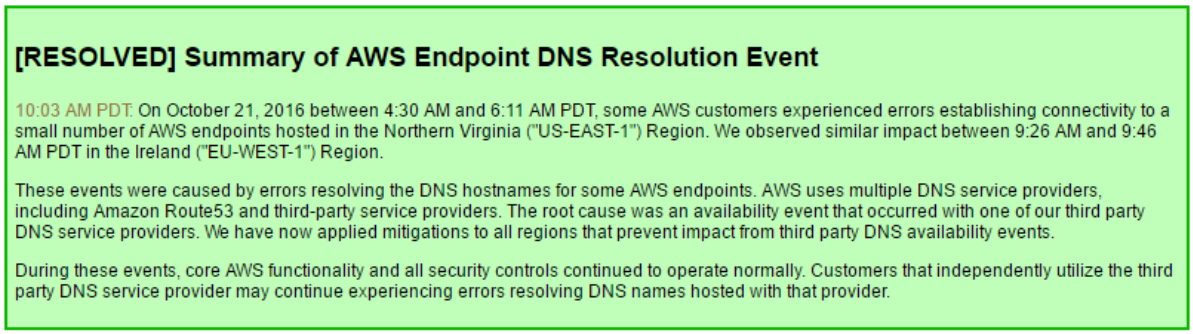
Abstract

On October 21, 2016, DYN - a leading US-based DNS provider – was knocked offline by a major DDoS attack. Consequently, the services of many US based enterprises, including Amazon, Netflix, Twitter, and CNN, were completely unreachable (see Figure 1). There is no official confirmation yet to who the attackers were or their motivations.



[RESOLVED] Summary of AWS Endpoint DNS Resolution Event

10:03 AM PDT: On October 21, 2016 between 4:30 AM and 6:11 AM PDT, some AWS customers experienced errors establishing connectivity to a small number of AWS endpoints hosted in the Northern Virginia ("US-EAST-1") Region. We observed similar impact between 9:26 AM and 9:46 AM PDT in the Ireland ("EU-WEST-1") Region.

These events were caused by errors resolving the DNS hostnames for some AWS endpoints. AWS uses multiple DNS service providers, including Amazon Route53 and third-party service providers. The root cause was an availability event that occurred with one of our third party DNS service providers. We have now applied mitigations to all regions that prevent impact from third party DNS availability events.

During these events, core AWS functionality and all security controls continued to operate normally. Customers that independently utilize the third party DNS service provider may continue experiencing errors resolving DNS names hosted with that provider.

Figure 1: Amazon status update from Dyn outage

The attackers leveraged several botnets against Dyn's servers. This included Mirai, a botnet comprised of over 140,000 Internet of Things (IoT) devices, that was recently used against Brian Krebs and OVH in a record breaking 1.1Tbps DDoS attack. It is likely that Mirai was modified and a variant of it was used against Dyn.

This attack highlights the lack of protection provided by traditional DDoS protection solutions that rely on rate-limit technology and underscores the need for behavioral-based DDoS protection to mitigate these types of cyber-attacks, such as those provided by Radware. Rate-based DDoS mitigation solutions will result in high percentages of false positives, resulting in legitimate users being blocked and frustrated customers.

Background

Mirai was released in September 2016 and allows its users to infect IoT devices (by leveraging manufacturer's default passwords). A command and control server connects to these devices via Telnet and transforms them into a botnet (specifically exploiting port 23, 2323 and 103). It is most likely that since then a number of attackers have modified and deployed the botnet for themselves.

One of the attack vectors in the Mirai bot is commonly known as DNS Waterfall Torture. In Waterfall Torture, the victim is attacked via the assistance of a middle-man (a mediator server). The bot sends a query to a recursive DNS server to resolve a random host in a domain that the end-target is authoritative. The recursive DNS server takes that hostname, does not find it in its cache since it is random, and forwards it the target. The target receives millions of queries to resolve from the real DNS server (the recursive ones) and cannot track the request back to a bot. Once the attacker ties up all of the DNS's resources, legitimate clients are unable to resolve their request. As mentioned, this is a very sophisticated tactic that bypasses rate-limiting DDoS mitigation solutions.

Reasons for Concern

Although it is very difficult to find unique traffic patterns when it comes from a real DNS server (as it appears legitimate), a smart traffic monitoring mechanism, if deployed at the recursive servers, could have intercepted the attacks as they would be able to identify the illegitimate bot traffic. Behavioral-based detection could have minimized the impact of the attack, if not blocked it altogether.

In addition, using a secondary DNS provider for high availability could have minimized the impact of the attack (see Figure 2). A large number of Internet clients leverage only one DNS provider for both their primary and secondary DNS. Companies that did not use a redundant DNS server suffered a complete outage and their users were unable to reach their website.

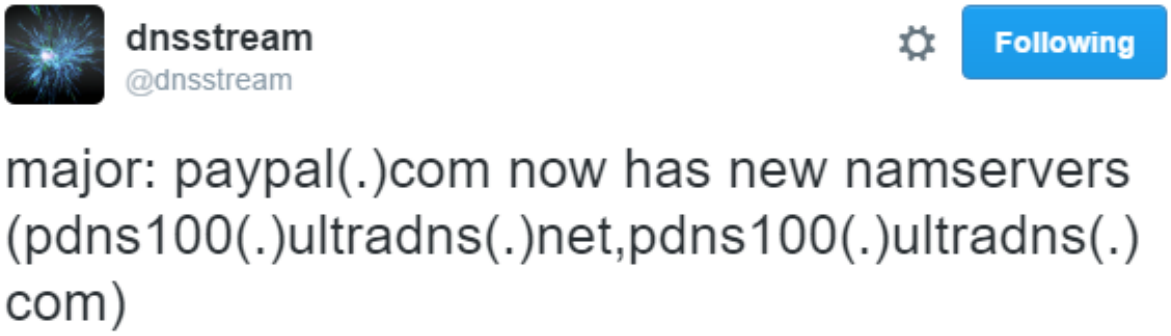


Figure 2: PayPal switches DNS during the Dyn Attack

How to Prepare:

- The IoT brings cyber-attacks into the realm of 1Tbps size attacks and requires security and service providers to adjust their approach and be able to protect from these sophisticated, automated attacks.
- Organizations should reevaluate today's DDoS protection security paradigms, and more specifically, solutions that rely on traditional, rate-based detection methods.

Organizations Under Attack Should Consider:

- **Hybrid DDoS Protection (on-premise + cloud)** – for real-time protection that also addresses high volume attacks and protects from pipe saturation.
- **Behavioral-Based Detection** – to quickly and accurately identify and block anomalies while allowing legitimate traffic through.
- **Real-Time Signature Creation** – to promptly protect from unknown threats and zero-day attacks.
- **A cyber-security emergency response plan** that includes a dedicated emergency team of experts

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.