websense

BEFORE, DURING & AFTER THREAT DETECTION & PROTECTION

Jeff Debrosse - Director, Security Research

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

websense® TRITON™

Security Environment

- Advanced Attacks
- Data Theft & Loss
- Declining Effectiveness
- Lack of Forensics
- Complexity Increasing
- Point Solutions
- Increased Risk

WHO'S GOT THEIR HANDS ON YOUR DATA?

WANT TO SEE HOW YOUR DEFENSES ARE BYPASSED?

TRADITIONAL SECURITY NO LONGER SECURES

There's a town in Romania known as Hackerville. It's where criminals turn data into expensive sports cars. This isn't just credit card fraud, this is monetizing intellectual property swiped from companies who thought they were protected.

We know where the bad guys lurk. Not just in Hackerville, but also in your network's blind spots. Put us to the test.

NO ONE STOPS MORE THREATS. LET US PROVE IT.

websense

Global Human Intelligence

websense

SC MAGAZINE AWARDS 2012 WINNER Honored in the U.S.

Best Corporate Security Blog

Websense Security Labs

120+ Researchers

Four Locations

US, UK, China, Israel

Content Security Research

Web, Email, Data & Mobile

Dedicated web site

securitylabs.websense.com

Obfuscation

Machine Learning & Automation

Malware Reverse Engineering

Big Data Clusters & Querying

Statistical Models

ThreatSeeker

Security Intelligence Cloud

Real-time Security classifier

Real-time Content classifier

Real-time Data classifier

Mobile App classifier

websense® ACE ADVANCED CLASSIFICATION ENGINE

© 2013 Websense, Inc.

By The Numbers…

websense®

92%

of all unwanted emails contain URLs

85%

of malicious URLs are on compromised hosts

© 2013 Websense, Inc.

More, more and more

	2011	2012
Unique threats discovered	16M	100.1 M (+625%)
Compromised web pages discovered		83,918,998

1.9 / second

REAL-TIME UPDATES

1.2 million
USA = 80%

UNIQUE PHISHING ATTACKS

19.4 billion
99.58% SPAM

BLOCKED E-MAILS

25.8 million
3.44 per seat

BLOCKED WEB THREATS EACH WEEK

© 2013 Websense, Inc.

Changing Threat Landscape

websense

Advanced Threats

THEN	NOW
Signature Based	Zero Day
High Volume	Low Volume
Mass Distribution	Trusted Entry

Data Theft

THEN	NOW
Goal: Damage	Goal: Financial gain
Inbound focus was enough	Assume holes in security
Data was easily identifiable	Theft can easily be hidden

Attack & Malware Forensics

THEN	NOW
Hands-Off	Hands-on
Reactive	Proactive
Focus on intrusion prevention	Holistic View

© 2013 Websense, Inc.

Why Current Defenses Fail

websense®

Signature & Reputation-based Defenses

- Dynamic Threats
- Targeted Attacks
- Timed Arming
- Trusted Hosts
- Sniper Profile

Lack of Inline Real-time Threat Analysis

- Passive Design
- Sample Collection
- Volume Focused
- Background Vote
- Pre-test Threats

Forward Facing Defenses

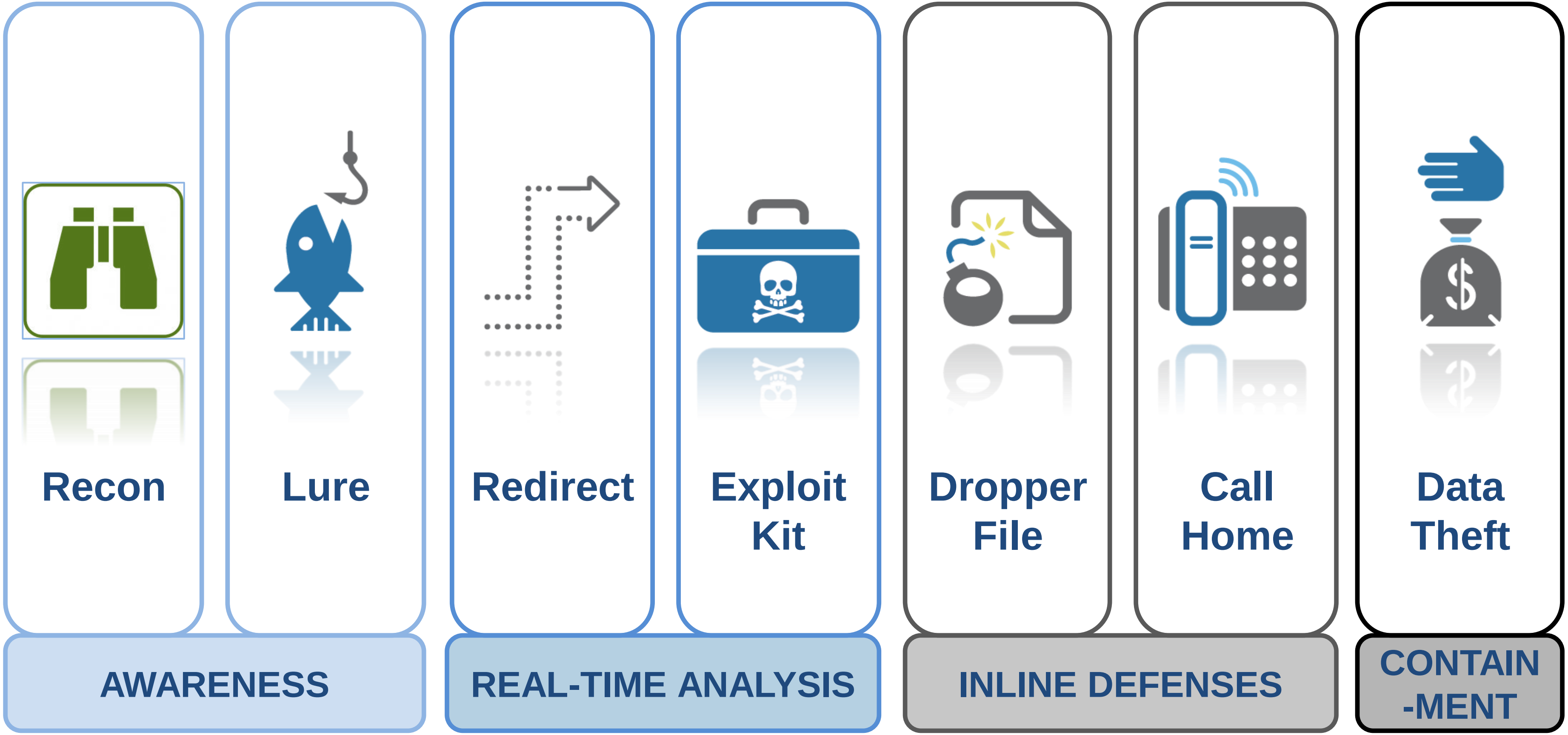
- Airport Model
- Screen Inbound
- Open Outbound
- No Containment
- No Data Protection

Blind Spots Using More Of the Same

- UTMs, NGFWs
- Consolidation
- Commodity AV/URL
- Security vs Perf.
- Growing SSL

© 2013 Websense, Inc.

