
The corporate threat posed by email Trojans

How to protect your network against Trojans

Describing what Trojans are and why they pose a danger to corporate networks, this paper discusses the need and method to protect your network from the threat of Trojans.

Introduction

This white paper outlines what Trojans are and why they pose a danger to corporate networks. As early as 2001, an eWeek article reported that tens of thousands of machines are infected with Trojans. And this is fast on the rise (InternetWeek.com, January 2004). The alarming fact is that Trojans can be used to steal credit card information, passwords, and other sensitive information, or to launch an electronic attack against your organization. The white paper discusses the need for a Trojan and executable scanner at mail server level in addition to a virus scanner, to combat this threat.

Introduction.....	2
What the attacker looks for.....	2
Different types of Trojans	3
How can I get infected?.....	5
How to protect your network from Trojans	6
Malicious executable analysis - Trojan and executable scanner	7
Gateway protection.....	8
About GFI	9

What is a Trojan horse?

In the IT world, a Trojan horse is used to enter a victim's computer undetected, granting the attacker unrestricted access to the data stored on that computer and causing great damage to the victim. A Trojan can be a hidden program that runs on your computer without your knowledge, or it can be 'wrapped' into a legitimate program meaning that this program may therefore have hidden functions that you are not aware of. (For a quick look at how Trojans work, please visit <http://kbase.gfi.com/showarticle.asp?id=KBID001671>).

What the attacker looks for

Trojans can be used to siphon off confidential information or to create damage. Within the network context, a Trojan is most likely to be used for spying and stealing private and sensitive information (industrial espionage). The attacker's interests could include but are not limited to:

- Credit card information (often used for domain registration or shopping sprees)
- Any accounting data (email passwords, dial-up passwords, Web services passwords, etc)
- Confidential documents
- Email addresses (for example, customer contact details)
- Confidential designs or pictures
- Calendar information regarding the user's whereabouts
- Using your computer for illegal purposes, such as to hack, scan, flood or infiltrate other machines on the network or Internet.

Different types of Trojans

There are many different types of Trojans, which can be grouped into seven main categories. Note, however, that it is usually difficult to classify a Trojan into a single grouping as Trojans often have traits which would place them in multiple categories. The categories below outline the main functions that a Trojan may have.

Remote access Trojans

These are probably the most publicized Trojans, because they provide the attacker with total control of the victim's machine. Examples are the Back Orifice and Netbus Trojans. The idea behind them is to give the attacker COMPLETE access to someone's machine, and therefore full access to files, private conversations, accounting data, etc.

The Bugbear virus that hit the Internet in September 2002, for instance, installed a Trojan horse on the victims' machines that could give the remote attacker access to sensitive data.

Traditionally, Trojans acted as a server and listened on a port that had to be available to Internet attackers. Attackers can now also make use of a reverse connection to reach the backdoored host so that they can reach the server even when it is behind a firewall. Some Trojans can also automatically connect to IRC and can be controlled through IRC commands almost anonymously, without the attacker and the victim ever making a real TCP/IP connection.

Data-sending Trojans (passwords, keystrokes etc.)

The purpose of these Trojans is to send data back to the hacker with information such as passwords (ICQ, IRC, FTP, HTTP) or confidential information such as credit card details, chat logs, address lists, etc. The Trojan could look for specific information in particular locations or it could install a key-logger and simply send all recorded keystrokes to the hacker (who in turn can extract the passwords from that data).

An example of this is the Badtrans.B email virus (released in the wild in December 2001) that could log users' keystrokes.

Captured data can be sent back to the attacker's email address, which in most cases is located at some free web-based email provider. Alternatively, captured data can be sent by connecting to a hacker's website - probably using a free web page provider - and submitting data via a web-form. Both methods would go unnoticed and can be done from any machine on your network with Internet and email access.

Both internal and external hackers can use data-sending Trojans to gain access to confidential information about your company.

Destructive Trojans

The only function of these Trojans is to destroy and delete files. This makes them very simple

to use. They can automatically delete all the core system files (for example, .dll, .ini or .exe files, and possibly others) on your machine. The Trojan can either be activated by the attacker or can work like a logic bomb that starts on a specific day and time.

A destructive Trojan is a danger to any computer network. In many ways, it is similar to a virus, but the destructive Trojan has been created purposely to attack you, and therefore is unlikely to be detected by your anti-virus software.

Denial of service (DoS) attack Trojans

These Trojans give the attacker the power to start a distributed denial of service (DDoS) attack if there are enough victims. The main idea is that if you have 200 infected ADSL users and you attack the victim simultaneously from each, this will generate HEAVY traffic (more than the victim's bandwidth can carry, in most cases), causing its access to the Internet to shut down.

WinTrinoo is a DDoS tool that has recently become very popular; through it, an attacker who has infected many ADSL users can cause major Internet sites to shut down; early examples of this date back to February 2000, when a number of prominent e-commerce sites such as Amazon, CNN, E*Trade, Yahoo and eBay were attacked.

Another variation of a DoS Trojan is the mail-bomb Trojan, where the main aim is to infect as many machines as possible and simultaneously attack specific email address/addresses with random subjects and contents that cannot be filtered.

Again, a DoS Trojan is similar to a virus, but the DoS Trojan can be created purposely to attack you, and therefore is unlikely to be detected by your anti-virus software.

Proxy Trojans

These Trojans turn the victim's computer into a proxy server, making it available to the whole world or to the attacker alone. It is used for anonymous Telnet, ICQ, IRC, etc., to make purchases with stolen credit cards, and for other such illegal activities. This gives the attacker complete anonymity and the opportunity to do everything from YOUR computer, including the possibility to launch attacks from your network.

If the attacker's activities are detected and tracked, however, the trail leads back to you not to the attacker - which could bring your organization into legal trouble. Strictly speaking, you are responsible for your network and for any attacks launched from it.

FTP Trojans

These Trojans open an FTP server on the victim's machine that might store and serve illegal software and/or sensitive data, and allow attackers to connect to your machine via FTP.

Security software disablers

These are special Trojans, designed to stop/kill programs such as anti-virus software, firewalls,

etc. Once these programs are disabled, the hacker is able to attack your machine more easily.

The Bugbear virus installed a Trojan on the machines of all infected users and was capable of disabling popular anti-virus and firewalls software. The destructive Goner worm (December 2001) is another virus that included a Trojan program that deleted anti-virus files.

Security software disablers are usually targeted at particular end-user software such as personal firewalls, and are therefore less applicable to a corporate environment.

How can I get infected?

For a network user who is protected by a firewall and whose ICQ and IRC connections are disabled, infection will mostly occur via an email attachment or through a software download from a website.

Many users claim never to open an attachment or to download software from an unknown website, however clever social engineering techniques used by hackers can trick most users into running the infected attachment or downloading the malicious software without even suspecting a thing.

An example of a Trojan that made use of social engineering was the Septer.troj, which was transmitted via email in October 2001. This was disguised as a donation form for the American Red Cross's disaster relief efforts and required recipients to complete a form, including their credit card details. The Trojan then encrypted these details and sent them to the attacker's website.

Infection via attachments

It is amazing how many people are infected by running an attachment that has been sent to their mailbox. Imagine the following scenario: The person targeting you knows you have a friend named Alex and also knows Alex's email address. The attacker disguises a Trojan as interesting content, for example, a Flash-based joke, and emails it to you in your friend's name. To do so, the attacker uses some relaying mail server to falsify the email's FROM field and make it look like Alex is the sender: Alex's email address is alex@example.com so the attacker's FROM field is changed to alex@example.com. You check your mail, see that Alex has sent you an attachment containing a joke, and run it without even thinking that it might be a malicious "because, hey, Alex wouldn't do something like that, he's my friend!"

Information is power: Just because the attacker knew you had a friend Alex, and knew and guessed that you would like a joke, he succeeded in infecting your machine!

Various scenarios are possible. The point is that it only takes ONE network user to get your network infected.

In addition, if you are not running email security software that can detect certain exploits, then

attachments could even run automatically, meaning that a hacker can infect a system by simply sending you the Trojan as an attachment, without any intervention on a user's part.

Infection by downloading files from a website

Trojans can also be distributed via a website. A user can receive an email with a link to an interesting site, for instance. The user visits the site, downloads some file that he thinks he needs or wants, and without his knowing, a Trojan is installed and ready to be used by attacker. A recent example is the ZeroPopUp Trojan, which was disseminated via a spam broadcast and enticed users to download the Trojan, describing it as a product that would block pop-up ads. Once installed, the Trojan would send a mail to everybody in the infected user's address book promoting the ZeroPopUp URL and software. As this email is sent from a friend or colleague, one is more likely to check out the URL and download the software.

In addition, there are thousands of "hacking/security" archives on free web space providers like Xoom, Tripod, Geocities and several others. Such archives are full of hacking programs, scanners, mail-bombers, flooders and various other tools. Often several of these programs are infected by the person who created the site. Again, a single network user could infect your whole network.

In January 2003, TruSecure, the risk management firm that also owns ICSA Labs and InfoSecurity Magazine, warned that malware code writers will increasingly disguise remote access Trojans as 'adult' entertainment, for example, and post these programs to pornography sites or news groups, to target new users. Specific users will also be targeted in this way, as the attacker can then send the URL containing the disguised malware to an unsuspecting victim.

On similar lines, the Migmaf or "migrant Mafia" Trojan that emerged in July 2003 hijacked about 2,000 Windows-based PCs with high-speed Internet connections, allowing them to be used to send ads for pornography. The Migmaf Trojan turns the victim computer into a proxy server which serves as a sort of middleman between people clicking on porn email spam or website links - it allowed the victim computer to fetch porn web ads from an undisclosed server and pass on the ads to other computers either through a spam mail or a web browser.

How to protect your network from Trojans

So how do you protect your network from Trojans? A common misconception is that anti-virus software offers all the protection you need. The truth is anti-virus software offers only limited protection. Anti-virus software recognizes only a portion of all known Trojans and does not recognize unknown Trojans.

Although most virus scanners detect a number of public/known Trojans, they are unable to scan UNKNOWN Trojans. This is because anti-virus software relies mainly on recognizing the "signatures" of each Trojan. Yet, because the source code of many Trojans is easily available,

a more advanced hacker can create a new version of that Trojan, the signature of which NO anti-virus scanner will have.

If the person planning to attack you finds out what anti-virus software you use, for example through the automatic disclaimer added to outgoing emails by some anti-virus engines, he will then create a Trojan specifically to bypass your virus scanner engine.

Apart from failing to detect unknown Trojans, virus scanners do not detect all known Trojans either - most virus vendors do not actively seek new Trojans and research has shown that virus engines each detect a particular set of Trojans. To detect a larger percentage of known Trojans, you need to deploy multiple virus scanners; this would dramatically increase the percentage of known Trojans caught.

To effectively protect your network against Trojans, you must follow a multi-level security strategy:

1. You need to implement gateway virus scanning and content checking at the perimeter of your network for email, HTTP and FTP - It is no good having email anti-virus protection, if a user can download a Trojan from a website and infect your network.
2. You need to implement multiple virus engines at the gateway - Although a good virus engine usually detects all known viruses, it is a fact that multiple virus engines jointly recognize many more known Trojans than a single engine.
3. You need to quarantine/check executables entering your network via email and web/FTP at the gateway. You have to analyze what the executable might do.

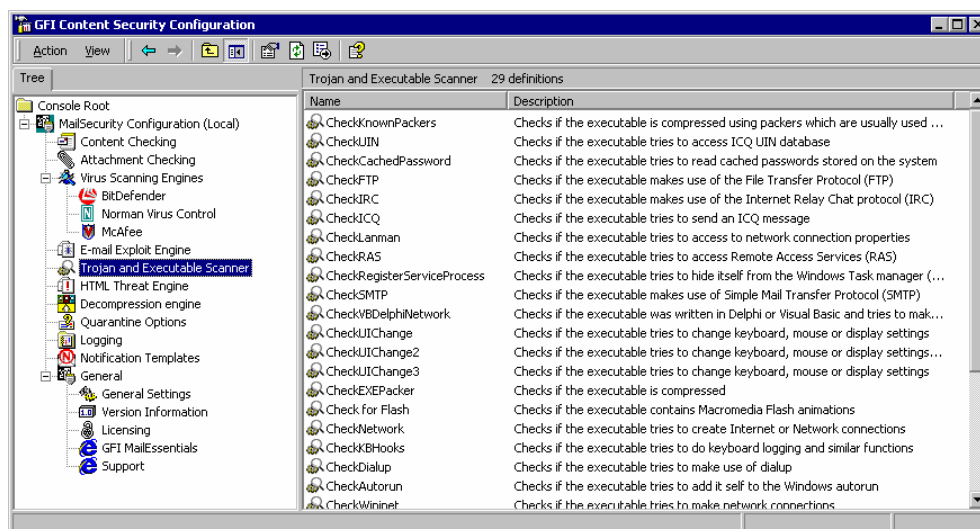
Fortunately, there are tools available that will automate a large part of this process.

