Viruses and Malware

Instructor: Daniel Chong Email: dchong@mybpl.org

Course Objective: To cultivate an understanding of how you can protect your computer, while browsing the internet, from viruses and malware.

Outline:

- Viruses and Malware, What Are They?
- Common Types of Malware and Viruses
- Common Ways People Infect Their Computer
  - High Risk Websites
- How To Tell If You've Been Infected With Malware
- Preventative Measures
  - Anti-Virus Software
  - Ad-Blocker
  - Link Safety and Good Password Habits
  - Backup, Backup, Backup!
  - Firewall
- Q/A

Viruses and Malware, What Are They?

It used to be that "Virus" was used as the encompassing term for anything that affected your Computer, this has changed and now the over-arching term used in the industry is Malware.

Malware blankets all types of programs that mean to cause your computer harm; be it: Viruses, Spyware, Ransomware, etc… but these can each be broken down a little bit more and it comes down to two different categories: ***Infection/Delivery Method and Actions.***

Common Types of Malware and Viruses

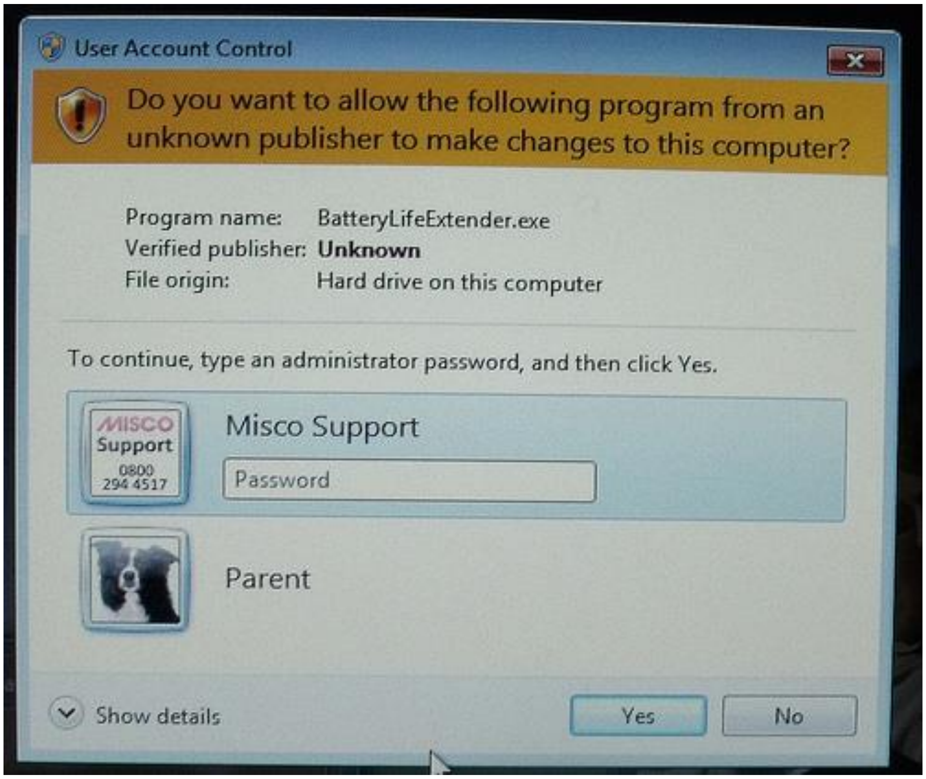
Infection and Delivery Methods

- *Virus* – We use the word "virus" to describe a program that self-replicates after hooking itself onto something that is running on Windows.

For example, one type of virus, called a Macro-Virus, will specifically attach itself to Office programs to infect and corrupt files of those types.

- *Worm* – A worm is another kind of self-replicating program, but worms generally are small, independent programs that run in the background of your system.

- *Trojan* – This is software that you thought was going to be one thing, but turns out to be something bad. Named for the fabled “Trojan Horse” that appeared to be a gift but in fact carried a dangerous payload.



User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

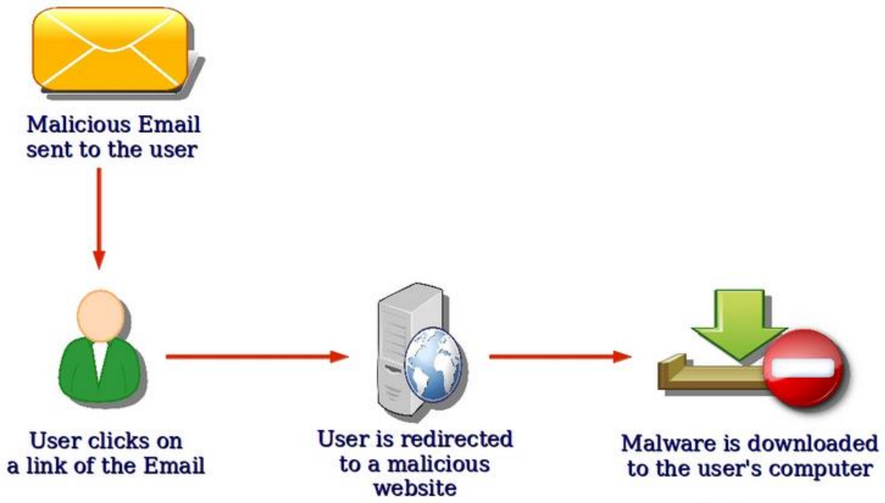
Program name: BatteryLifeExtender.exe
Verified publisher: **Unknown**
File origin: Hard drive on this computer

To continue, type an administrator password, and then click Yes.

For example, you notice that your battery life on your laptop has decreased significantly, so you scour the web and behold! You have found the mythical Battery Life Extender. So you install it and don’t think about it. It seems to work so you let it sit on your computer. This could potentially carry harmful malware to your computer! Always check who the download comes from and only install things from publishers that you know and trust.

