Akamai

FASTER FORWARD

State of the Internet Security – Q2 2017

Mihnea-Costin Grigore
Security Technical Project Manager

Topics

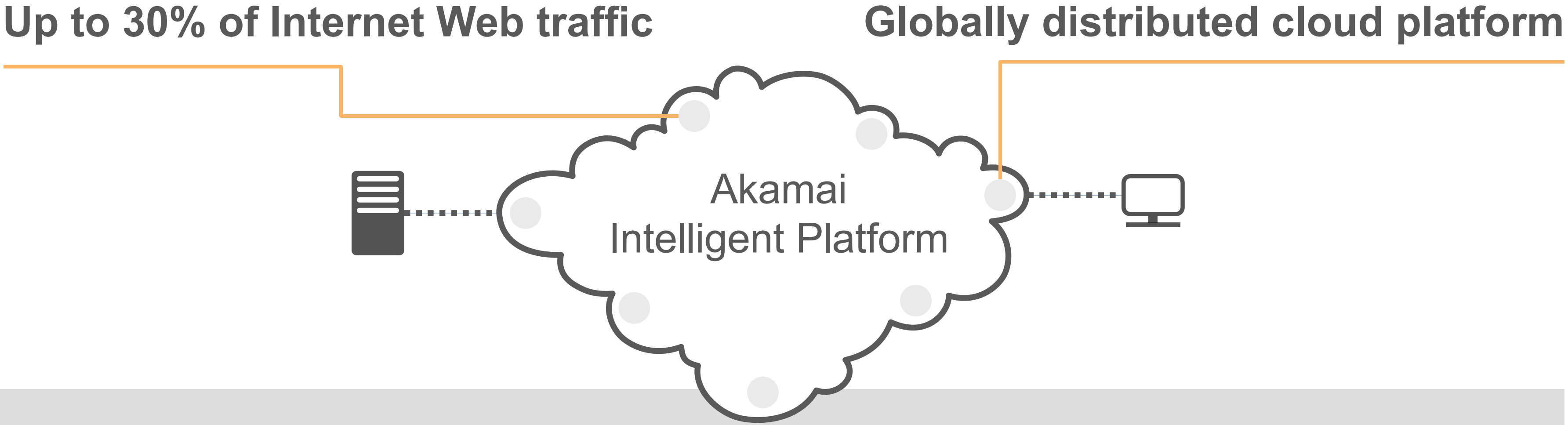
1. Introduction
2. DDoS Attack Trends
3. Web Application Attack Trends
4. Spotlights
5. Resources

Akamai

FASTER FORWARD

Introduction

Introduction – Akamai Intelligent Platform

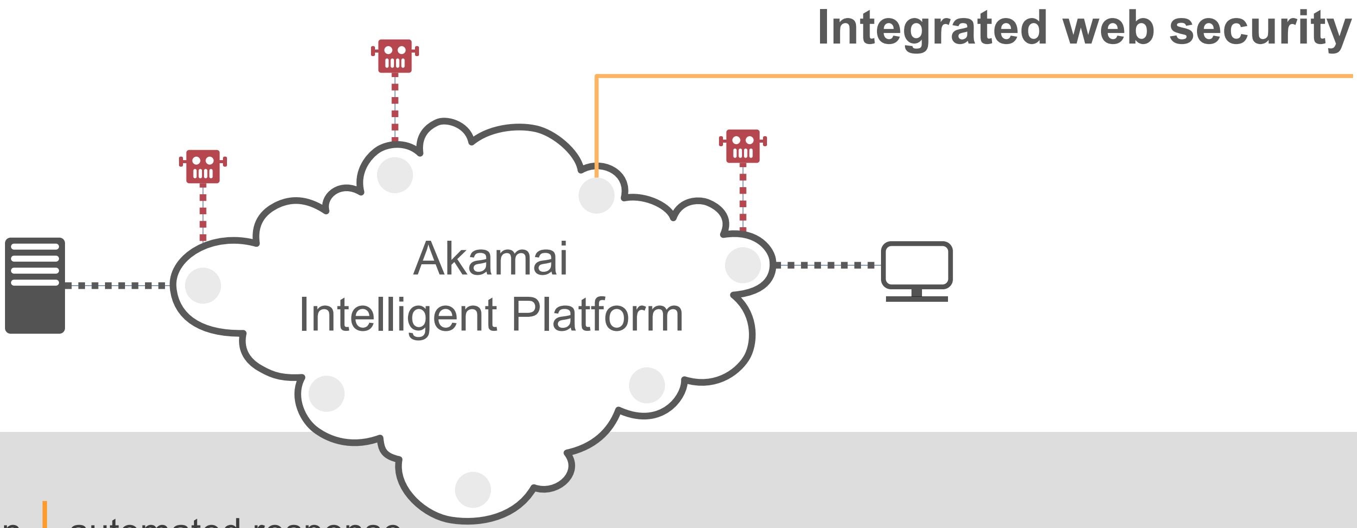

Up to 30% of Internet Web traffic
Globally distributed cloud platform
Akamai
Intelligent Platform

Scale | over 230,000 servers | seven scrubbing centers | thousands of name servers

Distribution | 120 countries | over 3,200 locations | more than 1,400 networks

Resiliency | automatic failover within network | multiple networks for independent services

Introduction – Akamai Cloud Security



DDoS | always-on | automated response

WAF | proprietary rules engine | highly accurate | no performance impact

Bot management | manage, not mitigate | customisable | granular visibility and reporting

IP reputation | hundreds of millions of IPs monthly | custom policies based on risk of attack

Akamai

FASTER FORWARD

DDoS Attack Trends

Compared to Q2 2016

18% ↓ Total DDoS attacks

17% ↓ Infrastructure layer (3 & 4) attacks

13% ↓ Reflection-based attacks

19% ↑ Average number of attacks per target

DDoS is a cyclic phenomenon. Attacks were down from Q2 last year, but not as much as might be expected given that the number of IP addresses involved in volumetric DDoS attacks dropped 98% from 595,000 in Q1 to 11,000 in Q2.

