



About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

e-mail: Isabella Santa, Senior Expert Awareness Raising — awareness@enisa.europa.eu

Internet: <http://www.enisa.europa.eu/>

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2010



Malicious software: *Train the trainer reference guide*

February 2010

Contents

ABOUT ENISA	2
CONTENTS	4
EXECUTIVE SUMMARY	5
HOW TO USE THIS MANUAL	6
STRUCTURE OF THE MANUAL	6
STRUCTURE OF THE PRESENTATION PAGES	6
THE PRESENTATIONS SLIDES	7
SLIDE 1	7
SLIDE 2	8
SLIDE 3	9
SLIDE 4	10
SLIDE 5	11
SLIDE 6	12
SLIDE 7	14
SLIDE 8	16
SLIDE 9	17
SLIDE 10.....	18
SLIDE 11.....	19
SLIDE 12.....	21
SLIDE 13.....	22
SLIDE 14.....	24
SLIDE 15.....	25
SLIDE 16.....	26
SLIDE 17.....	27
SLIDE 18.....	29
SLIDE 19.....	30
SLIDE 20.....	31
SLIDE 21.....	32
SLIDE 22.....	34
SLIDE 23.....	35
SLIDE 24.....	36
SLIDE 25.....	37
SLIDE 26.....	38

Executive summary

This training reference guide has been created by ENISA in conjunction with presentation materials for small and medium enterprises to raise awareness with their employees about the critical risks due to malicious software.

These documents are designed to provide easy to understand information that focuses employees' attention on information security and how to recognise and respond accordingly to malicious software.

This material may be used by individuals or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts. This reference guide provides additional notes and external references for trainers and presenters to utilize while performing security awareness training.

How to use this manual

This manual is intended to be a guide for instructors of any security awareness course based on ENISA's Malicious software presentation. This manual is only a guide, and instructors are welcome to use any portion of this material they deem appropriate. It is at the instructor's discretion how to conduct the course and which material to present.

It should be noted however that ENISA recommends that the instructor carefully consider the skills and knowledge of the students being taught in developing the course. The material should be tailored to fit the needs of the students including making it easy to understand, relevant to their position and responsibilities.

ENISA has chosen focus this material on the general user community outside of the Information Technology field. As such, this presentation focuses on the fundamentals of critical risks due to malicious software and avoids the use of complex technical terms to explain risks or solutions.

Structure of the Manual

This manual broken into two parts:

1. How to use this manual (this section)
2. The presentation slides with associated supporting material

Structure of the Presentation Pages

Each of the presentation pages are broken in to three parts:

1. The thumbnail of the slide from the presentation
2. Suggested narratives that provide supporting information and Discussion points
3. Reference materials that support the slide that can be used to do further research

The presentations slides

Slide 1



Discussion points

This is a good time to have the attendees introduce themselves.

When everyone is introducing themselves, ask them to also say what they expect to get from the course. The answers will tell you what scenarios you can use as examples for this course, and what their expectations are for this course. This information is very useful so that you can adjust your discussions accordingly.

References

N/A

Slide 2

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the Internet market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a watchboard of information for good practice. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry sectors.

Contact details

For contacting ENISA or for general enquiries on information security awareness matters, please use the following details:

Website: www.enisa.europa.eu - **E-mail:** enisa@enisa.europa.eu
Internet: <http://www.enisa.europa.eu>

Legal notice

Users must be aware that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies, unless adopted pursuant to the ENISA regulation (EC) No 468/2004. This publication does not necessarily represent the state of the art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorized provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2010.

Discussion points

Introduce ENISA and their activities. Suggest that attendees should examine some of ENISA's other presentations on other aspects of network and information security.

References

<http://www.enisa.europa.eu> – ENISA's website

Slide 3

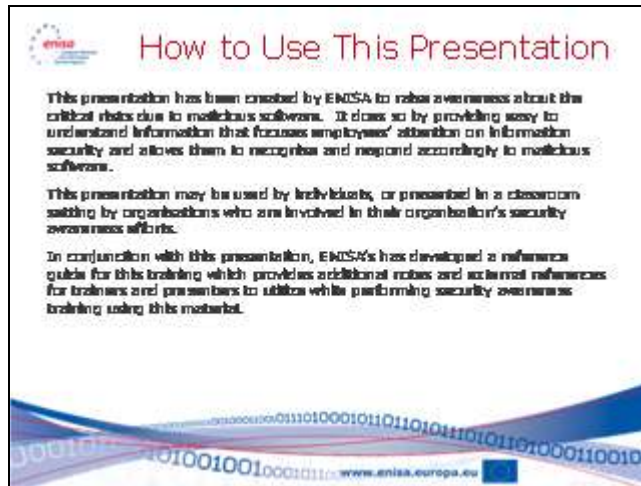


Discussion points

Point out that this presentation is intended to make users aware of the risks associated with malicious software, and also simple techniques that can eliminate a large percentage of these risks. Point out that the course is intended for all users, and that it offers best practices that can help protect each of them from malicious software at work and at home.

