Internet Attacks

DOWNLOADED BROWSER CODE

DYNAMIC CODE

Users of the Web demand an interface that changes based on certain events such as who the user is, the time of day, or what they click on.

This type of content is dynamic and cannot be created using static HTML code. Whenever dynamic code is introduced to a Web page, the browser has to obtain the code and process it.

The most common examples of downloaded browser code are **JavaScript**, **Java**, and **ActiveX**.

JAVASCRIPT

JavaScript cannot create a standalone program like C++ or Visual Basic. It is only meant to live in HTML code and be interpreted into a recognizable language by your browser.

If you wish to surf the web and not have to worry about running JavaScript, you can control the running of active script like JavaScript within your browser's settings. Click on the image or link below to see how this is done. Warning: if you enable prompting, you may find it annoying!

http://coursecontent.ntc.edu/CIT/husband/pois/lp3/ControlActiveScript/ControlActiveScript.html

JavaScript, by design, is not allowed to read, write, create, delete or list the files on the computer that runs the JavaScript. This is meant to prevent serious harm.

Click on the image or link below to see how JavaScript works.

http://coursecontent.ntc.edu/CIT/husband/pois/lp3/m21-JavaTest.html

JavaScript can be a created with the sole goal of getting information from a user such as a password, an e-mail, a credit card number, or an annoying prompt that never goes away.

Click on the image or link below to see for yourself - if you dare!

NOTE: The link below is currently disabled, but I am working on making this available soon.

http://www2.ntc.edu/IT/heckendo/other/greggs_js.html

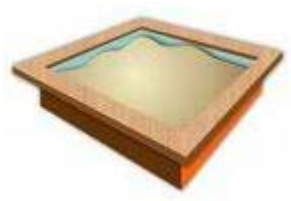
JAVA

Java is a complete programming language and it creates applications. When Java is included in HTML, it is referred to as a Java applet, much in the same way an image is included in a page.

When you use a Java technology-enabled browser to view a page that contains an applet, the applet's code is transferred to your system and executed by the browser's Java Virtual Machine (JVM).

Java applets can be trusted (signed) or not trusted (unsigned). Those applets that are unsigned run in a sandbox to fence them away from the resources on your computer. Sandboxing a Java applet is not always 100% effective, however.

Click on the image or link below to get more information.



http://www.securingjava.com/chapter-two/chapter-two-1.html

ACTIVEX

There is no scripting or programming involved with ActiveX because ActiveX are just controls (or add-ons). These controls can be activated through the use of a scripting language or by using HTML code.

ActiveX controls work similar to a Java applet and can perform many of the same functions; however, ActiveX controls do not run in a sandbox.

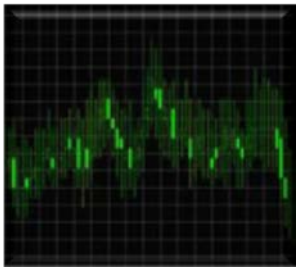
Click on the image or link below to get more information.

http://news.cnet.com/2009-1001-208208.html

ActiveX has risk. To minimize this risk, browsers register and authenticate ActiveX controls before downloading them. ActiveX controls can be signed or unsigned. Being signed does not guarantee trust, however.

ActiveX controls are usually allowed in by the user based on the source of the control, not the control itself. Security is initiated by the browser only; some applications that use ActiveX can bypass this security.

As with the control that can be initiated with action scripts, so to can control be initiated on ActiveX. Click on the image or link below to see how this is done.



http://coursecontent.ntc.edu/CIT/husband/pois/lp3/ControlActiveX/ControlActiveX.html

PRIVACY ATTACKS

An attack on your privacy means that someone is stealing your personal information. If the personal information is enough to claim your identity, then you are in for a ride of your life. This section describes how this can take place.

COOKIES

Cookies are small files that are stored on a user's hard drive that contain information about a user's preferences to a particular Web site. When these cookies are used by the Web site that created the cookies, these cookies are called 1st party cookies.

When these cookies are used by a Web site other than what they are intended to be used for, the cookie is called a 3rd party cookie and could be an invasion of the user's privacy, such as with web site tracking.