Compared to Q1 2017

28% ↑ Total DDoS attacks

27% ↑ Infrastructure layer (layers 3 & 4) attacks

21% ↑ Reflection-based attacks

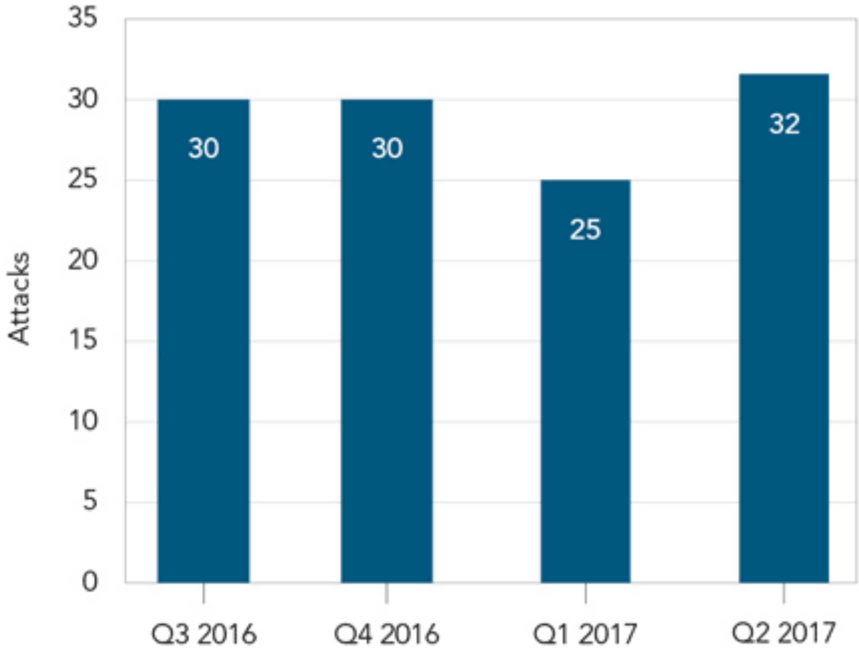
28% ↑ Average number of attacks per target

The largest DDoS attack was 75 Gbps, which while quite large was much smaller than the largest attack in 2016 of 623 Gbps. For the first time in many years, Akamai observed no large attacks exceeding 100 Gbps.

Largest attacks by quarter:

Q2 2017	Q1 2017	Q4 2016	Q3 2016
75 Gbps	120 Gbps	517 Gbps	623 Gbps

DDoS Attacks Per Target, Q3 2016 – Q2 2017



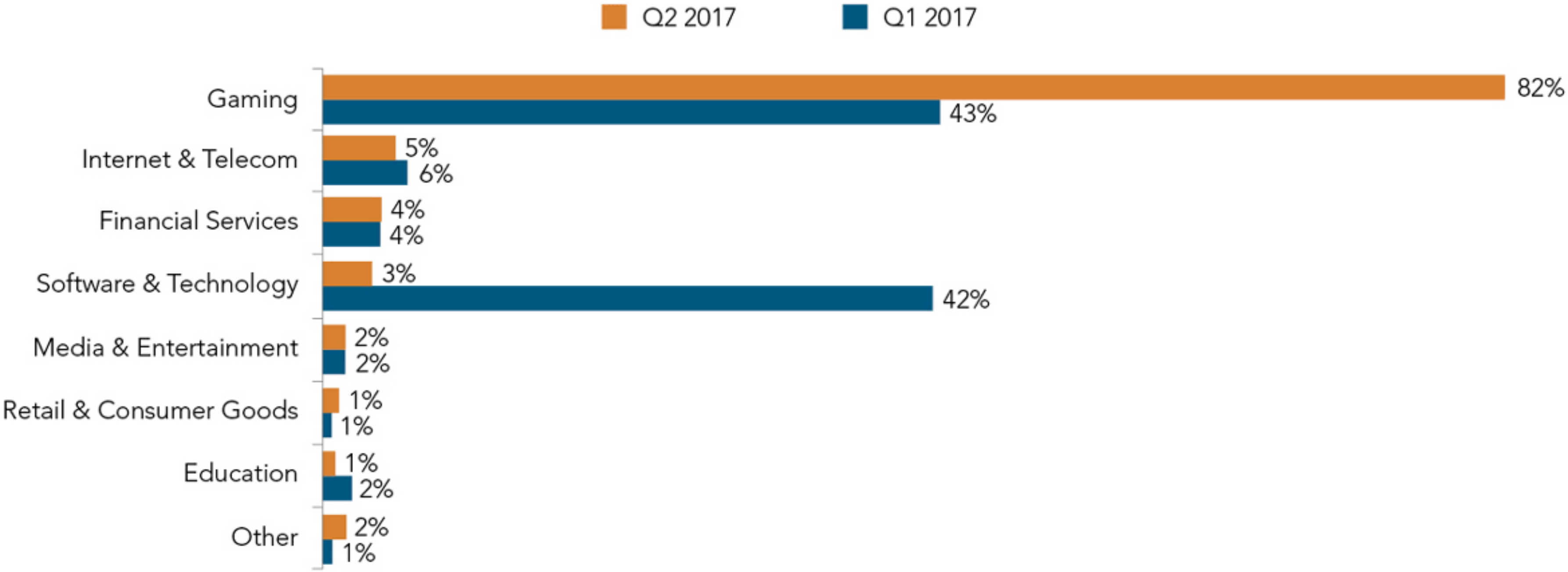
TOP TARGET ORGANIZATION

DDoS ATTACK COUNT Q2 2017: **558**

The average number of DDoS attacks per target in Q2 was 32.

