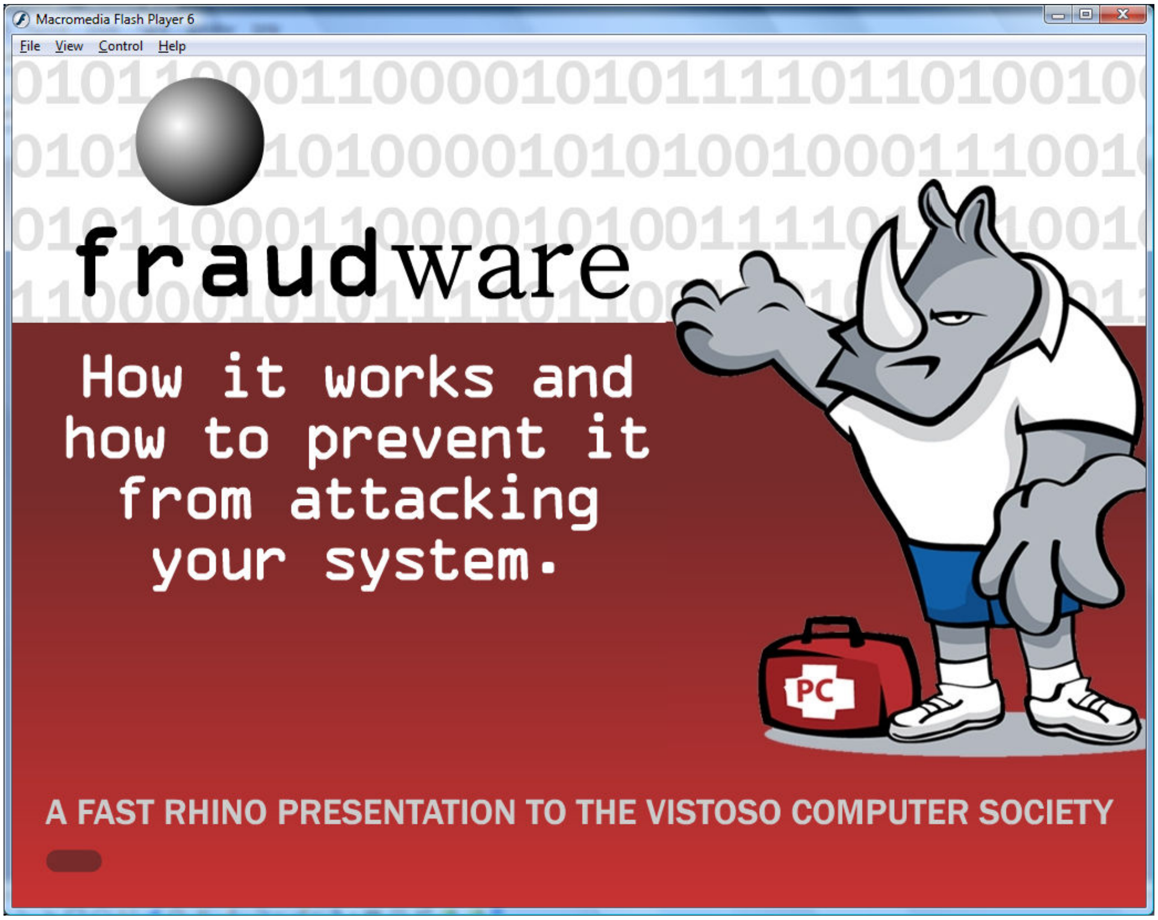
Fraudware

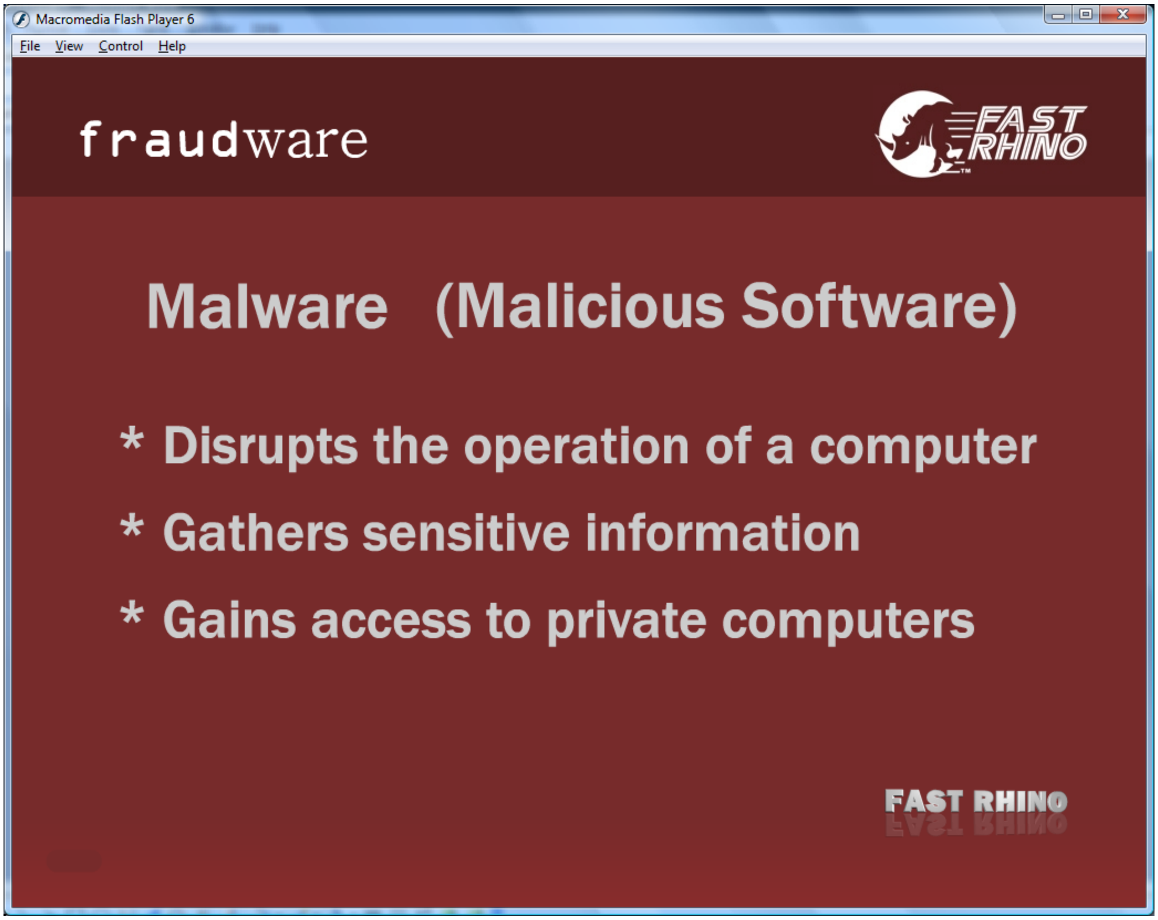
How it works and how to prevent it from attacking your system

A Fast Rhino Presentation to the Vistoso Computer Society

November 11, 2012


Macromedia Flash Player 6
File View Control Help
fraudware
How it works and how to prevent it from attacking your system.
PC
A FAST RHINO PRESENTATION TO THE VISTOSO COMPUTER SOCIETY

Before we jump in to Fraudware, we should most likely begin by defining "**Malware**", which is short for "Malicious software". We've all heard a lot in the past about viruses, adware, & spyware. Today, the industry basically refers to just about any software-based threat as "Malware". More specifically, Malware is a term used to define software that is intended to disrupt the operation of a computer, collect sensitive data, or gain access to private computer systems. Its definition is always expanding since new exploits continue to evolve.



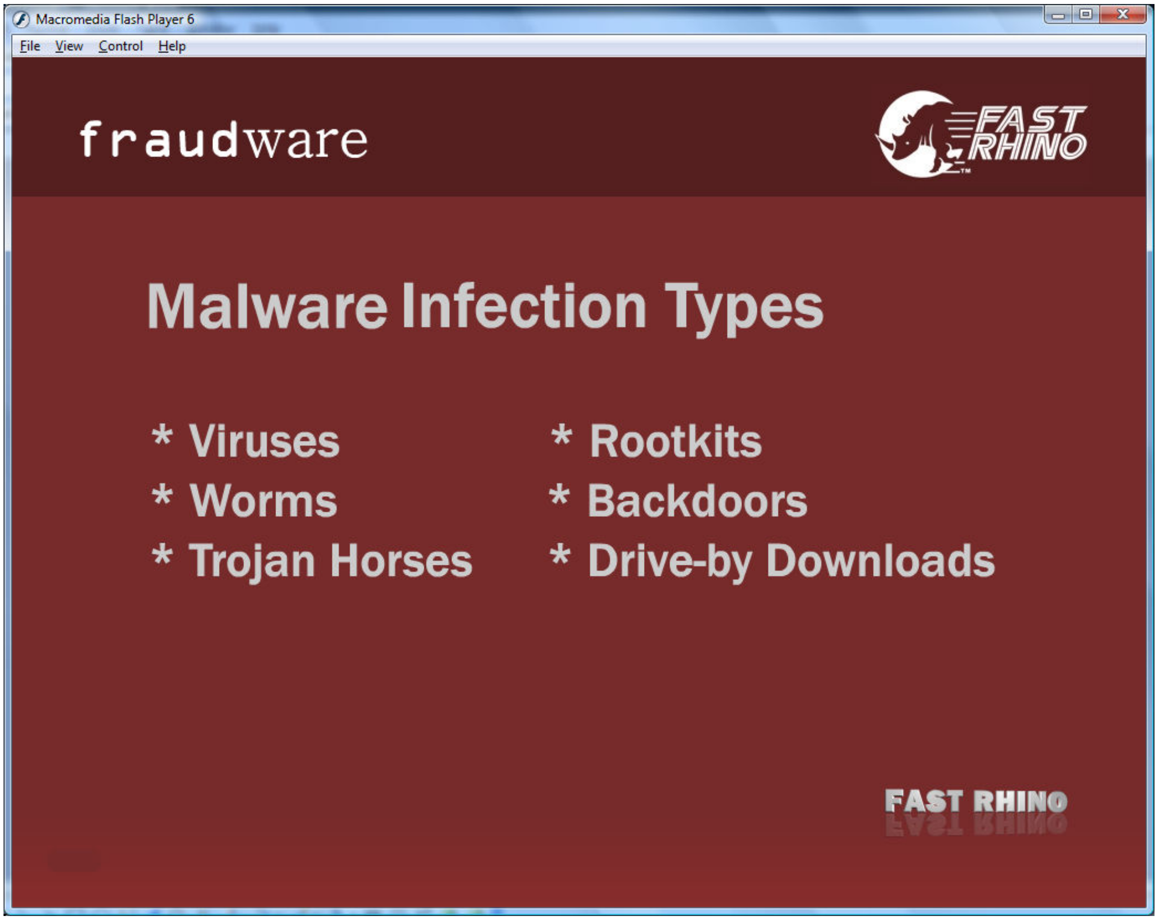
Malware (Malicious Software)

* Disrupts the operation of a computer

* Gathers sensitive information

* Gains access to private computers

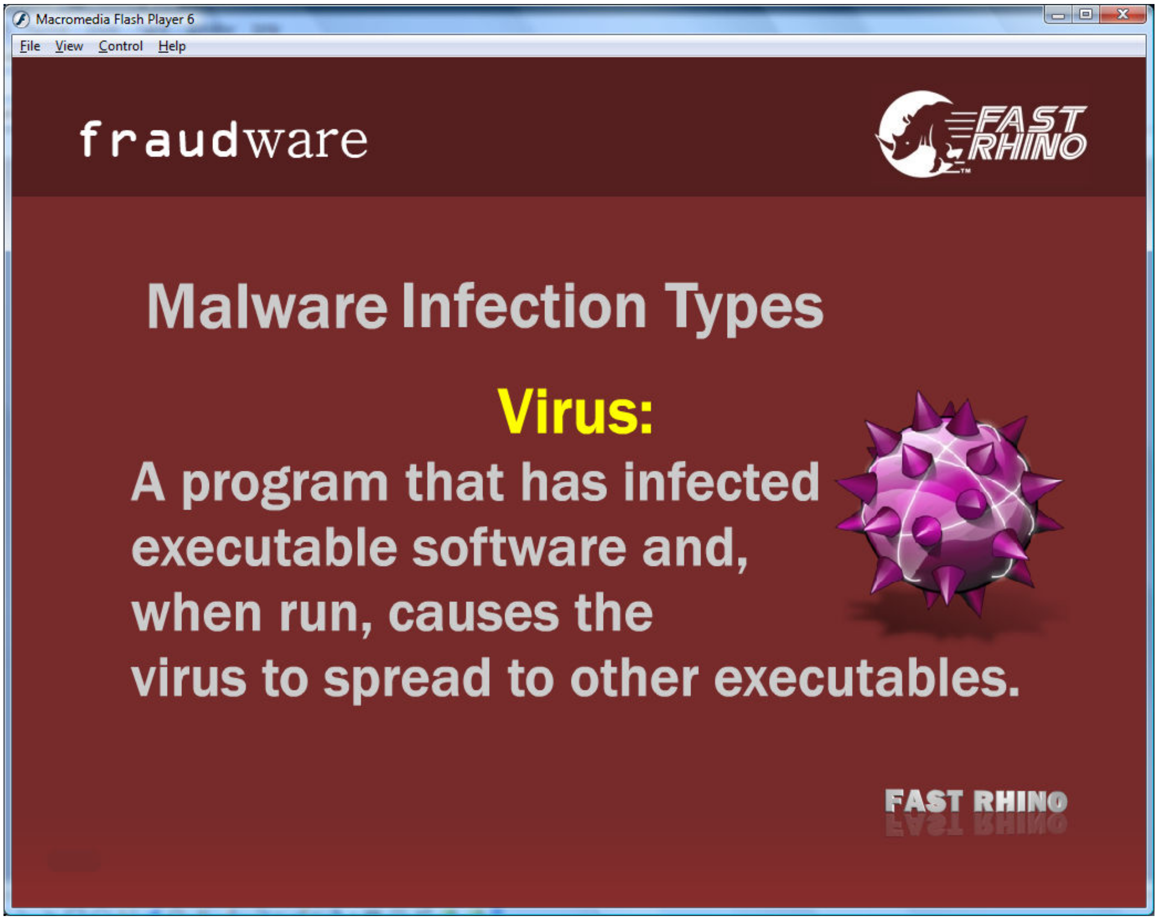
Malware consists of a broad spectrum of techniques used to infect systems, including viruses, worms, Trojan horses, rootkits, backdoors and drive-by downloads. Each of these operate differently, however, attacks can very often include a combination of these methods. And, although many of you in this room may already be aware of these, some of you may not, so please bear with me as we go through a basic understanding of these.



