The First Zombie War

The US has declared war against botnets – one of the Internet's greatest threats, and for good reason. A special review by Dr. Gil David

Dr. Gil David

Last April, a cyber security convention took place in Virginia in the US. The convention saw the participation of the White House representative for cyber-security, where he announced for the first time that the US government is moving up a level in its fight against one of the most rapidly expanding cybernetic threats: botnets.

So far, the US has not had much of an active role in the fight against botnets and their operators. However, in light of recent revelations, which showed that more than four million computers are infected and join botnet virtual armies each month, the White House representative announced the US is declaring war against them.

The White House understands that we are in a critical stage in the war against botnets, and that if we don't act quickly, we may find ourselves dealing with virtual armies that consist of dozens and even hundreds of millions of infected computers in the next cyber war.

Botnets were once considered the exclusive domain of criminals on the internet, who used them for spam, identity theft, fraud, and theft of sensitive information such as passwords and credit card numbers. Today, experts understand that botnets will take part in the most lethal attacks against countries, essential facilities, and financial institutes in the not-so-distant future.

For example, an attack by millions of botnets against the US Stock Market could completely paralyze the US's financial center. A similar event has already occurred in the past: a coordinated cyber-attack took place in April 2007 against Estonia. The attack, in which several botnets were involved, was a Distributed Denial of Service (DDoS) attack. It resulted in the halting of the country's essential facilities – starting with government institutions, through financial institutions, and even newspapers and media websites. This cyber war, which according to assessments was carried out by Russia, provided a brief glimpse of the tremendous power of the botnet army and the ability to redirect it from traditional cybercrime to future cyber warfare.

What are botnets?

A botnet is a decentralized network of computers scattered throughout the world. The computers that are members of the network – the bots (also called "zombies") – are essentially computers of innocent users that are infected with malicious software such as Trojan horses. This software causes them to secretly join the ranks of the botnet network, without the awareness of the computer's legal user. While operating the computer unit in its regular manner, its legal user is unaware that his computer has been recruited to a digital army.

A bot herder, the virtual version of the traditional sheepherder, controls the collection of bots gathered from various places around the world. The bot herder's role is to organize the bots in its network, deliver orders to them, get field reports from them, and of course expand the botnet count by recruiting new virtual soldiers.

The bot herder has various methods for communicating with the bots. For example, it can create several "mother ships," which are essentially innocent-looking websites scattered in various places around the world that leave instructions for the bots. Such websites are also referred to as command and control servers, since the bot herder uses them to deliver commands and control the bots.

The bots (meaning the malicious software installed in them) automatically know that they need to surf to one of the mother ships and check if there are any pending instructions they must carry out, such as stealing passwords from the user's computer. They can also report back to the mother ship about the results of their activities, upload stolen information, and more.

In order to hurt botnet activity, one of the links that comprises the botnet army must be taken out: either the bots, the bot herder, or the intermediary through which the bot herder delivers its commands to the bots.

Since a botnet is comprised of tens of thousands and up to tens of millions of innocent computers, it is very difficult to locate all of them and remove the malicious code. These are computers that belong to users whose internet addresses constantly change, and whose location occasionally changes as well. Because of this, taking out the bots is virtually impossible.

In contrast, the bot herder is singular (or comprised of a small group of operators), which makes it a convenient target to locate. However, the bot herders are veteran internet foxes that know innumerable ways to preserve their anonymity, and thus prevent their detection. They move quickly, change identities, and hide in the darkest corners of the web.

Therefore, it seems that the most promising way of dismantling a botnet is to take over the bot herder's command and control server. For example, in the case of mother ships concealed in internet websites, they should be disconnected from the internet, so that no bot can access them and no bot herder can use them to communicate with its bots. Unfortunately, this is also hardly a simple task. First, the mother ships are usually scattered across different countries, some of which will not cooperate with whoever is trying to shut down the servers.

Second, the bot herders have developed very sophisticated methods that prevent the detection of the mother ships.

For example, they randomly use bots to serve as intermediaries between the rest of the botnet and the mother ship. In other words, no bot is accessed directly by the mother ship. Instead, each both is accessed through an intermediary bot that links it to the mother ship. In this manner, the real internet address of the mother ship is concealed behind the internet address of the intermediary bot, and no one can reach the real location of the mother ship. Furthermore, the bot herder makes sure to replace the intermediary bots with other bots in the network every few minutes. This effectively makes the mother ship a rapidly moving target that alternates between one end of the world and the other every few minutes, and makes locating the mother ship nearly impossible. Such a network is known as a "fast flux network." In the past, several botnets have successfully implemented this type of network, one of the most famous among them is known as "Storm."

