

Enterprise Security Goes Mobile

Welcome

TRITON™

Web security

Email security

Data security

Mobile security

Agenda

9:10 – 10:10

Mobile security: trends, threats and challenges to IT security

10:10 – 10:20

Coffee Break

10:20 – 11:15

Websense® TRITON™ Mobile Security

11:15

Close

Mobile Breakfast Briefing

Carl Leonard
 Websense, Inc.

TRITON™

Web security

Email security

Data security

Mobile security

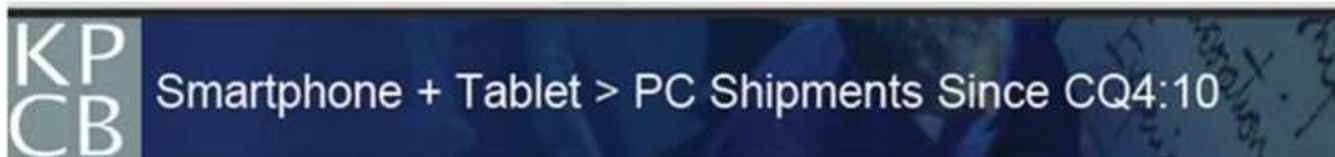


Trends in the Mobile Landscape

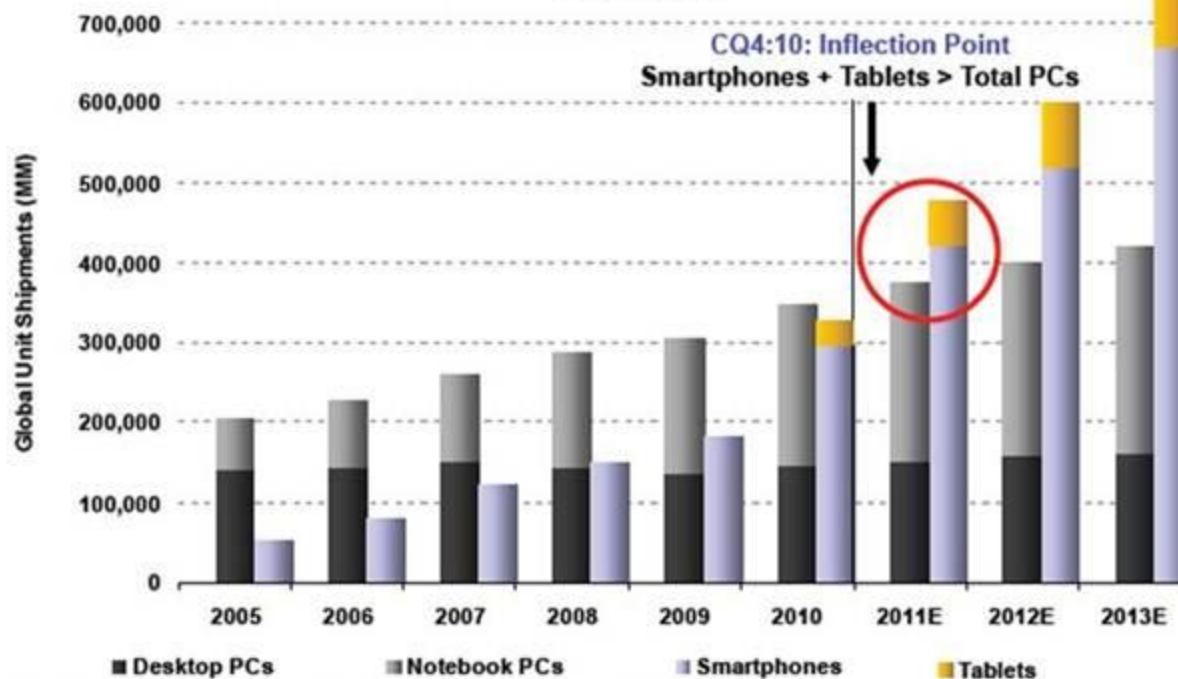
TRITON™

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

Tablets Outselling Laptops?



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.

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

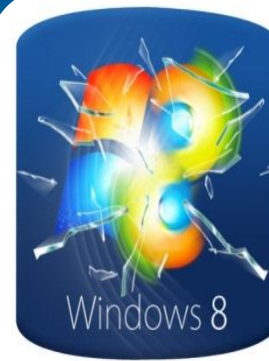
TRENDS



Externalization of
IT infrastructure



Consumerization &
virtualization
of the end point



Windows8 security
leaps forward



Business
enablement
via social web



Security
consolidation
continues



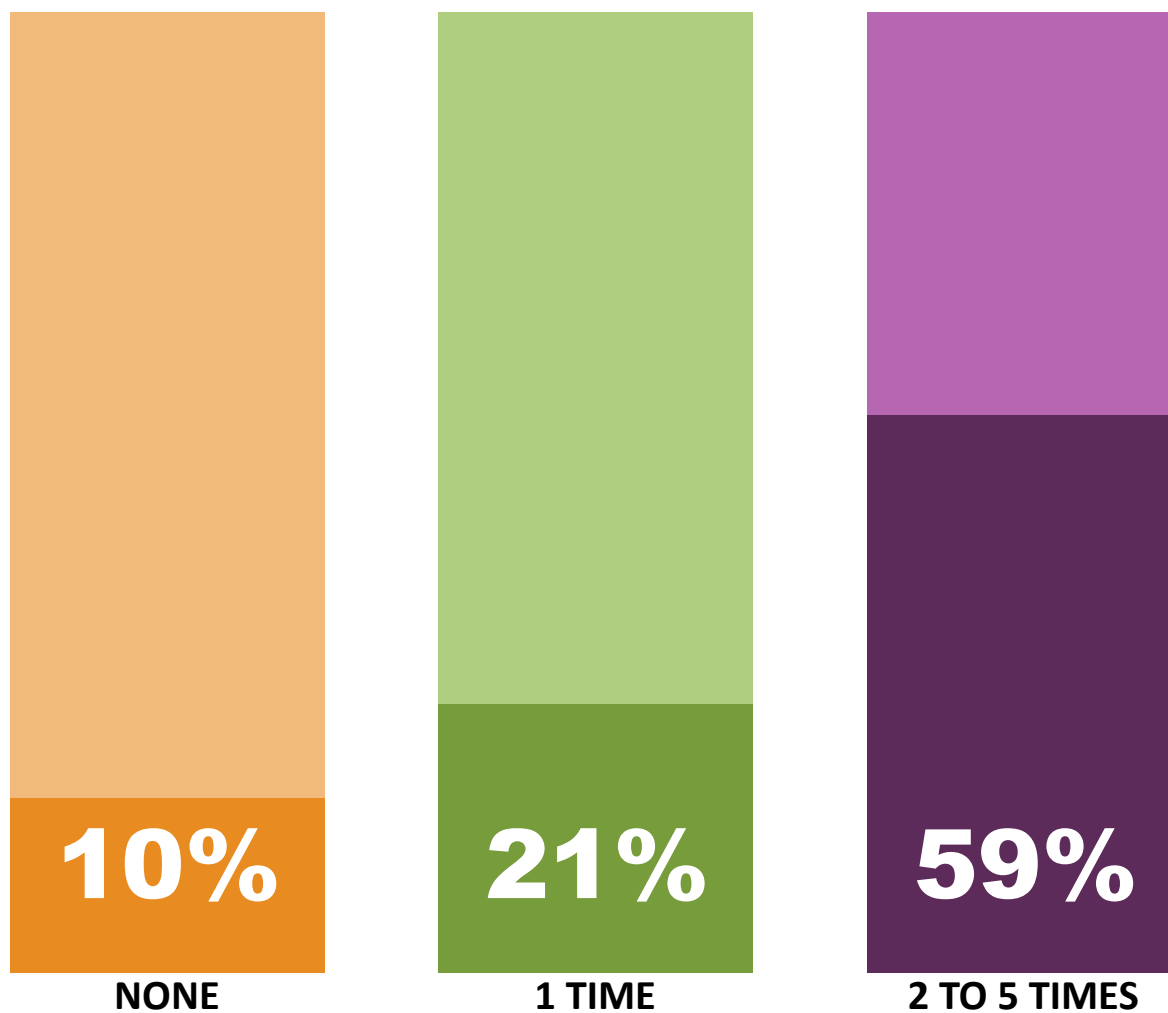
Data oriented
attacks are an
everyday event