References

N/A

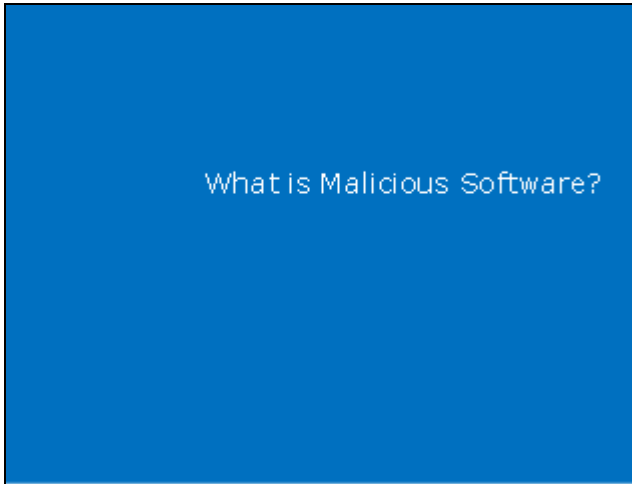
Slide 4**Discussion points**

This slide is an introduction, and is intended to inform readers that a presentation guide (this document) exists to support instructors in their security awareness efforts.

References

N/A

Slide 5



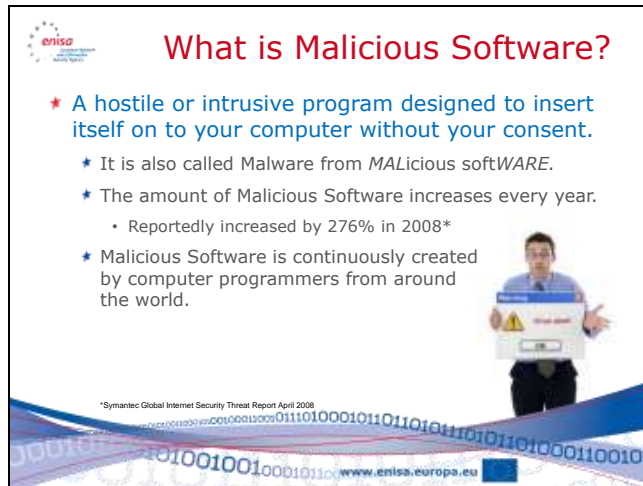
Discussion points

This is the start of Section 1, "What is Malicious Software?"

References

N/A

Slide 6



What is Malicious Software?

- ★ A hostile or intrusive program designed to insert itself on to your computer without your consent.
 - ★ It is also called Malware from MALicious softWARE.
 - ★ The amount of Malicious Software increases every year.
 - Reportedly increased by 276% in 2008*
 - ★ Malicious Software is continuously created by computer programmers from around the world.

*Symantec Global Internet Security Threat Report April 2008

www.enisa.europa.eu

Discussion points

It is important to point out that a program is malware if it meets one of two criteria:

- Is it hostile or intrusive
- Is it inserted on to your computer without your consent

A program can be Malware if it inserted itself on to your computer without your consent. It also (obviously) is malicious software if it is hostile or intrusive; which means it will perform hostile activities – deleting data or files, attacking other computers, or performing any other actions you do not consent to.

Throughout the presentation we will use the term Malware since it is easier to say. Malware is a combination of two words: **Malicious** and **Software**.

Malware is a difficult problem because it is created by programmers around the world. Some are searching for fame; some are curious programmers who do not see any harm in what they do. However, in recent years the most frequent type of malware is used by criminals to steal information, disrupt computer systems, or perpetuate fraud. Malware has been increasing at a rapid pace year after year, and shows no sign of slowing down. Because programmers are constantly creating new malware it is virtually impossible to completely eliminate malware.

Fun Fact: First recorded virus: Creeper Virus in 1971

References:

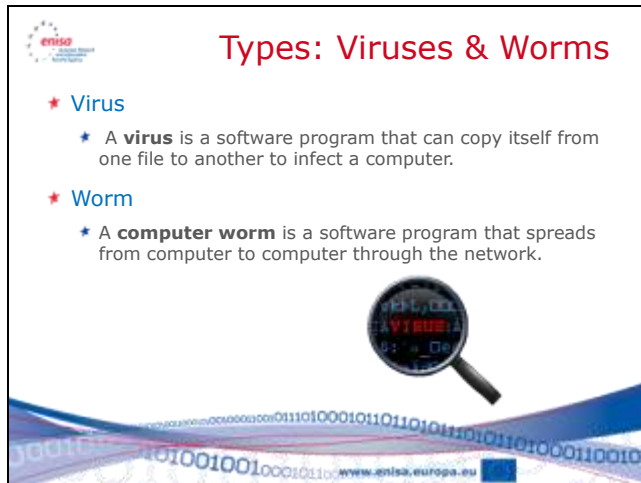
<http://technet.microsoft.com/en-us/library/dd632948.aspx>
<http://en.wikipedia.org/wiki/Malware>
http://malware.wikia.com/wiki/Main_Page

Good source for malicious software statistics:

<http://www.symantec.com/business/theme.jsp?themeid=threatreport>

An excellent timeline showing the history of malicious software:

http://malware.wikia.com/wiki/Timeline_of_noteworthy_computer_viruses,_worms_and_Trojan_horses

Slide 7

Types: Viruses & Worms

- ★ **Virus**
 - ★ A **virus** is a software program that can copy itself from one file to another to infect a computer.
- ★ **Worm**
 - ★ A **computer worm** is a software program that spreads from computer to computer through the network.

(The slide also features a magnifying glass over a computer screen displaying the word 'VIRUS' and a decorative background of binary code.)

Discussion points

Instructor: It is very easy to become very technical as you present the different types of malicious software. Stay focused on simple examples of how malware spreads and simple examples of what malware can do. Do not allow the discussion to become very technical in nature. The subject of Malicious Software is a science on to itself and can spark intense debates. The objective of this section is to make people aware of the risks and ways that they can become a victim of Malware. This approach will make it easier to explain why certain prevention tactics are so important.

