bot herder had the technical capabilities to have made the botnet harder to detect. But for this attack, the overwhelming majority, —95% — of the traffic contained the same user agent, identifying the traffic as being from a Samsung Galaxy SM-G531H smartphone, also known as

the Samsung Galaxy Grand Prime. Our research did not include determining if this traffic was coming from compromised smartphones or if the user agent was spoofed. But in either case, given the ease of changing the user agent, it's surprising to see such a big tell left available for researchers to identify the botnet.



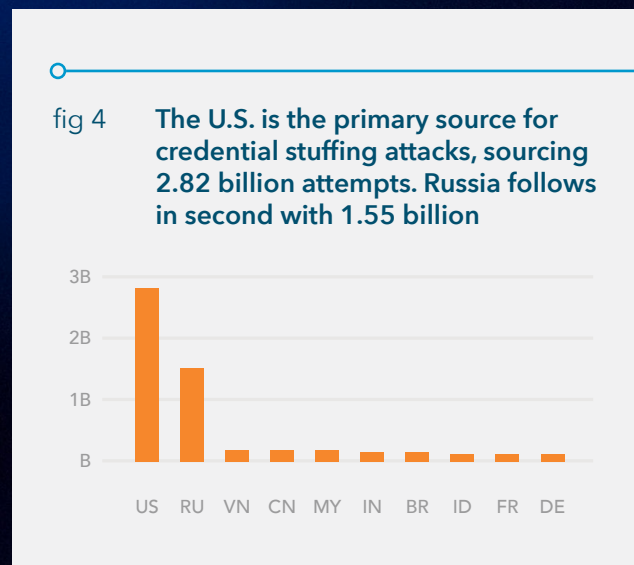
Prior to the attack, the target had not had any botnet mitigation controls in place. When Bot Manager Premier was enabled during the second day of the attack, the impact of the credential stuffing attempts was alleviated immediately. Even then, the traffic continued for more than 24 hours, despite being ineffective. It's likely that the botnet owner either did not realize their tool had been neutralized during that time frame or simply didn't check on the tool for a day.

As is often the case, a few nodes of the botnet are much "chattier" than the rest of the population. A single host generated nearly 37,000 malicious login attempts over the 48 hours the botnet was active and accounted for .7% of the total traffic. While the percentage may not make this seem significant, if all 20,000 nodes of the botnet generated a similar 13 requests per minute, instead of the average of one request per minute, the botnet would have been a crippling attack from the target's point of view.

Whether the sheer volume of login attempts from this botnet was by design or by accident, this attack was a blatant effort at brute force login to this financial services organization. The botherder was likely unconcerned with any reaction, possibly believing that the worst consequences would be a loss of the botnet itself. But for defenders such as Akamai, each attack like this is an opportunity to learn more about botnets and improve the defenses we offer.

Worldwide Credential Stuffing

Between the beginning of May and the end of June this year, Akamai collected data on 8.35 billion credential stuffing attempts across the globe. The data was captured and a set of post-processing heuristics was performed on the logs to identify login attempts across multiple organizations. This allowed Akamai to spot IP addresses that were being used to target multiple organizations. Email addresses as usernames and common field names were used to identify the majority of logins.