CONTROLLING COOKIES

If a person visits a lot of Web sites and never deletes cookies, thousands of them can accumulate. The accumulation of these cookies could become a security risk and will definitely slow the computer down.

Your browser has settings to control the storage and use of cookies.

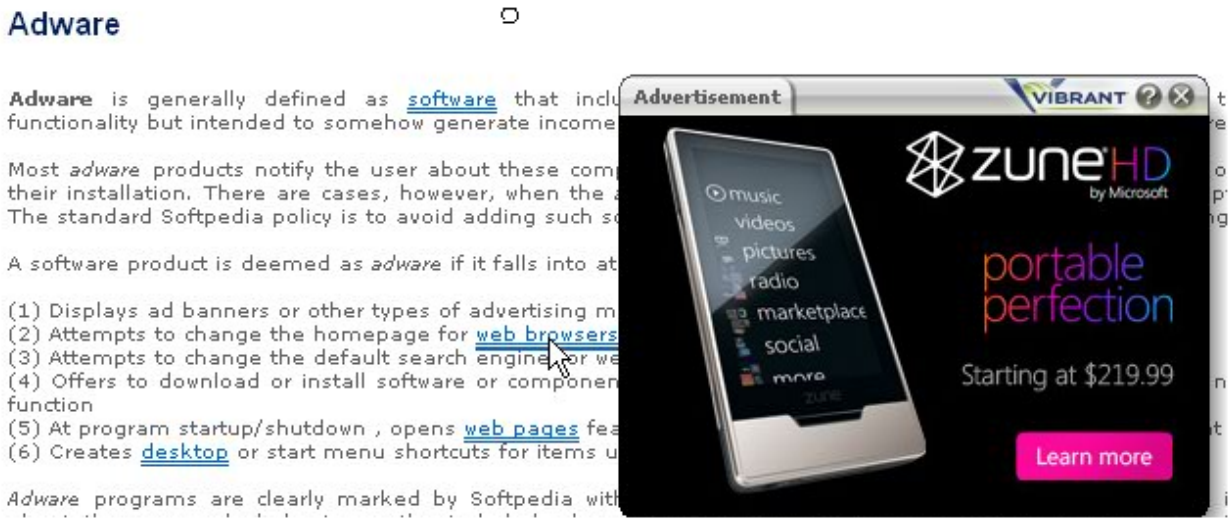
http://coursecontent.ntc.edu/CIT/husband/pois/lp3/ControlCookies/ControlCookies.html

SPYWARE/ADWARE

Spyware is software that has been created to spy on you. It is installed usually without your knowledge or consent as part of other software packages, or can be installed simply by browsing on a malicious webpage.

Some spyware will log your browsing habits, and send reports to databases elsewhere in the world. While some will search through your hard drive in order to find personal information and credit card numbers, passwords or any information that it has been designed to steal.

Adware is related to spyware, in that they both invade your computer through software that usually is installed without the user's consent or knowledge. What adware does, though, is turn your computer into a bill board by constantly loading advertisements onto your screen. An example is shown in the image below.



ATTACKS WHILE SURFING

Unfortunately, the "waters" of the Internet **cannot** be considered safe if all you do is passively search and do not interact with a Web site.

Just by going to a Web site you could be attacked and eaten. Swim at your own risk.

Common risks are being redirected to malicious web sites or drive-by downloads.

REDIRECTED TO MALICIOUS WEB SITES

Most of the web traffic redirection comes from user's mistyping a URL or typing a URL that they think is the appropriate Web site.

For example, if you type http://www.fedora.org thinking that you are going to the Fedora Linux Web site, you are wrong. Fortunately, this site is not malicious, at least not to me.

If the folks that owned this Web site changed it to look like the actual Fedora Web site, they could potentially cause you harm.

