Mirai botnet and the IoT security challenge - blueAPACHE

Canonical: https://www.blueapache.com/blog/mirai-botnet-and-the-iot-security-challenge

Details:

2017

Late last year, a massive distributed denial of service (DDoS) against Dyn, a company that controls much of the internet's domain name system (DNS) infrastructure, caused disruption to online services worldwide. With millions of users unable to access major websites such as PayPal, Reddit and Twitter, this attack was likely the largest of its kind. Dyn reported that the attack was orchestrated using the Mirai Botnet and estimated that up to 100,000 malicious endpoints were involved.

Mirai Botnet

Mirai, or a direct derivative of it, was also linked to attacks on internet service providers in the UK infecting network equipment via the maintenance interface of individual devices. Deutsche Telekom, UK Post Office, Irish-based ISP Eir and various others were affected, leaving thousands of paying customers without internet access. The Mirai botnet is malware that primarily targets Internet of Things or IoT devices such as routers, digital video recorders, surveillance cameras and other Internet-enabled embedded devices. It operates by taking control of the BusyBox systems that are commonly used in IoT devices, and enslaves vast numbers of these compromised devices into a botnet, which is then used to conduct DDoS attacks. Mirai even includes a scanner that automatically searched the internet to find unsecured, Linux-based IoT devices, and take them over using default credentials. The source code for Mirai was leaked online and has resulted in the emergence of several large Mirai-based botnets that were used to launch gigantic DDoS attacks that generated up to 1Tbps of traffic – the largest ever recorded.

The IoT Security Challenge

What makes Mirai particularly lethal is the wide-spread proliferation of IoT devices in our daily lives. With their myriad applications, the possibilities are seemingly limitless – from automatic air conditioning, lights, networked cars and even smart coffee machines – all connected to the internet and capable of receiving remote messages and operating via Wi-Fi or Bluetooth. Gartner recently predicted that there are 6.4 billion connected things in use worldwide in 2016 and that by 2020 this number will exceed 20 billion. The interconnectedness of IoT makes them particularly susceptible to 'brute force' attacks that can wreak havoc on your organisation. A single insecure IoT device connected to your network, be it a security camera, an old network printer or even a remote-controlled lightbulb, can become the gateway to your organisation. The challenge with IoT devices is that not only are they often insecure by design, but they lack the options to apply patches or upgrade. The Mirai botnet has given us the first real glimpse into the power of an IoT botnet and the damage that can be done.

The Takeaway

IoT devices are vulnerable by design and there is no easy fix in sight. For there to be any chance of preventing DDoS attacks, IoT device manufacturers will need to consider architecting fundamental security principles into the designs, such as avoiding the use of default credentials. Recently, the

Federal Trade Commission filed a complaint against Taiwan-based computer networking equipment manufacturer D-Link Corporation and its U.S. subsidiary, alleging that inadequate security measures taken by the company left its wireless routers and Internet cameras vulnerable to hackers and put U.S. consumers' privacy at risk. The lawsuit essentially puts all IoT device makers on notice, potentially holding them accountable for security holes that leave businesses and consumers vulnerable to attacks. While no organisation can be 100 percent secure all the time, it helps to be proactive about your security measures. Keeping devices and routers up-to-date with the latest vendor firmware can help avoid a single point of failure which could be used to penetrate your network. By deploying a layered defence and constantly monitoring your network traffic, DDoS attacks and other such threats can be detected quickly and resolved with minimal disruption to normal network services. Educating staff about the risks of IP-enabled devices and the importance of ongoing password management is also a key measure. It is all too easy to take technology for granted and often users fail to fully appreciate the risks before they have experienced a malicious attack themselves. For more information on how to better secure your business, contact the our account team .

What was the Mirai botnet attack against Dyn and when did it happen?

Late in 2016, a massive distributed denial of service (DDoS) attack was launched against Dyn, a company that controls much of the internet's domain name system (DNS) infrastructure. The attack, orchestrated using the Mirai botnet, disrupted online services worldwide, leaving millions of users unable to access major websites such as PayPal, Reddit and Twitter. Dyn estimated that up to 100,000 malicious endpoints were involved, making it likely the largest attack of its kind.

How does the Mirai botnet work?

The Mirai botnet is malware that primarily targets Internet of Things (IoT) devices such as routers, digital video recorders, surveillance cameras and other internet-enabled embedded devices. It operates by taking control of the BusyBox systems commonly used in IoT devices, enslaving vast numbers of these compromised devices into a botnet that is then used to conduct DDoS attacks. Mirai includes a scanner that automatically searches the internet for unsecured, Linux-based IoT devices and takes them over using default credentials.

What happened after the Mirai source code was leaked online?

After the Mirai source code was leaked online, it resulted in the emergence of several large Mirai-based botnets that were used to launch gigantic DDoS attacks generating up to 1Tbps of traffic — the largest ever recorded at the time.

Which internet service providers were affected by Mirai or its derivatives?

Mirai, or a direct derivative of it, was linked to attacks on internet service providers in the UK by infecting network equipment via the maintenance interface of individual devices. Deutsche Telekom, UK Post Office, Irish-based ISP Eir and various others were affected, leaving thousands of paying customers without internet access.

Why are IoT devices particularly vulnerable to attacks like Mirai?

IoT devices are often insecure by design and lack options to apply patches or upgrade. Their interconnectedness makes them particularly susceptible to 'brute force' attacks. A single insecure IoT device connected to an organisation's network — such as a security camera, an old network printer, or even a remote-controlled lightbulb — can become a gateway into the organisation.

How many connected IoT devices did Gartner predict would be in use, and by what year?

Gartner predicted that there were 6.4 billion connected things in use worldwide in 2016, and that by 2020 this number would exceed 20 billion.

What legal action did the FTC take related to IoT security, and what was it about?

The Federal Trade Commission filed a complaint against Taiwan-based computer networking equipment manufacturer D-Link Corporation and its U.S. subsidiary, alleging that inadequate security measures left its wireless routers and Internet cameras vulnerable to hackers and put U.S. consumers' privacy at risk. The lawsuit effectively puts all IoT device makers on notice, potentially holding them accountable for security holes that leave businesses and consumers vulnerable to attacks.