SOTI SUMMER 2018

[state of the internet] / security

WEB ATTACKS

AT A **GLANCE**

DDOS ATTACKS

SUMMER 2018 VS. SUMMER 2017

16%	16%	4%	38%
increase in total DDoS attacks	increase in infrastructure layer attacks (layers 3 & 4)	increase in reflection-based attacks	increase in application-layer attacks

KEY OBSERVATIONS

SUMMER 2018

- New attack vector: Memcached reflection
- New record DDoS attack: 1.35 Tbps
- 7,822 mitigated DDoS attacks
- Multi-vector reflection attacks using obscure vectors (IPMI and IKE)
- Mirai attacks still ongoing with new variants

WHAT YOU NEED TO KNOW

- The State of the Internet / Security: Web Attack report will be published twice a year going forward.
- DDoS isn't just about volume. Two recent examples of advance attacks highlight adaptable and interesting techniques in use.
- In April 2018, the Dutch National High Tech Crime Unit and the UK National Crime Agency teamed up in "Operation Power Off" to take down a commoditized DDoS platform.
- Russia and China are the sources of an outsized number of credential abuse attacks against the hotel and travel industries.

TABLE OF **CONTENTS**

LETTER FROM THE **EDITOR**

MARTIN MCKEAY,
SENIOR SECURITY ADVOCATE,
AKAMAI

> "Change is the only constant."
>
> *– Heraclitus of Ephesus*

Welcome to the Summer 2018 State of the Internet / Security: Web Attack report. This new naming schema is just one of the many changes you'll notice if you're a returning reader of our Web Attack report, and there are more changes coming as we work to bring you insights and intelligence from our data in as useful and timely a way as possible.

The Web Attack report is evolving into a shorter, leaner report. The Attack Spotlight was released as a stand alone paper. The statistical plots that made up a large part of the report have been published as blog posts. These changes will allow us to publish statistical data in a more timely manner in the future. At the same time, we are moving to more focused reports, published biannually, instead of a larger report published quarterly. Akamai has too many diverse types of data to contain in one report.

The State of the Internet / Security Report is about the changes we see. Our view into the Internet is constantly changing. The State of the Internet/Security: Carrier Insight we first published this spring is one example of how we're adding new capabilities. In this report, the team analyzed DNS lookups by botnet and malware command and control systems to better understand (and block) these threats.

Attackers haven't exactly been resting on their laurels in the last few months, as the new memcached reflection vector generated the largest attack Akamai has seen to date, breaking the 1 Tbps threshold. As a service that was never meant to be exposed to the Internet, and one that had a poor choice for default configuration, memcached became a serious vulnerability in a short time. Our Security Operations Command Center has contributed intelligence on a pair of interesting attacks from intelligent, adaptive threats. There is a lot to be learned both of these attacks.

In our last SOTI Security report, we looked at bot traffic and credential abuse against a wide variety of industries and found some surprising statistics. This quarter, we're taking a deeper look into the attacks directed against the hospitality industry - including hotel, travel, and airline sites - in an effort to understand why five out of six logins at these sites use fake or stolen credentials. We were surprised to find that many of these login attempts were coming from Russia and China, a departure from the general attack trends.

GUEST **AUTHOR**

RIK FERGUSON,
VP SECURITY RESEARCH,
TREND MICRO

The technology that shapes our world and informs the ways that we do business is, of course, in a constant state of change. If I think back to my first visit to my dad's office at Rank Xerox, all I picture is a sea of dark wood desks, unpopulated save for the occasional typewriter (and ashtray). Fast forward through the monochrome monitors, flat-screens and tablets that have littered our desks over the intervening 40 years and we still experience only the merest taste of the change that continues to sweep through industry.

Of course, this change, while gaining life and traction in the R&D backrooms of technology vendors, is not restricted to them. The current industry buzzwords - IoT, IIoT, Machine Learning, Biometrics and Artificial Intelligence - have already changed today's commercial world and will continue to shape the future. Whether we consider soil acidity sensors and livestock monitors in agriculture, cloud-based parcel delivery tracking, or smart traffic lights using AI to manage congestion, these technologies are already firmly embedded in today. So, what of the future?