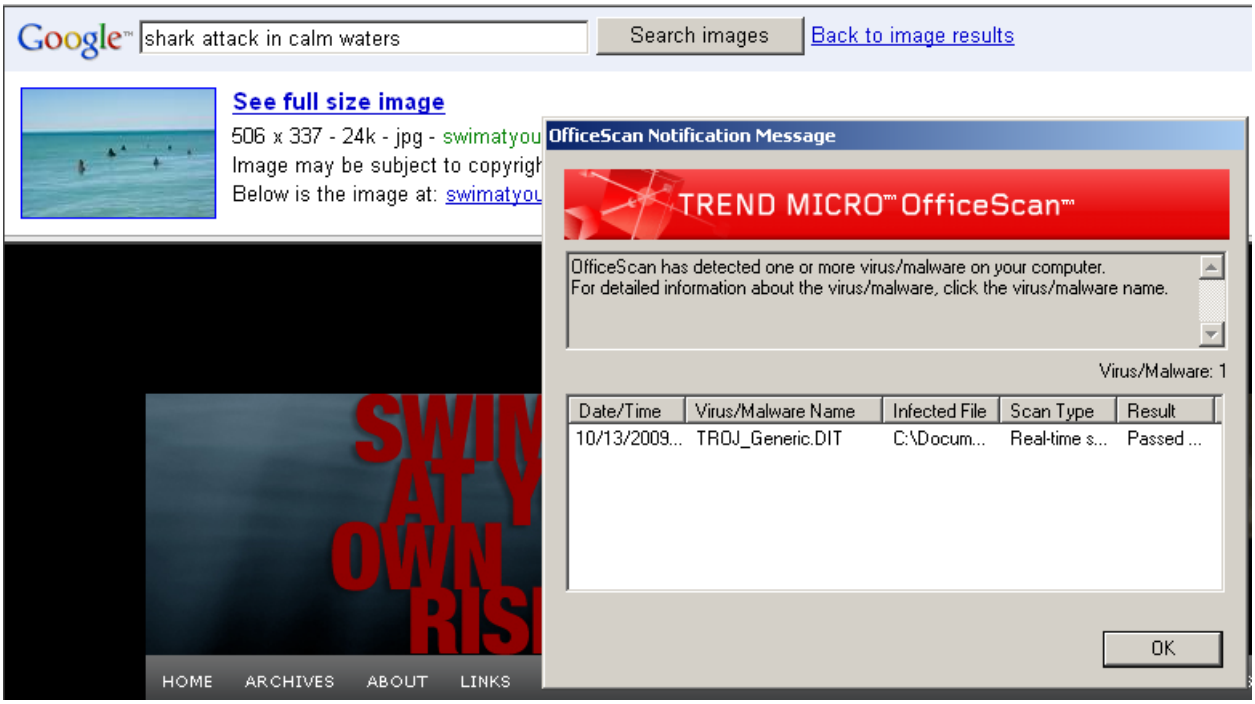
DRIVE-BY DOWNLOADS

Well known sites, as well as run-of-the-mill sites, are increasingly being compromised with code (such as JavaScript) that could exploit a VULNERABILITY in your browser and in-turn download malicious software from the ATTACKER'S computer to your computer - perhaps making your

computer a bot in a botnet.

This can be done without you knowing it through an invisible HTML Web page (an iFrame or Inline Frame) embedded in the Web page you are viewing. See image below for an example of iFrame HTML code.

Ironically, while researching (Google searching) this segment, I encountered numerous attacks. Fortunately, my anti-virus software stopped the attacks. See image below.



Warning: please do not search for the images associated with "shark attack in calm waters", unless you know you have really good anti-virus software.

E-MAIL ATTACKS

One of the more common means of distributing attacks is through e-mail. These include sending spam, malicious attachments, and embedded hyperlinks.

SPAM

If you are a frequent e-mail user, you've likely experienced the problem of spam cluttering your inbox. These unwanted mass mailings are usually sales pitches, money making schemes or special offers.

According to Nucleus Research, Spam can cost corporations an estimated $874.00 per person in loss of productivity.

You certainly can get rid of spam e-mail by deleting it, but most people would rather not see it - never.

You can unsubscribe to some spam, but most spam you have to filter, either thru the e-mail server or thru your e-mail client application.

Click on the image or link below to view a demo from spam bully.

http://www.spambully.com/demo4.php

Spam filtering is becoming difficult to manage because spammers use very clever ways to camouflage their spam.