There are several different types of malware that have been created. The next few slides will cover the most typical classifications. There are many types of malware which fall under multiple categories or change as they move from system to system. Malware is constantly evolving and new hybrid types of malware are created on a constant basis.

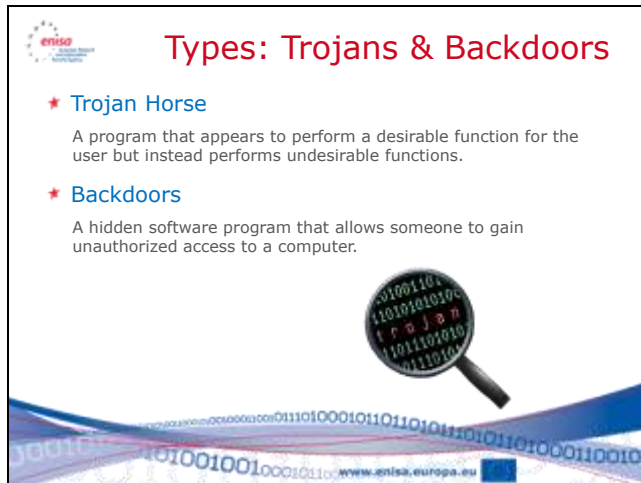
Viruses are typically programs that replicate themselves between files, memory, hard disks, or other data storage mediums. Typically viruses only spread when executing or copying a file that is already infected. Note that inserting a CDROM or thumb drive on some operating systems is equivalent to executing a program, and can also cause a virus to spread.

A worm is a program that spreads itself through a network and does not need to attach itself to an existing file or program. Worms spread themselves typically by exploiting existing vulnerabilities or weaknesses in an operating system or application. Some good examples are worms that exploited vulnerabilities in UNIX systems (the Morris Internet Worm of 1988) and worms that exploited vulnerabilities in Microsoft Windows (Mydoom of 2004). These worms spread rapidly through the Internet and continued until the vulnerabilities they exploited were fixed.

References


http://en.wikipedia.org/wiki/Computer_virus
<http://malware.wikia.com/wiki/Virus>

http://en.wikipedia.org/wiki/Morris_worm
<http://en.wikipedia.org/wiki/Mydoom>

Slide 8

Types: Trojans & Backdoors

- * **Trojan Horse**
A program that appears to perform a desirable function for the user but instead performs undesirable functions.
- * **Backdoors**
A hidden software program that allows someone to gain unauthorized access to a computer.



www.enisa.europa.eu

Discussion points

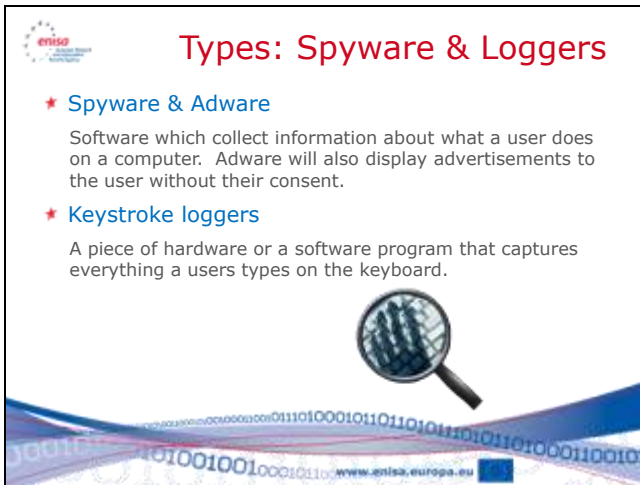
Trojan horses are named after the famous story of the Trojan Horse in the story of the Trojan War. Like the Trojan Horse in the story, the software Trojan Horse is designed to look like it is an innocent program. In some cases it may even use the name of an existing or standard file for an operating system. It may place itself in the same location as the standard file, or a different location. The software Trojan horse will, like its namesake, contain dangerous capabilities inside.

Backdoors are programs which allow an intruder or attacker to access a system in a way that bypasses normal authentication. Users normally have to log into a system using a username and password. A backdoor allows someone to not have to perform this process. Some backdoors are written by programmers to allow them access to software for problem solving, but can also be added to a computer to allow an attacker to access a system without needing a password, or in a way that cannot be detected. Backdoors may be created by installing a new program or by modifying an existing program that gives access to a system. Backdoors can be inserted by an intruder, a virus, or a worm.

References

http://malware.wikia.com/wiki/Trojan_horse
<http://malware.wikia.com/wiki/Backdoor>

Slide 9



Types: Spyware & Loggers

- ★ **Spyware & Adware**
Software which collect information about what a user does on a computer. Adware will also display advertisements to the user without their consent.
- ★ **Keystroke loggers**
A piece of hardware or a software program that captures everything a users types on the keyboard.

