Editor’s Notes

Happy 2019! It’s a new year, and what better time to look back at 2018 to fully prepare for what is heading our way? Looking at things that occurred, and how your team reacted to them, should be something to have an open and honest conversation about. What are your short-term and long-term goals for your business and your security teams?

This kind of foresight and goal setting is what will hopefully set your business up for a successful year. Since security professionals are in the business of trying to predict and protect, stress is—anecdotally speaking—a concern in our careers. Conferences have started to create specific tracks on stress and burnout within this industry. Amanda Berlin of Mental Health Hackers is our guest author for this edition, and she tackles the issue head on.

The DDoS Attack That Wasn’t

Sometimes an “attack” isn’t exactly that. What at first looked like a massive DDoS attack turned out to be a warranty tool gone haywire.
Traffic volume reached 875,000 requests per second at one point. Originally, the traffic from earlier visits to the customer’s domain were a mix of GET and POST requests, but during the incident, that traffic turned to an unrelenting stream of POST requests that almost crashed the database Akamai uses to log such things.

More Bots, More Problems

Bot defense systems aim to accomplish one goal: Block bad bot traffic, while allowing both humans and good bots to access the website. However, when a majority of the traffic to your online business presence comes from bots, there can be a profound ripple effect. 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.

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. And those bad bots? They’ll try anything they can to avoid detection. Bots are big money for attackers, and they’re constantly evolving to circumvent new defenses.

---

**EVOLVING BOT LANDSCAPE**

**DETECTION**

- User Behavior Analysis
- Browser Fingerprinting
- HTTP Anomaly Detection
- Rate Limiting
- IP Blocking

**Simple**

- Single IP
- Low Request Rate
- Browser Impersonation
- Full Cookie Support

**Sophisticated**

- Multiple IPs
- Randomized User Agent
- Session Replay
- Javascript Support
- Browser Fingerprint Spoofing

**Rate Limiting**

**IP Blocking**
Looking Forward

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. As we continue on into 2019, we expect to see attackers utilizing the new tools, technologies, and techniques to try to circumvent the protections we put in place.

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

For a more in-depth look at these stories, please download the State of the Internet / Security: DDoS and Application Attacks report, Volume 5, Issue 1.