To hide the content, they can put text in an image and they can vary the images by using layering, splitting and geometric variances. See the examples in the images below.

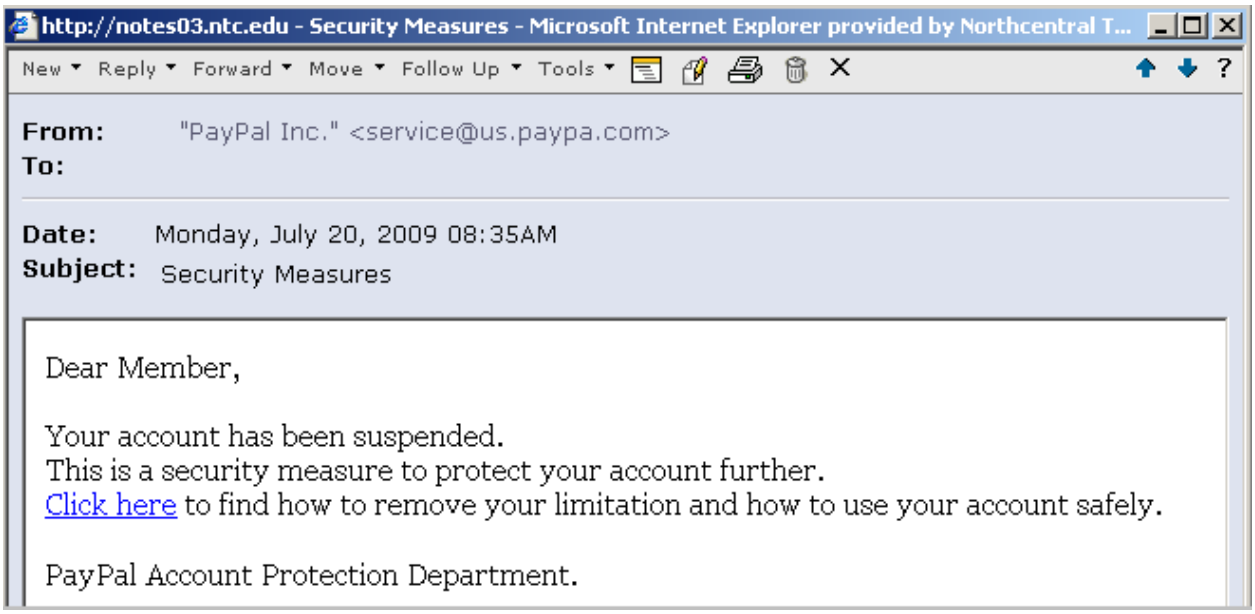
MALICIOUS ATTACHMENTS

Attachments are files that are sent along with your e-mail and are "attached" to your e-mail. These files could contain malicious code and likely to spread to other e-mail users in your e-mail address book if you open it, thus creating a distributed attack.

The trick to getting the user to open such a file is to make them believe that the source of the e-mail is someone they can trust - like a friend or co-worker.