The Seven Stages of Advanced Threats



Recon

Lure

Redirect

Exploit Kit

Dropper File

Call Home

Data Theft

AWARENESS

REAL-TIME ANALYSIS

INLINE DEFENSES

CONTAINMENT

© 2013 Websense, Inc.

Seven Advanced Threat Stages

Recon

Lure

AWARENESS

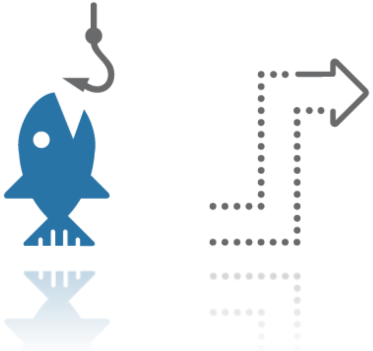
- Web & Email
- Facebook, Blogs, Tweets
- Spear-phishing
- Trusted entry
- Targeted
- Dynamic
- Timed

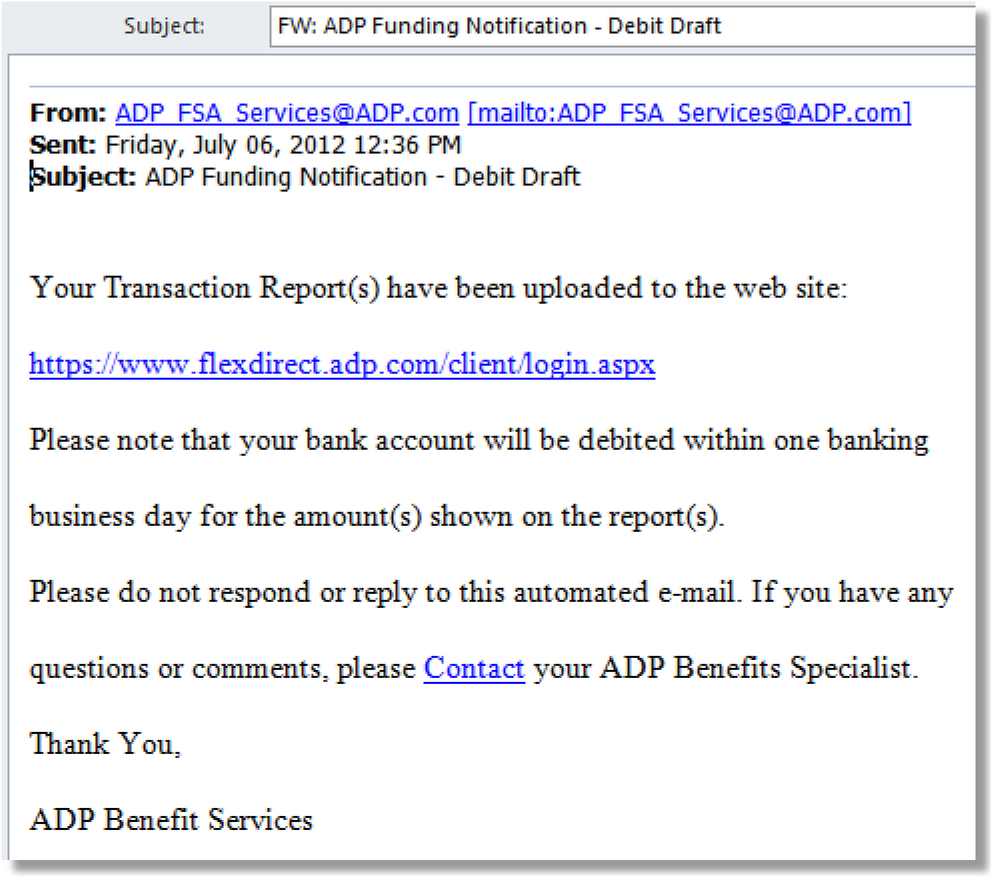
© 2013 Websense, Inc.

Example – Spear Phishing

websense

- 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

© 2013 Websense, Inc.

Seven Advanced Threat Stages

Redirect

Exploit Kit

REAL-TIME ANALYSIS

- Browser code & active scripts
- Link analysis
- Exploit analysis
- Composite scoring/ratings
- Predictive

© 2013 Websense, Inc.

Seven Advanced Threat Stages

INLINE DEFENSES

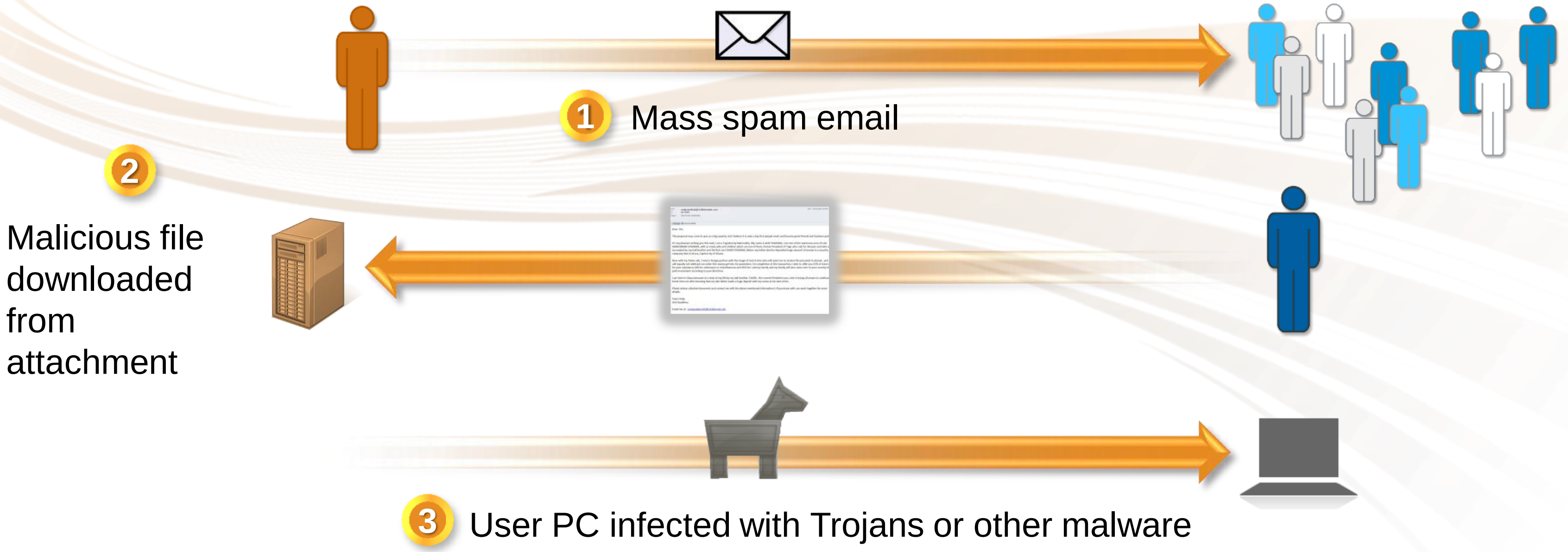
- App analysis
- Malicious PDFs
- Multiple AVs
- File compress.
- Dynamic DNS
- Botnet & CnC comms

Dropper File

Call Home

© 2013 Websense, Inc.

