# Large Denial Of Service Attack Against Dyn

Presentation prepared by the SANS Technology Institute's Internet Storm Center



SANS Technology Institute

The best. Made better.

# What is DNS?

- ”Internet Phone Book”. Translates human readable names into Internet Addresses:
  - Isc.sans.edu => 66.35.59.249, 2607:f1c0:846:9100::15c
- If you own a domain (”sans.edu”), then you need to provide DNS for this domain
- If DNS breaks, then customers can’t reach your web site. E-Mail service will likely be distrupted as well
- Companies like Dyn can run DNS for you

# Who is Dyn? (pronounced [ˈdaɪn])

- Company originally became known for providing DNS services for users with dynamic Internet Addresses (home users, small businesses)
- More recently, Dyn offers services to large enterprises that need a robust geographically diverse DNS infrastructure
- Dyn is one of the biggest, if not the biggest provider of such services. It maintains data centers around the globe and uses various techniques to provide redundancy

# Why Did Dyn Fail

- A large network of compromised devices was used to flood Dyn's servers with traffic
- In particular servers used as part of Dyn's enterprise offerings were targeted
- Dyn wasn't able to handle the additional traffic, and its servers either stopped responding or responses were substantially delayed.

# Who Did it and Why?

- It is unknown at this point who is behind the attack, or why they selected Dyn as a target.
- The “Mirai Botnet” is assumed to be responsible for the attack. This botnet uses hundred of thousands of compromised devices like security cameras and routers to launch these attacks
- DDoS attacks are often used to shut down web sites or companies for political reasons or for ransom. But at this point, nobody claimed responsibility
- It is possible that the target was a Dyn customer, not Dyn

# Can This Affect Us?

- Yes. Even if we are not a Dyn customer, any DNS provider could be hit by the same attack and would likely have similar problems
- In house hosted DNS is likely more vulnerable, but it would prevent us from getting caught up in an attack targeting others.
- At this point, there is no bullet proof defense against these attacks. A temporary outage can likely not be avoided
- This botnet has been used to attack web servers as well, not just DNS

# How can we minimize the risk?

- Use multiple DNS providers. This way, if one experiences problems, we can use the others as backup
- This requires additional tools and setup to make sure information is synchronized across different providers
- We can maintain some DNS servers in house to provide limited service to internal users and as a last resort if we are not targeted, but experience issues due to collateral damage
- Adjust our DNS configuration to allow for caching of our records (increase “Time to Live”)

# What Should We Do In Response?

- Review your DNS infrastructure and configuration (e.g. Time to Live)
- Evaluate your dependency on DNS, specifically for your most critical domains
- Review existing agreements with DNS providers
- Review existing agreements with Anti-DDoS providers
- Investigate the use of multiple DNS providers
- Review monitoring capability. To minimize downtime, it is important to quickly identify the attack and characterize the attack traffic

# What Can Be Done Against the Mirai Botnet?

- Most of the infected systems used in these attacks are owned by home users and small businesses with limited security capabilities
- ISPs are working on identifying infected users by disrupting the command and control infrastructure of the botnet
- This is a process that may take months if not years to show significant success

# Conclusion

- You can't defend against large scale DDoS attacks without the help from others (anti-DDoS services)
- It is important to diversify critical infrastructure like DNS
- DDoS attacks need to be characterized quickly to direct effective defenses and to coordinate with anti-DDoS service providers
- IoT type devises need to be reviewed and deployed carefully to not contribute to problems like "Mirai"

SANS Technology Institute

# Feedback

- Please send any feedback to https://isc.sans.edu/contact.html
- Feel free to share this presentation
- Check for updates at https://isc.sans.edu/diaries/

SANS Technology Institute