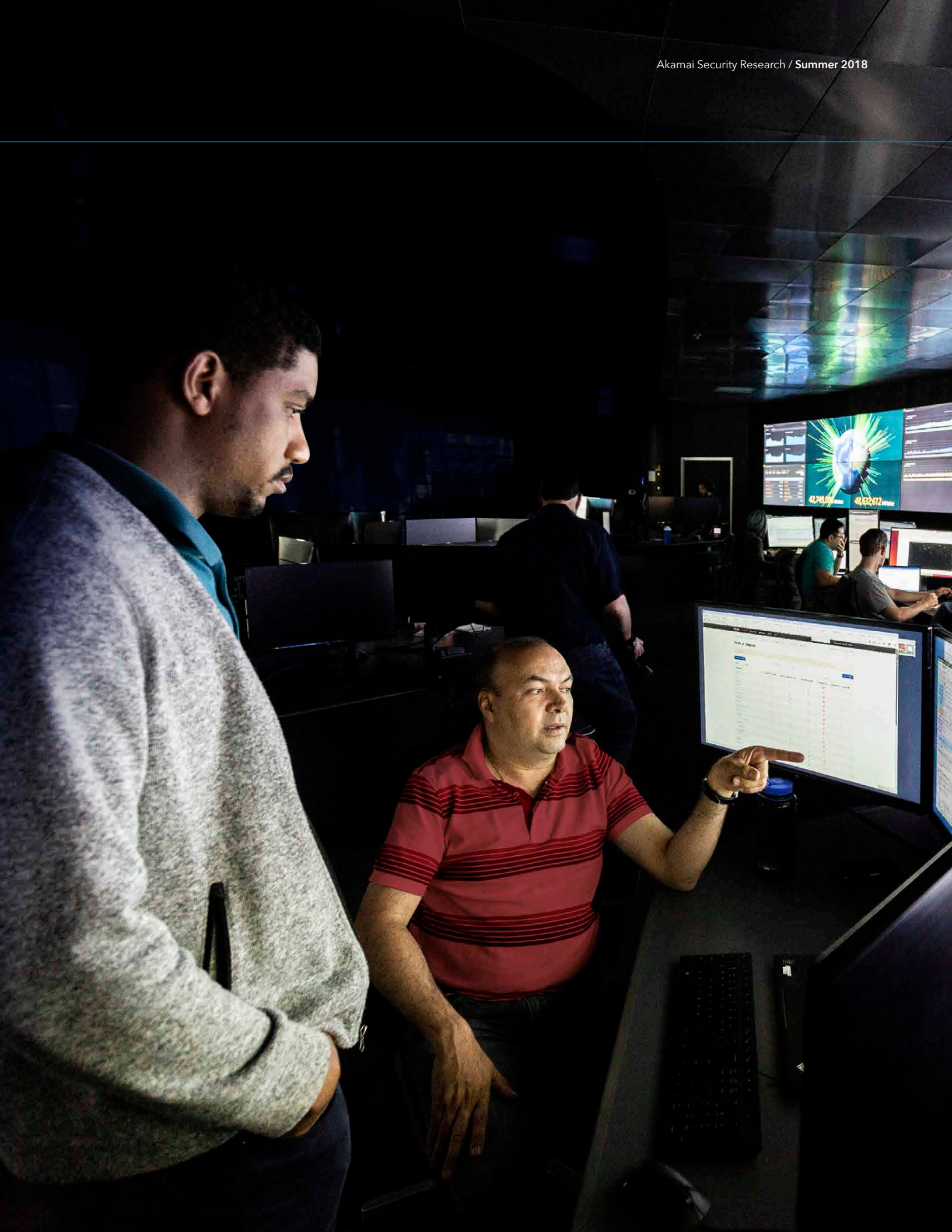
When you work in information security, some proportion of your day will always be spent firefighting, responding to the attacks of the moment. However, when designing a security strategy, it is vital that you design for the threats of tomorrow as well, or you'll never break out of that reactive trap. I'll propose a couple of future threat scenarios where the bad guys also benefit from these advances in technology and leave you to consider how your tools and process might stack up.

These attackers used to use Business Email Compromise to generate payments to their fraudulent invoices, but times have moved on, and so have your defences, making BEC a low-paying gig. Now they have done the research on your organisation, pulled all the online video, audio and still footage of your CEO, and fed it onto an off-the-shelf AI video manipulation tool. They can modify footage in real time, compositing the image of the CEO onto the face and body of the criminal caller. Not only that but the audio allows them to exactly replicate the tone of voice as they initiate a video call to the Director of Finance. You know the rest, it's late on a Friday, it's critical the invoice be paid this week. While change is constant, the crime remains the same.

Another attack group is focussing on ways to repurpose the failing ransomware model. Last month, they took control of a fleet of autonomous delivery trucks, rerouting all of them to downtown Manhattan at only 3 mph. Very quickly it was gridlock, but still it took the victim almost five hours to agree to pay the ransom. Not quick enough for the attackers. They turned their attention to London's Heathrow airport, where they have a connection into the baggage handling system. Taking a leaf from the DDoS Handbook for Success, they sent a message to the airport, "at 2pm we will shut down your baggage handling system until you pay one meeeellion dollars. At midday we will demonstrate our ability to do this, you will have three hours to pay". The airport knows how much is at stake here, they can't take the baggage handling system offline, and a million is small-change compared to the potential compensation, loss and brand damage.

All too often the adoption of technology that drives profits, facilitates business and grants a competitive advantage outstrips the adoption of the technology required to secure those innovations. The change that is required is a closer partnership between the manufacturers and technologists of tomorrow and the security professionals of today. As long as new technology is developed in an ivory tower, security will continue to be an afterthought.

Unparalleled visibility, integration and control, continuous education and improvement, and security embedded in every aspect of the business. Information Security is no longer the Department of No, it becomes the Department of Change.



SECTION 01

Emerging Threats

It's no secret that the end of February marked the biggest DDoS Akamai has seen to date. This 1.35 Tbps attack against a software development company made use of memcached servers as reflectors that enabled attack amplification at orders of magnitude greater than previously seen with other reflection attacks. The first sighting of memcached used in a DDoS attack was a few days before the attacks. This was, arguably, the largest attack seen on the Internet to date.

To understand the scale of such an attack, it helps to compare it to the intercontinental undersea cables in use today. The TAT-14 cable, one of many between the US and Europe, is capable of carrying 3.2 Tbps of traffic, while the Japan-Guam-Australia cable, currently under construction, will be capable of 36 Tbps. Neither of these hugely important cables would have been completely swamped by February's attack, but an attack of that magnitude would have made a significant impact on intercontinental traffic, if targeted correctly.

Luckily, attacks using memcached faded nearly as quickly as they rose. As more attackers incorporated this reflector into their tools, there was less attack bandwidth available for each. Clean-up efforts by administrators also had a powerful impact on reducing the attacks, as they strongly curtailed the number of available memcached servers. Many organizations responded quickly to this threat and protected the servers on their networks.

Law enforcement has not been quiet in the wake of attacks in 2018 either. Europol, the Dutch Police, and the U.K.'s National Crime Agency cooperated in Operation Power Off, which culminated in the takedown of the DDoS-for-hire site webstresser.org and the arrest of the site administrators on April 24. DDoS-for-hire has long been thought to be a low-risk crime, but these efforts are changing the risk-benefit equation for criminals.

Akamai has not yet seen a statistically significant reduction in the number of DDoS attacks arising from these efforts, which is not surprising, as the takedown happened at the end of the data collection period in this report.