Traditional Email Attack



1 Mass spam email

2 Malicious file downloaded from attachment

3 User PC infected with Trojans or other malware

© 2013 Websense, Inc.

Seven Advanced Threat Stages

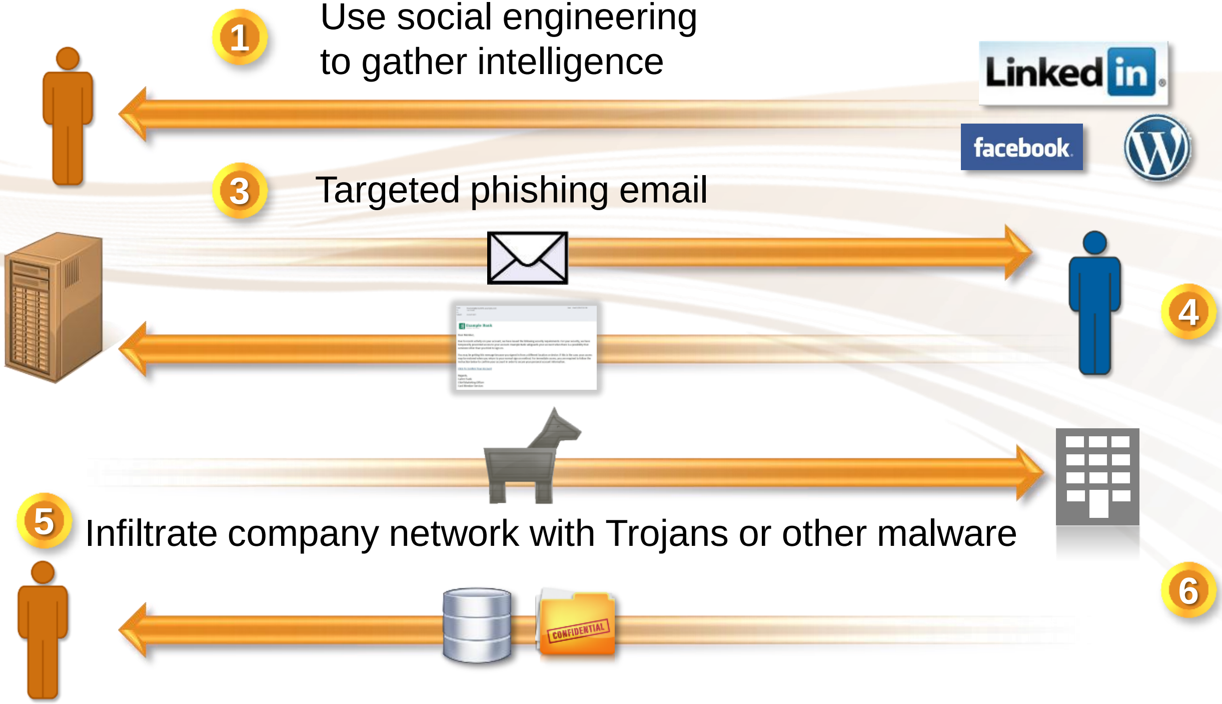
CONTAINMENT

- Data theft defenses
- Embedded DLP
- Data capture
- Geo-location
- Forensic details & reporting
- Alerts/severity

Data Theft

© 2013 Websense, Inc.

Modern Blended Attack



1 Use social engineering to gather intelligence

2 Hacker takes over legitimate business server

3 Targeted phishing email

4 Unsuspecting user clicks on URL embedded in email

5 Infiltrate company network with Trojans or other malware

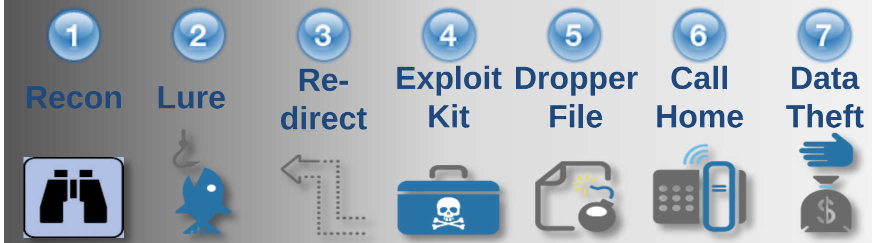
6 Confidential information transmitted to the attacker

© 2013 Websense, Inc.

Threats and Security Requirements

Changing Threat Landscape

- Advanced Threats
- Data Theft
- Attack and Malware Forensics



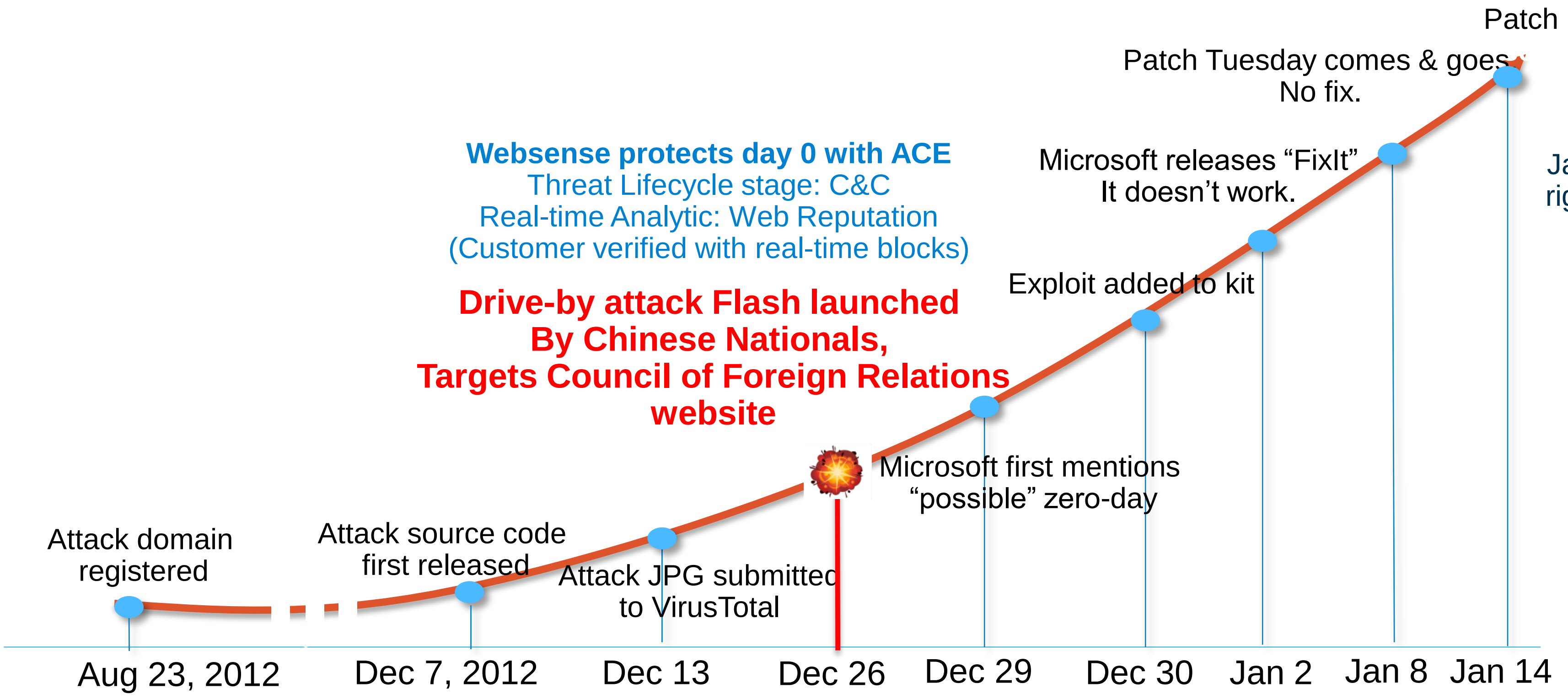
1. Recon
2. Lure
3. Re-direct
4. Exploit Kit
5. Dropper File
6. Call Home
7. Data Theft

