

Image Spam

Introduction

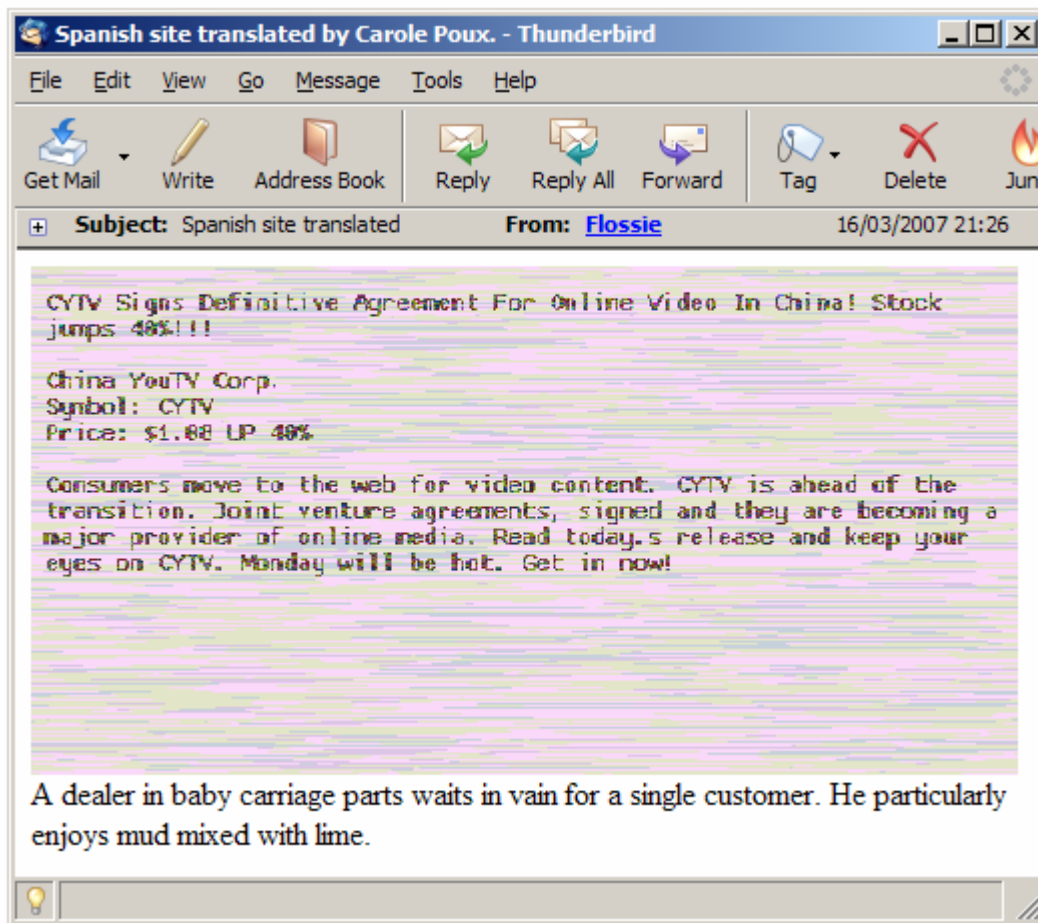
Image spam is a kind of E-mail spam where the message text of the spam is presented as a picture in an image file. Since most modern graphical E-mail client software will render the image file by default, presenting the message image directly to the user, it is highly effective at circumventing normal E-mail filtering software.

E-mail spam, also known as junk e-mail, is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. A common synonym for spam is unsolicited bulk e-mail (UBE). Definitions of spam usually include the aspects that email is unsolicited and sent in bulk. "UCE" refers specifically to unsolicited commercial e-mail.

Project description:

E-mail spam has steadily, even exponentially grown since the early 1990s to several billion messages a day. Spam has frustrated, confused, and annoyed e-mail users. Laws against spam have been sporadically implemented, with some being opt-out and others requiring opt in e-mail. The total volume of spam (over 100 billion emails per day as of April 2008[update]) has leveled off slightly in recent years, and is no longer growing exponentially. The amount received by most e-mail users has decreased, mostly because of better filtering. About 80% of all spam is sent by fewer than 200 spammers. Botnets, networks of virus-infected computers, are used to send about 80% of spam. Since the cost of the spam is borne mostly by the recipient, it is effectively postage due advertising.

E-mail addresses are collected from chatrooms, websites, newsgroups, and viruses which harvest users' address books, and are sold to other spammers. Much of spam is sent to invalid e-mail addresses. ISPs have attempted to recover the cost of spam through lawsuits against spammers, although they have been mostly unsuccessful in collecting damages despite winning in court. Spam averages 94% of all e-mail sent.



