The rise of Botnet IoT and how to protect smart devices

In this article, we will explore how the Internet of Things and smart home appliances are being used to form a 'digital army' and follow the command of hackers.

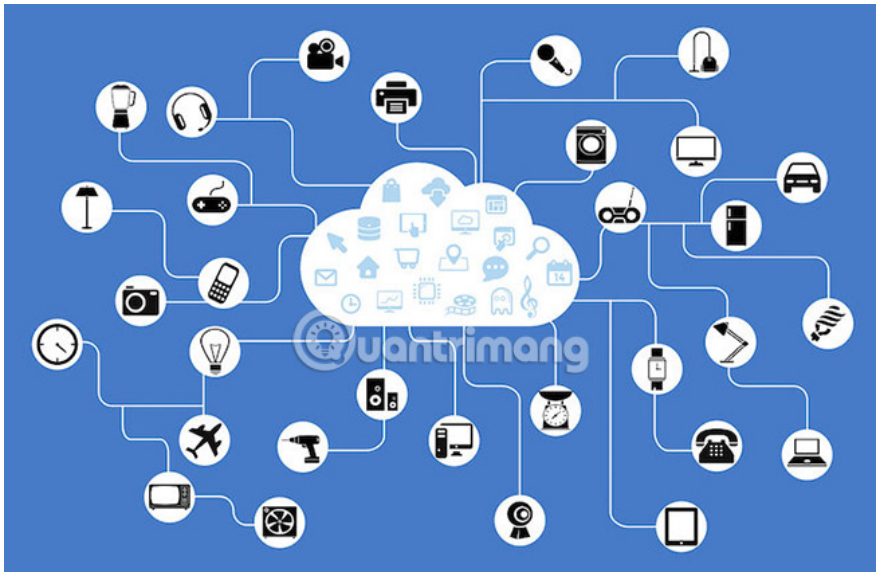
Connecting all utilities to the Internet is not a great idea. Although the Internet of Things allows you to perform remote tasks and monitor the device from anywhere in the world, it opens the door for hackers to take advantage of your device for bad purposes.

In this article, we will explore how the Internet of Things and smart home devices are being used to form a 'digital army' and follow the command of hackers.

Before learning about the effect of botnets on the Internet of Things, make sure you know what Botnet is, TipsMake.com has a pretty detailed article about Botnet, as well as how Botnet works, you refer. more

Learn about Botnet IoT

The impact of Botnet on the Internet of Things



Due to the autonomous nature of botnets, it is not too 'picky' of devices to bring into its network. If a device has a processor, Internet connection is consistent, malware can be installed, it can be used in a botnet.

Previously, this was limited to computers and mobile devices, as they were the only things that met the criteria. With the spread of the Internet of Things, more and more devices are joining the 'potential candidates' group for a botnet.

Worse, the Internet of Things is still in the development phase, so the security issue has not been finalized. A good example of this is that the hacker has access to the Nest security system at one's home and speaks to the person through a security camera.

With laxity in IoT security, it is not uncommon for botnet developers to take advantage of this new trend.

How can botnet IoT cause damage?

Botnet Mirai

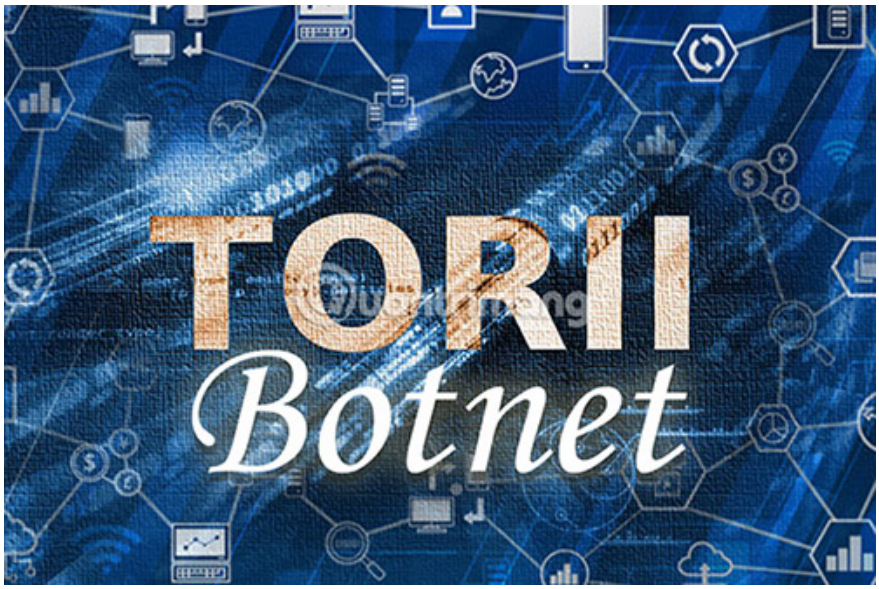
Although the IoT botnet is a new concept, the technology community has witnessed many devastating attacks from them. We saw such an attack at the end of 2017, when the Mirai botnet exploded. It scanned the Internet for IoT devices, then tried 60 default usernames and passwords to gain access to these devices.