SECTION 02

Advanced DDoS Attacks

1 Tbps
Threshold broken by the **memcached reflector**

The majority of DDoS attacks are volumetric, relying on sending enough traffic to the target site in order to clog their pipes, tie up services and generally become a pain for defenders. This type of attack requires very little sophistication or skill, making it perfect for a large variety of malicious entities. But defenders should be aware that there are edge cases and one-off DDoS attacks that don't follow the general form of most attacks.

A 'typical' simple attack might take the form of an attacker downloading a tool like the Low Orbit Ion Cannon (LOIC) created by Anonymous and firing off attacks from their home system. The next step up is using a DDoS-for-hire solution. These websites offer to send traffic, generally using a combination of large botnets and reflection attacks, to the site of your choice for just a few dollars a month; all you need is a credit card. This method is simple but has its own risk for the attacker, since takedown efforts at the end of April netted both the administrators of a DDoS-for-hire site and its customer list as well. We have more on Operation Power Off later in this report.

A small number of attacks show new or unusual variations in attack patterns. This might be the use of a seldom seen protocol, a new method of generating traffic, or perhaps hidden messages in the body of each packet. These attacks aren't necessarily more effective, but their novelty can sometimes gives them an outsized impact. Here are two such examples.

SYN Flood – in excess of

170 Gbps

and

65 Mpps

YouTube Tutorial

The majority of traffic in the first attack we discuss came from a set of traffic generators written in a YouTube tutorial channel by an enterprising 12 year old "developer." The attack was interesting, because rather than attacking a single IP address, it was aimed at an entire /24 subnet. Typically, attacks are aimed at a single host address, or maybe even a few hosts on the target network, so seeing an attack spread its capabilities across multiple hosts is unusual.

This was also a communal attack. Using the tutorial traffic, the programmer's peers (also well below the age of majority from what has been discovered) were writing messages in group chat on STEAM and IRC in order to coordinate their attacks. Not all of the traffic was generated using the tutorial tool. Some members used other tools downloaded from questionable sites, but still coordinated their attacks with the main group.

The attack primarily consisted of a very large SYN Flood - in excess of 170 Gbps and 65 Mpps (million packets per second). Packets per second is an important measurement to be aware of, since some routers and switches will be significantly impacted by the need to keep a large buffer open to track the connections. When the attack wasn't as effective as desired, the traffic moved from targeting a single IP to flooding the full /24 subnet using a SYN ACK flood reflected off of legitimate FTP and web servers across a host of geographies.

fig 2.1 An example of POST flood

```
POST Flood dest port 80  content length 800000
02:28:54.304346 IP x.x.x.x.27115 > x.x.x.x.80: Flags [P.], seq
2735299558:2735299741, ack 3531941806, win 14600, length 183
.e..E....&@.8...%.M....%i..P.    [...'.P.9.1...POST /bet/en-gb HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0)
like Gecko
Connection: close
Host: foo.bar.com
Content-Length: 800000
```

fig 2.2 Packets are often filled with repeated characters or insulting text

```
Ack flood with the following signature destined to port 80
02:55:22.312384 IP x.x.x.x.60518 > x.x.x.x.80: Flags [.], seq
1626053381:1626053917, ack 1741732526, win 5840, length 536.._..
.f.P`...g...P.......a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&
a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&
a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&
a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&
a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&
a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&
a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&
a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b[ ]=&a[ ]=&b
```

Defenders must constantly be re-evaluating the health of their network. Network saturation caused by an attack against a whole subnet can create unforeseen consequences in secondary servers within the same network. It may be more effective to deal with the collateral damage first, since these systems are not the target and may be easier to defend. In the same vein, it's important to supply a list of core assets to any vendor, supplier or other group helping with the defense of the network. There are often unused IP addresses and subnetworks that are less critical in nature that can be ignored or deprioritized while the main threat is being resolved.

Finally, get packet captures. This helps identify the nature of the attack and what tool is being used. Some attackers will even taunt the target with messages in the traffic, which can be useful if there is additional action to be taken by law enforcement.

They're Back Again

The second example highlights another type of uncommon attack, one that exemplifies the persistence of some attackers. Part of the DDoS-for-hire model is that any attack will have a time constraint, so that the owner of the botnet can maximize the use of its tool for many customers. Far fewer attackers have the capability to create or run more advanced tools that can be used for an extended attack.

This series of attacks started mid-morning for the attacker and continued for nearly two days, off and on. Rather than hitting the target's corporate web site, it was the company's DNS servers that came under attack. Unless an organization has external DNS providers, attacking an organization's DNS servers means no one can find them on the Internet. This type of attack is much harder to defend against, as legitimate traffic has to be carefully filtered from attack traffic in order to avoid dropping real customer requests.

The majority of the attack traffic seen was volumetric DNS queries, which ties up network resources and DNS server processing power by, for example, causing the servers to look for random, non-existent names. DNS traffic peaked at 1.8 Gbps and 2.5 Mpps, but rarely for more than several minutes at a time. The attack also included a secondary vector, a TCP-based attack peaking at 120 Gbps and 18.6 Mpps, consisting of PSH/ACK packets.

fig 2.3 **Each randomly generated domain name ties up a little bit of the server's resources**

```
IP x.x.x.x.11266 > y.y.y.y.53: 9092 zoneInit NoChange* [810q][|domain]

IP x.x.x.x.54298 > y.y.y.y.53: 33816[1au] A? Wjtf45ar01vp.foo.bar.com.

IP x.x.x.x.37955 > y.y.y.y.53: 59020 CNAME? ec8q1jtaqipr.foo.bar.com.
```

While the attacker was relying on these two vectors for the DDoS attack, the evidence shows that they were paying attention to mitigation efforts and changing the nature of their attack over time. The DNS queries they used relied on lookups for random strings, but were well-formed and targeting valid DNS servers. As the defenses changed, so did the nature of the attacks, with the PSH/ACK traffic being added to supplement the original DNS attacks. Even the pulsing nature of the attacks was an effort to make them harder to defend against, by wearing down the defenses and defenders, particularly if the defenders didn't have 24x7 coverage.

