# 9.1.2 Malware Overview Facts

As long as computers have been around, people have been creating malware programs. The term malware is short for malicious software. These are programs that are designed to perform malicious and destructive functions.

This lesson covers the following topics:

- Malware related laws
- Malware components
- Viruses
- Worms
- Virus and worm countermeasures

## Malware Related Laws

The follow table lists the regulations that apply to malware:

| Law | Description |
|---|---|
| Computer Fraud and Abuse Act | The Computer Fraud and Abuse Act (CFFA) was first introduced in 1984 and has been updated many times since. The CFFA essentially defines what computer related crimes are and ensures that these crimes can be punished. |
| USA Patriot Act | The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act) expanded on the powers already included in the CFAA. |
| CAN-SPAM Act | The Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act was signed into law in 2003. The CAN-SPAM Act established the rules and guidelines for commercial emails efforts to curb the assault of spam emails. According to the FTC, these guidelines are as follows:<br>1. Don't use false or misleading header information. The From, To, Reply-To, and routing information, including the originating domain name and email address, must be accurate and identify the person or business who initiated the message.<br>2. Don't use deceptive subject lines. The subject line must accurately reflect the content of the message.<br>3. Identify the message as an ad. The law gives you a lot of leeway in how to do this, but you must disclose clearly and conspicuously that your message is an advertisement.<br>4. Tell recipients where you're located. Your message must include your valid physical postal address. This can be your current street address, a post office box you've registered with the U.S. Postal Service, or a private mailbox you've registered with a commercial mail receiving agency established under Postal Service regulations.<br>5. Tell recipients how to opt out of receiving future email from you. Your message must include a clear and conspicuous explanation of how the recipient can opt out of getting email from you in the future. Guidelines include:<br>▪ Craft the notice in a way that's easy for an ordinary person to recognize, read, and understand.<br>▪ Creative use of type size, color, and location can improve clarity.<br>▪ Give a return email address or another easy internet-based way to allow people to communicate their choice to you.<br>▪ You may create a menu to allow a recipient to opt out of certain types of messages, but you must include the option to stop all commercial messages from you.<br>▪ Make sure your spam filter doesn't block these opt-out requests.<br>6. Honor opt-out requests promptly. Guidelines for this rule include:<br>▪ Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message.<br>▪ You must honor a recipient's opt-out request within 10 business days.<br>▪ You can't charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an internet website as a condition for honoring an opt-out request.<br>▪ Once people have told you they don't want to receive more messages from you, you can't sell or transfer their email addresses, even in the form of a mailing list.<br>▪ The only exception is that you may transfer the addresses to a company you've hired to help you comply with the CAN-SPAM Act.<br>7. Monitor what others are doing on your behalf. The law makes clear that even if you hire another company to handle your email marketing, you can't contract away your legal responsibility to comply with the law. Both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible. |

## Malware Components

Malware is made up of different components that allow it to achieve its goals. These components are:

| Component | Description |
|---|---|
| Crypter | Basically a shell around the malware code that keeps the malware from being analyzed and reverse engineered. This also helps prevent detection by anti-malware programs. |

| | |
|---|---|
| Exploit | This takes advantage of a bug or vulnerability to execute the malware. |
| Injector | The program that injects, or places, the malware into vulnerable running processes. |
| Obfuscator | Uses different techniques to conceal the malware. |
| Packer | Compresses the malware to reduce its size and also helps hide it. |
| Payload | This is the main piece of the malware. The payload is what performs the intended activity of the malware. |
| Malicious code | The programming that performs the malware's basic functionality. |

## Viruses

A virus is the most well-known type of malware. People often interchange the terms malware and virus. A virus is self-replicating malware that attaches itself inside a legitimate program. It must be attached to another program to run. Hackers will often use a virus making tool to create a virus or will write their own. A virus making tool allows the hacker to define what they want the virus to do and how to replicate itself. Writing a unique virus will make the virus harder for antivirus software to detect, but does require programming knowledge. There are many types of viruses. How the virus is executed and what it does will define the virus type. The following table describes common viruses.

