websense®

CyberSecurity Intelligence™ Services

CSI: On-Demand & CSI: Live

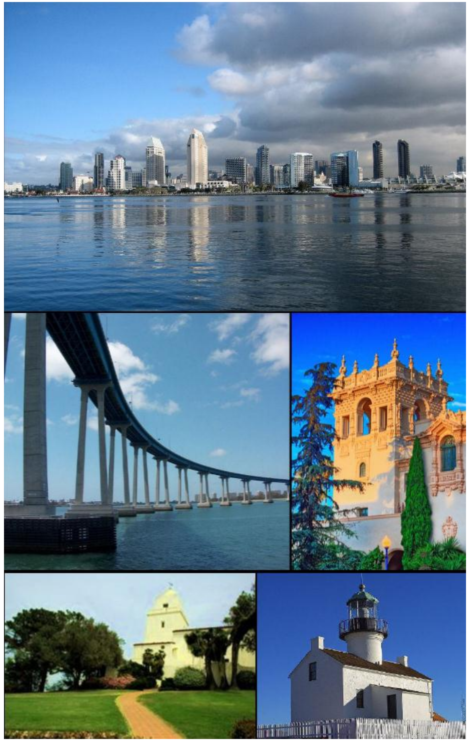
TRITON™

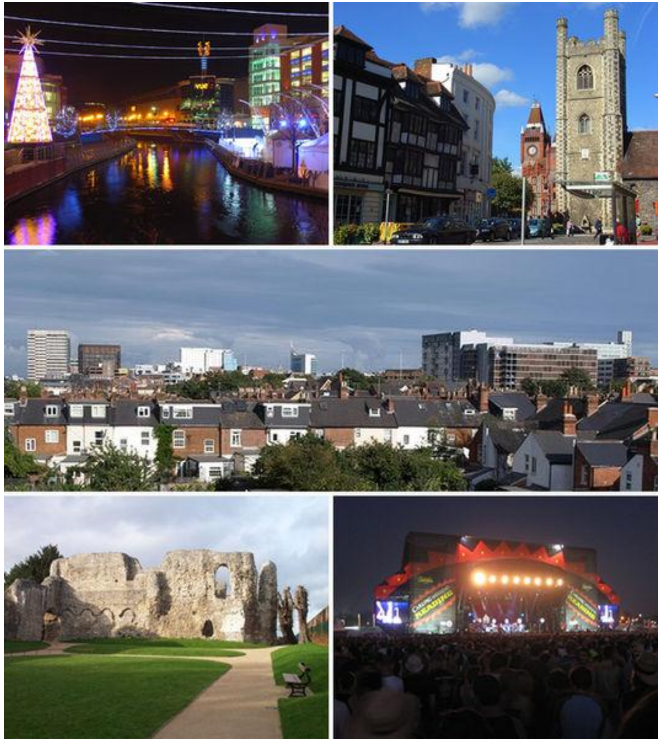
- Web security
- Email security
- Data security
- Mobile security

websense® CSI SERVICES

© 2012 Websense, Inc.

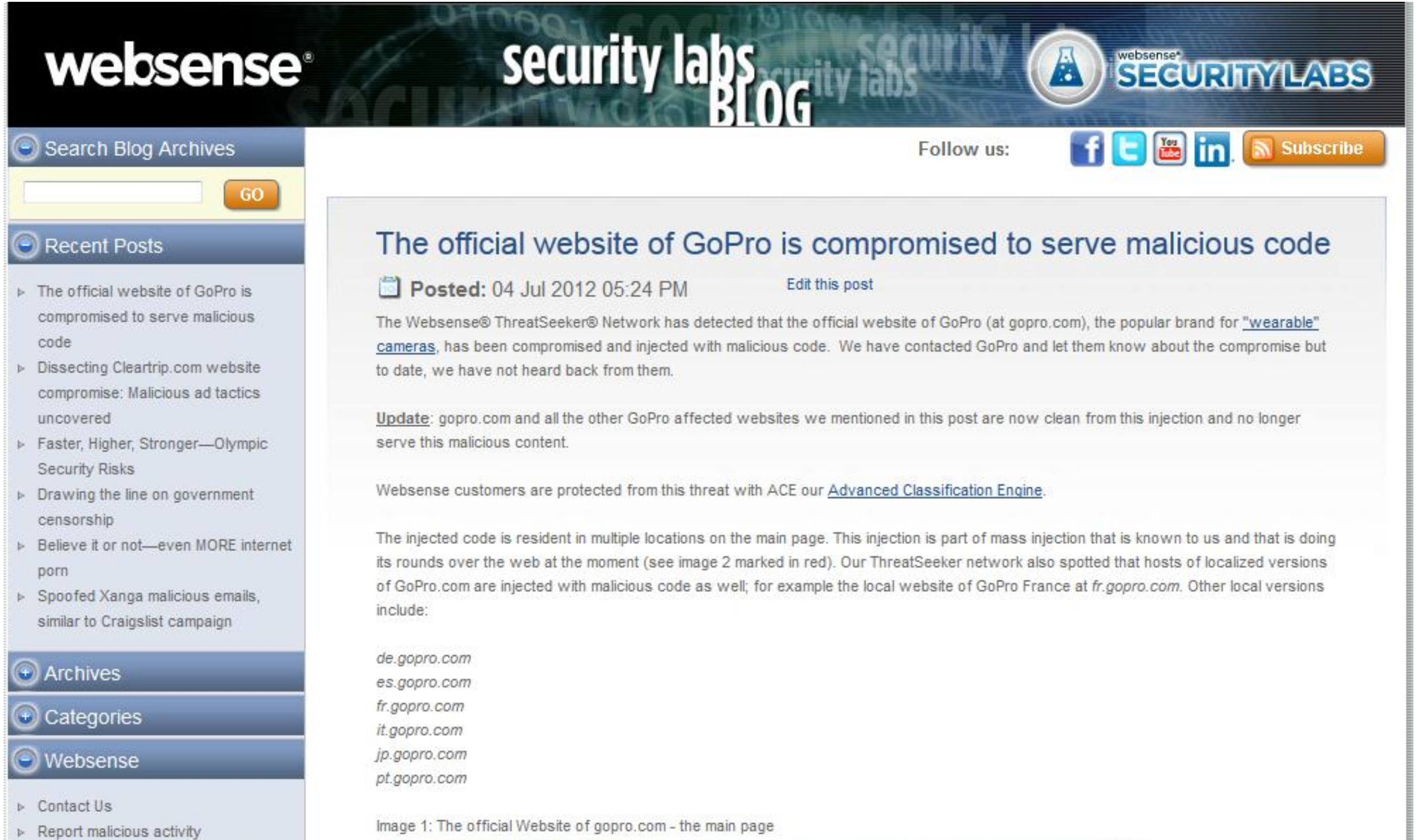
Websense Security Labs





© 2012 Websense, Inc.