Malware Infection Types

* Viruses
* Worms
* Trojan Horses
* Rootkits
* Backdoors
* Drive-by Downloads

A **virus** is a program that infects executable software. When it runs, it allows the virus to spread to other executables. In the spring of 1999, a man named David L. Smith created a computer virus based on a Microsoft Word macro. He built the virus so that it could spread through e-mail messages. Smith named the virus "Melissa," saying that he named it after an exotic dancer from Florida. "Melissa" was one of the first major computer viruses to get the public's attention.

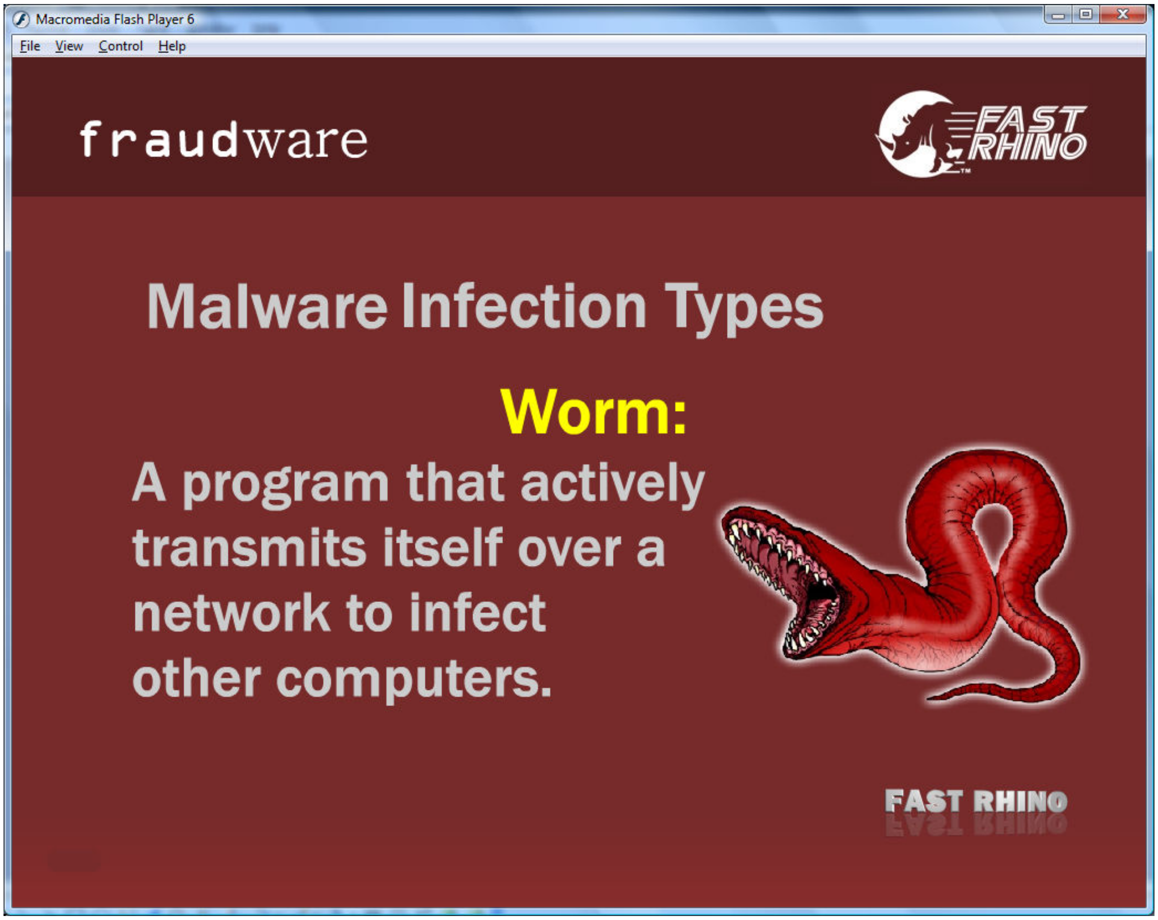


Malware Infection Types

Virus:

A program that has infected executable software and, when run, causes the virus to spread to other executables.

A **worm**, on the other hand, is a program that transmits itself over a network and infects other computers. If there's one word that causes shudders in Internet security circles, it's Conficker. Starting in late-2008, the Conficker worm exploited vulnerabilities in a number of Microsoft operating systems. Since its first detection, Conficker has infected millions of computers and business networks in countries around the world.

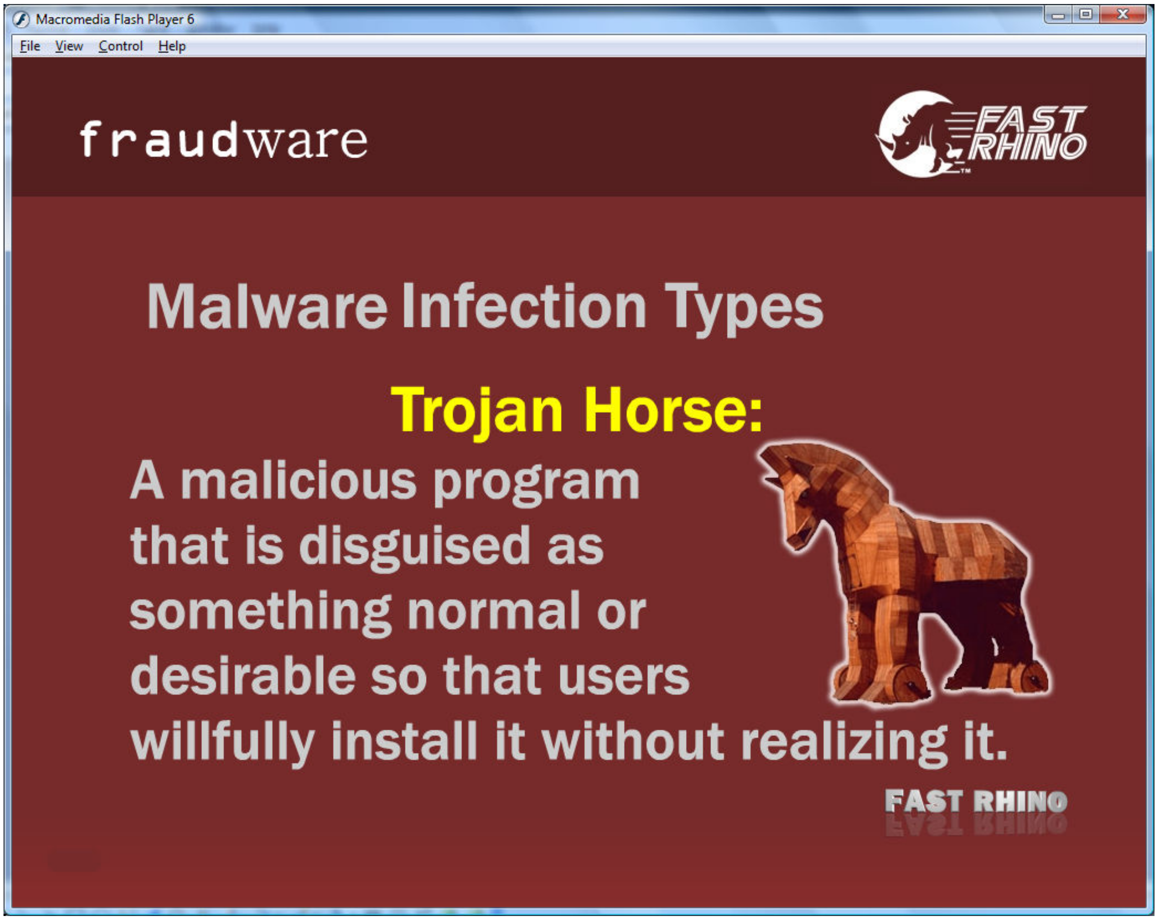


Malware Infection Types

Worm:

A program that actively transmits itself over a network to infect other computers.

A **Trojan Horse** is a malicious program that masquerades as a legitimate file or a helpful program but whose real purpose is to infect the user's system. If you use a Mac, you may have heard of a Trojan called, "Mac Flashback", which has infected more than a half a million Macs over the past 12 months. It was originally a fake Flash Player installer, however, the click fraud threat later evolved to exploit Java vulnerabilities within Mac OS X .

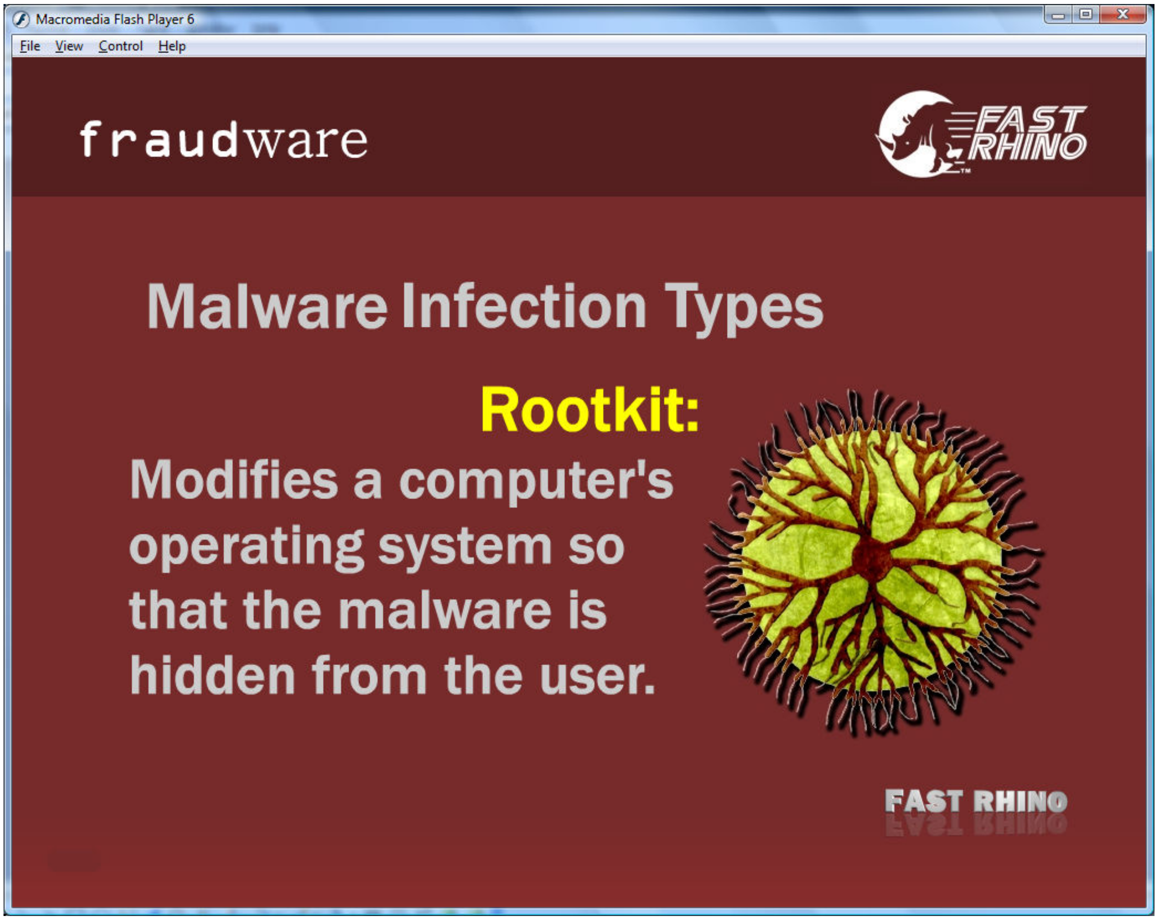


Malware Infection Types

Trojan Horse:

A malicious program that is disguised as something normal or desirable so that users willfully install it without realizing it.

Rootkits make changes to a computer's operating system to remain undetected and create a stealth environment. These infections can also make removal very difficult since they may be hard to find.

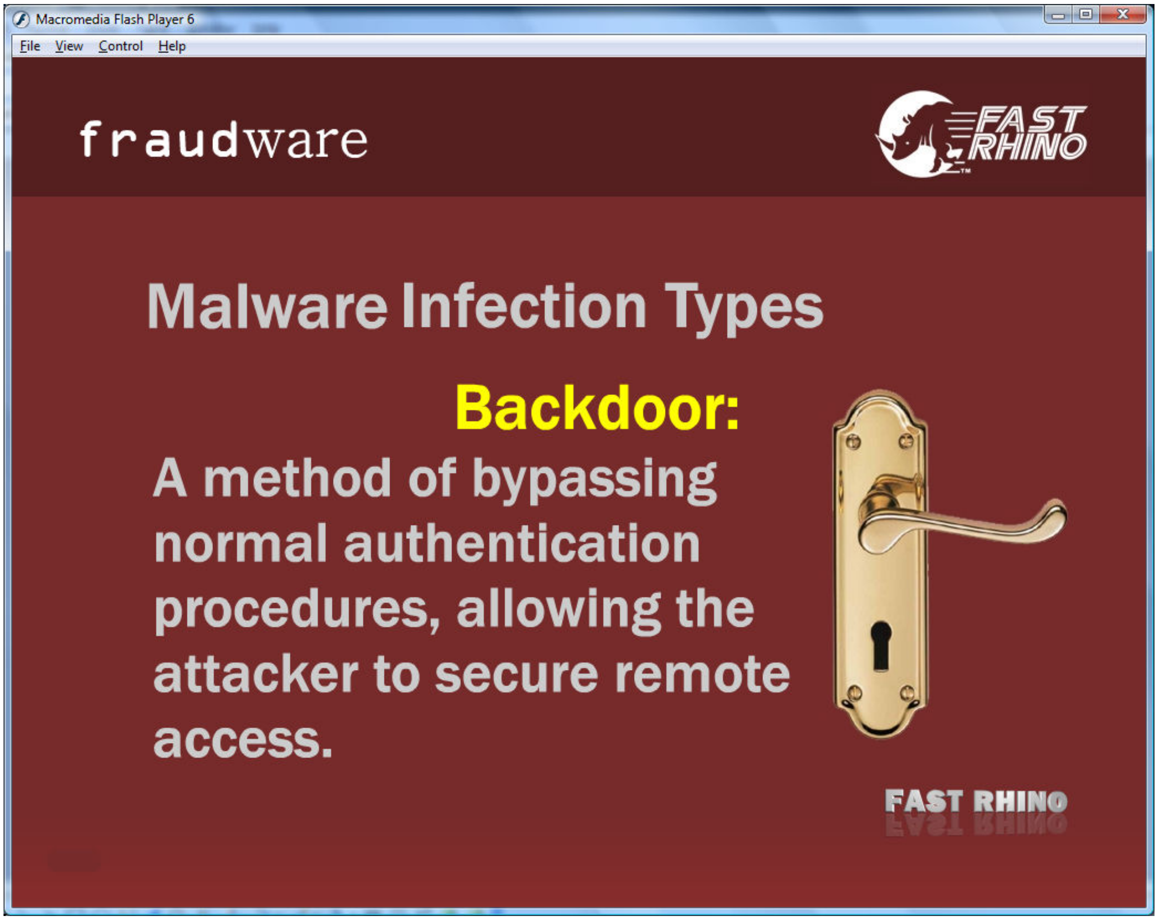


Malware Infection Types

Rootkit:

Modifies a computer's operating system so that the malware is hidden from the user.