| Virus Type | Description | Example |
|---|---|---|
| Direct action | Infects a program and runs only when that program is run. The virus stops when program is closed. The goal is to infect as many files and folders as possible. | VCL.428 |
| Logic bomb | Triggered by an event, such as specific date/time or a program being executed. If triggered by date/time, it is referred to as a time bomb. | AgentBase.exe |
| Overwrite | Overwrites the contents of an infected file or folder. The only way to get rid of this virus is to delete infected files. | Loveletter |
| Browser hijacker | Infects web browsers so when the user attempts to go to a web page, the virus will redirect the browser to a fake website that can harm the computer. | Onewebsearch |
| Web scripting | Resides in ads, videos, or the background of a website. When a user visits, the virus will infect the computer automatically through client-side scripting. There are two types of this virus, persistent and non-persistent. Persistent is when the user's cookies are stolen and can lead to session hijacking. Non-persistent is when the user is attacked without knowing. | JS.fornight |
| Boot sector | Moves the MBR to another location on the hard drive and embeds itself in the original location. When the computer boots, the virus runs first, then passes control to the MBR. | Polyboot.B |
| Cavity | Also known as an overwriting virus. This virus fills in empty space in a file or program without increasing the length of the file. It preserves the file or program's functionality. | Lehigh Virus |
| Email | A virus that is sent as an email attachment. This can be any type of virus. | (almost any virus) |
| Sparse-infector | Attempts to hide itself from antivirus by infecting at random times or by random triggers. These triggers can be a specific file size, name, date, or when a particular program is executed. | Dark Avenger |
| Polymorphic | Contains a mutating engine that changes the code every time the virus is replicated while keeping the original malware algorithm intact. This makes the virus extremely difficult to detect. | Elkern |
| Encryption | Also known as a cryptovirus, this virus infects the user files and folders and encrypts them. A decryption key is required to recover the data. | Cryptolocker |
| Macro | Infects files created by Microsoft Office or similar programs. These viruses will typically infect a template file and keep the appearance of a normal file. | Melissa |
| Cluster | Also known as a directory virus. The virus changes file paths of programs. When an infected program is run, the virus will also run in the background. These can be difficult to trace. | Dir-2 |
| File infector | Infects executable files so when the file is run, the virus executes. | Cascade |
| Companion | Also known as a camouflage virus. The virus creates a companion file for the infected file/program. | Stator |

| | | |
|---|---|---|
| | When the user runs the legitimate program, the virus is also run in the background. | |
| FAT | Attacks the File Allocation Table destroying the index, making it impossible for files to be found. This is a very destructive virus. | The Link Virus |
| Multipartite | Combines the approach of a File and Boot Sector virus and attempts to infect files and the boot sector simultaneously. | Ghostball |
| Stealth/tunneling | Tricks the antivirus software by appearing to be a real program or Windows service. When the AV software scans files, the virus will intercept the request and send the original, uninfected file to be scanned. | Frodo |
| Metamorphic | Rewrites itself completely each time it infects a new file. This virus type is similar to a polymorphic virus, but is more complex and effective. | Zmist |
| Armored | Wraps itself in code to hide its characteristics, protecting itself from being detected. | Whale |
| Terminate and stay resident (TSR) | This virus will reside in the system's RAM until the computer is shut down or rebooted. This virus can interrupt anything being run on the system and infect files or programs that are opened or closed. | MrKlunky |

Regardless of the type, all viruses have the same life cycle:

1. Design – virus is created.
2. Replication – virus replicates and spreads within victim machine.
3. Launch – virus is launched and executes payloads.
4. Detection – virus is detected and identified as a threat.
   - Slow system
   - Frequent Blue Screen of Death (BSOD)
   - Deleted files
   - Operating system won't load
5. Incorporation – antivirus software developers design defenses against virus.
6. Execute the damage routine – users update antivirus software and eliminate virus threat.

## Worms

Unlike viruses, worms are entirely self-replicating. Worms effectively use the power of networks, malware, and speed to spread. These malware programs are generally not destructive in nature, but do consume a large amount of bandwidth and can take down a network system quickly if not caught. Worms can also carry additional payloads, such as viruses, which will be destructive.

The following table compares worms and viruses:

| Worms | Viruses |
|---|---|
| Standalone malware program. | Requires a file or executable program to infect. |
| Generally does not modify files or folders. | Can be destructive and modify files including system files. |
| Can replicate through a network with no human interaction. | Can spread to other computers only through email or other media. |
| Consume network and system resources, such as CPU cycles and network bandwidth. | Changes the way a computer operates without the user's knowledge. |
| Can spread through a network extremely quickly. | Spreads and replicates as programmed. |

## Virus and Worm Countermeasures

Use these countermeasures to combat viruses and worms:

- Install antivirus software that detects and removes infections as they appear.
- Generate an antivirus policy for safe computing and distribute the policy to the staff.
- Pay attention to the instructions while downloading files or any programs from the internet.
- Update antivirus software regularly.