

WHITE PAPER

Malicious Intrusion Techniques

A Review of Rootkits, Bots, Trojan Horses,
and Remote Access Trojans (RATs)

Introduction

Memo to IT:

My PC has been experiencing some strange behavior and symptoms. The performance on my machine is very slow, the CD-ROM tray has opened and closed for no apparent reason, I get strange error messages and every once in a while, I get inverted images on my screen. There are times when my screen saver is on, I notice the disk access light flashes and the lights on my Internet hub are flashing like crazy.

I also can't seem to get my anti-virus software to work anymore.

Do I need a new PC?

The events described have become increasingly common, and indicate this PC has been compromised by software vulnerabilities or malware, which today affect millions computers on a daily basis. The terms used for these malicious intruders include Rootkits, Bots, Botnets, Trojans, Remote Access Trojans (RATs) and Scurrying RATs. Underground organizations such as "The Cult of the Dead Cow," with trendy software applications like "Back Orifice (BO2K)", "The Thing" and "SubSeven," have created sophisticated applications that include functionality for keystroke logging, registry editing, password detection, TCP/IP port redirection, and email messaging services to enable.

If a computer virus or email worm has ever infected your company, the PCs within your environment are prime candidates for further attacks. To protect your company, you should become familiar with these types of vulnerabilities, how they work, and how to detect and prevent these nuisances.

This White Paper examines the definitions of these vulnerabilities and some security measures that can be employed to protect your environment.

This White Paper examines the definitions of these vulnerabilities and some security measures that can be employed to protect your environment.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

What Are They?

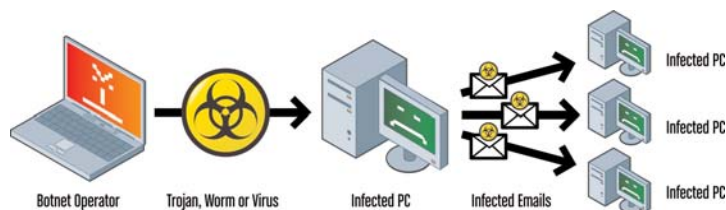
ROOTKITS

A Rootkit is software that can be installed and hidden on a computer without the knowledge of an end user. A Rootkit may be included in a larger software package as a subcomponent, or installed by an attacker who has been able to either take advantage of vulnerabilities on a computer or who has convinced an end user to download the file(s) via social engineering techniques. Rootkits are not necessarily malicious or destructive, but they may hide their activities by flying under the radar of the end user. Attackers may be able to access information, monitor user actions, modify programs, or perform other functions on the computer without being detected by the end user.

TROJAN HORSES

Trojans are similar to RootKits, in that software is installed on a PC without end user knowledge. The main difference is that Trojan horses can become more destructive in their nature. These are security-breaking programs that are disguised as benign attachments within an email, such as in a music file or other attachment, that once opened unleashes a dangerous program that can erase the computer's hard-disk, send credit cards numbers and/or passwords to the sender, or disable anti-virus software to enable further attacks. When the computer is hijacked it can be used to initiate further attacks by redistributing the malware to others via Instant Messaging, peer to peer file exchange or sent to email addresses harvested from the user address book with the Trojan attached within the email. The Trojan attack is meant to be "silent" and "hidden" in nature where the files are disguised by using multiple file extension techniques, or via Social Engineering tactics via offers for "smiley face" cursors, free games, movies, songs, etc. Victims typically download the Trojan from the WWW site, FTP site, or inside of an email attachment which they are tricked into clicking to open the file for installation. The silent nature of Trojans includes the installation of the program out of the view of the end user. In most cases, end users will remain unaware that their computers are launching attacks until they are told about them by other users.

When a network of owned PCs is created, it becomes a private remote-access network that the owner alone controls. If the network is "encrypted", only the owner can install or retrieve code from the owned PCs. Scale this up to 1,000, and you start getting botnets, invisible webs connecting unrelated, random "zombie" computers to individuals or groups who can control the data harvested off the linked computers or who can upload new software (such as keystroke loggers) onto those computers without the user's knowledge.



The Botnet operator harvests a new PC (victim) by distributing a Trojan, Worm or Virus. The infected PC attempts to re-distribute the affected files via email to their "friends and family" network.

A Rootkit is software that can be installed and hidden on a computer without the knowledge of an end user.

Trojans are similar to RootKits, in that software is installed on a PC without end user knowledge.

More Information:

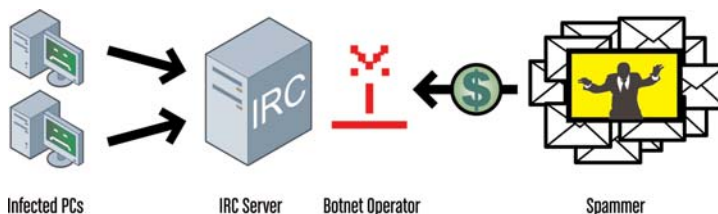
MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

REMOTE ACCESS TROJANS (RATS)

Remote Access Trojans (RATs) are "Trojans on steroids" that can change the security settings on a user's computer, expose communications ports for connectivity and bind or integrate with valid PC applications to remain undetected. RATs execute in a sophisticated client/server environment in the computer's background, which leaves the end user unaware of the unauthorized access. They mimic legitimate remote control programs, such as Symantec's pcAnywhere, but are specifically designed for stealth and the ability to cohabitate in the user's environment. A communication channel with standard encryption enables the installed RATs to be configured for logon passwords, scheduled modes of operations, where it is hidden and to create an email communications to the owner to report the successful take-over of the end user computer. The enhanced ability to create a communications channel over Internet Relay Channels (IRC) provides for immediate access of newly harvested machines.