A **Backdoor** is a method of bypassing normal authentication, which provides one with remote access to infiltrate a computer. Once a system has been compromised, one or more backdoors may be installed in order to allow easier access in the future.



Malware Infection Types

Backdoor:

A method of bypassing normal authentication procedures, allowing the attacker to secure remote access.

A **Drive-By Download** refers to a method whereby unintended software is downloaded when a user visits a website, views an e-mail message or clicks on a deceptive pop-up window.

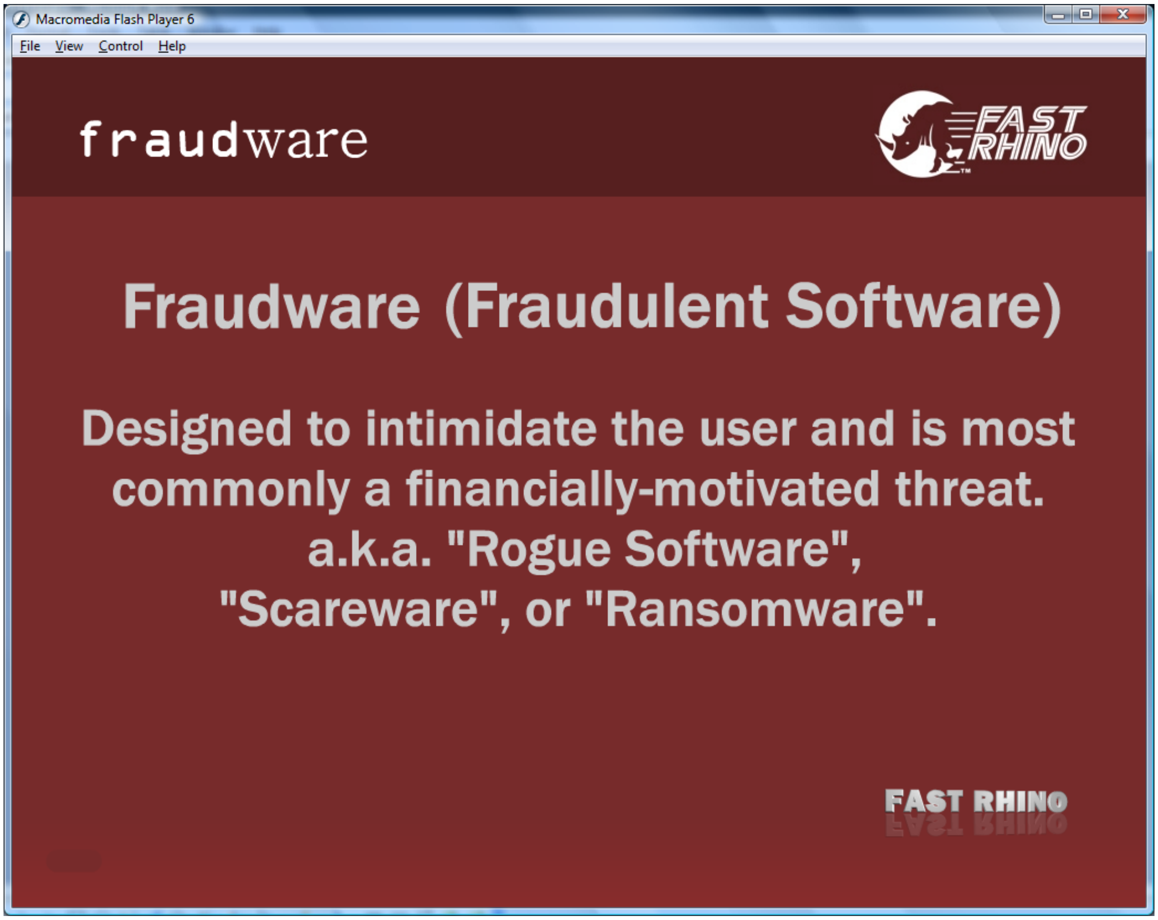
Malware Infection Types

Drive-By Download:

A method whereby unintended software is downloaded without the authorization of the user.

Today we're going to focus on **Fraudware**, which is a particular kind of Malware. Fraudware or "Fraudulent software", has been known to use some of the infection techniques we just discussed to invade a computer, most often Trojan horses and Drive-by downloads.

Fraudware is primarily designed to intimidate or frustrate the user. The attack is usually financially-motivated, as its purpose is to terrorize or confuse, designed to capture some form of ransom payment, or the release of credit card data. Fraudware is also referred to as "Rogue Software", "Scareware", or "Ransomware".



Fraudware (Fraudulent Software)

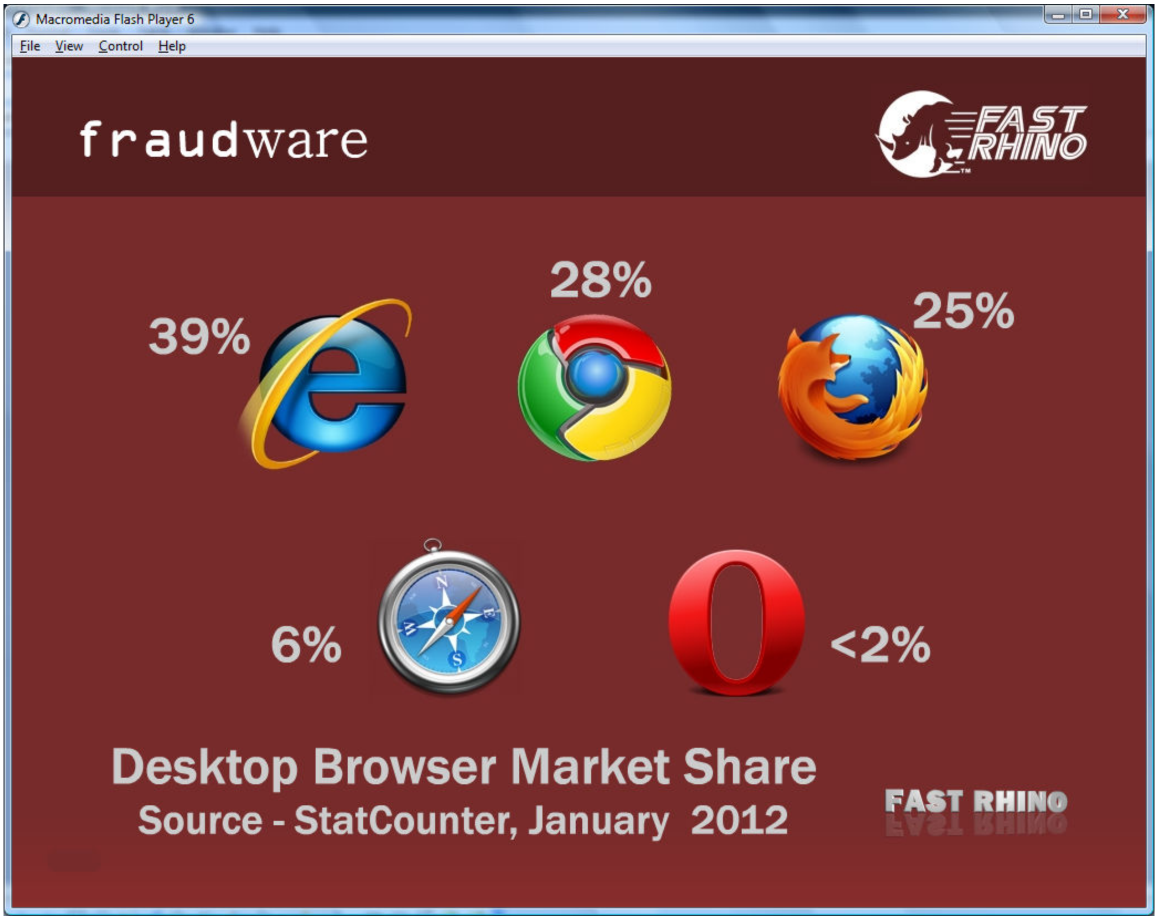
Designed to intimidate the user and is most commonly a financially-motivated threat. a.k.a. "Rogue Software", "Scareware", or "Ransomware".

First off, I would never recommend you try to install more than one anti-virus program on your computer. This is merely a representation showing how AV products in general can help protect you from traditional viruses. Since a vast majority of traditional virus attacks are being singled out and blocked by comprehensive anti-virus programs, attackers have switched gears and are now focusing on alternative ways in which to gain access to your computer.

This is why, in recent years, an increased target vector of infections has been the web browser. And as safe as you may feel with your antivirus software, today's threats are bypassing antivirus products altogether.

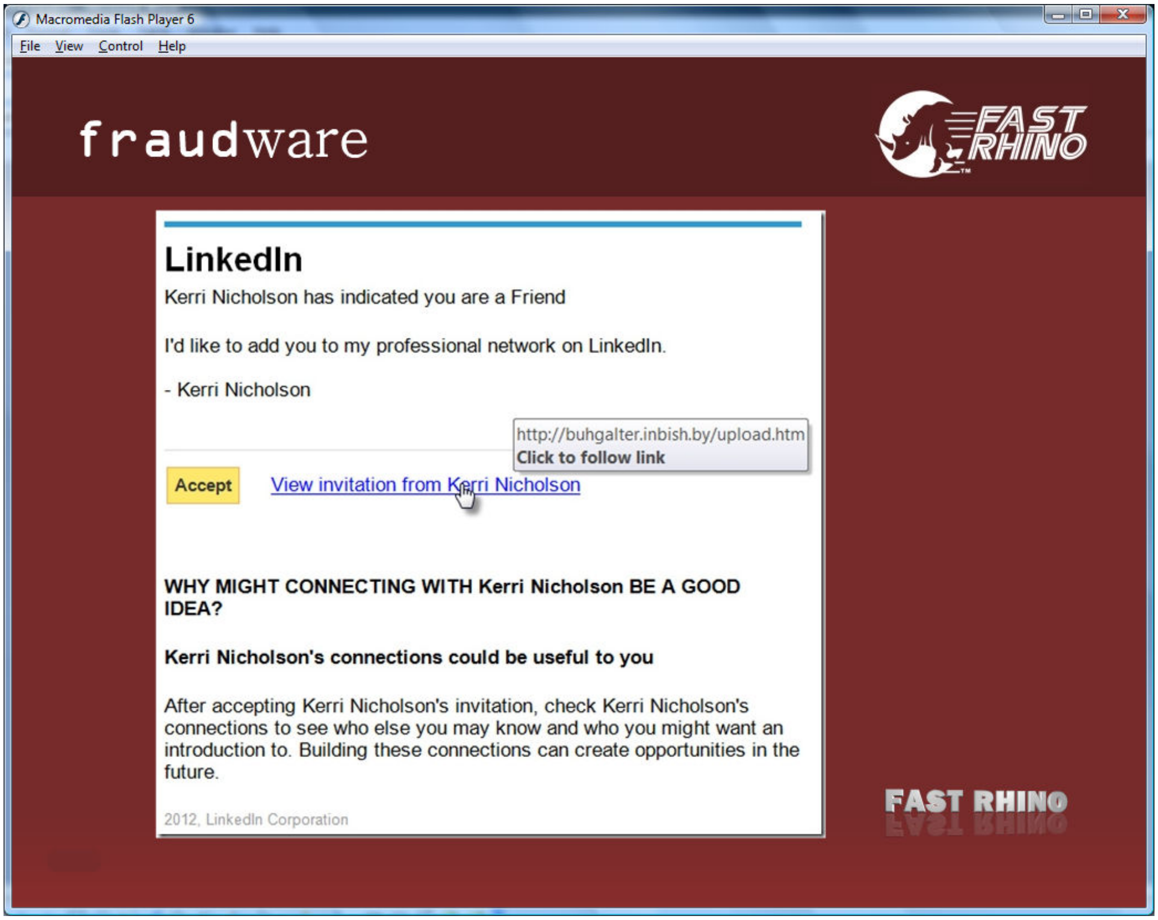
Vulnerabilities like service-centric exploitations require attackers to remotely gain access to vulnerable desktops/servers in order to exploit them. However, web browser vulnerabilities are commonly exploited when the user visits an infected web site.

As of the beginning of this year, more people used Internet Explorer than any other desktop browser, coming in at 39%. Google's Chrome came in second at 28%, Firefox edged just behind at 25% and Safari and Opera at 6% or less.



Desktop Browser Market Share
Source - StatCounter, January 2012

You need to know how the web is changing and how these new threats are being disseminated. So, let's go through the process of how fraudware works. First, fraudware attacks are usually initiated via a simple web link. It can be delivered via email, or to the browser via a drive-by exploit or in a search results list.



LinkedIn

Kerri Nicholson has indicated you are a Friend

I'd like to add you to my professional network on LinkedIn.

- Kerri Nicholson

http://buhgalter.inbish.by/upload.htm
Click to follow link

Accept View invitation from Kerri Nicholson

WHY MIGHT CONNECTING WITH Kerri Nicholson BE A GOOD IDEA?

