Client Side Attacks Come of Age

Michael Sutton, Security Evangelist

Overview

Background

- Evolution of attack vectors

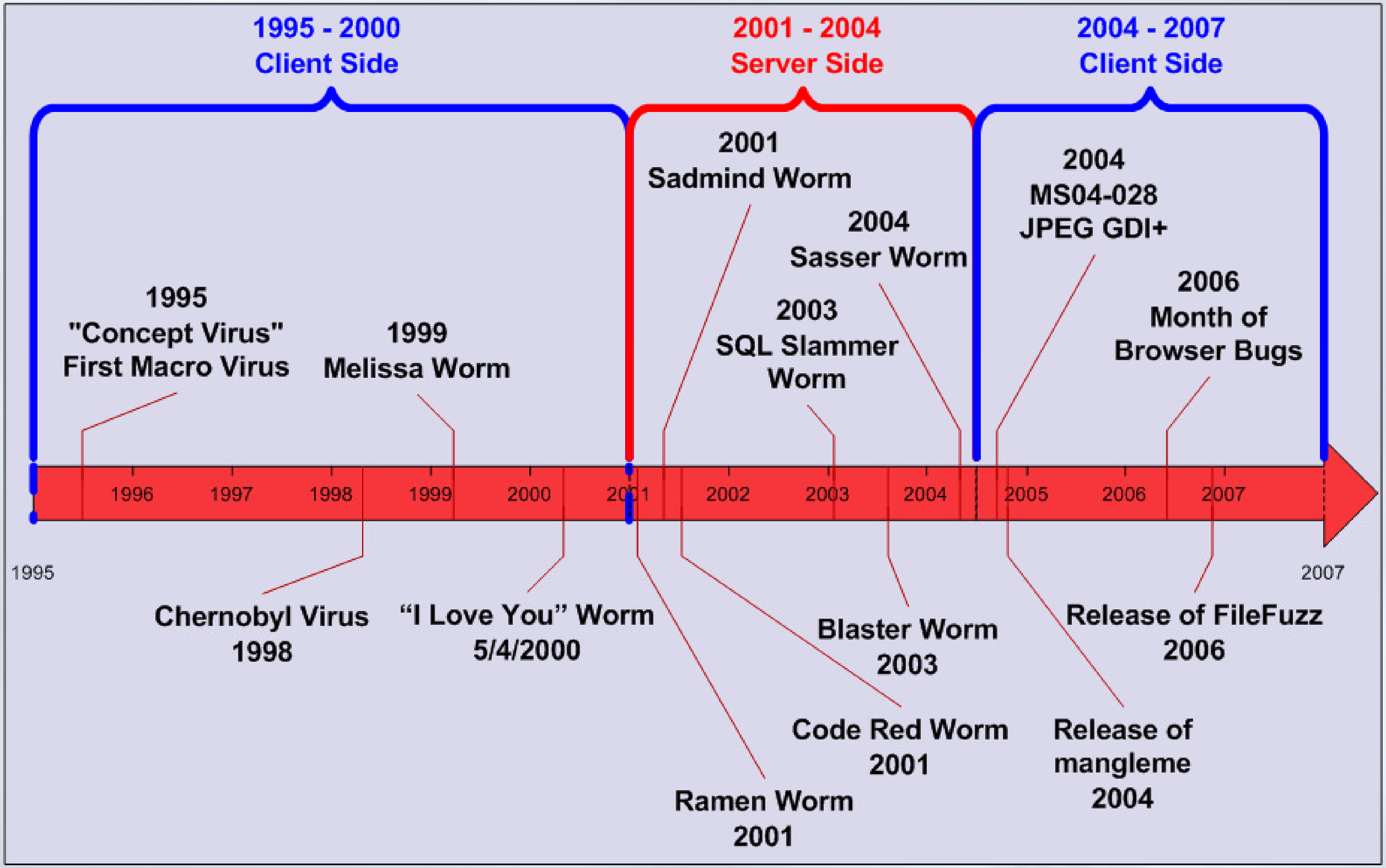
Client Side Vulnerabilities

- Web browser
- File format
- ActiveX Controls

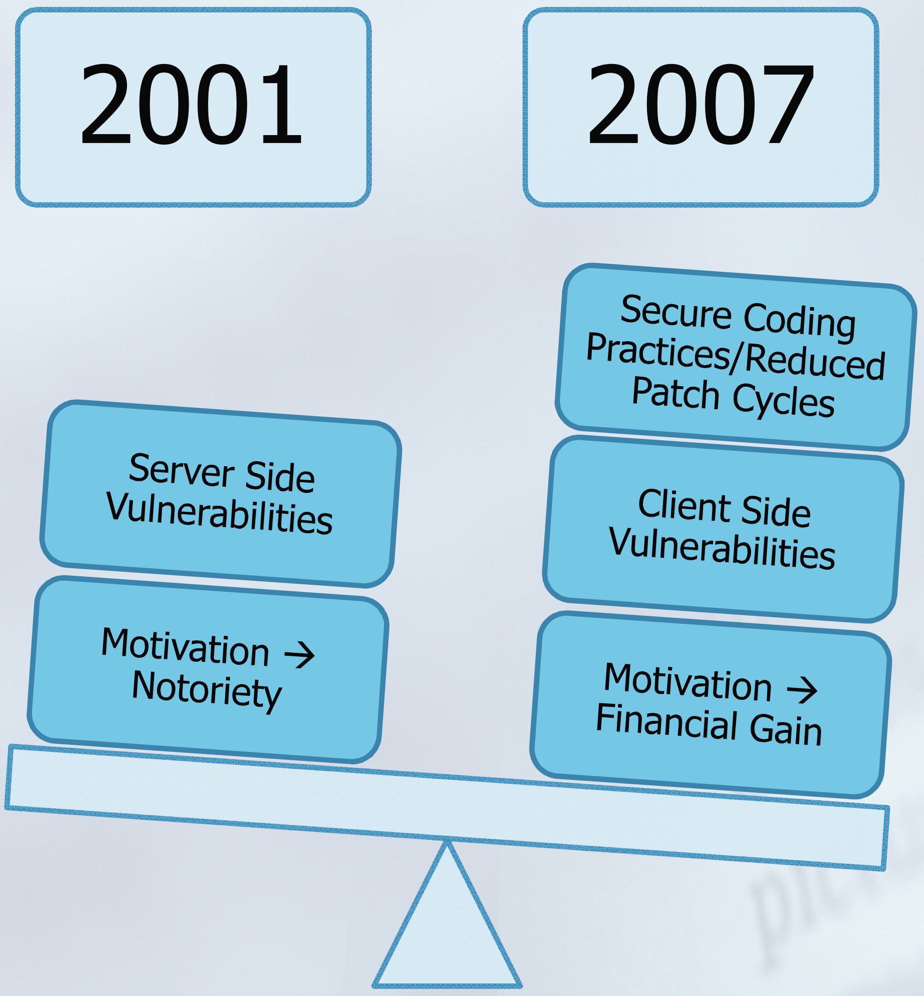
Predications

- Client side vulnerabilities going forward

Evolution of Attack Vectors



No More “Big Bang” Worms?



2001

2007

Server Side Vulnerabilities

Motivation → Notoriety

Secure Coding Practices/Reduced Patch Cycles

Client Side Vulnerabilities

Motivation → Financial Gain

Vuln Discovery Methodologies

White Box

- Internal perspective
- Static analysis
- Manual or automated testing
  - Insecure programming practices
  - Improper input validation

Black Box

- External perspective
- Run-time analysis
- Manual or automated testing
  - Known vulnerabilities
  - Unknown vulnerabilities

Client Side Vulnerabilities

Web Browser Vulnerabilities

- Numerous known vulnerabilities in all popular web browsers

File Format Vulnerabilities

- Malformed files trigger vulnerabilities in interpreting applications

ActiveX Vulnerabilities

- Buffer overflows and other vulnerabilities expose Microsoft applications, especially Internet Explorer