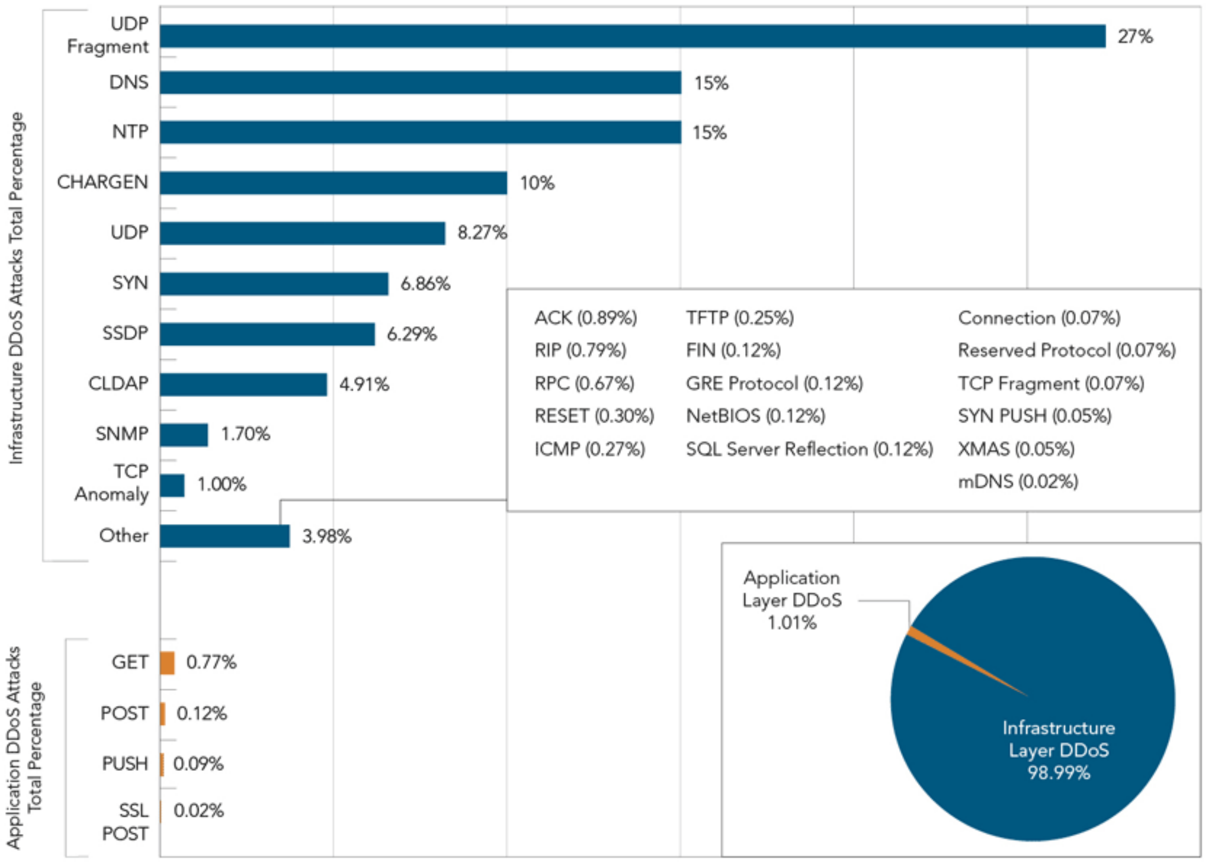
The most targeted organization faced 558 DDoS attacks.

DDoS Attack Frequency by Industry, Q1 2017 & Q2 2017



The gaming industry was targeted in 82% of DDoS attacks. A small number of gaming firms were the targets of most of these attacks.

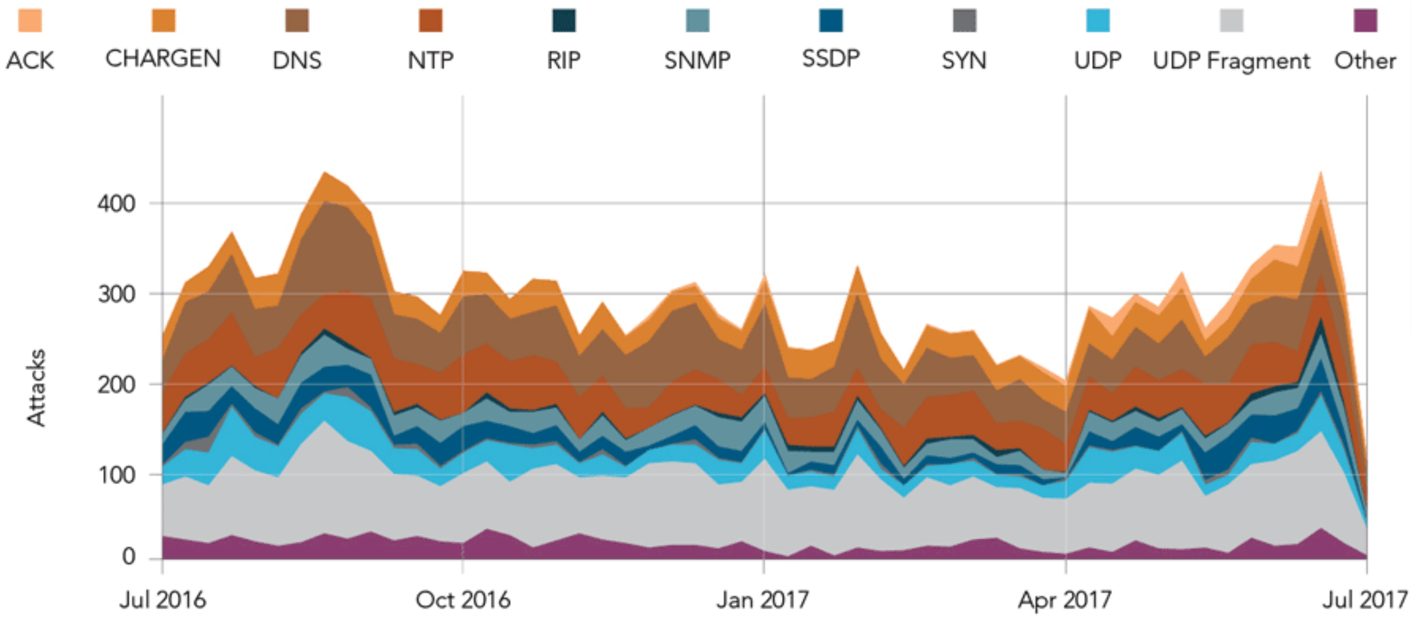
DDoS Attack Vector Frequency, Q2 2017



NTP, CHARGEN, and DNS continued in the top three places.

