ARHONT
ANSWERS TO INFORMATION SECURITY CHALLENGES

Viruses, Worms and Trojans

What they are and how to counter them.

The terms

They cause inconvenience, damage and potentially can ruin your network or even destroy your business. The first step to dealing with them is to understand the basic terms:

Malware: Malware is a common term to define all kinds of malicious software including viruses, worms and trojans.

Worm: A worm is a program that propagates from machine to machine by exploiting holes in a software that computers run. The propagation of worms is self-sufficient, thus, you don't have to click on the malicious file to get your machine infected. Many worms spread by exploiting running vulnerable services, such as web servers. Usually this is completely transparent for end users.

Virus: A virus is a program that makes multiple copies of itself and infects other programs.

Trojan: A trojan is a program that pretends to be harmless and needs to be clicked on in order to become activated. Binders are programs used to merge trojans with legitimate software to hide the trojan. When the resulting merged file is run, the legitimate program works as intended, but the machine is infected behind the scenes. Trojans do not spread by themselves, they are spread by crackers (malicious hackers) to gain access to the infected machines. A cracker can also install a trojan on a computer he broke into in order to preserve an access to that machine after logout and reboot.

Keylogger: A keystroke logger, or simply keylogger, is a malicious program that logs every pressed key into a hidden file that can be retrieved later. Keyloggers are frequently used to steal online banking data. Many sophisticated trojans and some worms / viruses include a keylogger functionality.

Spyware: This group of software is installed on users machines when browsing certain commercial websites. Spyware monitors which sites you visit to report your preferences to firms using it and bombards you with annoying advertisement pop-ups. While using spyware violates personal privacy, it is still legal and very common. Even though spyware does not damage your computer or grants remote access to it, other types of malware can piggyback on the top of it leading to the complete system compromise.

Ransomware: The latest wave of malware used by cybercrime groups for mass money extortion. It locks the infected computers or data, and demands money transfers (usually via Western Union) to criminals to unlock it. Ransomware can also threaten users with data deletion or corruption.

Modern malware is getting exceedingly complex and often combines characteristics of many malware types. The cases of complex malware granting remote access to cybercriminals, stealing all kinds of login credentials, launching automated attacks against other sites, and spreading SPAM are now an everyday routine

How to counter them

You can never achieve perfect security, and the majority of systems will be attacked. However, you can significantly reduce the vulnerability of your systems to attacks. It need not cost you a lot, and it is thought and preparation that are more important than equipment. The countermeasures against malware can be split into administrative/educational and technical.

The first category includes things you shouldn't do and/or must enforce among other users in your company via a correctly written security policy:

- Do not open any unknown attachments in e-mails. In fact be very careful about opening e-mails from complete strangers. Filter out SPAM.
- Do not download and install free or trial third party software unless absolutely necessary. Even if it sounds a good idea, stick to the software that gets your job done.
- Do not click OK on multiple banners and advertisement pop-ups at various websites and never download the files some websites automatically offer.
- Do not use instant messengers and peer-to-peer networks in working environment.
- Do not allow other employees to bring and use memory sticks and CD's from home. The same applies to plugging employees laptops and palmtops into the company computers or network.
- Make sure that various components of your systems, from services to the word processor and browser, are regularly updated to the latest available versions.
- Ensure that everyone in the company is aware of these limitations and suggestions. The company should have a well known and adhered to security policy.

The second category is related to selecting, installing and maintaining an antivirus. It is very important to apply these updates in a timely basis. With the current rate of new malware release, the antivirus signature database should be updated at least on a daily basis. Make sure that the protected computers are up and on-line when an automated antivirus update scheduled to takes place.

A separate issue is host-based vs. server/gateway-based centralised antivirus installation. A company with sufficient resources can afford having both, however many SME's might find such setup too costly to maintain. Very often, centralised antivirus protection can save cash. For a network larger than 10 computers, centralised malware filtering is clearly financially beneficial. It is much easier and cheaper to install and update a single server/gateway antivirus, rather than keep an eye on multiple end-user workstations. To add more benefits, a hardened, virus-proof operating system such as Linux or BSD, can be used on a virus-filtering server to make the main redoubt invulnerable to common virus and worm attacks.

Traditionally, centralised server-based antiviruses only filter the incoming and outgoing e-mail. However, the server hard drive can be shared between the employees as a file storage with every file being constantly checked on the subject of malware presence. Also, a web proxy can be installed and integrated with an antivirus to filter and disinfect all bypassing web traffic. Deploying such server can save you from a lot of trouble, and help you to avoid significant losses due to data exposure and loss, system damage and downtime, lost working hours and system repair costs. It is likely, that the indoors experience of your company would not be sufficient and the server/gateway design and installation will have to be outsourced to a specialist IT security firm.

The disadvantages of centralised malware protection include a difficulty in checking encrypted e-mails and web traffic, and a possibility of “out-of-band” infection by users bringing in memory sticks or connecting personal laptops etc. to company's network. The first problem can be sorted by decrypting and storing e-mails on a shared and protected server hard drive, while the second problem is removed administratively. Should the explicit need for such action arise, all brought memory sticks, CD's and computers of any size and shape must undergo a thorough antivirus check before the “contact” with the network.

Conclusion

The damage that can be done to a company by malware infections increases hugely while the Internet malware epidemics are on the rise, and malware capabilities and complexity evolve. On the up side, good security has little to do with cost, and some of the most insecure institutions might be those that spend the most on IT defences (we cannot give you the names for legal reasons). The secret is understanding the threat, effective spending to mitigate it, and making sure that all potential weak points are secured.

Dr. Andrew Vladimirov
Arhont Information Security