WSL: Discover, protect & alert important threats


websense
security labs BLOG
websense SECURITY LABS
Search Blog Archives
GO
Recent Posts
The official website of GoPro is compromised to serve malicious code
Dissecting Cleartrip.com website compromise: Malicious ad tactics uncovered
Faster, Higher, Stronger—Olympic Security Risks
Drawing the line on government censorship
Believe it or not—even MORE internet porn
Spoofed Xanga malicious emails, similar to Craigslist campaign
Archives
Categories
Websense
Contact Us
Report malicious activity
Follow us:
Subscribe
Edit this post

The official website of GoPro is compromised to serve malicious code

Posted: 04 Jul 2012 05:24 PM

The Websense® ThreatSeeker® Network has detected that the official website of GoPro (at gopro.com), the popular brand for "wearable" cameras, has been compromised and injected with malicious code. We have contacted GoPro and let them know about the compromise but to date, we have not heard back from them.

Update: gopro.com and all the other GoPro affected websites we mentioned in this post are now clean from this injection and no longer serve this malicious content.

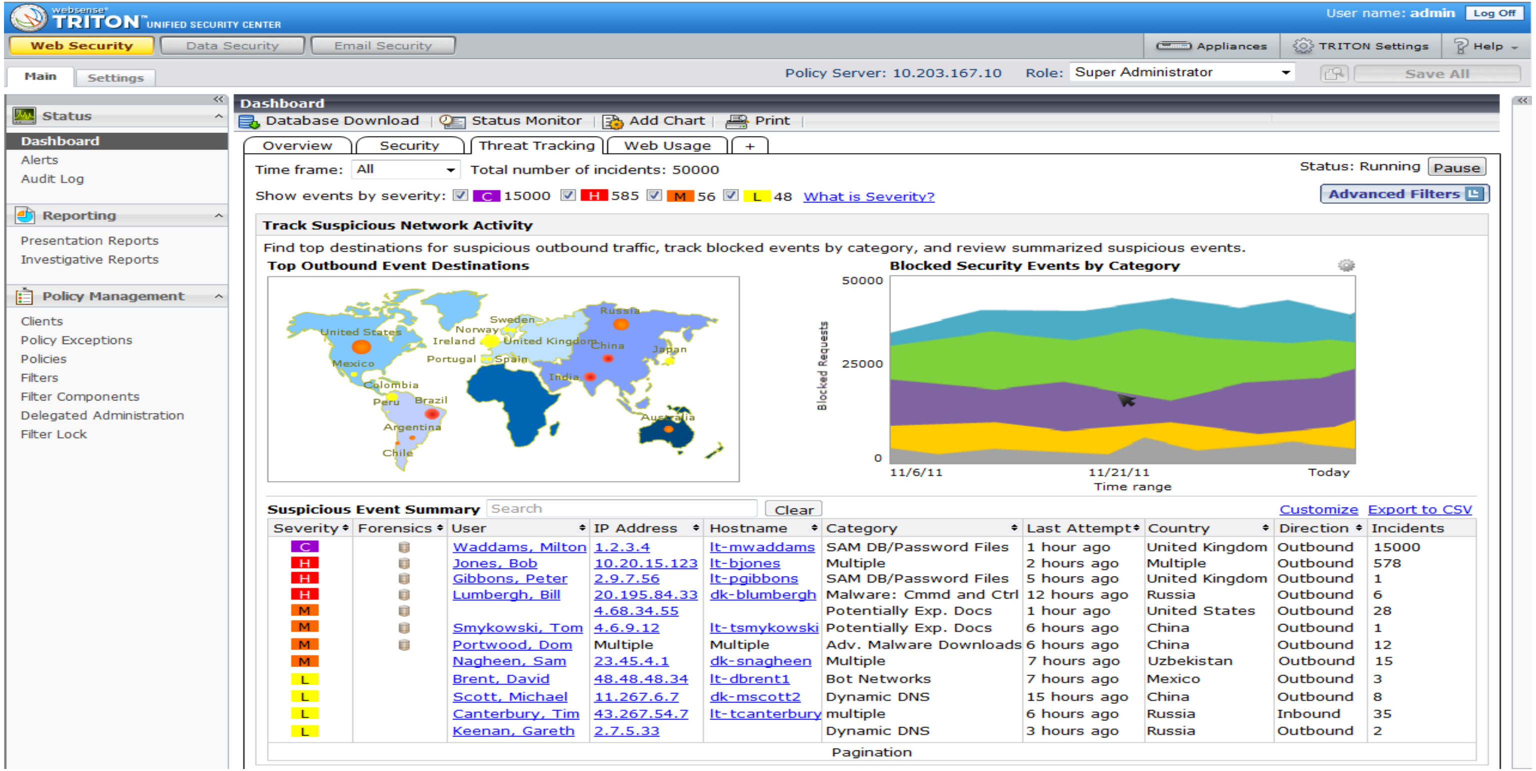
Websense customers are protected from this threat with ACE our Advanced Classification Engine.

The injected code is resident in multiple locations on the main page. This injection is part of mass injection that is known to us and that is doing its rounds over the web at the moment (see image 2 marked in red). Our ThreatSeeker network also spotted that hosts of localized versions of GoPro.com are injected with malicious code as well; for example the local website of GoPro France at *fr.gopro.com*. Other local versions include:

de.gopro.com
es.gopro.com
fr.gopro.com
it.gopro.com
jp.gopro.com
pt.gopro.com

Image 1: The official Website of gopro.com - the main page

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

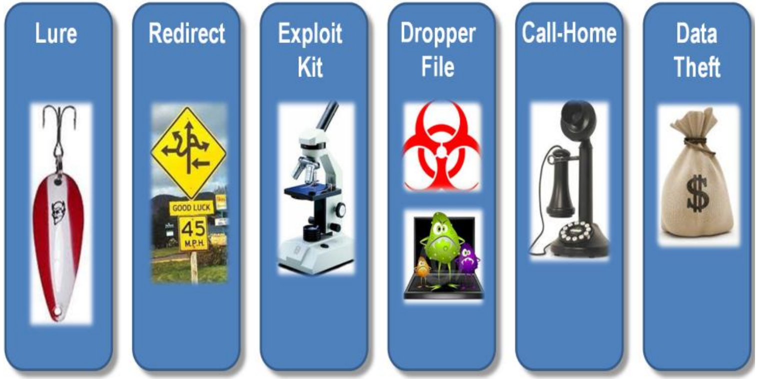
Blocked Security Events by Category

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.