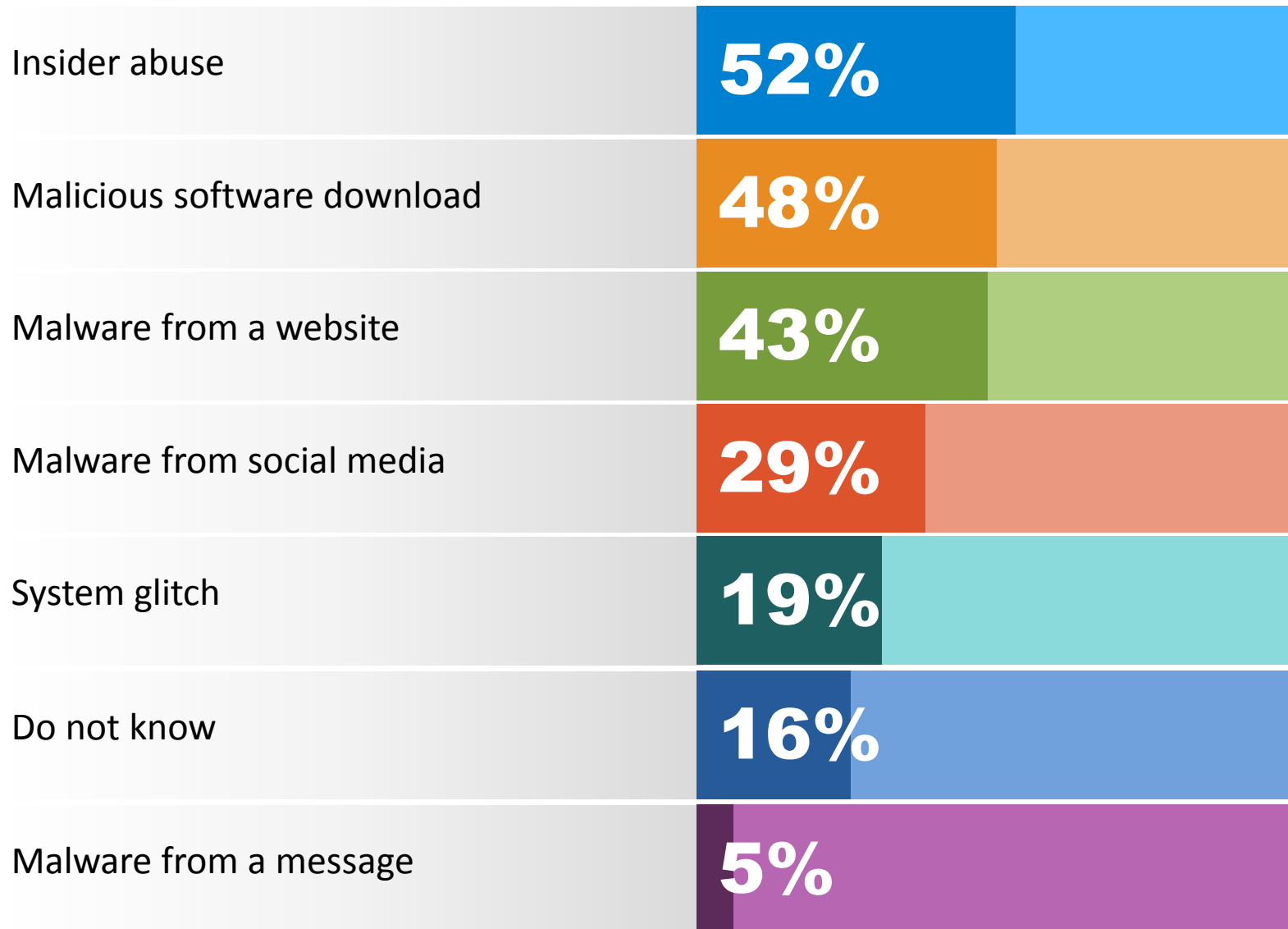
THE EMPOWERED USER

Fundamental shift in security needed

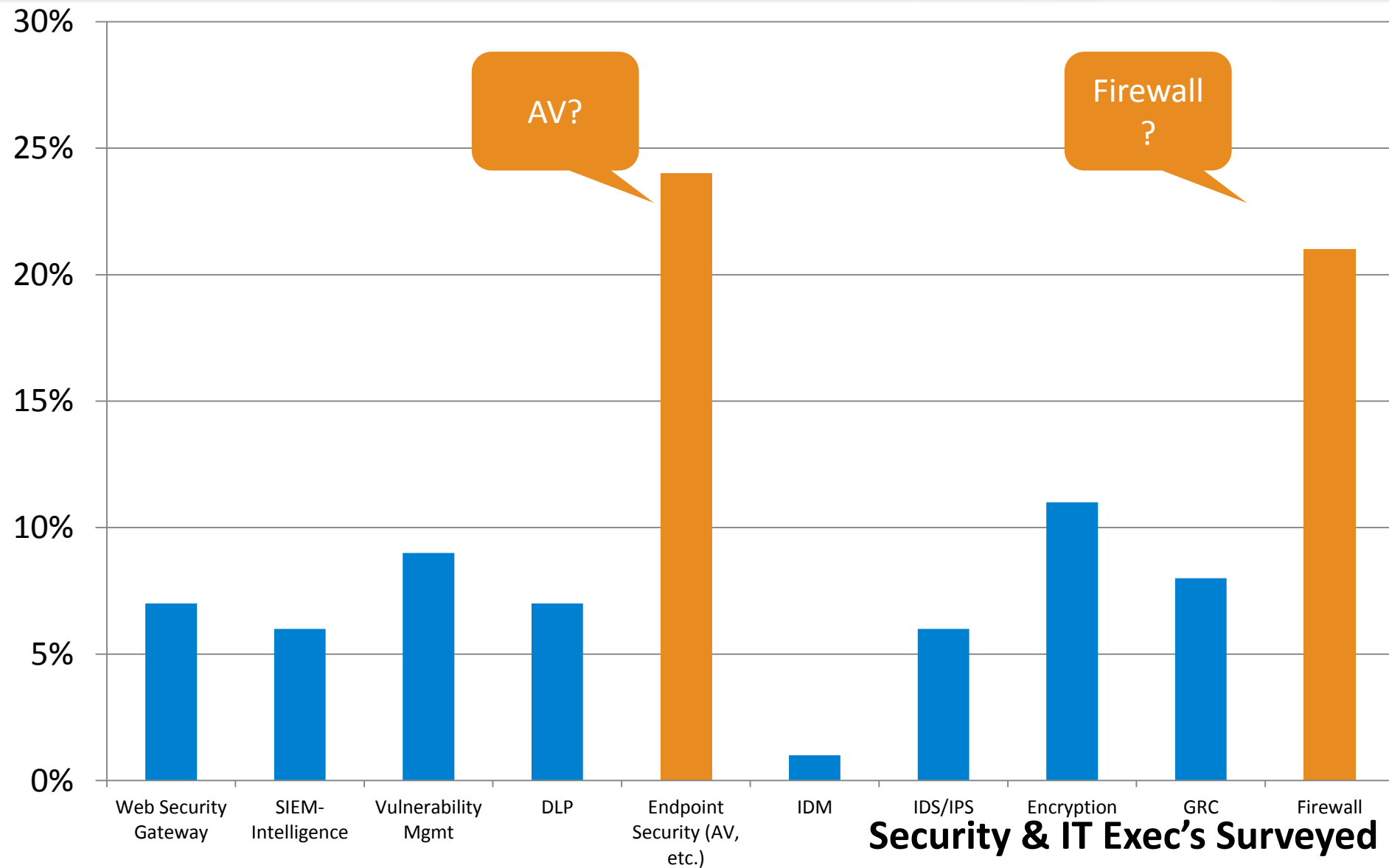
THE NUMBER OF SUCCESSFUL NETWORK SECURITY BREACHES OVER THE PAST YEAR