Web Browser Vulnerabilities

Denial of service

- Minimal severity

Code execution

- Buffer overflows
- ActiveX controls

Spoofing

- Address bar
- Status bar

Zone Bypass

- Internet zone content interpreted as local zone

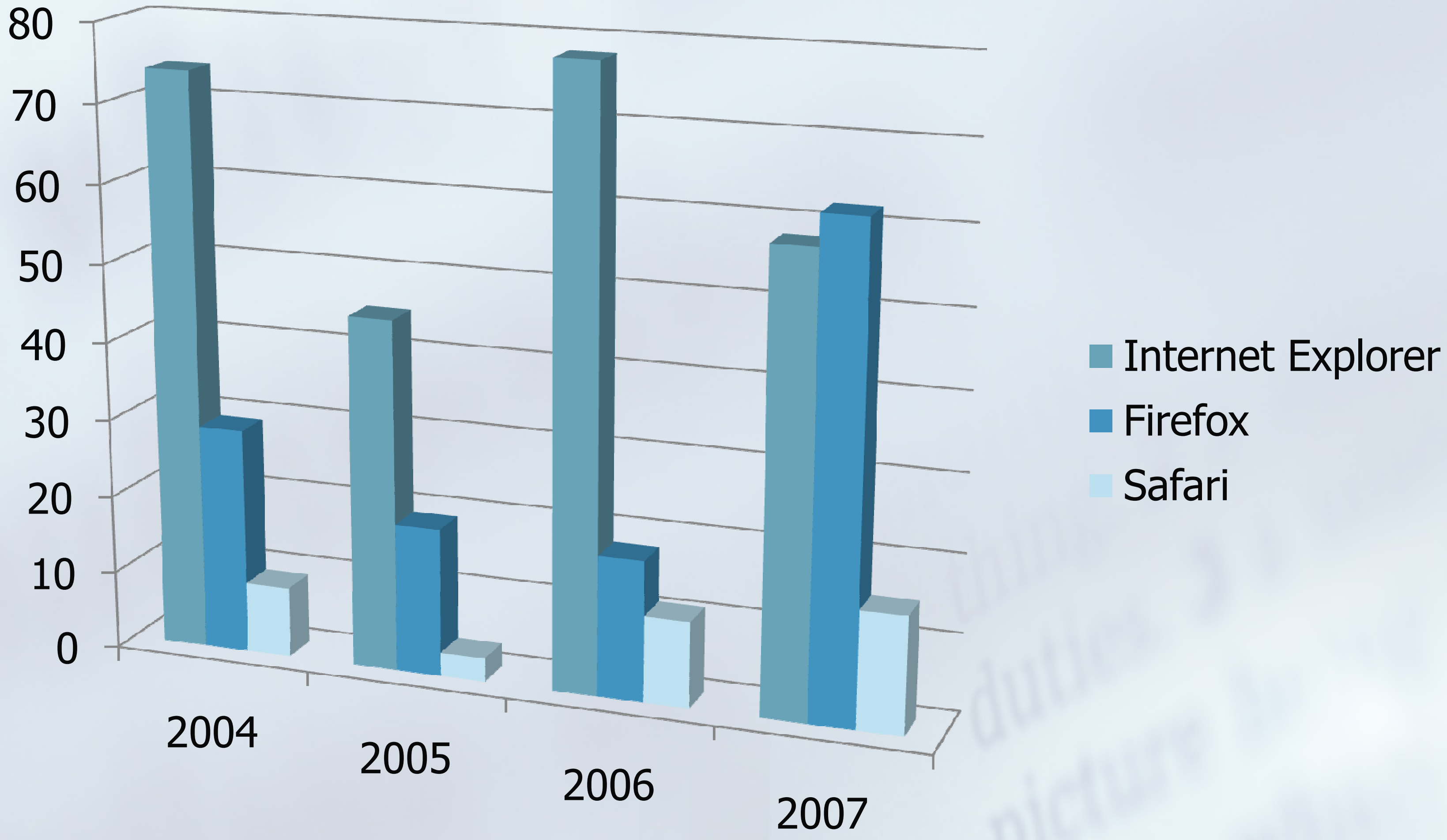
Cross Domain Restriction Bypass

- Accessing data from alternate sites

Information leakage

- File system access

Web Browser Statistics



Month of Browser Bugs

HD Moore

- Respected security researcher
- Co-founder of Metasploit project

31 vulnerabilities

- One per day throughout July 2006
- Full disclosure

All major browsers

- Internet explorer
- Mozilla
- Safari
- Opera
- Konqurer

Web Browser Fuzzers

mangleme

- HTML fuzzer
- lcamtuf

CSSDIE

- Cascading Style Sheet fuzzer
- H D Moore, Matt Murphy, Aviv Raff, and Thierry Zoller

Hamachi

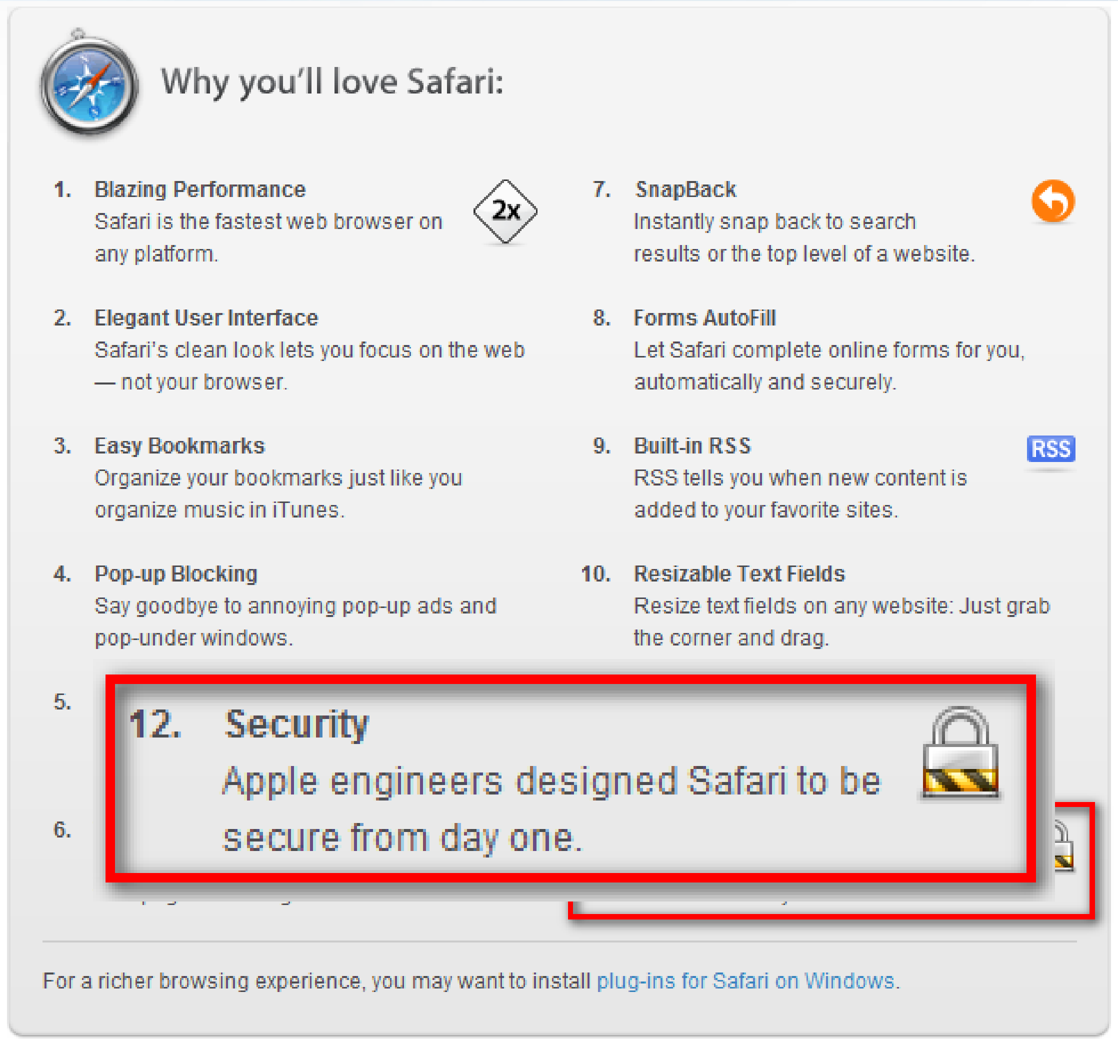
- DHTML fuzzer
- H D Moore and Aviv Raff

DOM-Hanoi

- Document Object Model fuzzer
- H D Moore and Aviv Raff

Safari for Windows

Case Study



Why you'll love Safari:

1. **Blazing Performance**
   Safari is the fastest web browser on any platform.
2. **Elegant User Interface**
   Safari's clean look lets you focus on the web — not your browser.
3. **Easy Bookmarks**
   Organize your bookmarks just like you organize music in iTunes.
4. **Pop-up Blocking**
   Say goodbye to annoying pop-up ads and pop-under windows.
5.
6.