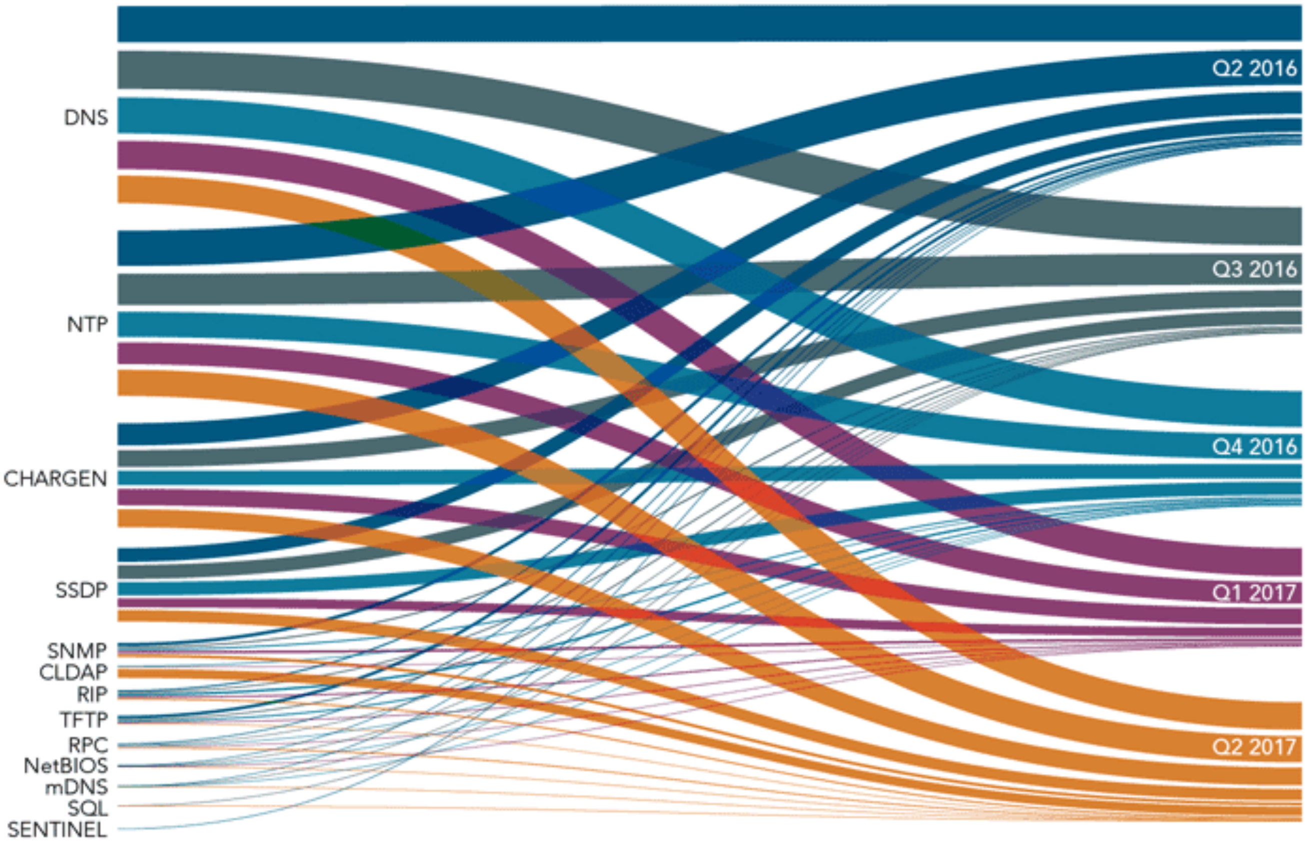
UDP Fragment traffic is technically in the top spot, but this is driven by the other UDP vectors and is extremely difficult to categorize.

Top 10 Most Frequent Attack Vectors, Q3 2016 to Q2 2017



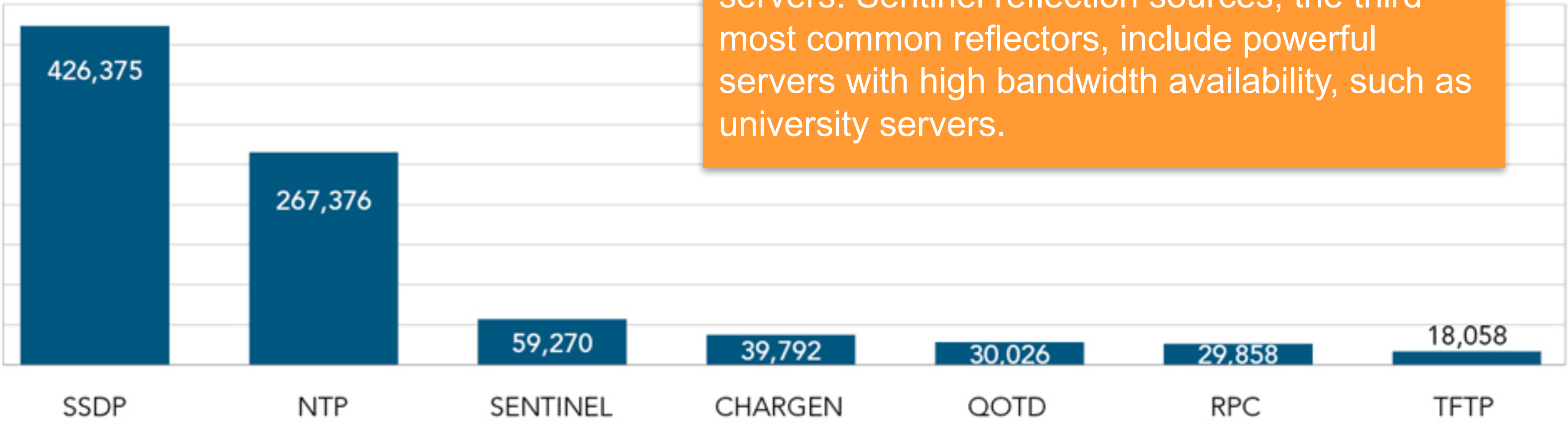
DDoS attack traffic jumped markedly in late June, after two quarters of decline.

Reflection-Based DDoS Attacks, Q2 2016 – Q2 2017



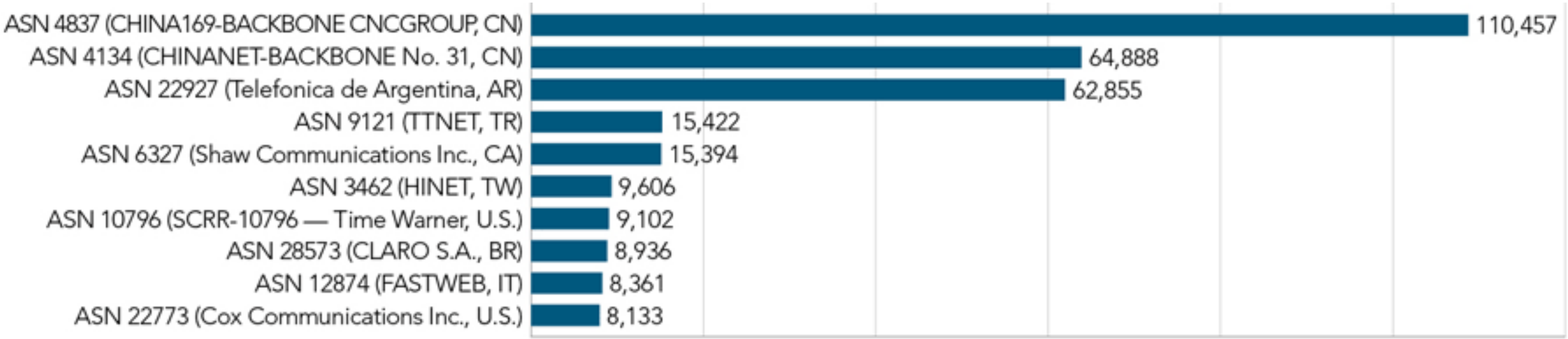
Reflection DDoS vectors use common Internet protocols to generate DDoS traffic aimed at the attacker's target. Reflection sources range from large servers to printers to small Internet of Things devices, such as surveillance cameras and home networking routers.

