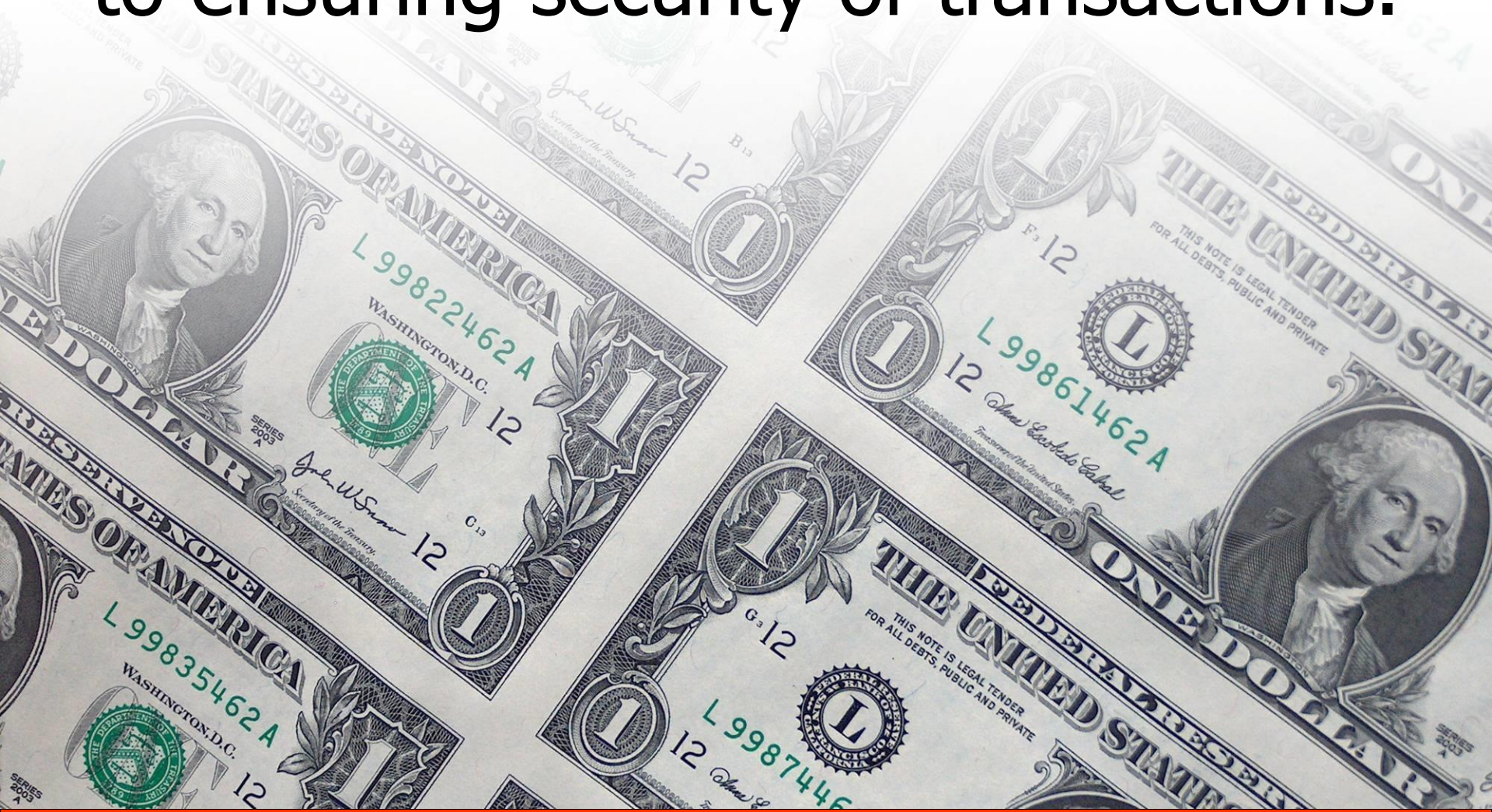

Web Browser Attacks: Summer 2006 Threat Landscape

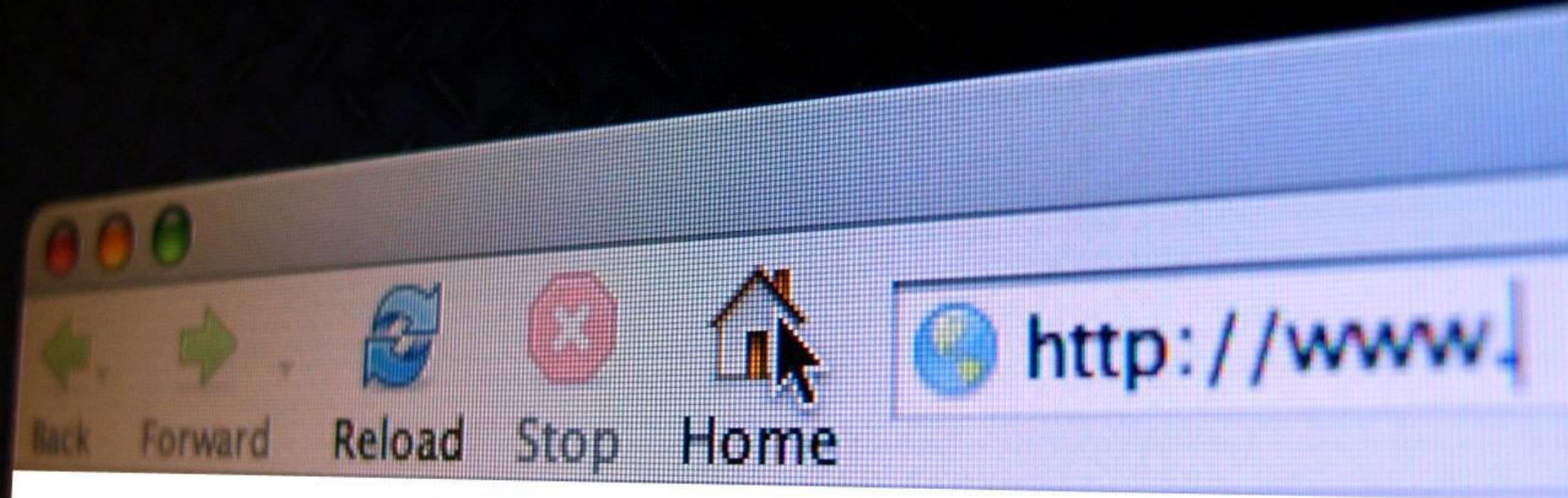
Lenny Zeltser

July 25, 2006

The browser is becoming a universal platform for important transactions.