WEB EXPOSURE DRIVES INFORMATION THEFT **websense®**

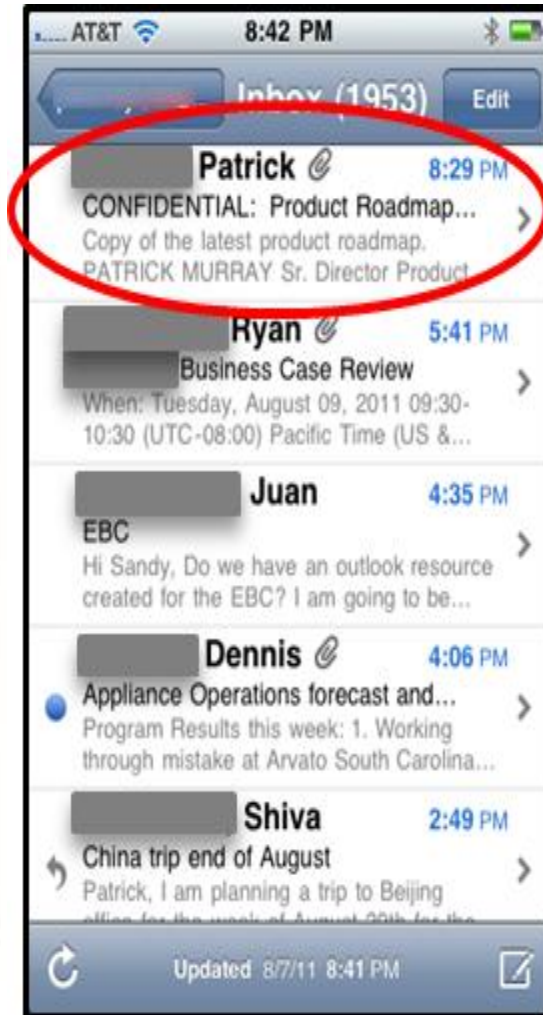
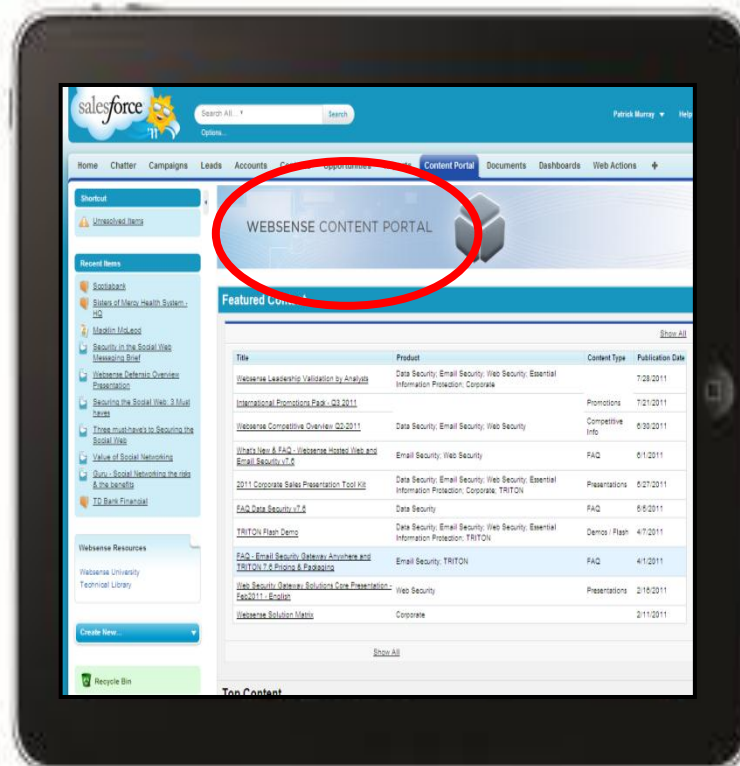
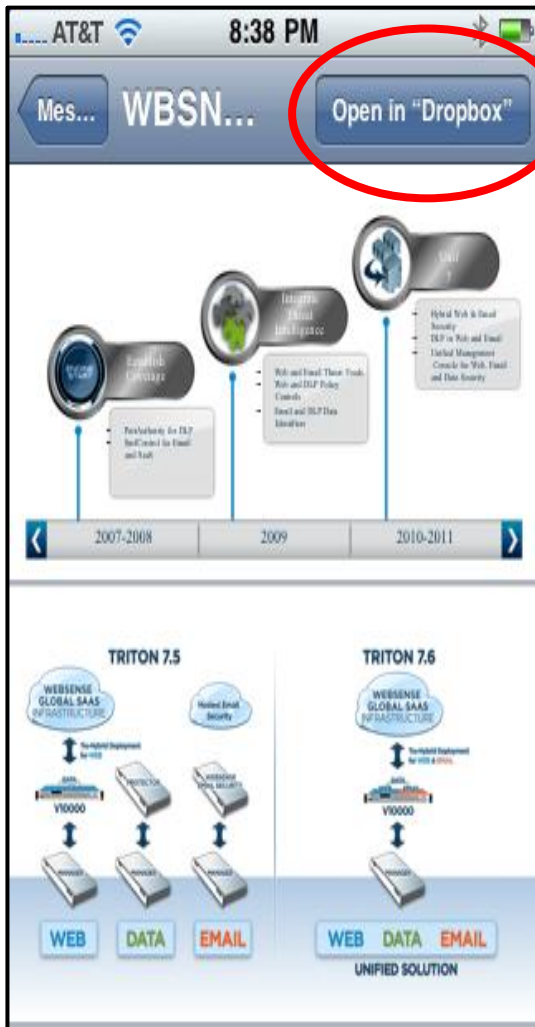