Top Reflection-Based DDoS Reflectors, Q2 2017



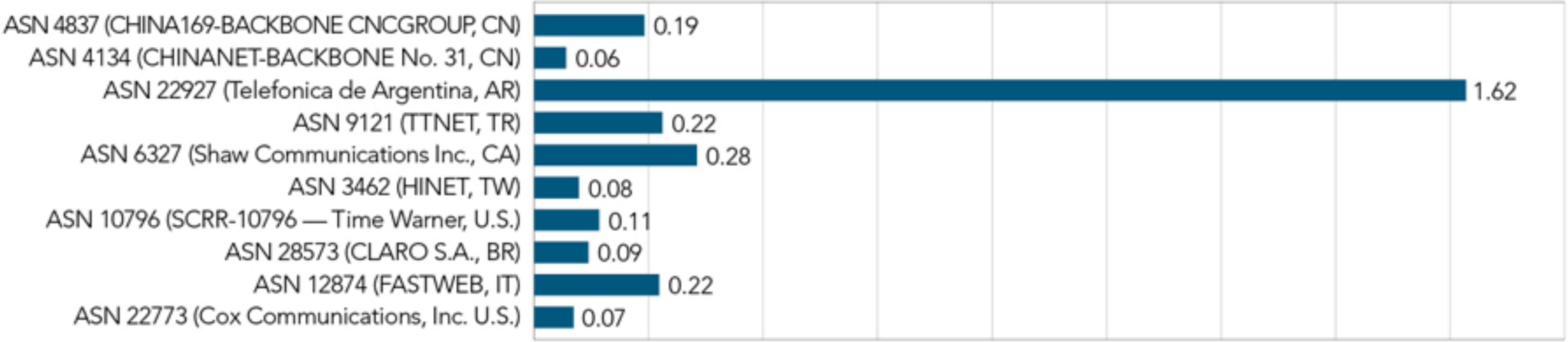
The most-used reflectors were SSDP and NTP. The use of SSDP reflection can be directly linked to Internet of Things devices. NTP reflection sources are typically unpatched servers. Sentinel reflection sources, the third most common reflectors, include powerful servers with high bandwidth availability, such as university servers.

Top Ten Reflection Source IP by ASN, Q2 2017



Two ASNs in China and an ASN in Argentina sourced the most DDoS reflection traffic, with the top 10 ASN reflection sources accounting for approximately 10% of reflection sources worldwide.

ASN Reflector Ratio by Total ASN IP Count (IPv4), Q2 2017



The ratio of reflector IP addresses to total IP addresses was highest for ASN 22927 in Argentina, with 1.62% of all its IP addresses serving as DDoS reflectors.

Akamai

FASTER FORWARD

Web Application Attack Trends

Compared to Q2 2016

25%	↑	Total web application attacks
86%	↑	Attacks from the U.S. (current top source country)
86%	↓	Attacks from Brazil (Q2 2016 top source country)
44%	↑	Increase in SQLi attacks

While DDoS attacks were down, the total number of web application attacks were up compared to the same quarter a year ago.

Much fewer attacks came from Brazil.

SQLi attacks were up 44%.

Compared to Q1 2017

5% ↑ Total web application attacks

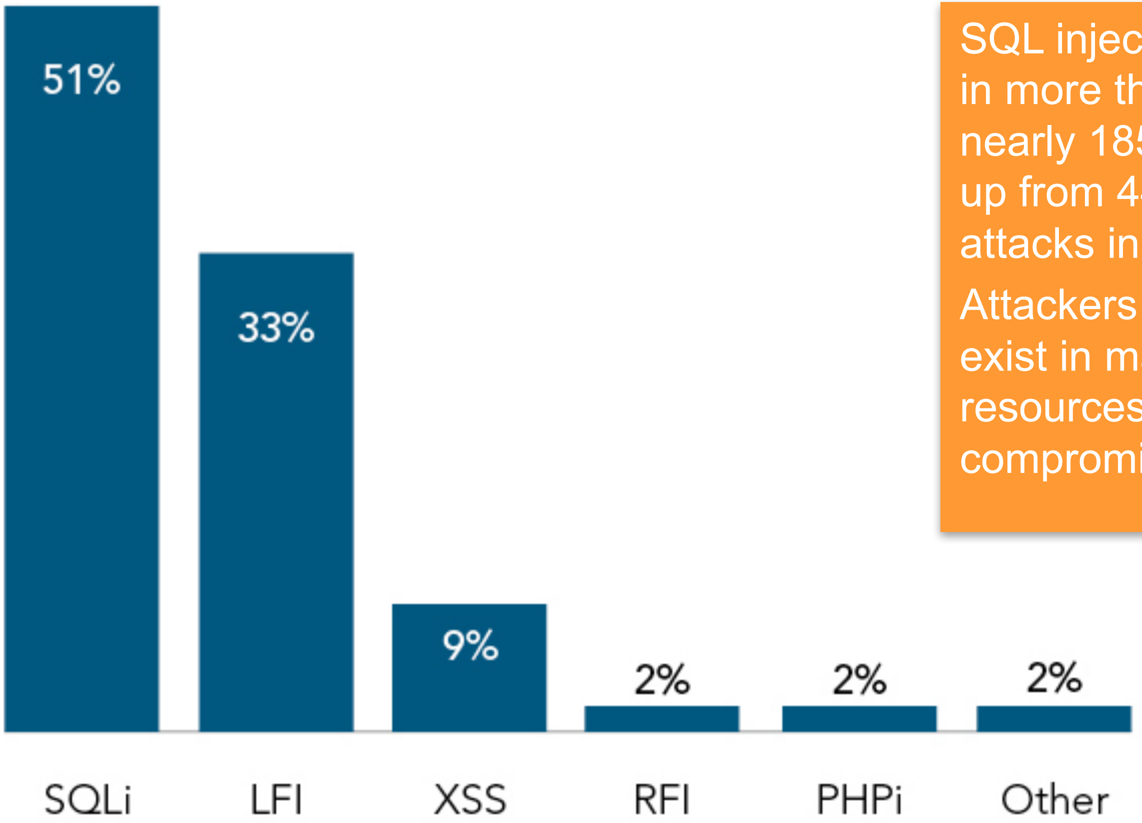
4% ↑ Attacks sourcing from the U.S. (top source country)

21% ↑ SQLi attacks

Application attacks continued to slowly grow with a 5% increase quarter-over-quarter and a 28% increase year-over-year.