Dealing with the botnets is a tough and complicated task that requires many resources as well as extensive cooperation between countries.

The following fascinating example will emphasize the complexity of the task: in 2009, a botnet was established in Russia named BredoLab. At its height, BredoLab had a virtual army consisting of approximately 30 million bots, with a recruitment rate of 3 million new bots each month. It dealt with the bot herder's most favorite activity – distributing billions of spam messages via email every day. The bot herder use to rent some of the bots in its network to third parties. In other words, the bot herder commanded an army of virtual soldiers comprised of different brigades that it marketed as a virtual army ready for hire to any interested party. Assessments estimate that the bot herder made hundreds of thousands of dollars each month this way while the mercenary army served different elements for a variety of targets, such as attacking internet websites, distributing malicious software, sending spam, and more.

The bot herder communicated with the botnet through a layout of over 140 mother ships, which were concealed in internet websites rented from a Dutch internet supplier. In 2010, when the botnet had grown to terrifying dimensions, a special Dutch police task force raided the facilities of the Dutch internet supplier, and succeeded in locating all of the docked mother ships, took control over them, and disconnected them from the internet.

At this stage, it seemed that BredoLab's fate had been sealed, as the bot herder's control channel had been destroyed. However, the bot herder employed several methods to regain control over the botnets. After all these methods failed, in a last move of desperation, the bot herder launched a decentralized attack against the Dutch supplier, which saw the participation of more than 200,000 bots. Several days later, BredoLab's chief bot herder was arrested in Armenia – a 27-year-old man named Georgy Avanesov, who was sentenced in May 2012 to four years in prison for committing severe computer crimes.

Seemingly, this was the end of one of the most dangerous botnets ever seen to date and its main operator. However, the story was not over. A new group of bot herders cleverly took control over what was left of BredoLab, established a new layout of mother ships in Russia and in Kazakhstan, and essentially brought at least part of the terrifying botnet network back to life, which is still in use today.

The US government's considerable concerns, as was made clear by the words of the White House representative, are completely justified. What was once the domain of mob organizations and criminals on the internet is now becoming a powerful tool in the hands of terrorists, guerrilla organizations, and even countries. These elements will use botnets not for spam or fraud purposes, but for cybernetic warfare purposes: powerful attacks against government institutions, financial institutions, military and intelligence entities, and critical infrastructures.

For example, attacks against banks and stock exchanges could result in the shutting down of a country's financial activities. Attacks against communication infrastructure could seriously harm a country's phone, cellular, and internet services. Attacks against transportation and electricity infrastructures could halt the movement of trains and blackout entire cities.

When an army consisting of dozens of bots from across the internet opens a prearranged frontal war against any infrastructure that is attached to the internet, it becomes very difficult to handle.

So how can we prepare for the zombie war?

As in any war, creative thinking can turn the tables around, and a serious threat such as botnets could actually become an advantage to the attacked country. Botnet armies can be tracked on the internet by investing in technology and intelligence resources. Once located, it becomes possible to learn their modus operandi, understand the way they communicate with the operator, examine the malicious software operator, and find weak spots that can be exploited.

From this point onwards, methods from the intelligence world can be used to advantage in the war against botnets. Duplicate bots can be deliberately planted in a botnet, for example. The botnet operator will think that his army has grown, when it actually contains spies that can report the botnet's movements and the intentions of its operator. Furthermore, instead of attempting to destroy botnets when locating an attacker's mother ship, it is possible to recruit the botnets to the defender's side without the attacker's knowledge. In this method, the defending side can use them to deliver instructions to the botnet at will. When the defending side gains control of the botnet without the operator's knowledge, it gains a tremendous advantage in the cybernetic campaign. When the operator of the virtual army begins an all-out cybernetic war, the defending side will be able to utilize its ruse and redirect the virtual army against the botnet operator (the attacking country or terror organization). Alternatively, the defending side can simply send an order that destroys the attacker's virtual army.

The understanding that these methods and others can improve the defense layouts of countries, while also strengthening their power in the cybernetic campaign, will result in the redirecting of vital resources for their implementation.

Dr. Gil David is the owner and CEO of Brainstorm Private Consulting, which deals in consulting for the cyber and intelligence world. He serves as a guest professor in a European university and cooperates with defense, commercial, and academic institutes in Israel and around the world.