What is your best security solution?



- Challenges
 - User owned device
 - You may or may not own the pipe
 - Lives outside your network
- Primary Risk
 - Secure corporate data on the device
 - If the device is lost
 - Employee leaves the company
 - Prevent data leakage to unauthorized destinations or recipients

Examples of Data at Risk



EMBARGOED DRAFT – Do not distribute before the morning of Wednesday, February 29, 2012 (12:01 a.m. ET)





Global Study on Mobility Risks

Survey of IT & IT Security Practitioners

Sponsored by Websense, Inc.
Independently conducted by Ponemon Institute LLC
Publication Date: February 2012

Ponemon Institute® Research Report

- Headlines

- 77% agree that employee use of mobile devices is essential or very important to their organization's ability to meet its business objectives. A similar percentage.
- 76% recognize that these tools put their organizations at risk.
- 51% experienced data loss because of unsecured mobile devices, including laptops, smartphones, USB devices, and tablets.
- 59% saw an increase in malware infections as a result of unsecured mobile devices in the workplace.
- 59% say that employees circumvent or disengage security features such as passwords and key locks.

Morning Exercises

TRITON™

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

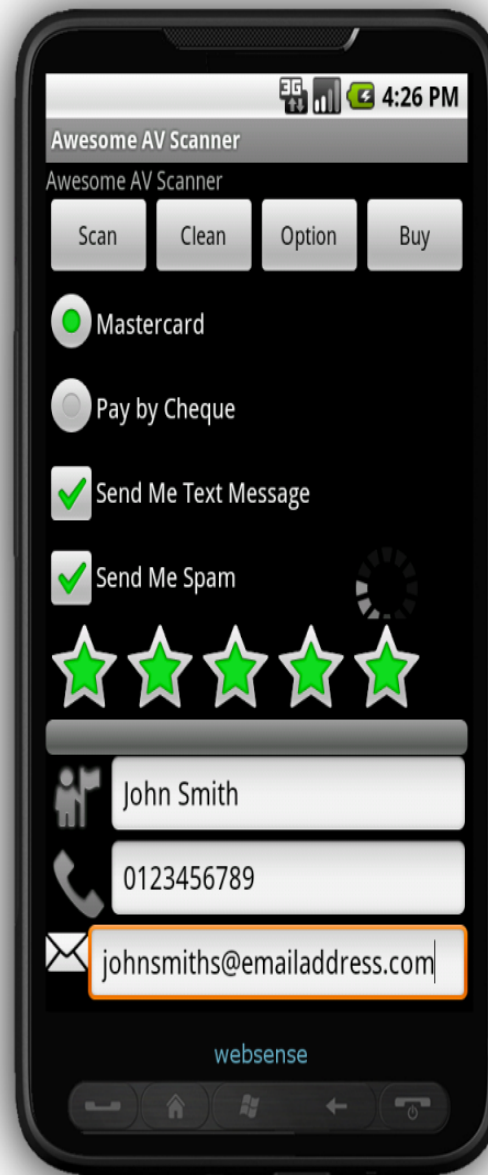
Activity Times	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Early Morning	Stretching, Resistance Exercises w/Bands, 10 minutes on Glider	Stretching, Leg Lifts & Dips on Exercise Tree, Ab-Roller , 10 minutes on Glider	Stretching, Resistance Exercises w/Bands, 10 minutes on Glider	Stretching, Leg Lifts & Dips on Exercise Tree, Ab-Roller , 10 minutes on Glider	Stretching, 10 minutes on Glider	Stretching, 10 minutes on Glider	Stretching
Mid-Morning		Power Walk Outside		Power Walk Outside			Go for Walk in the Woods
Afternoon		Sauna		Sauna			
Evening	Cook, Clean, Walk the Dog	Cook, Clean, Walk the Dog			Cook, Clean, Walk the Dog	Cook, Clean, Walk the Dog	Sweatlodge

Exercise: Think Like a Hacker

How would you attack
your organisation?



Exercise: Let's Create an App



Websense 
Security Labs



Rogue App - version 1

The screenshot displays the Eclipse IDE environment. The main editor window shows the source code for `AwesomeAVScannerActivity.java`. The code is as follows:

```
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);
    }
}
```

The Package Explorer on the left shows the project structure for 'Awesome AV Scanner'. The Outline on the right shows the class hierarchy and the `onCreate(Bundle)` method. The LogCat at the bottom is currently empty, with a search bar and a table for filtering messages.

L...	Time	PID	Application	Tag	Text

Rogue App - version 2

Java - Awesome AV Scanner/src/com/av/scanner/AwesomeAVScannerActivity.java - Eclipse SDK

File Edit Run Source Refactor Navigate Search Project Window Help

Package Explorer

Awesome AV Scanner

```
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);
    }
}
```

Outline

- com.av.scanner
- import declarations
- AwesomeAVScannerAct
 - onCreate(Bundle):
 - clickRegister(View)