Unlike DDoS attacks, web application attacks involve relatively little traffic and can be hard to detect.

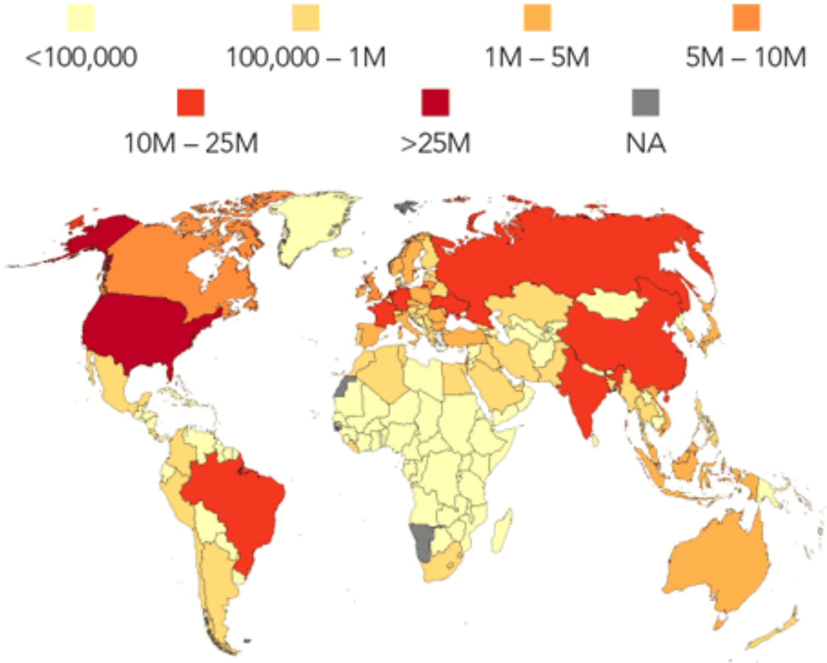
Web Application Attack Frequency, Q2 2017

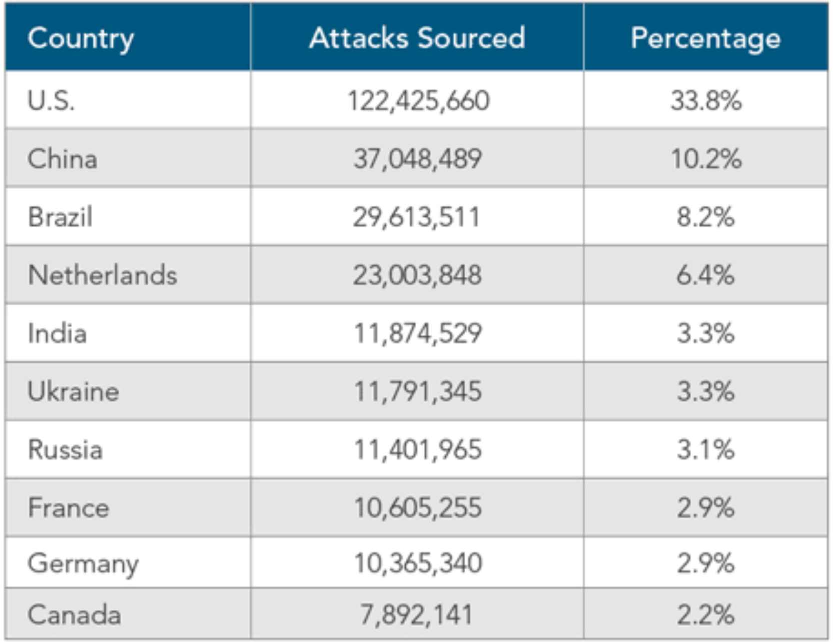


SQL injection (SQLi) attacks were used in more than half (51%) of attacks, nearly 185 million alerts in Q2. This is up from 44% of all web application attacks in Q1.

Attackers know these vulnerabilities exist in many sites and put increasing resources into finding ways to compromise them.