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





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

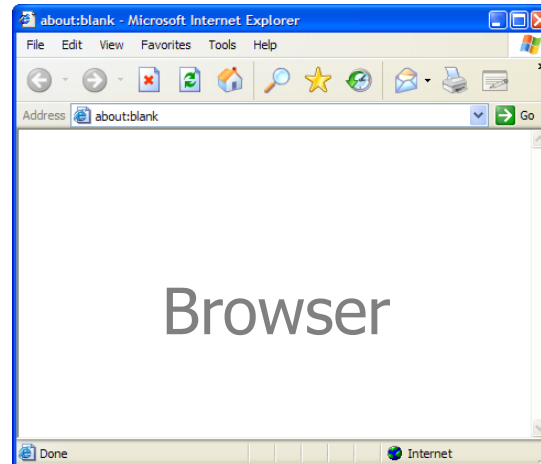
#1: A malicious site compromising the PC via the browser



Website

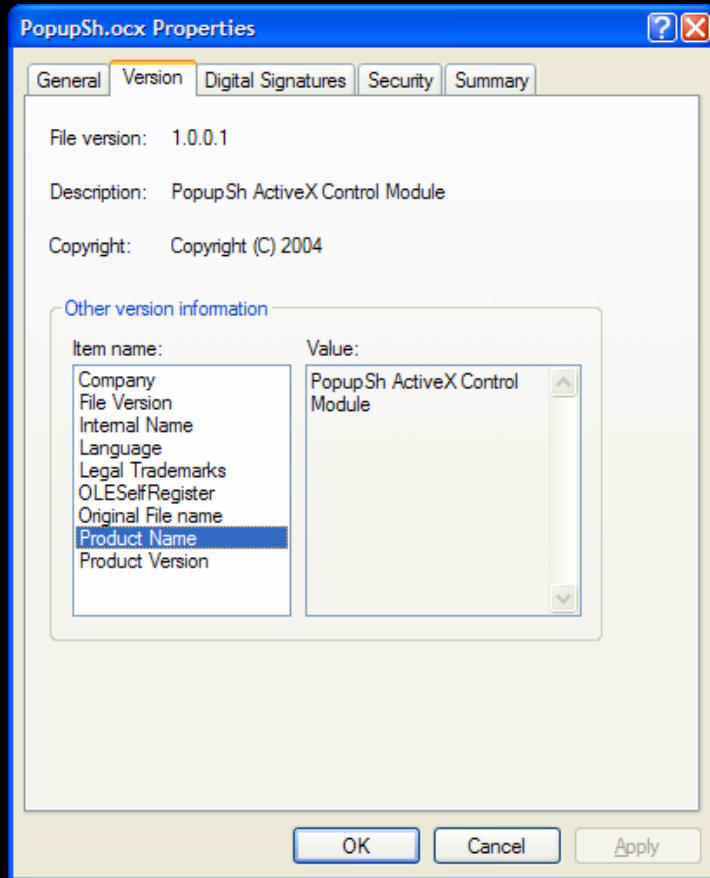


Personal Computer



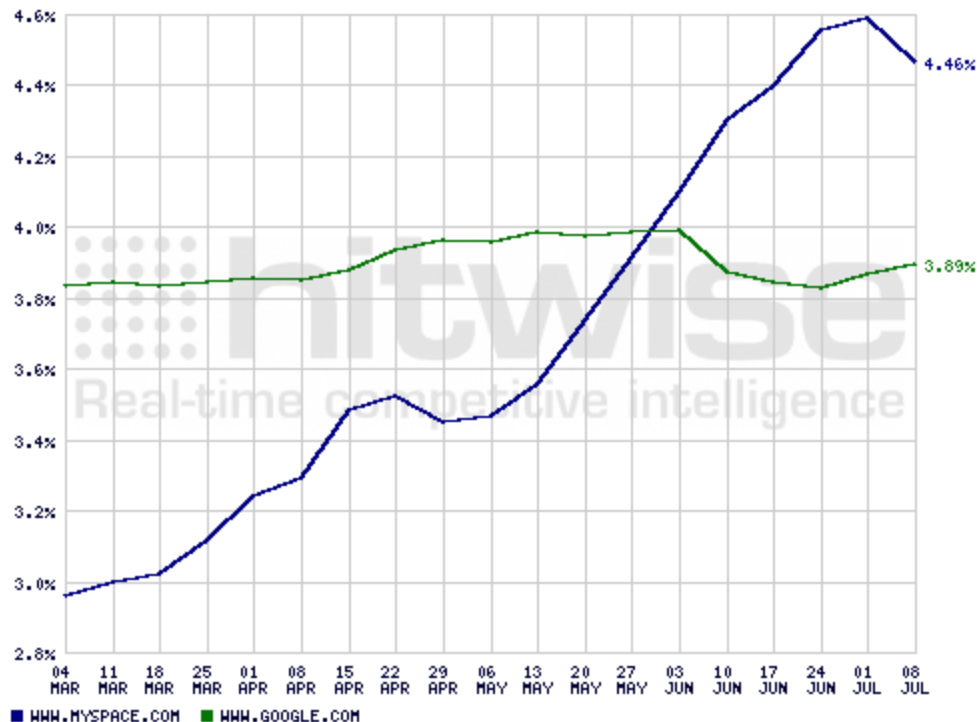
Browser





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

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



Visits to MySpace.com

Visits to Google.com

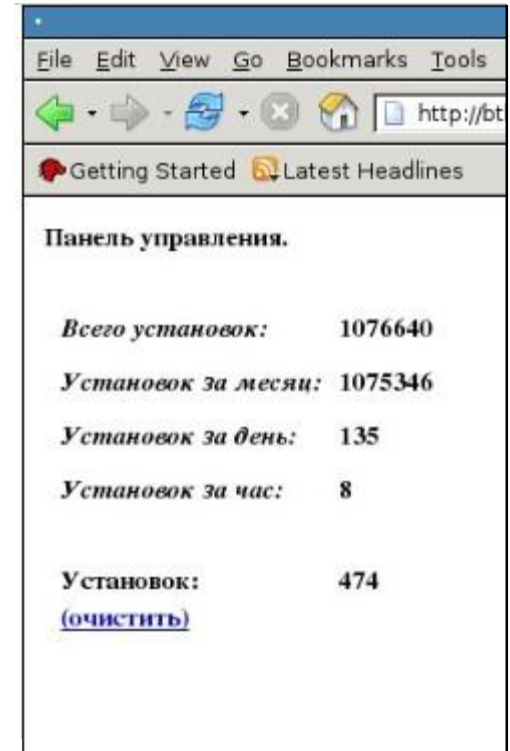
CHART OF THE WEEKLY ALL SITES MARKET SHARE IN 'ALL CATEGORIES', BASED ON VISITS.
TIME PERIODS REPRESENTED WITH BROKEN LINES INDICATE INSUFFICIENT DATA.
GENERATED ON: 07/12/2006. COPYRIGHT 2006 (C) 'HITWISE PTY LTD'.

Website market share chart by Hitwise

The PopupSh ActiveX Control has operated for about one month.

Control panel.

<i>Total installations:</i>	1076640
<i>Installations per month:</i>	1075346
<i>Installations per day:</i>	135
<i>Installations per hour:</i>	8
Installations:	474



