The Security Implications of The Mirai IoT Botnet Attack

Kevin Wells • November 1, 2016 • Feature Articles

In October 2016 a major hacker attack occurred in the United States.

The attack came from a so-called botnet which is estimated to have been coordinated using several hundred thousand bot-infected devices simultaneously.

The attack hit and partially knocked out several high profile websites including among others Twitter, Netflix, Spotify, and Paypal.

What's a Botnet?

Botnets are a form of malware which is becoming a serious threat around the world.

A "bot" is a small piece of software remotely controlled by a hacker which finds its way into your computer. The bot can also propagate itself, searching the Internet for other computers to infect.

A "botnet" is a network of computers infected with bots in this way. The entire botnet is remotely controlled by a hacker, who then uses the combined power of the botnet to perform illegal and destructive acts.

What Damage Can Botnets Inflict?

Most often, botnets launch attacks against web servers and other Internet services such as DNS – the server system that operates the domain name service which makes website and email domain names reachable for everyone on the Internet.

The combined processing power of the botnet host computers is used to send millions of small "requests" all at the same time.to attack a server or group of servers.

This has the effect of overloading the target server with more traffic than it can process. As a result, the server becomes extremely slow or even crashes completely – thus the term "denial of service".

What Made This Botnet Attack More Serious Than Previous Attacks?

Latest articles

The Best VPN for Dubai Of 2016
Reviews • 6 comments

3 Best VPN's For Apple Mac Computers
Reviews • 2 comments

Best VPN For Omegle
Reviews • 2 comments

How to Get Unbanned from Omegle
Reviews • 2 comments

ExpressVPN the VPN for you? Our Review
Reviews • 29 comments

Recommended topics

- Internet Security
- Protect Your Information
- Phone and Tablet Security
- Protecting Your Children

The October 2016 Mirai Botnet attack, after the name of the Mirai bot program responsible for the incident, targeted DNS or domain name service servers. Such an attack can have serious consequences for a large number of websites.

But what made this incident especially unusual was that instead of being launched from bot-infected PCs and laptops as is usually the case with botnet attacks, this one was deployed from Internet-connected household devices such as cameras and DVRs.

This wasn't actually the first attack by the Mirai botnet. There have been at least two other known high profile Mirai botnet attacks. In September 2016, the website of security expert Brian Krebs was targeted by a massive DDoS attack which was one of the largest in the world to date.

It's estimated over 380,000 IoT devices were under the control of the Mirai botnet involved in the attack on the krebsonsecurity.com website.

France's TV5 broadcasting network also experienced a massive DdoS attack. There have also been attacks on other infrastructure such as electric power utility stations and networks.

The October attack relied heavily on bot-infected digital video recorders and web cameras which were manufactured using components made by the Chinese electronics manufacturer XiongMai Technologies.

Xiongmai subsequently announced a product recall for webcam devices sold in the United States and stated that it will strengthen password functions. It will also be sending users a patch for products made before April 2015.

So Who Was Behind The Botnet Attack?

The answer is that we don't know for sure. Was the attack purely a hacker phenomena, a geek wanting to see how much damage they could inflict?

Or was it directed by a government or an intelligence group testing their cyberwarfare capabilities?

The latter is certainly possible, but it's difficult to prove. Intelligence authorities don't usually advertise their cyberwarfare preparations and activities and they cover their tracks carefully.

Are Further Botnet Attacks Likely In Future?

Whoever was behind the Mirai botnet attack, the fact is it's an indication of what we can expect in future unless manufacturers of IoT devices start to take security seriously.

Security specialists have warned about the dangers of insecure IoT devices for some time now. In October 2016 the US Computer Emergency Readiness Team US-CERT warned of the danger posed by the Mirai Botnet.

Only now are people starting to wake up to the dangers posed by botnets running on IoT devices.

The problem right now is that ioT devices are just not designed with security in mind. IoT devices are a gaping hole sitting there waiting to be exploited by hackers and those planning cyber warfare.

Anti-virus and anti-malware software tools are available for conventional computers such as PCs and laptops. Computer users also tend to be aware of these tools and they generally provide a reasonable layer of protection against many bots and Trojans.

With IoT devices it's a different matter. Cyber criminals who run botnets to carry out DDoS attacks are switching to IoT devices because these are easier to locate, infect and manage than PCs.

The devices particularly favored by botnets are video devices, webcams, digital TV recorders, printers, and routers. These tend to have default usernames and passwords and no security software installed on them.

It's estimated hundreds of millions of devices on the Internet could already be infected with bots.

What Should You Do If You Suspect Your Device Has Been Infected By A Bot?

Most people have no idea their computer or other device is infected by a bot. Usually there's little or no sign that your device has become part of a botnet.

