Editor’s Note

Security teams are increasingly becoming an integral part of business, and are more vital than ever to success. They have evolved and are increasingly seen as legitimate business partner and growth enabler.

One of the more important factors for a security team to be considered a business partner is their ability to identify the risks that the business faces. Identifying risks is not an exact science. Many security teams understand the nuances in the risks associated with various technologies – however, it can be a difficult process to identify the potential risk and how it will impact the business. This becomes even harder when businesses and security teams are faced with unknowns that the organization has virtually no visibility into. All three stories in this edition of the State of the Internet / Security report cover topics we feel organizations are not as cognizant of as they should be.

### Rise of API Traffic

Our October 2018 survey of API traffic revealed that 83% of the hits we see are API driven.

For security practitioners, growth in API volume is important when considering risk, because some tools can’t handle it. If current tools aren’t able to handle this traffic, it means an organization could be missing a major source of malicious traffic. With the proliferation of IoT devices, API traffic will be something that all organizations will have to deal with to keep their businesses and customers protected.
Tools of Mass Retail Destruction

We took a further look at credential stuffing as it relates to the retail industry in this report. Akamai detected nearly 28 billion credential stuffing attempts between May and December 2018. This works out to more than 115 million attempts to compromise or log in to user accounts every single day.

The hardest-hit industry? Retail took the top spot, with 10 billion credential stuffing attempts directed toward it. The apparel vertical experienced 3.7 billion attempts, making it the largest targeted vertical within the retail industry during the same timeframe. Akamai also tracked credential stuffing attempts against direct commerce (1.427 billion); department stores (1.426 billion); office supply stores (1.3 billion); and fashion, such as jewelry and watches (129,725,233).

**Figure 2:** Four of the top days for credential stuffing are highlighted between May 1 and December 31, 2018
Bad actors are using tools known as AIOs, or All-In-One bots, to access accounts and automate purchasing. Some AIO usage fuels the resale market, while other AIOs are used to control existing accounts or collect valuable personal and financial information.

Is IPv6 Being Underreported?

Researchers also looked at DNS traffic to reveal an interesting fact: IPv6 traffic might be underreported since many systems capable of IPv6 usage still prefer IPv4. Since IPv6 is still seen as a minority of traffic, it’s not a major selling point for a number of security tools.

Looking Forward

The security world encompasses virtually everything now, and security has taken center stage when it comes to business planning and growth. Gone are the days where businesses can treat security as an afterthought.

Each of the stories in this issue of the State of the Internet / Security report looks at aspects of security that might be overlooked, but they are nevertheless important for day-to-day operations. These stories create a backdrop for what we expect to see in the upcoming quarters and years.

If you are interested in learning more about the methodologies that were used to curate the data in the report, we have included an entire section that delves a little deeper.

For a more in-depth look at these stories, please download the full State of the Internet / Security: Retail Attacks and API Traffic report.