Akamai detected the Fast Flux botnet with 14,000 IP addresses

Researchers at Akamai have discovered a botnet with more than 14,000 IP addresses used to spread malware, using smart technology called Fast Flux.

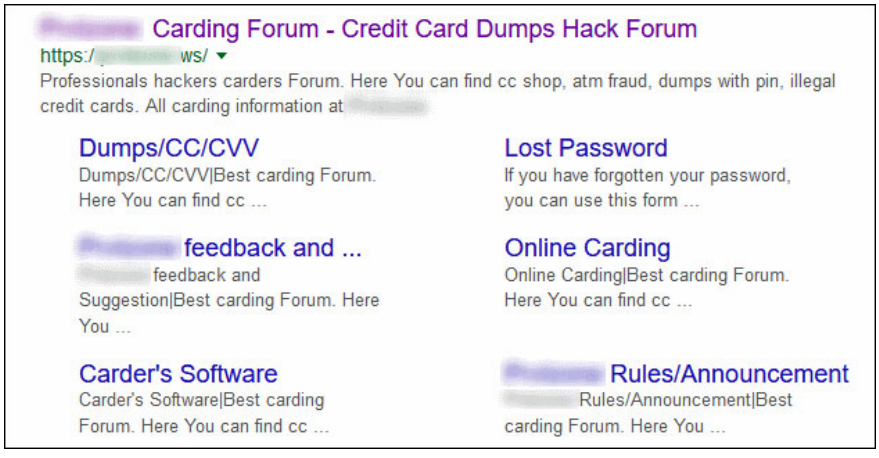
Researchers at Akamai have discovered a botnet with more than 14,000 IP addresses used to spread malware. The botnet is still running and experts believe it will be difficult to knock down using smart technology called Fast Flux.

The rule behind Fast Flux is when someone hosts a domain name that uses multiple IP addresses by switching from IP to another after a short time. Therefore the domain name in this technique will go through a very fast flow of IPs.

The first malware to use this technique was the Storm Worm, at the end of 2006, and used it to hide the IP address for the C&C server. The online criminal network, the malware host Avalanche also uses Fast Flux to hide its structure.

Botnet used to host malware activity

Presented at Akamai EDGE 2017, Akamai researchers revealed the existence of a similar structure of Avalanche, hosting everything from fake sites to web proxies, from online store cards to C&C servers. for multiple malware campaigns.



A forum host types of cards for online shopping on botnets

Besides hosting C&C servers for malware and scams, botnets are also used to perform automated attacks such as automatically collecting website information, injecting SQL statements and trying wrong on password libraries to steal passwords. .

The infected host is used as a proxy relay in the DNS Fast Flux botnet

Researchers believe that the malware-infected device used as a malware host has changed, by installing the proxy package on each host so that it appears on the Internet and transferring traffic to the botnet operator.

When someone wants to connect to the infected page, the DNS server will issue the IP of the currently infected host that is hosting the domain at that time.

Infected IP (via proxy package) will then redirect traffic to the actual infected page, hosted elsewhere. Researchers must pay attention not to record DNS as a real host for the site.

Botnets are made up of 2 separate networks

A closer look at the structure of the botnet, the researchers found that the entire structure is made up of two separate parts - the host network (to host and redirect traffic to the infected site) and the C&C network (C&C structure). of the botnet, not another active C&C host server).

1. What is a botnet, who does it use to attack, and how can you prevent botnet?

Each subnet has its own boojIP to host a temporary domain before moving to another domain. Most IPs come from Ukraine, Russia and Romania. The combination of subnets of botnets is also very different.

Most IPs contain private IPs, like 10.xxx, 192.168.xx, meaning they are hosts hosted on closed, private networks. In addition, there are clues that some IPs are likely to be Fortune's top 100 companies.

Does the botnet live on the router and modem?

Akama also analyzed ports for all IPs and found that most host networks have ports 80 and 443 (specifically for each proxy server), and most C&C networks have ports 7547.
This is very unusual because 7547 is a separate port for the TR-069 protocol used to manage remote routers and modems. This also reveals the types of devices used to create botnets.

Currently, there seems to be a shift in the IoT botnet market from using DDoS attacks to redirecting malicious traffic.

Akamai has not yet made a final conclusion about the structure of botnets or devices that make botnets as routers, IoT devices, computers . These are just observations. Research is still ongoing.