Q4 STATE OF THE INTERNET SECURITY SPOTLIGHT

Internet of Things and the Rise of 300 Gbps DDoS Attacks

Akamai
FASTER FORWARD

1.0 / Overview / The Internet of Things (IoT) provides massive resources for Distributed Denial of Service (DDoS) and web application attacks. Attackers harness IoT devices for malware-based DDoS botnets, reflection DDoS attacks, and as proxies for malicious activity. Working together, IoT devices overwhelm their targets, making DDoS attacks of 300 Gbps more common.

623 Gbps, 555 Gbps, 517 Gbps — some of the largest DDoS attacks ever Akamai has ever mitigated occurred in the second half of 2016. Mega DDoS attacks, i.e. attacks greater than 100 Gbps, were up by 140% in Q4 2016 when compared to Q4 2015. Q4 2016 saw 12 of these mega attacks, five of which exceeded 200 Gbps, with three reaching 300 Gbps.

2.0 / DDoS Fueled by the Internet of Things / The primary purpose of IoT malware is DDoS attacks. All of the 300 Gbps attacks in 2016 were fueled in full or in part by the Internet of Things. More than half of the mega attacks in Q4 came from Mirai botnets.

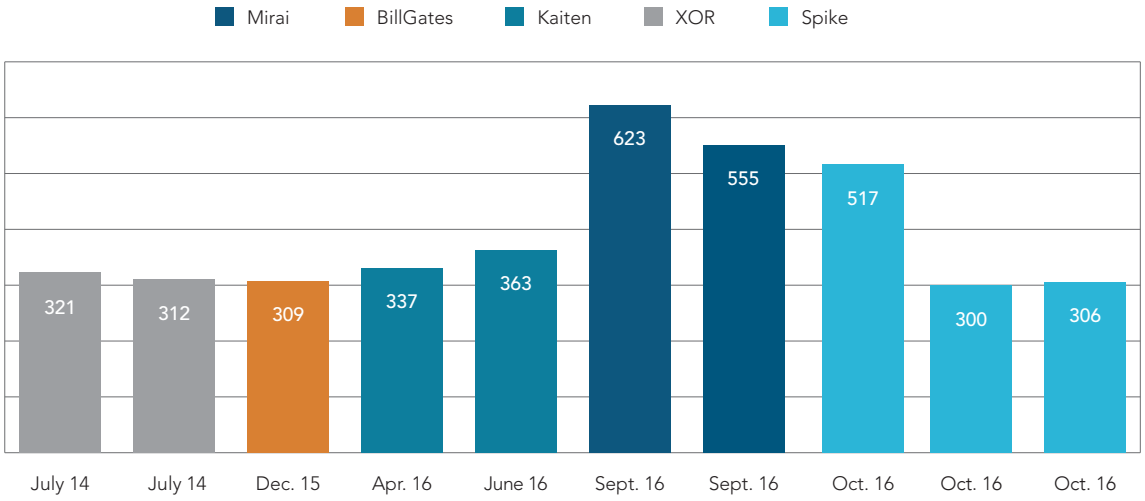
And yet, although Mirai caused a huge amount of DDoS traffic in Q4, claiming headlines in September and October, the largest DDoS attacks of Q4 were not from Mirai. The largest DDoS attacks, including an attack at 517 Gbps, arose from another botnet malware that employs IoT bots — the Spike DDoS toolkit.

The rapid proliferation of insecure IoT devices has provided an expanding pool of DDoS attack resources. It's a continual process whereby existing vulnerable devices are identified, new devices are deployed, and new vulnerabilities are discovered. Many types of malware then take advantage of these vulnerabilities.

3.0 / 300 Gbps DDoS Attacks from Malware Botnets / DDoS attacks consistently greater than 300 Gbps are relatively new, but that doesn't mean we haven't seen them before. Five types of botnet malware were responsible for the ten 300+ Gbps DDoS attacks ever mitigated by Akamai. All of them can use IoT devices.

The first two 300 Gbps DDoS attacks occurred in mid-2014 and were generated by XOR. BillGates generated the next 300 Gbps DDoS attack more than a full year later in December 2015. Those attacks were followed in 2016 by seven 300 Gbps attacks: two in the first half of the year from Kaiten, two attacks in September from Mirai, and three attacks in Q4 from Spike.

Each type of malware spawns any number of separately controlled botnets that may launch DDoS attacks at the same target all at once — for the largest attacks — or independently.



Four botnets generated 10 DDoS attacks exceeding 300 Gbps between July 2014 and December 2016. Seven of these occurred in 2016

4.0/ IoT Used for Reflection DDoS / Infection-based botnets are not the only way in which attackers use IoT devices to generate DDoS attacks. Reflection and amplification DDoS techniques abuse common Internet protocols, such as Simple Services Discovery Protocol (SSDP), used for device connectivity.

The number of SSDP reflectors sending DDoS floods exploded in Q4, expanding by 321%. In 2014, we first observed the SSDP reflection DDoS vector. At that time, there were 4 million potentially vulnerable Internet-facing devices. In Q4 alone, 508,000 unique SSDP reflectors were involved in DDoS attacks. Home routers are a common source of DDoS traffic employing SSDP reflection.

5.0 / As Proxies for Web Application Attacks / IoT devices are also used by malicious actors to hide the source of web application attacks. In October 2016, IoT devices were being used in account checking attacks. Malicious users access the web administration panel of a device with a factory default password, or via an SSH connection that does not require a password. Once breached, the device is available for attacks both on external websites and on the private network hosting the device. Video surveillance equipment and networking devices are among the vulnerable.

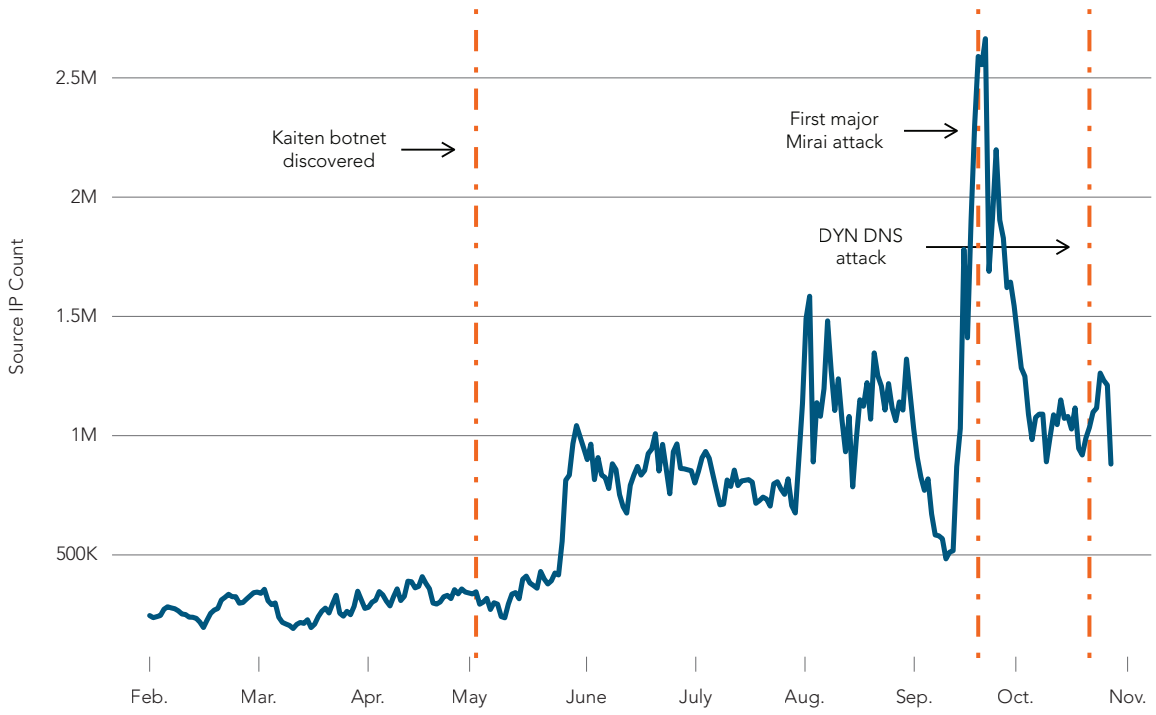
6. 0 / Spike Returns with Massive DDoS Attacks / IoT devices are also being co-opted by old malware. In 2014, Akamai issued a threat advisory about the Spike DDoS botnet. A key feature of Spike was its adaptability to infect a wide range of systems, from Linux servers to ARM-based embedded devices. At the time, the peak DDoS attack size from the Spike botnet measured 215 Gbps and 150 million packets per second (Mpps).

Two years later, Spike malware generated the largest DDoS attack (517 Gbps) of Q4, an attack more than twice the size of the Spike attack in 2014. Q4's near-record DDoS attack from Spike demonstrated that an attacker can modify an old, customizable DDoS toolkit, build a botnet, and generate one of the largest DDoS attacks to date.

XOR and BillGates botnets are built from the same family of malware as Spike. They too have generated DDoS attacks measuring greater than 300 Gbps. An attacker gains full control of any system infected with this family of malware.

7. 0 / Kaiten and Mirai Remain Serious Threats / Part of a newer family of malware for DDoS botnets and built to target IoT devices specifically, Kaiten and Mirai target DVRs, IP cameras, networking devices, and other devices. The devices targeted use processors as diverse as `MIPS`, `ARM`, `PowerPC`, `x86` and `x86_64`. The infection begins with either an exploitation of a vulnerability or brute forcing of default login credentials. The tools provide a powerful array of options and customizable parameters. Backdoor functionality allows the attacker to execute arbitrary commands on an infected system.

In Q3, Akamai mitigated a Mirai DDoS attack that was measured at a whopping 623 Gbps. While initial DDoS attacks in September from Mirai botnets were the largest ever observed on Akamai's Prolexic routed network, later attacks lessened in intensity. In Q4, the bandwidth peak of DDoS attacks from Mirai botnets, although still substantial, dipped below 100 Gbps and 30 Mpps.



A rapid increase in scans of port 23 and 2323 began on May 13, 2016 as the Mirai botnet attempted to log into unsecure IoT devices.

8.0 / Searching for Mirai's Birthdate / IThe birthdate of a botnet is often unknown. However, Mirai burst onto the DDoS landscape in 2016 in a big way. It is the youngest of the five types of malware to form botnets that launched DDoS attacks of 300 Gbps and more. Kaiten and Mirai scan Ports 23 and 2323 to spread infection. Akamai analyzed the background noise of the Internet, looking for scans of these two ports.

Early Kaiten activity wasn't noticeable, but abrupt increases in scanning of Ports 23 and 2323 were visible as early as May 13, and again at the end of July. We believe these increases correspond to the first run of Mirai testing and the full release of Mirai into the wild.

9.0 / When Smart Devices Do Dumb Things / The Internet of Things is creating a massive DDoS problem. Few organizations are equipped to mitigate DDoS attacks of more than 100 Gbps, facing 300 Gbps and more from hundreds of thousands of IoT devices makes the situation worse.

Review your DDoS protection. To learn more about Akamai's DDoS protection solutions, and reducing the overall risk of DDoS attacks to your organization, please visit www.akamai.com/cloud-security

Akamai FASTER FORWARD