Bots don't create that much of a processing overhead for the device itself. At most you might notice a slower response in functionality with video or music streaming devices. Gaming devices too might experience some lag or delay in responsiveness.

US-CERT advises you take the following action in this order to remove the Mirai botnet malware from an infected IoT device:

- Disconnect the device from the Internet.
- Perform a hard reboot. That means physically switching the device off and on. The Mirai bot only exists in RAM, so rebooting the device will remove the infection.
- Change the password for accessing the device from the default password to a new, stronger password.
- Then – and only then – reconnect to the network and Internet. If you reconnect before changing the password, you risk the device being re-infected soon after once again by the Mirai bot.

How To Prevent Your Devices Being Taken Over By A Botnet

US-CERT recommend you do the following:

- Change default passwords to new and stronger passwords before connecting the device to the Internet. However, one problem here is that some IoT devices don't provide any interface or means to change the password.
- Update IoT devices with security patches as soon as patches become available.
- Disable the Universal Plug and Play (UPnP) function on routers
- Only purchase IoT devices from companies with a reputation for providing secure devices.
- If you think an IoT device might be infected by a bot, then disconnect it from the Internet and perform a cold reboot.

How Can We Prevent More Botnet Attacks Occurring In Future?

Lawmakers are also concerned about the threat posed by botnets.

The main US law covering the issue of computer hacking is the CFAA or Computer Fraud and Abuse Act of 1986. Lawmakers and the computer industry generally agree this law is long overdue for reform.

The Dangers To Liberty Posed By The Botnet Prevention Act

The US Senate now proposes the Botnet Prevention Act which aims to widen the scope of the CFAA to include botnets as one of the offenses that entitle the Department of Justice to apply for an injunction to seize equipment or demand their disconnection.

The DoJ says it needs this additional authority to protect people the dangers of botnets.

The EFF or Electronic Frontier Foundation are concerned about the impact of this proposed new legislation on digital freedom and individual liberty.

The concern is that the Botnet Act constitutes over-criminalization and would allow law enforcers greater freedom to seize computers and other digital devices.

Federal law enforcers aren't allowed access to your home without a search warrant obtained from a court of law.

So surely this should also apply to our computer equipment?

Our computer devices contain our personal data and to seize or search them without a warrant surely goes against the ideals of individual liberty and privacy.

Given the nature and cause of the botnet problem, trying to tackle this issue through draconian new legislation is not going to resolve the cause of the problem.

What Are The Alternatives To The Botnet Prevention Act?

One idea being implemented in Japan is to create a public-private partnership to warn people when their devices are infected. Another suggestion is to educate people in the dangers of bots and malware and increase awareness of the problem.

The difficulty here is that most people don't want to be bothered with technical issues of security, particularly when there's no clear direct loss to themselves.

Many of these IoT devices are at present practically unfixable and so they are open to repeated botnet infection for as long as they are connected to the Internet.

Usernames and passwords are often hard-coded into the firmware of the device.

With the exploding growth in the market for IoT devices, this poses enormous security problems for the future.

A more practical solution will have to be found. The problem is not with law-making or the lack of suitable legislation.

The IoT botnet problem is already a global one, affecting manufacturers and Internet users – both businesses and consumers worldwide.

The solution needs to involve combined action by an industry-wide security association of manufacturers and software companies. Security standards will have to be defined and implemented by all those active in the industries involved in the IoT sector.

Until then the door is wide open for further IoT-based botnet attacks and sooner or later all those involved in the industry will have to take combined and concerted action to resolve the issue of IoT device security.

Have any of your devices been affected by the Mirai bot or other botnet malware? We're interested to hear about your experiences and how you dealt with the problem of removing the malware. You can enter your comments below.

0

RELATED ARTICLES

16 Experts Reveal How To Protect Your Credit Card Online

How Data Encryption Could Save You a Million Euros

Top 40 Security and Technology Resources for 2016

We will be happy to hear your thoughts

LEAVE A REPLY

Name E-mail Website

Post comment

Notify me of followup comments via e-mail. You can also subscribe without commenting.

Latest Articles

The Best VPN for Dubai Of 2016

3 Best VPN's For Apple Mac Computers

Best VPN For Omegle

How to Get Unbanned from Omegle

ExpressVPN the VPN for you? Our Review

SECURETHOUGHTS
INTERNET SECURITY FOR EVERYDAY PEOPLE

Secure Thoughts is the industry leader in helping everyday people make sure their information and loved ones are protected online.

Feature Guides

How To Watch Netflix Outside the USA
Best VPN Service Review Guide
Reviews

Your future and the future of those you love is too important to gamble with.

When you need the right advice, trust Secure Thoughts.