WSL: Provide Insight



Lure

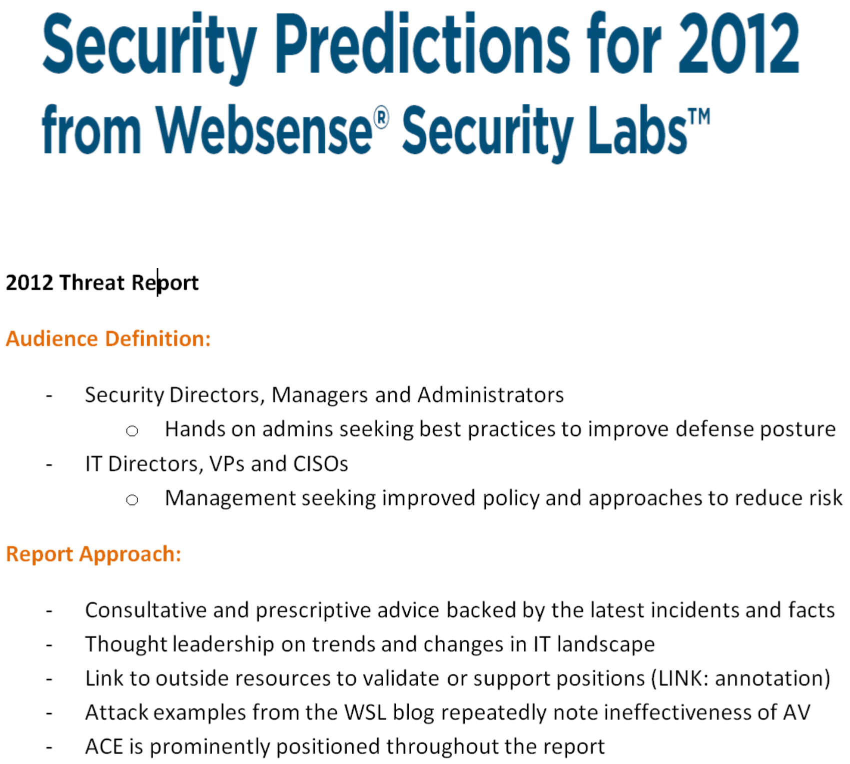
Redirect

Exploit Kit

Dropper File

Call-Home

Data Theft



Security Predictions for 2012 from Websense® Security Labs™

2012 Threat Report

Audience Definition:

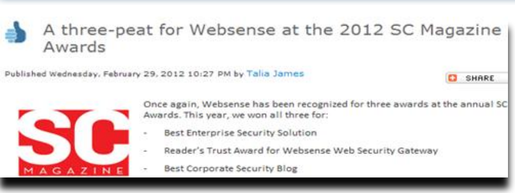
- Security Directors, Managers and Administrators
  - Hands on admins seeking best practices to improve defense posture
- IT Directors, VPs and CISOs
  - Management seeking improved policy and approaches to reduce risk

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

WSL: Summary

websense®



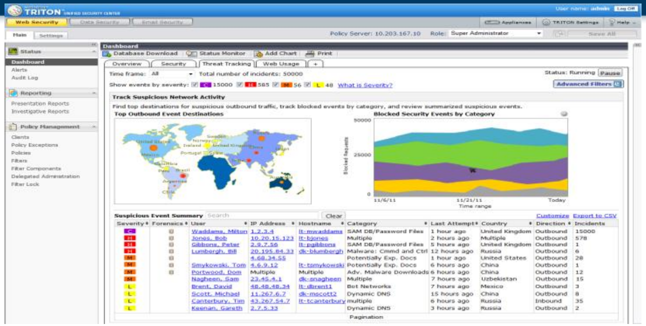
A three-peat for Websense at the 2012 SC Magazine Awards

Published Wednesday, February 29, 2012 10:27 PM by Talia James

SHARE

Once again, Websense has been recognized for three awards at the annual SC Awards. This year, we won all three for:

- Best Enterprise Security Solution
- Reader's Trust Award for Websense Web Security Gateway
- Best Corporate Security Blog



Policy Server: 10.203.167.10 Role: Super Administrator

Dashboard

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 Search

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

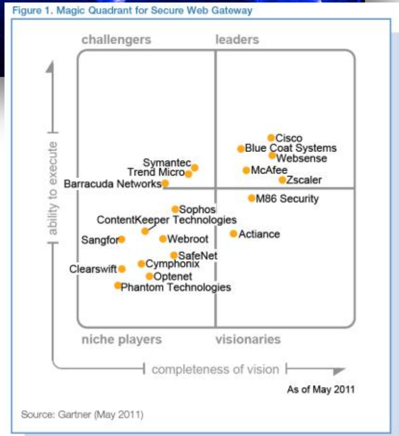
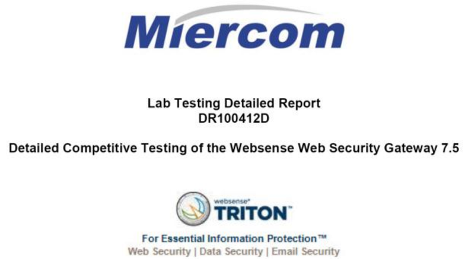


Figure 1. Magic Quadrant for Secure Web Gateway

As of May 2011

Source: Gartner (May 2011)



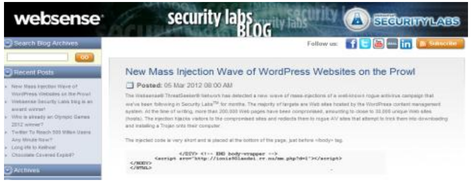
Miercom

Lab Testing Detailed Report
DR100412D

Detailed Competitive Testing of the Websense Web Security Gateway 7.5

websense® TRITON™

For Essential Information Protection™
Web Security | Data Security | Email Security



- 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?

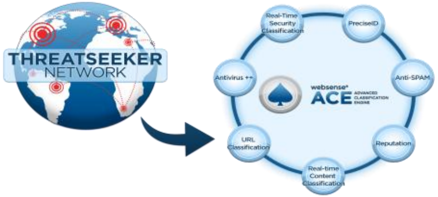
New Mass Injection Wave of WordPress Websites on the Prowl

Posted: 05 Mar 2012 08:00 AM

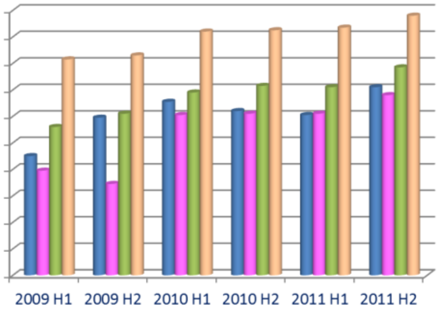
The Websense® ThreatSeeker® Network has detected a new wave of mass-injections of a well-known rogue antivirus campaign that we've been following in Security Labs™ for months. The majority of targets are Web sites hosted by the WordPress content management system. At the time of writing, more than 200,000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

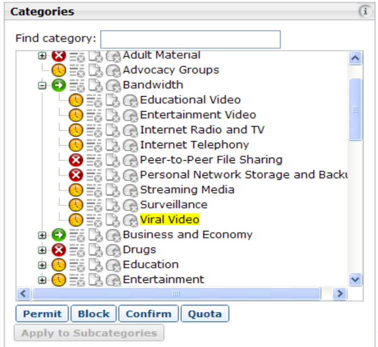
The injected code is very short and is placed at the bottom of the page, just before <body> tag.

```
                </DIV> <!-- END body-wrapper -->
            <script src="http://[illegible]"></script>
</BODY>
</HTML>
```



