Presentation by Carefree Computing Inc.
1-866-377-6275 ext. 8

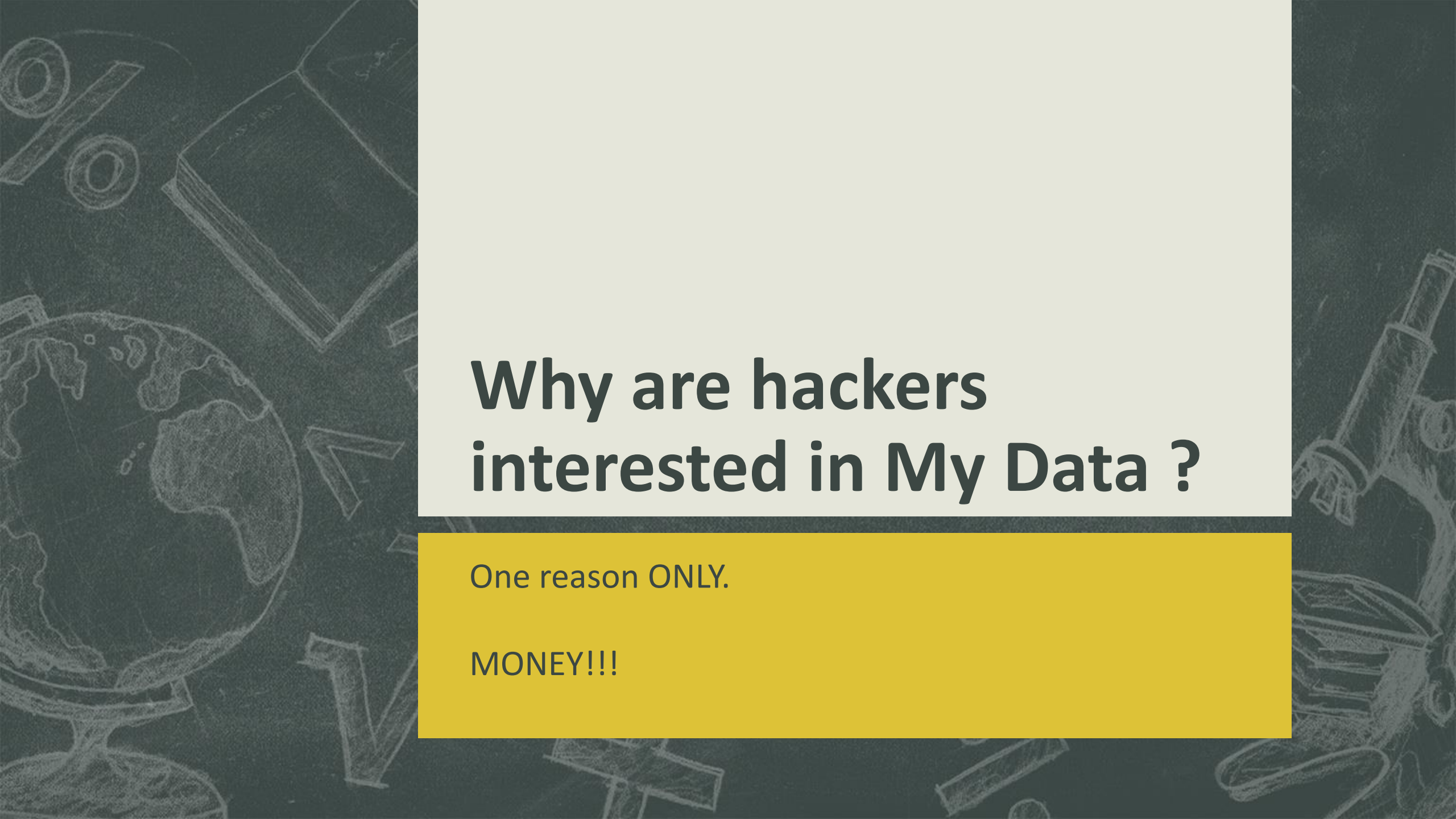
info@carefreecomputing.com

Providing Managed Services for Small Businesses Including Law Offices and Accounting Firms, etc. in the USA 866-377-6275 ext. 8

info@carefreecomputing.com

How to Remove Malware and Bot Net software from your computer system

By Carefree Computing Inc. info@carefreecomputing.com or call 866-377-6275 ext. 8



Why are hackers interested in My Data ?

One reason ONLY.

MONEY!!!

Why is this happening ? And how can I stop this problem from occurring again ?

- When you click on links or files that are in emails, your computer can be compromised. Hackers can take advantage of you when you are in a hurry. Stop and think twice, “Is this something I requested?”
- Outdated versions of Java®, Flash Player® and Adobe Reader® allow Malware to be secretly installed on your computer system.
- Security updates for Windows need to be run at least once a month to ensure you have the latest patches and fixes from Microsoft®. **Firefox® , Chrome® or Opera®** are alternative’s to Internet Explorer®. Try these browsers and see if you like their performance and security features.
- Antivirus programs need to be current as well. Free versions of antivirus programs provide minimal protection and should be used with caution. We recommend registering your antivirus program and using the full versions and not the “free” software. Read all available information regarding your choice for antivirus protection.

Now lets get started. Step One.

Registry Roll Back is the first way to get your system back to normal from infection.

- Most people don't know that this is the first line of defense in restoring your system to its last known good working state.
- First: Use the F8 Key when you restart and choose Safe Mode.
- Second: When your system asks you to roll back, select two weeks prior to your infected state.
- This will NOT change or alter your documents or email.