Techniques can include:

- Blurring of text outlines
- Construction of the image from multiple image layers assembled within an HTML e-mail
- Use of animated image formats

- Random noise added to the image (also known as confetti) to prevent the detection of multiple similar images using hash algorithms

Currently, the surest known countermeasure for image spam is to discard all messages containing images which do not appear to come from an already whitelisted E-mail address. However, this has the disadvantage that valid messages containing images from new correspondents must either be silently discarded, or that bogus "backscatter" bounce messages must necessarily be generated to the reply-to addresses in junk mail messages, enabling denial-of-service attacks by spammers.

To the casual observer, this message appears to be a standard text-based email complete with hyperlinks. Only a careful look reveals that the entire message is actually an image. The message didn't contain any text, just the HTML code to display this image. My spam filter apparently didn't recognize the source of the message as a known spammer and there weren't any keywords to analyze, so it arrived in my inbox.

The image above doesn't contain any clickable links and it's unlikely someone would be so enthralled with a spam message that they would type the URL into their browser. So why do spammers use this technique? The majority of these messages are classic "pump and dump" stock scams, where the spammer invests in a stock and then sends out messages hyping the stock, hoping to inspire a quick, profitable run.

The best security measure against image spam is tried-and-true end user awareness. Make sure your users are aware of this risk and understand the classic instructions about responding to spam and phishing attempts. Second, consider updating your antispam infrastructure. Vendors are aware of this threat and are investing in research to improve their products' detection capabilities. If you're already running an enterprise antispam solution, you may be able to get a free upgrade as part of your maintenance agreement.

Image spam is just the latest salvo in the battle between spammers and those of us who just want to peacefully send and receive email. Watch as technologies evolve to battle this threat, and don't expect it to be the last novel attack against our infrastructures.



Stock spam has increased in volume in recent times and now represents a significant percentage of what we see each day. In 2006 alone we saw more than 300 different stocks being spammed. The nature of this type of spam allows spammers to use images to hide the information on the stock they are promoting without the need for any URLs or filterable content in the body making it harder to detect. The following is a recent example of a stock spam image:

Investors Report: 03/06/2007
THIS STOCK WILL EXPLODE ON WEDNESDAY 03/07/2007

****This Weeks TOP PICK****
IFTC.OB

-LOOK AT OUR RECENT NEWS!!!-

Company	:	Infotec Business SYS
Symbol	:	IFTC.OB
Current Price	:	\$0.06
5 Day Target	:	\$0.80
Last Traded	:	226,600

-IN THE NEWS-

Wavelit.com Announces Strategic Relationship
with Broadband Enterprises

Thursday March 1, VANCOUVER,

British Columbia--(BUSINESS WIRE)--(OTCBB:IFTC)
and Broadband Enterprises. Considered the premier
online video network, Broadband Enterprises
has been contracted to sell the pre-roll video
commercials shown before all video content on
Wavelit.com

READ OUR NEWS NOW!
IFTC.OB

THIS STOCK WILL EXPLODE ON WEDNESDAY 03/07/07

Phishing:

Spam is also a medium for fraudsters to scam users to enter personal information on fake Web sites using e-mail forged to look like it is from a bank or other organization such as PayPal. This is known as phishing. Spear-phishing is targeted phishing, using known information about the recipient, such as making it look like it comes from their employer.

SOFTWARE SPECIFICATION

- ◆ Front end : Java / .Net
- ◆ Back end : My SQL /MS SQL Server
- ◆ Operating system : LINUX/ Windows
- ◆ IDE : Net beans/ Visual Studio

MICROSOFT WINDOWS :

Any windows based operating system (such as Windows 95, Windows 98, Windows 2000) can be used to operate the software. We have used Windows 2000 Professional as the platform of our project. This operating system is more reliable in working ASP.NET.

.NET

The **Microsoft .NET Framework** is a software framework that can be installed on computers running Microsoft Windows operating systems. It includes a large library of coded solutions to prevent common programming problems and a virtual machine that manages the execution of programs written specifically for the framework. The .NET Framework is a key Microsoft offering and is intended to be used by most new applications created for the Windows platform. Programs written for the .NET Framework execute in a software environment that manages the program's runtime requirements. Also part of the .NET Framework, this runtime environment is known as the Common Language Runtime (CLR).

ASP.NET :

Microsoft ASP.NET is a free technology that allows programmers to create dynamic web applications. ASP.NET can be used to create enterprise-class web applications and webpages. ASP.NET is the latest version of Microsoft's Active Server Pages technology (ASP).ASP.NET is a part of the Microsoft .NET framework, is a powerful tool for creating dynamic and interactive web pages.

SQL SERVER 2000 :

It is computer based record keeping system, ie. a system whose overall purpose is to be record and maintain information . This SQL SERVER system allow users to create containers (eg. tables) for data storage and management. A group of Tables with Related data in them is called a Database.

HARDWARE SPECIFICATION

- ◆ Processor : Pentium IV OR Above
- ◆ Primary Memory : 256 MB RAM
- ◆ Storage : 40 GB Hard Disk
- ◆ Display : VGA Color Monitor
- ◆ Key Board : Windows compatible
- ◆ Mouse : Windows compatible