Problems Javadoc Declaration Console LogCat Devices

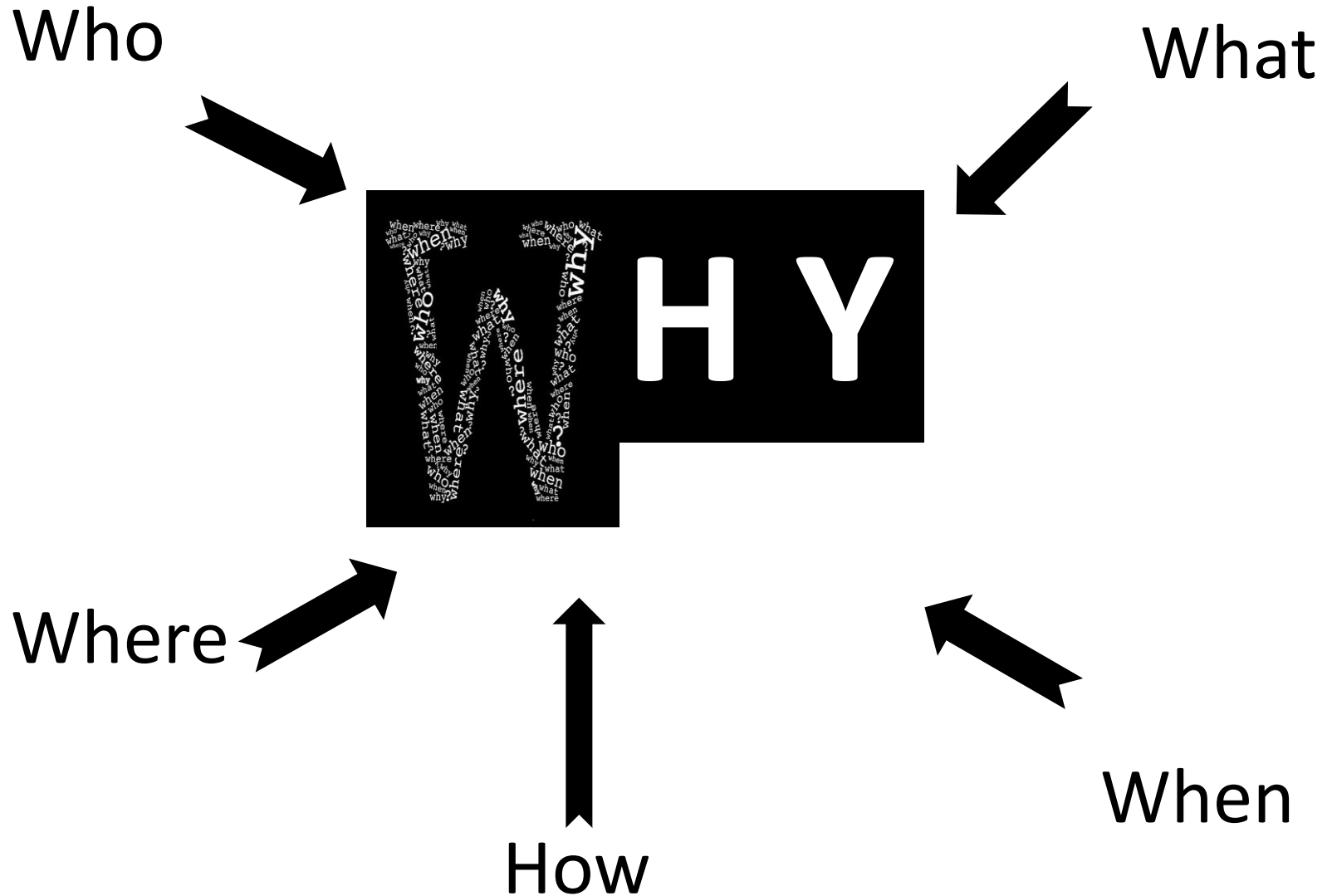
Saved Filters + -

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

What are we interested in?



Websense App Tracker

[Upload and Analysis](#) | [Search](#) | [Report](#) | [Top lists](#)

Search

You can search for app analysis reports

☒ 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	<ul style="list-style-type: none">- Allows applications to open network sockets.- Allows an application to write to external storage
App Network Actions	<ul style="list-style-type: none">- 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?