Top 10 Source Countries for Web Application Attacks, Q2 2017

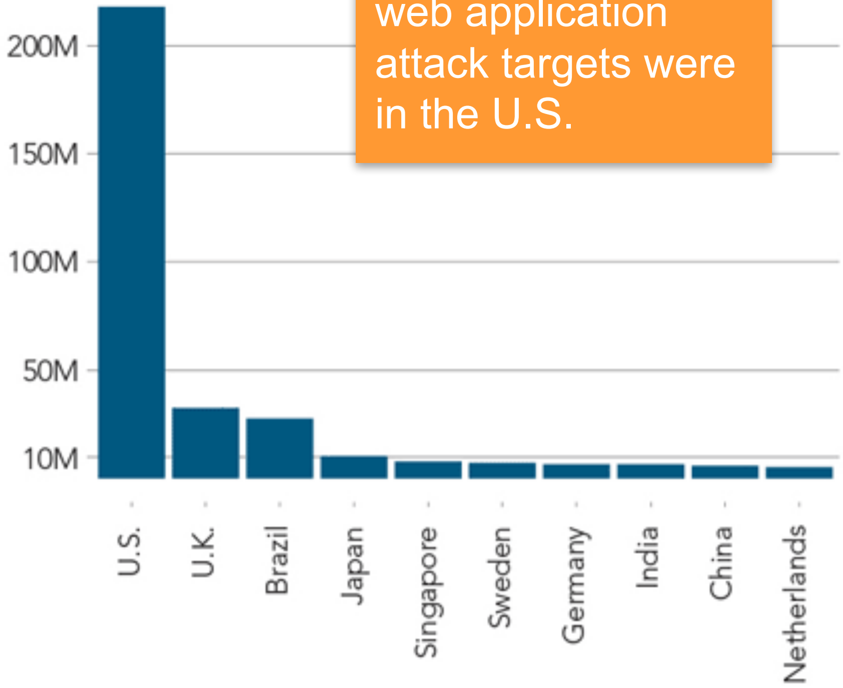




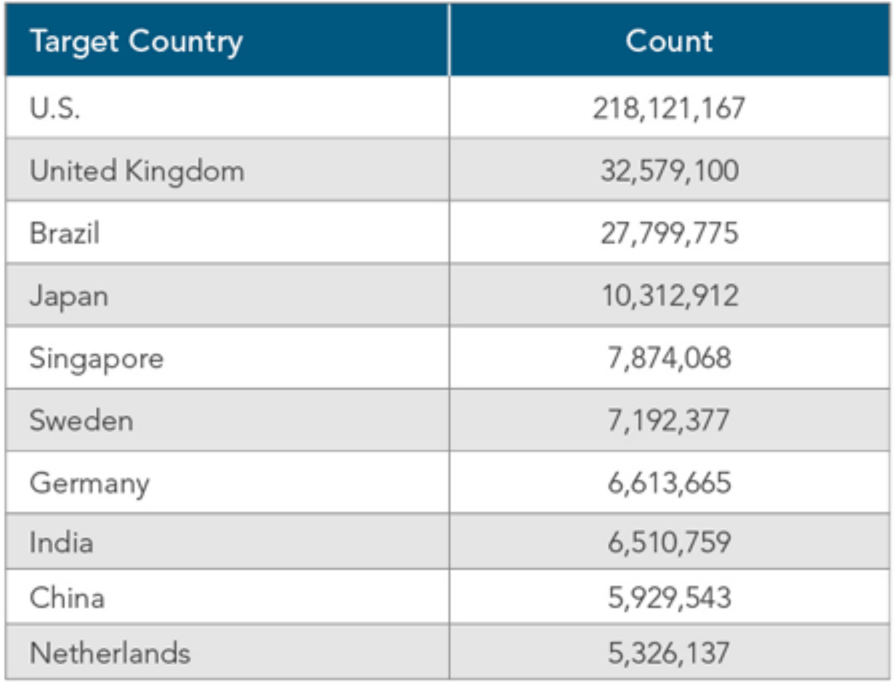
Country	Attacks Sourced	Percentage
U.S.	122,425,660	33.8%
China	37,048,489	10.2%
Brazil	29,613,511	8.2%
Netherlands	23,003,848	6.4%
India	11,874,529	3.3%
Ukraine	11,791,345	3.3%
Russia	11,401,965	3.1%
France	10,605,255	2.9%
Germany	10,365,340	2.9%
Canada	7,892,141	2.2%

The U.S. (34%) and China (10%) were the leading sources of web application attacks, followed by Brazil (8%) and the Netherlands (6%).

Top 10 Target Countries for Web Application Attacks, Q2 2017



The vast majority of web application attack targets were in the U.S.



Target Country	Count
U.S.	218,121,167
United Kingdom	32,579,100
Brazil	27,799,775
Japan	10,312,912
Singapore	7,874,068
Sweden	7,192,377
Germany	6,613,665
India	6,510,759
China	5,929,543
Netherlands	5,326,137

Akamai

FASTER FORWARD

Spotlights

PBot DDoS Botnets: More Power, Fewer Bots

These UDP and DNS DDoS attacks occurred in May and June 2017.

Attackers recycled PBot, decades-old PHP code.

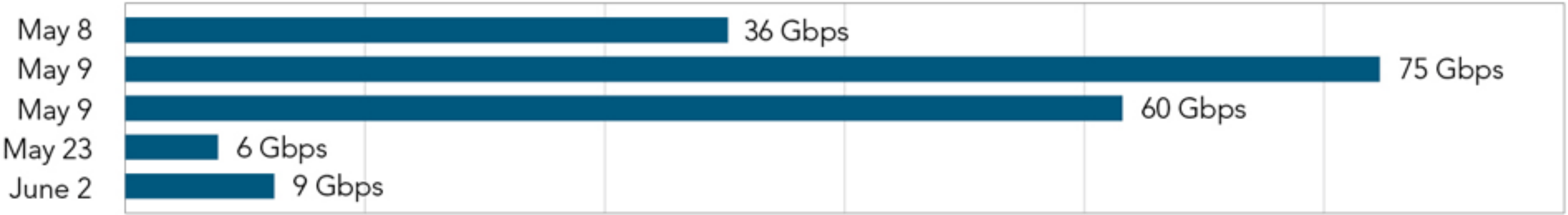
Infected devices appeared to be web servers.

Method of infection might be Apache Struts vulnerabilities.

Number of bots per botnet is fewer than 400, much smaller than IoT botnets.

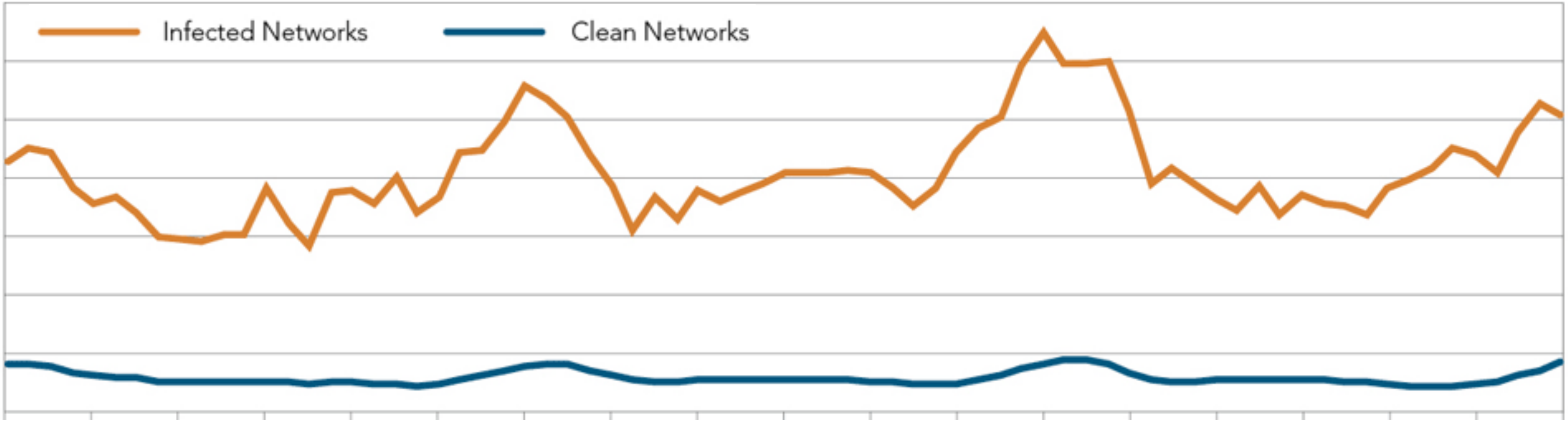
Largest attack to date was 75 Gbps, the largest DDoS attack in Q2.