New Security Requirements

- Protection from advanced threats
- Containment against data theft
- Threat dashboard / Severity alerting
- Forensic reporting / SIEM integration
- Malware analysis sandboxing & services
- Performance & availability of defenses

© 2013 Websense, Inc.

Catching the hard stuff



Java 0-day right on the heels

© 2013 Websense, Inc.

Websense Core Technologies

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

A Balanced View on Web Security

Inbound

- Advanced Malware Payload Detection
- Potentially Exploited Documents
- Mobile Malware
- SSL Traffic Inspection
- Cloud Sandboxing of Email Links
- Application Control

Outbound

- Criminal Encrypted Uploads
- Password File Theft Detection
- Dynamic Malware Command and Control
- Unauthorized Mobile Market Places
- OCR (Optical Character Recognition
- Drip (Stateful) DLP
- Geo-Location

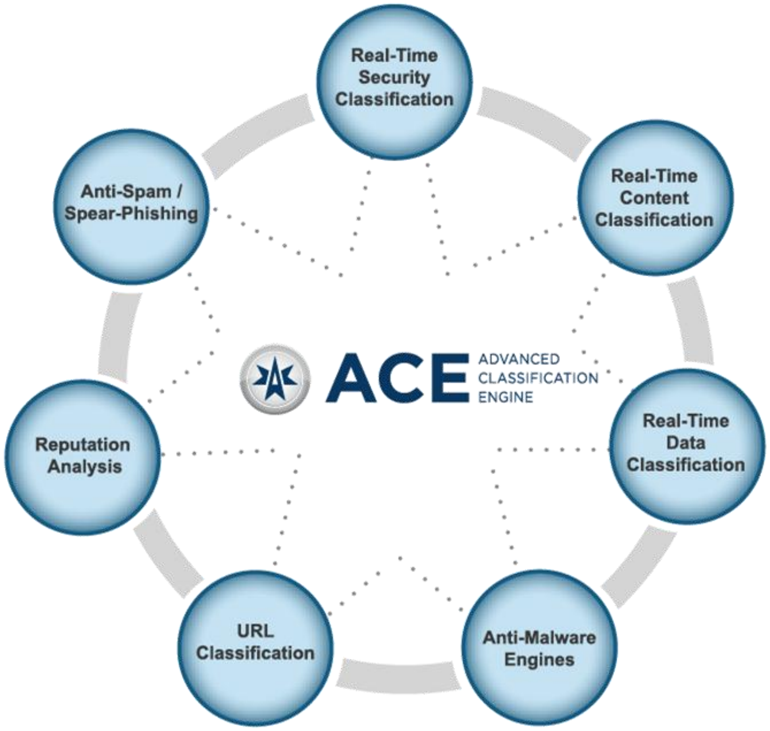
Analysis Tools

- Sandboxing Service
- Advanced Threat Dashboard
- Forensic Reporting

© 2013 Websense, Inc.

Real-time Threat & Content Analysis

Websense 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

- **Real-time Threat Engines**
  - Security, Data, Content
  - Over 10,000 Analytics
- **Three Anti-Malware Engines**
  - Commercial AV Engine
  - Heuristic Analysis Engine
  - Malicious PDF Engine
- **Spear-Phishing, Reputation and Web Link defenses**
- **Composite Scoring Model**

© 2013 Websense, Inc.

10 New ACE Defenses

INBOUND

- Advanced Malware Payloads ←
- Potentially Exploited Documents ←
- Mobile Malware ←

OUTBOUND

- Criminal Encrypted Uploads →
- Files Containing Passwords →
- Advanced Malware Command & Control →
- Unauthorized Mobile Marketplaces →
- OCR (Optical Character Recognition) →
- Drip (Stateful) DLP →
- Geo-Location →

© 2013 Websens

Full Life Cycle Threat Protection

Before

ThreatSeeker Intelligence Cloud
Global Threat Awareness
Facebook Partnership
Websense Security Labs

Finding threats ***before*** *our customers…*

During

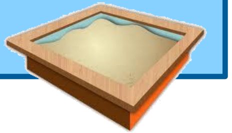
ACE
Real-time Defenses

Integrated DLP/DTD

Protecting ***during*** *the Point of Click…*

After

ThreatScope Malware Sandboxing
Web & Email Gateway Integration
Advanced Threat Dashboard
Forensic Reporting w/SIEM Export

