Attack Trends and Mitigation

Matt Jansen
Akamai Technologies
APF 2015, Bangkok, August 12\textsuperscript{th} 2015
The Akamai Intelligent Platform

The world’s largest on-demand, distributed computing platform delivers all forms of web content and applications

The Akamai Intelligent Platform:

- **175,000+** Servers
- **2,000+** Locations
- **1,300+** Networks
- **700+** Cities
- **108+** Countries

**Typical daily traffic:**
- More than **2 trillion** requests served
- Delivering over **30+ Terabits/second**
- **15-30%** of all daily web traffic
The datapoints in the following slides are primarily derived from attacks seen on Akamai’s CDN, DNS and Scrubbing Center platforms.

While those are very large scale and do see a significant amount of attacks those are not necessarily representative of all global traffic, and are biased towards those targeted at the set of customers using Akamai’s services.
Attack Trends 2015

- significant increase in number of DDOS attacks
  - More than double YoY
  - 35% compared to q4 2014

- average peak volume decreases
  - function of there being more attacks
  - does not mean there’s less big attacks!

- average duration increases
  - now over 24hrs

- DDOS for hire

- Online gaming platforms still top target
Attack Trends 2015 – Size distribution
Attack Trends 2015 – Attack Types

Percentage

- ACK: 1.99%
- CHARGEN: 5.78%
- DNS: 5.93%
- ICMP: 3.59%
- XMAS-DDoS: 1.15%
- SNMP: 1.15%
- SSDP: 20.78%
- SYN: 15.79%
- UDP FLOODS: 13.25%
- UDP FRAGMENT: 12.00%
- NTP: 6.87%
- Other: 2.40%

- FIN PUSH (0.15%)
- RESET (0.65%)
- RP (0.45%)
- SYN PUSH (0.35%)
- TCP Fragment (0.05%)

Infrastructure DDoS Layer: 90.68%
Application DDoS Layer: 9.32%
Attack Trends 2015 – Mega Attacks
Attack Trends 2015 – Source Countries

DDOS Attacks (non spoofed addresses)

Web Application Attacks
Reflection Attacks

- hides origin, difficult to attribute
- preserves botnets longer
- amplifies attacks
- less resources needed by attacker
- uses ‘legitimate’ protocols
- harder to detect/filter
- have been around for a long time
- target protocols shifting
  - SSDP new top vector (consumer devices)
  - NTP/DNS declining
Reflection Attacks

- NTP
- DNS
- SSDP
Complex Attack Example
Web Application Attacks

- as seen by our CDN/WAF platform
IPv6 and Security
CDN Platform
CDN Platform

- ‘build in’ DDoS protection
- very widely distributed
- Web Application Firewall option
DNS Platform

- anycast based
- widely distributed
- custom DNS software
Scrubbing Center Platform

- anycast based
- redirecting traffic to protected prefixes via scrubbing center
- clean traffic gets delivered to customer via GRE tunnel/MPLS IPVPN/dedicated link
Peering and Security
Questions?

Matt Jansen mj@akamai.com

as20940.peeringdb.com