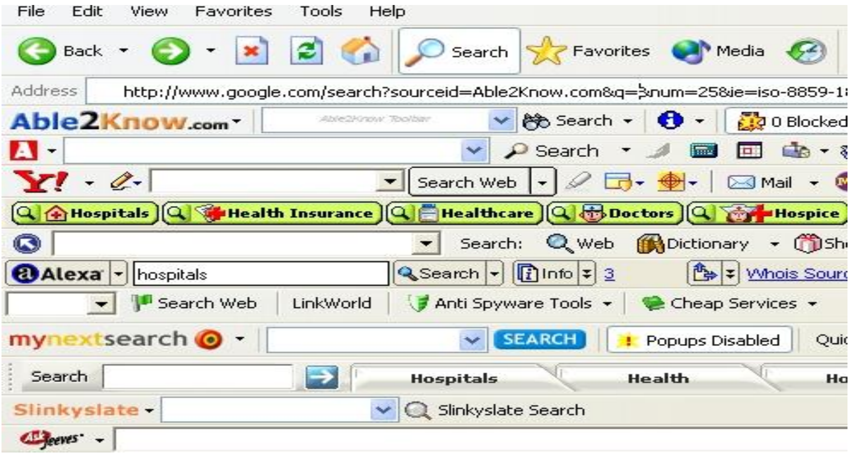
- *Drive-by Download/Email Phishing* – **Probably the most popular way to get something nasty on your computer**. This occurs from visiting a bad web page or clicking a malicious link in an email. That web page(s) exploits a weakness in your browser and causes your system to become infected.

Phishing is when you are targeted with an email asking you to enter in personal information in the hopes of stealing your identity or gaining access to accounts. Phishers usually attempt to pretend to be a legitimate company, such as Microsoft.

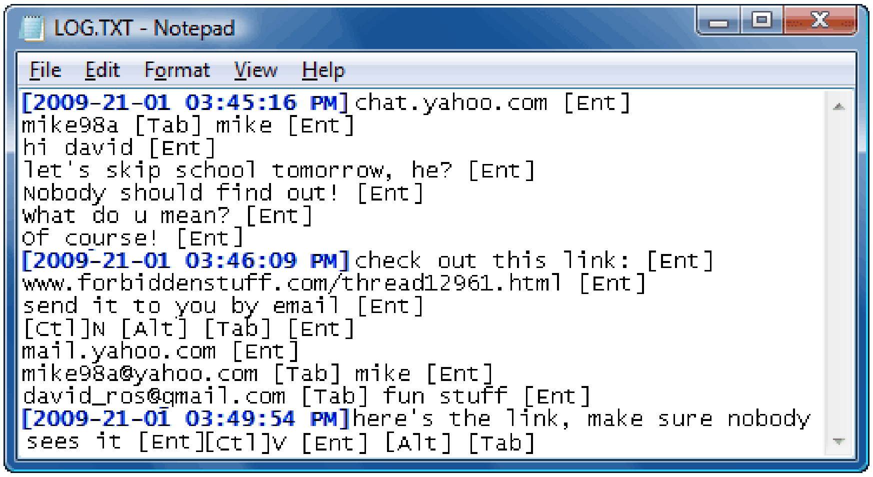

Malicious Email sent to the user
User clicks on a link of the Email
User is redirected to a malicious website
Malware is downloaded to the user's computer

Malware Actions

- *Adware* – While it is not truly malware and almost never delivered using one of the methods above, this type of malware can be very annoying. Adware is software that uses some form of advertising delivery system. Sometimes the way that advertisements are delivered can be deceptive in that they track or reveal more information about you than you would like. **Most of the time, you agree to the adware tracking you when you install the software that it comes with**. Generally, it can be removed by uninstalling the software it was attached to.

