Takedown Client-Server Botnets the ISP-way

Trần Minh Quảng
Viettel Group
Hanoi, Vietnam
quangtrm@gmail.com

ABSTRACT

Botnet is currently a existing threat to Internet users around the world. Users can lose money, personal information if infected. Bonet takedown has been a pressing need of many organizations in the world: the FBI, the national governments, the Internet service provider (ISP). For ISPs, this is actually a legitimate need to protect their consumers, their networks and meet the requirements of law enforcement agencies.

Basically, there are two types of botnet network model: Client-Server and Peer-to-Peer. In particular, ISPs can play a significant role in client-server botnet shutdown based on their inherent advantages.

Normally, in order to demolish a client-server botnet network, organizations must cooperate with service providers (domain name registrars, hosting/server providers) to acquire the malicious domain or server, then monitor the connections to shutdown. However, this method is quite passive when having to wait for the coordination of service providers. In particular, this method is not feasible for the bullet-proof server.

However, ISPs have a lot of advantages to takedown client-server botnets: own the user's Internet infrastructure, capable of monitoring/ processing/routing traffic on their network, own the technology allow deep analysis of packets.

In this paper, I will discuss methods which an ISP can use to takedown a client-server botnet on its network based on the ability to redirect malicious connections from C&C server to ISP analysis server using ISP DNS infrastructure, IP routing, that can easily track and shutdown botnet.

Keywords - Client-Server Botnet Takedown, Sinkhole.

I. INTRODUCTION

Beside direct victims of botnet, ISPs always take the most consequences from botnet activities. They continuously have to deal with many pressure from their customers as well as authorities. Also, they have to make sure that their network is working normally without bad activities such as spamming, scanning… which are the result of infected devices inside their network.

Customer is alway one of the most important subject in ISP activities. They are the main source of profit, the reason for the existence of any ISP companies. Nowadays, customer has a lot of choices in using Internet service. Naturally, with the increase of Internet threats, they tend to choose the safer ISP, who can

provide them a more secure Internet environment.

Sometimes, ISPs have to deal with requests from law enforcement agencies about stopping malicious activities from inside their network, that they event do not know where the infected devices are or how to clean those.

Besides, ISPs also want to get rid of any malicious activities inside their network to get a higher rank in global security ranking tables, which will give them the higher chance to be chosen by customer.

Last but not least, too many infected devices inside the network may lead to many unexpected consequences to network security. For example, a large scale DDoS attack caused by many infected computers may make the network out of bandwidth and then interrupt the whole company Internet service.

Obviously, ISPs care about how to takedown botnets in their network to make their customers as well as authorities happy and keep the company growing. And luckily, ISPs have some big advantages in taking down client-server botnets, which is the most popular botnet types in the world.

II. BACKGROUND

Botnet Infrastructure

Basically, there are two types of botnet based on their network infrastructure. The first one, called client-server botnet, has the following characteristics:

- They use centralized command-and-control (C&C) server(s). These usually are rented and placed at foreign countries where the law are not too tight that these servers would not be taken down when being discovered as a botnet C&C server or where it is cheap and easy to rent a server. Some popular places are United States, British Virgin Islands, Netherlands, Russia, Germany… [1].
- The C&C server addresses (IP address or domain name) are usually hardcoded in malware binary or configuration files. When the attacker wants to change the C&C, they will send an update to the zombies, which contains new C&C servers.
- Infected computers - zombies - are controlled directly via those C&C servers by receiving and executing various commands such as downloading and executing an executable files, which often are other malware, or sending spam emails, or starting a DoS attack…
- Some examples of these botnets are: Ramnit, Andromeda, Conficker…

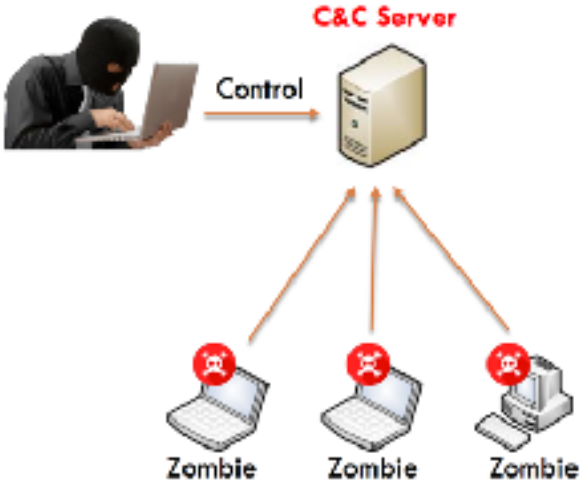

Figure 1. Client-server botnet network model.