The DNS portion of the attack required multiple, overlapping controls to effectively limit the impact. First, rate limits were created to prevent the traffic from any IP address or network from overwhelming the DNS servers. Second, GeoIP data was used to review the source of the traffic and make educated decisions based on where the traffic was originating. Akamai's data has long shown that traffic from some regions is more likely to be malicious than the average. PSH/ACK traffic is also a complex vector, as the number of half-established TCP connections tie up network resources and need the use of sophisticated filtering rules to combat.

Defending against an intelligent, adaptive attacker is never simple. Experience, communication and a little luck are all needed. But forewarning and an understanding of what an attacker might be capable of goes a long way in making it easier.

SECTION 03

Abusing Hospitality

In the *Q4 2017 State of the Internet / Security* report, we took our first look into two data sets: the logs from our Bot Manager service and logs focusing on malicious login attempts (specifically, at sites using email as the username). One of the more interesting aspects of this analysis was the discovery that the hospitality industry experiences a much larger proportion of credential abuse attacks relative to other industries among Akamai's customers.

For this report, we take a deeper look into this vertical to understand the nature of both the types of bots connecting to hotel and travel industry sites, as well as what geographic regions credential abuse is coming from. It's important to remember the term "bot" does not refer simply to malicious programs in our analysis. Search engines, partner systems, and business intelligence systems are just several examples of necessary and beneficial bots that are included in our data.

This data includes nearly 112 billion bot requests and 3.9 billion malicious login attempts against sites belonging to airlines, cruise lines, hotels, online travel, automotive rental and transport organizations. The data was collected starting November 2017 and ending April 2018. Bot Manager uses multiple heuristics to identify bot traffic in real time, while the credential abuse data was based on post-event processing to recognize login attempts based on known compromised accounts and responses from login pages.

50B
Events captured by **Akamai**

Cruising By

In our data, it's easy to see that cruise lines are the target of many of the bots we see connecting to sites. Akamai captured 50 billion events targeting our cruise line customers over the last six months, more than twice the connections of airlines and hotels. In comparison, retail targets saw just shy of 800 billion bot events over the same six month period.

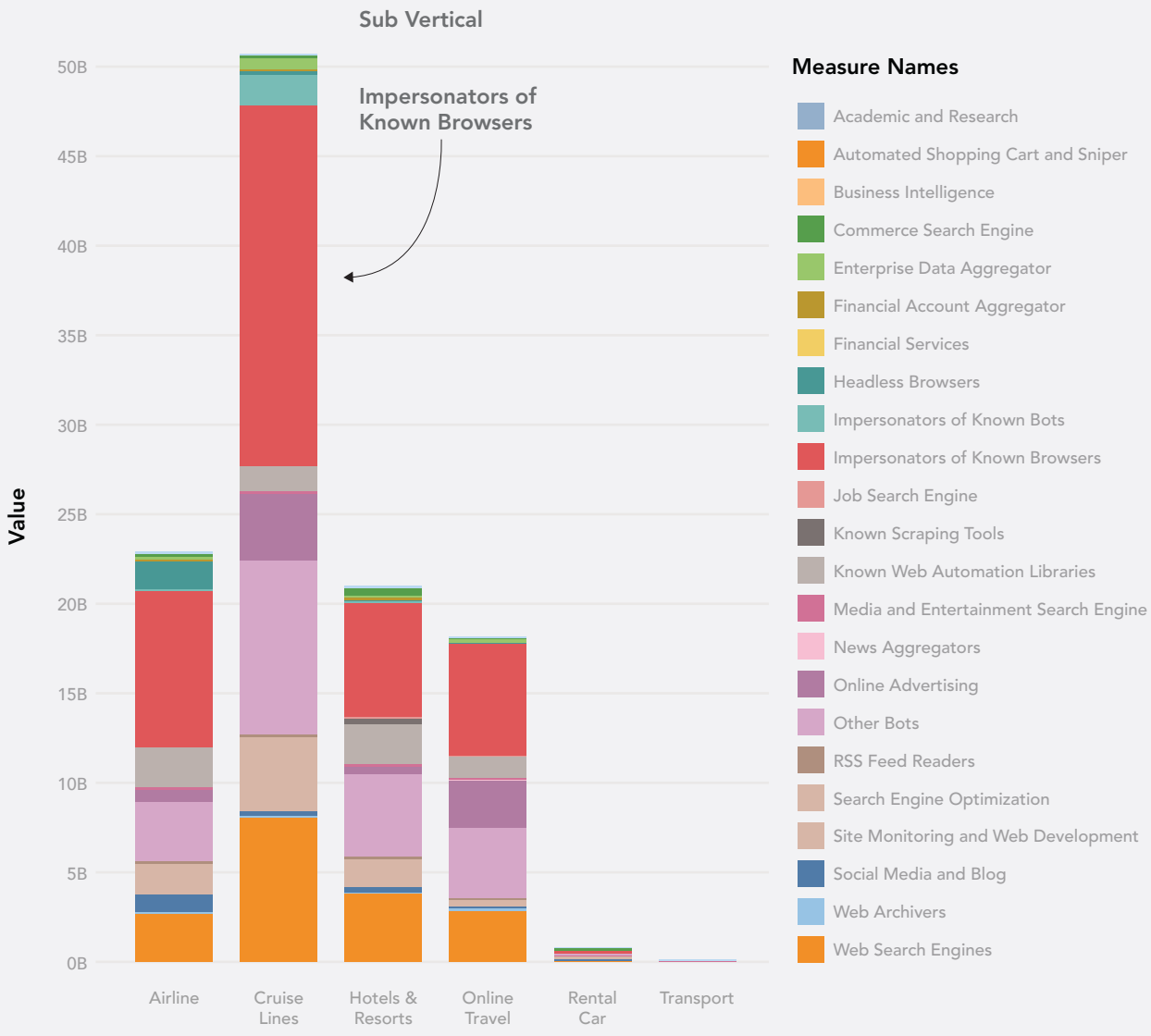
Nearly 40% of the traffic seen across hotel and travel sites is classified as "impersonators of known browsers", which is on par with our data set as a whole. This category refers to bots that are attempting to mimic legitimate browsers but display subtle differences in their traffic. This could be an error in a header, bytes out of order in the packets, or even misspellings in identification fields, just to name a few possibilities.