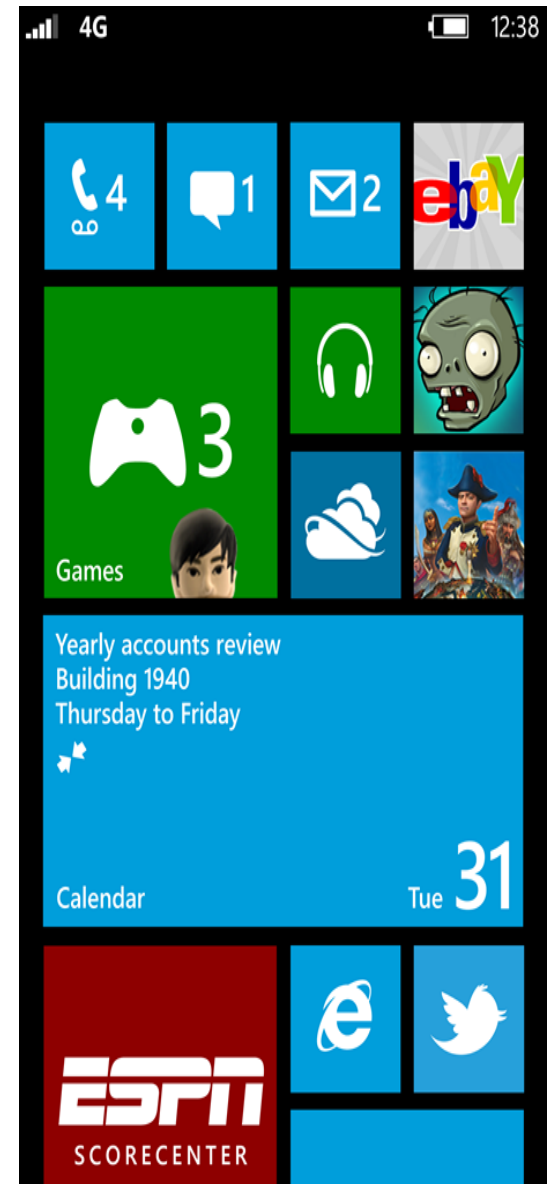
Attack Vectors to Look Out For

TRITON™

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

Windows Phone 8

websense®

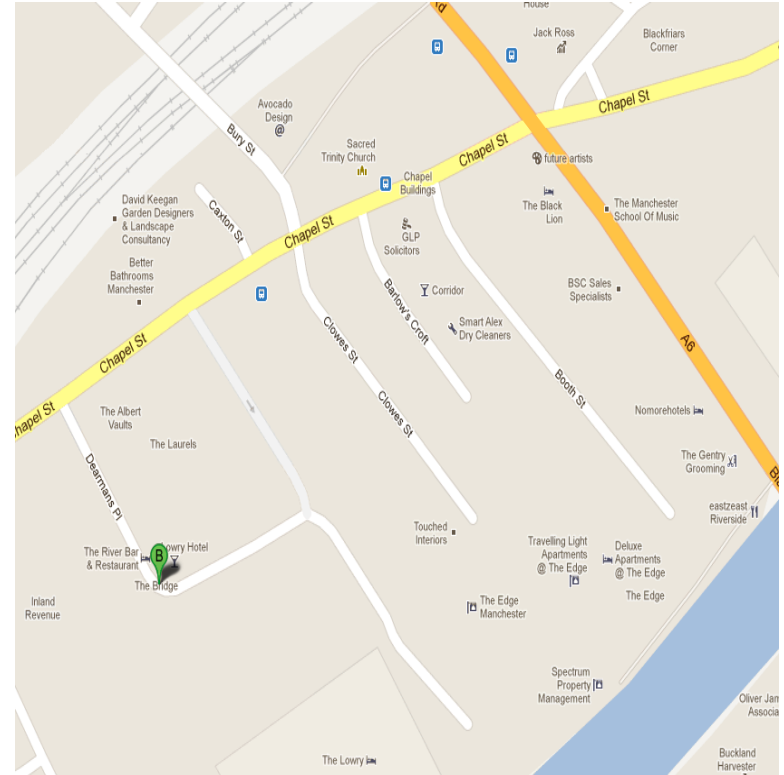




VS



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



Hi, please click here

Hi Dan, shall we meet at [The Black Lion](#) later?



<http://iJustStoleYourData.co.cc/>

Spear Phishing



Announcing Cyber Security Intelligence Services

TRITON™

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

"It's becoming clear that many of these emerging threats cannot be defended against in-house, creating a shift in security posture toward being more proactive."

IDC Senior Analyst Christine Liebert

IDC press release, Jan. 31, 2012, <http://www.idc.com/getdoc.jsp?containerId=prUS23290912>

When defenses fail...

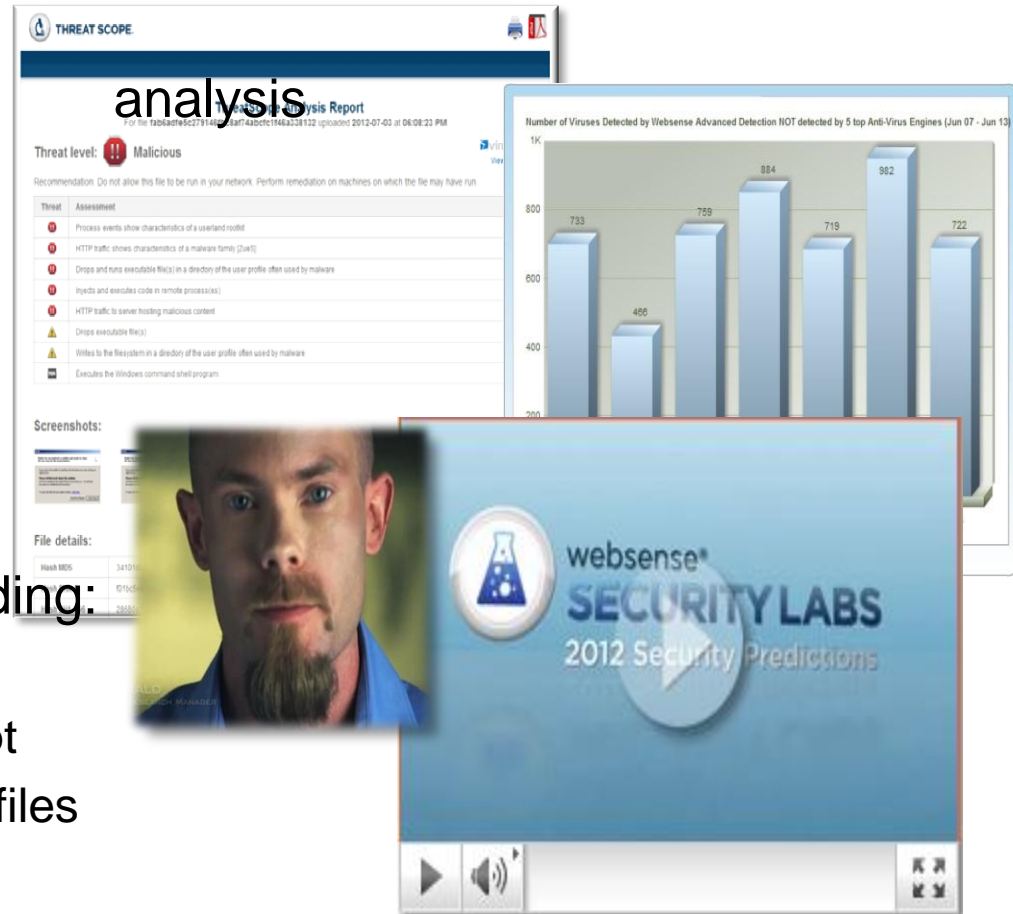
- How did it get in?
- Which defense worked?
- Which defense failed?
- How is the PC/server/device affected?

You need answers.

- Who was targeted?
- What data was targeted?
- Where is it now?
- How do we tighten defenses to prevent a repeat?

Blocking is not enough. IT needs resources to become proactive.

- ThreatScope malware sandbox
- Priority access to a variety of research tools/services
- On-demand videos
 - Security Labs TAB events
 - Research presentations
- Threat & Security training including:
 - Analyzing mobile malware
 - How to de-obfuscate JavaScript
 - Dynamic analysis of malicious files



Websense ThreatScope™ Sample Report

websense®



ThreatScope Analysis Report

For file: fab6adfe5c279146fbc8af74abcf1146a339132 uploaded: 2012-07-03 at 06:08:23 PM

Threat level: **Malicious**



[View results >](#)

Recommendation: Do not allow this file to be run in your network. Perform remediation on machines on which the file may have run.

Threat	Assessment
	Process events show characteristics of a userland rootkit
	HTTP traffic shows characteristics of a malware family (Zus)
	Drops and runs executable file(s) in a directory of the user profile often used by malware
	Injects and executes code in remote process(es)
	HTTP traffic to server hosting malicious content
	Drops executable file(s)
	Writes to the filesystem in a directory of the user profile often used by malware
	Executes the Windows command shell program

Screenshots:



File details:

Hash MD5	34101da4902000dcb0143a4e845023b7	File size	233.82 KB
Hash SHA-1	10101e4305ab4e345e12a08250a19b786568464	File uploaded	2012-07-03 06:08:23 PM
Hash SHA-256	28580a11e4b3450bac080817cc0309909d60b14aeb01943ca7b0592007e	Report created	2012-07-03 06:10:11 PM

Technical Details



Requested HTTP URLs

The analyzed file requests the following URLs:

URL	IP Address	Category	Details	Method	Status	MIME
www.google.co.kr/webhp	74.125.235.212	Search Engines and Portals		GET	200	text/html; charset=UTF-8
109.169.37.149/~admin/config/ate.php	109.169.37.149	Malicious Web Sites		POST	200	text/html
109.169.37.149/~admin/config/omfg-bin	109.169.37.149	Malicious Web Sites		GET	200	application/octet-stream

www.google.co.kr/webhp 74.125.235.212 GET 200 charset=UTF-8



Resolved hostnames

The analyzed file used DNS to resolve the following hostnames:

Hostname	Category	IP address
www.L.google.com	Search Engines and Portals	74.125.235.212
www.L.google.com	Search Engines and Portals	74.125.235.209
www.L.google.com	Search Engines and Portals	74.125.235.211
www.L.google.com	Search Engines and Portals	74.125.235.208
www.L.google.com	Search Engines and Portals	74.125.235.210
www.cdnl1.google.com	Search Engines and Portals	74.125.235.223
www.cdnl1.google.com	Search Engines and Portals	74.125.235.215
www.cdnl1.google.com	Search Engines and Portals	74.125.235.216



IP addresses

The analyzed file requests the following IP addresses:

IP Address	ASN
74.125.235.223	AS15169 Google Inc.
109.169.37.149	AS20880 Iomart
109.169.37.149	AS20880 Iomart
74.125.235.212	AS15169 Google Inc.