After its success, the attack infested the malware Mirai botnet to the compromised device.

With the 'Force' forming rapidly, the Mirai botnet began attacking websites on the Internet. It uses its 'forces' to perform DDoS attacks, flooding websites with connections from botnet devices.

Mirai is open source, so botnet owners can create copycat variants of malware.

Torii botnet



At the end of 2018, the new candidate, Torii, appeared. Unlike other IoT botnets that use Mirai's code, this botnet uses its own, highly advanced code, which can infect most Internet-connected devices. Torii has yet to attack anything, but it may be accumulating 'force' for a major attack.

MadIoT

A Princeton study demonstrated that IoT botnets can attack power grids. The report describes an attack method called 'Manipulation of demand via IoT', (MadIoT), which works similarly to a DDoS attack but targets the grid. Hackers can install botnets on high-power IoT devices, then activate them all at once to cause power outages.

Other potential threats from Botnet

Although collective processing power is very useful for performing DDoS attacks, it is not the only thing that botnets are capable of performing. Botnets that specialize in any task require a lot of processing power. What botnet will be used will be decided by the operator.

If someone wants to conduct an email spam campaign, it is possible to use the processing power of the botnet to send millions of messages at once. It is possible to direct all bots to a website or advertisement to generate inaccurate and pocketed traffic. That person may even order the botnet to install malware by itself, such as ransomware.

Some botnet owners may not even want to use what they create. Instead, these people will aim to create a large and impressive network to sell in darknet to benefit. Some people even hire botnets as a subscription service (like renting a server).

Why is it difficult to detect botnet violations?

The main problem with IoT botnet is that it works very quietly. This is not a type of malware that makes a big difference in the way devices are compromised. It silently installs itself and does not work until it is called by the command server to perform an action.

Those who are using the device may find it slow, but nothing warns them that their smart camera is being used to perform a cyberattack!

Thus, it is perfectly normal for everyone's daily life to continue without knowing that their device is part of the botnet. This makes it difficult to remove a botnet, because the owners of these devices do not realize they are part of it.

Even worse, some botnets also install potentially malicious software even though the device has been reset.

How to protect smart devices

If you're a fan of the Internet of Things, don't fret too much! Although this attack may sound scary, you can still do some things to make sure your devices are not added to the botnet.

Do you remember how the Mirai botnet has access to the device using the 60 usernames and passwords mentioned above? The only reason it can do this is because people do not set up the device correctly. If the username and password for your IoT devices are 'admin', it will be attacked very quickly.

Be sure to log in to any device with an account system and set up strong passwords.

Be sure to install security software on the device. This acts as an additional layer of protection to 'grab' malware when it tries to spread into the system.

Botnets can also be spread through device vulnerabilities. To prevent this, always make sure the IoT utility is installed with the latest firmware version. In addition, only buy new equipment manufactured by reputable companies. That way, you will know if the device has gone through all the appropriate security checks before the device is used in your home.

As more and more devices connect to the Internet, botnet developers are very eager to take advantage of this. With evidence of what botnet IoT can do (through the case of Mirai and Torii), device security is very important. By purchasing reputable hardware and ensuring it is installed correctly, the device will avoid the risk of being added to the 'digital army' of the botnet.