While there are a number of legitimate reasons a bot might need to use impersonation, more often than not, it tends to be for less than savory reasons. A legitimate bot might be imitating a browser for testing purposes or to pull data from a popular site. A less legitimate reason could be that the bot is trying to evade detection or pretending to be a human being for fraud and abuse purposes. Imitation of mobile device browsers is on the rise and currently one of the most common types of browser imitator.

"Other Bots" is the second most common category of bots seen across hotel and travel sites. Accounting for 20% of detected bot traffic, this is a catch-all for bots that are too new, too old, or too infrequently seen to be easily categorized. This likely indicates that bots that are being changed in order to evade the controls meant to thwart their efforts. Similar to other aspects of security, dealing with malicious (and sometimes beneficial) bots is a cat and mouse game played by software developers.

The third major category of bot traffic seen in this industry comes from web search engines such as Google, Bing, Baidu, and many lesser known search sites. For many organizations, ensuring that search engine bots can reach and index their site is nearly as important as making sure the end user has access. That being said, less well-behaved bots can have a severe effect on a site if they overload servers when attempting to spider through content.

fig 3.1 **Bot Traffic: Hotel and Travel**

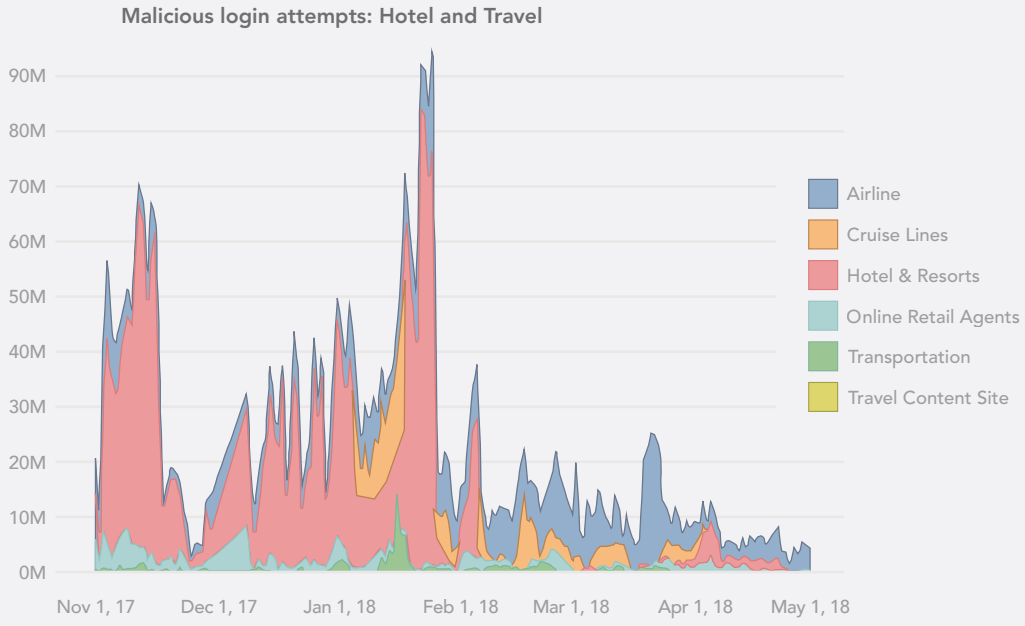


Where Are The Logins Coming From?

There are vast troves of usernames and passwords for sale and download on the Internet, many of which come from compromises like those we see in the news every day. When combined with a pattern of username and password reuse by the public, these dictionaries give attackers a potent tool to compromise user accounts around the globe.

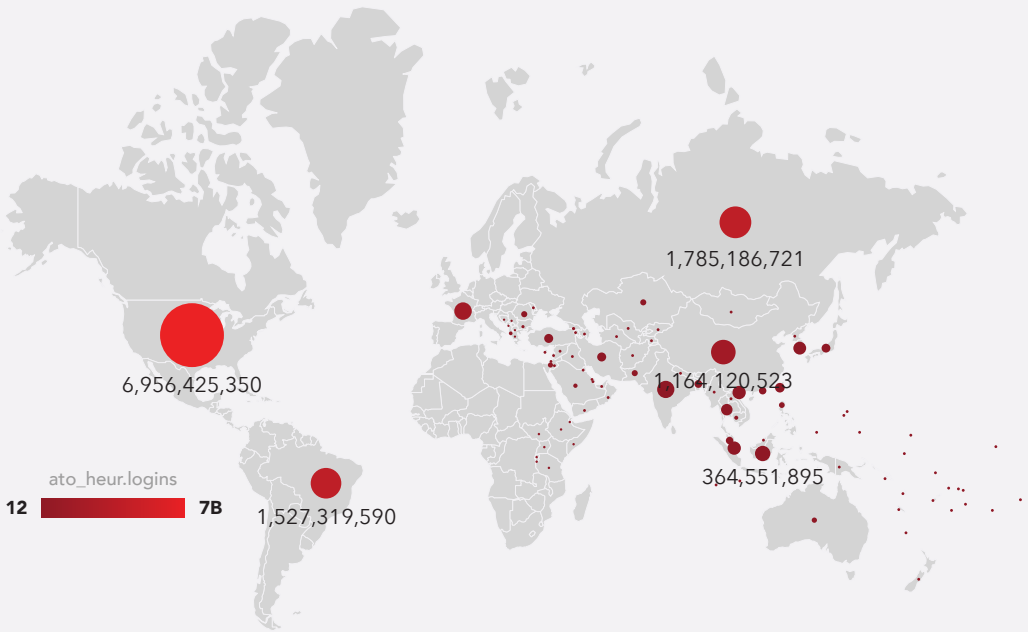
While cruise lines may see the most bot traffic, our data indicates that hotel and resort sites see the most credential abuse connections by far, at least until the beginning of February. At that time, there were changes made to global rules for TLS traffic and the closure of several routes that were the sources of a significant amount of malicious traffic. One theory is that the top few percent of all networks are responsible for the majority of attacks on many networks, which seems to be supported by the steep drop in attack traffic shown in Figure 3.2.

