CRS INSIGHT

Did a Thermostat Break the Internet?

October 26, 2016 (IN10600)

|

Related Author

- Chris Jaikaran

|

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov, 7-0750)

On September 20, 2016, the computer security blog KrebsonSecurity (Krebs) was hit with a massive attack —one that surpassed the scale of previously known attacks. One month later, on October 21, 2016, domain name system provider Dyn experienced a similar attack which prevented many users in the United States from accessing popular websites, such as Amazon, Reddit and Twitter.

Both these attacks have in common a malicious botnet named Mirai.

Botnets and Denial of Service Attacks

A botnet is a network of computers or other Internet-connected devices that an attacker has infected with malware that grants them control and use of the resources of that device (e.g., the processing power, network access, microphone and camera, etc.). A single device in that network is called a 'bot.' Adversaries may use botnets they cultivate for their own purposes, or they may rent out their botnets for other attackers to use, such as to carry out a denial of service (DOS) attack, like those which hit Krebs and Dyn. A DOS attack is an attack against the availability of data. In this attack, an attacker overloads a network or website with information, monopolizing the bandwidth of that site and making it so that legitimate users cannot get their requests for service through, resulting in the user experiencing the site as down. A DOS attack itself does not constitute an intrusion into the network or website, but it may be combined with other forms of attack to compromise the confidentiality or integrity of the network or its data. A distributed denial of service attack (DDOS) occurs when many, disparate devices are used in the attack, as is the case when a botnet is employed for a DOS attack.

In some ways, DOS attacks are like heavy storms that overload gutters. As more rainwater falls into the gutter system than it can handle, water backs up, unable to flow through until the rain lets up.

The Internet of Things Ganged Up

The Mirai botnet is unique because it takes advantage of Internet of Things (IOT) devices. In this case, many of those devices were web-enabled cameras and digital video recorders (DVRs) with published and unchanged administrative usernames and passwords. Some of these devices were sold directly to consumers, while others were components sold to other companies who incorporated those parts into their products. The Mirai botnet scanned the Internet for these devices, and when it encountered one, it used the known credentials to gain access to the device and reprogram it to

execute commands from botnet servers. Many of the devices used in Mirai-based DOS attacks had predominantly Asian internet protocol (IP) addresses.

Internet of Things Risk

DOS attacks happen frequently, but network administrators have ways of mitigating those attacks so that users do not experience degradation in service. The use of IOT devices in a DOS attack is significant because it dramatically increases the capacity of attack beyond what was previously observed and beyond what network administrators have had to mitigate. For instance, the content delivery network Akamai, which provided services to Krebs when that site was attacked, had previously seen attacks peak at around 320 gigabits per second (gbps). However, the attack against Krebs peaked at over 620 gbps—doubling their previous record. Authoritative numbers for the size of the Dyn attack are not publicly available.

These attacks highlight some risks with IOT devices. Many of those devices are relatively inexpensive, are connected to the Internet without security measures in place, are rarely updated to fix vulnerabilities, and linger on the Internet as long as users find the device itself useful—making them susceptible to attack and use in botnets. In addition to risks with the IOT devices themselves, their use presents policy challenges such as shifts in expectations in privacy from the information they collect, the lack of security and other standards for them, and unexplored responsibilities for liability for IOT devices in a global economy.

As consumers deploy IOT devices for their benefits, such as safety, efficiency and improved user experience, the common infrastructure everyone uses for network access may experience increased attacks from infected IOT devices. These types of attacks may compromise the very core of the Internet and jeopardize interstate commerce and national security.

Policy Implications

U.S. government agencies have started to take steps to address risks with IOT devices. The FTC issued a report that encourages companies to apply cybersecurity best practices to their IOT devices: such as building security into devices on the onset, employing multiple defensive strategies, and monitoring them throughout their expected life cycles, including providing continual security updates as needed. The DOT has issued guidance on autonomous vehicles. HHS has engaged partners in a Health Care Industry Cybersecurity Task Force which, among other things, will inform ways to secure medical devices.

IOT issues, including security, have received attention in the 114th Congress and may be of interest to the 115th as well. House and Senate resolutions have called for a national strategy. House and Senate bills would require the Secretary of Commerce to convene a federal working group to report recommendations to Congress on facilitating IOT development, including consideration of security and privacy issues, among others. Both the House and the Senate have held hearings on the IOT, addressing a range of issues, including its ramifications for security, privacy, and the integrity of the Internet.

In response to the attack on Dyn, Senator Mark Warner asked federal agencies to examine the tools available to secure IOT devices and what additional tools might be needed. Additionally, congressional committees, as part of their oversight activities, may engage with federal agencies as they pursue rulemaking and issuing guidance on IOT devices. Congress could also encourage industry to ensure it adequately considers security needs in manufacturing and deployment of IOT devices in a manner that not only considers consumer needs but also security of the Internet. Congress could also work to further define roles and responsibilities and acceptable actions for security of the Internet.