the Availability Digest

www.availabilitydigest.com
@availabilitydig

U.S. Internet Traffic Comes to a Halt

November 2016

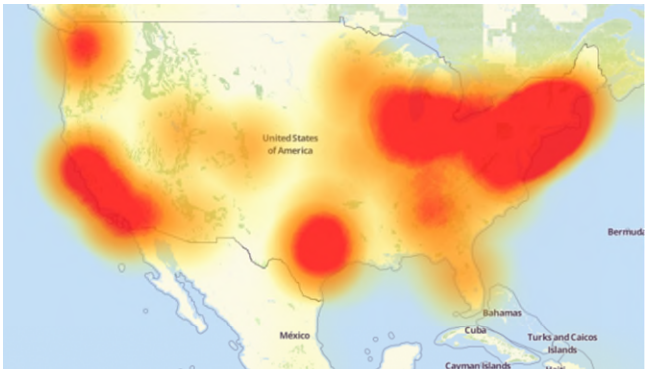
In our article in last month's issue of the *Availability Digest*, "Can a Country Shut Down Its Internet," we concluded that most developed countries could not do so – certainly not the United States nor the western European countries. Internet access is provided by too many Internet Service Providers (ISPs), and all would have to be taken out of service. The Internet has been taken down by the governments of countries that have only one or two ISPs, such as Syria and Libya.

However, now we must backpedal a bit on that statement. The Internet was taken down over a large swath of the United States in mid-October, 2016. How did that happen? The short answer is a massive DDoS attack on a major DNS provider.

The Internet Outage

At 7:10 am Eastern Time on October 21, 2016, users around the world started to have problems accessing some of the most popular sites on the web. The sites included Netflix, Twitter, Spotify, Reddit, CNN, PayPal, Pinterest, Fox News, Amazon, Github, and Airbnb. Many newspapers also were included in the outage, including the Guardian, the New York Times, and the Wall Street Journal.

The web sites that were inaccessible seemed to be concentrated in the United States in the Northeast, Texas, Los Angeles, San Francisco, and Seattle. Some web sites in Europe were also affected.



A depiction of the Internet outages. (Source: Downdetector)

The morning outage lasted about two hours. It was determined that the outage was caused by a massive DDoS (Distributed Denial of Service) attack on Dyn, a major Domain Name System (DNS) company located in New Hampshire, U.S.A. The outage was resolved by Dyn around 9:30 am.

© 2016 Sombers Associates, Inc., and W. H. Highleyman
www.availabilitydigest.com
For discussion, contact editor@availabilitydigest.com

A second attack occurred just before noon. A third attack was launched against Dyn a little after 4 pm. During each of the attacks, the affected web sites were unavailable for access by anyone.

How Did It Happen?

As a DNS provider, Dyn resolves URLs entered by users into IP addresses so that the web sites being referenced by the URLs can be accessed via the Internet. When Dyn was hit by the massive DDoS attack, normal URL requests could not reach Dyn and could not be resolved.

Dyn provides DNS services to many predominant web sites, including those listed above as being unreachable. This is why these web sites could not be reached during the Dyn attacks. DNS registrars such as Dyn typically provide DNS services for thousands or tens of thousands of domain names.

According to Dyn, the DDoS attacks were coming from tens of millions of IP addresses at the same time.

Dyn has no idea who launched the attack or why.

Attacking a DNS server is a very effective way to take down multiple web sites (perhaps thousands in the case of Dyn). Rather than targeting individual web sites, a DNS server attack takes out the entire Internet for any web sites served by the DNS server and for any end users whose URL resolution requests route through that server. The volume of malicious DDoS requests directed toward the DNS server is amplified by automatic re-requests when IP resolutions are not received and by well-meaning users hitting “refresh” over and over.

The IoT Conundrum

The DDoS attack launched against Dyn used the Mirai virus. The Mirai malware is a very sophisticated virus. It is self-propagating malware that builds a botnet of devices by scouring the Internet for IoT devices that are protected by little more than factory-default usernames and passwords. The botnet can then be directed to launch a DDoS attack against a target by the botnet director.

Any device connected to the Internet is a candidate for a Mirai infection – DVRs, cable set-top boxes, routers, even Internet-connected cameras used by stores and businesses for surveillance.

Mirai malware is estimated to have infected over 500,000 devices so far. About 10% of these devices participated in Friday’s attack against the Internet. Apparently, other botnets also were involved.

Interestingly, the Internet attack was launched the day after Dyn’s principal data analyst wrote a blog about these types of IoT-based attacks entitled “What Is The Impact On Managed DNS Operators?”

The developer of Mirai released the source code for the Mirai malware on September 30, 2016. The source code was posted on dark web sites that operate as sort of an online underground for the hacker community.

The Mirai source code now available to hackers allows any hacker to build his own IoT attack army. This virtually guarantees that the Internet will soon be flooded with attacks from many new botnets powered by insecure routers, IP cameras, digital video recorders, and other easily hackable devices.

Summary

The Mirai Internet attack has drawn the attention of the FBI, which is investigating all potential causes of the attack. However, until IoT device manufacturers incorporate powerful security features into their software to deter malware infections, such attacks are likely to continue. There is no indication that IoT device manufacturers are going to follow this route.

© 2016 Sombers Associates, Inc., and W. H. Highleyman
www.availabilitydigest.com
For discussion, contact editor@availabilitydigest.com

What can you do to protect yourself against such a DNS attack? Make sure that you have contractual relations with a backup DNS server to which you can switch if your DNS provider is taken down.

Acknowledgements

Information for this article was taken from the following sources:

Internet of Things comes back to bite us as hackers spread botnet code, *USA Today*; October 3, 2016.
Recent IoT-Based Attacks: What Is The Impact On Managed DNS Operators, *Dyn Blog*; October 20, 2016.
What We Know About Friday's Massive East Coast Internet Outage, *Wired*; October 21, 2016.
Major cyber attack disrupts internet service across Europe and US, *The Guardian*; October 21, 2016.
An IoT botnet is partly behind Friday's massive DDoS attack, *PC World*; October 21, 2106.
Widespread cyberattack takes down sites worldwide, *CNN*; October 21, 2016.
Hacked Cameras, DVRs Powered Today's Massive Internet Outage, *Krebs on Security*; October 21, 2016.
That massive internet outage, explained, *Cnet*; October 21, 2016.
Hacked home devices caused massive Internet outage, *USA Today*; October 22, 2016.

© 2016 Sombers Associates, Inc., and W. H. Highleyman
www.availabilitydigest.com
For discussion, contact editor@availabilitydigest.com