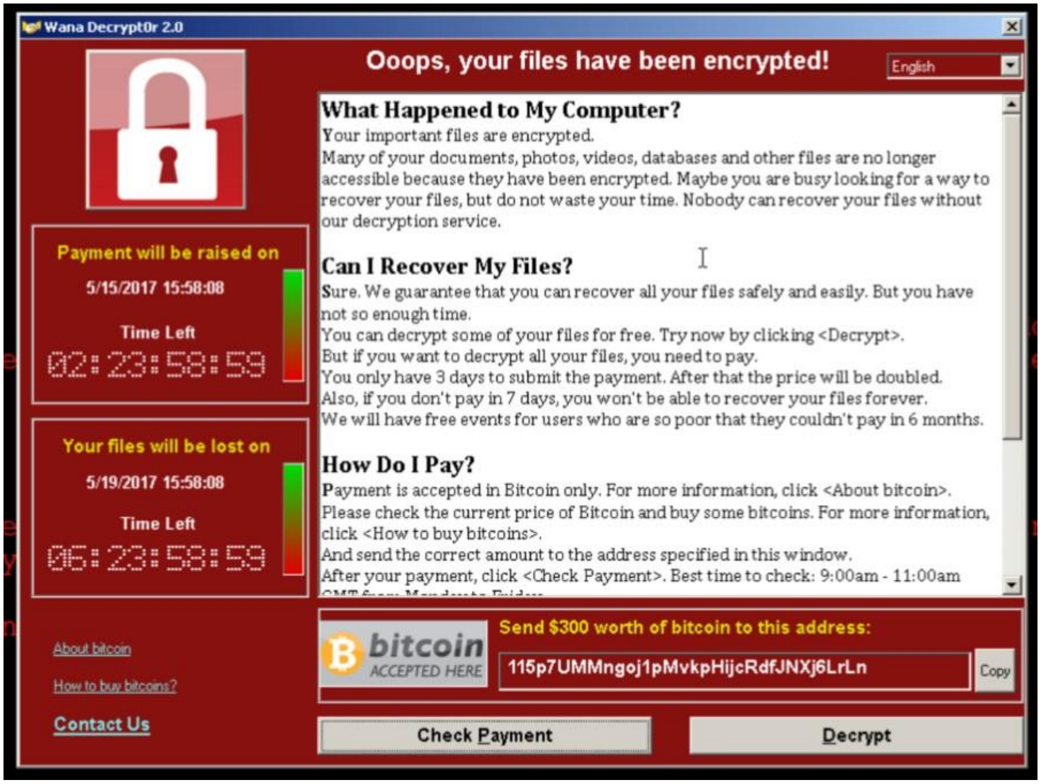


- *Spyware* – This software monitors your computer and reveals collected information to an interested party. This can be benign when it tracks what webpages you visit; or it can be incredibly invasive when it monitors everything you do with your mouse and keyboard.



```
[2009-21-01 03:45:16 PM]chat.yahoo.com [Ent]
mike98a [Tab] mike [Ent]
hi david [Ent]
let's skip school tomorrow, he? [Ent]
Nobody should find out! [Ent]
What do u mean? [Ent]
Of course! [Ent]
[2009-21-01 03:46:09 PM]check out this link: [Ent]
www.forbiddenstuff.com/thread12961.html [Ent]
send it to you by email [Ent]
[Ctl]N [Alt] [Tab] [Ent]
mail.yahoo.com [Ent]
mike98a@yahoo.com [Tab] mike [Ent]
david_ros@gmail.com [Tab] fun stuff [Ent]
[2009-21-01 03:49:54 PM]here's the link, make sure nobody
 sees it [Ent][Ctl]V [Ent] [Alt] [Tab]
```

- *Ransomware* – **Lately a very popular way for Internet criminals to make money. This malware is truly the worst in the bucket.** It alters your system in such a way that you're unable to get into it normally while also encrypting your files. It will then display some kind of screen that demands some form of payment to have the computer unlocked. Access to your computer is literally ransomed by the cyber-criminal.



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59

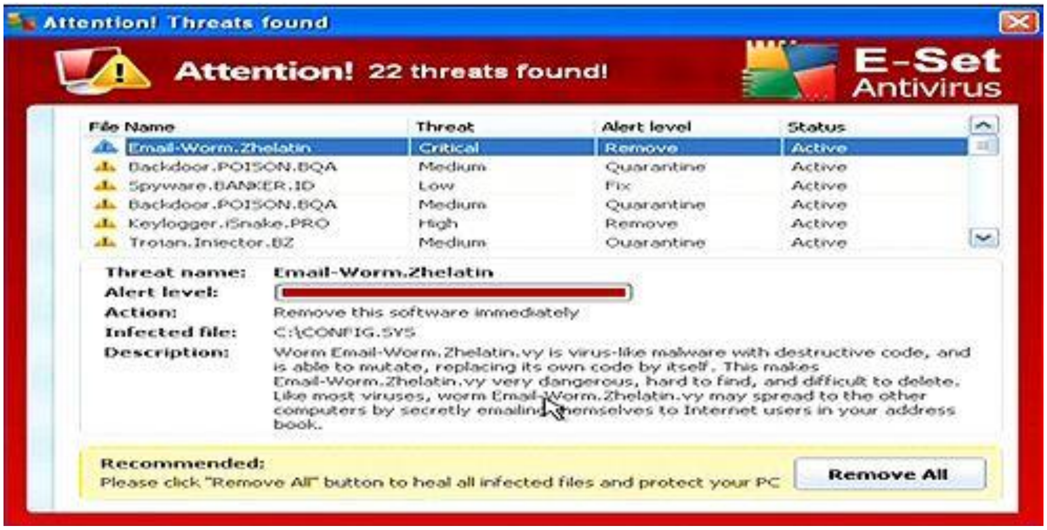
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

- *Scareware* – This software appears to be something legitimate (usually masquerading as some tool to help fix your computer) but when it runs it tells you that your system is either infected or broken in some way. This message is generally delivered in a manner that is meant to frighten you into doing something. The software claims to be able to fix your problems if you pay them.



Attention! Threats found

Attention! 22 threats found!

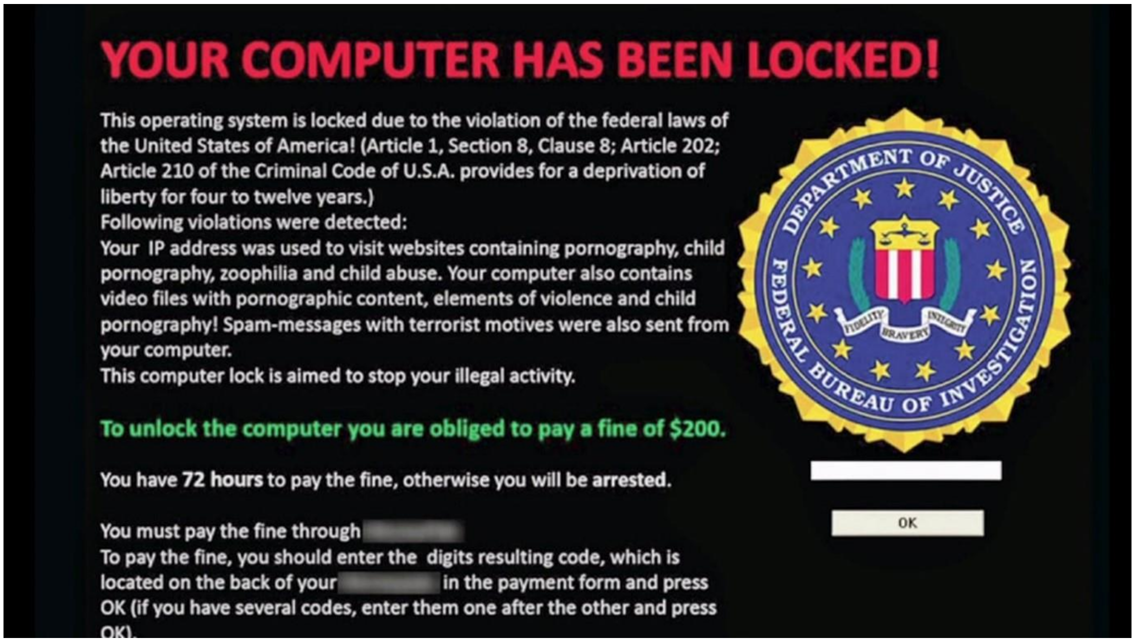
E-Set Antivirus

File Name	Threat	Alert level	Status
Email-Worm.Zhelatin	Critical	Remove	Active
Backdoor.POISON.BQA	Medium	Quarantine	Active
Spyware.BANKER.ID	Low	Fix	Active
Backdoor.POISON.BQA	Medium	Quarantine	Active
Keylogger.iSnake.PRO	High	Remove	Active
Trojan.Injector.BZ	Medium	Quarantine	Active

Threat name: Email-Worm.Zhelatin
Alert level:
Action: Remove this software immediately
Infected file: C:\CONFIG.SYS
Description: Worm Email-Worm.Zhelatin.vy is virus-like malware with destructive code, and is able to mutate, replacing its own code by itself. This makes Email-Worm.Zhelatin.vy very dangerous, hard to find, and difficult to delete. Like most viruses, worm Email-Worm.Zhelatin.vy may spread to the other computers by secretly emailing themselves to Internet users in your address book.

Recommended:
Please click "Remove All" button to heal all infected files and protect your PC

Another form of Scareware are false accusations from the "FBI" or another government agency, saying that you have been doing all things terrible on your computer and if you don't pay them $200 dollars they will come and arrest you. This is never the case as a government agency needs a warrant to do anything to your personal property.



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

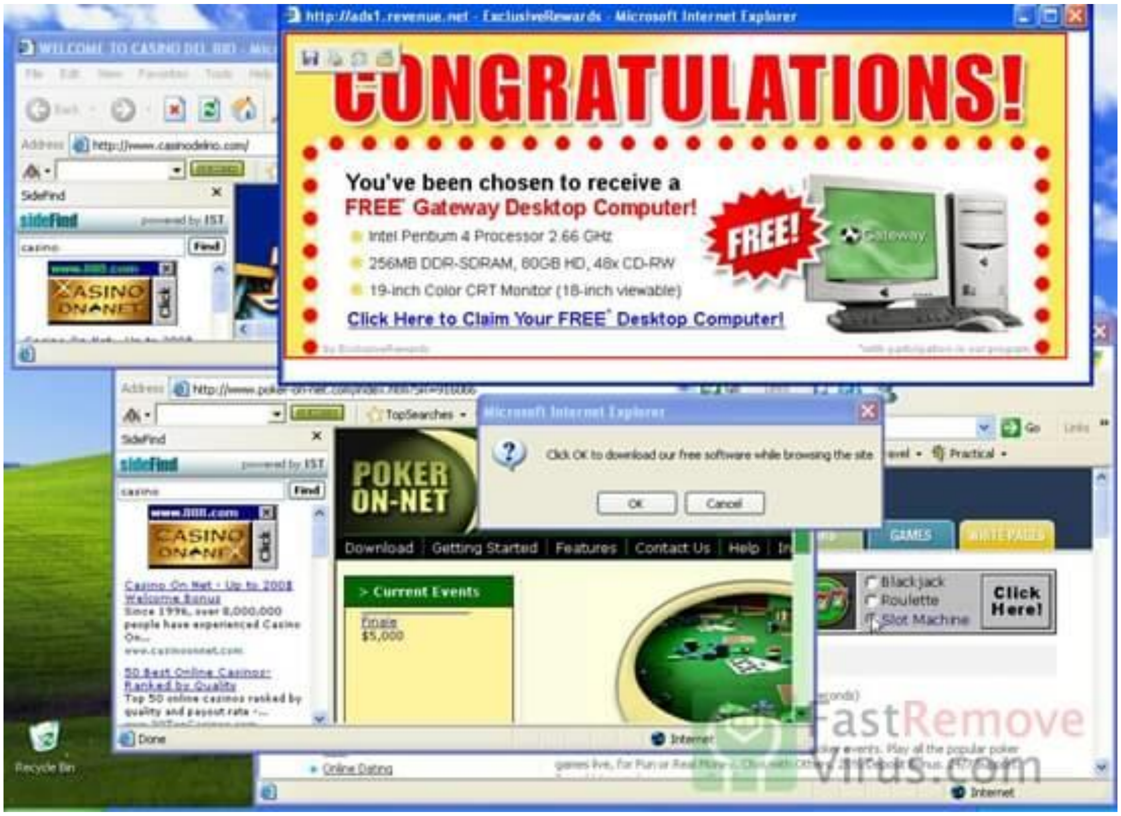
Common Ways People Infect Their Computer

There are many different ways that your computer system could become infected with malware. Some of the most common are:

- Permission is given by the User!
- Phishing Attempts
- Clicking on a link without looking where it is going.
- Outdated Programs i.e. Adobe Flash or Java.
- Downloading Movies or Music via Torrent Websites.

How to Tell If you've Been Infected with Malware

There are some tell-tale signs that you have become infected with malware but don't let that fool you. Sometimes your system could be running completely normal and you may still have malware installed on your computer. Usually though if one or more of these symptoms appear, you will want to scan your computer for viruses.



http://ads1.revenue.net - ExclusiveRewards - Microsoft Internet Explorer

CONGRATULATIONS!

You've been chosen to receive a FREE* Gateway Desktop Computer!

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)

Click Here to Claim Your FREE* Desktop Computer!

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

Casino On Net - Up to 200$ Welcome Bonus
Since 1996, over 8,000,000 people have experienced Casino On...
www.casinoonnet.com

50 Best Online Casinos: Ranked by Quality
Top 50 online casinos ranked by quality and payout rate -...

- You receive Ransom Demands. (Ransomware) **Note: <u>THIS IS A VERY SERIOUS ISSUE!!</u>**
- Significant decrease in performance/speed. (General Malware)
- Popups Everywhere! (Adware)
- You keep getting redirected to random webpage(s) in your browser. (Adware)
- An Unknown App keeps sending Messages i.e. "YOUR COMPUTER IS INFECTED WITH 1,502 MALICIOUS PROGRAMS! CLICK HERE >>>> TO CLEAN YOUR INFECTED SYSTEM!" (Scareware)
- Mysterious posts to your Social Media accounts with Links attached to them. (Spyware)
- System Tools are unresponsive i.e. Task Manager or Registry Editor. (Rootkit)

Preventative Measures

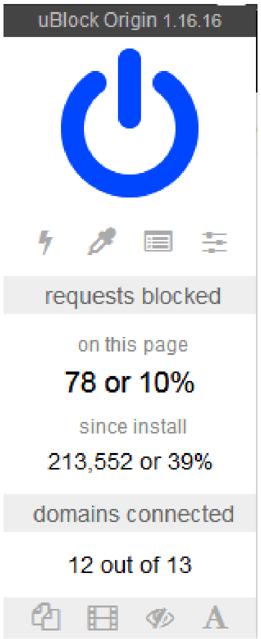
The best way to prevent malware is actually you! Just by being here tonight you have become aware of all the ways these things may get onto your system and by actively looking out and keeping a watchful eye, you will be able to prevent MOST malware that you see today. Now that isn't to say you shouldn't be extra careful and take every step you can to secure your computer, and in this section we will be going over those extra steps you could take. The first of which is having an active Anti-Virus Software running on your computer.

Anti-Virus Software

If you have a Windows Computer it will come pre-loaded with Windows Defender, this is Microsoft's built in Anti-Virus Software. This will 9 times out of 10 do the job, especially when it is run in conjunction with a third-party Anti-Virus Software. There are a lot of third-party Anti-Virus Solutions that you can use, and a lot offer free versions. One of the best is Malwarebytes (Which we use here in the Library for malware removal) which offers free and premium versions. The free version can be used to remove malware **IF** you have already become infected, while the premium version will actively scan your system for any threats. Among other Anti-Virus Software solutions there are (in no particular order or preference):

- Norton
- Bitdefender
- ESET
- Avira

Note: Many of these offer free and premium solutions but the free ones can come with some strings attached so do your research! Compare Anti-Virus Solutions here! https://www.av-test.org/en/antivirus/home-windows/



uBlock Origin 1.16.16

requests blocked

on this page

78 or 10%

since install

213,552 or 39%

domains connected

12 out of 13

Ad-Blocker

In today's day and age we are constantly bombarded with ads, some of these ads can be malicious! So why not protect yourself with an ad-blocker? You can add these extensions on to any browser and they are free-open source software that is released to the public. The overall best rated ad-blocker is called **uBlock Origin**. Along with ad-blockers you can also use anti-tracking extensions or even some that will not allow any sort of script run over the internet without your permission.

Note: Anti-Script Extensions can sometimes "break" the webpage you are viewing. Although they make your computer secure by not allowing any sort of JavaScript to run on your computer, many websites rely on JavaScript to present their content to you. This is where the fine line of convenience and security meet.

Link Safety and Good Password Habits

Link Safety

Knowing where a link is going to take you can be the difference between getting malware on your computer and keeping your computer secure.

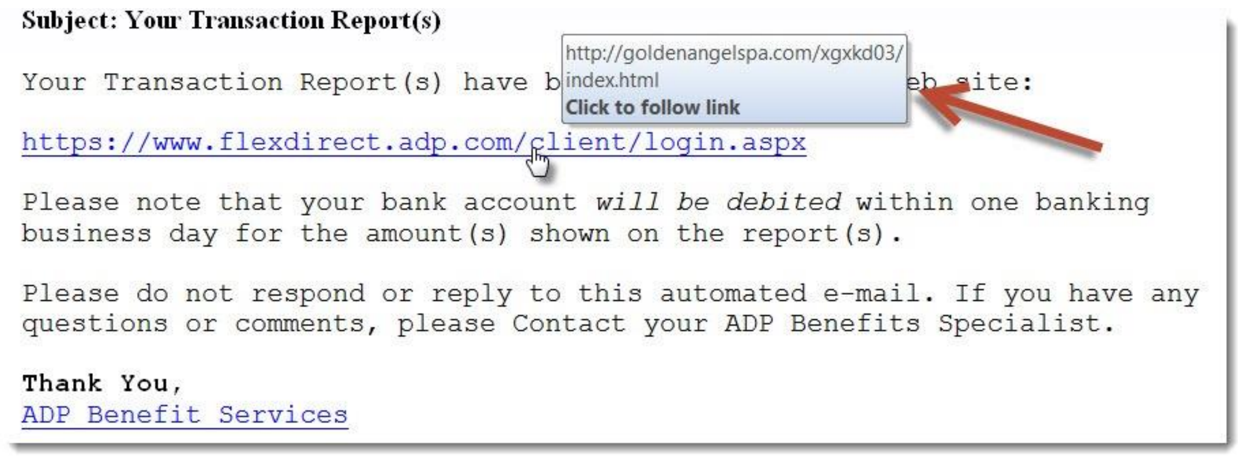
For instance we all know that https://www.google.com will take us to Googles homepage.

Even though a link in an email may look like it is going to the place it says, it is incredibly easy to make a link say one thing but take you somewhere completely different.

When you are sent a link, think before you click. If you hover over a link without clicking, the destination of that link will either appear under your cursor OR on the bottom left side of your browser/email client.

Never login to a banking website from a link provided in an email!

Notice in this Phishing Attempt where the actual link goes.



Subject: Your Transaction Report(s)

Your Transaction Report(s) have b eb site:

http://goldenangelspa.com/xgxkd03/index.html
Click to follow link

https://www.flexdirect.adp.com/client/login.aspx

Please note that your bank account *will be debited* within one banking business day for the amount(s) shown on the report(s).

Please do not respond or reply to this automated e-mail. If you have any questions or comments, please Contact your ADP Benefits Specialist.

Thank You,
ADP Benefit Services

Keep an eye out for country codes! If you see them at the end of a link know that you will be visiting a website from another country.

- Australia (.au)
- China (.cn)
- Czech Republic (.cz)
- France (.fr)
- Germany (.de)
- Japan (.jp)
- Russia (.ru)
- United Kingdom (.uk)

Good Password Habits

You probably hear about it in the news often enough, there are data breaches every day. Over 700 million records were compromised in 2015 alone. To prevent yourself from falling victim to identity theft, fraud and other things you will want to make sure you practice good password keeping habits. These include:

- **Never** use important dates from your life as a password
- **Never** use family names as a password
- **Never** use the same password for all login information
- Change your password every month
- Use a password manager (wallet) to keep all passwords secure *

*This is advanced, only use after doing thorough research on how it works.

Backup, Backup, Backup!

When I was learning how to take care of my own finances, I was told so often to: “save for a rainy day, you’ll never know when you’ll need it.”

The same can be said about backing up your computer’s files. This will prevent you from losing all your precious files (family photos, tax documents, work documents, etc…) and can make the process of getting back on your feet after a malware attack that much easier.

Create a System Restore Point by: hitting the windows key and searching for System Restore and following the Wizard setup. This will allow you to take a snap shot of how your computer is at that moment and restore it to that point.

External Hard Drives

The most reliable way to back up your files is to purchase an external hard drive. These can be found for a myriad of prices, but a 1TB SSD will set you back around $60-$80. This is an extremely good investment as not only can it save you from a malware attack that locks your computer, but incase a hardware component fails you will still also have your files.

Cloud Services

Other ways to do this include services like Google Drive and Dropbox, these will offer you 15GB of storage free of charge, and upgraded premium versions with unlimited storage for a monthly fee.

This can also come back to bite you if you’ve set them up to auto-sync your files. **Due to the nature of auto-sync if one of you files on your computer gets changed (i.e. corrupted by malware), then it will automatically back that corrupted file up to the cloud service. When you go to restore, your files will still be corrupted.**

Note: This can also happen with an external hard drive, but is less common.

Firewalls

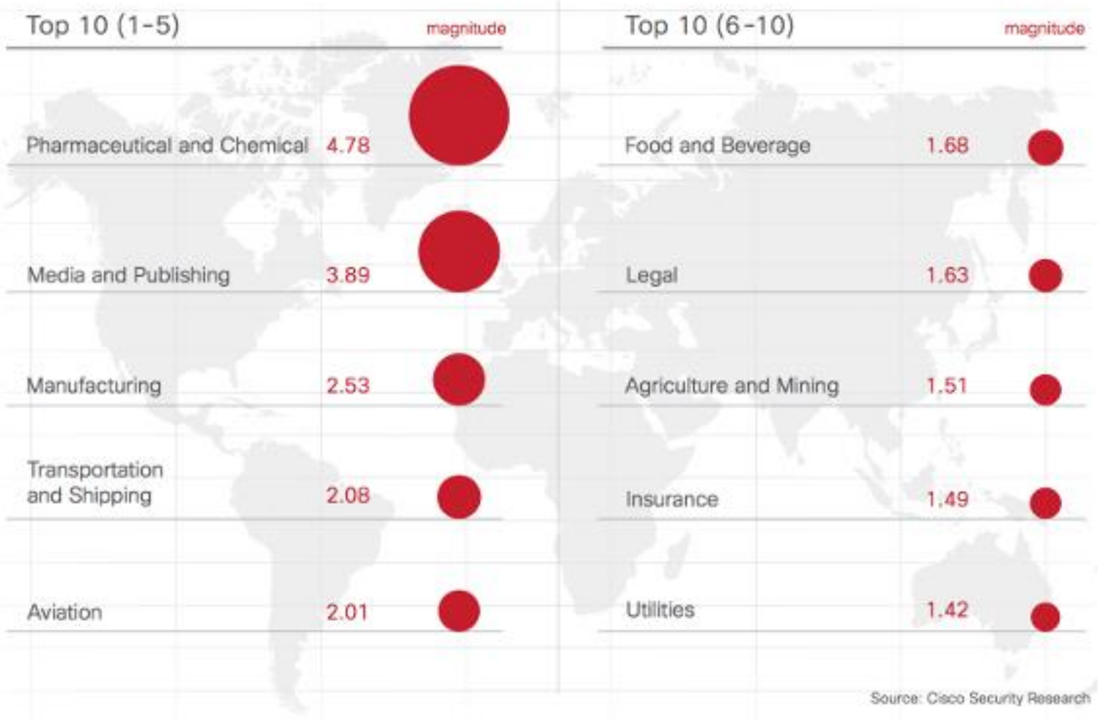
Think of a firewall as a filter for your computer. This feature comes standard on all Windows Devices, most routers, and antivirus software. This feature on a Windows device is called “Windows Firewall” and can be found under the **Control Panel >> Systems and Security.**

When it first came out it was often considered buggy and rather basic for a firewall, offering a lot of compatibility issues. Now, in conjunction with Windows Defender and a Second-Opinion malware sweeper (Malwarebytes Free) Windows Firewall will keep you protected from most malware on the internet.

You might be asking yourself, “What’s the difference between a firewall and anti-virus solution?” The answer is actually simple, a firewall will allow you to filter what kind of traffic (data) you want to allow onto your computer AND from whom. While an anti-virus actively scans and removes any malware that actually gets through your firewall set up.

High Risk Websites (Cisco Study)

Figure 9. Vertical Risk of Web Malware Encounters,
All Regions, January 1 – November 15, 2014



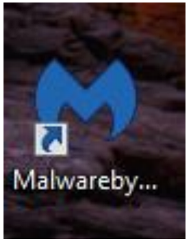
Source: Cisco Security Research

Perform a Scan/Removal of Malware (Follow-Along)

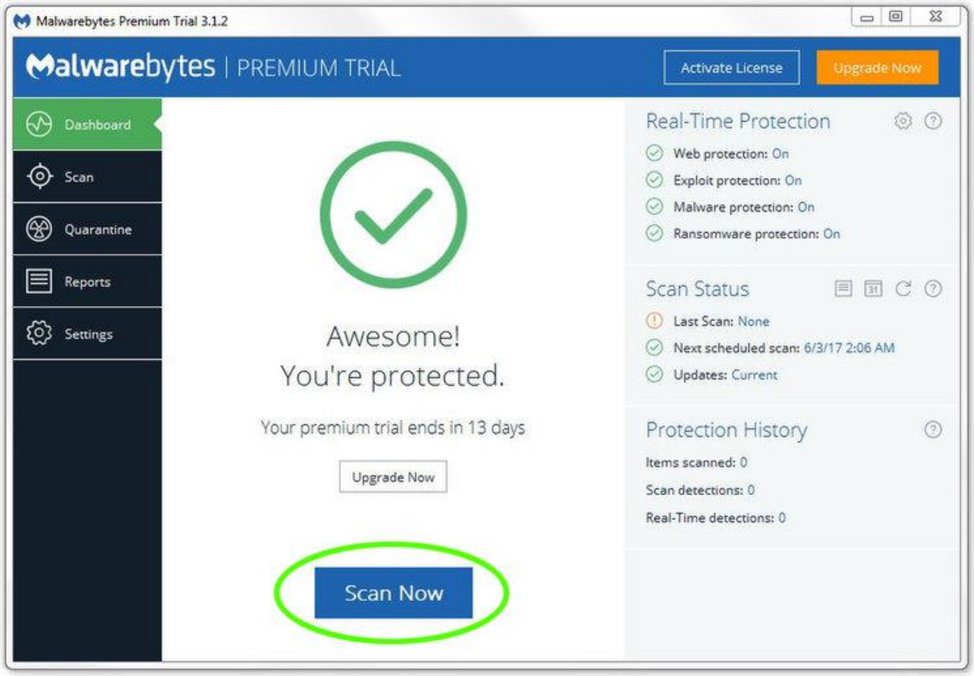
The software that we use for the removal of malware here at the library is called Malwarebytes. It can be found, for free, here: https://www.malwarebytes.com/ As our computers here at the library already have the software that we are going to use to scan our system installed we will not be going over how to install it. If you are interested in using this utility software but are unsure how to install it then you can follow the full guide here: https://www.tomsguide.com/us/malwarebytes-how-to,news-18841.html

Now onto how to scan your computer using Malwarebytes

1. Open Malwarebytes using the desktop shortcut.



2. It will now open to the Dashboard Screen. From here you can see the status of your last scan, and navigate the side ribbon which we will cover in a moment. You will want to hit the blue "Scan Now" button at the bottom of the window.



Awesome!
You're protected.

Your premium trial ends in 13 days

Real-Time Protection

Web protection: On
Exploit protection: On
Malware protection: On
Ransomware protection: On

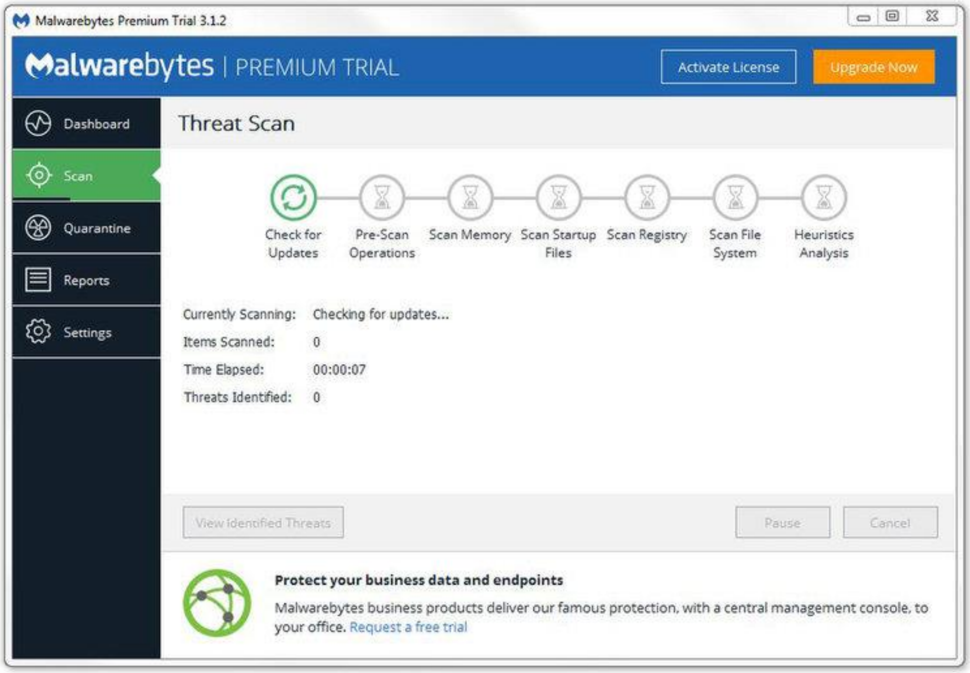
Scan Status

Last Scan: None
Next scheduled scan: 6/3/17 2:06 AM
Updates: Current

Protection History

Items scanned: 0
Scan detections: 0
Real-Time detections: 0

3. After hitting the scan button you will be directed to the “Threat Scan” which is located in the “Scan” portion of the left-side ribbon; one below the “Dashboard”, This will run for a bit depending on how many scans you have performed. The initial run could take anywhere from 10 minutes to 30 minutes.



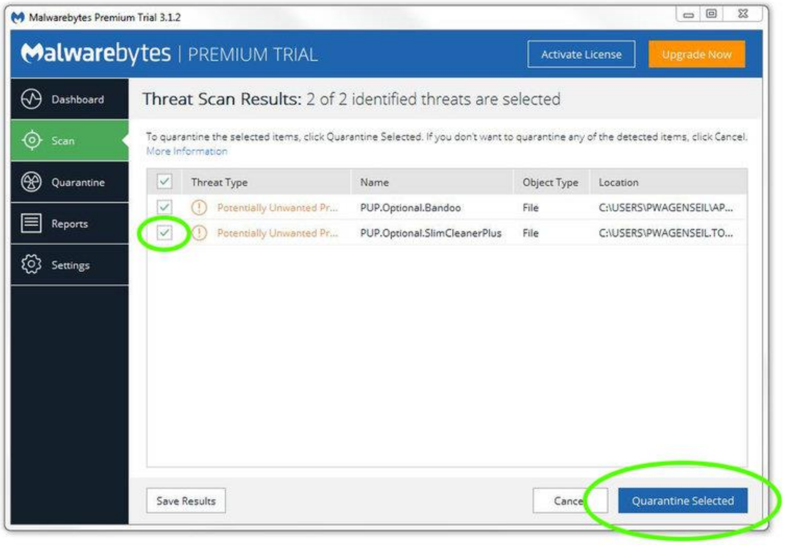
Threat Scan

Currently Scanning: Checking for updates...
Items Scanned: 0
Time Elapsed: 00:00:07
Threats Identified: 0

Protect your business data and endpoints

Malwarebytes business products deliver our famous protection, with a central management console, to your office. Request a free trial

4. After the scan finishes, you will want to review the results of the scan. It will tell you if you have any “Potentially Unwanted Programs” (PUPs) or Malware. By default everything that is flagged in the scan is checked for “Quarantine.” If you believe there is a false positive program you can uncheck it before quarantining the rest. If not you will hit the blue “Quarantine Selected” button at the bottom right of the window.

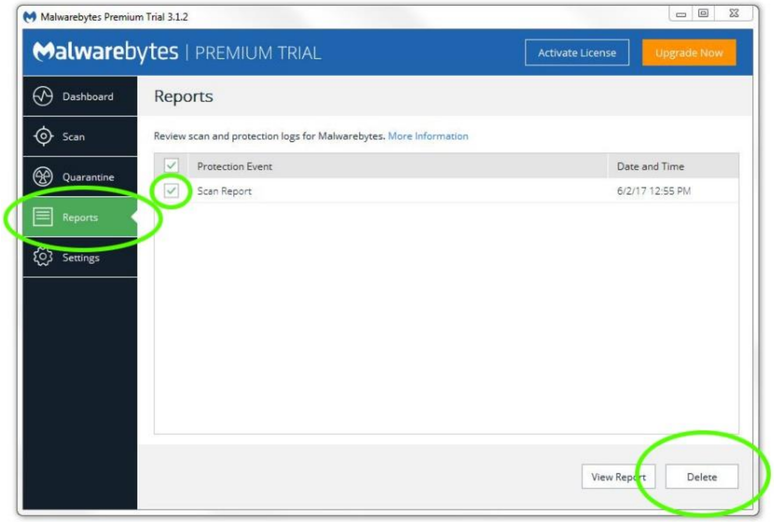


Threat Scan Results: 2 of 2 identified threats are selected

To quarantine the selected items, click Quarantine Selected. If you don't want to quarantine any of the detected items, click Cancel.

☑	Threat Type	Name	Object Type	Location
☑	Potentially Unwanted Pr...	PUP.Optional.Bandoo	File	C:\USERS\PWAGENSEIL\AP...
☑	Potentially Unwanted Pr...	PUP.Optional.SlimCleanerPlus	File	C:\USERS\PWAGENSEIL.TO...

5. If you would like to see a detailed report of the scan and what it found you can navigate to the “Reports” section on the left side ribbon. You can choose to view or delete the report.

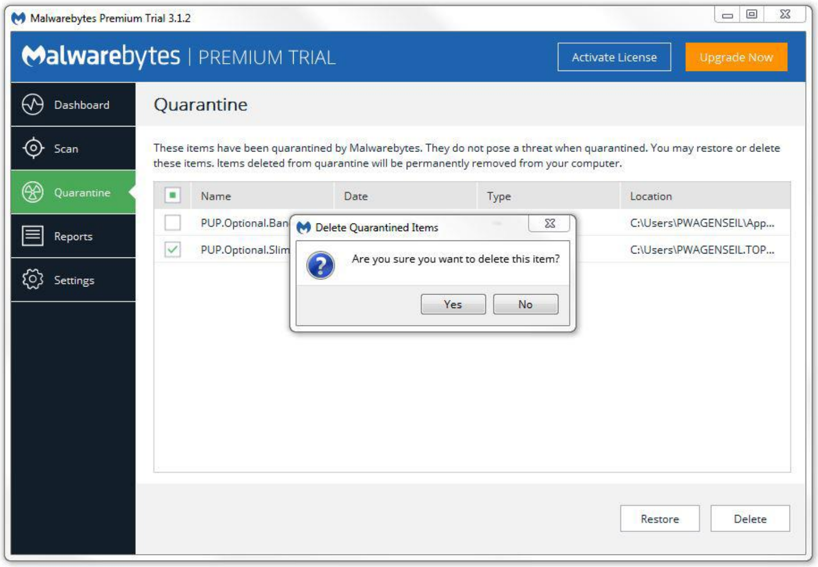


Reports

Review scan and protection logs for Malwarebytes. More Information

☑	Protection Event	Date and Time
☑	Scan Report	6/2/17 12:55 PM

6. Navigate to the quarantine section of the left-side ribbon. Now that our potential malware is safely quarantined from the rest of the system, we can remove them from our computer.



Quarantine

These items have been quarantined by Malwarebytes. They do not pose a threat when quarantined. You may restore or delete these items. Items deleted from quarantine will be permanently removed from your computer.

■	Name	Date	Type	Location
☐	PUP.Optional.Ban			C:\Users\PWAGENSEIL\App...
☑	PUP.Optional.Slim			C:\Users\PWAGENSEIL.TOP...

Delete Quarantined Items

Are you sure you want to delete this item?

Yes No

7. Restart your computer to fully remove all the malware.