THREATSEEKER NETWORK
Real-Time Security Classification
PreciseID
Anti-SPAM
Reputation
Real-time Content Classification
URL Classification
Antivirus ++
websense® ACE ADVANCED CLASSIFICATION ENGINE





Categories

Find category:

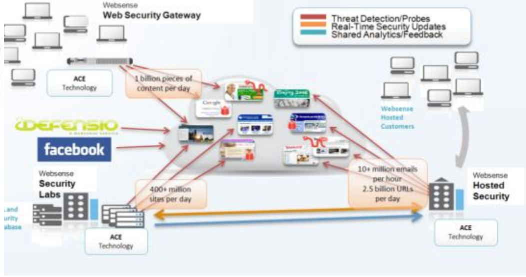
- ⊞ ☒ Adult Material
- ⏱ Advocacy Groups
- ⊟ ✓ Bandwidth
  - ⏱ Educational Video
  - ⏱ Entertainment Video
  - ⏱ Internet Radio and TV
  - ⏱ Internet Telephony
  - ☒ Peer-to-Peer File Sharing
  - ☒ Personal Network Storage and Backu
  - ⏱ Streaming Media
  - ⏱ Surveillance
  - ⏱ Viral Video
- ⊞ ✓ Business and Economy
- ⊞ ☒ Drugs
- ⊞ ⏱ Education
- ⊞ ⏱ Entertainment

Document # 208326

The Web Security Challenge:
A Competitive Guide to Selecting Secure Web Gateways

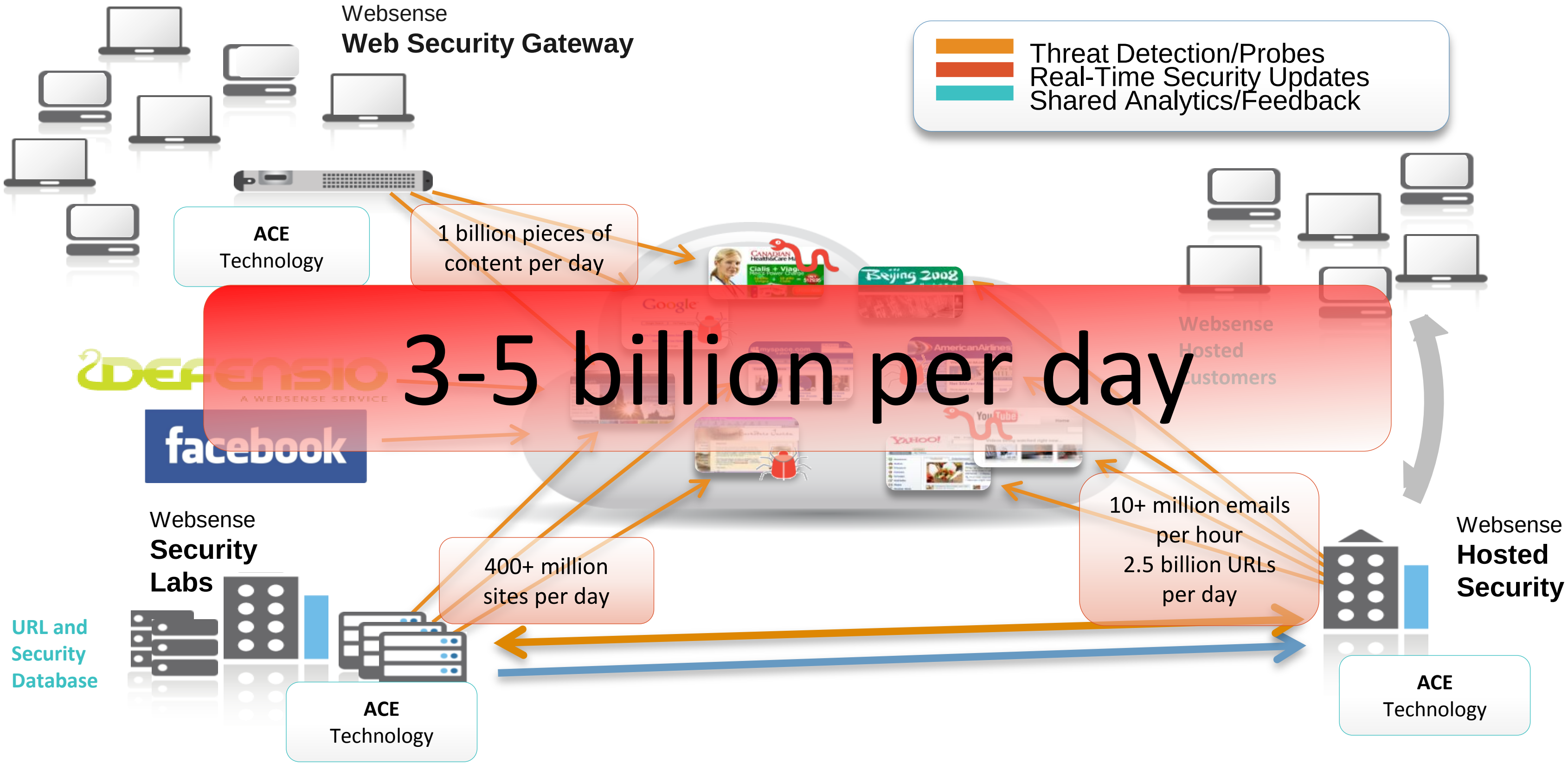
A white paper commissioned by Websense, Inc.

TOLLY GROUP
White Paper
December 2009



Big Data = Big Opportunity

websense



Websense **Web Security Gateway**

ACE Technology

1 billion pieces of content per day

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

Websense Hosted Customers

3-5 billion per day

Websense **Security Labs**

URL and Security Database

400+ million sites per day

ACE Technology

10+ million emails per hour
2.5 billion URLs per day

Websense **Hosted Security**

ACE Technology

© 2012 Websense, Inc.

A Lesson From History – The Tower of London

Announcing Security Intelligence Services

TRITON™

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

© 2012 Websense, Inc.

Security Intelligence Services

"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.

© 2012 Websense, Inc.

Websense® CyberSecurity Intelligence™ Services

- Enhance incident response capabilities
- Optimize your security posture
  - **Defenses** – Ensure optimal configuration and application of existing defenses
  - **Personnel** – Build and maintain professional in-house security expertise
  - **Practices** – Apply custom use cases and other resources to upgrade best practices

- Powered by researchers from

websense® SECURITY LABS

© 2012 Websense, Inc.