Discussion points

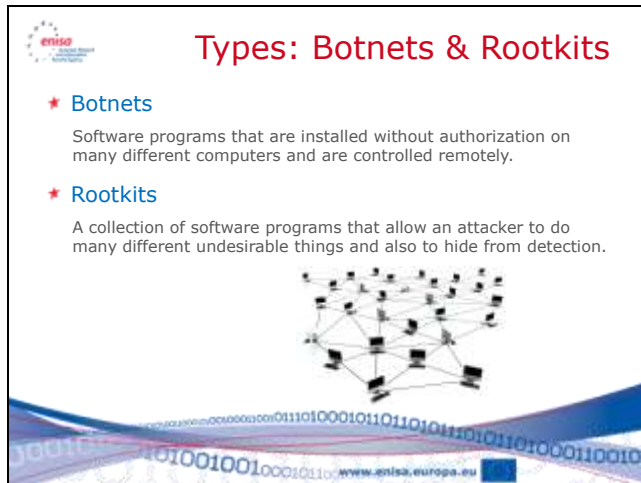
Spyware can be spread as a virus, worm, or through various other methods of delivering software (installing software from the Internet, visiting a malicious website). It has one goal – to track what you do on your computer and report that back to another system. Spyware may report what you type, what sites you visit on the Internet, and even what content is presented. This can include your banking information, passwords, and other confidential and personal information.

It can also cause your computer to become unstable and perform poorly as the adware and spyware send their information out to the Internet.

There are numerous keylogging methods, and can include spyware, or even pieces of hardware which are inserted into a system to monitor keystrokes. Like all other malicious software, it is placed there without the user’s consent.


References

<http://en.wikipedia.org/wiki/Spyware>
<http://malware.wikia.com/wiki/Spyware>

Slide 10

Types: Botnets & Rootkits

- * **Botnets**
Software programs that are installed without authorization on many different computers and are controlled remotely.
- * **Rootkits**
A collection of software programs that allow an attacker to do many different undesirable things and also to hide from detection.



www.enisa.europa.eu


Discussion points

Botnets refer to “robot networks” and are a new evolution of malicious software and has become wide-spread. Botnets consist of software which infects a user’s computer (called a robot or a zombie) and which is controlled by a remote system. Some popular botnets include Confiker from 2009. These botnets can be used for many different tasks. The software which infects the user’s computer waits for instructions on what to do from the remote system. The remote system may instruct it to collect information from the infected system, or it may instruct it to attack other computers it finds. Some botnets have been identified to consist of millions of systems. Current numbers are hard to estimate but they are extensive.

Rootkits are collections of software that help an attacker or intruder hide from detection. They may hide files, conceal that an intruder is present on the system, or to hide any processes that are running. Rootkits are a mix of tools that can include backdoors, keyloggers, and other tools that an intruder may find useful to hide their presence.



References

<http://en.wikipedia.org/wiki/Botnet>
<http://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets>
<http://malware.wikia.com/wiki/Rootkit>

Slide 11

How Does Malware Spread?

- ★ Malware usually attacks weaknesses and vulnerabilities in other computer programs
- ★ You can also spread Malware by:
 - ★ Opening email attachments infected with Malware
 - ★ Downloading infected files from the Internet
 - ★ Sharing files that are infected with Malware
 - ★ Visiting websites that contain Malware

**Discussion points**

Malware typically will infect a system through weaknesses and vulnerabilities in other computer programs, but this usually requires some help from a user. Many virus infections are due to users who open attachments or visit websites which contain malware, or users who do not install or keep their anti-virus software up-to-date.

One of the most common methods of spreading malware is through downloading files from the Internet or opening e-Mail attachments. Even files sent to you by people you know can contain malware. They may not recognize it because the malware wasn't detected by their anti-virus tool, or they use a different type of computer than you do. The malware will still exist and can affect your computer. Someone might invite you to download a file that contains some enticing picture, music or program. These invitations are usually an attacker attempting to spread malware.

File sharing sites also contain a large percentage of infected files. While it can be enticing to be able to download the latest music, pictures or programs, the high probability and risk of infecting your system with malware should be considered.

The same issue applies to many pop-up windows that tell you that your computer is infected with a virus, and you need to quickly download the software they present you with to clean the infection. In reality the software will install the infection. Many sites which carry controversial content such as open "hacker", violence, and pornography sites often contain malware as well.

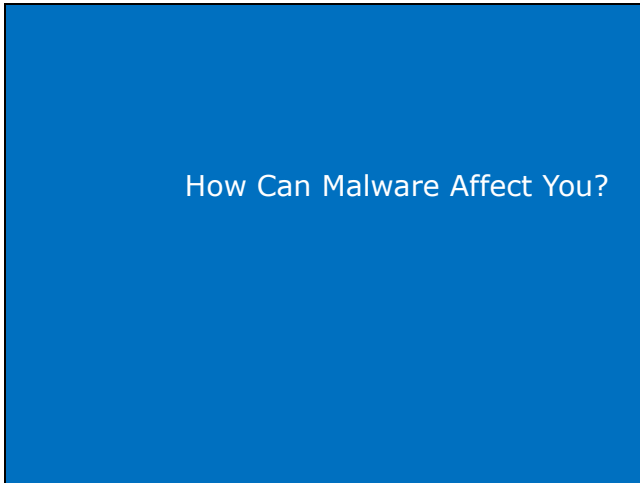
Always be careful when you are asked to download or install a file. There is a strong possibility that it contains malware. The best recommendation? Avoid files from untrusted sources, and always be sceptical of suggestions or invitations to download files and programs.