Malicious executable analysis - Trojan and executable scanner

Detecting unknown Trojans can only be done by manually reviewing the executable, or by using a Trojan and executable scanner.

The process of manually reviewing executables is a tedious and time-intensive job, and can be subject to human error. Therefore it is necessary to tackle this process intelligently and automate part of it. This is the purpose of a Trojan and executable analyzer.

An executable scanner intelligently analyses what an executable does and assigns a risk level. It disassembles the executable and detects in real time what the executable might do. It compares these actions to a database of malicious actions and then rates the risk level of the executable. This way, potentially dangerous, unknown or one-off Trojans can be detected. The Trojan and executable scanner deals with advanced hackers who create their own versions of Trojans, the signatures of which are not known by anti-virus software.



The Trojan executable scanner configuration

Gateway protection, together with multiple anti-virus engines AND a Trojan and executable scanner will guard your network from the dangerous effects of Trojans.

Gateway protection

Two products that offer gateway protection that includes multiple virus engines and a Trojan and executable scanner, as well as other security features are:

GFI MailSecurity for Exchange/SMTP is an email content checking, exploit detection, Trojan and executable scanning, threats analysis and anti-virus solution that removes all types of email-borne threats before they can affect your email users. GFI MailSecurity's key features include multiple virus engines, for virus engine independence and better security; email content and attachment checking, to quarantine dangerous attachments and content; an exploit shield, to detect emails with OS and application exploits; an HTML threats engine, to disable HTML scripts; and a Trojan & Executable Scanner, to detect potentially malicious executables. Read more and download a trial version at <http://www.gfi.com/mailsecurity/>.

GFI DownloadSecurity for ISA Server enables you to assert control over what files your users download from HTTP and FTP sites. Downloaded files are content checked for malicious content, viruses, and Trojans and can be quarantined based on file type and user. GFI DownloadSecurity handles the security risk of file downloads without resorting to blocking all file downloads at firewall level. Read more and download a trial version at <http://www.gfi.com/dsec/>.

About GFI

GFI is a leading provider of network security, content security and messaging software. Key products include the GFI FAXmaker fax connector for Exchange and fax server for networks; GFI MailSecurity email content/exploit checking and anti-virus software; GFI MailEssentials server-based anti-spam software; GFI LANguard Network Security Scanner (N.S.S.) security scanning and patch management software; GFI Network Server Monitor that automatically sends alerts, and corrects network and server issues; GFI LANguard Security Event Log Monitor (S.E.L.M.) that performs event log based intrusion detection and network-wide event log management; and GFI LANguard Portable Storage Control that enables network-wide control of removable media. Clients include Microsoft, Telstra, Time Warner Cable, Shell Oil Lubricants, NASA, DHL, Caterpillar, BMW, the US IRS, and the USAF. GFI has offices in the US, the UK, Germany, Cyprus, Romania, Australia and Malta, and operates through a worldwide network of distributors. GFI is a Microsoft Gold Certified Partner and has won the Microsoft Fusion (GEM) Packaged Application Partner of the Year award. For more information about GFI, visit <http://www.gfi.com>.

© 2005 GFI Software Ltd. All rights reserved. The information contained in this document represents the current view of GFI on the issues discussed as of the date of publication. Because GFI must respond to changing market conditions, it should not be interpreted to be a commitment on the part of GFI, and GFI cannot guarantee the accuracy of any information presented after the date of publication. This White Paper is for informational purposes only. GFI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. GFI, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI LANguard, GFI Network Server Monitor, GFI DownloadSecurity and their product logos are either registered trademarks or trademarks of GFI Software Ltd. in the United States and/or other countries. All product or company names mentioned herein may be the trademarks of their respective owners.