Kerri Nicholson's connections could be useful to you

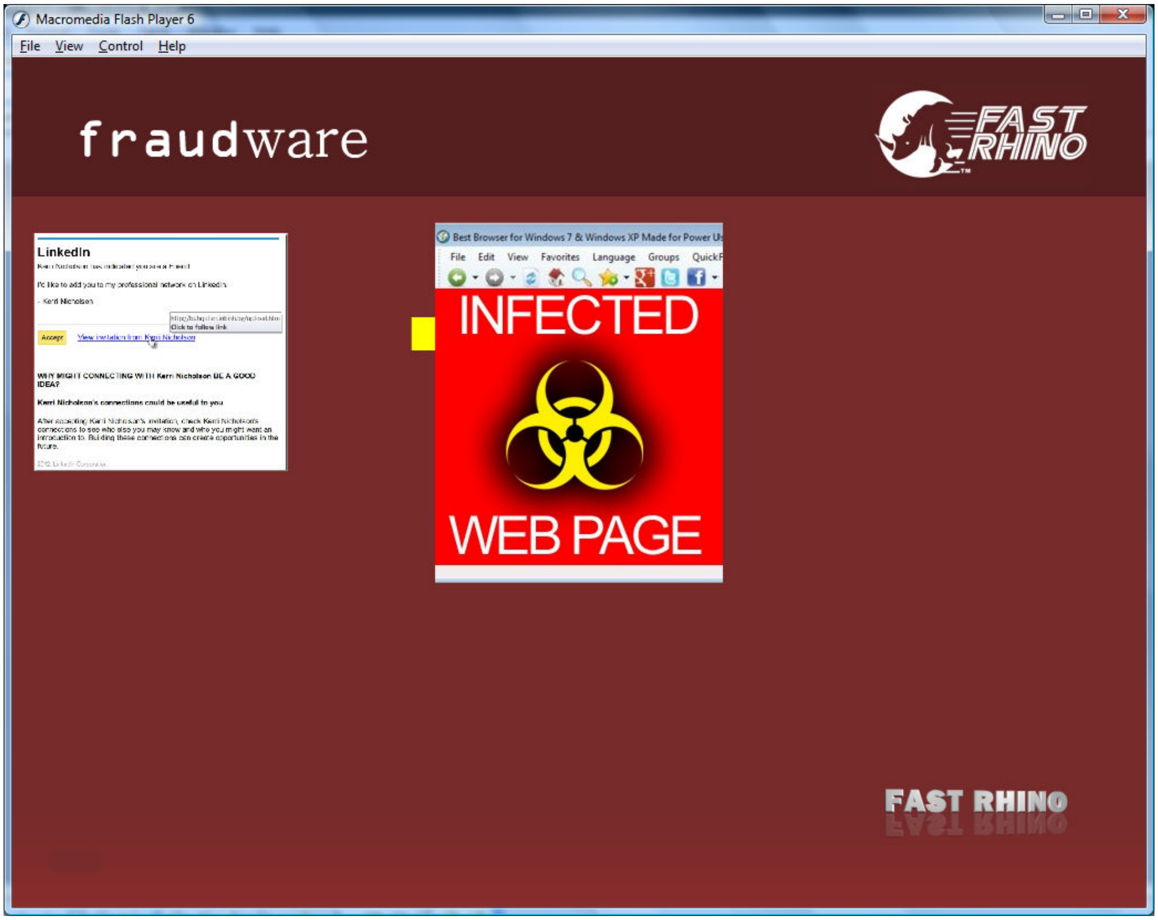
After accepting Kerri Nicholson's invitation, check Kerri Nicholson's connections to see who else you may know and who you might want an introduction to. Building these connections can create opportunities in the future.

2012, LinkedIn Corporation

Here we see a fraudulent email posing as a message from the popular social networking site, LinkedIn. The link in the email actually points to an infected webpage. Keep in mind that you can end up on an infected webpage by simply browsing the web, as well. This is where it get's tricky, since you don't really know what lies on the other end of most web links.

In fact, according to Symantec, “61% of malicious sites are actually regular web sites that have been compromised and infected with malicious code.” This malicious code can be found in a hidden web page that the site owner is unaware of, or through a carefully crafted ad. Legitimate ad networks unknowingly have malicious ads placed into their networks and these ads are proliferated across a multitude of client sites.

So let's say you actually clicked on this bogus link in this, what looks like, a legitimate email... Surprise! You've just landed on an infected web page. Oh, and for the purposes of today's presentation, this page is blatantly marked as an infected web page. In the real world, infected pages won't be this obvious. Behind the code of these infected pages contain redirection scripts, which are basically tiny client-side instructions.


Macromedia Flash Player 6
File View Control Help
fraudware
FAST RHINO
Best Browser for Windows 7 & Windows XP Made for Power U
File Edit View Favorites Language Groups Quick
INFECTED
WEB PAGE
FAST RHINO

LinkedIn

Kerri Nicholson has indicated you are a Friend

I'd like to add you to my professional network on LinkedIn.

- Kerri Nicholson

Click to follow link

Accept   View invitation from Kerri Nicholson

WHY MIGHT CONNECTING WITH Kerri Nicholson BE A GOOD IDEA?

Kerri Nicholson's connections could be useful to you

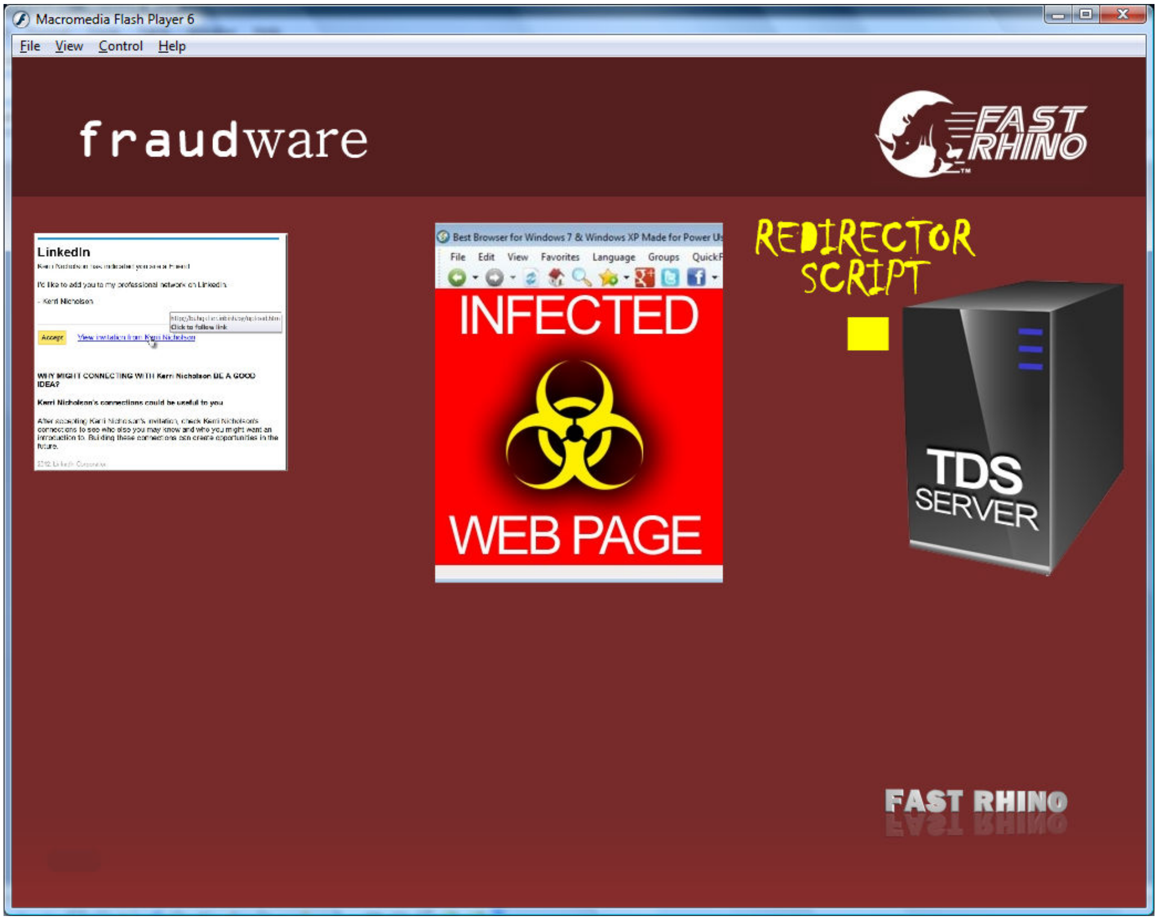
After accepting Kerri Nicholson's invitation, check Kerri Nicholson's connections to see who else you may know and who you might want an introduction to. Building these connections can create opportunities in the future.

2012 LinkedIn Corporation

If the scripts on this page are allowed to run in your browser,

then, at that very moment...

A redirector script points your system to a hosting server. This server is actually quite intelligent because it utilizes its own "traffic direction system" or TDS, for short.



Macromedia Flash Player 6
File View Control Help
fraudware
FAST RHINO
Best Browser for Windows 7 & Windows XP Made for Power Us
File Edit View Favorites Language Groups QuickF
INFECTED
WEB PAGE
REDIRECTOR SCRIPT
TDS SERVER
FAST RHINO

LinkedIn

Kerri Nicholson has indicated you are a Friend

I'd like to add you to my professional network on LinkedIn.

- Kerri Nicholson

[illegible]
Click to follow link

Accept View invitation from Kerri Nicholson

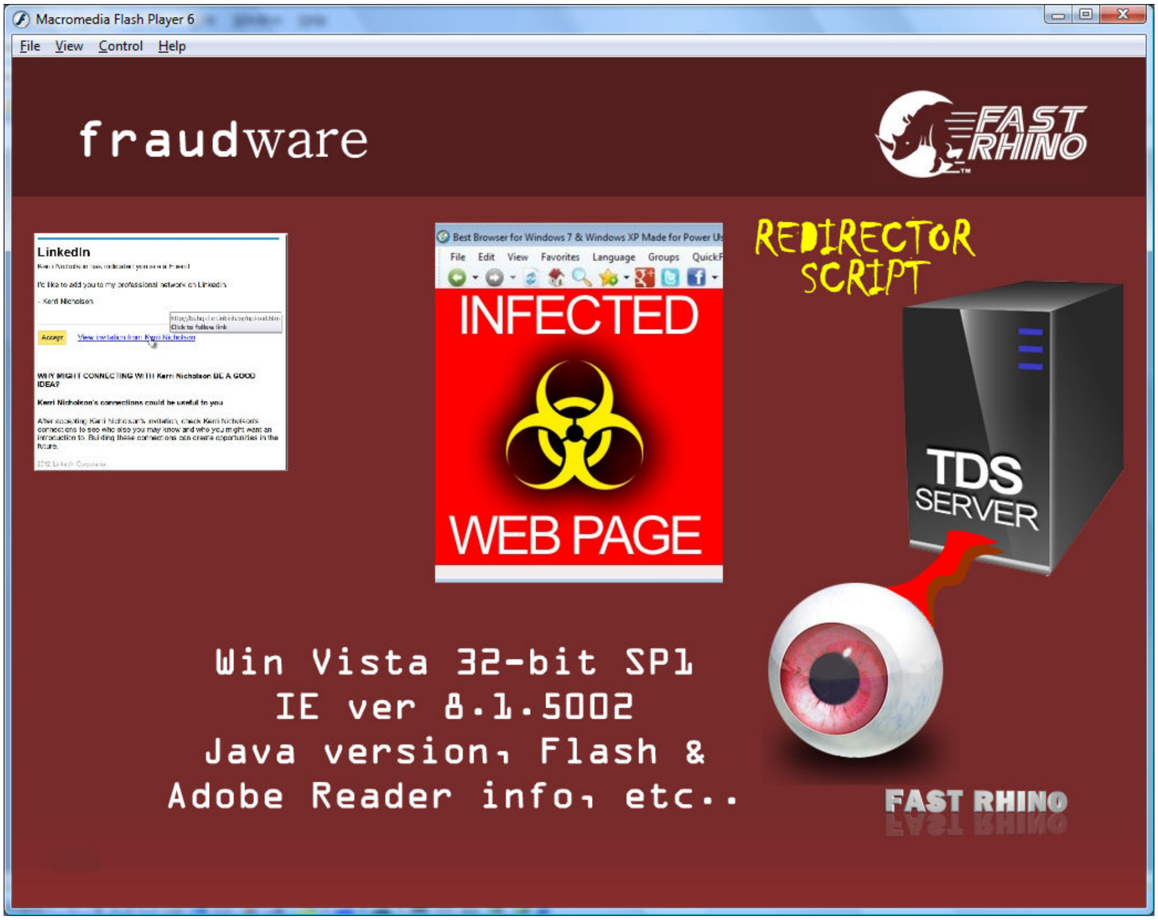
WHY MIGHT CONNECTING WITH Kerri Nicholson BE A GOOD IDEA?

Kerri Nicholson's connections could be useful to you

After accepting Kerri Nicholson's invitation, check Kerri Nicholson's connections to see who else you may know and who you might want an introduction to. Building these connections can create opportunities in the future.

