

## Protect Your IT Systems from Malware

Malware is a group of malicious software-like applications that can cause damage to your computers as well as compromise your business's uptime and affect your bottom line. A malware outbreak at your business could slow down machines to a crawl, crash servers and network equipment, as well as corrupt or delete important data. "Dealing with viruses, spyware, PC theft and other computer-related crimes costs U.S. businesses a staggering \$67.2 billion a year, according to the FBI." (ZDNet, 2006) To protect your IT systems you need to know what malware is and how it works.

Malware consists of the following types of applications:

- **Virus**- an application that copies itself and infects a computer without the user's knowledge. A virus spreads by attaching itself to documents or emails.
- **Worm**-an application that replicates itself by spreading across a computer network or the internet. Worms usually spread by finding programming faults in software applications to gain access to the operating system.
- **Trojan Horse**- an application that appears useful, but has the ulterior motive of downloading or installing another application to perform unapproved tasks like logging keystrokes, viewing documents, and remotely controlling your computer.
- **Rootkit**-an application that conceals itself by replacing parts of the operating system to avoid detection when a security program is run. Carefully hidden, the rootkit then runs any application that the programmer wants, giving the programmer full access to your computer. Rootkits are very hard to find, and even harder to get rid of.



- **Spyware**- an application designed to collect personal information about a user without their knowledge. Spyware can also redirect internet traffic, record keystrokes, and change internet settings.

## The Best Way to Catch a Case of Malware

Each type of malware spreads in a unique way:

- **Viruses** are spread when a user sends an infected document to another user as an email attachment or by sharing the file on a disk or across the network.
- **Worms** spread across the network looking for un-patched computers and servers. As each machine is infected, the worm looks for new machines to infect, quickly infecting an entire network within minutes.
- **Trojans, root kits, and spyware** are frequently installed accidentally without the knowledge of the user—usually through internet downloads or through peer-to-peer networks.

## Protect Your IT Systems

Educate yourself, your staff, your friends and family to be aware of possible malware threats:

- **Don't** open email attachments from unfamiliar people.
- **Don't** click on an unexpected link in an email unless you trust the sender Never install free software that you obtained from the internet.
- **Never** purchase online software from suspect sites where the offer is too good to be true.
- **Always** keep your computer systems software and operating system updated.



- **Perform** an in-depth security scan with an industry approved software program such as LanGuard or Nessus on a regularly scheduled basis to check for malware.

### **Too Little, Too Late**

Sometimes, malware will slip by even the most vigilant user. Symptoms of a malware infection include:

- slow computer
- slow internet browsing
- unapproved redirection of your homepage
- random pop-up windows when connected to the internet
- Outlook is slow or starts emailing people without permission.
- malfunctioning instant messenger

### **Seek Professional Help**

Getting help for your malware outbreak is less painful than going to the doctor's office for your yearly checkup. All Covered's technical engineers are familiar with all the tools and techniques needed to remove even the most malicious malware floating around. They can fix your current outbreak as well as get your IT systems up-to-date to help prevent a future outbreak.

Of course, you don't need to wait for malware to seek preventative maintenance—All Covered is happy to help you protect your systems before you have any problems. To learn more about how to protect your network against malicious applications, please contact All Covered.