fig 3.2 **The closure of malicious routes resulted in a significant drop in credential abuse**



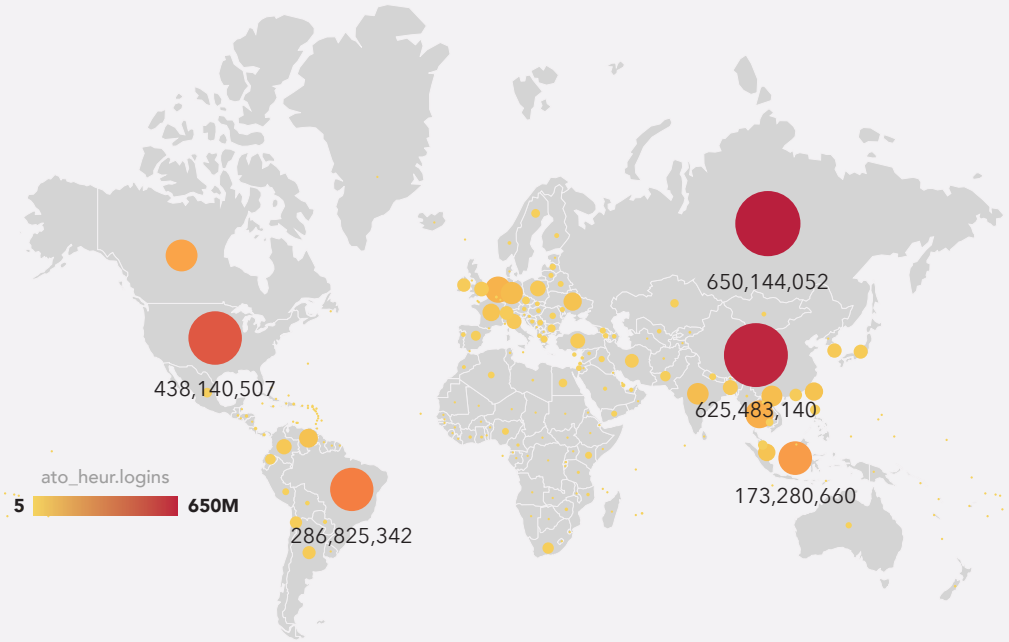
Our examination of the sources of credential abuse led to an interesting contrast between the hotel and travel industry and our overall statistics. Most choropleth maps (that is, maps that use shading, coloring, or a symbol to display a measurement) look very similar. This is because many, if not most, maps of Internet traffic reflect the general population. And when we look at a map of all organizations, this is generally true. There are exceptions, like Brazil and the Netherlands. Both countries have displayed a long-term trend of being significant sources of malicious traffic, while the U.S. is both the largest source and destination of nearly all types of malicious traffic.