CSI: On-Demand

TRITON™

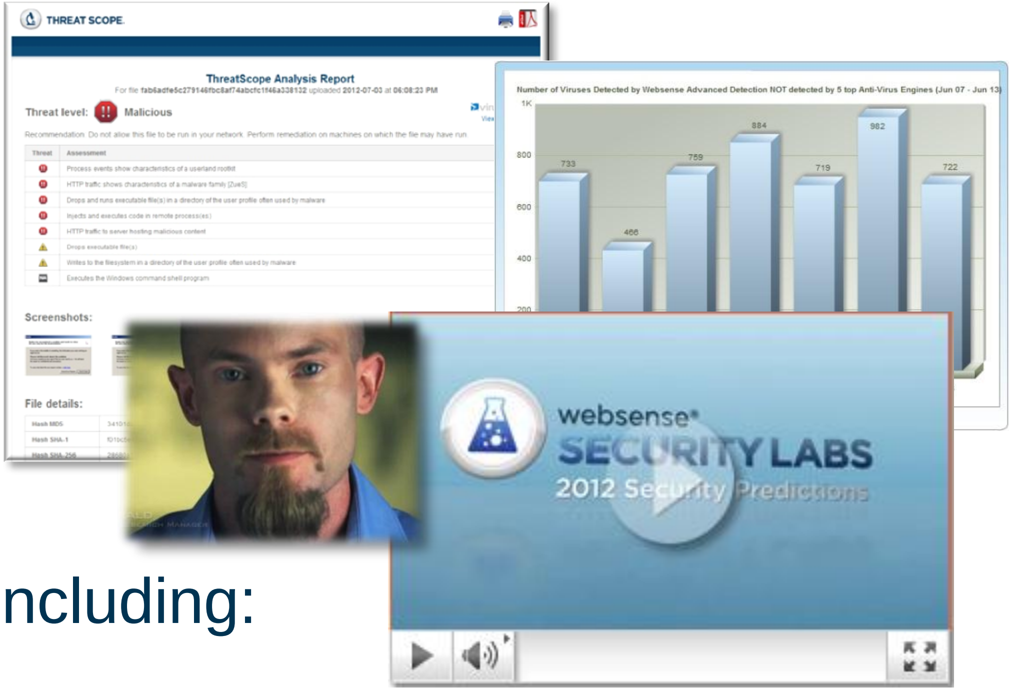
- Web security
- Email security
- Data security
- Mobile security

websense® CSI SERVICES

© 2012 Websense, Inc.

CSI: On-Demand

- ThreatScope malware analysis 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



THREAT SCOPE

ThreatScope Analysis Report

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

Threat level: Malicious

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

Screenshots:

File details:

Hash MD5

Hash SHA-1

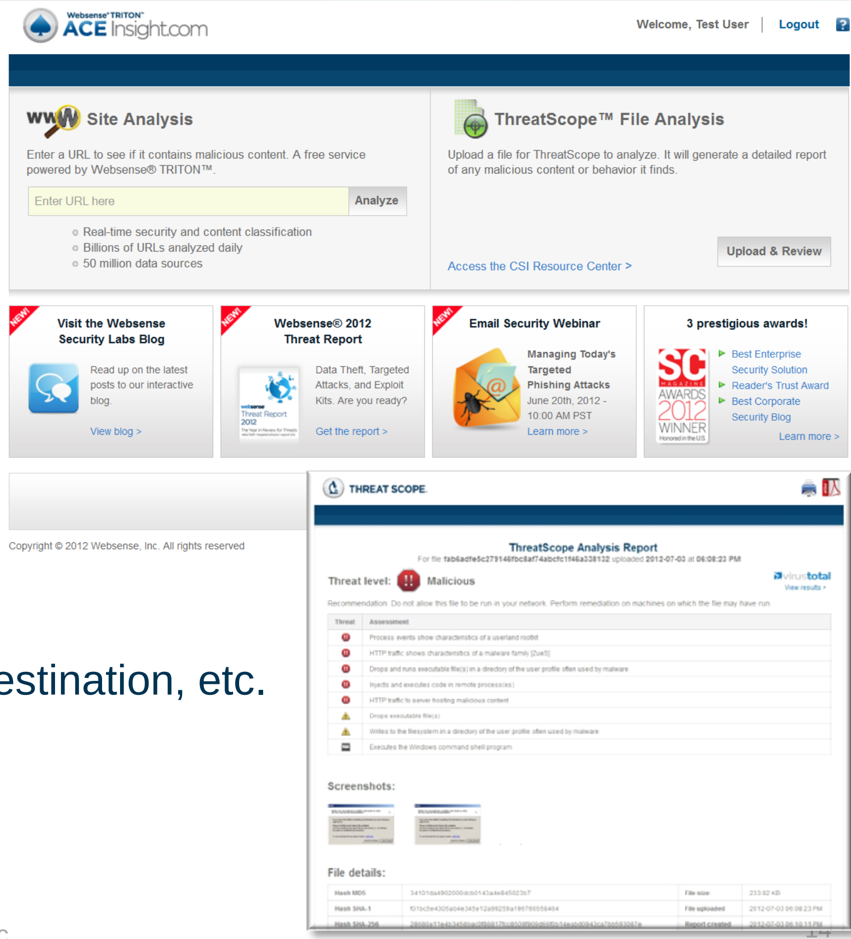
Hash SHA-256

Number of Viruses Detected by Websense Advanced Detection NOT detected by 5 top Anti-Virus Engines (Jun 07 - Jun 13)

websense CSI SERVICES

Websense ThreatScope™

- Applies key ACE analytics
- Monitor infection lifecycle
  - Infection process
  - post-infection activity
- Track infected system activity
  - System level events/behavior/changes
  - Changes to processes, registry, files, etc.
- Communication monitoring
  - Network communications
  - Includes connections used, methods used, destination, etc.
- Complete, easily understood report
  - activity observed, malware profile, etc.



Websense® TRITON™ ACE Insight.com

Welcome, Test User | Logout

Site Analysis

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

Enter URL here | Analyze

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

ThreatScope™ File Analysis

Upload a file for ThreatScope to analyze. It will generate a detailed report of any malicious content or behavior it finds.

Access the CSI Resource Center >

Upload & Review

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! **Email Security Webinar**

Managing Today's Targeted Phishing Attacks
June 20th, 2012 - 10:00 AM PST

Learn more >

3 prestigious awards!

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

Learn more >

Copyright © 2012 Websense, Inc. All rights reserved

THREAT SCOPE

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.