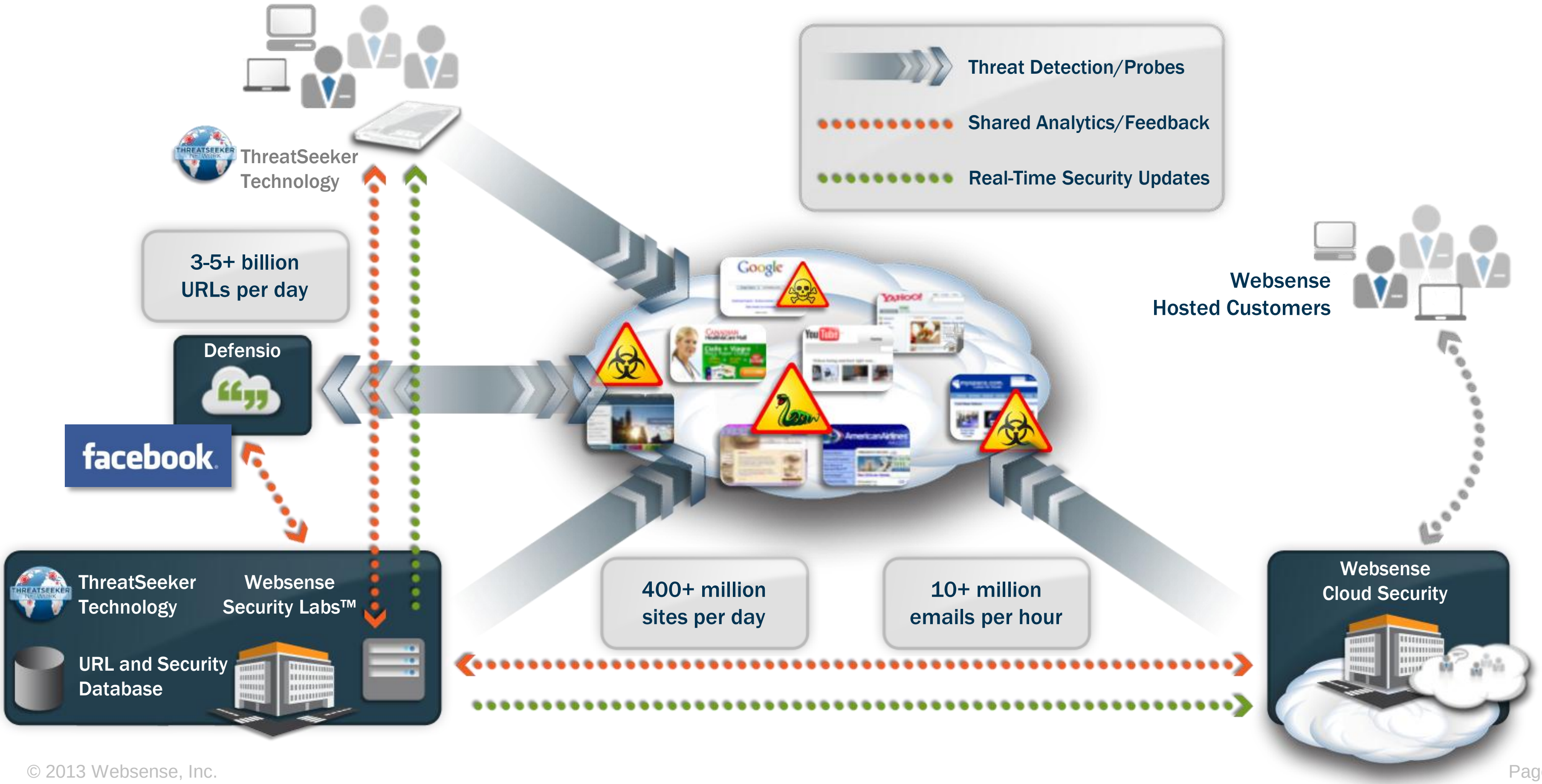


Malware sandboxing to uncover hidden threats ***after****, plus forensic reporting*

© 2013 Websense, Inc.

ThreatSeeker Intelligence Cloud

websense



ThreatSeeker Technology
Threat Detection/Probes
Shared Analytics/Feedback
Real-Time Security Updates
3-5+ billion URLs per day
Defensio
facebook
Websense Hosted Customers
400+ million sites per day
10+ million emails per hour
ThreatSeeker Technology
Websense Security Labs™
URL and Security Database
Websense Cloud Security

© 2013 Websense, Inc.

Web Security Solutions For a New World

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

TRITON Security Platform

websense

websense TRITON™

WEB

The **most effective** anti-malware protection from **advanced threats** and **data theft**.

EMAIL

The **most advanced** email defenses against **blended** and **targeted attacks**.

DATA

Enterprise DLP with **proven risk reduction in 5-6 weeks**. Features user & destination awareness.

CLOUD

The **best protection** for web & email for **any location** at the lowest TCO and easiest deployment.

MOBILE

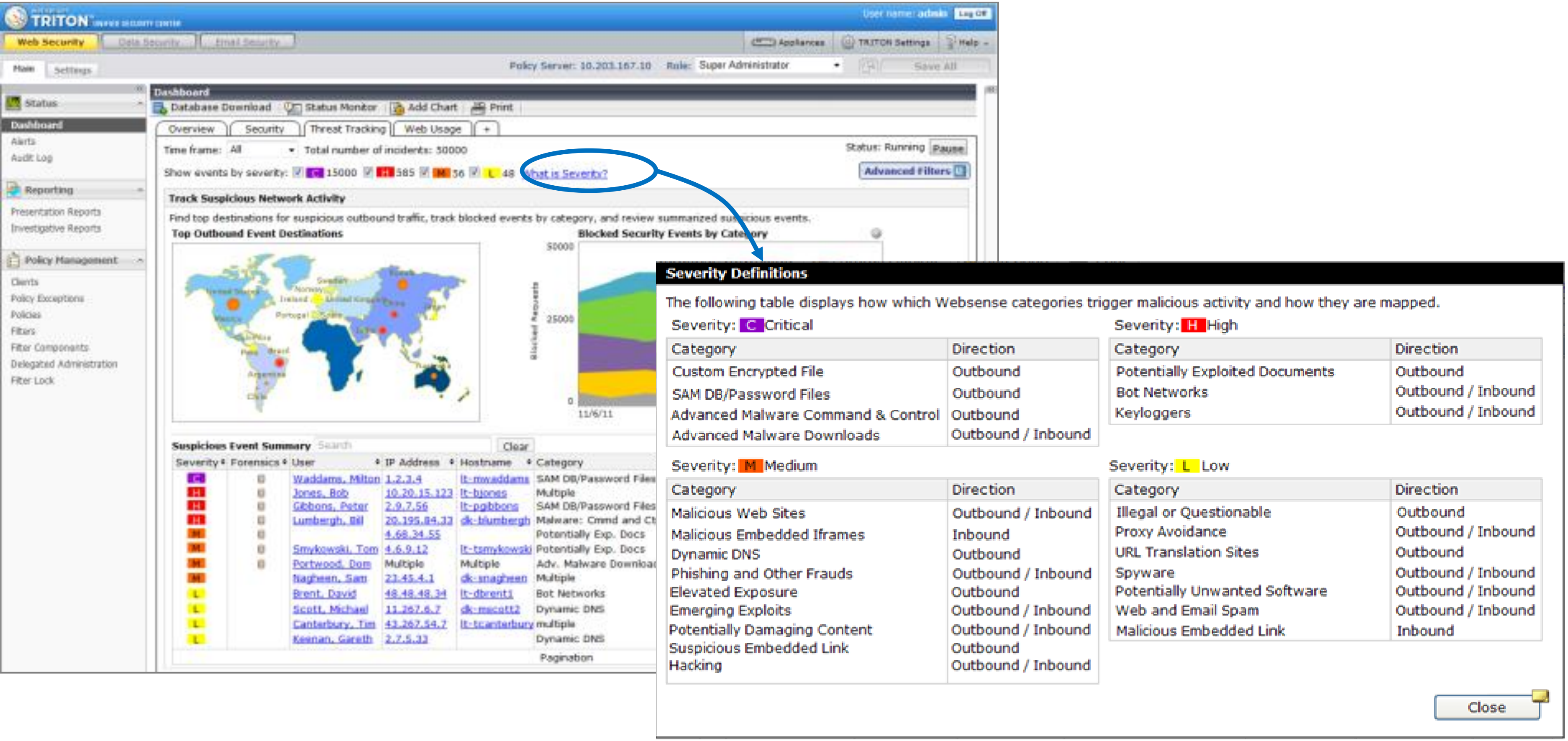
Uniquely effective protection for mobile data from **theft, loss, malicious apps** and **web threats**.