File system modifications

The analyzed file changes the following items in the file system. This type of change can be performed by both malicious and benign files.

Event	File path
Creates file	c:\Documents and Settings\Administrator\Application Data\Ykiblood.exe
Opens file	c:\Documents and Settings\Administrator\Application Data\Ykiblood.exe
Writes file	c:\Documents and Settings\Administrator\Application Data\Ykiblood.exe
Creates file	c:\Documents and Settings\Administrator\Local Settings\Temp\mp43c431b7.bat
Opens file	c:\Documents and Settings\Administrator\Local Settings\Temp\mp43c431b7.bat
Writes file	c:\Documents and Settings\Administrator\Local Settings\Temp\mp43c431b7.bat



Process modifications

The analyzed file affected the following system processes:

Event	File path
Creates process	Sample started
Creates process	C:\WINDOWS\system32\cmd.exe
Creates process	C:\Documents and Settings\Administrator\Application Data\Ykiblood.exe



ThreatScope Analysis Report









For file fab6adfe5c279146fbc8af74abcf1f46a338132 uploaded 2012-07-03 at 06:08:23 PM

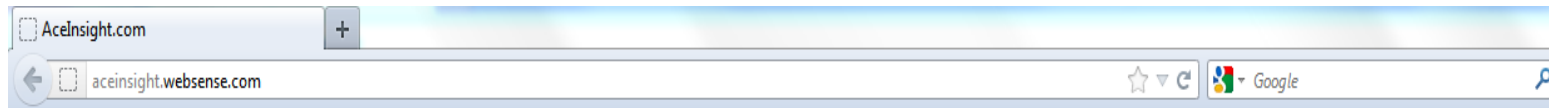
Threat level:  **Malicious**



[View results >](#)

Recommendation: Do not allow this file to be run in your network. Perform remediation on machines on which the file may have run.

Threat	Assessment
	Process events show characteristics of a userland rootkit
	HTTP traffic shows characteristics of a malware family [ZueS]
	Drops and runs executable file(s) in a directory of the user profile often used by malware
	Injects and executes code in remote process(es)
	HTTP traffic to server hosting malicious content
	Drops executable file(s)
	Writes to the filesystem in a directory of the user profile often used by malware
	Executes the Windows command shell program



[Register](#) for an account, or [Login](#) ?

www Site Analysis

Enter a URL to see if it contains malicious content. A free service powered by Websense® TRITON™.

Analyze

- Real-time security and content classification
- Billions of URLs analyzed daily
- 50 million data sources



ThreatScope™ File Analysis

Find out if a file contains malicious content or behavior. A service for Websense® CyberSecurity Intelligence (CSI) customers.

- Threat classification based on behavioral analysis
- Comprehensive forensic report
- Powerful behavioral file analysis

[Learn more about CSI >](#)

Login

NEW!

Visit the Websense Security Labs Blog



Read up on the latest posts to our interactive blog.

[View blog >](#)

NEW!

Websense® 2012 Threat Report



Data Theft, Targeted Attacks, and Exploit Kits. Are you ready?

[Get the report >](#)

NEW!

New release: Websense® TRITON™ v7.7

No one stops more threats than Websense.



[Let us prove it >](#)

3 prestigious awards!



- ▶ Best Enterprise Security Solution
- ▶ Reader's Trust Award
- ▶ Best Corporate Security Blog

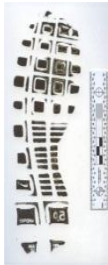
[Learn more >](#)

Follow Websense on Facebook, Twitter and Security Labs [f](#) [t](#) [s](#)

Work Directly with Websense Security Labs Researchers

Forensic Investigation

- Partner with a researcher and Websense Security Labs
- Completely Confidential
- Forensic 4 pack add-on



Hands-on Security Training

- Security Labs Instructors
- 3-day security class w/hands-on
- Offered twice annually (EMEA and NA locations)



Proactive Security Reviews

- Policy and configuration
- Define use case exercises
- Industry, regional, and custom network concerns
- Semi-Annual



websense®
SECURITY LABS

Custom Control Assessments

- Full white/black list analysis
- Assess each item for
 - Security classifications
 - Categorization
- Performed quarterly





<http://securitylabs.websense.com/>

Coffee break

TRITON™

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

Appendix

TRITON™

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

Mobile Device Security

Jon Noel

TRITON™

Web security

Email security

Data security

Mobile security

- Consumerization of IT
- IT challenges with mobile devices
- TRITON Mobile Security Overview
- Best practices for BYOD strategy
- New iOS 6 features





Fast & disruptive

Enables business

Increases productivity

- Data on devices
- Types of devices on network
- Policies for BYOD
- Mobile app use, jail broken devices
- Administration & deployment



**IT
control**



**Personal
device**

Current Approaches

OPTION #1 **ActiveSync** **for device** **controls**



Provides basic controls such as access to Exchange, password enforcement, remote wipe but no data leakage prevention or threat protection.

OPTION #2 **Backhaul** **traffic over** **VPN**



Using a VPN client to backhaul traffic to enterprise network. Results in higher infrastructure and management costs.

OPTION #3 **Tablet as a** **terminal**



Run enterprise apps on a server farm and display them on the tablet. Significant investment in infrastructure with limited data protection.

OPTION #4 **Mobile Device** **Management** **(MDM)** **solutions**



Provides device level controls but these systems are content unaware and vulnerable to malware & data loss.