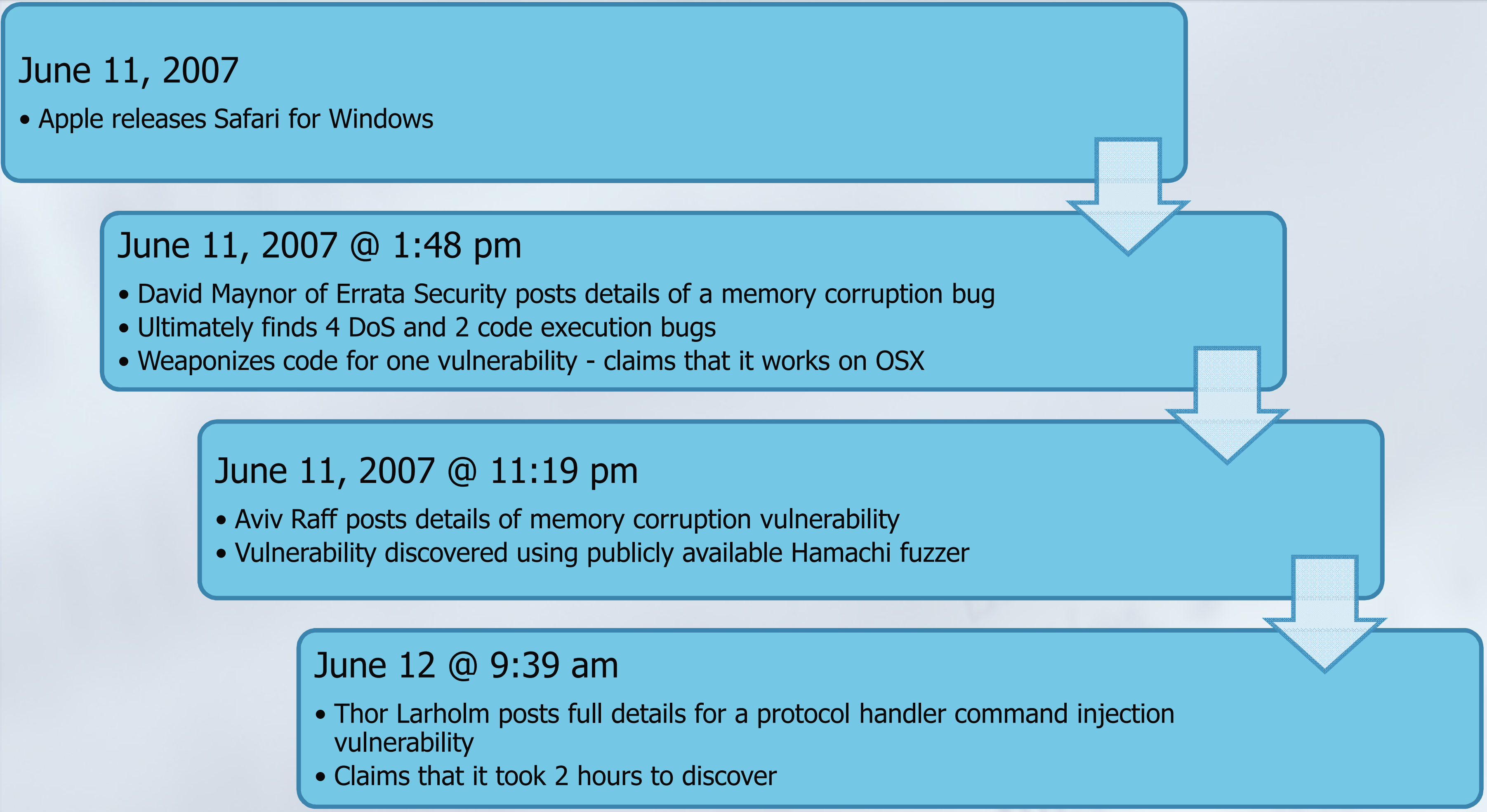
7. **SnapBack**
   Instantly snap back to search results or the top level of a website.
8. **Forms AutoFill**
   Let Safari complete online forms for you, automatically and securely.
9. **Built-in RSS**
   RSS tells you when new content is added to your favorite sites.
10. **Resizable Text Fields**
    Resize text fields on any website: Just grab the corner and drag.

12. **Security**
    Apple engineers designed Safari to be secure from day one.

For a richer browsing experience, you may want to install plug-ins for Safari on Windows.

Safari for Windows

Case Study



June 11, 2007

- Apple releases Safari for Windows

June 11, 2007 @ 1:48 pm

- David Maynor of Errata Security posts details of a memory corruption bug
- Ultimately finds 4 DoS and 2 code execution bugs
- Weaponizes code for one vulnerability - claims that it works on OSX

June 11, 2007 @ 11:19 pm

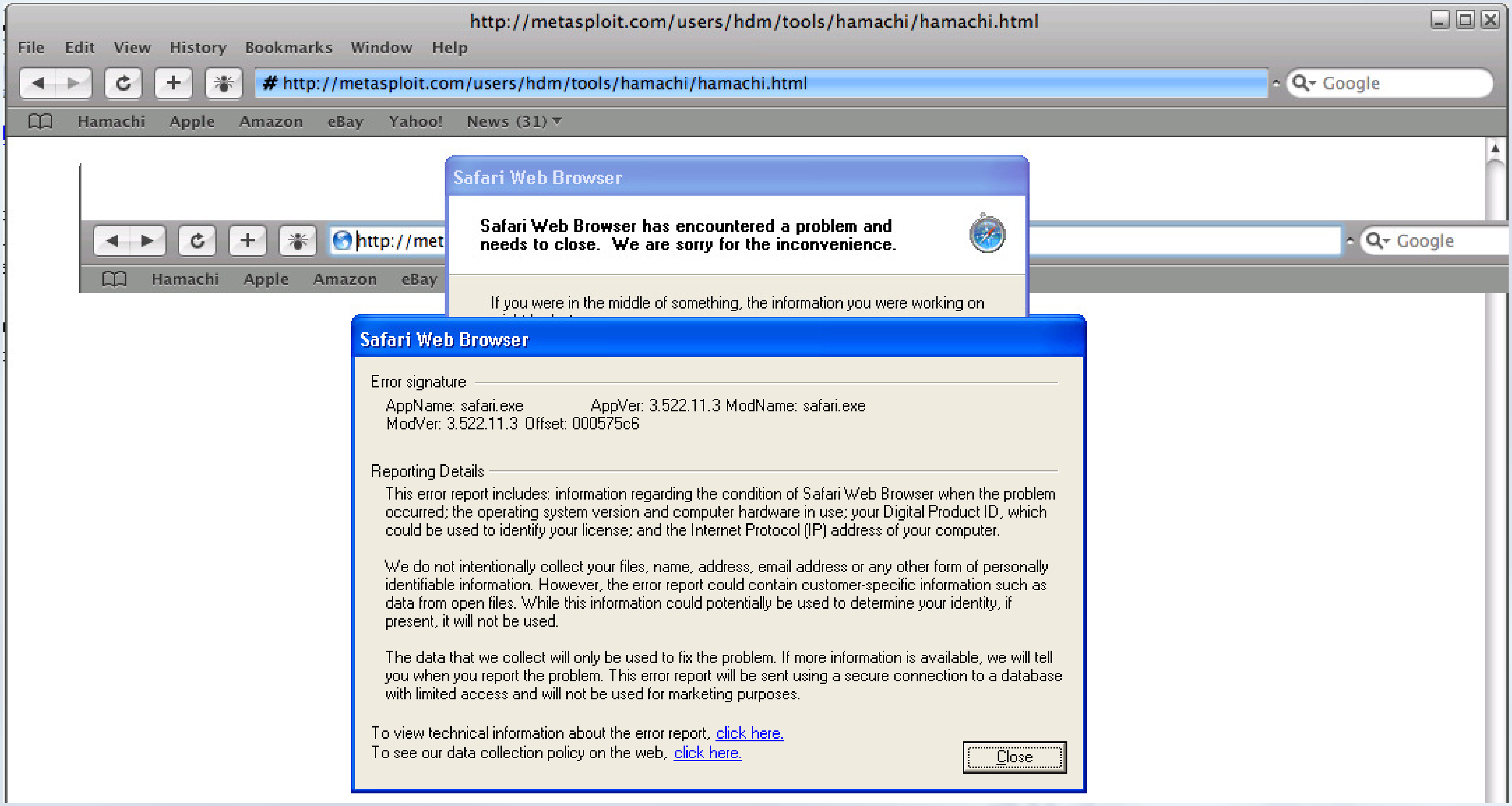
- Aviv Raff posts details of memory corruption vulnerability
- Vulnerability discovered using publicly available Hamachi fuzzer

June 12 @ 9:39 am

- Thor Larholm posts full details for a protocol handler command injection vulnerability
- Claims that it took 2 hours to discover

Safari for Windows

Case Study


http://metasploit.com/users/hdm/tools/hamachi/hamachi.html
File Edit View History Bookmarks Window Help
# http://metasploit.com/users/hdm/tools/hamachi/hamachi.html
Google
Hamachi Apple Amazon eBay Yahoo! News (31)
http://met
Google
Hamachi Apple Amazon eBay
Safari Web Browser
Safari Web Browser
Close

Safari Web Browser has encountered a problem and needs to close. We are sorry for the inconvenience.

If you were in the middle of something, the information you were working on

Error signature

AppName: safari.exe AppVer: 3.522.11.3 ModName: safari.exe
ModVer: 3.522.11.3 Offset: 000575c6

Reporting Details

This error report includes: information regarding the condition of Safari Web Browser when the problem occurred; the operating system version and computer hardware in use; your Digital Product ID, which could be used to identify your license; and the Internet Protocol (IP) address of your computer.

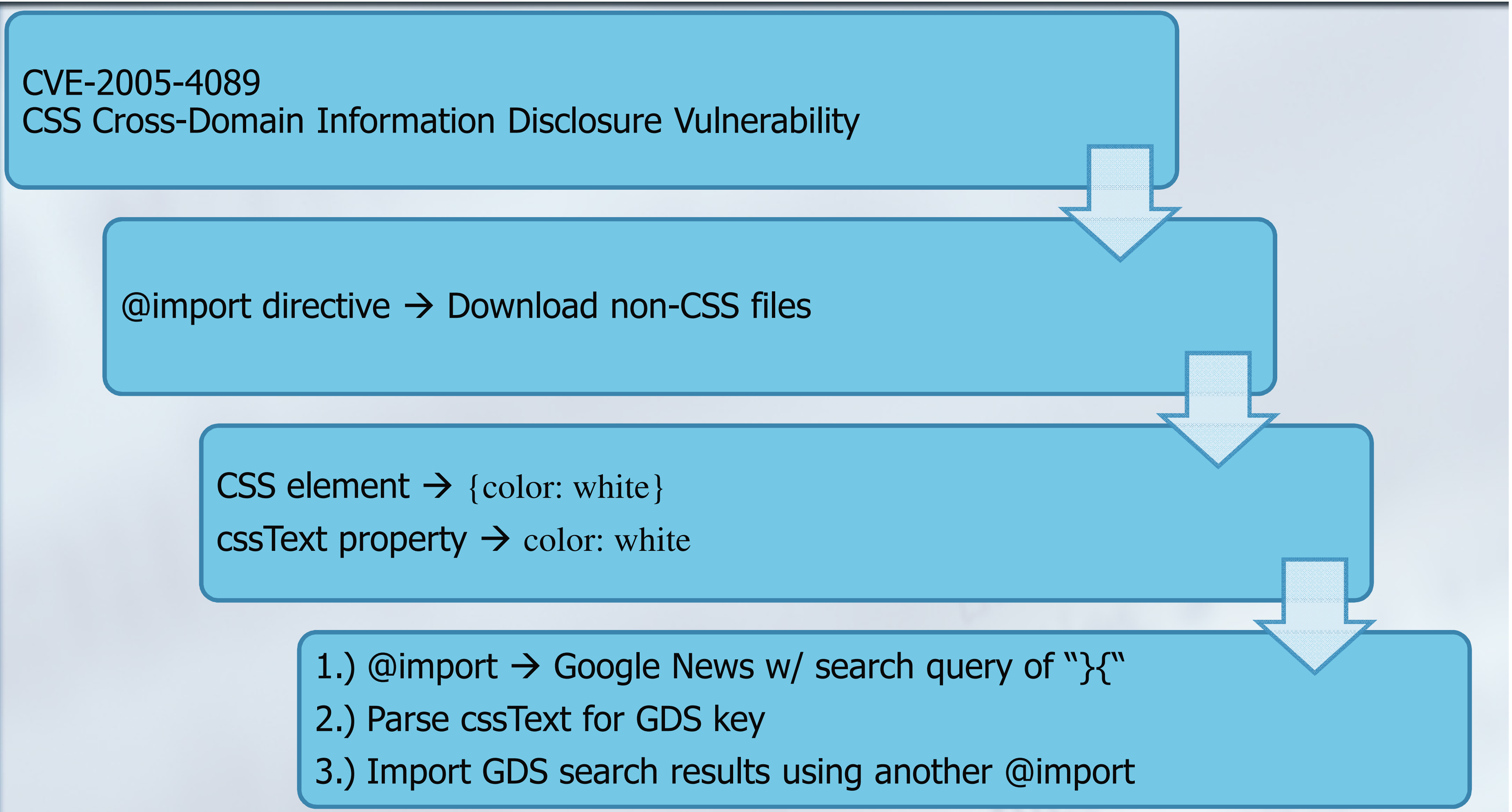
We do not intentionally collect your files, name, address, email address or any other form of personally identifiable information. However, the error report could contain customer-specific information such as data from open files. While this information could potentially be used to determine your identity, if present, it will not be used.

The data that we collect will only be used to fix the problem. If more information is available, we will tell you when you report the problem. This error report will be sent using a secure connection to a database with limited access and will not be used for marketing purposes.

To view technical information about the error report, click here.
To see our data collection policy on the web, click here.

GDS Cross Domain Bypass

Case Study



CVE-2005-4089
CSS Cross-Domain Information Disclosure Vulnerability

@import directive → Download non-CSS files

CSS element → {color: white}
cssText property → color: white

1.) @import → Google News w/ search query of “}{“
2.) Parse cssText for GDS key
3.) Import GDS search results using another @import

Courtesy of Matan Gillon from hacker.co.il

ActiveX

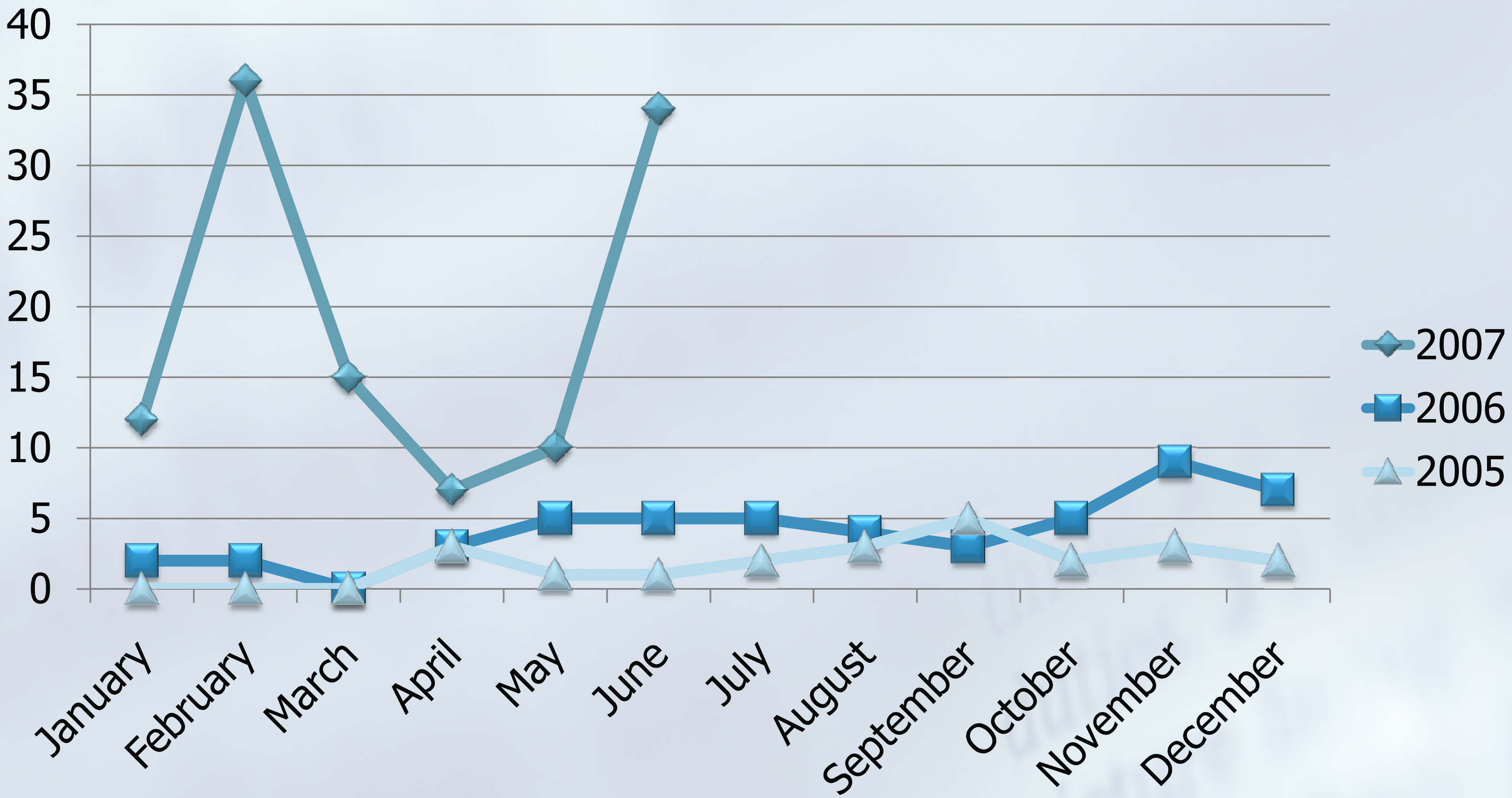
Technology

- Proprietary Microsoft technology built upon Microsoft's Component Object Model (COM)
- Framework for building reusable software components
- Often used by web developers to extend functionality

Vulnerabilities

- Susceptible to same vulnerability classifications as other desktop applications
- High Risk - Web accessible ActiveX controls with vulnerabilities
- Average desktop has hundreds of third party ActiveX controls

ActiveX Vulnerabilities

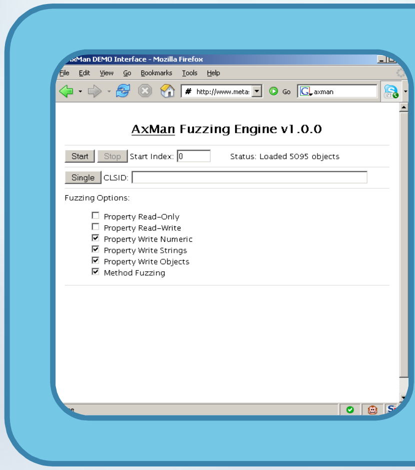


Courtesy of Secunia.com

ActiveX Fuzzers

AxMan

- Released August 2006
- Developed by HD Moore
- Used to find most MoBB ActiveX vulns



AxMan Fuzzing Engine v1.0.0

Start Index: 0 Status: Loaded 5095 objects

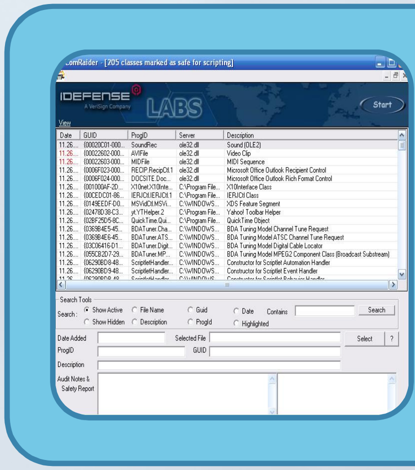
CLSID:

Fuzzing Options:

- ☐ Property Read-Only
- ☐ Property Read-Write
- ☑ Property Write Numeric
- ☑ Property Write Strings
- ☑ Property Write Objects
- ☑ Method Fuzzing

COMRaider

- Released August 2006
- Developed by David Zimmer



omRaider - [205 classes marked as safe for scripting]

Date	GUID	ProgID	Server	Description
11.26....	{00020C01-000...	SoundRec	ole32.dll	Sound (OLE2)
11.26....	{00022602-000...	AVIFile	ole32.dll	Video Clip
11.26....	{00022603-000...	MIDFile	ole32.dll	MIDI Sequence
11.26....	{0006F023-000...	RECIP.RecipCtl.1	ole32.dll	Microsoft Office Outlook Recipient Control
11.26....	{0006F024-000...	DOCSITE.Doc...	ole32.dll	Microsoft Office Outlook Rich Format Control
11.26....	{001000AF-2D...	X10net.X10Inte...	C:\Program File...	X10Interface Class
11.26....	{00CEDC01-86...	IERJCtl.IERJCtl.1	C:\Program File...	IERJCtl Class
11.26....	{0149EEDF-D0...	MSVidCtl.MSVi...	C:\WINDOWS...	XDS Feature Segment
11.26....	{02478D38-C3...	yt.YTHelper.2	C:\Program File...	Yahoo! Toolbar Helper
11.26....	{02BF25D5-8C...	QuickTime.Qui...	C:\Program File...	QuickTime Object
11.26....	{0369B4E5-45...	BDATuner.Cha...	C:\WINDOWS...	BDA Tuning Model Channel Tune Request
11.26....	{0369B4E6-45...	BDATuner.ATS...	C:\WINDOWS...	BDA Tuning Model ATSC Channel Tune Request
11.26....	{03C06416-D1...	BDATuner.Digit...	C:\WINDOWS...	BDA Tuning Model Digital Cable Locator
11.26....	{055CB2D7-29...	BDATuner.MP...	C:\WINDOWS...	BDA Tuning Model MPEG2 Component Class (Broadcast Substream)
11.26....	{06290BD8-48...	ScriptletHandler...	C:\WINDOWS...	Constructor for Scriptlet Automation Handler
11.26....	{06290BD9-48...	ScriptletHandler...	C:\WINDOWS...	Constructor for Scriptlet Event Handler
11.26....	{06290BDB-48...	ScriptletHandler...	C:\WINDOWS...	Constructor for Scriptlet Behavior Handler

Search Tools

Search : ● Show Active ○ File Name ○ Guid ○ Date Contains
○ Show Hidden ○ Description ○ ProgId ○ Highlighted

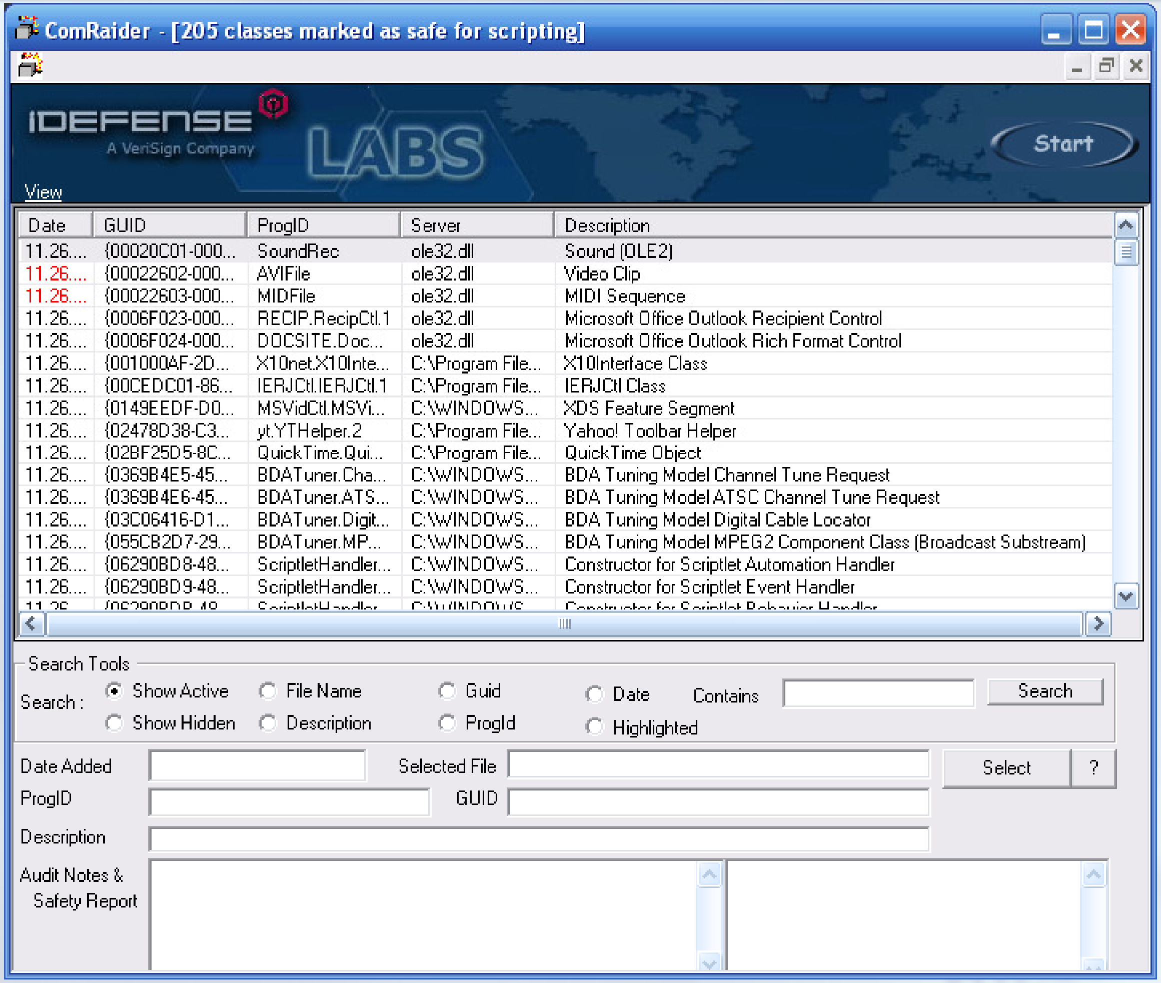
Date Added Selected File

ProgID GUID

Description

Audit Notes & Safety Report

COMRaider



ComRaider - [205 classes marked as safe for scripting]

Date	GUID	ProgID	Server	Description
11.26....	{00020C01-000...	SoundRec	ole32.dll	Sound (OLE2)
11.26....	{00022602-000...	AVIFile	ole32.dll	Video Clip
11.26....	{00022603-000...	MIDFile	ole32.dll	MIDI Sequence
11.26....	{0006F023-000...	RECIP.RecipCtl.1	ole32.dll	Microsoft Office Outlook Recipient Control
11.26....	{0006F024-000...	DOCSITE.Doc...	ole32.dll	Microsoft Office Outlook Rich Format Control
11.26....	{001000AF-2D...	X10net.X10Inte...	C:\Program File...	X10Interface Class
11.26....	{00CEDC01-86...	IERJCtl.IERJCtl.1	C:\Program File...	IERJCtl Class
11.26....	{0149EEDF-D0...	MSVidCtl.MSVi...	C:\WINDOWS...	XDS Feature Segment
11.26....	{02478D38-C3...	yt.YTHelper.2	C:\Program File...	Yahoo! Toolbar Helper
11.26....	{02BF25D5-8C...	QuickTime.Qui...	C:\Program File...	QuickTime Object
11.26....	{0369B4E5-45...	BDATuner.Cha...	C:\WINDOWS...	BDA Tuning Model Channel Tune Request
11.26....	{0369B4E6-45...	BDATuner.ATS...	C:\WINDOWS...	BDA Tuning Model ATSC Channel Tune Request
11.26....	{03C06416-D1...	BDATuner.Digit...	C:\WINDOWS...	BDA Tuning Model Digital Cable Locator
11.26....	{055CB2D7-29...	BDATuner.MP...	C:\WINDOWS...	BDA Tuning Model MPEG2 Component Class (Broadcast Substream)
11.26....	{06290BD8-48...	ScriptletHandler...	C:\WINDOWS...	Constructor for Scriptlet Automation Handler
11.26....	{06290BD9-48...	ScriptletHandler...	C:\WINDOWS...	Constructor for Scriptlet Event Handler
11.26	{06290BDB-48	ScriptletHandler	C:\WINDOWS	Constructor for Scriptlet Behavior Handler

Search Tools

Search : ● Show Active ○ Show Hidden ○ File Name ○ Description ○ Guid ○ ProgId ○ Date ○ Highlighted Contains

Date Added

Selected File

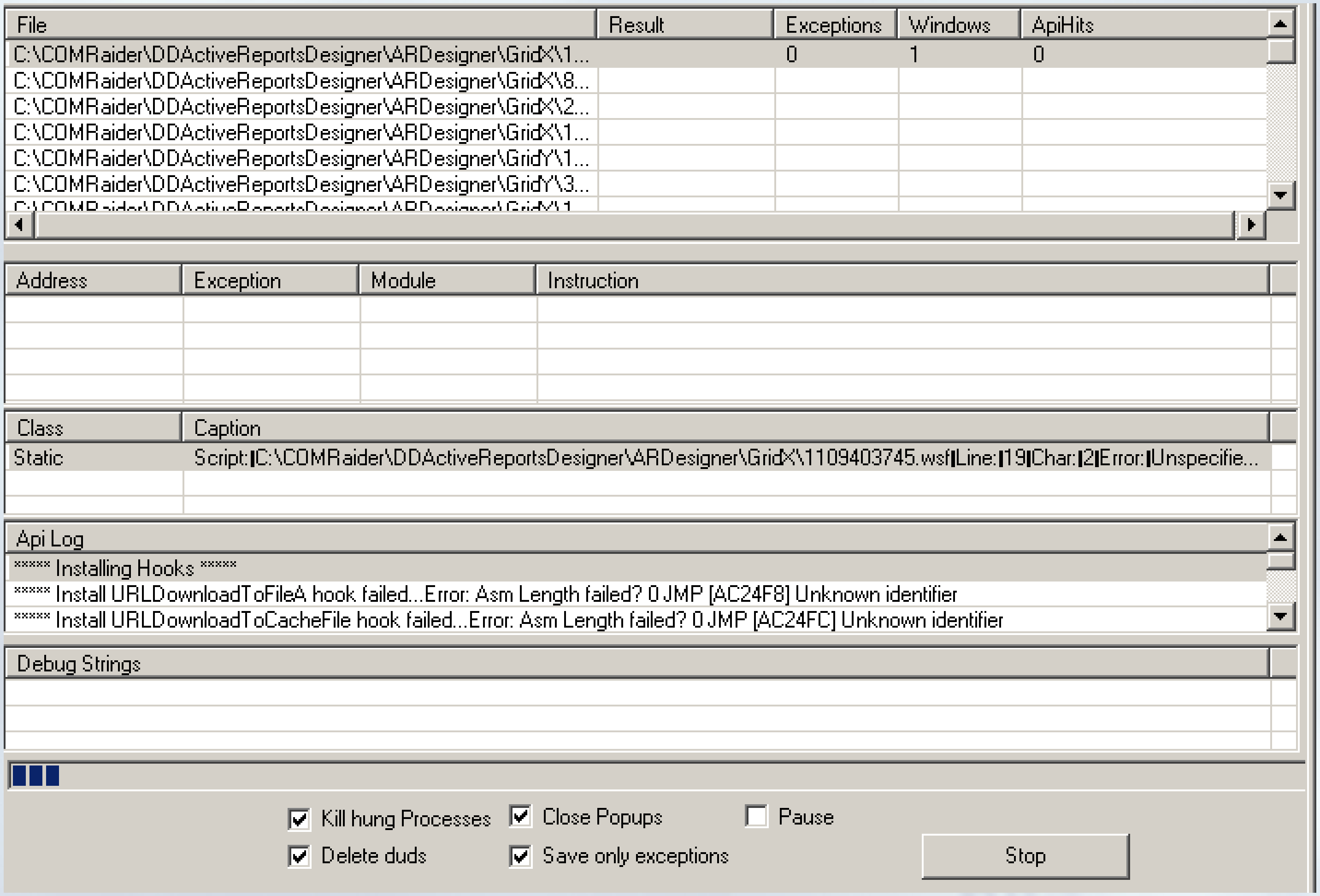
ProgID

GUID

Description

Audit Notes & Safety Report

COMRaider in Action



File	Result	Exceptions	Windows	ApiHits
C:\COMRaider\DDActiveReportsDesigner\ARDesigner\GridX\1...		0	1	0
C:\COMRaider\DDActiveReportsDesigner\ARDesigner\GridX\8...				
C:\COMRaider\DDActiveReportsDesigner\ARDesigner\GridX\2...				
C:\COMRaider\DDActiveReportsDesigner\ARDesigner\GridX\1...				
C:\COMRaider\DDActiveReportsDesigner\ARDesigner\GridY\1...				
C:\COMRaider\DDActiveReportsDesigner\ARDesigner\GridY\3...				
C:\COMRaider\DDActiveReportsDesigner\ARDesigner\GridY\1				

Address	Exception	Module	Instruction

Class	Caption
Static	Script:|C:\COMRaider\DDActiveReportsDesigner\ARDesigner\GridX\1109403745.wsf|Line:|19|Char:|2|Error:|Unspecifie...

Api Log

```
***** Installing Hooks *****
***** Install URLDownloadToFileA hook failed...Error: Asm Length failed? 0 JMP [AC24F8] Unknown identifier
***** Install URLDownloadToCacheFile hook failed...Error: Asm Length failed? 0 JMP [AC24FC] Unknown identifier
```

Debug Strings

☑ Kill hung Processes ☑ Close Popups □ Pause

☑ Delete duds ☑ Save only exceptions

Microsoft File Format Vulns

Microsoft Office Documents

- 2006 – 41 of 104 critical flaws were in Microsoft Office programs

Image Files

- WMF vulnerability (MS06-001)
  - Unintended functionality
  - Forced ‘out of cycle patch’ in January 2006
  - Reportedly sold in underground for $4,000
- JPG GDI+ vulnerability (MS04-028)
  - Integer overflow
  - Numerous PoC exploit codes quickly released

Media Files

- Windows Media Format ASF Parsing Vulnerability (CVE-2006-4702)
- Windows Media Format ASX Parsing Vulnerability (CVE-2006-6134)

File Format Vulnerabilities

Attack

- Malformed file triggers vulnerability in interpreting application
- Single vulnerability may affect multiple applications due to shared code/libraries

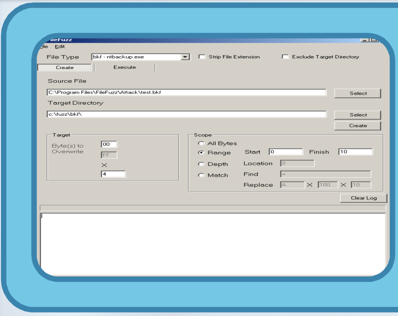
Attack

- Attack vector has exploded since 2004
- Commonly used in targeted attacks

Defense

- Zero day attacks virtually impossible to defend against

File Format Fuzzers



File Type: bkf - ntbackup.exe

□ Strip File Extension

□ Exclude Target Directory

Source File: C:\Program Files\FileFuzz\Attack\test.bkf

Target Directory: c:\fuzz\bkf\

Target

Byte(s) to Overwrite: 00 FF × 4

Scope

○ All Bytes

● Range Start 0 Finish 10

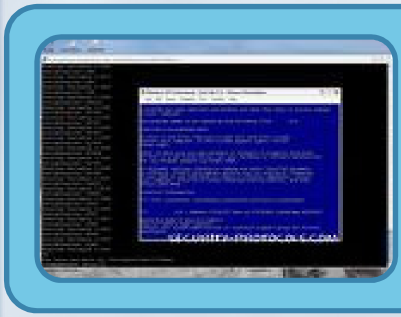
○ Depth Location 0

○ Match Find -

Replace A × 100 × 10

FileFuzz

- Michael Sutton
- Windows GUI
- Brute force fuzzer



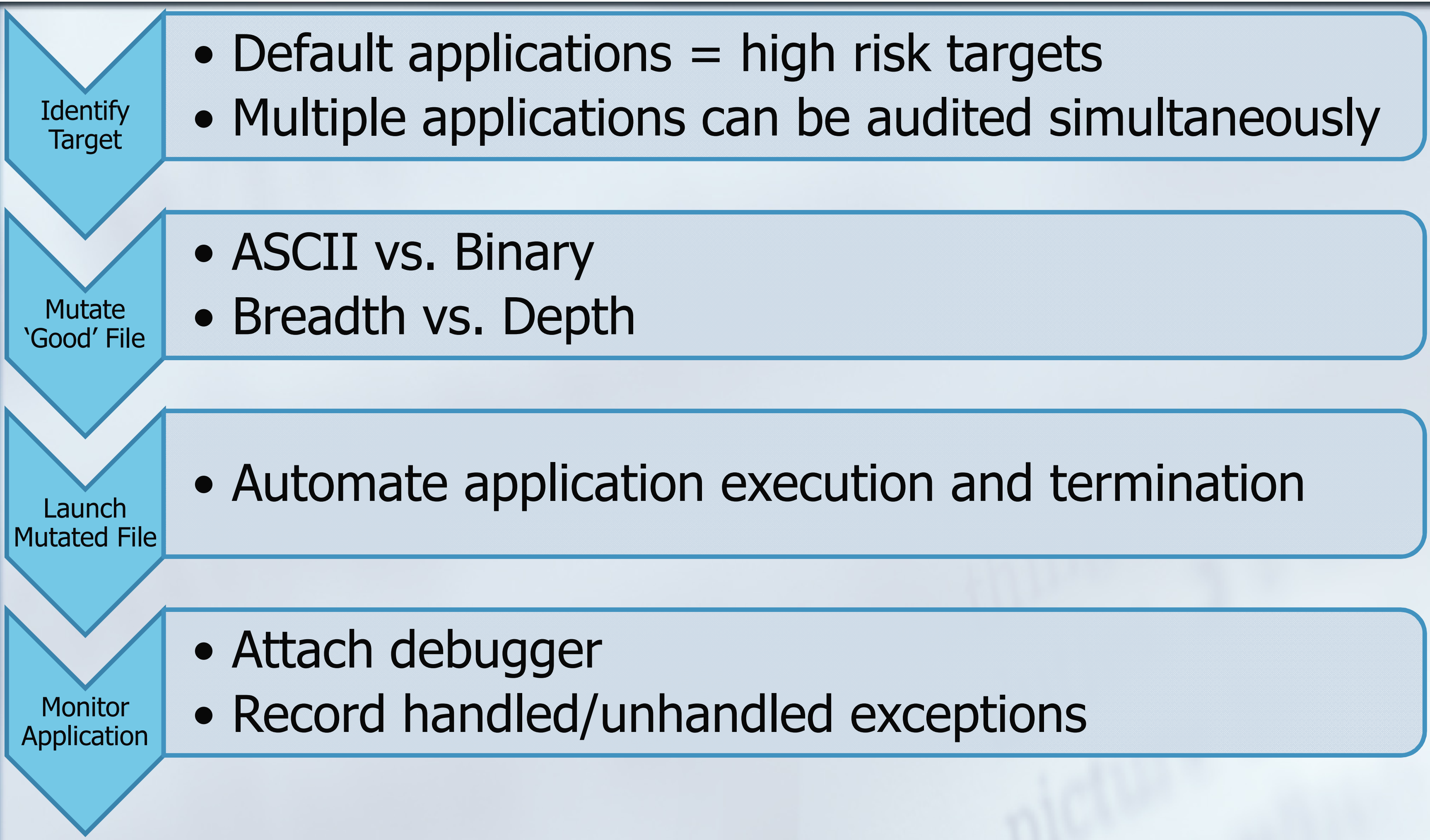
SPIKEfile

- Adam Greene
- Linux command line
- Based on SPIKE by Dave Aitel
- ‘Intelligent’ fuzzer

notSPIKEfile

- Adam Greene
- Linux command line
- Brute force fuzzer

FileFuzz Process



Identify Target

- Default applications = high risk targets
- Multiple applications can be audited simultaneously

