

newsletter

Botnets

Security threat in the Internet

Botnets are a relatively new phenomenon on the Internet crime front. Experts see them as one of the biggest Internet security threats. Attacks using botnets are targeted and are generally intended to obtain confidential information or inflict financial damage on their victims.

Explanation terms

"Botnet" is short for "robot network". This is a remotely controlled network of computers that are linked via the Internet. A piece of software has been secretly installed on each computer that belongs to the botnet – generally without the knowledge of its user – by means of viruses or trojans. This software can then be used to control the computer remotely.

Computers usually become infected because security updates have not been installed and anti-virus programs or databases are out of date.

Systems (computers) that are connected to form a botnet are also sometimes referred to as "zombies". The computers in a botnet are controlled centrally and can be used for a wide range of cyber-crimes.

A botnet typically contains hundreds or even thousands of computers; in fact, networks consisting of hundreds of thousands of zombie systems have been observed. Enormous botnets of this kind have so many zombie systems under their control that they can bombard servers with a data load of several hundred Mbits per second. A massive data stream like this can cause significant problems for even the biggest Internet Service Providers (ISPs).

Background

At the start of February 2007 the root name servers of the Domain Name System (DNS), which are essential for communication via the Internet, were targeted in a sustained large-scale attack. For some years now attacks of this kind carried out by botnets have posed a serious threat, particularly to businesses that operate on the Internet. More and more frequently, network operators and ISPs are targeted by botnets, which carry out coordinated attacks with the intention of paralysing entire server networks. Several individuals who had constructed a botnet consisting of approx. 1.5 million computers were arrested in the Netherlands in 2005. Their intention had been to blackmail businesses in the US by threatening them with so-called "denial of service" (DoS) attacks. In mid-2004, for example, a botnet attack on the server network of webhoster Akamai brought down the websites of Apple, Google, Microsoft and Yahoo for more than two hours.

Botnets are the "multi-purpose tools" of computer crime and can be used for a multitude of criminal purposes. Botnets are also rented out to other criminals by their owners.

Possible uses of botnets

Botnets are most frequently used in the following ways:

- Denial of service attacks: Denial of service attacks have been a feature of the Internet for several years. These attacks are intended to paralyse network services (e.g. web or mail servers). To achieve this aim, the network connection of the target is bombarded with a large number of data packets. This eventually leads to an overload and may cause the system to collapse. The data load required to do this is generated with the help of a botnet.
(See: Distributed Denial of Service Attacks on the Internet, AssTech newsletter 2002).
- Blackmail: Companies that do business on the Internet – e.g. ISPs, online services or e-commerce providers – are threatened with a denial of service attack that will paralyse their systems unless they pay a ransom/protection money.
- Spam: Botnets are of central importance in today's spam industry. Botnets are used to send the spam e-mails from many different zombie systems. This makes it very difficult to locate the actual sender of the messages.
- Phishing: Botnets are very often used for phishing attacks – both for sending the fraudulent phishing e-mails and for hosting the illegal websites that are associated with them.

(See: Phishing – Security threat in the internet, AssTech newsletter 2005).

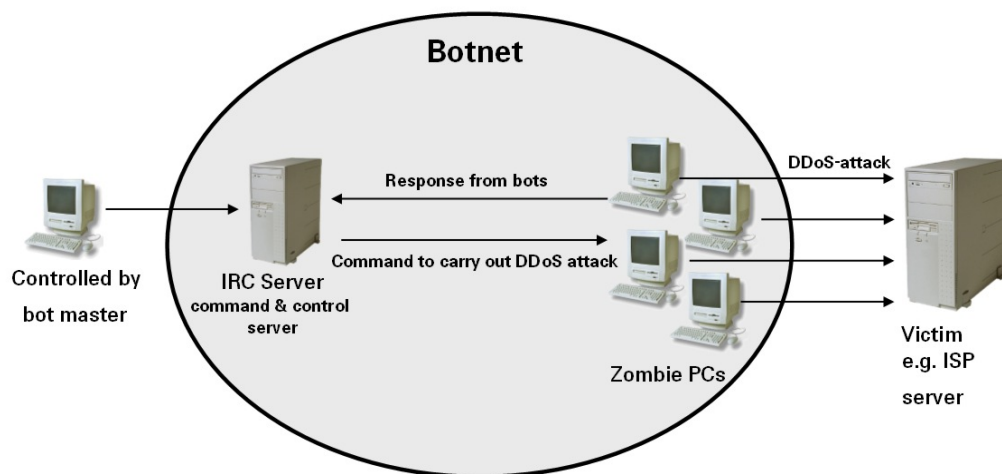


Illustration: Structure of a typical botnet with a central Internet Relay Chat (IRC) server which is controlled by a so-called bot master. In this example the botnet's zombie systems are carrying out a distributed denial of service (DDoS) attack.

Summary

Botnets are a core element in the commission of cyber crime. Through targeted attacks – or the threat of them – they illustrate the current trend away from hackers acting on their own to groups of well-organised criminal attackers. Precisely because the global economy is increasingly networked and digitalized and depends to an ever greater extent on the availability of IT systems, botnets – by dint of their very size and the fact that their shadowy operators are hard to identify – represent a threat that must be taken seriously.

Distributed denial of service (DDoS) attacks carried out using botnets represent a growing threat to companies whose business depends to a large extent on their Internet presence. Until now these attacks have usually targeted particular e-commerce providers and institutions. However, targeted attacks on the core elements of the Internet's infrastructure, leading to a large-scale commercial loss scenario, represent a massively more serious threat.

**Information for
the underwriter**

Overall, it is difficult to estimate the potential losses that could be caused by botnets because many attacks on businesses are not made public for image reasons. Because of the very high level of "attack resources", attacks carried out via botnets can represent a serious risk even for major companies that use the Internet as a business platform.

System downtime resulting from botnet attacks – e.g. denial of service attacks – can lead to financial losses that are not usually insured under standard property and liability covers. Special insurance products, which offer limited cover for IT and Internet risks including network downtime, have been developed for scenarios of this kind.

Inadequate protection of IT systems against unauthorised access makes it possible for these systems to be used as zombies in attacks on third parties. This can lead to liability claims by the injured parties against the operators of these systems.

A business interruption caused by a botnet attack – for example, as a result of the collapse of external networks – can lead to contingent losses (suppliers/customer extension). Here, too, risk assessment is of crucial importance, especially with regard to interfaces and dependencies on ISPs, hosters and carriers.

In the case of insurance concepts that cover business interruptions to IT systems without underlying material damage, there is exposure to accumulation losses due to attacks on the Internet infrastructure, particularly with regard to the failure of central infrastructure elements. This accumulation loss scenario is extremely difficult to control.

Contact

AssTech GmbH
Postfach 1211
85766 Unterföhring bei München
Telephone + 49 89 3844-1585
Telefax + 49 89 3844-1586
info@asstech.com
www.asstech.com