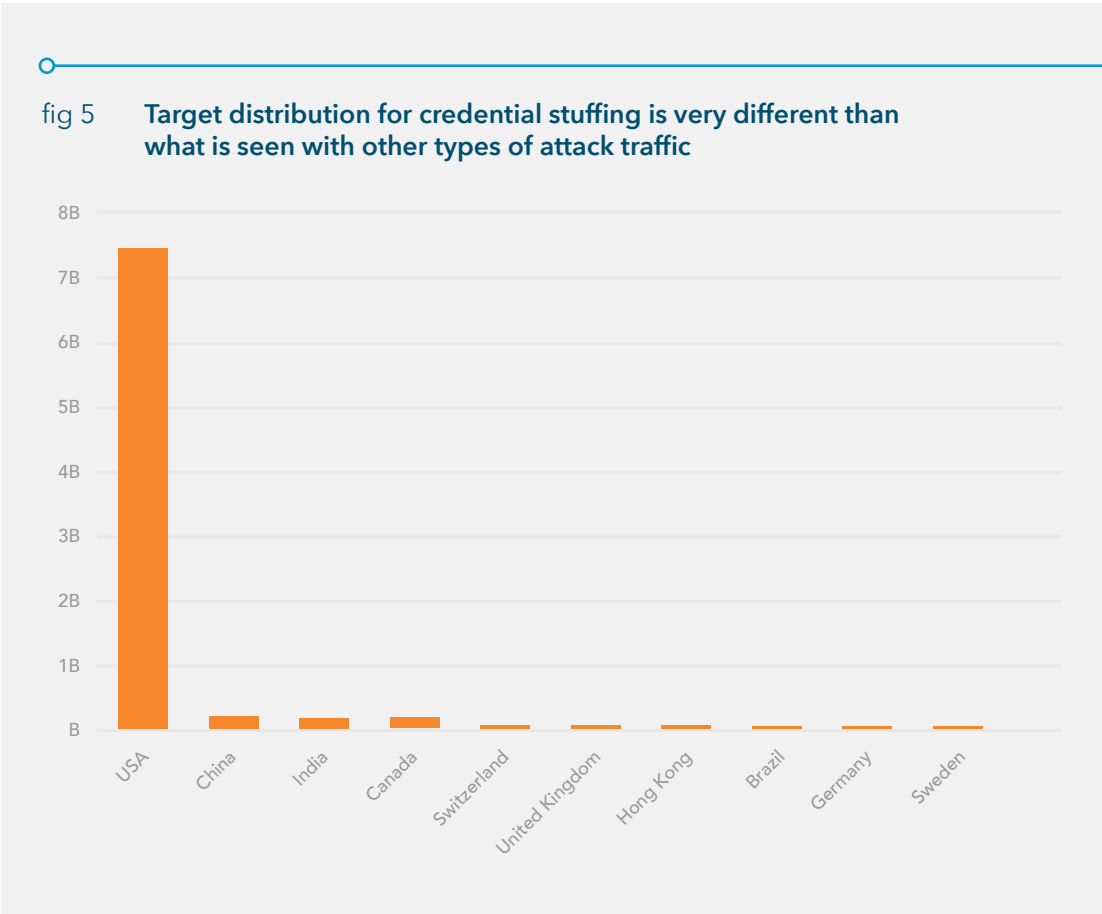


The U.S. was the primary source, responsible for 2.82 billion attempts, followed by Russia, with 1.55 billion credential stuffing attempts. The remaining countries of the top 10 offenders were each responsible for between 250 million and 165 million malicious login attempts apiece. While there are two clear leaders, this is clearly a global problem.

A first look at the destination traffic shows the U.S. as the largest target of credential stuffing traffic by a significant margin. In part, this is

because of the number of businesses relying on cloud services that have their main login sites in the U.S. Akamai's customer base also influences this statistic, but these issues are not enough to fully explain the imbalance by themselves.

One other factor that likely tilts the table towards the U.S.: the makeup of the usernames and passwords contained in the dictionaries used by criminals. While it is slowly changing to become a worldwide trend, it has historically been U.S. companies that have been breached; in 2016, according to Symantec, 90% of all breaches targeted U.S. companies. The usernames and passwords of compromised sites are used to build “dictionaries” that are traded or sold and used by botnets. One such dictionary released earlier this year contained nearly 1.4 billion records. This ratio is likely to change, as the number of international data breaches continues to rise.



When we look past the U.S. attacks, the target distribution for account takeover attempts is dissimilar to other types of attacks Akamai defends against. Canada, Switzerland, and Sweden rarely show up in the list of top 10 targets of DDoS or web application attacks. China is not an unfamiliar target, and although India and Hong Kong aren't generally primary destinations of attack traffic, they make a showing in the credential stuffing data. Clearly, botnets are a worldwide issue.

These statistics reflect the large number of noisy botnets currently scanning the Internet, hoping to find examples of password reuse, not caring what site they find them on. The attempts by these botnets will always find a fraction of a percentage of vulnerable accounts, which is enough to make the attempt economically viable for the botnet owner.



Lesson Learned

In October of 2017, Akamai commissioned a Ponemon report, *The Cost of Credential Stuffing*¹. The strength of survey-based reports like Ponemon's is that they reflect how respondents view the problem in question. There are several common concerns held by defenders that are directly related to the trends in this issue of the *State of the Internet* report.

One of the main reasons many organizations don't have stronger controls to prevent credential stuffing is that 70% of the people surveyed believe the tools needed to defend against these attacks diminish the web experience of legitimate users. The tension between web teams and security teams often revolves around user experiences, with any control that impacts the user experience, and therefore conversion rates, facing an uphill battle from the start. Clearly, credential stuffing defenses need to be able to function without introducing user lag to be successful.

1. The Cost of Credential Stuffing, Ponemon 2017:

<https://www.akamai.com/us/en/multimedia/documents/report/the-cost-of-credential-stuffing.pdf>



A second issue of concern highlighted by *The Cost of Credential Stuffing* is that in 40% of the cases, no one function has overall responsibility for dealing with the attacks. Even in the best of organizations, lack of a clear line of responsibility often means that no one takes responsibility. At best, it means a conscientious team takes charge but faces problems because of a lack of authority. Couple this with the fact that nearly half (48%) of respondents feel their organizations lack sufficient budget to combat the issue, and it can be seen why credential stuffing defenses are lagging in many organizations.

It's easy for an enterprise to underestimate the impact of credential stuffing on its organization. The constant background noise of malicious login attempts can be ignored, unless a spike similar to that shown by our second example hits and impacts customer logins. While those attacks create a lot of noise and show an immediate result, it is the low and slow type of attack from the first example that can be even more dangerous in the long run. After all, an attacker who's willing to run silent can, over time, match or exceed the number of login attempts of a noisy attacker.

As botnets continue to evolve based on defenders' capabilities, point solutions are becoming increasingly ineffective against many attacks. There will always be bot herders with minimal understanding of their own tools. They are the same type of attacker who uses a DDoS-for-hire botnet. These attackers are relatively easy to defend against. But an attacker who understands their own tools, understands their targets' defenses, and has the patience to stay quiet over time requires a very different defense — one that gathers intelligence from many enterprises, instead of just one.

Because credential stuffing is still no one's responsibility at many organizations, it will almost certainly continue to be profitable for the attacker. Until we can raise the negative consequences of these types of attacks, there's no reason for bot herders to do anything else.

State of the Internet / Security Team

Elad Shuster, Security Data Analyst

Renny Shen, Security Product Marketing Manager

Editorial Staff

Martin McKeay, Senior Security Advocate, Senior Editor, Writer

Amanda Fakhreddine, Sr. Technical Writer, Editor

Creative

Shawn Broderick and Sajeesh Alakkaparambil, Art Direction & Graphic Design

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 09/18.

Questions? Email us at research@akamai.com