Screenshot on right by Michael La Pilla via Security Fix

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

```
MSFConsole
msf > info ie_xp_pfv_metafile

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

Provided By:
H D Moore <hdm [at] metasploit.com>
san <san [at] xfocus.org>
0600K078RUS[at]lunknown.ru

Available Targets:
Automatic - Windows XP / Windows 2003 / Windows Vista

Available Options:

  Exploit:   Name      Default  Description
  -----
optional    REALHOST
optional    HTTPHOST    0.0.0.0  The local HTTP listener host
required    HTTPPORT    8080    The local HTTP listener port

Payload Information:
Space: 1504
Avoid: 1 characters
! Keys: noconn tunnel reverse

Nop Information:
SaveRegs: esp ebp
! Keys:
```

WebAttacker automates the creation of malicious websites.

Web-Attacker (IE0604) config editor

Enter here an URL path for CGI-script on your server

Enter here the folder name for placing an output exploit components

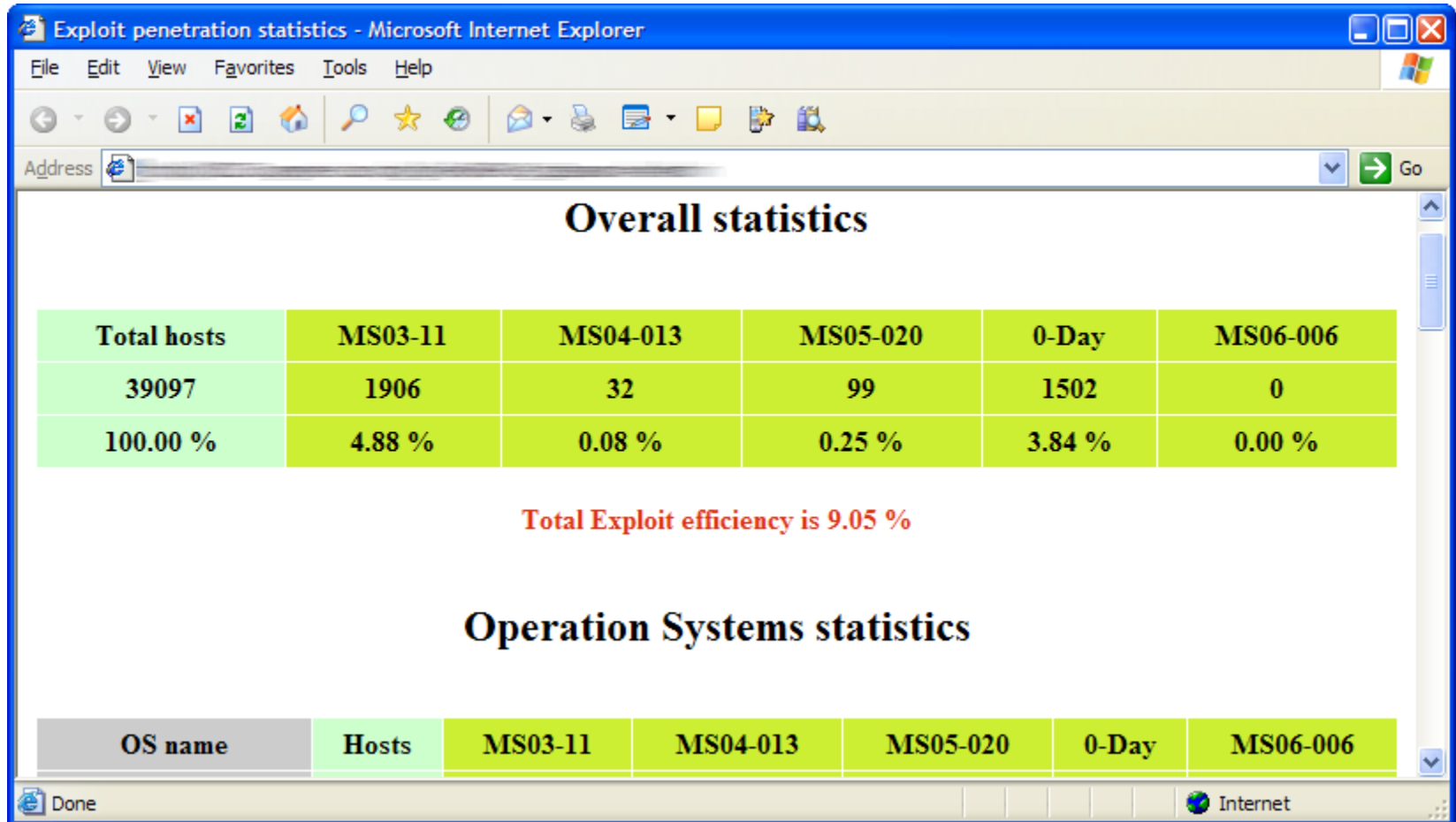
Web-Panel password :

