Fast Flux networks: What are they and how do they work?

By Josep Albors

The term Fast Flux can refer to networks used by several botnets to hide the domains used to download malware or host phishing websites, says Josep Albors.

12 Jan 2017 • , 4 min. read

After dismantling the Avalanche network, we found that it was using a Fast Flux network ... and this is not the first time that we've seen this kind of scenario either. This type of network has been around for several years now and is a real headache when it comes to dismantling a botnet built using this structure.

Let's start at the beginning.

What is a Fast Flux network and how does it work?

The term Fast Flux can refer to those networks used by several botnets to hide the domains used to download malware or host phishing websites. It can also refer to a type of network similar to a P2P network used to host both the command and control (C&C) centers or proxies used by these botnets, making them difficult to find and even more difficult to dismantle.

> "The basic concept of a Fast Flux network is having multiple IP addresses associated with a domain name, and then constantly changing them in quick succession."

The basic concept of a Fast Flux network is having multiple IP addresses associated with a domain name, and then constantly changing them in quick succession. In the case of Avalanche, for example, more than 800,000 malicious domains used by criminals have been discovered since it appeared in 2009, with IP addresses being changed within periods as short as five minutes, which would initiate connections to different machines despite requesting to see the same website controlled by attackers.

Most machines that make up this type of network are not actually responsible for hosting and downloading malicious content for victims. This task is reserved for a few machines that act as servers of this malicious content; the rest just act as redirectors that help to mask the real addresses of these systems controlled by criminals.

And to complicate matters even further, criminals ensure that the critical systems in their network have the highest possible availability and bandwidth, and even deploy load-balancing systems to handle all of the requests to download malicious content generated by their victims' systems. Another common practice is to review the network status at regular intervals in order to discard any inaccessible nodes and to ensure that their malicious content is still active and downloading.

Types of Fast Flux networks

There are two main types of Fast Flux networks:

1. Single Flux networks

A Single Flux network is characterized by multiple individual nodes registering and deregistering their IP addresses as part of a DNS A (address) for a single domain name. These registrations have a very short lifespan (five minutes on average) and create a constantly changing flow of IP addresses when attempting to access a specific domain.

The large number of nodes ready to register their IP addresses ensures that when one or more of them drop, others quickly take their place. Moreover, the domains used are usually hosted on “bulletproof” servers that some providers offer their clients, which ensures that any orders from law enforcement agencies to take down that domain will be ignored.

2. Double Flux networks

This type of network uses components and methods of establishing connections between the victim’s system and systems controlled by criminals that are similar to the previous one, but it is more sophisticated in that it has an additional layer that makes it difficult to **locate** the machine actually serving the malware.

In this case, zombie computers that are part of the botnet are used as proxies, which prevent the victim from interacting directly with the servers hosting and serving the malware and make it difficult to locate. Essentially, it is an additional concealment measure that criminals use to keep their infrastructure running for longer.

Detecting Fast Flux networks

> "It is relatively easy for a criminal to set up infrastructure using Fast Flux networks, which are difficult to trace."

When news of dismantling Avalanche first broke, it may have surprised some users to learn that this botnet had actually been active since 2009. And while six years is clearly a long time for a botnet of this nature to be active, it must be understood that it was its design itself that made investigating it difficult.

It is relatively easy for a criminal to set up infrastructure using Fast Flux networks, which are difficult to trace and use multiple nodes to mislead investigators. And different laws hinder these types of investigations even further, since the legal regulations of several countries usually apply, so the law enforcement agencies of several countries have to reach an agreement before action can be taken.

The constant change of the IP addresses used and the continuous generation of thousands of random domains (DGAs) doesn’t help investigators either. They have to spend a lot of time analyzing the lifespans of each connection established with the botnet. They also have to obtain information from ISPs that are not always willing to collaborate, and analyze innumerable domain registrar logs to find and filter any malicious activity that could give them a valid trail in their efforts to locate the botnet’s command and control centers.

That is why these types of investigations tend to drag on for years. Even a simple bureaucratic oversight could cause a whole operation to fail and to give those responsible for these criminal activities a chance to escape.

As users, the main thing we must ensure is that our systems are not part of one of these services managed by cybercriminals. Therefore, it is crucial to follow instructions on updating our systems and applications, to always keep antivirus systems up to date, and to check cyber security blogs regularly to be aware of threats like this and how to detect them.