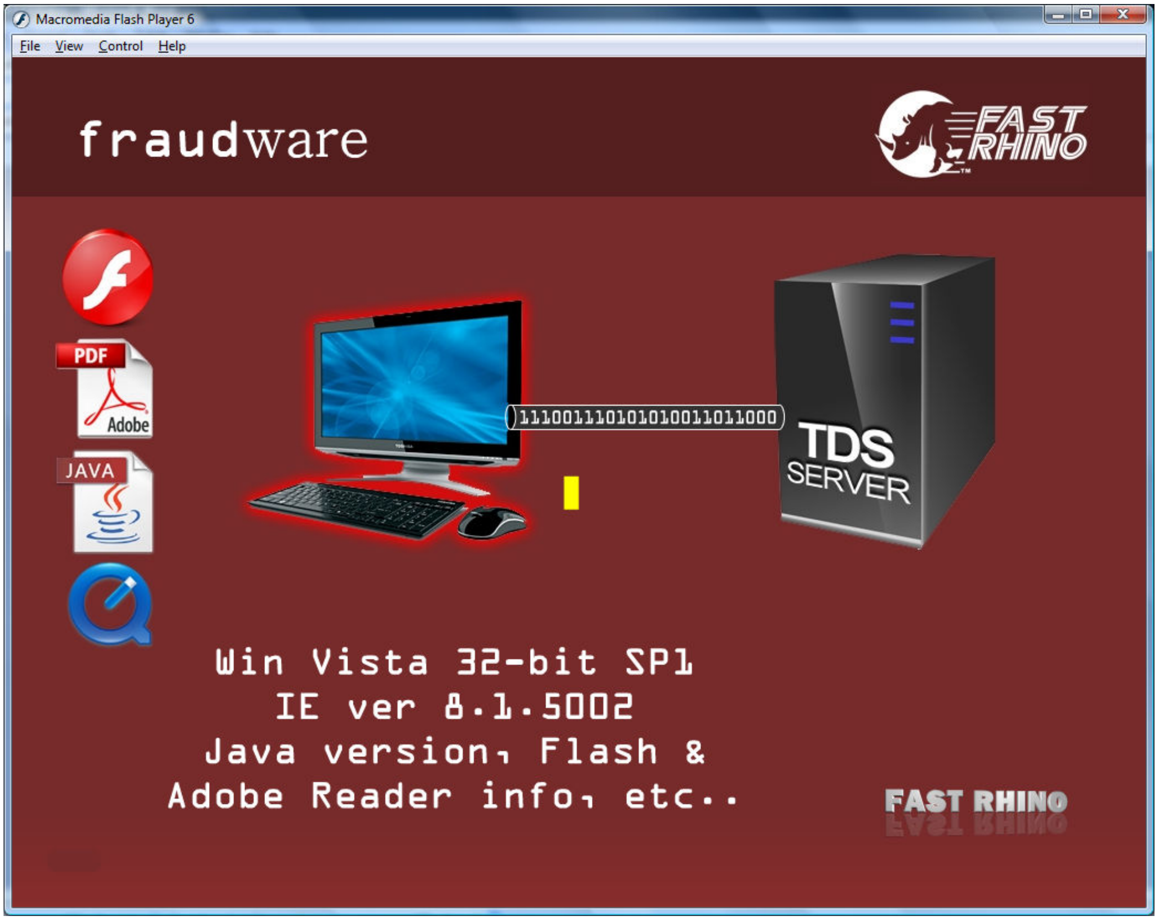
2012 LinkedIn Corporation

This very inquisitive TDS server collects various details about which browser and what operating system you're using and the versions or lack of updates you have installed. It also eyeballs information about your plug-ins, like the version of your Adobe Flash Player, which version of Adobe Reader you're running, what version of Java, Quicktime, etc... It can even identify your geographical location from your IP address.


Macromedia Flash Player 6
File View Control Help
fraudware
FAST RHINO
LinkedIn
Kerri Nicholson has indicated you are a Friend
I'd like to add you to my professional network on LinkedIn.
- Kerri Nicholson
Click to follow link
Accept
View invitation from Kerri Nicholson
WHY MIGHT CONNECTING WITH Kerri Nicholson BE A GOOD IDEA?
Kerri Nicholson's connections could be useful to you
After accepting Kerri Nicholson's invitation, check Kerri Nicholson's connections to see who else you may know and who you might want an introduction to. Building these connections can create opportunities in the future.
2012 LinkedIn Corporation
Best Browser for Windows 7 & Windows XP Made for Power Us
File Edit View Favorites Language Groups QuickF
INFECTED
WEB PAGE
REDIRECTOR SCRIPT
TDS SERVER
Win Vista 32-bit SP1
IE ver 8.1.5002
Java version, Flash &
Adobe Reader info, etc..
FAST RHINO

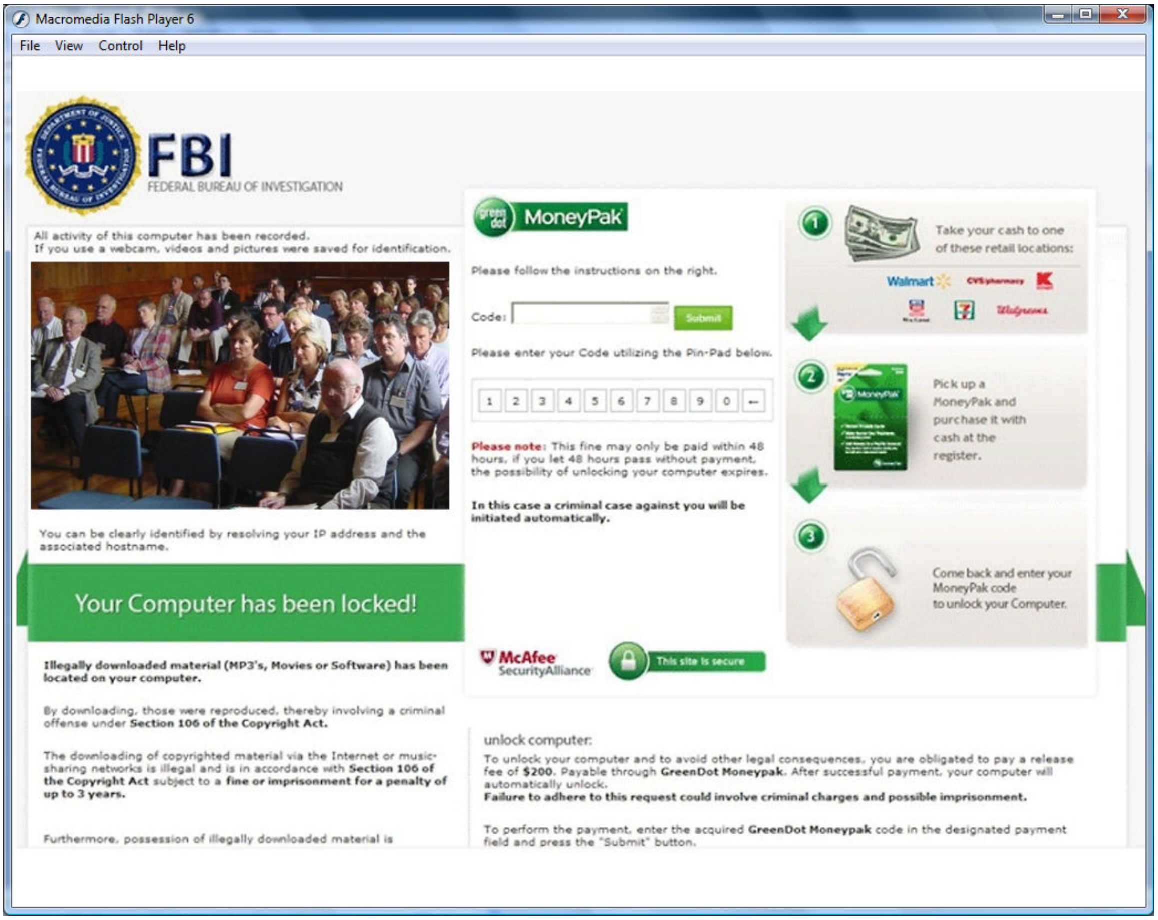
TDS then returns a collection of exploits tailored to the specific vulnerabilities present in your system. Delivered content may contain simple VBScript downloaders, PDF, Flash or Java exploits. Should these exploits be successful, the victim's machine reconnects to the hosting server for a binary payload, which is subsequently downloaded and executed.

It is at this point when the damage is done.



Win Vista 32-bit SP1
IE ver 8.1.5002
Java version, Flash &
Adobe Reader info, etc..

This is a typical FBI Fraudware screen that we see regularly on infected systems. The problem is that once you see this on your computer screen, trying to use your computer becomes a real nightmare. Depending on the severity of the binary payload, this type of infection can be almost impossible to remove manually. Most people give up trying to make this screen go away and either take their computer in to have it repaired, pay the "fine" to the fraudware attacker (which, by the way, doesn't necessarily remove the fraudware), reformat their hard drive (losing any data they didn't previously have backed up, or in some cases, go buy another computer altogether.



All activity of this computer has been recorded.
If you use a webcam, videos and pictures were saved for identification.

You can be clearly identified by resolving your IP address and the associated hostname.

Your Computer has been locked!

Illegally downloaded material (MP3's, Movies or Software) has been located on your computer.

By downloading, those were reproduced, thereby involving a criminal offense under **Section 106 of the Copyright Act.**

The downloading of copyrighted material via the Internet or music-sharing networks is illegal and is in accordance with **Section 106 of the Copyright Act** subject to a **fine or imprisonment for a penalty of up to 3 years.**

Furthermore, possession of illegally downloaded material is

Please follow the instructions on the right.

Code:

Please enter your Code utilizing the Pin-Pad below.

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

In this case a criminal case against you will be initiated automatically.

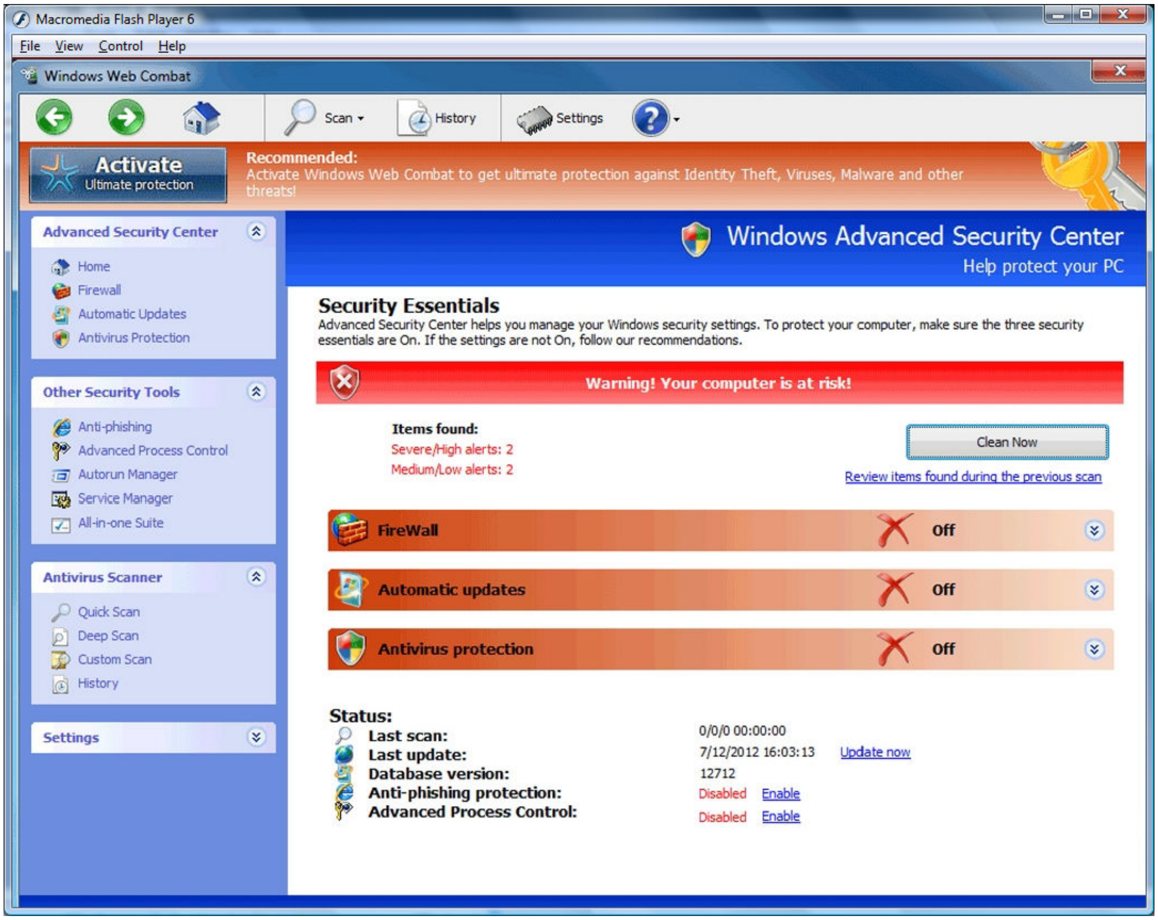
1. Take your cash to one of these retail locations:
2. Pick up a MoneyPak and purchase it with cash at the register.
3. Come back and enter your MoneyPak code to unlock your Computer.

unlock computer:

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of **$200**. Payable through **GreenDot Moneypak**. After successful payment, your computer will automatically unlock.
Failure to adhere to this request could involve criminal charges and possible imprisonment.

To perform the payment, enter the acquired **GreenDot Moneypak** code in the designated payment field and press the "Submit" button.

Here is another example of a fraudware screen that demands "registration", which is their code word for "payment". Fraudware, as you can see, utilizes ransom-style tactics.



Recommended:
Activate Windows Web Combat to get ultimate protection against Identity Theft, Viruses, Malware and other threats!

Security Essentials

Advanced Security Center helps you manage your Windows security settings. To protect your computer, make sure the three security essentials are On. If the settings are not On, follow our recommendations.

Warning! Your computer is at risk!

Items found:
Severe/High alerts: 2
Medium/Low alerts: 2

FireWall Off

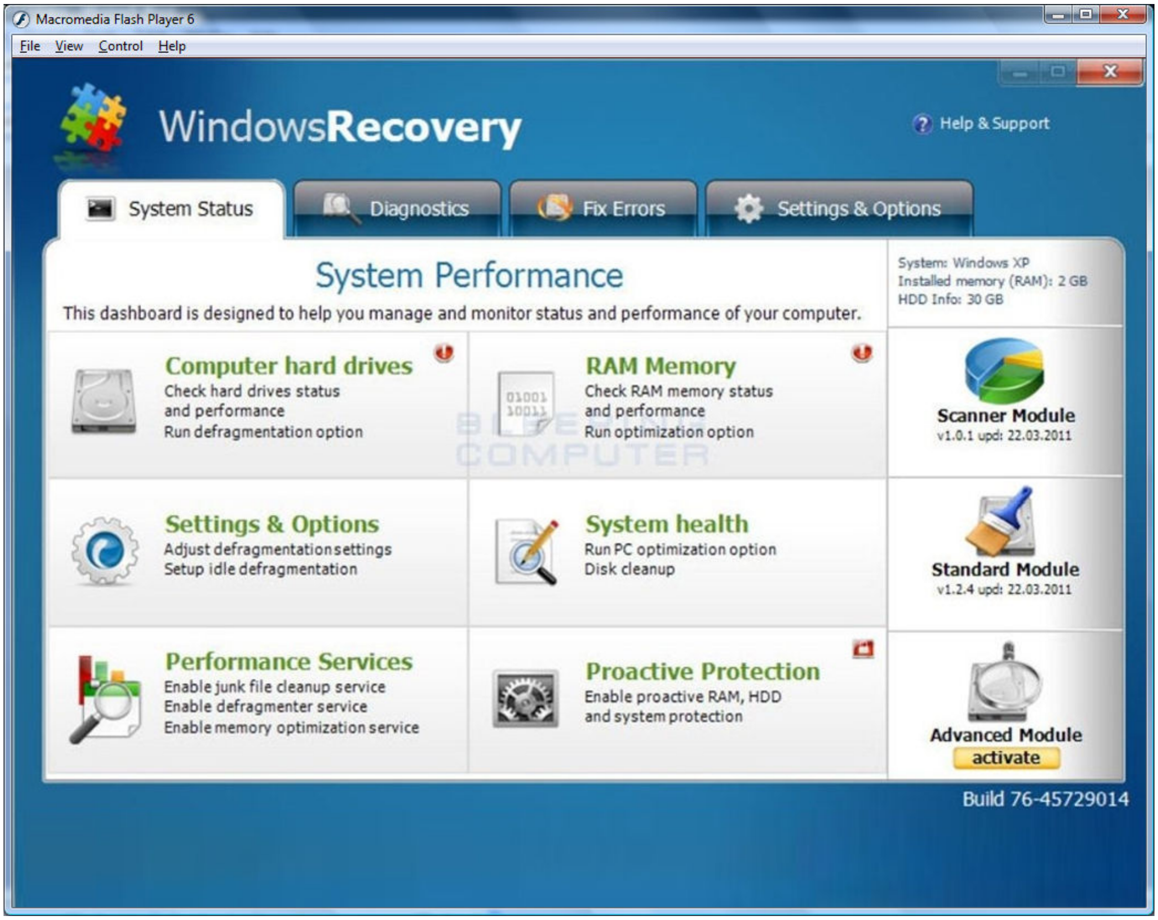
Automatic updates Off

Antivirus protection Off

Status:

Last scan:	0/0/0 00:00:00
Last update:	7/12/2012 16:03:13
Database version:	12712
Anti-phishing protection:	Disabled
Advanced Process Control:	Disabled

And another....



