### Web Browser Attacks: Summer 2006 Threat Landscape

### Lenny Zeltser

### July 25, 2006

# The browser is becoming a universal platform for important transactions.

### Protecting the web browser is critical to ensuring security of transactions.

1 998744

99861462A

12 Anna State State

NIES OF ADIRICIUM

L 99835462A

.99822462A

12

# Attackers use the web browser as a gateway for application-level attacks.



Understand browser threats to establish an effective defense strategy.

# Let's group browser-oriented attacks in three general categories.



### #1: Website to personal computer



#2: Personal computer to website



#3: Website to website

### #1: A malicious site compromising the PC via the browser



Website





**Personal Computer** 



PopupSh.ocx Properties	? 🛛			
General Version Digital Sign	atures Security Summary			
File version: 1.0.0.1				
Description: PopupSh Active	eX Control Module			
Copyright: Copyright (C) 2004				
Other version information —				
Item name:	Value:			
Company File Version Internal Name Language Legal Trademarks OLESelfRegister Original File name <b>Product Name</b> Product Version	PopupSh ActiveX Control			
	OK Cancel Apply			

### An ad on MySpace installed adware on up to 1 million PCs.

## According to Hitwise, MySpace is the Web's most popular destination.



GENERATED ON: 07/12/2006. COPYRIGHT 2006 (C) 'HITWISE PTY LTD'.

Website market share chart by Hitwise

# The PopupSh ActiveX Control has operated for about one month.

### Control panel.

*Total installations: Installations per month: Installations per day: Installations per hour:* 

Installations:



Screenshot on right by Michael La Pilla via Security Fix

## The WMF exploit and the patch have been available for 7 months.

MSFConsole				_ 🗆 X
msf > info ie_	_xp_pfv_metaf	ile		<b>^</b>
Name: Windows XP/2003/Vista Metafile Escape() SetAbortProc Code Execution Class: remote Version: \$Revision: 1.18 \$ Target OS: win32, winxp, win2003 Keywords: wmf Privileged: No Disclosure: Dec 27 2005				
san <san [<="" td=""><td><hdm [at]="" me<br="">[at] xfocus.o ]S[at]unknown</hdm></td><td>rg&gt;</td><td>n an an</td><td></td></san>	<hdm [at]="" me<br="">[at] xfocus.o ]S[at]unknown</hdm>	rg>	n an	
Available Targ Automatic	rets: - Windows XP	) ∕ Windows	2003 / Windows Vista	
Available Opti	ions:			
Exploit:	Name	Default	Description	
optional optional required	REALHOST HTTPHOST HTTPPORT	0.0.0.0 8080	External address to use for redirects (NAT) The local HTTP listener host The local HTTP listener port	
Payload Inform Space: 150	)4 :haracters			
Avoid: 1 c Keys: noc	onn tunnel r	everse		

### WebAttacker automates the creation of malicious websites.

Veb-Attacker (IE0604) config editor 🛛 🛛 🔀		
Enter here an URL path for CGI-script on your server		
http://www.yourhost.com/cgi-bin/ie0604.cgi		
Enter here the folder name for placing an output exploit components		
c:\Ie0604\Output		
Web-Panel password : admin		
OK Cancel Encrypt HTML files		
OK Cancel Г Encrypt HTML files Эксплойт - Web-Attacker I антивирусами:	Е0604 не обнаруж	ивается следующим
Эксплойт - Web-Attacker I	Е0604 не обнаруж [Версия]	кивается следующим [Дата баз]
Эксплойт - Web-Attacker I антивирусами:		
Эксплойт - Web-Attacker I антивирусами: Названия Антивируса	[Версия]	
Эксплойт - Web-Attacker I антивирусами: Названия Антивируса Doctor Web	[Версия] 4.33	
Эксплойт - Web-Attacker I антивирусами: Названия Антивируса Doctor Web NOD32 Antivirus	[Версия] 4.33 2.5	

Panda Titanium Antivirus

11.04.2006

2005

# A control panel lets the operator monitor campaign effectiveness.

🔮 Exploit penetration statistics - Microsoft Internet Explorer						
<u>File Edit View Favorites Tools H</u> elp				<i>.</i>		
G · O · 🖹 🛢 📢	🏠 🔎 🛧 😔	🖉 • 💺 📑 • 🖵	P 🛍			
Address	Address 🖉			Go		
		<b>Overall</b> s	tatistics			^
						=
Total hosts	M803-11	MS04-013	M805-020	0-Day	<b>MS06-006</b>	
39097	1906	32	99	1502	0	
100.00 %	4.88 %	0.08 %	0.25 %	3.84 %	0.00 %	
Total Exploit efficiency is 9.05 %						
<b>Operation Systems statistics</b>						
OS name	Hosts M	4803-11 M80	4-013 M805-	-020 0-Day	<b>MS06-006</b>	~
ど Done					🥑 Internet	

# Average exploit success rate: 10%

## The malicious site attack often includes three components.

Exploit

Dropper

### Payload

## #2: Malware on the PC compromising website interactions via the browser



### **Personal Computer**





Website

Copyright © 2006 Lenny Zeltser. All rights reserved.