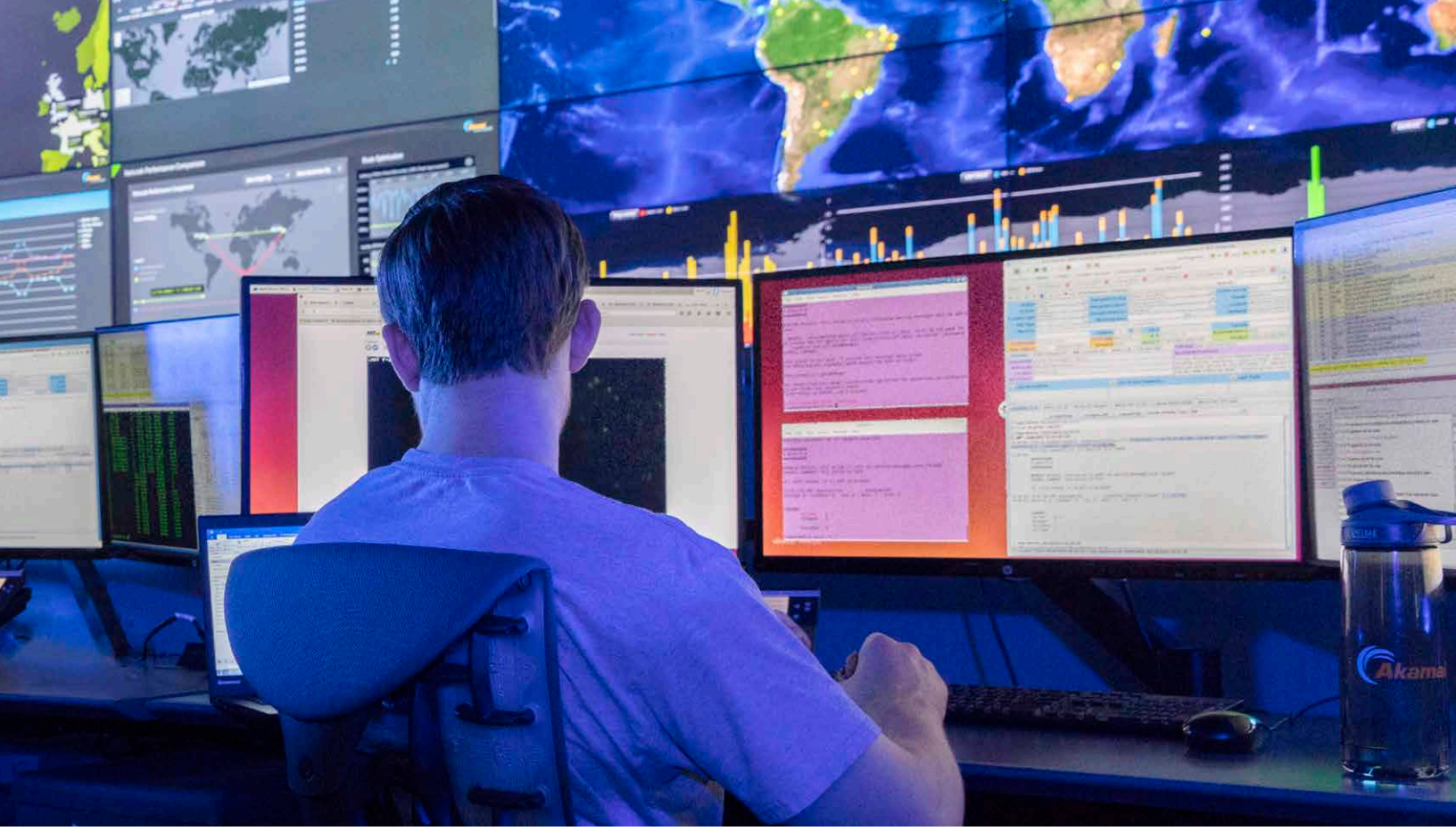
fig 3.3 **Like other attack types, the U.S. is the biggest source and destination of credential abuse**



Limiting the target of attacks to the hotel and travel industries reveals a far different picture, however. Attacks from the Russian Federation and China dwarf other countries; each is responsible for nearly 1.5 times the amount of attacks coming from the U.S. Indonesia also shows a larger role in our map at this level. Approximately half of the credential abuse traffic from Russia, China, and Indonesia is aimed at hotels, cruise lines, airlines, and travel sites.

fig 3.4 **Login Attempts by Country: Hotels and Travel**





There are several possible theories as to why hotel and travel sites figure so prominently in the traffic from these three countries. One hypothesis is that this traffic is coming from organized criminals. If this thesis is true, then there is significant money to be made in compromising the accounts of travelers. Over time, there have been numerous articles highlighting different point-based rewards systems as being tempting targets because they are profitable and hard to track when compromised.

Another possibility is that local knowledge and toolsets make this type of attack easier to exploit hotel and travel systems. In this case, it is less that the attackers are making a bigger profit than from other sites, and more that the knowledge is easier to find and exploit in these regions. This seems a less likely explanation, as many tools and their supporting knowledge are being translated, negating the need for specific local talent.

It's also possible that a very small number of attackers are responsible for throwing off our traffic distribution. While unlikely, it's possible that a small number of criminals are generating hundreds of millions of malicious login attempts. Our data did not show a distinct pattern that would support the likelihood of this theory, but it remains a viable possibility.

One final thought on the sources of credential abuse traffic: The attacker and the attack traffic are not necessarily in the same country or region. As we constantly see with DDoS traffic, bots and compromised systems can hide where the master commands are coming from. Our data may simply be evidence of a large number of compromised systems (perhaps routers) in these regions that are being used to proxy attacks on hotel and travel sites.

SECTION 04

Operation Power Off

DDoS attacks can be extremely disruptive to organizations, and are unfortunately very easy to launch, particularly through one of the many DDoS-for-hire platforms available online. This commoditization of DDoS has a simple model. Anyone can hire one of these services in order to launch an attack. All the criminal needs is a credit card, although many may prefer to use bitcoin for greater anonymity. Then the criminal can use the attack platform of the DDoS-for-hire site to launch their attack. This serves to lower the barrier to entry for the attacker since they are able to leverage a large distributed platform that they do not need to create or maintain themselves.

These commoditized platforms like to make use of terms such as "stresser" in a not so subtle way to avoid being overt about nefarious use. While stress-testing a system is a potentially reasonable use for one of these attack platforms, these enterprises are using the term "stresser" simply to paint a thin veneer of legitimacy on their services.

In April 2018, the Dutch National High Tech Crime Unit and the U.K. National Crime Agency teamed up in "Operation Power Off" to take down one such DDoS platform called Webstresser.org. According to Europol, this service had over 136,000 users who had signed up, and the platform was responsible for between 4 and 6 million attacks over the life of the site. For a nominal fee, customers of this platform could launch attacks that they would likely not have had the capability to conduct of their own accord. These efforts took down a site that was responsible for a number of attacks against Dutch financial organizations last year, but it is only one of many stresser sites being run.

The platform admins were based in United Kingdom, Croatia, Canada and Serbia and were arrested in a coordinated effort with local law enforcement. The associated infrastructure was seized in Netherlands, Italy, Spain, Croatia, the United Kingdom, Australia, Canada, and Hong Kong.

Much like other stresser offerings, the users could pay a small fee, starting at $25 or less, to utilize the platform. In this case, they accepted PayPal and Bitcoin. They treated this as a business and did little to mask the illegal nature of their endeavor. This was a massive and successful undertaking by law enforcement, but Webstresser.org was merely one of many such services available to criminals today. This underscores the need to have proper denial of service and web application firewalls in place to mitigate attacks.