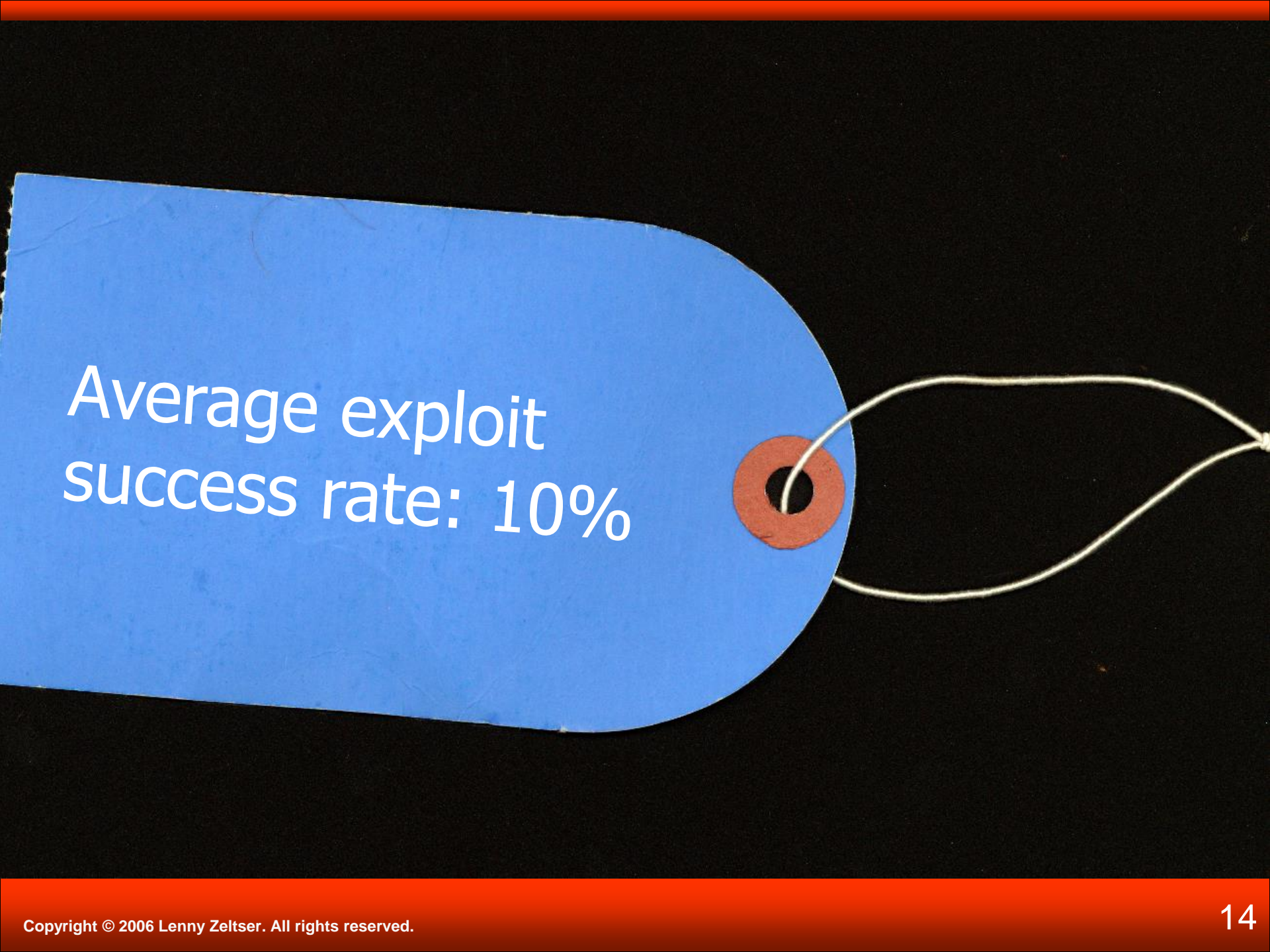
☐ Encrypt HTML files

Эксплойт - Web-Attacker IE0604 не обнаруживается следующими антивирусами:

Названия Антивируса	[Версия]	[Дата баз]
Doctor Web	4.33	-
NOD32 Antivirus	2.5	-
McAfee VirusScan	10.0.27	-
Norton Antivirus	2006	13.04.2006
Kaspersky Antivirus	5.0.391	14.04.2006
Panda Titanium Antivirus	2005	11.04.2006