The second type, called peer-to-peer botnet, has the following characteristics:

- Using peer-to-peer network to deliver commands. Each infected computer - bot - will receive commands from its neighbor and send them to others.
- Usually, there are two kinds of peer: master and slave. Master peers are those having

public IP address that can be connected to by other bots (for example: web servers, public service…). Meanwhile, slave peers are those only available to connect to master peers and cannot listen for other connections (for example: computers behind NAT). Slave peers would receive commands from their master peers list while master peers receive commands among them.

- Bot owner only own some master peers and control the whole network by spread commands via those ones.
- Some examples of these botnets are: ZeroAccess, Sality…

Figure 2. Peer-to-peer botnet network model.

Normally botnet takedown

There are some differences in taking down these two kinds of botnet above. To takedown a client-server botnet, we have to identify its C&C servers by analyzing malware samples, monitoring network… then we have to work with service providers, such as domain registrar or hosting provider to obtain those servers. Normally we will have to re-buy expired C&C domains or request for domain/hosting termination or transfer when they have not expired yet.

The disadvantages of this method is that we have to depend on service providers cooperation, which is not always ready to use. Furthermore, there is almost nothing we can do with bullet-proof domains/hostings, of which service providers do not care about such requests.

In case of peer-to-peer botnets, the takedown process is more complicated. The takedown process may be divided into five steps:

- Step 1: Join peer-to-peer botnet network by pretending to be a bot.
- Step 2: Identify owner's master peers by monitoring all master peers behaviors.
- Step 3: Pretend to be a master peer by emulating a master peer behavior.
- Step 4: Send commands to isolate owner's peers from network to prevent reinfection.
- Step 5: Send commands to every peer in the network to remove itself.

In the scope of this paper, I will discuss more about takedown client-server botnets, which is benefit from ISP advantages.

III. THE SOLUTION

Methodology

ISPs have many advantages in taking down client-server botnets:

- ISPs own the network Domain Name Server (DNS) system, which is required to resolve any C&C domain to IP address for bot to connect.
- ISPs can monitor and intercept any malicious traffic, an so response those with whatever they want.
- ISPs also have the ability to route any traffic to any destination to their desired

target regardless of the packet destination IP address.

In general, taking down a peer-to-peer botnet using ISP advantages could be described in these steps:

- Firstly, we need to redirect any C&C traffic to our analysis server. By doing this, we isolate the whole network from attacker control. He is now not able to send commands to infected machine inside ISP's network and of course cannot update those bots to use another C&C server. This analysis server is called sinkhole server.
- Secondly, we have to ensure that our sinkhole server working exactly the same as the real C&C server so we are able to control every bot in the network. This would be a huge advantage to clean those malware from infected computers.
- After taking control of the botnet, we send termination commands from our server to all bot in the network. This is doing continuously as newly infected machines connect to our sinkhole server.
- If customers accidentally browse to C&C address, which is actually pointed to our sinkhole server, they would see a notification about the sinkhole process explaining why they see that.

Target selection

In reality, there are hundreds of botnets and it will take plenty of time to sinkhole all of them. So, which botnet should be sinkholed first? The answer depends on each particular ISP. These are some hints on choosing botnets to sinkhole:

- Firstly, ISPs need to collect information about as many botnets as possible and identify their C&C server by analyzing malware samples or reading public report or event sharing information with other ISPs, researchers…
- Then, ISPs should do some analytics to identify which botnets are running in ISP network, which botnets have the largest number of customers infected. Those will be the botnets to be cared first.