Targeted customer was in the financial industry

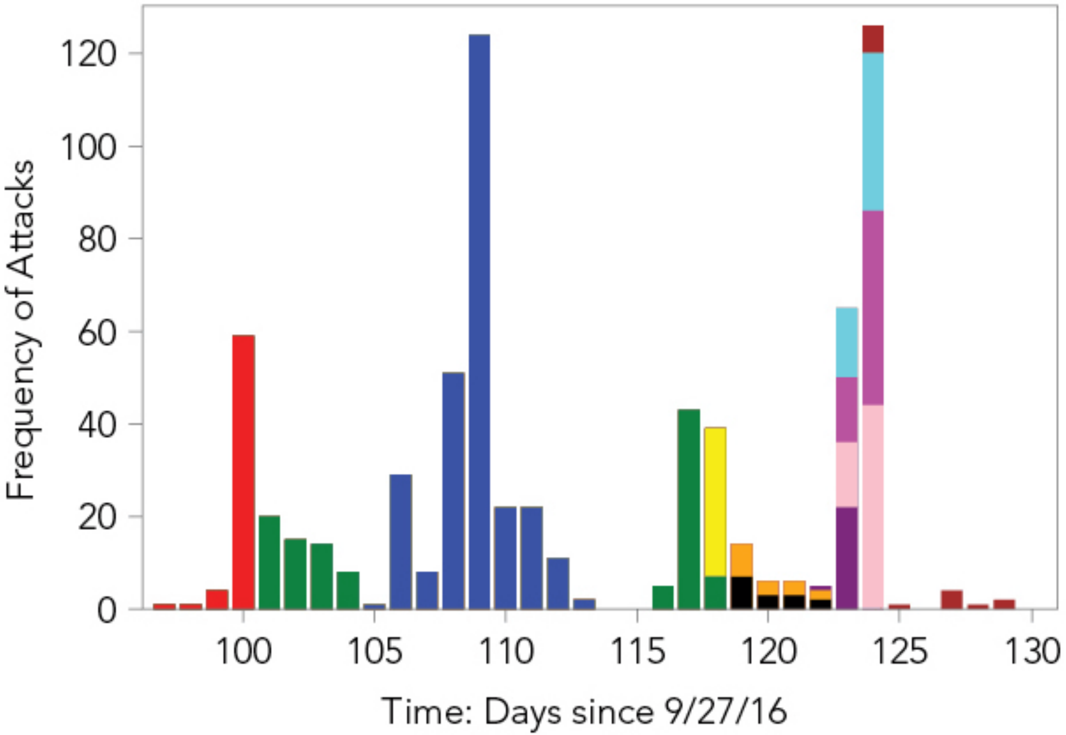


Identifying Behavior of Networks Infected by DGA Malware

Domain generation algorithms (DGAs) are used by malware to establish command and control that is difficult to take down. This graph reveals a difference in the DNS NX response rate on infected and clean networks. Knowing this and using machine learning can lead toward the detection of malware activity.



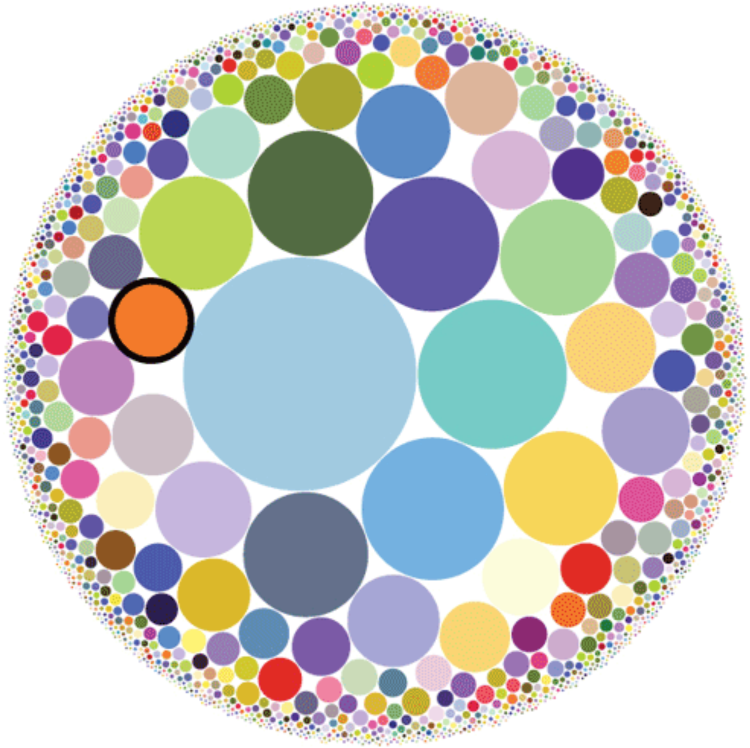
Mirai Botnet Command and Control Structure and Behavior



We found that Mirai command and control nodes are usually active for only a short time.

This plot shows the activity of 12 Mirai C&C nodes. Each color is a unique IP address. The blue node, for example was active for a week, and then went quiet or disappeared.

Mirai Botnet Targeting Behavior



This cloud of dots shows all the networks targeted by Mirai command and control nodes in our 288-day dataset. Some targets received very few DDoS attacks while others were targeted by thousands of DDoS attacks.

The larger dots received more attacks. The largest dot represents more than 10,000 attack commands.

Akamai is on the left, in orange outlined in black. Akamai was targeted more than 1,200 times.

Akamai

FASTER FORWARD

Cloud Security Resources

Q2 2017 Cloud Security Resources

The Akamai Blog is a timely source of threat intelligence. Some of the topics covered in Q2 include:

- Passive HTTP2 Client Fingerprinting, a white paper
- DDoS Attacks against DNS Infrastructure in the News
- Low Risk Threat: DDoS Extortion Letters
- Spotlight on Malware DGA Communication Technique
- WannaCry: What We Know
- Dealing with Petya

Full Report:

- http://akamai.me/2faEf2k