System Performance

This dashboard is designed to help you manage and monitor status and performance of your computer.

System: Windows XP
Installed memory (RAM): 2 GB
HDD Info: 30 GB

Computer hard drives
Check hard drives status
and performance
Run defragmentation option

RAM Memory
Check RAM memory status
and performance
Run optimization option

Scanner Module
v1.0.1 upd: 22.03.2011

Settings & Options
Adjust defragmentation settings
Setup idle defragmentation

System health
Run PC optimization option
Disk cleanup

Standard Module
v1.2.4 upd: 22.03.2011

Performance Services
Enable junk file cleanup service
Enable defragmenter service
Enable memory optimization service

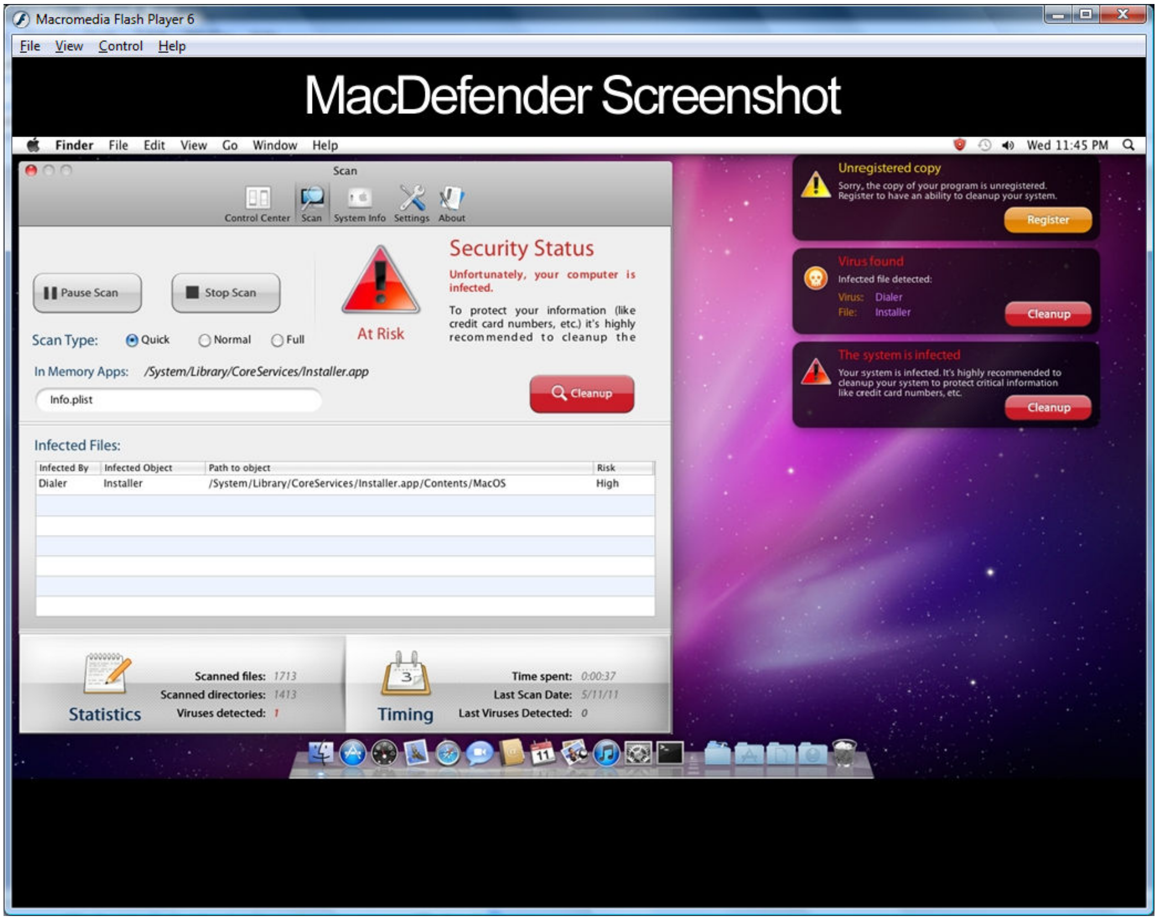
Proactive Protection
Enable proactive RAM, HDD
and system protection

Advanced Module

Build 76-45729014

We've seen a number of Fraudware variations as far back as 2007. A few of the more notable names included WinFixer, WinAntiVirus, WinAntiSpyware, XP Security, Windows Web Combat, and of course, the FBI Virus, which we saw earlier.

It's interesting to note that fraudware has attacked both PC and MAC platforms. It's also been found in mobile apps available in the Android Market.



Security Status

Unfortunately, your computer is infected.

To protect your information (like credit card numbers, etc.) it's highly recommended to cleanup the

Scan Type: ● Quick ○ Normal ○ Full

In Memory Apps: /System/Library/CoreServices/Installer.app

Info.plist

Infected Files:

Infected By	Infected Object	Path to object	Risk
Dialer	Installer	/System/Library/CoreServices/Installer.app/Contents/MacOS	High

Scanned files: 1713
Scanned directories: 1413
Viruses detected: 1

Time spent: 0:00:37
Last Scan Date: 5/11/11
Last Viruses Detected: 0

Unregistered copy

Sorry, the copy of your program is unregistered. Register to have an ability to cleanup your system.

Virus found

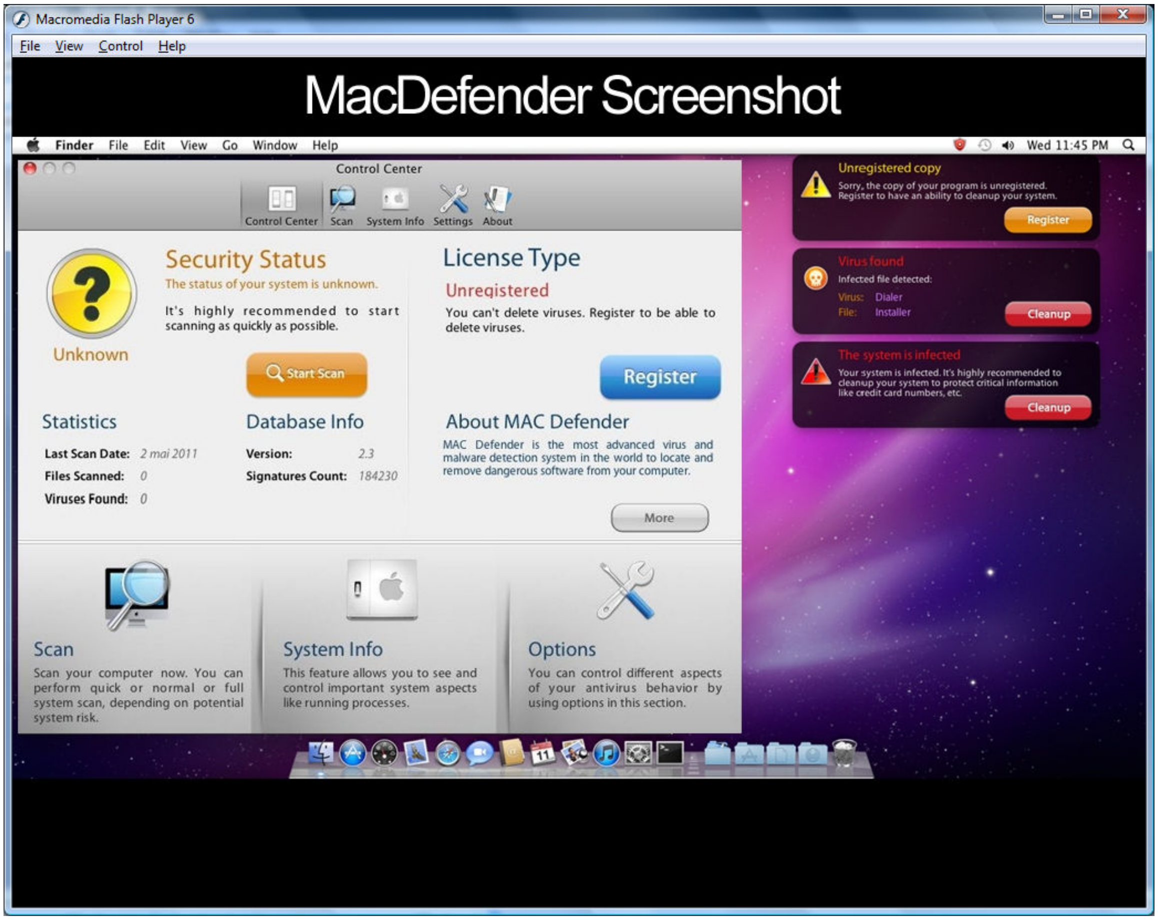
Infected file detected:
Virus: Dialer
File: Installer

The system is infected

Your system is infected. It's highly recommended to cleanup your system to protect critical information like credit card numbers, etc.

Here is a screenshot of "MacDefender", a fake antivirus software designed to trick users into providing their credit card numbers to supposedly clean out infected files on their Macs. It was first identified back in 2009 and it was also known by other names like MacProtector and MacSecurity.

Here, you can see how they require the user to register in order to "delete" the so called viruses they found.


Macromedia Flash Player 6
File View Control Help
Finder File Edit View Go Window Help
Wed 11:45 PM
Control Center
Control Center Scan System Info Settings About
Start Scan
Register
More
Register
Cleanup
Cleanup

MacDefender Screenshot

Security Status

The status of your system is unknown.

It's highly recommended to start scanning as quickly as possible.

Unknown

License Type

Unregistered

You can't delete viruses. Register to be able to delete viruses.

Statistics

Last Scan Date: 2 mai 2011
Files Scanned: 0
Viruses Found: 0

Database Info

Version: 2.3
Signatures Count: 184230

About MAC Defender

MAC Defender is the most advanced virus and malware detection system in the world to locate and remove dangerous software from your computer.

Scan

Scan your computer now. You can perform quick or normal or full system scan, depending on potential system risk.

System Info

This feature allows you to see and control important system aspects like running processes.

Options

You can control different aspects of your antivirus behavior by using options in this section.

Unregistered copy

Sorry, the copy of your program is unregistered. Register to have an ability to cleanup your system.

Virus found

Infected file detected:

Virus: Dialer
File: Installer

The system is infected

Your system is infected. It's highly recommended to cleanup your system to protect critical information like credit card numbers, etc.

Now, as we mentioned before, these types of browser-based attacks need only be rendered by an unprotected browser. If not exploiting the browser's built-in interpreter through malicious javascripts or cascading style sheets (css), they could also gain access through a vulnerable (Read that... an **un**updated) plug-in like Adobe Flash, Adobe Reader, QuickTime, or Java... etc. Open vulnerabilities lying within these rendering technologies become exposed to malicious techniques developed by the attacker.

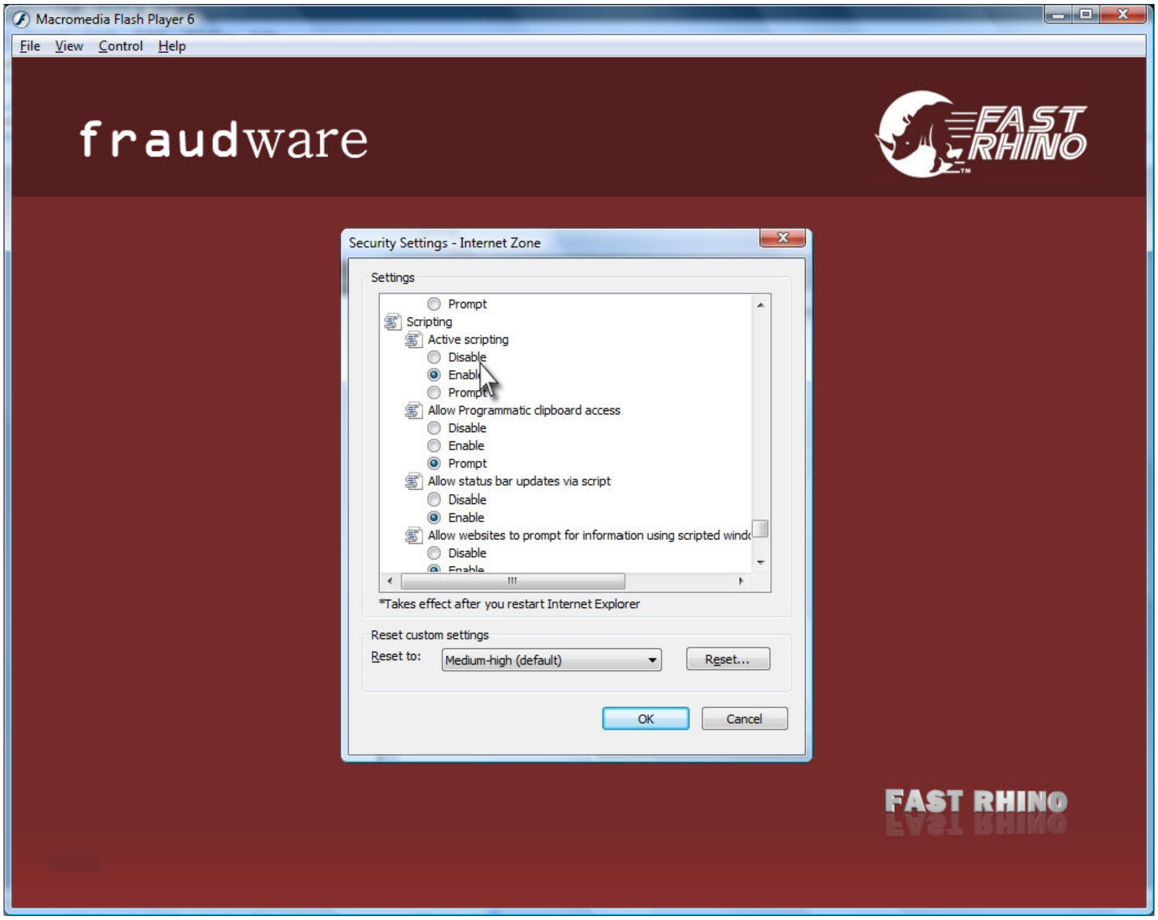
Some people may think, hmm, what if I just simply uninstall these plug-in programs from my computer? That may prevent vulnerabilities, however, you won't be able to see certain content that utilizes these plug-ins on your favorite web sites.