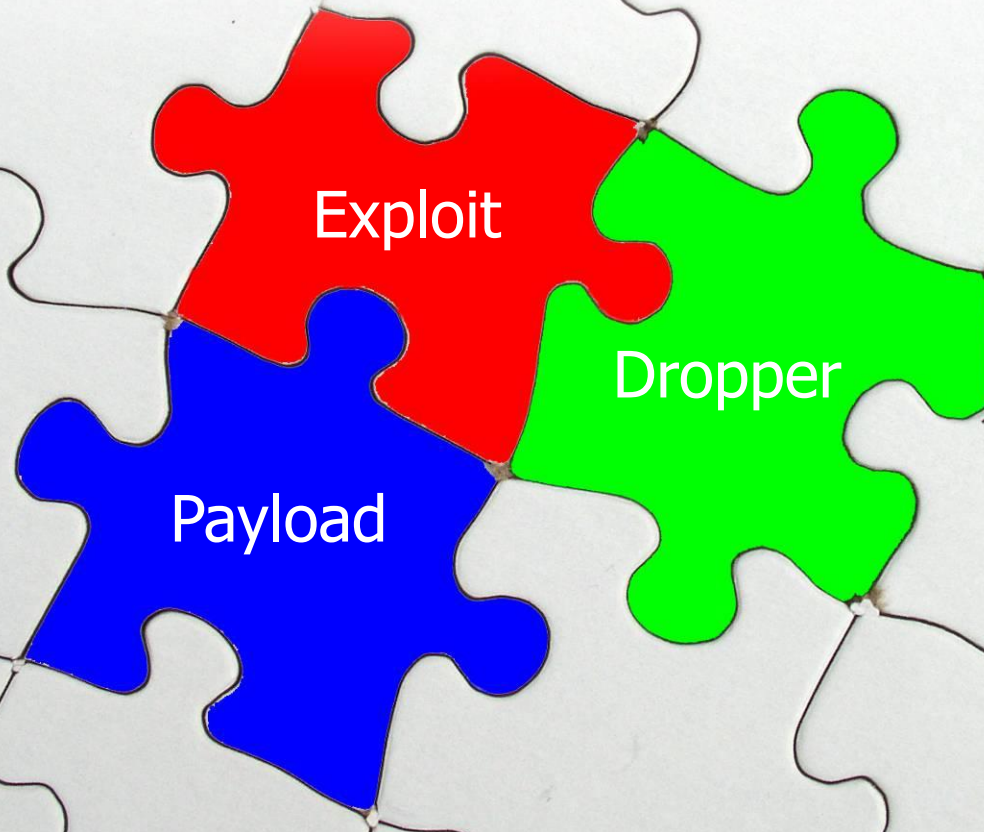
A control panel lets the operator monitor campaign effectiveness.



A blue, rectangular tag with rounded corners and a red circular hole on the right side. A white string is threaded through the hole and forms a loop. The tag is set against a black background.

Average exploit
success rate: 10%

The malicious site attack often includes three components.



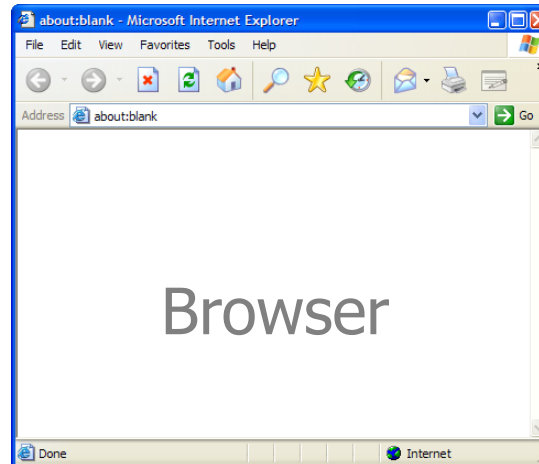
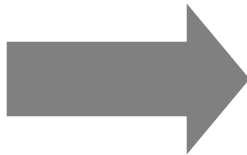
#2: Malware on the PC compromising website interactions via the browser



