Security Tip (ST06-006)

TLP:WHITE

Understanding Hidden Threats: Corrupted Software Files

Original release date: March 09, 2011 | Last revised: February 06, 2013

What types of files can attackers corrupt?

An attacker may be able to insert malicious code into any file, including common file types that you would normally consider safe. These files may include documents created with word processing software, spreadsheets, or image files. After corrupting the file, an attacker may distribute it through email or post it to a website. Depending on the type of malicious code, you may infect your computer by just opening the file.

Malicious code is not always hidden in web page scripts or unusual file formats. Attackers may corrupt types of files that you would recognize and typically consider safe, so you should take precautions when opening files from other people.

When corrupting files, attackers often take advantage of vulnerabilities that they discover in the software that is used to create or open the file. These vulnerabilities may allow attackers to insert and execute malicious scripts or code, and they are not always detected. Sometimes the vulnerability involves a combination of certain files (such as a particular piece of software running on a particular operating system) or only affects certain versions of a software program.

What problems can malicious files cause?

There are various types of malicious code, including viruses, worms, and Trojan horses (see Why is Cyber Security a Problem? for more information). However, the range of consequences varies even within these categories. The malicious code may be designed to perform one or more functions, including

- interfering with your computer's ability to process information by consuming memory or bandwidth (causing your computer to become significantly slower or even "freeze")
- installing, altering, or deleting files on your computer
- giving the attacker access to your computer
- using your computer to attack other computers (see Understanding Denial-of-Service Attacks for more information)

How can you protect yourself?

- **Use and maintain anti-virus software** - Anti-virus software can often recognize and protect your computer against most known viruses, so you may be able to detect and remove the virus before it can do any damage (see Understanding Anti-Virus Software for more information). Because attackers are continually writing new viruses, it is important to keep your definitions up to date.
- **Use caution with email attachments** - Do not open email attachments that you were not expecting, especially if they are from people you do not know. If you decide to open an email attachment, scan it for viruses first (see Using Caution with Email Attachments for more information). Not only is it possible for attackers to "spoof" the source of an email message, but your legitimate contacts may unknowingly send you an infected file. If your email program automatically downloads and opens attachments, check your settings to see if you can disable this feature.
- **Be wary of downloadable files on websites** - Avoid downloading files from sites that you do not trust. If you are getting the files from a supposedly secure site, look for a website certificate (see Understanding Web Site Certificates for more information). If you do download a file from a website, consider saving it to your computer and manually scanning it for viruses before opening it.
- **Keep software up to date** - Install software patches so that attackers cannot take advantage of known problems or vulnerabilities (see Understanding Patches for more information). Many operating systems offer automatic updates. If this option is available, you should enable it.

TLP:WHITE

- **Take advantage of security settings** - Check the security settings of your email client and your web browser (see Evaluating Your Web Browser's Security Settings for more information). Apply the highest level of security available that still gives you the functionality you need.

Related information

- Securing Your Web Browser
- Recovering from Viruses, Worms, and Trojan Horses

Author

Mindi McDowell

TLP:WHITE