SECTION 05

Looking Forward

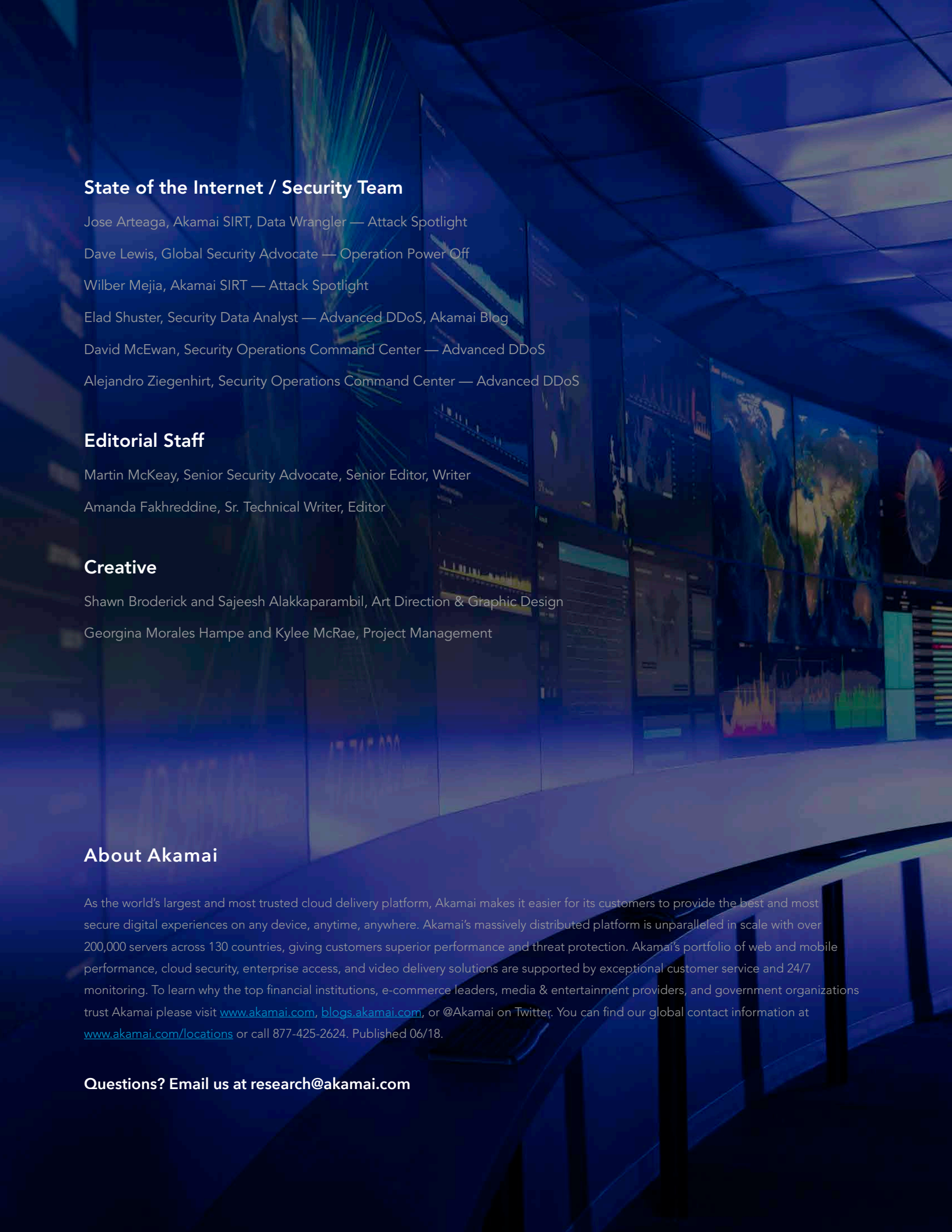
The evolution of the Akamai State of the Internet / Security report will continue for the foreseeable future, and we hope you like the changes you see. If you have feedback -- something you like, something you hate or something you'd like to see more of -- please let us know at SOTI@akamai.com.

While we have control over the look and feel of our report, the threat landscape of the Internet is strange and unpredictable. Most people had never heard of the memcached service before the attacks in February. While protocols like DNS and NTP are useful, garden variety reflection tools, the next big source of reflection traffic could easily be coming from another network service only a niche set of administrators have heard of. It's also quite possible that the next big attack will be led by a class of compromised Internet of Thing devices with hard-coded logins.

Don't be surprised to see larger, more destructive DDoS attacks before the end of 2018. Bandwidth keeps growing and Internet connectivity continues to extend into every region of the world. You might be able to get a 5G connection at the top of Mount Everest in just a few years. But extending connectivity means more devices in those new regions, many of which will never see a software update in their lifespan.

Tracking the global trends of attack traffic and being aware of the attacks hitting networks each day are important. But it's usually more interesting to find the new or unusual attacks, the edge cases that no one else has seen or recognized. Good security practitioners are constantly looking for something new to learn; no one should choose this profession because they want to do the same thing over and over again.

We have previously reported on DDoS and web application attacks every quarter, but no more. We'll be back at the end of the year with our Winter report, but in the meantime, expect to see us tackling new data sets, investigating new problems, and analyzing new attacks. One thing Akamai doesn't lack is data. The hard work comes in making sense of it, making it relevant, and sharing it -- and that's what we strive to do.



State of the Internet / Security Team

Jose Arteaga, Akamai SIRT, Data Wrangler — Attack Spotlight

Dave Lewis, Global Security Advocate — Operation Power Off

Wilber Mejia, Akamai SIRT — Attack Spotlight

Elad Shuster, Security Data Analyst — Advanced DDoS, Akamai Blog

David McEwan, Security Operations Command Center — Advanced DDoS

Alejandro Ziegenhirt, Security Operations Command Center — Advanced DDoS

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

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please 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 06/18.

Questions? Email us at research@akamai.com