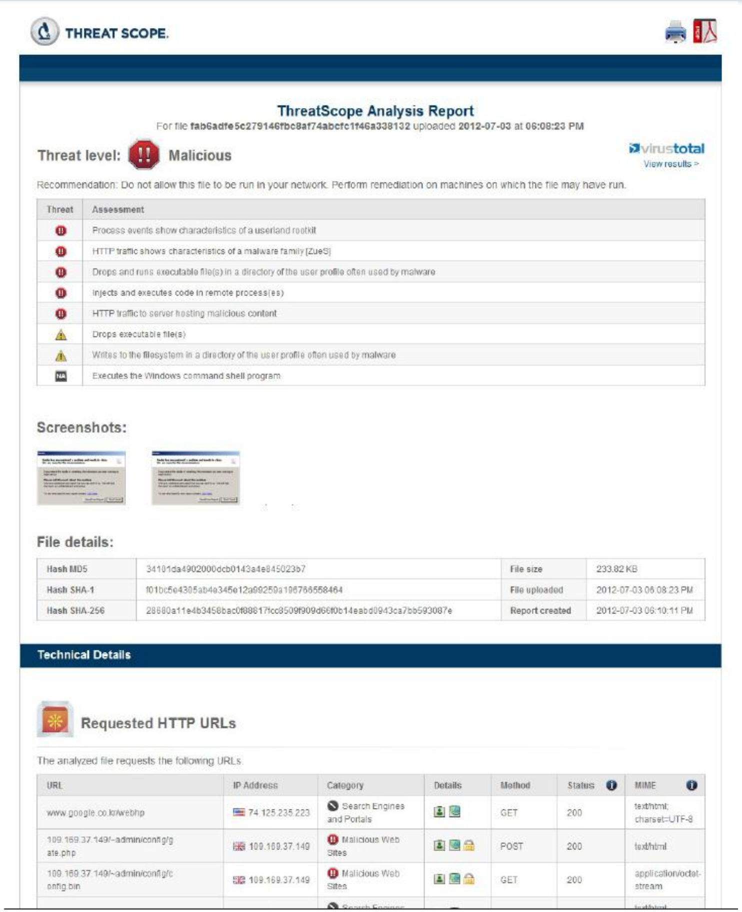
Threat	Assessment
●	Process events show characteristics of a userland rootkit
●	HTTP traffic shows characteristics of a malware family [ZueS]
●	Drops and runs executable file(s) in a directory of the user profile often used by malware
●	Injects and executes code in remote process(es)
●	HTTP traffic to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

Screenshots:

File details:

Hash MD5	34101da4902000dcb0143a4e845023b7	File size	233.82 KB
Hash SHA-1	f01bc5e4305a04e345e12a99259a196766558464	File uploaded	2012-07-03 06:08:23 PM
Hash SHA-256	28680a11e4b3458ba0f88817fcc8509f909d66f0b14eabd0943ca7b0593087e	Report created	2012-07-03 06:10:11 PM

Websense ThreatScope™ Sample Report



THREAT SCOPE.

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
N/A	Executes the Windows command shell program

Screenshots:

File details:

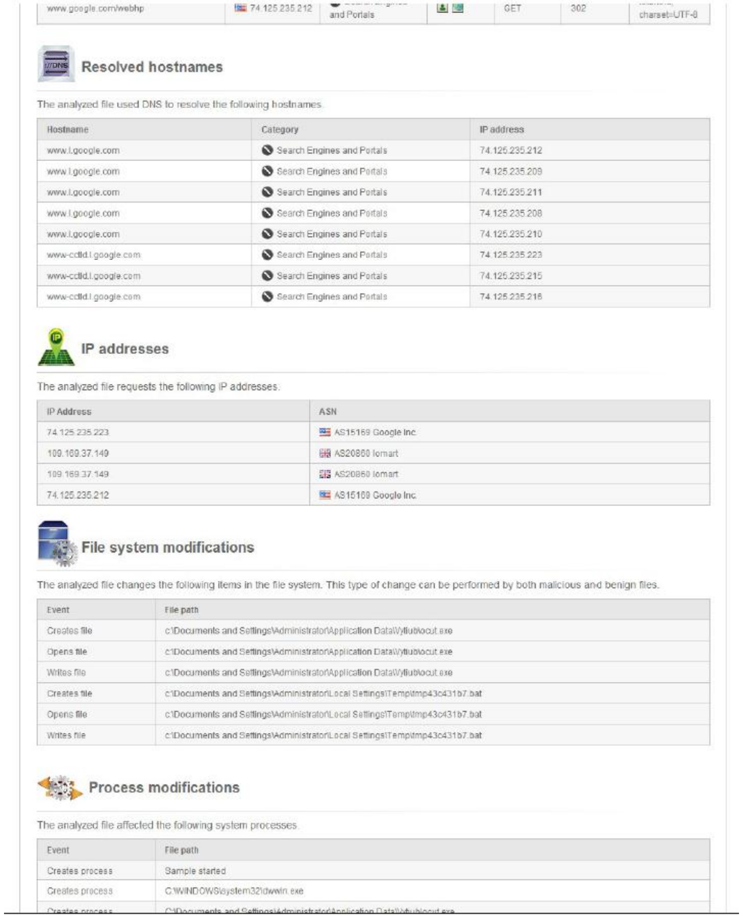
Hash MD5	34101da4902000dcb0143a4e845023b7	File size	233.82 KB
Hash SHA-1	f01bc5e4305ab4e345e12a99259a196766558464	File uploaded	2012-07-03 06:08:23 PM
Hash SHA-256	28680a11e4b3458bac0f88817fcc8509f909d66f0b14eabd0943ca7bb593087e	Report created	2012-07-03 06:10:11 PM

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	74.125.235.223	Search Engines and Portals		GET	200	text/html; charset=UTF-8
109.169.37.149/~admin/config/gate.php	109.169.37.149	‼ Malicious Web Sites		POST	200	text/html
109.169.37.149/~admin/config/config.bin	109.169.37.149	‼ Malicious Web Sites		GET	200	application/octet-stream
www.google.com/webhp	74.125.235.212	Search Engines and Portals		GET	302	text/html; 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-cctld.l.google.com	Search Engines and Portals	74.125.235.223
www-cctld.l.google.com	Search Engines and Portals	74.125.235.215
www-cctld.l.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	AS20860 Iomart
109.169.37.149	AS20860 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.