websense THREATSEEKER NETWORK

websense ACE

websense SECURITY LABS™

Threat Dashboard



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
C	▢	Waddams, Milton	1.2.3.4	lt-mwaddams	SAM DB/Password Files
H	▢	Jones, Bob	10.20.15.123	lt-bjones	Multiple
H	▢	Gibbons, Peter	2.9.7.56	lt-pgibbons	SAM DB/Password Files
H	▢	Lumbergh, Bill	20.195.84.33	dk-blumbergh	Malware: Cmmd and Ct
M	▢		4.68.34.55		Potentially Exp. Docs
M	▢	Smykowski, Tom	4.6.9.12	lt-tsmykowski	Potentially Exp. Docs
M	▢	Portwood, Dom	Multiple	Multiple	Adv. Malware Download
M		Nagheen, Sam	23.45.4.1	dk-snagheen	Multiple
L		Brent, David	48.48.48.34	lt-dbrent1	Bot Networks
L		Scott, Michael	11.267.6.7	dk-mscott2	Dynamic DNS
L		Canterbury, Tim	43.267.54.7	lt-tcanterbury	multiple
L		Keenan, Gareth	2.7.5.33		Dynamic DNS

Severity Definitions

The following table displays how which Websense categories trigger malicious activity and how they are mapped.

Severity: C Critical

Category	Direction
Custom Encrypted File	Outbound
SAM DB/Password Files	Outbound
Advanced Malware Command & Control	Outbound
Advanced Malware Downloads	Outbound / Inbound

Severity: H High

Category	Direction
Potentially Exploited Documents	Outbound
Bot Networks	Outbound / Inbound
Keyloggers	Outbound / Inbound

Severity: M Medium

Category	Direction
Malicious Web Sites	Outbound / Inbound
Malicious Embedded Iframes	Inbound
Dynamic DNS	Outbound
Phishing and Other Frauds	Outbound / Inbound
Elevated Exposure	Outbound
Emerging Exploits	Outbound / Inbound
Potentially Damaging Content	Outbound / Inbound
Suspicious Embedded Link	Outbound
Hacking	Outbound / Inbound

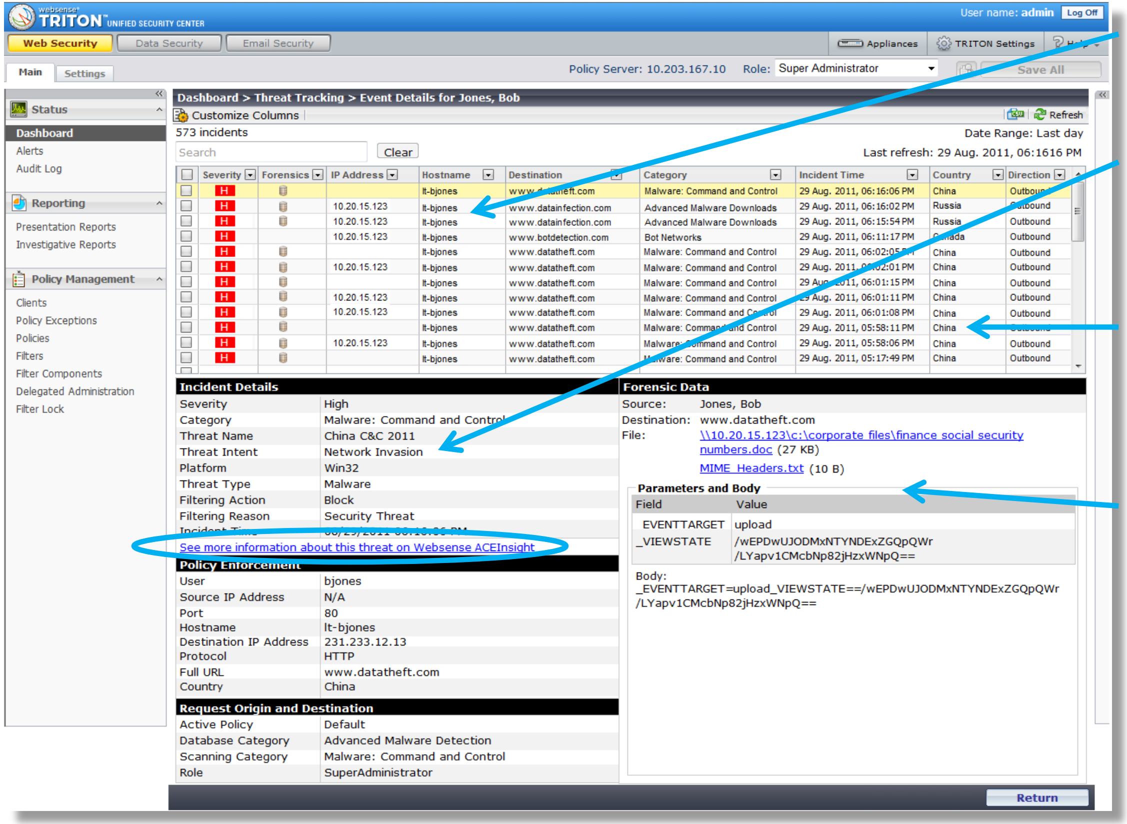
Severity: L Low

Category	Direction
Illegal or Questionable	Outbound
Proxy Avoidance	Outbound / Inbound
URL Translation Sites	Outbound
Spyware	Outbound / Inbound
Potentially Unwanted Software	Outbound / Inbound
Web and Email Spam	Outbound / Inbound
Malicious Embedded Link	Inbound

© 2013 Websense, Inc.

Forensic Reporting

websense®



Policy Server: 10.203.167.10 Role: Super Administrator

Dashboard > Threat Tracking > Event Details for Jones, Bob

573 incidents

Date Range: Last day

Last refresh: 29 Aug. 2011, 06:1616 PM

□	Severity	Forensics	IP Address	Hostname	Destination	Category	Incident Time	Country	Direction
□	H	●		lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:16:06 PM	China	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datainfection.com	Advanced Malware Downloads	29 Aug. 2011, 06:16:02 PM	Russia	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datainfection.com	Advanced Malware Downloads	29 Aug. 2011, 06:15:54 PM	Russia	Outbound
□	H		10.20.15.123	lt-bjones	www.botdetection.com	Bot Networks	29 Aug. 2011, 06:11:17 PM	Canada	Outbound
□	H	●		lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:02:05 PM	China	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:02:01 PM	China	Outbound
□	H	●		lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:01:15 PM	China	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:01:11 PM	China	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 06:01:08 PM	China	Outbound
□	H	●		lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 05:58:11 PM	China	Outbound
□	H	●	10.20.15.123	lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 05:58:06 PM	China	Outbound
□	H	●		lt-bjones	www.datatheft.com	Malware: Command and Control	29 Aug. 2011, 05:17:49 PM	China	Outbound

Incident Details

Severity	High
Category	Malware: Command and Control
Threat Name	China C&C 2011
Threat Intent	Network Invasion
Platform	Win32
Threat Type	Malware
Filtering Action	Block
Filtering Reason	Security Threat
Incident Time	08/29/2011 06:16:06 PM

See more information about this threat on Websense ACEInsight

Policy Enforcement

User	bjones
Source IP Address	N/A
Port	80
Hostname	lt-bjones
Destination IP Address	231.233.12.13
Protocol	HTTP
Full URL	www.datatheft.com
Country	China

Request Origin and Destination

Active Policy	Default
Database Category	Advanced Malware Detection
Scanning Category	Malware: Command and Control
Role	SuperAdministrator

Forensic Data

Source: Jones, Bob
Destination: www.datatheft.com
File: \\10.20.15.123\c:\corporate files\finance social security numbers.doc (27 KB)
MIME_Headers.txt (10 B)

Parameters and Body

Field	Value
EVENTTARGET	upload
_VIEWSTATE	/wEPDwUJODMxNTYNDExZGQpQWr /LYapv1CMcbNp82jHzxWNpQ==

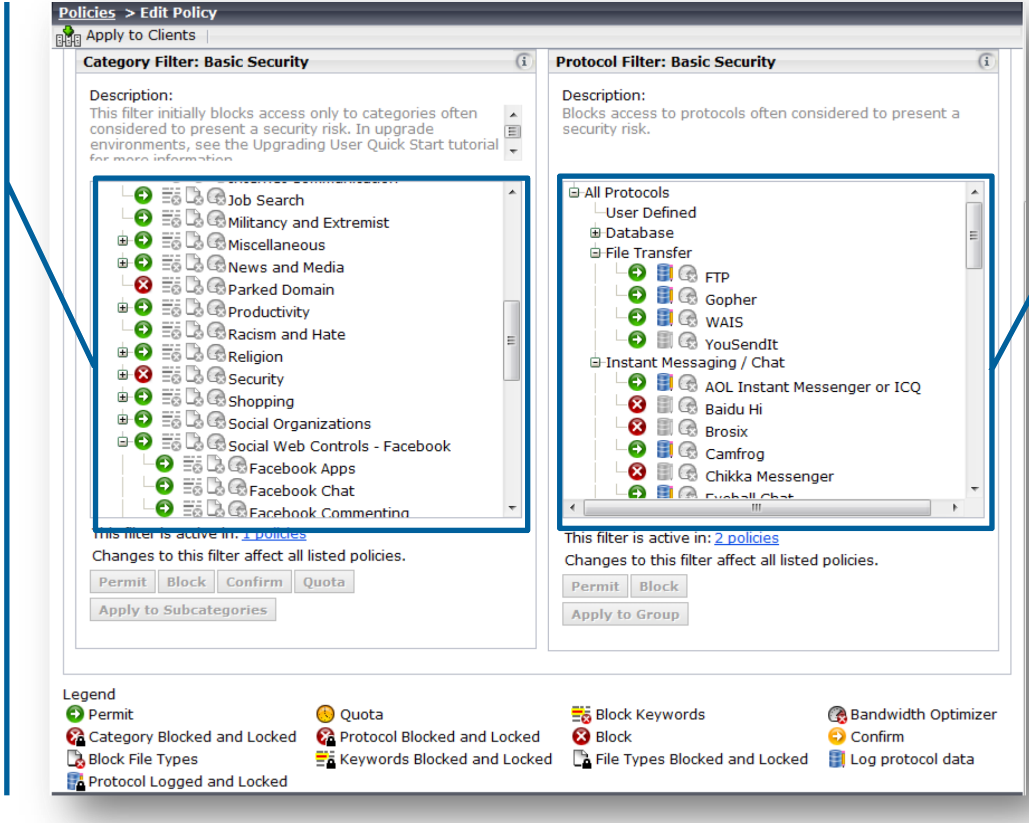
Body:
_EVENTTARGET=upload_VIEWSTATE==/wEPDwUJODMxNTYNDExZGQpQWr
/LYapv1CMcbNp82jHzxWNpQ==

- Know **WHO** was compromised
- Know **HOW** the malware operates (intent)
- Know **WHERE** the data was being sent
- Know **WHAT** was prevented from being stolen

© 2013 Websense, Inc.

Granular Category and App Control

- 120 Security and URL Categories
- Granular Social Media Control
- Simple Click and Set policy creation



Policies > Edit Policy

Apply to Clients

Category Filter: Basic Security

Description:
This filter initially blocks access only to categories often considered to present a security risk. In upgrade environments, see the Upgrading User Quick Start tutorial for more information.

- Job Search
- Militancy and Extremist
- Miscellaneous
- News and Media
- Parked Domain
- Productivity
- Racism and Hate
- Religion
- Security
- Shopping
- Social Organizations
- Social Web Controls - Facebook
  - Facebook Apps
  - Facebook Chat
  - Facebook Commenting

This filter is active in: 1 policies

Changes to this filter affect all listed policies.

Permit | Block | Confirm | Quota

Apply to Subcategories

Protocol Filter: Basic Security

Description:
Blocks access to protocols often considered to present a security risk.

- All Protocols
  - User Defined
  - Database
  - File Transfer
    - FTP
    - Gopher
    - WAIS
    - YouSendIt
  - Instant Messaging / Chat
    - AOL Instant Messenger or ICQ
    - Baidu Hi
    - Brosix
    - Camfrog
    - Chikka Messenger
    - Eyeball Chat

This filter is active in: 2 policies

Changes to this filter affect all listed policies.