After selecting the right botnet to sinkhole, we have to do a deep reverse engineering on botnet malware samples collected from every sources. Some good sources to collect malware samples are VirusTotal and online sharing databases such as malwr.com, virusshare.com…

The target of malware reversing is for not only identifying C&C domains/IPs but also more importantly, fully rebuild of bot protocol. Sometimes, we have to capture some real malicious traffic to verify our protocol analysis. Fully understanding botnet protocol help to make the sinkhole server working exactly the same as the real one, ensure that every bot would receive and execute commands from our server.

Sinkhole server

The hardest part of the server is to handle multiple protocols of multiple botnets or multiple versions of the same botnet on the same port, which means the server has to know how to distinguish a zombie of a specific botnet by the data receiving and treat it by the corresponding protocol. This is completely different between a sinkhole server and a real one. The real C&C server only has to serve one protocol version of a single botnet at a time, so it has not to worry about other versions or other botnets but simply drops every invalid packet that does not match its protocol.

Our solution is building the sinkhole server with the model similar to COM object, which means there is a main dispatcher responsible for

handling a connection and pass it to the plugins. Each plugin only handles a single protocol of a botnet version and refuses to serve if the input packet does not match its protocol.

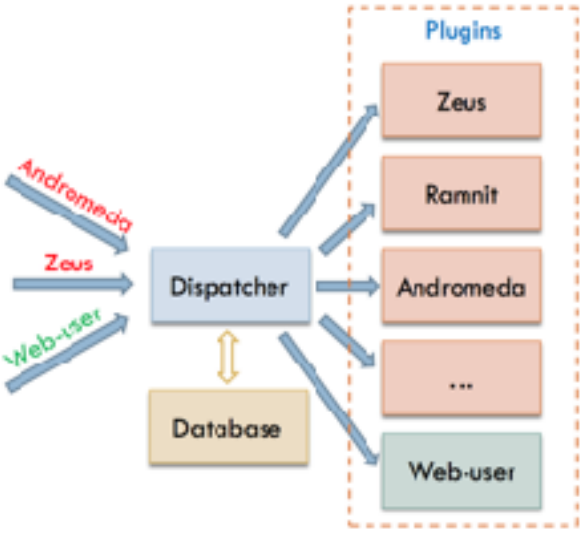

Figure 3. Sinkhole server diagram.

Each time the dispatcher receives a new connection, first packets will be passed to every plugin until one recognizes its protocol and return good result. From that on, the connection packet will only be forward to the corresponding plugin.

Moreover, the dispatcher also save every information of the botnet and zombies into database for further analysis such as statistics or reporting.

Command-and-control redirection

The most important part of the solution is C&C redirection, where the ISP power play a significant role. There are three scenarios which require ISP advantages to accomplish C&C redirection.

The first one is when a botnet uses domains in its bot configuration to connect to C&C server and the bots use default ISP DNS to resolve that domain. This is the simplest case where all the ISP has to do is to change the DNS records of C&C domains to the sinkhole server IP address, which can easily be achieved in DNS server configuration.

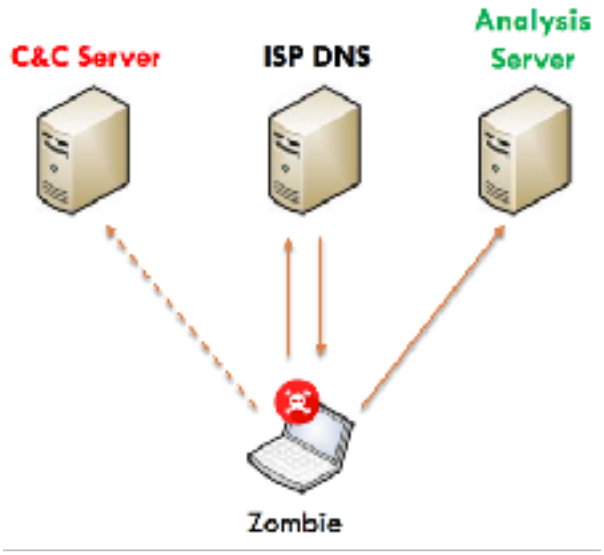

Figure 4. *C&C domain redirection using ISP DNS server.*

The second scenario is a bit more complicated when the botnet still uses domains but the zombies now use public DNS for resolution, such as Google DNS or OpenDNS… In this case, ISPs have to intercept DNS requests in their network, and response to them more quickly than other DNS servers. By doing this, the infected machines would accept ISP DNS response and using it as the result for their DNS request. Public DNS response, which come later, would be treated as junk packet and ignored.

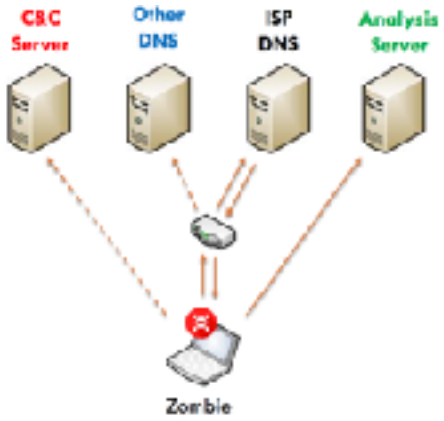

Figure 5. C&C domain redirection using early DNS response from ISP server.

The third also the most complicated scenario is when a botnet uses IP address as configuration for bots to connect to C&C server. In this case, ISPs have to do two steps to accomplish C&C redirection:

- Firstly, ISPs have to route the C&C IP address to sinkhole server, which could be done by configuration on ISP routers, which may be a large number of devices.
- Secondly, the sinkhole server has to have two difference network interfaces, one to receive connections from zombies then NAT it into the other to process. The response then is NAT back to the first interface to have the same source IP address as the destination address of the bot request.

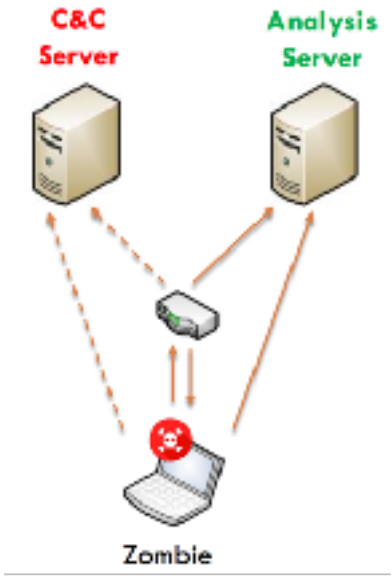

Figure 6. C&C IP redirection using routing and NAT technique.

After fully redirect all malicious traffic into the sinkhole server, ISPs now can simply send uninstall/termination command to connected bot to clean a specific botnet in theire network.

IV. RESULTS

We were successful in redirection and sinkhole of these botnets:

- **Ramnit**: 20.000 infected computers. This is a file virus which will infect every executable file on computer. It has been taken down once in 2015 by Europol [2] but restored and still running now.
- **Andromeda**: 100.000 infected computers. This is a quite simple botnet capable of download and execute other malware.
- **PlugX**: 200 infected computers. This is the most popular APT malware in Asia. It is used in almost every APT attack reported on Asia.

V. FUTURE WORK

Although this solution is helping ISPs effectively in taking down botnets in their network, but it is still having some limitations:

- At the moment, this solution is only support client-server botnet.
- The redirection process is still running manually, which is not really fast to response to redirection requests and may have mistake in configuration.
- The performance of the sinkhole server is not really high. Currently, it can handle only around 100.000 concurrent bots with a medium hardware configuration.

In the future, this solution would be upgrade to fulfill its limitations:

- Support for redirection and sinkhole of peer-to-peer botnets.
- Automatically redirect C&C domains/IPs to sinkhole server.
- Ability to horizontal expansion by using Load Balancing technology.

VI. CONCLUSION

Although the solution is still having some limitations, it is undenied that it helps ISPs a lot

in controlling and terminating client-server botnets in their network by themself, which is a lot easier than cooperating with dozens of hosting/domain providers all over the world.

Source code of the demo version of the sinkhole server can be downloaded from the following URL: https://github.com/piggybird.

REFERENCES

[1] McAfee, "Botnet Control Servers Span the Globe", *https://blogs.mcafee.com*, 2013.

[2] Europol, "Botnet taken down through international law enforcement cooperation", *https://www.europol.europa.eu*, 2015.