What is botnet DDoS?

As the number of IoT devices continues to grow, fears of cyberattacks also increase. One of the main sources of attack is DDoS botnets targeting unsecured IoT devices.

As the number of IoT devices continues to grow, fears of cyberattacks also increase. One of the main sources of attack is DDoS botnets targeting unsecured IoT devices.

Knowing the true dangers of DDoS threats and how to fix them are very important for consumers. Today's article takes a look at the current state of this issue and explores its impact on the IoT.

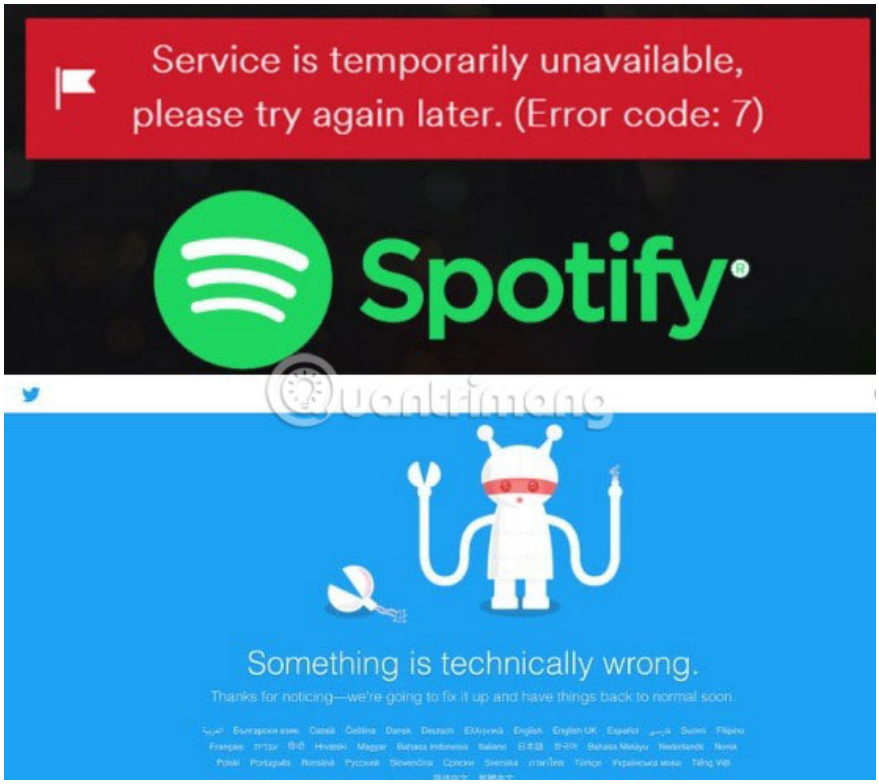
Learn about the DDoS botnet and its impact

What is botnet DDoS?

The Distributed Denial of Service Botnet (DDoS) is a self-propagating malware that weaponizes infected IP connections, is protected by weak passwords, often intended to destabilize the item's device. target or steal information on the device. There is always a big surge in traffic, which can cause an entire system to crash.

A well-known example of DDoS botnet is October 21, 2016, the Dyn network attacks brought down the Internet for millions of users worldwide. Dyn is a dynamic DNS service of Oracle Group. Attackers targeted the company's cloud service, using the Mirai botnet as the source, while concealing TCP and UDP traffic through port 53.

As the bots multiply, they weaponize infected IP cameras, access ports and child surveillance equipment. However, the impact is limited to sites like Twitter and Spotify being shut down for hours.



How many DDOS botnet attacks have taken place?

There have been a few more DDoS botnet attacks since the Dyn incident. Although not at the same scale as Dyn, these attacks have used various vectors. This is a major concern for security researchers.

Satori DDoS botnet attack

On September 4, 2019, a Washington state hacker named Kenneth Schuchman, along with an accomplice, launched the Satori botnet. To do this, they used a leaked Mirai botnet source (used in Dyn attacks). More than 100,000 IoT devices have been compromised including GoAhead cameras and intelligent digital video recording systems (DVRs).

The worst thing is that the exploit devices are based in Vietnam and the target is a Canadian ISP. It shows the true global nature of the problem and it's relatively easy to launch a DDoS attack from insecure IoT devices in another country.

DDoS Imperva botnet attack

On July 24, 2019, a Silicon Valley company called Imperva witnessed a DDoS attack in the application layer 7, where more than 400,000 IoT devices were compromised. The source of the attack is Brazil.

QBot

This botnet attacks Telnet networks and has been around for the past two years. Although no serious security incidents have yet occurred, this botnet can be easily downloaded online for attack.

Which IoT devices are more vulnerable to DDoS botnet attacks?

With Mirai in the past, it was clear that IoT devices such as IP cameras were most vulnerable to DDoS botnet attacks. Video doorbells are a serious area of ??concern, and there have been reports of hackers providing fake doorbell images to gain unauthorized access to homes.

To date, there have been no reports of DDoS botnets targeting smart speakers, smart displays or consumer electronics such as smart refrigerators. The main reason may be that many popular product manufacturers use Amazon or Google cloud services, ensuring stable security.

Meanwhile, video doorbells or IP cameras are manufactured by many companies and some of them may have lax security standards.

Will 5G increase the risk of DDoS attacks?

Some IoT security analysts believe that the advent of 5G networks could bring new power to DDoS botnet attackers. The main reason is that the increased bandwidth and lower latency of the 5G network will help attackers of IP cameras and other devices take immediate action.

Many IoT devices are not secure connected to 5G. Therefore, 5G network is a viable path for an attack vector under the right conditions. If ISPs do not take adequate precautions to make their 5G access points 'inviolable', that could lead to negative consequences.

DDoS botnets can have the effect of crippling an organization and disabling connected systems. While the current threat landscape is not as bad as the 2016 Dyn disaster, downloading DDoS botnets too easily and neglecting continuous security between certain types of IoT devices can lead to crashes.

Are you concerned about IoT devices turning into tools for botnet attackers? Please express your views in the comment section below!