First Step – Roll Back your System Registry

- If you know when this happened, reboot in Safe Mode and roll back your settings to a couple of weeks prior to this happening. This is the easiest and fastest way to clean your system. If you don't know when this attack occurred, then lets go to the next step.

Step Two: Your computer is still infected and you have the problem reoccurring.

Malware comes in over 2 Million varieties.

- Since the first virus in 1971 to infect the military network ARPANET. Now we have over 2 million Trojans, Viruses, Worms throughout the Internet. Now we have Bot Nets that combine the forces of millions of computers to compromise systems that are unprepared for this type of attack.

Second Step

- Download Malware Bytes® from Download.com. If you use other spyware removers they can be less reliable. Carefree Computing Inc. always recommend starting with Malware Bytes® FIRST. Install it, update it and run it 2 or 3 times till you get a clean bill of health. But don’t stop here.

Step Three: If you got a positive reading from Malware Bytes check for Bot Nets next.

Bot Nets are the hardest to find and need a multi level approach to find them.

- As of March 2014, we are finding more and more ways to scan for Bot Nets. Carefree Computing has 4 different tools in this presentation to assist you in finding out if you are infected or not. It is the most dangerous and most difficult thing to discover you are infected.

Third Step

- Bot nets are much harder to find.
- We use 4 other scanners for Bot Nets.
- Trend Micro® RUBottedSetup.exe. This file is available at www.download.com.
- Install and run this file. It will require a reboot of your computer and will run in your system tray. This is the first step to cleaning your system.

Step Four: Run TDSS Killer from Kaspersky Labs

Kaspersky Labs has a great tool for discovering Bot Nets

- We find that using several scanners for Bot Nets is the best approach to ensuring that your computer system is free of remote control software by hackers.

Fourth Step:

- TDSSkiller® is a tool offered by Kaspersky Labs® to help clean bot nets from your computer. Find it at : http://usa.kaspersky.com/downloads/tdsskiller

Step Five: Run Malware Bytes® Root Kit Scanner

Malware Bytes® has developed a Root Kit Scanner that keeps updating for the latest Bot Net threats.

- If your computer comes up positive for a Bot Net, we recommend rebuilding your system from scratch. This will ensure that your system is once again safe and secure from hackers.

Fifth Step:

- Malware Bytes Root Kit Scanner is a new utility put out by the famous Malware Bytes Corporation®. Find it at Download . Com Search for Malware Bytes.

Step Six: Update your Java® Program

Update your Java Program

- Remove old versions of Java®. They have security issues that allow your computer to be compromised while browsing the web.
- If you find any versions of Java 5 -7, remove them from your computer system. Go to Oracle® and get the latest version of Java.

Sixth Step:

- See what version of Java you are currently running. If you are running anything but the latest, Version 8, of Java by Oracle®, remove them all and install Java 8 found at www.java.com
- Java has been improved to resolve the issues of using it to compromise your computer.

Step Seven: Update your Flash Player®

Old versions of Flash Player® are also responsible for threats to your computer system.

- Flash Player® Version 13 is now secure. Remove old versions and upgrade to Version 13 on your computer to ensure a safe and secure browsing experience.

Seventh Step:

- Old versions of Flash Player® is currently one of the other major ways your computer can be compromised. You must always keep Flash Player® updated to not be vulnerable to computer attacks. Get it at www.flash.com.

Step Eight: Update your Adobe Acrobat Reader®

Adobe Acrobat Reader® needs to be updated to be safe.

- Adobe Acrobat Reader® was once thought to be impervious to attacks. It is important that you keep this critical software program updated on your PC to ensure that it is not used to install Malware on your computer.

Eighth Step:

- Adobe Reader ® has vulnerabilities: Download it at www.adobe.com . If you are using older versions of Acrobat Standard® or Acrobat Pro®, consider upgrading these older software programs for the latest security updates. Adobe® offers competitive pricing for Acrobat Standard and Pro updates.

Step Nine : If you got a positive reading from Malware Bytes check for BHO's next.

Browser Helper Objects are found using HijackThis .

- HijackThis is a utility that scans plugins in your browser. This tool will find hidden programs that launch and reinfect your computer system. Most plugins are not necessary and actually slow down the browser.

Ninth Step

- 1) Scan your browser with HijackThis© from sourceforge.net. Hijack This® takes skill in recognizing what could have infected your browser, (most of the plugins are not necessary), only remove the suspicious entries.

Use Malware Bytes Anti Exploit® protection for Browsers and applications.

Protect your Browsers and Programs with MB Anti Exploit.

- Anti Exploit® does what other programs cannot, it locks the ability for changes to occur in your settings.
- Anti Exploit® prepares the browser for unknown threats and runs on your computer to stop threats from modifying your computer system.

Install Browser protection with Malware Bytes Anti Exploit

- Protects Internet Explorer®, Firefox®, Chrome® and Opera® Browsers.
- Blocks unknown as well as common exploits. It doesn’t use a signature database- No need to update the software.

If all else fails : Call us to help you remove the Malware from your computer system.

Conclusion: Carefree Computing cannot guarantee that this will solve all problems. We are here to help you if you fail in removing the Malware from your system.

- If your system requires rebuilding we can assist you in this process.
- We hope that this helps protect the millions of computer systems on the Internet from getting infected.

If All Else Fails:

Call Carefree Computing, Inc. for a consultation. We will tell you our assessment and what it would cost for the removal of the malware from your system.

1-866-377-6275 ext. 8 or send an email at info@carefreecomputing.com