Someone is Using Mirai Botnet to Shut Down Internet for Entire Nations – US Next?

By Swati Khandelwal

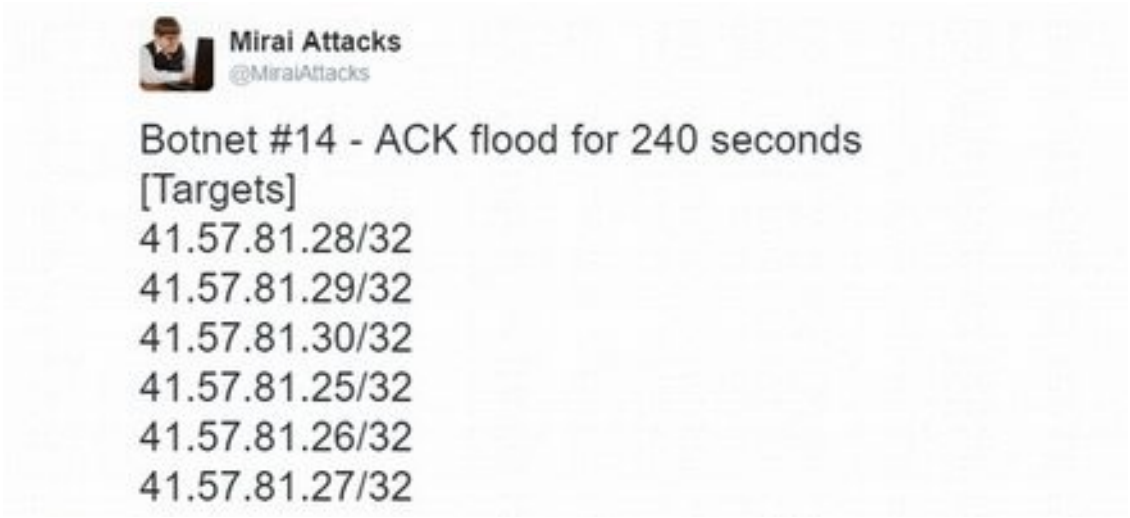
Someone is trying to take down the whole Internet of a country by launching massive distributed denial-of-service (DDoS) attacks using a botnet of insecure IoT devices infected by the Mirai malware.

It all started early October when a cybercriminal publically released the source code of Mirai – a piece of nasty IoT malware designed to scan for insecure IoT devices and enslaves them into a botnet network, which is then used to launch DDoS attacks.

Just two weeks ago, the Mirai IoT Botnet caused vast internet outage by launching massive DDoS attacks against DNS provider Dyn, and later it turns out that just 100,000 infected-IoT devices participated in the attacks.

Experts believe that the future DDoS attack could reach 10 Tbps, which is enough to take down the whole Internet in any nation state.

One such incident is happening from past one week where hackers are trying to take down the entire Internet of **Liberia**, a small African country, using another Mirai IoT botnet known as Botnet 14.



Security researcher **Kevin Beaumont** has noticed that Botnet 14 has begun launching DDoS attacks against the networks of "Lonestar Cell MTN ", the telecommunication company which provides the Internet to entire Liberia via a single entry point from undersea fiber cable.

> "From monitoring, we can see websites hosted in country going offline during the attacks — Additionally, a source in country at a Telco has confirmed to a journalist they are seeing intermittent internet connectivity, at times which directly match the attack," Beaumont said in a blog post published today.

According to Beaumont, transit providers confirm that the attacks were over 500 Gbps in size, but last for a short period. This volume of traffic indicates that the "**Shadows Kill**" Botnet, as the researcher called it, is *"owned by the actor which attacked Dyn."*

Why Taking Down Liberia's Internet Is easy?

Over a decade of civil war in Liberia destroyed the country's telecommunications infrastructure, and at that time a very small portion of citizens in Liberia had access to the internet via satellite communication.

However, some progress were made later in 2011 when a 17,000 km Africa Coast to Europe (ACE) submarine fiber-optic cable was deployed from France to Cape Town, via the west coast of Africa.

The ACE fiber cable, at depths close to 6,000 meters below sea level, eventually provides broadband connectivity to more 23 countries in Europe and Africa.

What's shocking? The total capacity of this cable is just 5.12 Tbps, which is shared between all of the 23 countries.

Since massive DDoS attack against DynDNS used a Mirai botnet of just 100,000 hacked IoT devices to close down the Internet for millions of users, one can imagine the capability of more than 1 Million hacked IoT devices, which is currently in control of the Mirai malware and enough to severely impact systems in any nation state.

This is extremely worrying because, with this capacity, not just Liberia, an attacker could disrupt the Internet services in all 23 countries in Europe and Africa, which relies on the ACE fiber cable for their internet connectivity.

The root cause? More insecure, vulnerable IoT devices, more Mirai bots.

So, in order to protect yourself, you need to be more vigilant about the security of your smart devices because they are dumber than one can ever be.

In our previous article, we provided some basic, rather effective, solutions, which would help you protect your smart devices from becoming part of the Mirai botnet. You can also check also yourself if your IoT device is vulnerable to Mirai malware. Head on to this article.