IRC

Internet Relay Chat (IRC) is a program that lets anyone hold live keyboard conversations with people or computers around the world. It's a lot like an international CB radio and uses "channels" and "handles / nicknames". Type something on your computer and it's instantly echoed around the world to whoever happens to be on the same channel or to a Botnet computer that has been specifically configured to listen for command instructions. IRC is a protocol designed for real time chat communication (refer to RFC 1459, update RFC 2810, 2811, 2812, 2813), based on client-server architecture. Most IRC servers allow free access for everyone. IRC is an open network protocol based on Transmission Control Protocol (TCP), which is sometimes enhanced with Secure Sockets Layer (SSL) encryption.



The harvested PCs connect to the IRC server to report successful takeover and await instructions. A spammer purchases access to the Botnet from the operator.

Remote Access Trojans (RATs) are "Trojans on steroids" that can change the security settings on a user's computer, expose ommunications ports for connectivity and bind or integrate with valid PC applications to remain undetected.

Internet Relay Chat (IRC) is a program that lets anyone hold live keyboard conversations with people or computers around the world.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

BOTNETS

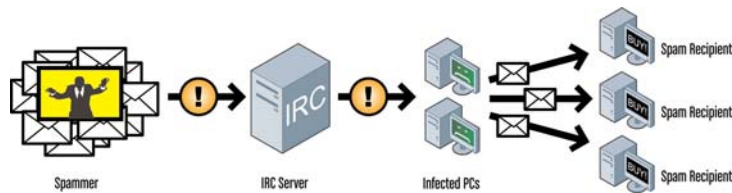
A botnet (derived from robot + network, and also known as a zombie army) is a group of Internet computers that are set up, without the owner's knowledge, to forward transmissions (spam, viruses, Trojans) to other computers on the Internet. In its most basic form, a bot is simply an automated computer program, or robot, that performs tasks directed from an external source. In the context of botnets, bots refer to computers that are controlled by one, or many, outside sources.

GT-Bot: All Global Threat (GT) bots are based on a popular IRC client for Windows called mIRC. The core of these bots is made up of a set of mIRC scripts, which are used to control the activity of the remote system. This type of bot launches an instance of the client enhanced with control scripts and uses a second application, usually HideWindow, to make mIRC invisible to the user of the host computer. An additional DLL file adds new features to mIRC in order for scripts to be able to influence various aspects of the controlled host.

Agobot: An Agobot is one of the most popular bots, and is written in C++ and released on a General Public License (GPL). What's interesting about Agobots are their source code, which is highly modular, making it simple to add new functions. An Agobot provides many mechanisms to hide its presence on the host computer, including NTFS Alternate Data Stream, Antivirus Killer and the Polymorphic Encryptor Engine. Agobots offer traffic sniffing and sorting functionality, and protocols other than IRC can also be used to control this bot.

DSNX: The Datsapy Network X (DSNX) bot is also written in C++ and its source code is also available on a GPL license. Adding new functionality to this bot is very easy thanks to its simple plug-in architecture.

SDBot: SDBot is written in C and also available on a GPL license. Unlike an Agobot, its code is not very clear and the software itself comes with a limited set of features. Nevertheless, it is still very popular and available in different variants.



The spammer takes control of the Botnet, sending instructions to the harvested PCs via the IRC. The harvested PCs become mass mailing spammers sending junk mail or hyper-link for Phishing sites for the capture of sensitive information.

Botnet is derived from robot + network, and is also known as a zombie army.

GT-Bot, Agobot, DSNX, and SDBot are all types of botnets – automated computer programs that perform tasks directed from an external source.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

What can they do?

DENIAL-OF-SERVICE (DOS)

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the infected computer.

The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. For instance, when a URL for a particular website is typed into a browser, the computer sends a request to the site's computer server to view the requested page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site.

An attacker can use spam email messages to launch a similar attack on a particular email server or on a particular email account. The attack on an email server can be accomplished by combining random email address to a specific domain and creating a scenario where the email server becomes overloaded and can't respond to normal email requests. By sending many, or large, email messages to the account, an attacker can consume a pre-configured quota, preventing the account owner from receiving legitimate messages.

DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

In a distributed denial-of-service (DDoS) attack, an attacker can take advantage of security vulnerabilities to take control of a computer to attack another computer. The attacker can also force a computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers to launch the denial-of-service attack.

SPAMMING

Spam continues to be a common threat from these zombie networks. The creation of a Windows Sockets (SOCKS) proxy protocol for TCP/IP can enable most computers to be configured for Simple Mail Protocol Support (SMTP). Using the botnet, attackers can send massive amounts of bulk, unsolicited email to unsuspecting recipients. In most instances, the junk spam email circulating the Internet is coming from an old compromised Windows computer that is under command of the bot owner.

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services.

In a distributed denial-of-service (DDoS) attack, an attacker can take advantage of security vulnerabilities to take control of a computer to attack another computer.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

SNIFFING TRAFFIC

The use of packet sniffer to watch for clear-text data passing through a compromised machine can detect sensitive information like usernames and passwords. Of greater use to the owner of these networks is the ability to retrieve other information that may contain intellectual property, including personal information and even credit card information. The interesting point is that traffic sniffing is being used to detect other bot or botnets and gather information which could be used to "steal" the already configured botnets.

KEYLOGGING

Sniffing encrypted communications from compromised machines is useless since the appropriate key to decrypt the packets is missing. Bots can be configured to resolve this situation by capturing keystrokes to gather sensitive information. Sophisticated bots can assist with the capture of keystrokes for pre-defined situations (i.e. "interested in key sequences near the keyword 'www.bank.com'"), which can be used to gather login information and passwords for access to bank accounts.

SPREADING "NEW" MALWARE

In almost all cases, botnets under control of a bot owner are used to spread the infection to new bots. An end user who downloads the "special" music file, becomes part of a botnet that can be used to open a SOCKS proxy and email the "special" music file to the end user's entire address book. A botnet with thousands of infected hosts can also be used to distribute newly-created viruses, creating a fast spreading infection.

INSTALLING ADVERTISEMENT ADD-ONS AND BROWSER HELPER OBJECTS (BHO'S)

Botnets can also be used for financial gain. For instance, a botnet owner sets up a bogus website with advertisements, and then establishes a relationship with companies that pay for clicks on ads. The botnet automates these clicks from the harvested machines and instantly generates thousands of clicks. This process can further be enhanced by using RATs to bind to a victim's browser that executes clicks every time the browser is activated.

CONTROLLING ONLINE POLLS AND GAMES

Online polls and games can be rather easy to manipulate with botnets. The majority of online polls have been established to give the "right" to vote to unique visitors. Since every bot will have a distinct IP address and a unique name, a community of bots will have the same credibility as "real" users. Online games can be affected in a similar manner.

Botnets can also be used for financial gain. For instance, a botnet owner sets up a bogus website with advertisements, and then establishes a relationship with companies that pay for clicks on ads.

The combination of the different functions described above can be used for large-scale identify theft, which is one of the fastest growing for-profit crimes on the Internet.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

MASS IDENTITY THEFT

The combination of the different functions described above can be used for large-scale identity theft, which is one of the fastest growing for-profit crimes on the Internet. Bogus emails ("phishing") that appear to be from legitimate companies direct their intended victims to go online and submit sensitive, private information. These fake emails are generated and sent by bots via their email spamming mechanisms. These same bots can also host multiple fake websites, which appear to represent legitimate companies. The private information collected on fake websites is sold to criminals. Often, these sites are taken down just as quickly as these sites are set up, protecting the botnet for a later day, when they are configured to capture information "for" another legitimate company.

How Can I Avoid Getting Infected?

You must always be certain of the Source and the Content of each file you download and the email you open.

- IMPLEMENT a layered security approach for your company. Using anti-spam and anti-virus solutions either before or at your gateway will increase the security for your company.
- IMPLEMENT a Firewall Solution. Firewalls may be able to prevent some types of infection by blocking malicious traffic before it can enter the network.
- USE "strong" passwords. Select passwords that will be difficult for attackers to guess and use different passwords for different applications.
- DO NOT choose options that allow your computer to remember your passwords.
- KEEP your software up to date. Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. Enable these updates and have them installed periodically.
- NEVER download blindly from people or sites that you do not know or cannot trust. Insure that the website you are visiting is the actual site.
- INSURE that your anti-virus software is active and is up-to-date.
- DON'T be lulled into a false sense of security just because you have anti-virus software. In some cases, the anti-virus software cannot accurately detect viruses and Trojans.

You must always be certain of the Source and the Content of each file you download and the email you open.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

- BE CAUTIOUS, If the file comes from a "friend", make sure you know what the file contains before opening the file. As discussed, an infected machine will attempt to propagate to other "friends."
- BEWARE of hidden file extensions. Implement techniques to validate the appropriate S Mime and Mime structures of attached files.
- FOLLOW good security practices. Take appropriate precautions when using email and web browser to reduce the risk that your actions will trigger an infection.

ABOUT MX LOGIC

MX Logic Inc. provides innovative, easy-to-use email defense solutions to businesses of all sizes. Processing billions of messages each month for over 8,300 organizations worldwide, MX Logic distributes its email security and protection solutions directly and through an extensive partner network. For more information, visit www.mxlogic.com.

Processing billions of messages each month for over 8,300 organizations worldwide, MX Logic distributes its email security and protection solutions directly and through an extensive partner network. For more information, visit www.mxlogic.com.