References

<http://www.us-cert.gov/cas/tips/ST05-007.html>

<http://www.wired.com/techbiz/media/news/2004/01/61852>
http://malware.wikia.com/wiki/Rogue_security_software
<http://www.symantec.com/business/theme.jsp?themeid=threatreport>

Slide 12

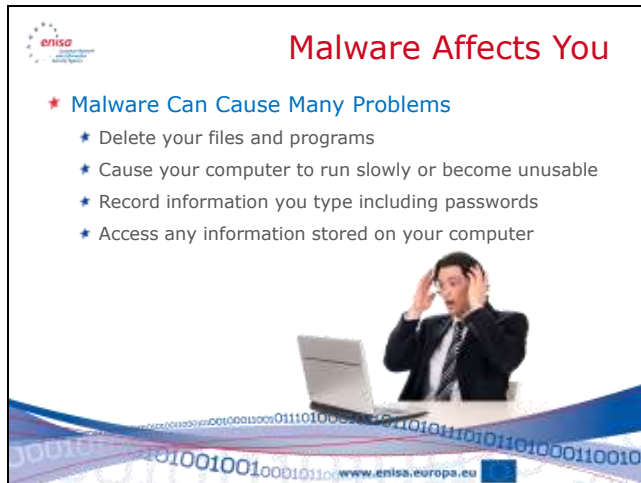


Discussion points

This is the start of Section 2, "How Can Malware Affect You?"

References

N/A

Slide 13**Discussion points**

Malware has a long history of causing damage to computers and networks.

Some famous malicious software:

Jerusalem virus – one of the first destructive viruses. It was discovered in 1988. It deletes files every Friday the 13th.

ILOVEYOU – a worm from 2000 that emails itself to everyone in the victim's address book. It is the most costly malware to date with estimates upwards of \$5.5 to \$10 billion (USD) in damages due to his worm.

Code Red / Code Red II / Nimda – a series of worms which exploited bugs in Microsoft IIS, and caused major Internet outages over three months in 2001.

SQL Slammer – an attack against vulnerabilities in Microsoft SQL that causes major outages on the Internet.

MyDoom – a worm from 2004 that spread quickly through email. It creates a way for a remote attacker to control the computer.

Instructor: Ask the audience to think of things that could be damaged, lost, stolen, or impact them if malicious software infected their computer, and a computer at their work. Use this discussion to make the audience aware of the risks of malicious software. The risks will make them more aware and attuned to methods to prevent and block malicious software. Watch for the types of information that the audience discusses. Encourage people to think of the impact to the things they value:

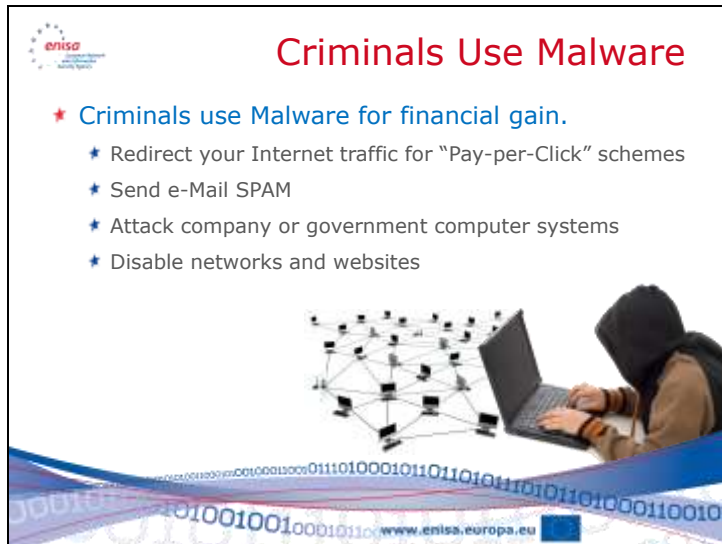
- *Personal information like their bank account information, passwords and PINs*
- *Passwords to Internet services like e-Mail, social networking sites, online stores and auction sites.*

- *Some users are most concerned with their pictures and music (think of teenagers, youth who do not have bank accounts)*

Focus on what a person considers valuable – what they worry about that exists on their computer, and what would happen if it wasn't available because of Malware.

References

http://malware.wikia.com/wiki/Timeline_of_noteworthy_computer_viruses,_worms_and_Trojan_horses

Slide 14

Criminals Use Malware

- ★ Criminals use Malware for financial gain.
 - ★ Redirect your Internet traffic for "Pay-per-Click" schemes
 - ★ Send e-Mail SPAM
 - ★ Attack company or government computer systems
 - ★ Disable networks and websites

Discussion points

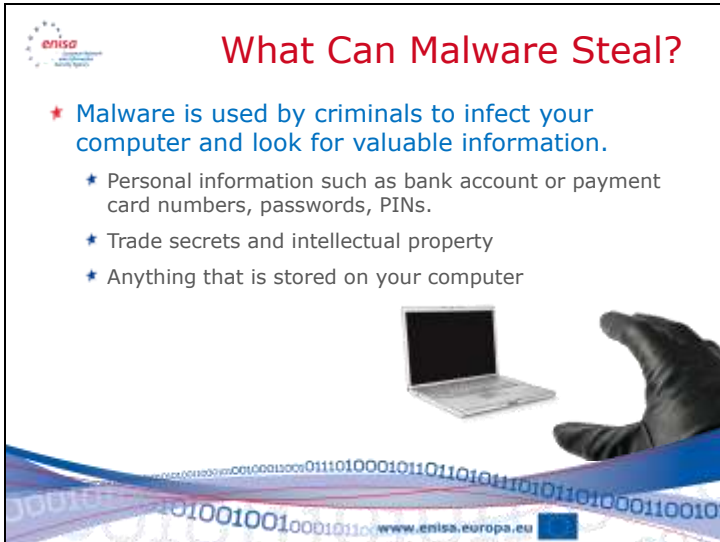
Today, much of malware is driven by criminal activity. Malicious software is used to collect personal and confidential information that can be sold for profit. Internet browsing is re-directed for monetary gains – many advertising programs pay money for every visitor to a website. Redirecting traffic can generate money for the owner of a site.