OPTION #5 **Container** **approach**



Provides a container to access email, calendar, contacts and a some other apps. Good but expensive approach and impacts user experience





**Web & Email
security**



**Web & Email
security**



**Malicious app and
mobile malware protection**





**Web & Email
security**



**Malicious app and
mobile malware protection**



MDM

Protection from:

- Mobile malware
- Malicious apps
- Phishing & scams
- Advanced malware
- Data theft



Control for:

- BYOD
- Enterprise devices
- Mobile DLP for email
- Web security & apps
- Compliance



Cloud

Web Security



Mobile Security



TRITON™ Mobile Security

ACE + ThreatSeeker Network
Malicious Mobile App Tracker
Management + Reporting

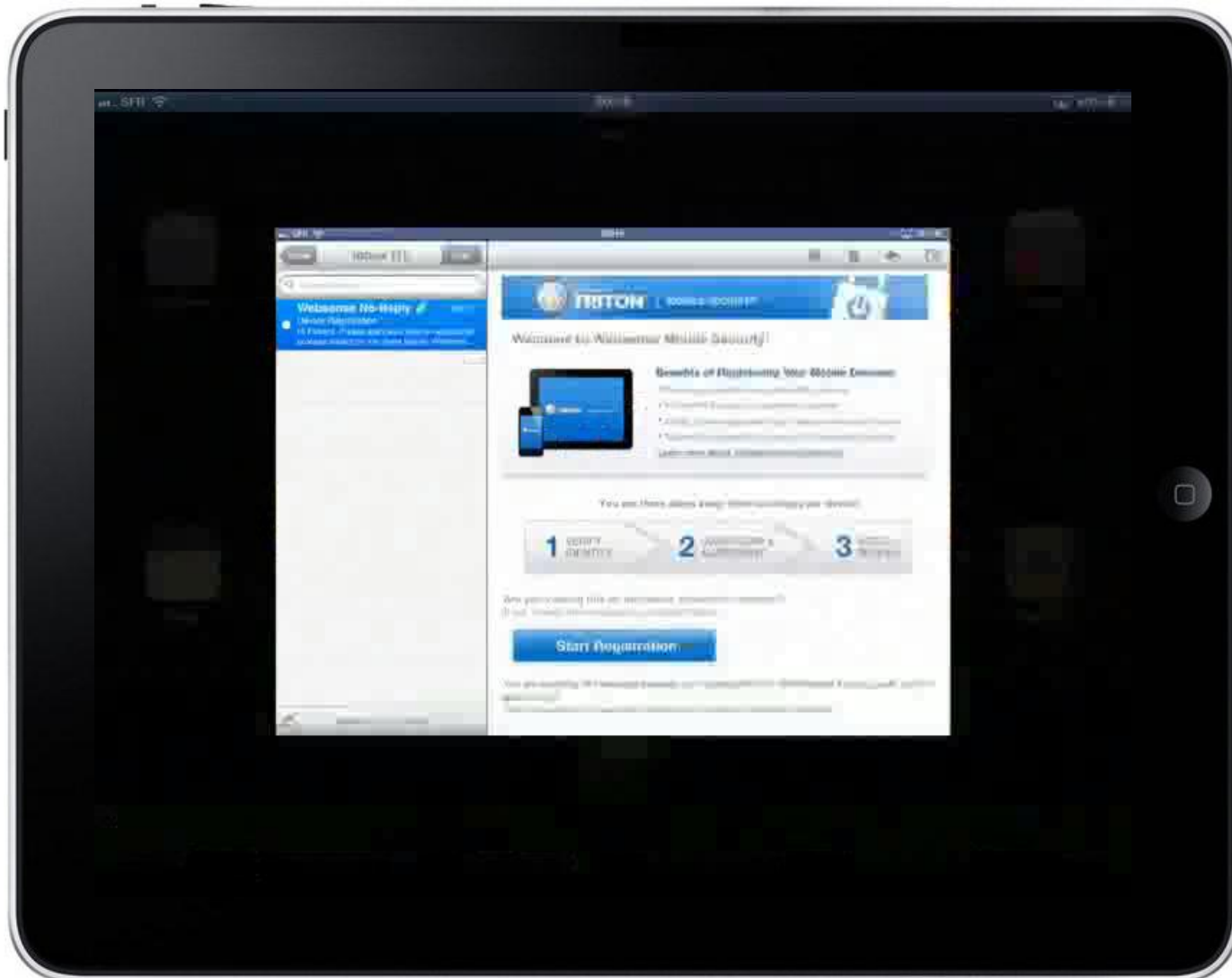
VPN**
WiFi/3G



** iOS, Android







- **Identify your objectives**
 - Protecting corporate data on the device and the use of it
 - Regulatory compliance
- **Understand the threats**
 - Lost or stolen device
 - Misuse of corporate data
 - Web/network based attacks



Best Practices for BYOD Strategy- Continued **websense®**

- **Countermeasures and controls**
 - Allow only a specific set of devices



- **Countermeasures and controls**
 - Allow only a specific set of devices
 - Establish security policy for mobile devices



- **Countermeasures and controls**

- Allow only a specific set of devices
- Establish security policy for mobile devices
- Integrate policies for personal devices with your Acceptable Use Policy



- **Countermeasures and controls**

- Allow only a specific set of devices
- Establish security policy for mobile devices
- Integrate policies for personal devices with your Acceptable Use Policy
- Establish minimum security posture for devices accessing corporate data



- **Countermeasures and controls**

- Allow only a specific set of devices
- Establish security policy for mobile devices
- Integrate policies for personal devices with your Acceptable Use Policy
- Establish minimum security posture for devices accessing corporate data
- Decide what mobile apps are allowed or banned



- **Countermeasures and controls**

- Allow only a specific set of devices
- Establish security policy for mobile devices
- Integrate policies for personal devices with your Acceptable Use Policy
- Establish minimum security posture for devices accessing corporate data
- Decide what mobile apps are allowed or banned
- Be clear about privacy and employee responsibility of personal data and apps



- **Countermeasures and controls**

- Allow only a specific set of devices
- Establish security policy for mobile devices
- Integrate policies for personal devices with your Acceptable Use Policy
- Establish minimum security posture for devices accessing corporate data
- Decide what mobile apps are allowed or banned
- Be clear about privacy and employee responsibility of personal data and apps
- Define a clear service policy for devices that fall under BYOD criteria



- **Countermeasures and controls**

- Allow only a specific set of devices
- Establish security policy for mobile devices
- Integrate policies for personal devices with your Acceptable Use Policy
- Establish minimum security posture for devices accessing corporate data
- Decide what mobile apps are allowed or banned
- Be clear about privacy and employee responsibility of personal data and apps
- Define a clear service policy for devices that fall under BYOD criteria
- Have a strategy when an employee leaves the company



More Info: <http://www.websense.com/content/mobile-aup.aspx?cmpid=prblog>

Devices on iOS6

- Disable Shared Photo Stream
- Disable Passbook from appearing on the screen when locked
- Automatically remove profiles after a given period of time
- Set device wallpaper
- Prevent recent contacts from syncing to the mail server

Devices set-up in supervised mode

- Lock down devices to one app with App Lock and disable the home button
- Force all device network traffic through global HTTP proxy
- Prevent installation of certificated or unmanaged configuration profiles
- Disable iMessage
- Disable Game Center and iBookstore and set iBookstore rating restrictions

Thank you

TRITON[™]

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

QUESTIONS..?

TRITON™

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