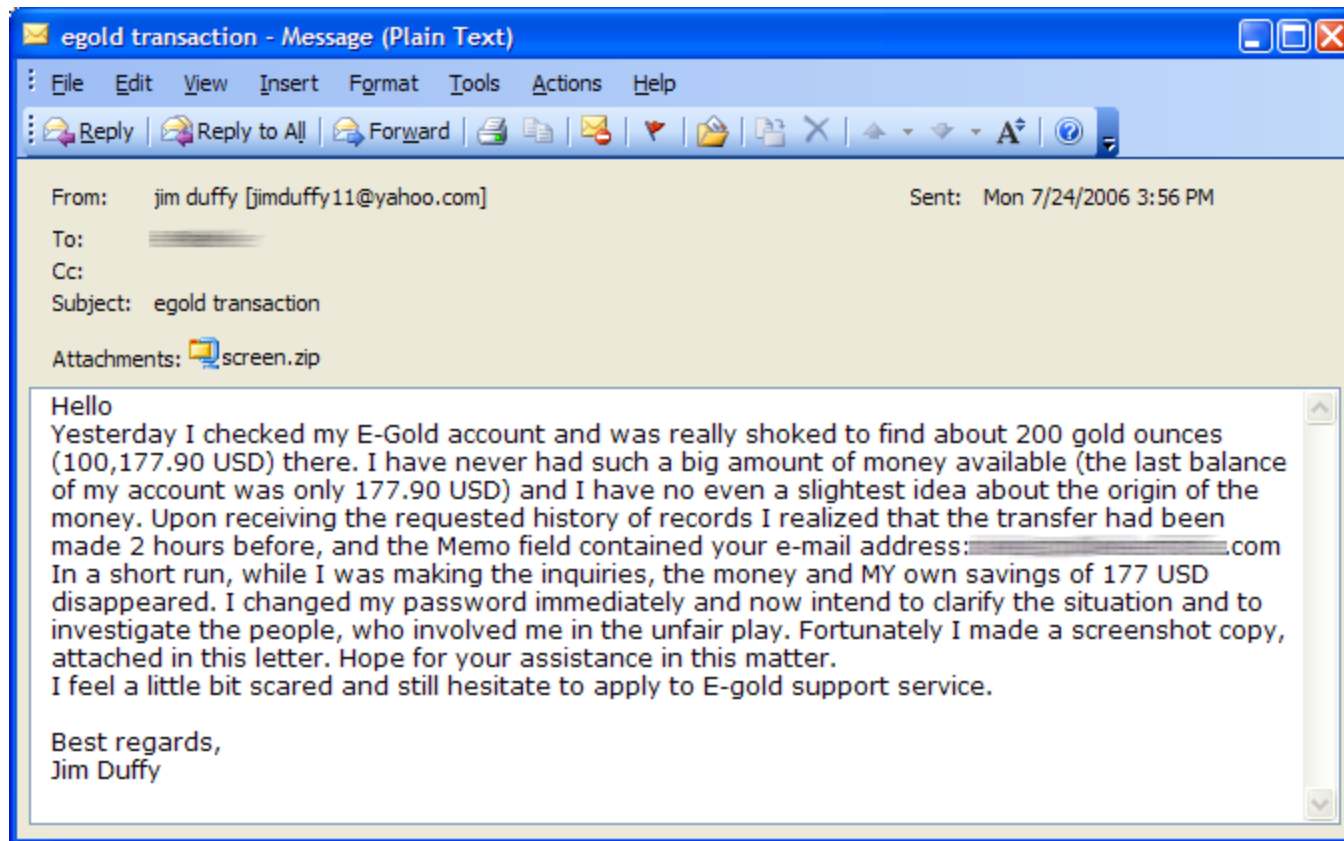
Personal Computer



Website



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



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>

URL details courtesy of Trend Micro

Another spyware spread via spoofed email targeted banking credentials.

From: "Spysoftcentral Team" <sales@spysoftcentral.com>
Subject: Order Approval Notification

