BLACK

CLIENT ADVISORY

DYN / DDoS ATTACK

BLACK

DDoS ATTACK

EXECUTIVE SUMMARY

On Friday, October 21, 2016, Dyn, a cloudbased Internet Performance Management company was the target of a disruptive Distributed Denial of Service (DDoS) attack.The attack directed networked devices to route traffic at the Dyn's Domain Name Servers (DNS). As a result, Dyn could not respond to DNS requests and consumers could not reach websites.

- The three waves of the attack caused outages and slow internet for significant portions of the United States and other nations. The attack occurred through the weak configurations of Internet of Things (IoT) devices, such as default passwords.

- Security researchers have indicated the malicious actor(s) infected systems with the "Mirai" malware to create a botnet. The malware searches for networked devices with default passwords to exploit in order to build a larger botnet.

- Dyn provides critical infrastructure services to a major internet sites so when their services were attacked it impacted the ability to access other websites such as Twitter, Netflix, or Amazon.

- This advisory goes behind the headlines to explain the events and provides practical advice to protect yourself.

BLACK

ATTACK PATH

Reports reveal the Dyn DDoS attack was one of the largest against a DNS provider in terms of global scale, overall length of time, and the number of compromised devices reaching approximately 100,000[1]. According to researchers, this attack is "roughly twice as powerful as any similar attack on record".[2]

Dyn released a statement on Saturday, October 22, 2016 detailing the coordinated attack[3]. The attack can be broken down into three (3) waves, each with varying tactics and impact.

1st Wave

7am EST - The attack began and was directed against three data centers – Chicago, Washington D.C., and New York. Dyn struggled to restore service but managed to after two hours. According to Dyn, "internet users directed to Dyn servers on the East Coast of the US were unable to reach some of [Dyn's] sites."

2nd Wave

12pm EST - Dyn recovered from this attack in one hour. According to Dyn, "some customers would have seen extended latency delays during that time."

3rd Wave

A little after 4pm EST - Dyn was "able to successfully mitigate it without customer impact."

In all 3 waves, traffic to Dyn's U.S.- based DNS (the address book for the internet) servers were flooded with requests from tens of millions of IP addresses intending to disrupt the system. The attackers exploited upwards of 100,000 Internet of Things (IoT) devices and infected them with the malware "Mirai". Once the devices were infected they were part of a controlled botnet for this attack.[4] Of the devices used as part of the botnet, a significant portion were from the "Chinese hi-tech company called XiongMai Technologies. The components that XiongMai makes are sold downstream to vendors who then use them in their own products".[5]

1 https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
2 https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
3 https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
4 https://www.flashpoint-intel.com/mirai-botnet-linked-dyn-dns-ddos-attacks/
5 https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

IMPACT

The damage of malware Mirai was first evident in the September 2016 attack on the information security blog, Krebs on Security, which houses cybercrime research and data breach alerts authored by former Washington Post journalist Brian Krebs. Forensics for the September 2016 attack said the maximum traffic peaked around 600 Gbps. That same month the European Web hoster OVH was hit with a record DDoS attack that leveraged IoT-based botnets at 1 Tbps.[6] In comparison, the Dyn attack strength of 1.2 Tbps was the largest and strongest DDoS in history. Moreover, the Mirai malware was released to the public following the September attack and concerns have been raised that additional DDoS attacks are likely by additional cybercriminals planning to reuse the malware.

For nearly twelve hours, major internet sites faced either sluggish connection or lack of availability. The Ponemon Institute calculated the average cost per minute of downtime at $22,000.[7] And, while the total economic impact of this attack is still unknown, the consequences have already been felt. Security personnel are concerned the use of DDoS attacks could cause wide scale interruptions to our critical infrastructure, including public health and safety services.

Financial institutions, in particular, are susceptible to DDoS attacks. The 2015 Verizon Data Breach Investigations Report (DBIR) indicates that DDoS attacks are the most common form of attack against the financial services industry and actually account for 32% of all attacks reviewed by Verizon.