Botnets are frequently used to distribute SPAM or phishing e-mails which can cause congestion of networks, and lead people to websites that propagate even more malware! Botnets have also been used to attack specific websites in an attempt to make them unusable or unreachable. Since botnets often consist of thousands of computers working together, they can cause serious disruption to networks and websites.

References

<http://www.symantec.com/business/theme.jsp?themeid=threatreport>
<http://www.honeynet.org/node/52>

Slide 15



What Can Malware Steal?

- ★ Malware is used by criminals to infect your computer and look for valuable information.
 - ★ Personal information such as bank account or payment card numbers, passwords, PINs.
 - ★ Trade secrets and intellectual property
 - ★ Anything that is stored on your computer

The slide features an image of a hand in a black glove pointing towards a laptop. The background of the slide has a blue and white binary code pattern. The ENISA logo is in the top left corner, and the URL 'www.enisa.europa.eu' is at the bottom.

Discussion points

The goal of most criminals is to find a way to steal money. There are cyber-crime groups which write malicious software for specific tasks. This type of malicious software will look for anything of value on your computer. It typically will search for personal information, or try to direct you to sites which ask you to input personal information. More sophisticated tools will look for certain keywords that may indicate trade secrets, new product designs, or other information that can be sold to competitors.

References

<http://www.symantec.com/business/theme.jsp?themeid=threatreport>

Slide 16***Discussion points***

This is the start of Section 3, "How to Protect Yourself From Malware"

References

N/A

Slide 17



Discussion points

By regularly applying manufacturer’s patches for your operating system and applications you eliminate the way that most malicious software infects your computer. Most malicious software looks for vulnerabilities and weaknesses that exist in operating systems and applications. By fixing these problems you can minimize the opportunity malware has to infect your system. Be aware that every operating system and application has some vulnerability, and that it is almost impossible to discover and correct every vulnerability or weakness. Sometimes people discover these vulnerabilities before the manufacturer finds them, and instead of telling the manufacturer, they write a program to exploit the vulnerability. Be aware that applying patches is not the only defence, and is only one step in protecting yourself.

By configuring your browser to block pop-up windows you reduce the possibility of a site displaying a pop-up with malware embedded in it, or with links that will install malicious software. This, like patches is only a partial fix to the problem. Blocking pop-ups only address one possible way that malware can be presented to a user. An attacker can still place the malware on a main page of a website and achieve the same results. The only advantage to a pop-up is that it makes the situation seem far more immediate and urgent to a user and encourages them to take action based on the pop-up window. By blocking pop-up windows you reduce one tool in an attacker’s bag of tricks as they attempt to infect your computer with malware.

Backing up your file and programs regularly can help you avoid a disaster if your system ever is infected. If malware cannot be removed from your system you may have to re-install the entire system. Doing so may destroy all your files. A backup will ensure that you can restore these files. Be careful when restoring the files that you do not re-infect your system, as your backup may contain the file that contains the malware.

References

<http://www.microsoft.com/windowsxp/using/networking/security/protect.mspx>

<http://www.cert.org/homeusers/HomeComputerSecurity/>

Slide 18



Protect Your Computer

- ★ Install a reputable anti-virus, anti-spyware, browser filter, and personal firewall product.
 - ★ Update virus definition at least once a day
 - ★ Perform a full scan of your computer every week
 - ★ Alert you of dangerous websites
- ★ Beware of fake antivirus product offers




Discussion points

Installing full featured personal computer security products that offer anti-virus, anti-malware, anti-spyware, browser filters, website alerting, and personal firewalls will give you a high level of protection. There are many reputable companies who produce these types of products.

In order for them to be effective however, they must be updated regularly. This includes virus definitions, and software updates as they are released. Configure the software carefully. The frequency suggested here are minimums. Updating your virus definitions more frequently can help address outbreaks quickly, and full scans (or scans performed when your computer is idle) help ensure ongoing protection.

Personal computer security and anti-virus products are not full-proof. They cannot detect all malware. Some malware is disguised as Trojans – programs that look normal but which really contain malicious software inside. It is still important for you to be aware and avoid common user mistakes that result in malware infections.

Some sites will present pop-up windows that tell you that your computer is infected with a virus, and you need to download the software they offer to clean the infection. In reality their software will install the infection. Only use reputable anti-virus software vendors.

References

<http://www.microsoft.com/windowsxp/using/networking/security/protect.msp>
<http://www.cert.org/homeusers/HomeComputerSecurity/>
http://malware.wikia.com/wiki/Rogue_security_software
<http://www.symantec.com/business/theme.jsp?themeid=threatreport>

Slide 19

Avoid Risky Behaviour

- ★ **Avoid Unknown Files & Programs**
 - ★ Do not download programs or files that are sent to you, even if you know who sent it.
 - ★ Do not download files or programs offered over Chat or IRC.
 - ★ Do not download or install programs from pop-up windows.
 - ★ Do not open email attachments from people you do not know.
 - ★ Be careful what Internet sites you visit.
 - ★ Avoid programs and files from file sharing sites.

VIRUS

www.enisa.europa.eu

Discussion points

One of the most common methods of spreading malware is through e-Mail attachments. Even files sent by people you know can contain malware. They may not recognize it because the malware wasn't detected by their anti-virus tool, or they use a different type of computer than you. But the malware still exists and can affect your computer.