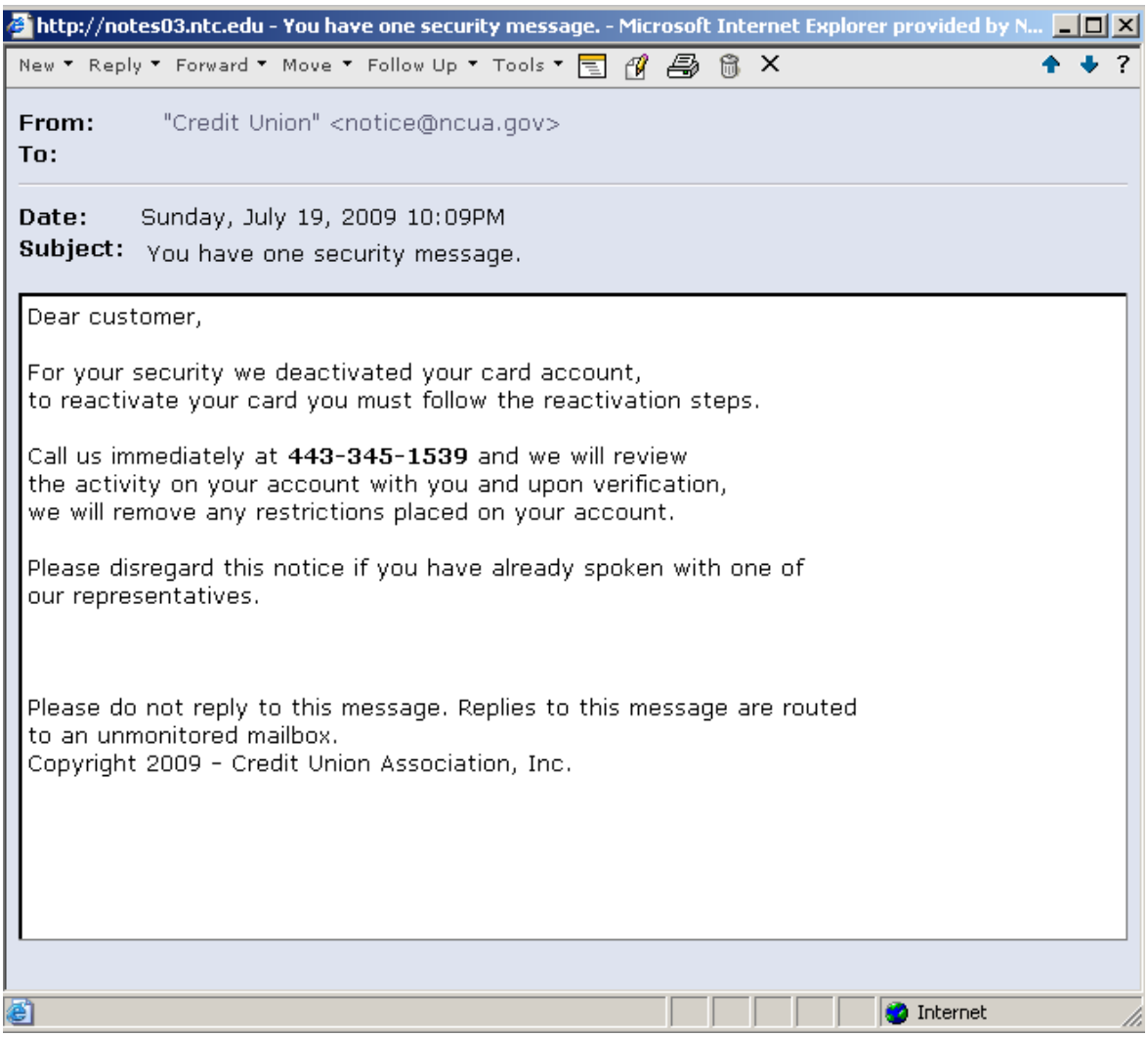
IMBEDDED HYPERLINKS

Have you ever gotten an e-mail from PayPal, Bank One, or Visa saying that your account has been tampered with and then asking you to click on the link inside the e-mail wanting you to confirm your account information - like the one in the image below?



DO NOT OPEN THESE EMAILS! MOST COMPANIES SUCH AS PAYPAL, BANK ONE, ETC. DO NOT SEND EMAILS TO THEIR CUSTOMERS. IT IS VERY EASY TO SEND AN EMAIL WITH A FAKE "FROM".

How about just plain old phone scams via. e-mail? See image below.


http://notes03.ntc.edu - You have one security message. - Microsoft Internet Explorer provided by N...
New
Reply
Forward
Move
Follow Up
Tools
From: "Credit Union" <notice@ncua.gov>
To:
Date: Sunday, July 19, 2009 10:09PM
Subject: You have one security message.
Dear customer,
For your security we deactivated your card account,
to reactivate your card you must follow the reactivation steps.
Call us immediately at 443-345-1539 and we will review
the activity on your account with you and upon verification,
we will remove any restrictions placed on your account.
Please disregard this notice if you have already spoken with one of
our representatives.
Please do not reply to this message. Replies to this message are routed
to an unmonitored mailbox.
Copyright 2009 - Credit Union Association, Inc.
Internet