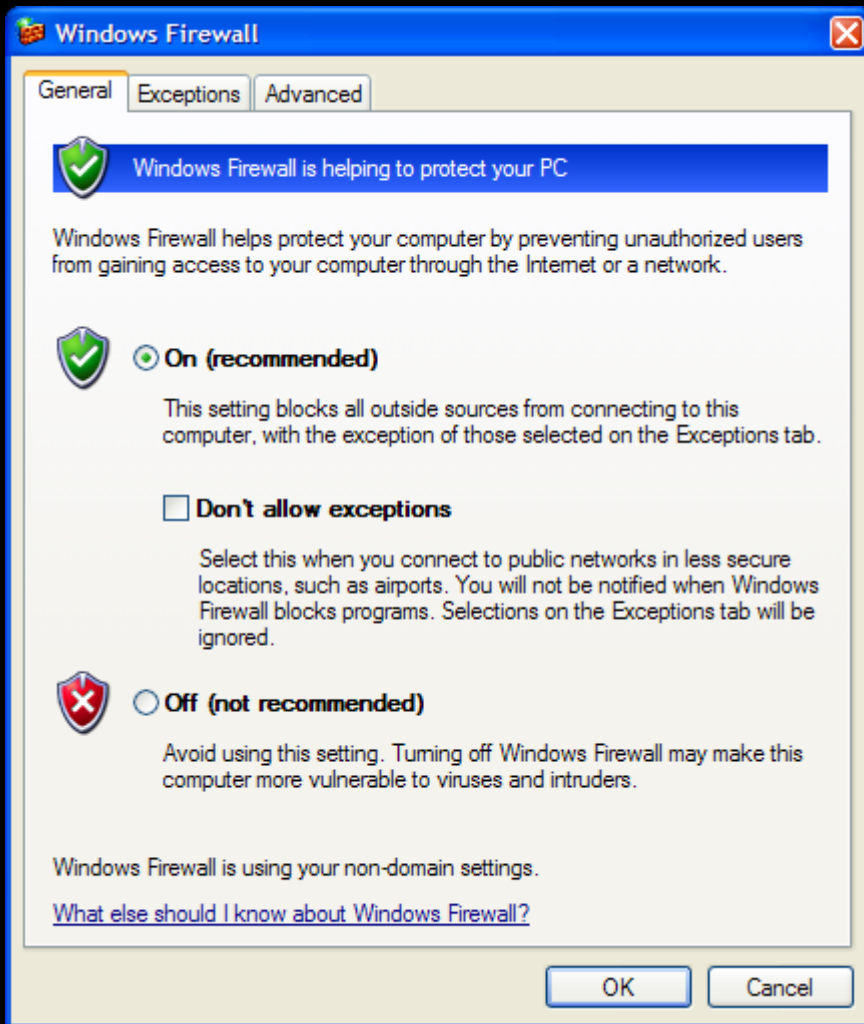
SPY DOCTOR / Order : DD269901/

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,

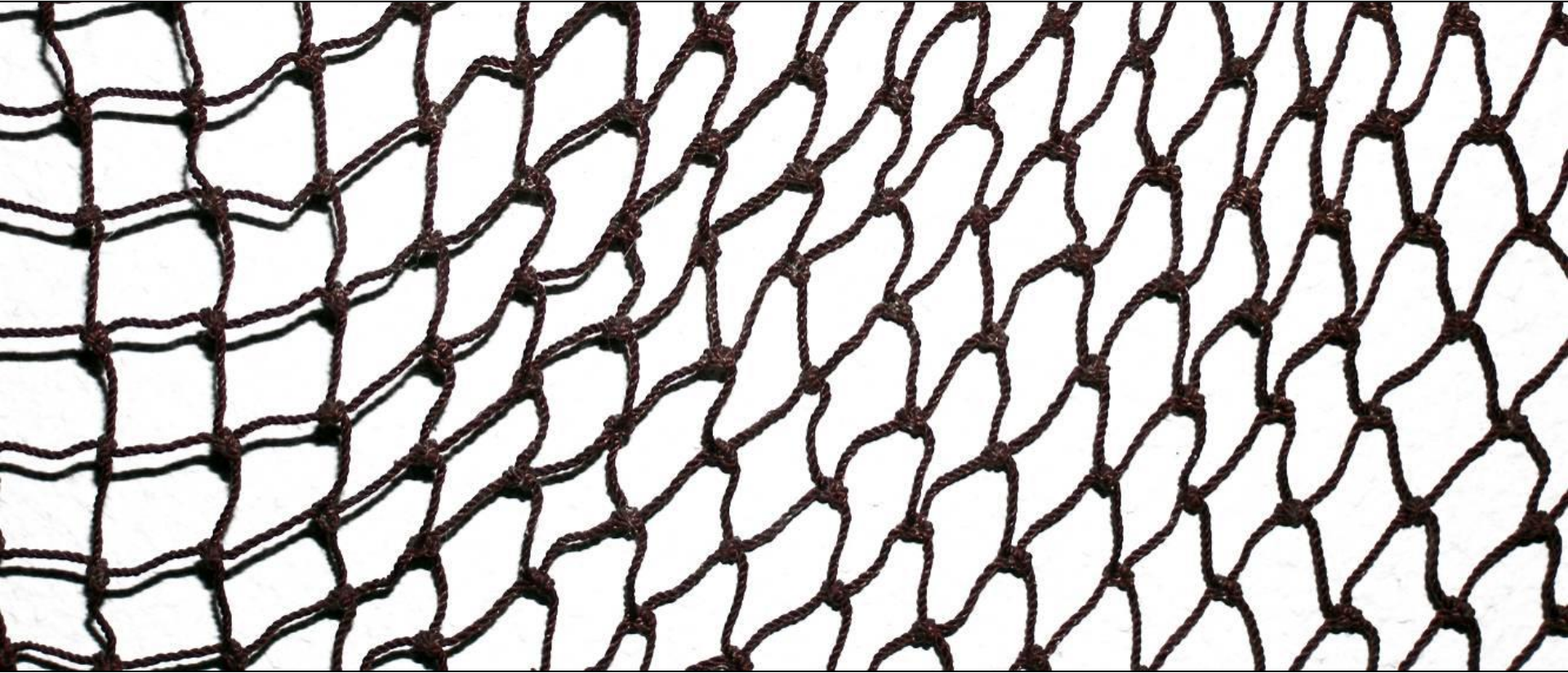
Thank you for your order. Spysoftcentral processes
orders and collects payments on behalf of PC Tools.

...



The dropper
tweaked Windows
firewall settings
before downloading
the spyware.

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



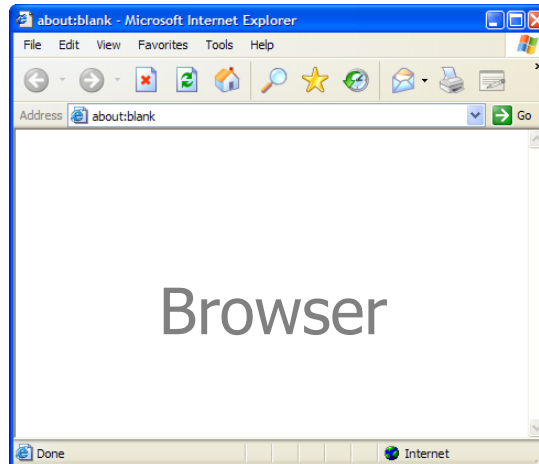
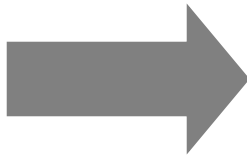


Text file “devenv.dll”
contained a log of the
day’s activity.

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



Website



Browser



Website



Books NEW!	Chat Rooms	Games	Music Videos
Blogs	Comedy NEW!	Horoscopes	MySpaceIM NEW!
Careers	Filmmakers	Movies NEW!	Schools



MySpace Music

[more music]

**TEXT CRAZY
TO 20FOX**
-for a free mobile ringtone-

CLICK TO LISTEN**Member Login**E-Mail: Password: ☐ Remember Me

LOGIN

SIGN UP!

[Forgot your password?](#)

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.

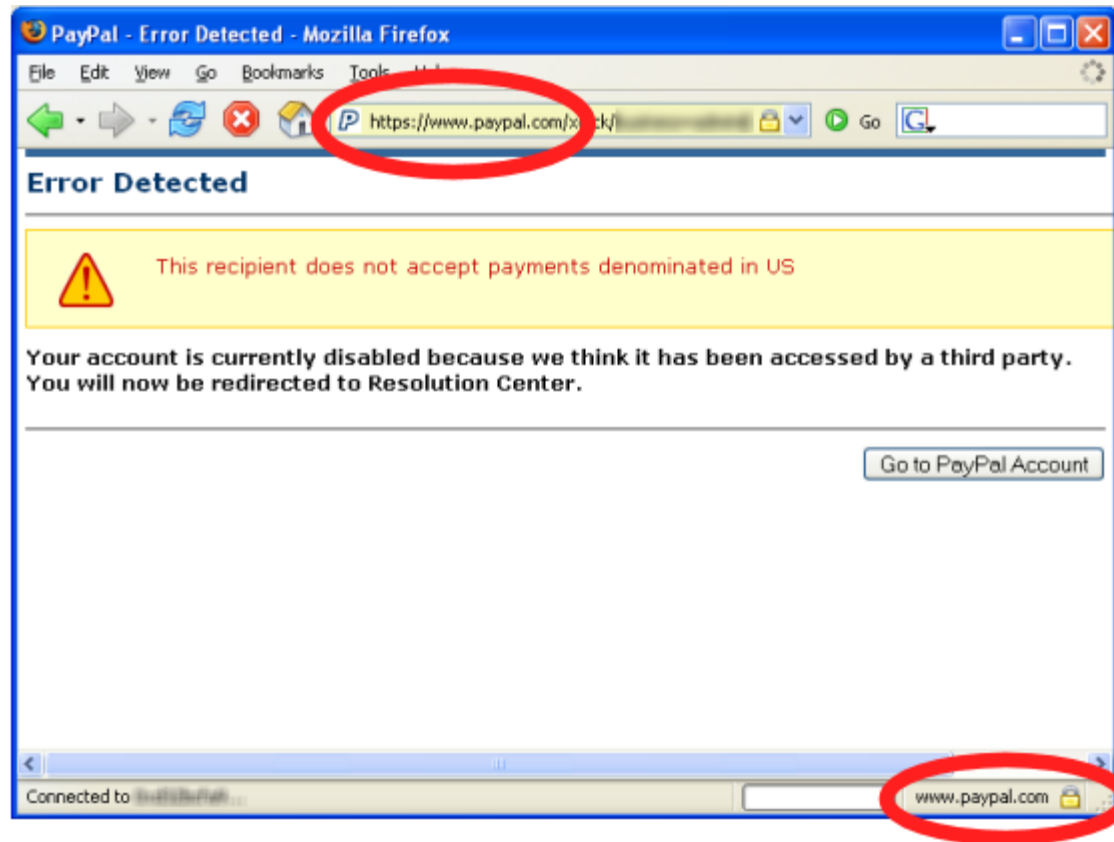


```
allowNetworking="internal"
```

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



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



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"



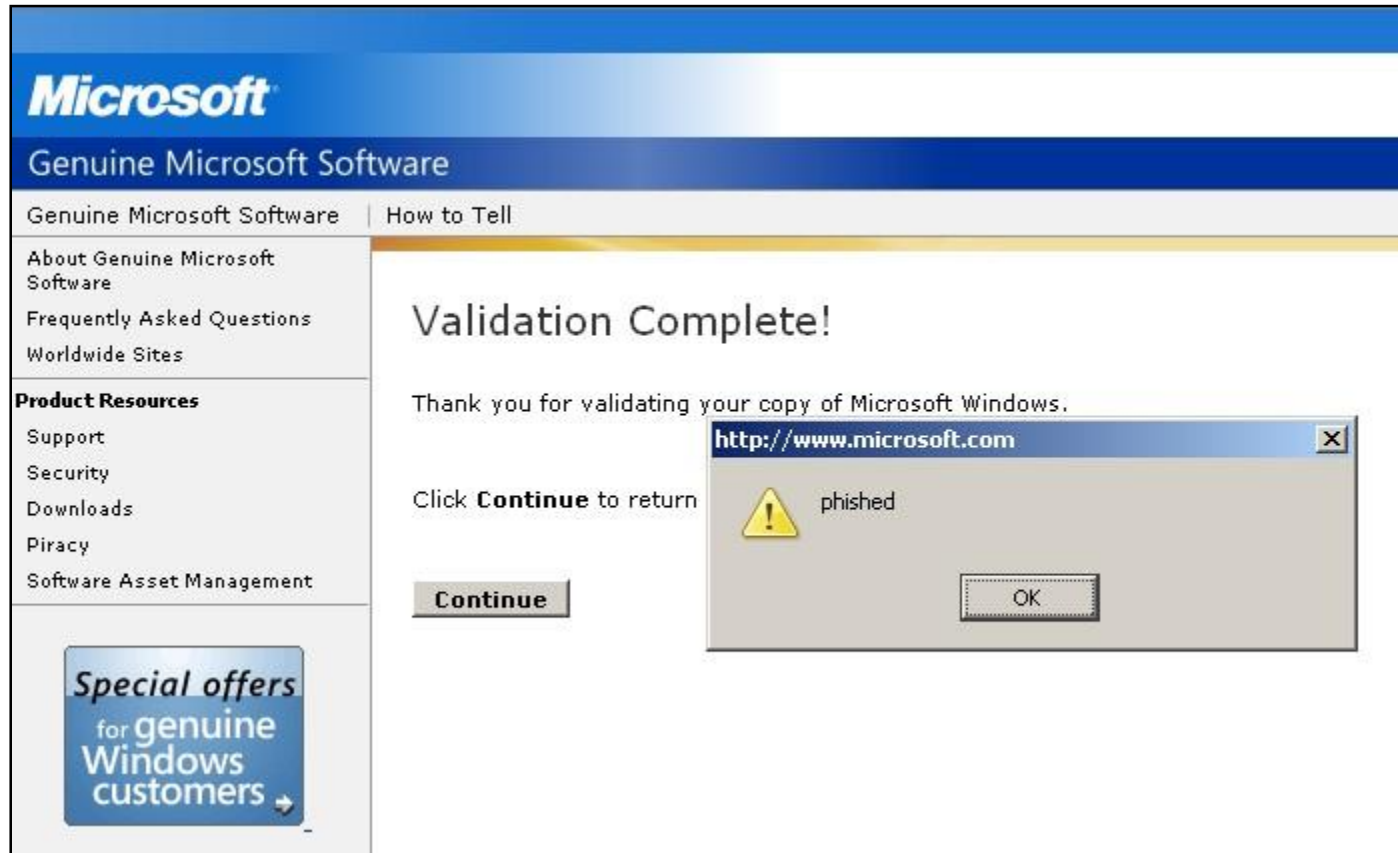
Many other websites have similar
XSS vulnerabilities.

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



Screenshot by Lance James via Security Fix

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



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