You may be asked to download a file containing some enticing picture, music or program. These invitations are usually an attacker attempting to spread malware. The same applies to some pop-up windows that state your computer is infected with a virus, and you need to quickly download their software to remove the malware. In reality their software will install the malware. Many sites which carry controversial content also contain malware.

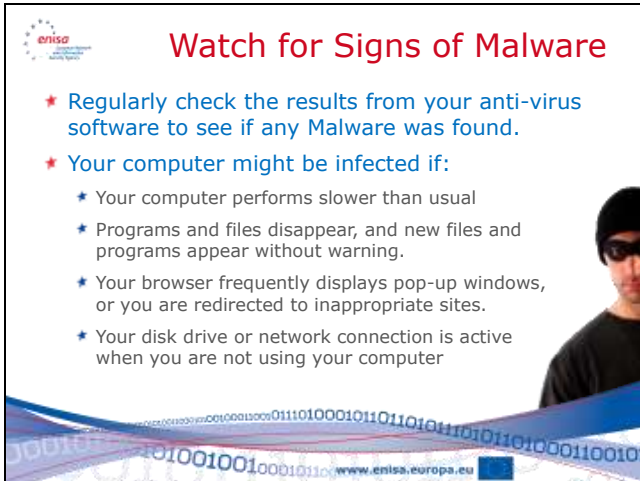
File sharing sites also contain a large percentage of infected files. While it can be enticing to be able to download the latest music, pictures or programs, the high probability and risk of infecting your system with malware should be considered.

Always be careful when you are asked to download or install a file. There is a good possibility that it contains malware. The best recommendation? Avoid files from untrusted sources, and always be sceptical.

References

http://malware.wikia.com/wiki/Rogue_security_software
<http://www.us-cert.gov/cas/tips/ST05-007.html>
<http://www.wired.com/techbiz/media/news/2004/01/61852>

Slide 20



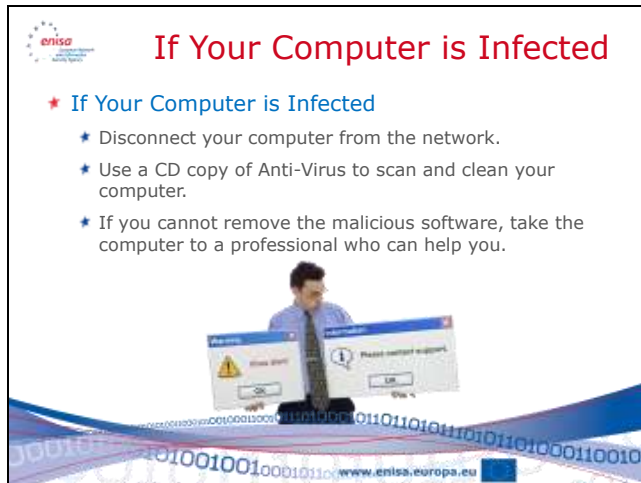
Discussion points

There are many signs that malware has infected your system. Some are very easy to see – check the logs and reports from your anti-virus software to see if it found any Malware. In some rare cases it may report that it could not fix or remove some malware. Usually it will report when malware was detected. Notice what when the infection happened and what file was infected, and if it corresponds to some activity you were doing. It may be associated with an email, a website you visited, software you ran, or a file you downloaded. Be very aware of what actions might have caused the infection and be careful not to repeat them.

Poor computer performance can be an indication of malware using computer resources (memory, processing time, and transmitting via the network). If your disk drive is active when you are not using your computer, it may be a sign of malicious software. Also note however that many anti-virus programs will scan you disks for malware automatically if you leave your computer idle for a period of time. If you frequently see undesirable pop-up windows or are redirected to undesirable websites there is a good possibility that you are infected with Spyware, Adware or other Malware.

References

<http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280800>

Slide 21

If Your Computer is Infected

*** If Your Computer is Infected**

- ★ Disconnect your computer from the network.
- ★ Use a CD copy of Anti-Virus to scan and clean your computer.
- ★ If you cannot remove the malicious software, take the computer to a professional who can help you.

The slide includes an image of a man in a blue shirt sitting at a desk with a computer. The computer screen displays two error messages: 'Warning' and 'Please contact support'. The background of the slide features a blue and white digital pattern with binary code and the ENISA website URL 'www.enisa.europa.eu'.

Discussion points

Instructor: These are best practices for handling viruses and are directed at the average user. This example is applicable more for home users since in a company environment the user would have already engaged the helpdesk, incident response team, or any other applicable groups or individuals.

It is our recommendation that you discuss with the security officer the current procedures within the company for handling an incident, and include those in the training.

Instruct the attendees to follow the company incident response procedures – e.g. who to notify, what other steps to take such as writing down what they were doing before they noticed the infection, what symptoms or issues they noticed before discovering their system was infected. While a good incident response plan is outside the scope of this paper, it is critical for any business to be able to respond to an incident like a virus outbreak.

If you find your computer is infected, always first disconnect the computer from the network. This will limit the ability of the malicious software to spread and limit the damage it can cause to other systems.

Use a CD copy of anti-virus to scan and clean your computer. By using a CD copy you can be certain that the anti-virus software has not been affected by the malicious software. Anti-virus software is one of the first things that malware will target in order to disable any attempt to remove or stop the malware. By using a copy of the malware that cannot be altered (on an original installation CD) you can be reasonably certain that the malware cannot alter the anti-virus software.

