Black Paper

MALWARE DEFINITIONS

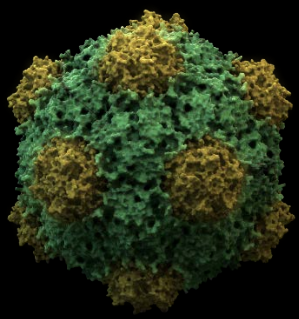
January 15, 2016

DIFFERENT TYPES OF MALWARE

There are many types of malware floating around on the internet. Here are some quick definitions and descriptions of them.

VIRUS

A virus is a general term for a small computer program that is able to copy itself and spread through computer networks by attaching to a file. Recommended software Kaspersky or Bitdefender.



TROJAN

The term comes from the Greek story of the Trojan war, where the Greeks give a large wooden horse as a gift to the Trojans. The Trojans accepted the horse and took it inside their gates. At night Greek men snuck out of the horse and open the gates, letting in the Greek army. Trojan viruses operate in a similar way. They act like beneficial software but their real purpose is to open a back door to allow other malicious software to install over the internet without you knowing. Recommended software Kaspersky or Bitdefender.

CAO IT Service / 1 250 979 7457 / # 201B, 260 Harvey Ave. / Kelowna
www.caoitservice.com / office@caoitservice.com

Black Paper

MALWARE DEFINITIONS

January 15, 2016

SPYWARE

This software obtains private or personal information from your computer and transmits it covertly through the internet. Recommended Malwarebytes Antimalware, Bitdefender Rootkit remover and Kaspersky Security Scan.

ADWARE

This software makes pop-ups on your computer with advertisements. Recommended Malwarebytes Antimalware, Bitdefender Rootkit remover and Kaspersky Security Scan.

RANSOMWARE

This software comes in an encrypted zip file in an email. When the user clicks on the email, the virus is launched. The software runs in the background and starts to encrypt all important personal data, drives and network devices it has access to. When the virus is done encrypting all data, it pops up on the desktop and requests payment in the form of bitcoin or anonymous money order. If the user

MALWARE DEFINITIONS

January 15, 2016

does not pay within a specified time period, the virus deletes the private key and all data that was encrypted is lost. There is no software to combat this unfortunately. The encryption is too strong to crack therefore your options are limited. Please contact our office right away if you get infected!

WORM

A worm is a small computer program that is able to copy itself and spread through computer networks automatically. Unlike a virus, which needs to piggy back on other files, a worm is self-contained. This makes it replicate faster than most viruses as no work needs to be done to execute it. Recommended Malwarebytes Antimalware, Bitdefender Rootkit remover and Kaspersky Security Scan.

Black Paper

MALWARE DEFINITIONS

January 15, 2016

EMAIL VIRUS

Viruses that spread exclusively through email clients. Recommended software Kaspersky or Bitdefender.

BROWSER HIJACKER

This software infects your internet browser. It typically re-directs your web requests to unwanted websites. Sometimes the hijacker will display ads in your browser. Occasionally the hijacking software will try to sell you software to clean the infection off. Never give your credit card information to hijacking software. Recommended Malwarebytes Antimalware, Bitdefender Rootkit remover and Kaspersky Security Scan.

ROOTKIT VIRUS

This virus infects the root of your operating system, called the kernel. The virus can load before the operating system to mask its presence. Sometimes these viruses modify the master boot record and can directly inject code into RAM to go around software safeguards. This software is not normally caught with free antivirus and requires special apps designed to detect root kits. Recommended

Black Paper

MALWARE DEFINITIONS

January 15, 2016

Malwarebytes Antimalware, Bitdefender Rootkit remover and Kaspersky Security Scan.

KEYLOGGER

This software installs silently in the background of your operating system. It records every key you press into a file. The software periodically sends these files back to the hacker that scans them for credit cards, passwords or personal information. Recommended software Kaspersky or Bitdefender.

PROTECT YOURSELF

All these threats can be mitigated with a few basic guidelines.

1. Be careful! An ounce of prevention is worth a pound of cure. Avoid the “back alleys” of the internet. Only go to reputable websites.
2. Emails are the most common way for viruses to spread. Be vigilant with your email. Turn off “Message Preview” on your emails to stop viruses from launching when you click on the message. Do not open attachments until you verified they are legitimate. Do not click on links in emails until you know they are legitimate. Be wise and not too trusting of emails.
3. Install a paid antivirus. Free is ok, but you get what you pay for. The top rated antiviruses for 2016 are Kaspersky and Bitdefender. Norton and

MALWARE DEFINITIONS

January 15, 2016

McAfee are not recommended. A good antivirus works all the time to keep your computer clean.

4. Get a good anti-malware. These tools should be installed and run periodically to catch anything missed by the Antivirus. Some good ones are Malwarebytes Antimalware, Bitdefender Rootkit remover and Kaspersky Security Scan.
5. Get regular maintenance on your computer. An expert technician can clean and tune your PC to run its best. Every 3-6 months is a good rule of thumb.

We hope that this Black Paper was informative and useful to you.

Thank you,

Chris please put our footer with our names on it here.