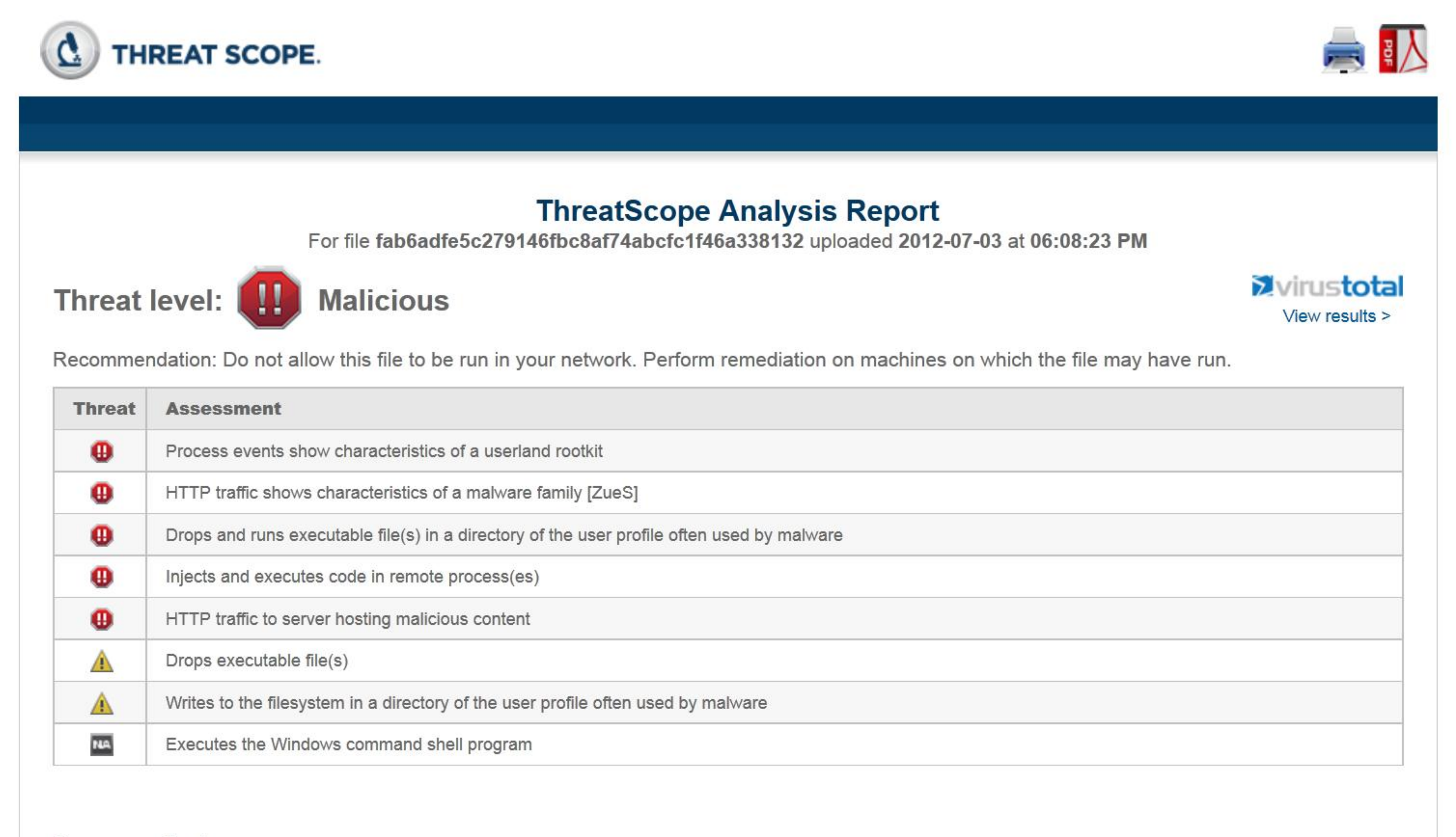
Event	File path
Creates file	c:\Documents and Settings\Administrator\Application Data\Vytlub\ocut.exe
Opens file	c:\Documents and Settings\Administrator\Application Data\Vytlub\ocut.exe
Writes file	c:\Documents and Settings\Administrator\Application Data\Vytlub\ocut.exe
Creates file	c:\Documents and Settings\Administrator\Local Settings\Temp\tmp43c431b7.bat
Opens file	c:\Documents and Settings\Administrator\Local Settings\Temp\tmp43c431b7.bat
Writes file	c:\Documents and Settings\Administrator\Local Settings\Temp\tmp43c431b7.bat

Process modifications

The analyzed file affected the following system processes.

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

© 2012 Websense, Inc.



THREAT SCOPE.

ThreatScope Analysis Report

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

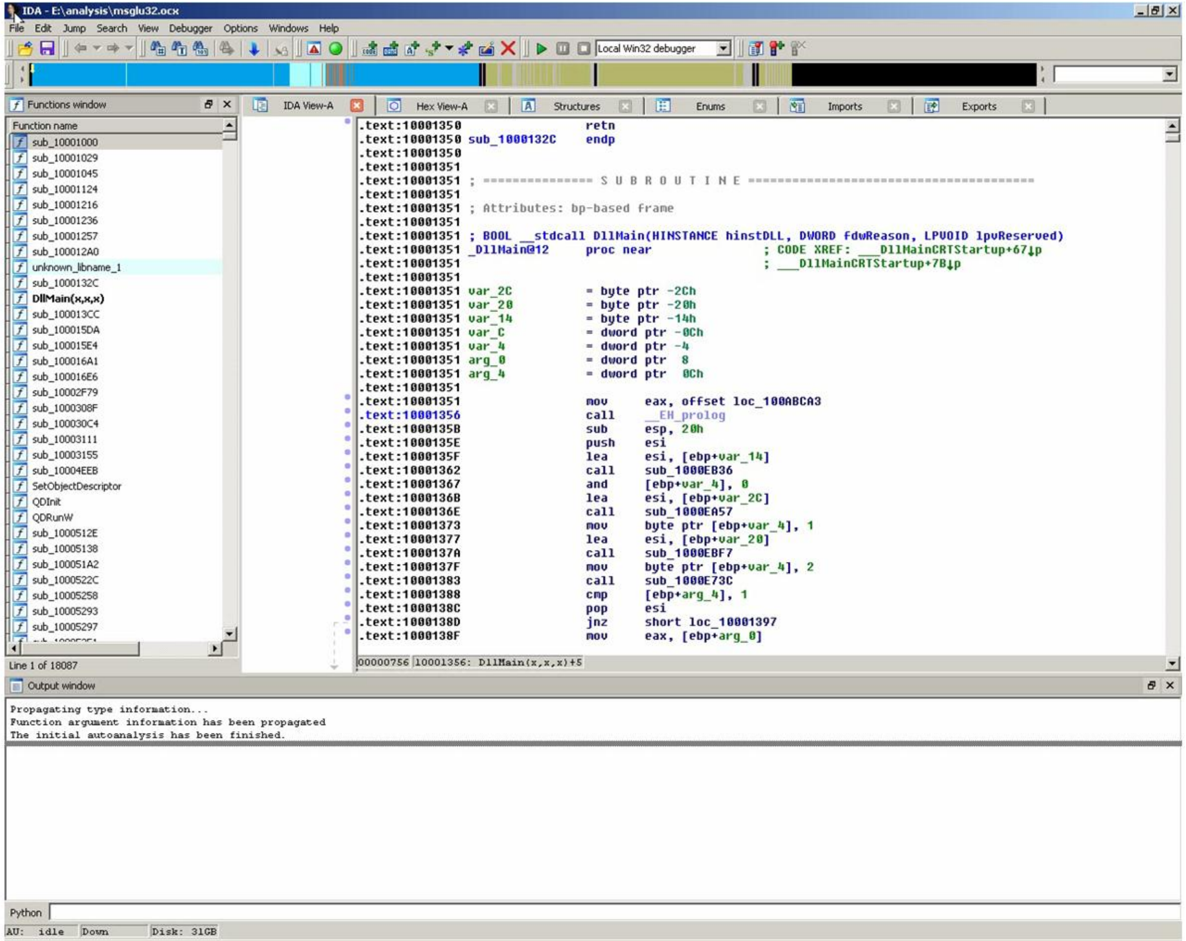
Threat level: !! Malicious

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

Sample Video of Flamer Analysis



Function name

```
sub_10001000
sub_10001029
sub_10001045
sub_10001124
sub_10001216
sub_10001236
sub_10001257
sub_100012A0
unknown_libname_1
sub_1000132C
DllMain(x,x,x)
sub_100013CC
sub_100015DA
sub_100015E4
sub_100016A1
sub_100016E6
sub_10002F79
sub_1000308F
sub_100030C4
sub_10003111
sub_10003155
sub_10004EEB
SetObjectDescriptor
QDInit
QDRunW
sub_1000512E
sub_10005138
sub_100051A2
sub_1000522C
sub_10005258
sub_10005293
sub_10005297
```