So how do we protect ourselves from fraudware? It all started when we clicked on a link and we ended up on that infected web page. Since we can't possibly know what's on the other end of every link we click, we need to tell our browser not to run those client-side redirection scripts.

Then we could avoid the TDS server eyeballing our system, sending us an exploit, and ultimately downloading a binary payload.

Macromedia Flash Player 6
File View Control Help
fraudware
FAST RHINO
Best Browser for Windows 7 & Windows XP Made for Power Us
File Edit View Favorites Language Groups QuickF
INFECTED
WEB PAGE
FAST RHINO

Most browsers offer a way to disable Javascripts from running altogether, which is great, until you go to one of your favorite sites that requires it. Turning it on and off this way is not a very reasonable solution.



Settings

○ Prompt

Scripting

Active scripting

○ Disable

● Enable

○ Prompt

Allow Programmatic clipboard access

○ Disable

○ Enable

● Prompt

Allow status bar updates via script

○ Disable

● Enable

Allow websites to prompt for information using scripted windo

○ Disable

● Enable

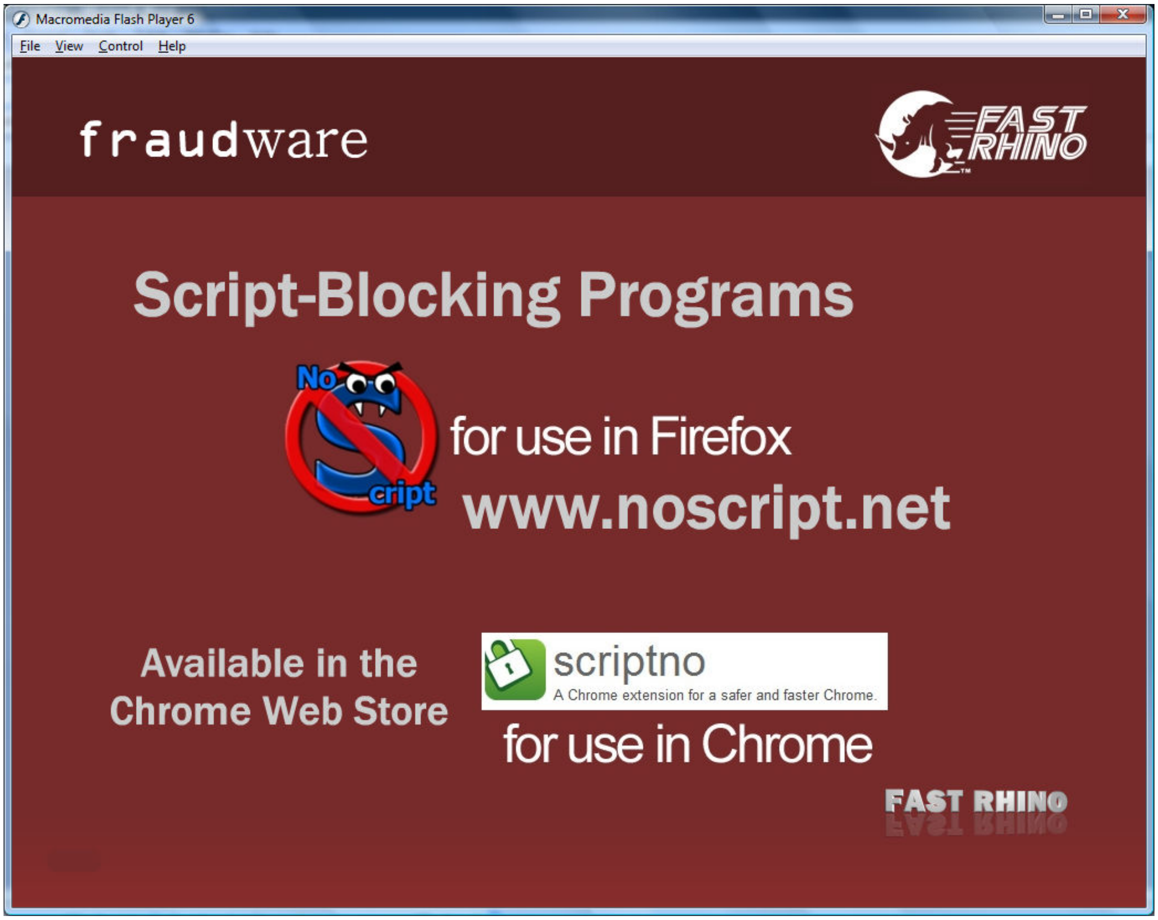
*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-high (default)

Fortunately, there are a couple of programs you can use to block scripts on a site-for-site basis. "NoScript", a free, Open Source Software plug-in for FireFox, found at www.noscript.net or "ScriptNo", a free extension for Chrome found in the Chrome Web Store.

The NoScript/ScriptNo products are both easy to download and they block all scripts unless you specifically enable them for a particular site. These script blocking programs work within the browser and provide excellent protection anytime you are browsing the web, regardless of which site you visit.



Script-Blocking Programs

for use in Firefox

www.noscript.net

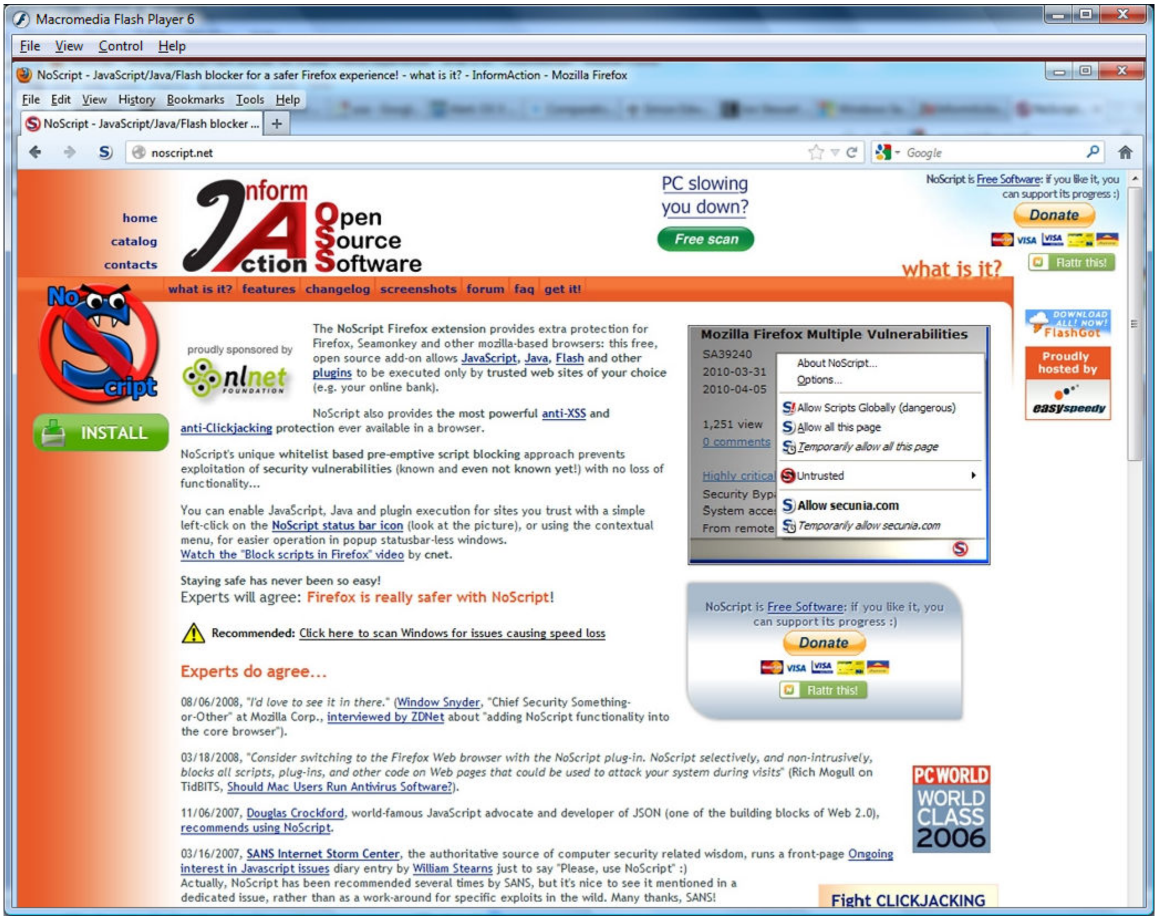
Available in the Chrome Web Store

A Chrome extension for a safer and faster Chrome.

for use in Chrome

As long as you do not override the blocked scripts, the browser cannot run the redirector scripts found on fraudware infected sites. This stops the entire process - You do not get pointed to the traffic direction system. It does not collect your browser or OS version information, and it doesn't have a chance to return a collection of exploits to your system.

Here's a quick look at NoScript, which is the script blocker we use at Fast Rhino. This product works within the Firefox browser. After installing Firefox, which is also free, you can navigate to www.noscript.net. Then click on the install link in the upper left corner. This will start the installation process, which goes very quickly. Once it has been installed, you'll need to restart Firefox.


Macromedia Flash Player 6
File View Control Help
NoScript - JavaScript/Java/Flash blocker for a safer Firefox experience! - what is it? - InformAction - Mozilla Firefox
File Edit View History Bookmarks Tools Help
NoScript - JavaScript/Java/Flash blocker ...
noscript.net
Google
home
catalog
contacts
InformAction
Open Source Software
PC slowing you down?
Free scan
NoScript is Free Software: if you like it, you can support its progress :)
Donate
Flattr this!
what is it?
what is it? features changelog screenshots forum faq get it!
NoScript
INSTALL
proudly sponsored by
nlnet FOUNDATION
Mozilla Firefox Multiple Vulnerabilities
SA39240
2010-03-31
2010-04-05
1,251 view
0 comments
Highly critical
Security Byp
System acce
From remote
About NoScript...
Options...
Allow Scripts Globally (dangerous)
Allow all this page
Temporarily allow all this page
Untrusted
Allow secunia.com
Temporarily allow secunia.com
DOWNLOAD ALL! NOW! FlashGot
Proudly hosted by
easyspeedy
NoScript is Free Software: if you like it, you can support its progress :)
Donate
Flattr this!
PC WORLD WORLD CLASS 2006
Fight CLICKJACKING

The NoScript Firefox extension provides extra protection for Firefox, Seamonkey and other mozilla-based browsers: this free, open source add-on allows JavaScript, Java, Flash and other plugins to be executed only by trusted web sites of your choice (e.g. your online bank).

NoScript also provides the most powerful anti-XSS and anti-Clickjacking protection ever available in a browser.

NoScript's unique whitelist based pre-emptive script blocking approach prevents exploitation of security vulnerabilities (known and even not known yet!) with no loss of functionality...

You can enable JavaScript, Java and plugin execution for sites you trust with a simple left-click on the NoScript status bar icon (look at the picture), or using the contextual menu, for easier operation in popup statusbar-less windows.
Watch the "Block scripts in Firefox" video by cnet.

Staying safe has never been so easy!
Experts will agree: Firefox is really safer with NoScript!

⚠ **Recommended:** Click here to scan Windows for issues causing speed loss

Experts do agree...

08/06/2008, *"I'd love to see it in there."* (Window Snyder, "Chief Security Something-or-Other" at Mozilla Corp., interviewed by ZDNet about "adding NoScript functionality into the core browser").

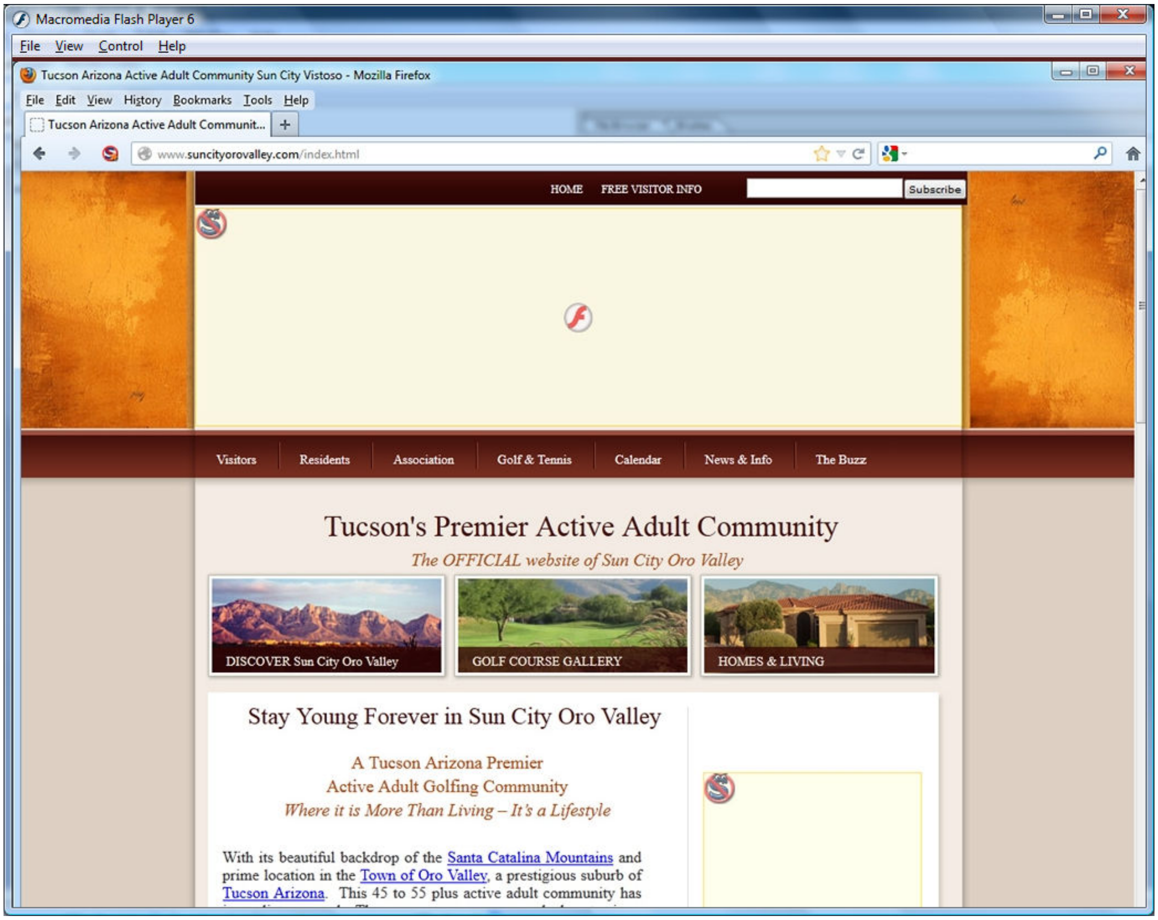
03/18/2008, *"Consider switching to the Firefox Web browser with the NoScript plug-in. NoScript selectively, and non-intrusively, blocks all scripts, plug-ins, and other code on Web pages that could be used to attack your system during visits"* (Rich Mogull on TidBITS, Should Mac Users Run Antivirus Software?).