Permit | Block

Apply to Group

Legend

Permit	Quota	Block Keywords	Bandwidth Optimizer
Category Blocked and Locked	Protocol Blocked and Locked	Block	Confirm
Block File Types	Keywords Blocked and Locked	File Types Blocked and Locked	Log protocol data
Protocol Logged and Locked			

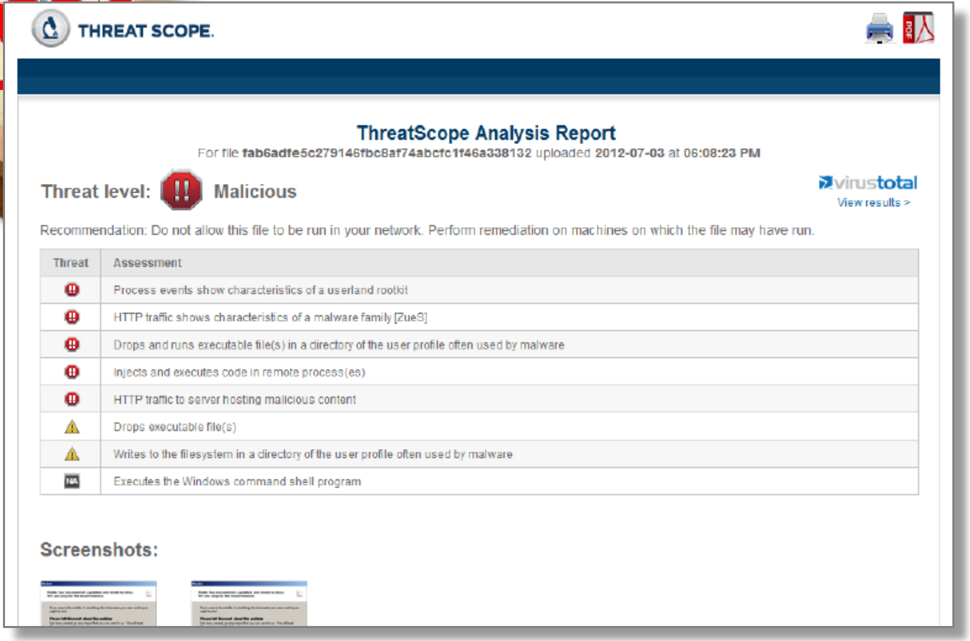
- Hundreds of Application Controls
- Includes Video Controls
- SSL Traffic Inspection

© 2013 Websense, Inc.

Forensic Analysis with Actionable Results

Websense ThreatScope

- Analyze URL and Files in a safe environment.
- Study and see how files and URLs behave.
- Get a rating for each tested URL/file.
- Plan response or action based on ThreatScope results.



ThreatScope Analysis Report

For file **fab6adfe5c279146fbc8af74abcfc1f46a338132** uploaded **2012-07-03** at **06:08:23 PM**

Threat level: ‼ **Malicious**

virustotal
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.

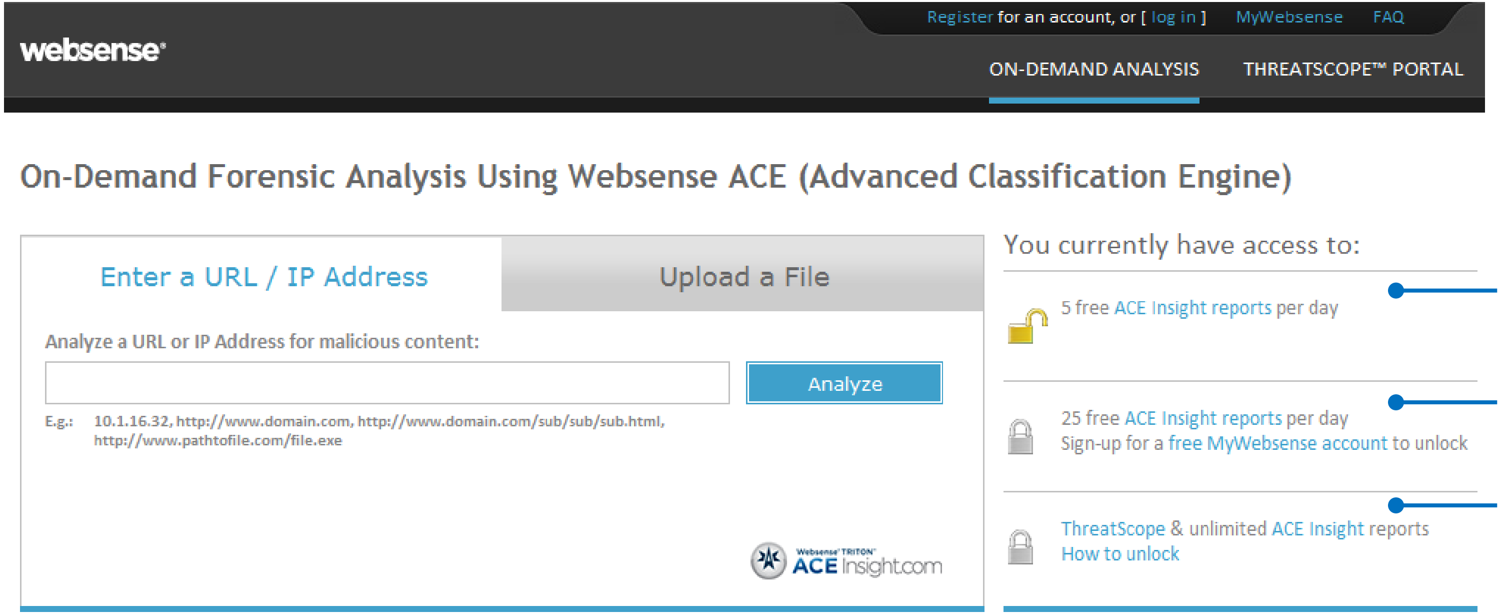
Threat	Assessment
‼	Process events show characteristics of a userland rootkit
‼	HTTP traffic shows characteristics of a malware family [ZueS]
‼	Drops and runs executable file(s) in a directory of the user profile often used by malware
‼	Injects and executes code in remote process(es)
‼	HTTP traffic to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

Screenshots:

© 2013 Websense, Inc.

Online Analysis Tools

websense



websense

Register for an account, or [log in]   MyWebsense   FAQ

ON-DEMAND ANALYSIS   THREATSCOPE™ PORTAL

On-Demand Forensic Analysis Using Websense ACE (Advanced Classification Engine)

Enter a URL / IP Address | Upload a File

Analyze a URL or IP Address for malicious content:

Analyze

E.g.: 10.1.16.32, http://www.domain.com, http://www.domain.com/sub/sub/sub.html, http://www.pathtofile.com/file.exe

Websense TRITON ACE Insight.com

You currently have access to:

5 free ACE Insight reports per day

25 free ACE Insight reports per day
Sign-up for a free MyWebsense account to unlock

ThreatScope & unlimited ACE Insight reports
How to unlock

Public Use

Account Use

Customer Use
URLs & Files
Unlimited Use
Cloud Service

websense® CSI SERVICES

csi.websense.com

© 2013 Websense, Inc.

Let Us Prove It!

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

QUESTIONS

Thank You

TRITON STOPS MORE THREATS. WE CAN PROVE IT.