# A spoofed E-Gold email encouraged the recipient to open the attachment.

🞽 egold transaction - Message (Plain Text)	
Eile Edit View Insert Format Tools Actions Help	
📴 🕰 Reply   🖓 Reply to All   😂 Forward   🎒 🗈   😽   🏲   🍅   👫 🗙   🔶 🔹	≻ - A <sup>‡</sup>   🕐 📮
From:       jim duffy [jimduffy11@yahoo.com]       Sen         To:	it: Mon 7/24/2006 3:56 PM
Hello Yesterday I checked my E-Gold account and was really shoked to find a (100,177.90 USD) there. I have never had such a big amount of money of my account was only 177.90 USD) and I have no even a slightest ide money. Upon receiving the requested history of records I realized that made 2 hours before, and the Memo field contained your e-mail address In a short run, while I was making the inquiries, the money and MY own disappeared. I changed my password immediately and now intend to c investigate the people, who involved me in the unfair play. Fortunately attached in this letter. Hope for your assistance in this matter. I feel a little bit scared and still hesitate to apply to E-gold support serv Best regards, Jim Duffy	v available (the last balance ea about the origin of the the transfer had been ss:com n savings of 177 USD larify the situation and to I made a screenshot copy,

## The dropper downloaded a program that spied on E-Gold transactions.

https://www.e-gold.com/acct/

https://www.e-gold.com/acct/spend.asp

https://www.e-gold.com/acct/verify.asp

# Another spyware spread via spoofed email targeted banking credentials.

From: "Spysoftcentral Team" <sales@spysoftcentral.com> Subject: Order Approval Notification SPY DOCTOR / Order : DD269901/ This e-mail was generated by a mail handling system. Please do not reply to the address listed in the "From" field. Please read the CUSTOMER SERVICE section for answers to your questions. Dear Madame/Sir, Thank you for your order. Spysoftcentral processes orders and collects payments on behalf of PC Tools. . . .

### 😻 Windows Firewall

General Exceptions Advanced

### Ø

### Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.



### On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

### Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.



### Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

0K

Cancel

Windows Firewall is using your non-domain settings.

What else should I know about Windows Firewall?

The dropper tweaked Windows firewall settings before downloading the spyware.

## A powerful Sdbot variant had worm, backdoor and spyware capabilities.





### Text file "devenv.dll" contained a log of the day's activity.

## #3: A malicious site compromising website interactions via the browser



Website





Website



Web | MySpace | People | Music | Blogs | Video | More »

Search

Home | Browse | Search | Invite | Film | Mail | Blog | Favorites | Forum | Groups | Events | Videos | Music | Comedy | Classifieds



**HySpace Music** 

Cool three P

### A worm spread through MySpace via embedded Flash objects.

# A Flash object in a person's profile redirected to another MySpace page.

ActionScript in redirect.swf:

getURL("http://editprofile.myspace.com/index.cfm? fuseaction=blog.view&friendID=94634371& blogID=143876075", "\_self");

ActiveScript above from kinematictheory.phpnet.us

The malicious page embedded the worm in the victim's profile.

## MySpace has disabled network access from embedded Flash objects.

allowNetworking="internal"

# An XSS flaw on the PayPal website fueled a powerful phishing campaign.



### The spoofed page seemed to reside on www.paypal.com.

😉 PayPal - Error Detected - Mozilla Firefox 📃	
Eile Edit View Go Bookmarks Tools Hele	
🖕 • 🛶 - 🛃 😣 😭 (P https://www.paypal.com/x tk/	
Error Detected	
This recipient does not accept payments denominated in US	
Your account is currently disabled because we think it has been accessed by a third part You will now be redirected to Resolution Center.	ty.
Go to PayPal Acc	count
	5
Connected to www.paypal.com	n 📇 🍃

Screenshot by Netcraft

# The exploit may have been active for two years before it got fixed.

If the email address of the account you are donating to has the following message on the donation page:

'This recipient is currently unable to receive money.'

You can exploit this flaw by replacing the currency value in the donation form with a "> followed by any html you wish to execute.

Exploit by "e\_D"

## Many other websites have similar XSS vulnerabilities.

### An XSS hole was found on visa.com; it's now fixed.

🥹0wn3d again - Mozilla Firefox		
<u> Eile E</u> dit <u>V</u> iew <u>Go B</u> ookmarks <u>T</u> ools <u>H</u> elp		
🗇 • 🛶 • 🔗 • 🛞 🚷 🚺 http://visases	rch.visa.com/UsaSearch/query.html?col=usa&qp	
FIRST BANK OF PHISHING		
View Your Accounts	Welcome to Secure Science ( (DFP) on-line demo site!	
New user? <u>Learn more   Enroll</u> Username:	Become your own phisher. D your own phishing server!	
Password:	➤ Generate a phishing email	
Sign On	≻ <u>Track</u> a phisher	
Forgot your ID?	► Detect a proxy	

Screenshot by Lance James via Security Fix

### An XSS hole was found on Microsoft; it's now fixed.

Microsoft	
Genuine Microsoft Sof	tware
Genuine Microsoft Software	How to Tell
About Genuine Microsoft Software Frequently Asked Questions Worldwide Sites	Validation Complete!
Product Resources Support Security Downloads Piracy Software Asset Management Special offers for genuine Windows customers	Thank you for validating your copy of Microsoft Windows. Click Continue to return Continue Continue Continue Continue

Screenshot by Lance James via Security Fix

# Consider the 3 categories when devising a browser defense strategy.



### #1: Website to personal computer



#2: Personal computer to website



#3: Website to website



### Lenny Zeltser InfoSec Practice Leader Gemini Systems, LLC

lenny.zeltser@gemini-systems.com www.zeltser.com