SECURITY CONTROLS

As noted, the Dyn attack is the largest and strongest DDoS attack known to date. And, unlike many attacks, security researchers and government officials are not able to determine the motive or actor(s) behind this attack. The FBI[8] has confirmed as recently as October 26, 2016, that it does not have any confirmation of a group or individuals responsible for the DDoS.

The amount of networked devices, especially IoT devices, will only increase in years to come. There are currently 15 billion internet connected devices in use today and it is predicted that there will be 200 billion by 2020[9]. Akamai accounted DDoS attacks were up 129 percent in the second quarter of 2016 compared to last year.[10] And, due to the public nature of the Mirai malware, there is a possibility we can see more damaging DDoS attacks.

6 https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/
7 https://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf
8 For FBI Infragard members, please refer to the Infragard Security Alert, Pin Number 161026-001
9 http://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html
10 https://www.akamai.com/us/en/multimedia/documents/social/q2-2016-state-of-the-internet-security-infographic.pdf

BLACK

PHASE 1

PHASE 2

To protect your business, here is a phased action plan that lists our go-to steps and vital security controls:

1. Change the default passwords of your company's networked devices.
2. Protect all your devices with a firewall and only expose what is absolutely necessary to external connections
3. Disconnect devices if there is a concern they were part of the DDoS attack.
4. Call your Internet Service Provider (ISP) and ask if they can detect DDoS attacks; in the event of an attack, ask if they are able to proactively re-route your traffic versus waiting for your approval. Ask your ISP to explain their full suite of DDoS protective services.
5. Disable Universal Plug and Play (UPnP) on your firewall and gateway router. Test this implementation first as it improves security but could cause application problems.
6. Disable remote management of routers over the Internet or restrict management to a specific set of trusted IP addresses.
7. Ensure inbound ports 23 (telnet), 2323 (used for telnet on some IoT devices), and 103 (Mirai backdoor) are blocked at your Internet firewall or gateway router.

1. Incident Response Planning: Update your incident response plans with DDoS mitigation strategies.

a. Perform an internal analysis of what impact a DDoS attack can have our your business.
b. Document the approach and integrate your DDoS protection and security strategy into your company's policies and procedures, and most importantly, Business Continuity / Disaster Recovery Plans.
c. Create a DDoS organization chart defining roles, authorities, and responsibilities during an attack.
d. Articulate company protocols during a DDoS attack to end users.
e. Create the call tree your company will use in the event of a DDoS attack for internal and external partners. Ensure this includes phone numbers that would not be impacted by a DDoS attack, such as VOIP phones.
f. PR/Communications – prepare an explanation for customers and how they can reach you during the attack. Have multiple communication paths in case the attack is widespread.
g. Implement a data back-up and disaster recovery plan that maintains air gapped copies of sensitive or proprietary data in a separate and secure location. Consider an additional set of backup copies of sensitive data that are not readily accessible from local networks.

2. Practice a massive DDoS disaster exercise with your team and service providers.

a. Perform ongoing tests and evaluations of your systems and of new technologies available in the marketplace.
b. Create a communications strategy that is well rounded and not fully reliant upon the internet for reaching your customers.
c. Ensure your vendors are involved and have a plan for their own services.

3. Add DDoS protection to an existing SLA with your ISP. Contact your ISP and discuss your concerns in advance of an attack. Identify a DDoS hotline number that your team can call.

4. Discuss business continuity risk and determine whether or not you should engage a backup ISP in the event of a DDoS attack to keep your operations running

PHASE 3

1. Join your local sector-based Information Sharing and Analysis Centers (ISAC) or consider joining FBI's InfraGard to build a peer group of companies like you that could be facing the same challenges in deflecting DDoS attacks. For members of the financial sector ISAC (FS-ISAC), consider inclusion in the Financial Systems Analysis and Resilience Center (FSARC).

2. Evaluate Mitigation Defenses and Tools

a. Reduce malicious traffic by using Unicast Reverse Path Forwarding (uRPF)
b. Implement load balancers to balance traffic across multiple servers, sites, and providers.
c. Consider a cloud-based anti-DDoS solution to filter or divert malicious DDoS traffic.
d. Consider other routing options such as Anycast.
e. Examine options for advance blocking, such as Reputation-Based and Access Control Lists.

888-733-5007

Fortalice