11/06/2007, Douglas Crockford, world-famous JavaScript advocate and developer of JSON (one of the building blocks of Web 2.0), recommends using NoScript.

03/16/2007, SANS Internet Storm Center, the authoritative source of computer security related wisdom, runs a front-page Ongoing interest in Javascript issues diary entry by William Stearns just to say "Please, use NoScript" :)
Actually, NoScript has been recommended several times by SANS, but it's nice to see it mentioned in a dedicated issue, rather than as a work-around for specific exploits in the wild. Many thanks, SANS!

Now that NoScript is installed in Firefox, let's go look at a webpage and see how this works. I've chosen the Sun City Oro Valley Administration's web site as our guinea pig, today.

You'll notice that some elements are missing from the page. The top image header is missing and there's some content on the lower right that's been blocked as well. No Script puts a little icon over the area (notice the red circle with a line through it?) to let you know it has blocked an element on the page that uses scripts. Just so you know, not all scripts are dangerous, but NoScript doesn't play favorites since it cannot tell which ones are good or bad. It blocks all scripts. These embedded Flash elements are being blocked because Flash is a script-based technology.


Macromedia Flash Player 6
File View Control Help
Tucson Arizona Active Adult Community Sun City Vistoso - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Tucson Arizona Active Adult Communit...
www.suncityorovalley.com/index.html
HOME
FREE VISITOR INFO
Subscribe
Visitors
Residents
Association
Golf & Tennis
Calendar
News & Info
The Buzz
DISCOVER Sun City Oro Valley
GOLF COURSE GALLERY
HOMES & LIVING

Tucson's Premier Active Adult Community

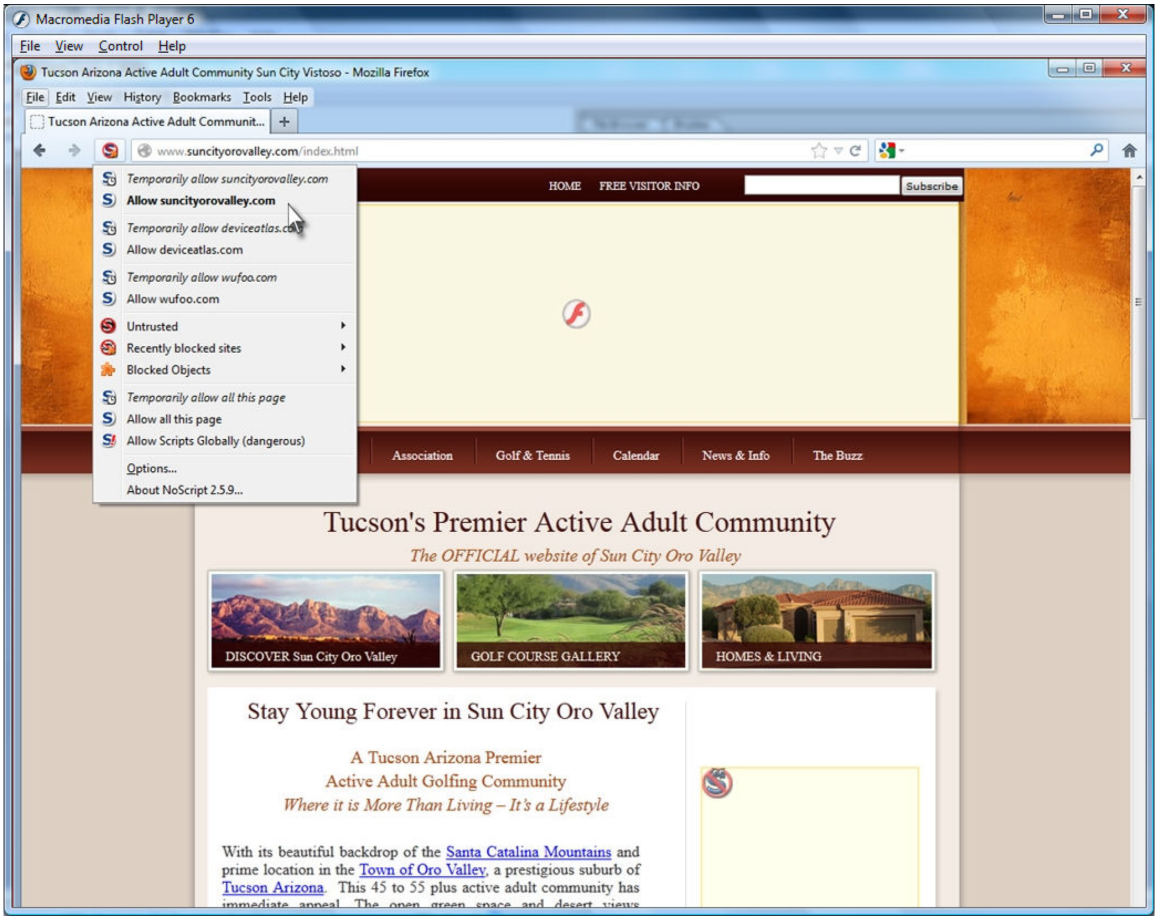
The OFFICIAL website of Sun City Oro Valley

Stay Young Forever in Sun City Oro Valley

A Tucson Arizona Premier
Active Adult Golfing Community
Where it is More Than Living – It's a Lifestyle

With its beautiful backdrop of the Santa Catalina Mountains and prime location in the Town of Oro Valley, a prestigious suburb of Tucson Arizona. This 45 to 55 plus active adult community has

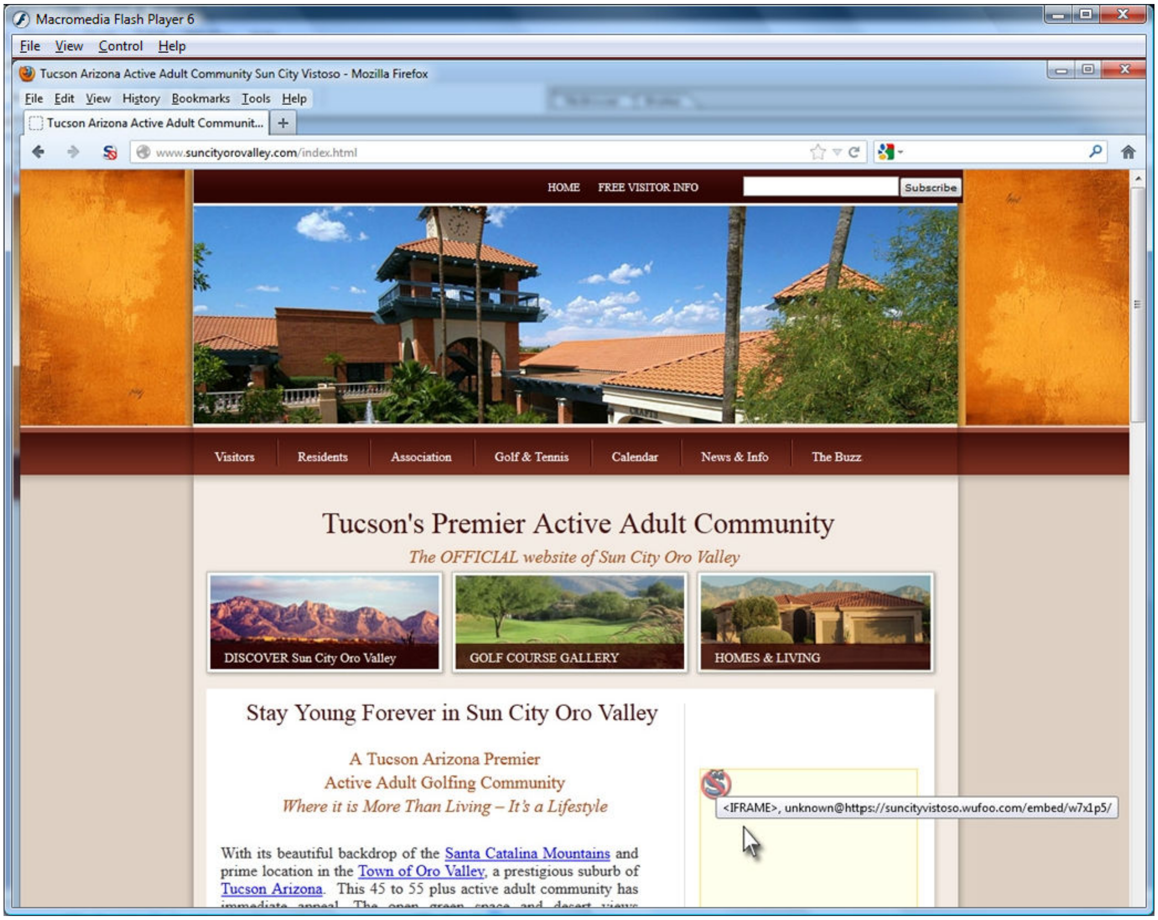
So, this is where we need to make some decisions. Do we trust this web page enough to allow the scripts on this page to run in our browser? Remember, NoScript is stopping ALL scripts on this page unless you tell it otherwise. Since I trust that the Sun City Oro Valley Administration's home page is safe, I'm going to click on the No script icon located just to the left of the URL field in my browser.


Macromedia Flash Player 6
File View Control Help
Tucson Arizona Active Adult Community Sun City Vistoso - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Tucson Arizona Active Adult Communit...
www.suncityorovalley.com/index.html
Temporarily allow suncityorovalley.com
Allow suncityorovalley.com
Temporarily allow deviceatlas.com
Allow deviceatlas.com
Temporarily allow wufoo.com
Allow wufoo.com
Untrusted
Recently blocked sites
Blocked Objects
Temporarily allow all this page
Allow all this page
Allow Scripts Globally (dangerous)
Options...
About NoScript 2.5.9...
HOME
FREE VISITOR INFO
Subscribe
Association
Golf & Tennis
Calendar
News & Info
The Buzz
Tucson's Premier Active Adult Community
The OFFICIAL website of Sun City Oro Valley
DISCOVER Sun City Oro Valley
GOLF COURSE GALLERY
HOMES & LIVING
Stay Young Forever in Sun City Oro Valley
A Tucson Arizona Premier
Active Adult Golfing Community
Where it is More Than Living – It's a Lifestyle

With its beautiful backdrop of the Santa Catalina Mountains and prime location in the Town of Oro Valley, a prestigious suburb of Tucson Arizona. This 45 to 55 plus active adult community has immediate appeal. The open green space and desert views

This initiates a drop-down window with a number of options to choose from. I'm going to trust all content that is hosted at suncityorovalley.com by left-clicking on the 'Allow suncityorovalley.com' option.

There, that's better. Now I can see the top header image properly. NoScript actually puts my approvals into a white-list for me, so that I don't have to go through this process every time I visit this site.


Macromedia Flash Player 6
File View Control Help
Tucson Arizona Active Adult Community Sun City Vistoso - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Tucson Arizona Active Adult Communit...
www.suncityorovalley.com/index.html
HOME FREE VISITOR INFO
Subscribe
Visitors Residents Association Golf & Tennis Calendar News & Info The Buzz
DISCOVER Sun City Oro Valley
GOLF COURSE GALLERY
HOMES & LIVING

Tucson's Premier Active Adult Community

The OFFICIAL website of Sun City Oro Valley

Stay Young Forever in Sun City Oro Valley

A Tucson Arizona Premier
Active Adult Golfing Community
Where it is More Than Living – It's a Lifestyle

With its beautiful backdrop of the Santa Catalina Mountains and prime location in the Town of Oro Valley, a prestigious suburb of Tucson Arizona. This 45 to 55 plus active adult community has

<IFRAME>, unknown@https://suncityvistoso.wufoo.com/embed/w7x1p5/

Ah, but did you notice that there's still a problem with the content on the right side of this page? Since this content isn't hosted at suncityorovalley.com, it's actually being pulled in from another domain. If I decide to trust this content also, I can also choose from the NoScript options menu and allow it as well.

Final Summary:

Don't forget that NoScript is installed, otherwise you'll get confused/aggravated when a web page does not look or behave as you might have expected.

A note on configuring No Script: To prevent against implementations of iFrames, you should change the default settings under “NoScript Options|Embedded” and check the relevant “Forbid Frames/iFrames" options.

Fraudware distributors have been utilizing "SEO Poisoning" (search engine optimization) techniques by pushing infected URLs to the top of search engine results about recent news events. People looking for articles on such events on a search engine may encounter results that, upon being clicked, are instead redirected through a series of sites before arriving at a landing page that contains a Drive-by download.

Cold-calling has also become a vector for distribution of fraudware, with callers often claiming to be from "Microsoft" or "Windows" or another legitimate-sounding organization. The caller claims that the user's computer is infected and that the caller needs access in order to remove the infection. The caller then provides the user with a link to a web page containing a backdoor client, giving the caller complete access to the user's computer.