Mutate 'Good' File

- ASCII vs. Binary
- Breadth vs. Depth

Launch Mutated File

- Automate application execution and termination

Monitor Application

- Attach debugger
- Record handled/unhandled exceptions

MS04-028 – JPEG GDI+

Case Study

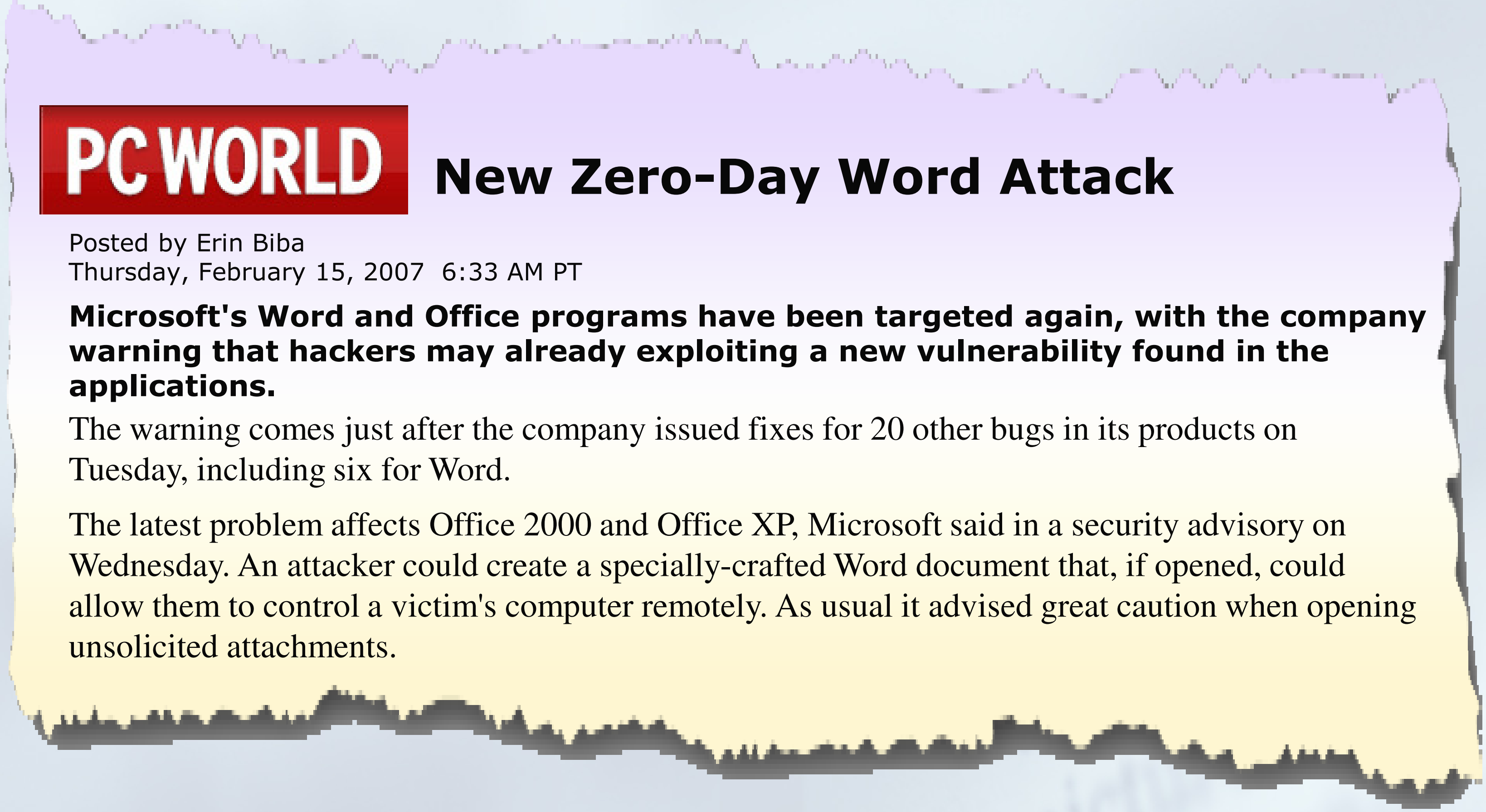
Vulnerability

- JPEG specification permits comments
- Comments prefaced by 0xFFFE and two byte size value
- Minimum valid size is 2 bytes as the comment size includes the two bytes used by the size value itself
- Size value of 0 or 1 leads to an integer overflow
- Affected numerous Windows applications leveraging GDI+ library (gdiplus.dll)

Fallout

- September 14, 2004 - MS04-028 published
- September 22, 2004 – PoC exploit published – adds user
- September 23, 2004 – “JPEG Downloader Toolkit” exploit published
- September 25, 2004 – Connect back shell exploit published
- September 28, 2004 – First reported attack

Microsoft Word Zero Day Attack



PC WORLD

New Zero-Day Word Attack

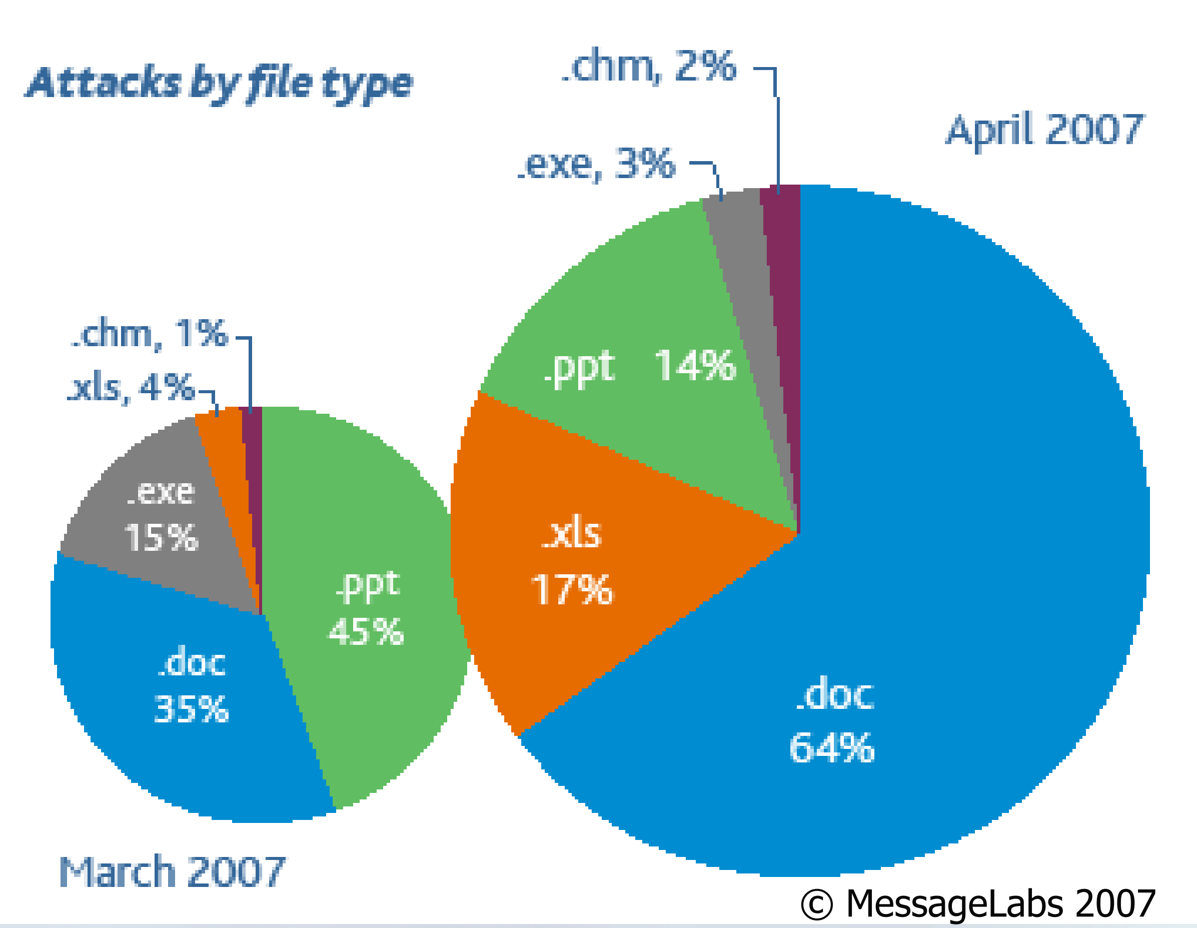
Posted by Erin Biba
Thursday, February 15, 2007 6:33 AM PT

Microsoft's Word and Office programs have been targeted again, with the company warning that hackers may already exploiting a new vulnerability found in the applications.

The warning comes just after the company issued fixes for 20 other bugs in its products on Tuesday, including six for Word.

The latest problem affects Office 2000 and Office XP, Microsoft said in a security advisory on Wednesday. An attacker could create a specially-crafted Word document that, if opened, could allow them to control a victim's computer remotely. As usual it advised great caution when opening unsolicited attachments.

Targeted Attacks



© MessageLabs 2007

April 2007

- 595 emails
- 180 targeted attacks
- 192 domains targeted
- 168 customers

March 2007

- 716 emails
- 249 targeted attacks
- 263 domains targeted
- 216 customers

Why Targeted Attacks?

Detection

- Individual emails are less likely to trigger network spam/AV filters

Social Engineering

- Targeted attacks can be customized
- More likely to be read/opened by victims

Challenges

Blocking attacks at the perimeter

- ‘Normal’ traffic
  - HTTP
  - Office documents
  - Media files
- Volume
  - Thousands/Millions
- Encoding
  - Difficult to develop detection signatures

Patching

- Thousands of machines
- Mobile machines
- Geographically dispersed

Predictions

Criminal Use

- Increased use of client side vulnerabilities in targeted attacks
- Focused, funded research

Vulnerability types

- Decrease in Microsoft file format vulnerabilities due to various changes in Office 2007/Vista
- Increased vulnerability discovery in non-Microsoft applications

Questions

Michael Sutton, Security Evangelist

http://portal.spidynamics.com/blogs/msutton

Michael.Sutton@hp.com