The Internet of Things (IoT) comprises billions of devices that can send and receive data and are present in homes, offices, and the community. IoT devices infected by Mirai malware include residential security and entertainment equipment, such as Internet cameras, digital video recorders (DVRs), and routers.

Mirai source code and how-to instructions for building a botnet were leaked publically by a malicious actor. Within two weeks of the release of the code, Akamai observed the first round of updated capabilities. Because millions of deployed IoT devices have lax security and vulnerable firmware, they are a ready source of DDoS fuel. The Mirai botnet will continue to grow, both in numbers and strength.

The largest DDoS attacks have increased greatly in strength, doubling in attack size during 2016. They are bigger, more complex, and require more expertise to defend against than past Distributed Denial-of-Service (DDoS) attacks. They are not limited to a specific industry.

On October 21, 2016, Internet of Things-fueled DDoS attacks on Dyn Managed DNS infrastructure prevented user access to major web properties in the U.S., including Twitter, Spotify, PayPal, and others. Dyn is not an Akamai customer, and we were not involved in the mitigation of its attack. A month earlier, however, Akamai mitigated a whopping 623 Gbps DDoS attack involving the same infection-based botnet malware, which is called Mirai. The 623 Gbps attack was just one of 10 Mirai-based attacks against a single target during an eight-day period; five of them peaked at more than 100 Gbps.

The attack against Dyn demonstrates that in addition to direct attacks, organizations also need to manage the risk of DDoS attacks against the Internet’s central infrastructure, such as DNS servers. Such targeting can have a ripple effect on any organization that directly or indirectly bases its Internet presence on a vulnerable vendor.

Mirai Botnet and the Internet of Things

Mirai malware has harnessed hundreds of thousands of smart-connected devices. It installs malware, achieves control, and builds a global army by gaining access to devices with weak default passwords. Each infected device then scans the Internet to identify and infect more vulnerable devices while waiting to be commandeered for a DDoS attack.

The Internet of Things (IoT) comprises billions of devices that can send and receive data and are present in homes, offices, and the community. IoT devices infected by Mirai malware include residential security and entertainment equipment, such as Internet cameras, digital video recorders (DVRs), and routers.

DDoS Attacks on a DNS Service Provider

In a report from Forrester after the Dyn attacks, the researchers wrote, "Many of the businesses affected by the attack were unable to recover because they had introduced a single point of failure in their services by relying on a single primary authoritative DNS provider, lacking a secondary authoritative DNS provider."1

The attacks on Dyn neither targeted Akamai nor impacted any Akamai services. Akamai maintains a history of IP addresses and if DNS is down we use the last one of record. This allowed us to resolve nearly 60,000 DNS requests per second that would have otherwise failed, keeping Akamai customers who were using Dyn Managed DNS online.

Why Akamai: Architected for DDoS Resilience

Akamai’s services are architected for DDoS resilience. We protect Akamai customers against DDoS attacks with the Akamai Intelligent Platform™, the Prolexic Network, and the distributed Fast DNS infrastructure. We make investments to constantly improve the DDoS resilience of these platforms in the face of adversary action.
At the highest level, our capacity planning model takes the largest DDoS attacks we’ve been able to verify and multiplies that traffic by a scaling factor to provide ample headroom as attacks grow in size. As a result, we’ve mitigated successfully the largest and most sophisticated DDoS attacks in history, including the Qassam Cyber Fighters (QCF) attacks on U.S. financial institutions and, in September, a record-breaking 623 Gbps attack on a pro-bono Akamai customer.

Our Adversarial Resilience team continually evaluates new threats and incidents to discover potential breaking points in Akamai systems and works with engineering teams to improve resiliency.

**DDoS Resilience in the Akamai Intelligent Platform**

Akamai maintains sufficient global capacity to absorb the largest DDoS attacks. Beyond capacity, we architect our Content Delivery Network (CDN) for availability and resiliency through adverse conditions — not just DDoS attacks.

The Akamai CDN connects end users to an optimal Akamai edge server, as adjusted for the status of individual servers, and automatically routes user traffic around local network outages.

With over 220,000 servers currently deployed around the world today, Akamai can maintain connectivity through the most adverse conditions — from network congestion to ISP outages to DDoS attacks.

In addition, Akamai deploys a wide range of controls to defend against DDoS attacks within each server, such as rate controls, blacklists, and geo-blocking.

**DDoS Resilience in the Prolexic Network**

The Prolexic Network is among the most powerful DDoS scrubbing networks in the world. It consists of seven global scrubbing centers, over 3 Tbps of capacity, and a team of 150 security professionals who protect more than 500 customers from more than 200 DDoS attacks every week.

We continue to add DDoS protection capacity. Each scrubbing center has multiple Tier 1 carrier connections. We have public peering with more than 500 peers, and high-performance traffic analysis and active mitigation at multiple layers of the OSI stack.

**DDoS Resilience in the Fast DNS Infrastructure**

Akamai operates an authoritative DNS service similar to Dyn Managed DNS. Akamai architected Fast DNS for availability and resilience against DDoS attacks in addition to performance. We have segregated our Fast DNS infrastructure into 20 separate DNS clouds, each specifically architected for availability. We then distribute the name servers assigned to our customers across the DNS clouds to minimize the impact that DDoS attacks against any one Akamai customer can have on others.

Within each DNS cloud, Akamai deploys clusters of name servers in such a way as to minimize the impact that localized DDoS attacks can have against the entire network, such as by deploying name servers directly into end-user ISPs to maintain service for ISP users.

In addition, Akamai maintains additional controls to defend against DDoS attacks, such as rate limiting and whitelisting DNS requests.

**Conclusion**

Akamai has defended against DDoS attacks for nearly two decades and has protected customers and maintained infrastructure availability, even while withstanding the largest DDoS attacks of the time. Akamai continues to investigate and report on new threats, such as the threat advisory issued in August 2016 for what is now known as the Mirai botnet. We continue to evolve our procedures and platform to stay ahead of those with malicious intent.

As DDoS attacks grow larger, we continue to monitor our network to anticipate requirements and build out the capacity to mitigate such attacks.

As DDoS attacks become more complex, we continue to apply what we learn defending all of our customers to make our protections more resilient. We are committed to providing Akamai customers with the most robust platform in the industry.

**Review your own end-to-end DDoS Resiliency**

If you would like Akamai’s help in reviewing your own end-to-end infrastructure resiliency and provide guidance on whether or not your setup leverages all of our best practices, reach out to our Professional Services organization for a consultation by our Enterprise Security Architects.

---

1. Pollard, Jeff, Joseph Blankenship, and András Cser. Quick Take: Poor Planning, Not an IoT Botnet, Disrupted the Internet: Dyn Outage Underscores the Need to Plan for Failure. 24 October 2016. Forrester Research