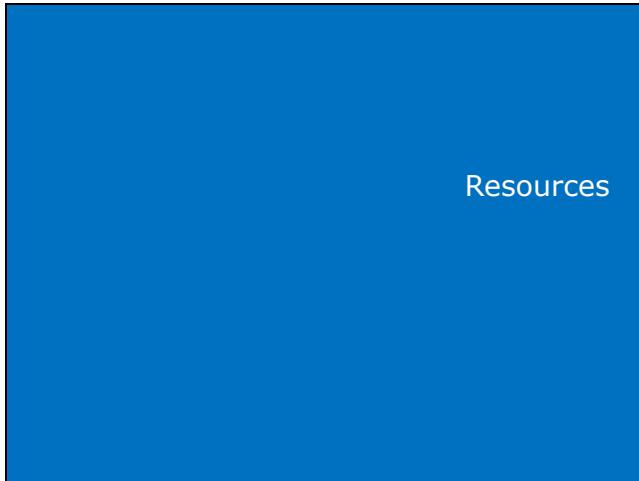
If the anti-virus software is unable to detect and remove the malware, contact a computer professional who can help you remove the software. Avoid attempting to remove the software yourself unless you are trained to do so. Many different types of malware are very resistant to removal. They will hide in different locations, and even avoid detection and removal after a new

operating system removal. A professional can help identify the malware, and choose an appropriate response to eradicate it.

References

<http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280800>

<http://www.onguardonline.gov/topics/malware.aspx>

Slide 22***Discussion points***

This is the start of Section 4 which lists some resources if you are dealing with Malicious Software.

References

N/A

Slide 23



Resources

★ **Free Online Tools & Scanners**

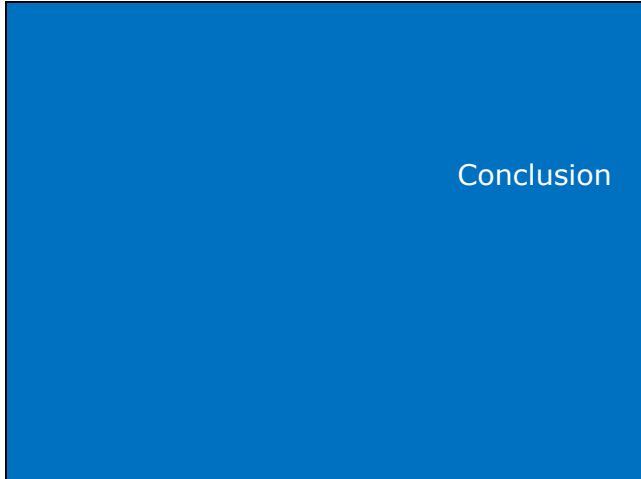
- BitDefender: <http://www.bitdefender.com/scanner/online/free.html>
- ESET: <http://www.eset.com/onlinescan/>
- F-Secure: http://www.f-secure.com/en_IN/security/security-lab/tools-and-services/
- Kaspersky: <http://www.kaspersky.com/virusscanner>
- McAfee: <http://home.mcafee.com/Downloads/FreeScan.aspx>
- Microsoft: <http://onecare.live.com/site/en-us/default.htm>
- Trend Micro: <http://housecall.trendmicro.com/>
- Symantec: <http://security.symantec.com/sscv6/WelcomePage.asp>

Discussion points

Instructor: This is a list of well known online virus scanning tools made available by various anti-virus vendors. This list is provided purely as an example of possible solutions, and does not constitute an endorsement or guarantee of any kind for that vendor.

References

N/A

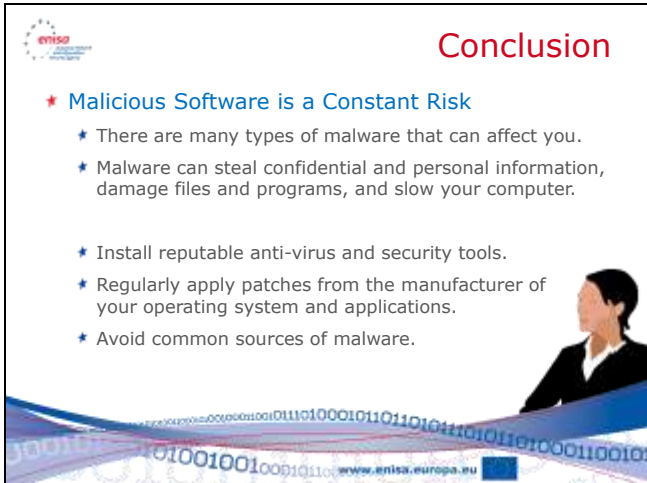
Slide 24***Discussion points***

This is the conclusion of the presentation.

References

N/A

Slide 25



Discussion points

Instructor: This is a summary slide that provides an opportunity to repeat the key themes of the presentation.

As we pointed out in this presentation, there are many different types of malicious software that can affect you and your computer.

We discussed how malware can steal confidential and personal information, can damage files and programs, and slow down, or even cause your computer to stop running.

And we talked about key ways to protect yourself:

Install reputable anti-virus and security tools.

Regularly apply patches from the manufacturer of your operating system and applications so you can stay up to date.

And lastly, avoid common sources of malware including fraudulent e-mails, malicious or suspicious websites, and free files offered through file sharing, chat or pop-up windows.

References

N/A

Slide 26**Discussion points**

N/A

References

N/A



PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu