As you may already know, FAST RHINO provides a number of computer services to include virus & malware removal, traditional & wireless networks, data recovery and backup solutions, system sales and upgrades, hardware & software installations, preventative maintenance, PC training, and web development. Our computer store is located in the Mountain View Plaza shopping center at the Northeast corner of E. Rancho Vistoso Blvd. and Sun City Blvd. We've been at this location for about a year and a half now. We are really excited because this year, 2014, marks Fast Rhino's 10 year anniversary serving Northwest Tucson. I appreciate your interest in today's subject matter. Thank you for attending.

Some of you here may have attended a talk I gave back in November of 2012 to the computer club regarding fraudware. Since malicious software (aka malware) has taken center stage and become one of the most prominent concerns for computer users, I find script blocking to be one of the most important topics to share with you today.

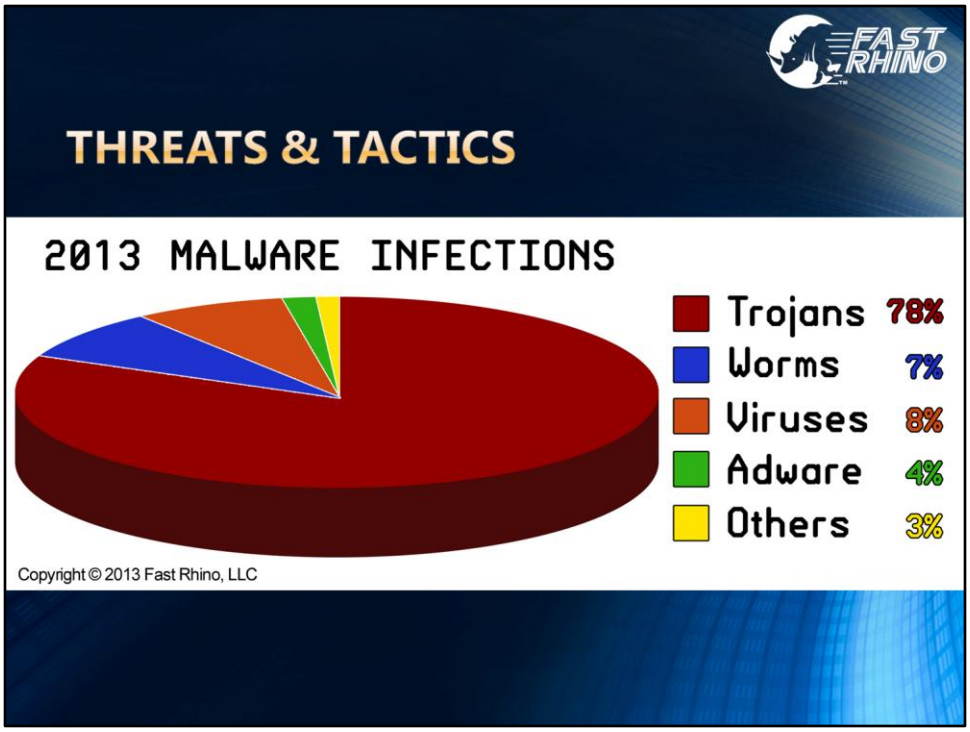
Fast Rhino has witnessed quite an evolution in the world of malware. It's unfortunate, but using the Internet today can be quite painful if you're not actively aware of the hidden dangers awaiting you. Hopefully, you can use some of today's information to help you become more knowledgeable in defensive browsing, while being able to identify the traps and avoid the repercussions.

Imagine getting in your car and driving down the highway in somewhat heavy traffic. You've got a few things on your mind, but overall, you are staying cautious and aware of the other drivers around you. Luckily, you are able to avoid this oncoming 18 wheeler as it pulls into your lane.

The difference between defensive driving and defensive browsing is that the other drivers on the road are not intentionally trying to kill you (that is, unless you are driving in Phoenix). Malware threats are definitely out to get you and unless you are practicing defensive strategies, they will succeed.

If I haven't yet mentioned it, there is a war going on out there.
And to win this war, what we need first is a defensive strategy.

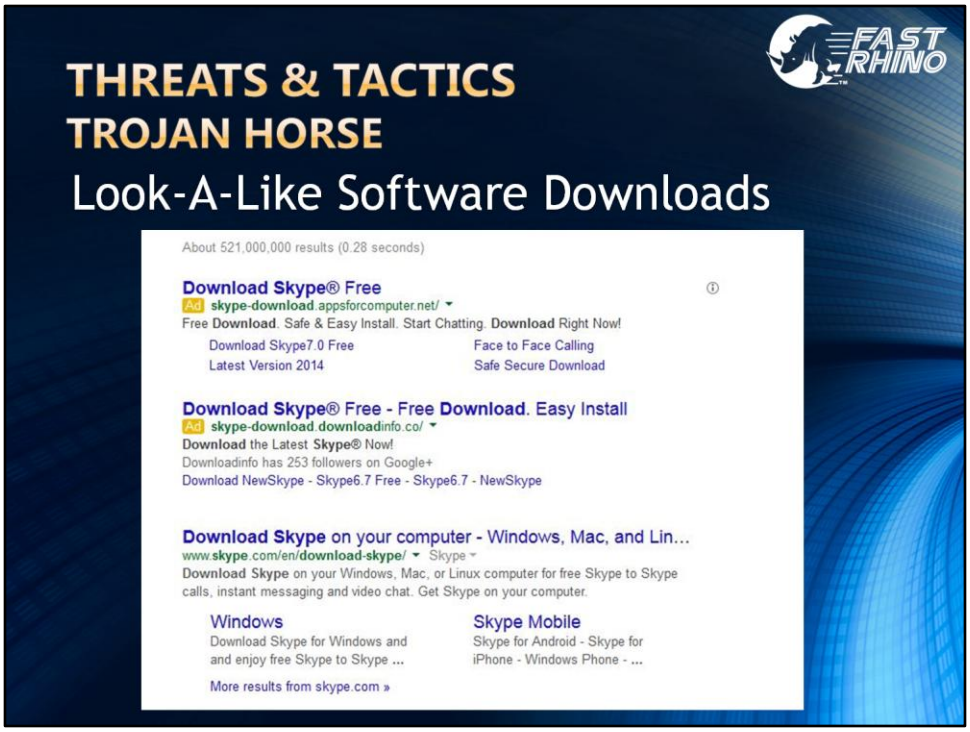
First we need to identify our enemy. We can do this by becoming better educated on the types of threats out there and get familiar with the ways they attack.
Next, we need to build a defensive shield to help protect us from these attacks.
Finally, we need to change the way we interact with the Internet. In case you didn't realize it, the Internet is evolving at in a dramatic way and very quickly. It is important that you adapt to these changes, as well.



Although this presentation is about script blocking, it's very important to identify some of the bad guys out there and how they operate. Malicious Software, or Malware is a term used to represent the entire universe of computer threats. Specifically, it is defined as any software that is intended to damage or disable computers and computer systems. When people think of computer infections, they identify mostly with viruses, but viruses are merely a small piece of the Malware pie. In fact, this past year, we've seen a massive increase in the number of Trojan infections, accounting for almost 80 percent of all infections. That's a huge number! So let's take a few moments and discuss Trojans.

The term Trojan, comes from the fabled story of the wooden horse used to deceive the defenders of Troy. What they thought was a gift, in fact, was merely a large container of concealed warriors. Computer Trojans often present themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.

There are numerous propagation tactics used to deploy these Trojan Horses. Some of these include:



Look-a-Like software downloads. Think you're downloading the genuine Skype program? You'd better make sure you're getting it from the official site. Today there are a growing number of web sites that are paying to be at the top of search results pages hoping you will quickly click on the link to download what you think is the official product. Instead, the program you download has a bundled package of malware that installs on your system without your knowledge.

Look-a-Like software downloads.

Here we see an ad claiming that you do not have Flash and in order to see the content, you need to download the HD Flash Player. This is not a genuine Adobe Flash notice. If you download and install this product you will have infected your system. This is true for both PC and MAC users, so be warned. Anytime you want to download or update a program you should go to the original manufacturer's site. Never trust an ad or any notice on a web site.

The Trojans found in these Look-a-Like downloads can manifest in various forms known as Potentially Unwanted Programs (otherwise referred to as PUPs) that include, but are not limited to names like Conduit, OneWebSearch, Delta Search, Babylon Toolbar, Mixi.DJ, & Snap.do The results of these types of infections can range from browser hijacking, cyber crime, invasion of privacy, or they can simply slow down the performance of your computer. One way to see if you have these, is to check your browser add-ons. Alternatively, you could also check your installed programs.

Remote Access Granted – It seems everyone by now should know about the fraudulent "I'm with Windows" telephone scam that attempts to con people into allowing remote access to their computers. Surprisingly, we hear of many people still getting tricked by this type of scam. The amazing thing is that this sort of theft not only occurs by a telemarketer initiating the call, it also can be done if you are the one initiating the call to what you think is a legitimate company's support line. Just because you read it on the Internet doesn't make it legit. There are a ton of imitators out there just waiting for you to allow them remote access to your system. If you do not know the person, do not allow them onto your computer… and even then, think twice about it.

E-mail Attachments – I don't think I have to remind you of the dangers of email attachments. Even hyperlinks within an email can point you to an infected web site. I just recently received this email with an attached HTML document. After checking out the source code, I could see a web form that looked quite legitimate from a coding perspective. Even though I do not have a Schwab account, I know that financial organizations do not practice these types of communications as a matter of policy. Never click on any attachment or link within an email unless you are absolutely sure about it.

To continue a bit further regarding E-mail Attachments - One of the most insidious infections being sent via email today is CryptoLocker, a ransomware Trojan that first surfaced in September 2013. This nasty payload installs itself in the Documents and Settings folder with a random name, and adds a key to the registry that causes it to run on startup. It then attempts to contact one of several designated command and control servers; once connected, the server then generates a 2048-bit RSA key pair, and sends the public key back to the infected computer. That's military grade encryption, folks. It would take decades to decrypt. The payload then proceeds to begin encrypting files across local hard drives and mapped network drives with the public key, and logs each file encrypted to a registry key. The process only encrypts certain personal data files. The payload then displays a message informing the user that files have been encrypted, and demands a hefty payment through an anonymous pre-paid cash voucher like MoneyPak, or an equivalent amount in Bitcoin. Due to the length of the key employed by CryptoLocker, experts considered it practically impossible to use a brute-force attack to obtain the key needed to decrypt files without paying. Others have stated that even after paying the ransom, their files were still not accessible.

From time to time, Windows Vista/7/8 create point-in-time copies of your files. These snap shots are called Shadow Copies. And this feature was at first a great way to recover your files after removing CryptoLocker, since these shadow copies were not encrypted. But the originators of this Trojan are some very sick people. Newer instances of CryptoLocker execute a command to delete all your Shadow Copies silently in the background.

Using Peer to Peer file sharing networks, such as Frostwire, MicroTorrent and other BitTorrent clients is like asking the devil over for dinner. You'll find that no matter what is on the menu, you'll ending up being dessert. These networks are absolutely crawling with malware infected content. We highly recommend that you do not use these types of sites and that you should always keep an eye on any younger users of your computer to insure that these programs are not being installed. Kids today love to use these file sharing programs to download the latest movies and music for free, and we've seen a host of infected systems resulting from such use. Many times the client had no idea the program was even installed on their system.

Client-Side Vulnerabilities –

Here we see one of the more popular variations of the Acronym Agency infections. This is the ICE version, however, different templates suggest you are being threatened by the FBI or the DOJ. These ransomware/fraudware infections lock down and hold your computer system hostage while posing as an authority claiming that you must pay a fine for illegal activity on your computer.

Client-Side Vulnerabilities are one of the most concerning tactics we see out there, simply because it can attack your system without any interaction on your part, namely through the exploitation of client-side vulnerabilities in third-party software and browser plug-ins. Fast Rhino highly recommends that you use a script blocker because of this type of attack. We believe that script blocking is the most important element to maintain a defensive posture, simply because without it, you can become a victim of client-side attacks and never initiate it.

You can avoid these attacks altogether by keeping your plug-ins updated and using a script-blocker, which we will cover shortly.

My father passed away earlier this year after being diagnosed with pancreatic cancer. He used to own and operate the computer store up in Saddlebrooke until his health turned for the worse and he sold it; however, one of the more humorous stories he shared with me was one about an infected laptop that he had picked up from a client. He had already spent a day or two cleaning out the virus and restoring the customer's data. He still had an hour before he had to take it back to the customers' home, so he was wrapping up with all the minor details of getting it ready. One of the common things we like to do to save time is to download the printer software from the manufacturer's web site just in case the client can't find their printer installation disc. His client owned an HP printer, so naturally, he opened Internet Explorer and typed in HP.com to go get the driver software. As you can see from the layout of a standard keyboard, the O and the P are right next to each other. Unknowingly, my Dad typed in HO.com by mistake.

I'm sure you realize that ho.com doesn't offer print drivers. Instead, the notebook was immediately hit by a Client-Side attack, infecting it with ransomware. You can imagine how upset my Dad was knowing that he just re-infected the system with a simple fat-fingered mistake. All of his work on the notebook had to be redone and obviously he was not able to deliver it to the customer on-time.

The lesson here is that by just visiting the wrong web site, or being directed to the wrong site can get you infected…. regardless of what antivirus software you are using. What my Dad experienced was not that unusual. There are a growing number of web sites that can attack your system without you clicking on anything, without you downloading anything… And they don't have to be ho.com. In fact, that site has since been taken down by the way. I suppose there were too many other people making the same mistake and complaining about it.

Unlike the previous types of attacks we've discussed, Client-Side Attacks are completely invisible to the naked eye. There is no human defensive behavior that will protect you. I hear people say, Oh well I only go to certain web sites and I would never get anything like that on my computer. Believe me when I tell you that there are millions of infected pages just waiting for you to land on them. Your only defense is to keep your plug-ins updated and use a script-blocker. But what is a script blocker and how does it work?

At this time, only two major browsers have third party script blockers, however, both are free to download and easy to use.
As a reminder, make sure you go to the developer's official website to download these products.

ScriptSafe for Chrome (Browser can be downloaded from google.com/chrome and the script blocker, ScriptSafe can be downloaded from the Chrome Web Store)
NoScript for Firefox (Browser can be downloaded from mozilla.org and the script blocker, NoScript can be downloaded from noscript.net)

If you use Chrome as your browser, use ScriptSafe.
ScriptSafe is a free, open source add-on which prevents JavaScript, Java, Flash and other plug-ins to execute, unless you authorize them for the sites that you trust.

ScriptSafe used to be called ScriptNo, but I think the newer name is a better descriptive. You'll notice that ScriptSafe has a somewhat graphical interface. This feature alone makes it easier to use for those interested in using a script blocker for the first time. When you go to a web site that you trust you can quickly click on the ScriptSafe icon in the Chrome browser to the right of the address bar. This provides a menu of options where you can **Allow** the scripts to run and adds the respective domain to your Approved list. If you choose **Trust**, you are allowing the scripts to run and adding the entire top level domain (to include any sub-domains) to your Approved list… such as (*.domain.com). **Deny** moves the domain back into the blocked list. **Clear** erases the domain from both lists.

If you use Firefox as your browser, you'll need NoScript.
NoScript, is also a free, open source add-on that blocks harmful scripts unless you override it.
There's a great introduction to NoScript that was put together by CNET….
You can find it here: http://www.youtube.com/watch?v=GzBqnLgOzwM

Use a browser that supports script-blocking. Get familiar with your script blocker. Remember that script blockers are the most important element of defensive browsing. Because without them, you are blindly asking for trouble, no matter how safe you think you are.

Exercise caution about the programs you install, the links you click on and the attachments you open.

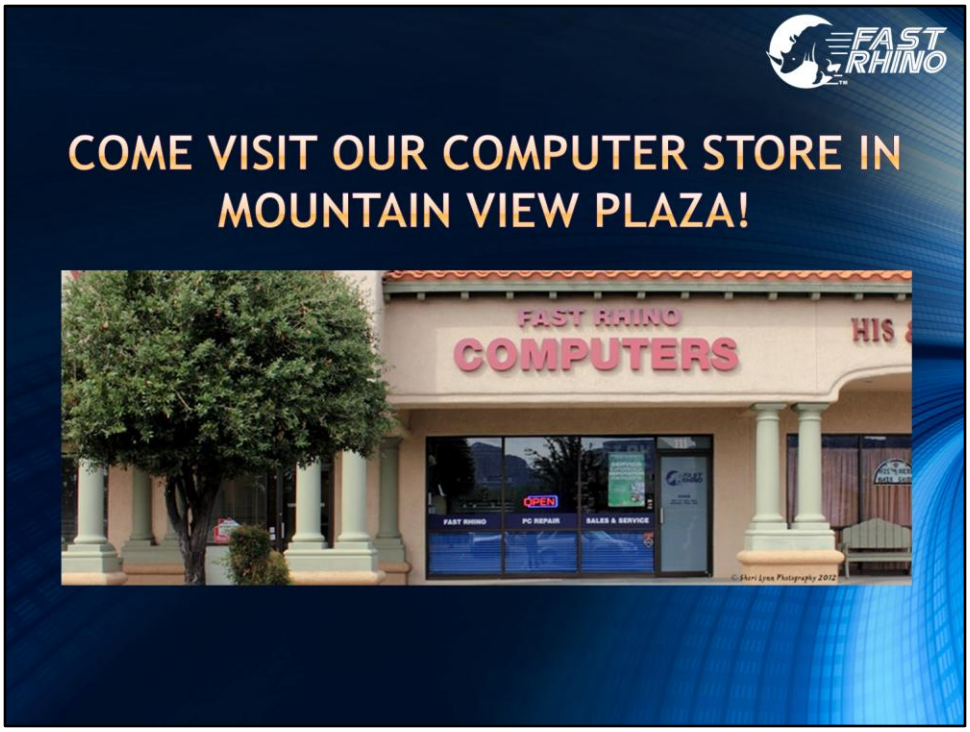
Never trust anyone who wants to remote on to your computer.

Always question advertisements on the web.

Make regular backups and keep them offline and disconnected from your computer.

Install a comprehensive anti-virus program like Norton and an anti-malware program like MalwareBytes.

This time is reserved for Q&A



Thank you for attending and we hope you will visit Fast Rhino's computer store soon.