[state of the internet] / security

A YEAR IN REVIEW

EXECUTIVE SUMMARY: VOLUME 4, ISSUE 5

EDITOR'S NOTES

Since November 2017, Akamai's research team has published an average of more than one article, blog post, or paper a week. These range from posts about upcoming events, to crisis communication about emerging threats, to the State of the Internet / Security report itself. This is why we decided to look back at our work and how it fits into the larger security story of the past year. With that in mind, we've asked our Chief Security Officer, Andy Ellis, to reflect on where current trends might lead us in 2019. The following is an excerpt from his essay.

OFFICE OF THE CSO

> **"plus ça change, plus c'est la même chose —**
> Jean-Baptiste Alphonse Karr

If there is a single truth about trends in the Internet security space, it's that every year brings more of the same. In 1998, during Operation Desert Fox, adversaries used a distributed denial of service attack, which also leveraged the *teardrop* vulnerability, to attempt to bring down USCENTAF networks (I was the defensive engineer on duty at the time, so I remember the excitement of identifying the attack, testing a config, and pushing it out to our perimeter security systems). This isn't strategically different from actions taking place in our, and other, Security Operations Centers every day — only the scale and automation have changed.

So as we look forward into 2019, it is easier to note ongoing patterns from the past few years, suggest they'll continue, and surmise that they'll likely continue to evolve mostly in the ways that they have been advancing.

Akamai
Experience the Edge

BRUTE-FORCE DDoS

DDoS is always a great place to start, mostly because the trends in DDoS are remarkably stable. It might be easiest to think about attacks along two different axes: leverage and bandwidth. *Bandwidth* is simply the measurement of traffic an adversary can generate at any given time. Historically, we've seen the size of the largest attack grow by about 9% per quarter, which nets out to doubling every two years. But, fascinatingly, that isn't a continuous growth. A new peak gets set — along that 9% QoQ curve — whenever an adversary discovers a new way to build a botnet or reflection, as in the case of Mirai or memcached reflection attacks.

Between new peaks, two things happen. First, affected parties, like systems administrators and ISP operators, take action to reduce the number of systems available for use in attacks. Second, adversaries begin to fight for control of these resources, and we see botnets begin to fragment, causing individual attacks to become smaller.

From an effectiveness standpoint, this isn't actually detrimental to the attacker. DDoS defense styles don't generally scale linearly in size. The largest attacks occur at the edge of the network, where services like Akamai's Kona Site Defender or Prolexic Routed live. Mid-tier defenses live in the core of ISPs, providing "clean-pipe" services to site owners. The smallest defenses, on-prem solutions, live solely inside target data centers. For an adversary whose botnet isn't large enough to target an edge-based defense, an attack on someone using only data center-based defenses can still be effective — even at a hundredth of the size.

Given that bandwidth-based DDoS attacks come in many shapes, it's interesting that the maximum size of the attacks appears to be constrained by a 9% quarterly growth curve. Interesting, but not inexplicable. Rather than being caused by some naturally occurring limit, the most likely explanation is that the underlying growth of the Internet limits the aggregate capacity of botnets. The Internet's capacity attenuates the total throw weight a DDoS attack can generate; the farther a target is from components of a network, the less traffic that will make it across any congested links between the target and the attack source.

For more of Andy's thoughts on DDoS, application-level attacks, credential stuffing, the gig economy, and blockchain, please download the **State of the Internet / Security: A Year in Review** report, Volume 4, Issue 5.

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 12/18.