Line 1 of 18087

```
.text:10001350                 retn
.text:10001350 sub_1000132C    endp
.text:10001350
.text:10001351
.text:10001351 ; =============== S U B R O U T I N E =======================================
.text:10001351
.text:10001351 ; Attributes: bp-based frame
.text:10001351
.text:10001351 ; BOOL __stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
.text:10001351 _DllMain@12     proc near               ; CODE XREF: ___DllMainCRTStartup+67↓p
.text:10001351                                         ; ___DllMainCRTStartup+7B↓p
.text:10001351
.text:10001351 var_2C          = byte ptr -2Ch
.text:10001351 var_20          = byte ptr -20h
.text:10001351 var_14          = byte ptr -14h
.text:10001351 var_C           = dword ptr -0Ch
.text:10001351 var_4           = dword ptr -4
.text:10001351 arg_0           = dword ptr  8
.text:10001351 arg_4           = dword ptr  0Ch
.text:10001351
.text:10001351                 mov     eax, offset loc_100ABCA3
.text:10001356                 call    __EH_prolog
.text:1000135B                 sub     esp, 20h
.text:1000135E                 push    esi
.text:1000135F                 lea     esi, [ebp+var_14]
.text:10001362                 call    sub_1000EB36
.text:10001367                 and     [ebp+var_4], 0
.text:1000136B                 lea     esi, [ebp+var_2C]
.text:1000136E                 call    sub_1000EA57
.text:10001373                 mov     byte ptr [ebp+var_4], 1
.text:10001377                 lea     esi, [ebp+var_20]
.text:1000137A                 call    sub_1000EBF7
.text:1000137F                 mov     byte ptr [ebp+var_4], 2
.text:10001383                 call    sub_1000E73C
.text:10001388                 cmp     [ebp+arg_4], 1
.text:1000138C                 pop     esi
.text:1000138D                 jnz     short loc_10001397
.text:1000138F                 mov     eax, [ebp+arg_0]
```

```
00000756 10001356: DllMain(x,x,x)+5
```

```
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

CSI: Live

TRITON™

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

websense® CSI SERVICES

© 2012 Websense, Inc.

CSI: Live*

Work directly with a live, Websense Security Labs' Researcher

- Custom consultation
- Security reviews
- Forensic assistance

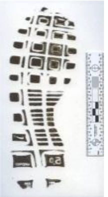
websense® SECURITY LABS

**Includes CSI: On-Demand resources*

© 2012 Websense, Inc.

CSI: Live

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)

websense® SECURITY LABS

Proactive Security Reviews

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

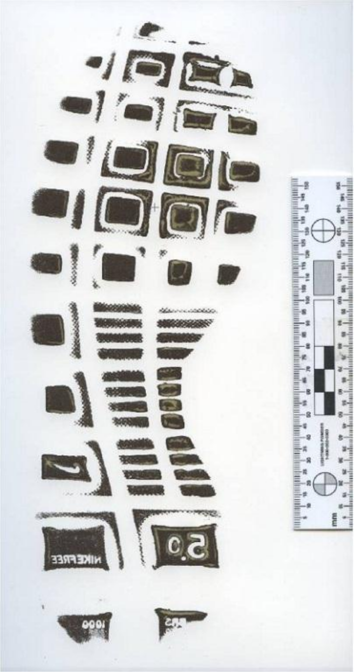
Custom Control Assessments

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

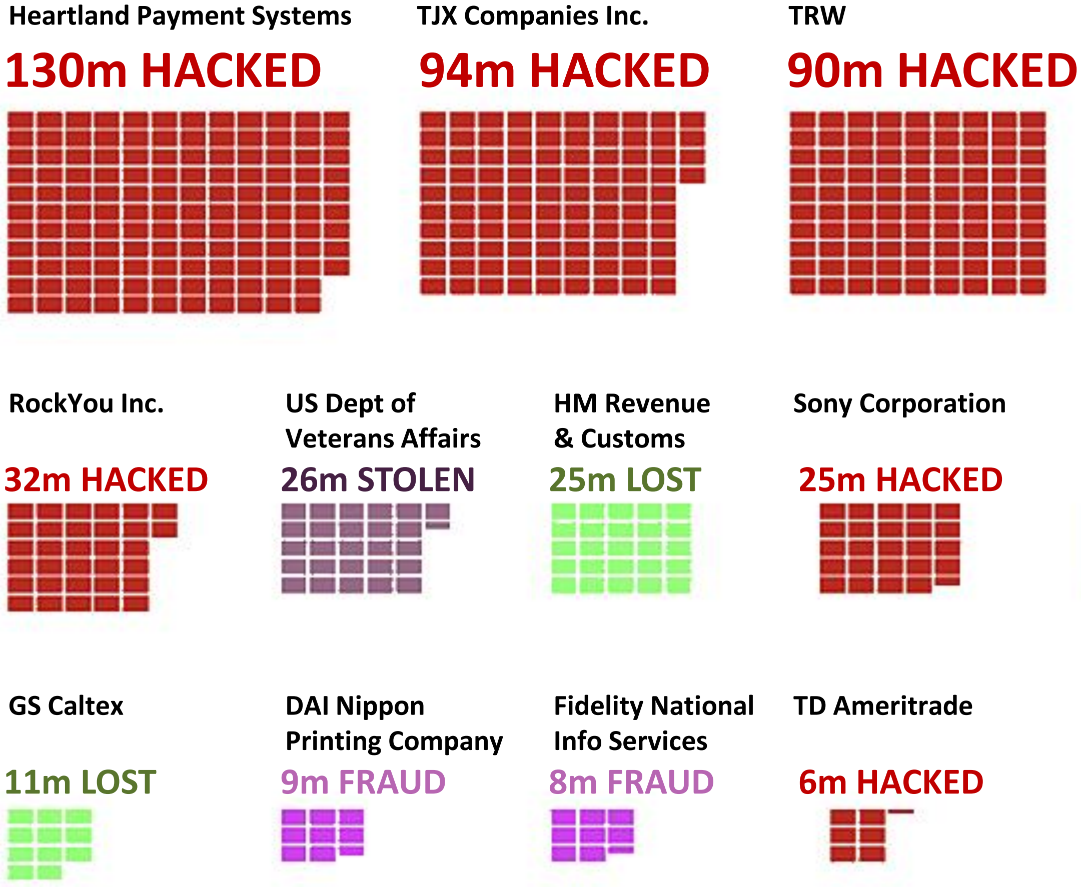
© 2012 Websense, Inc.

CSI: Live – Forensic Investigation

- Work directly with a live Websense Security Researcher
- Completely Confidential
- As needed forensic investigation support
- 4 Incidents
  (per annual contract period)
- “Forensic 4 Pack” option for additional incidents



websense®
CSI SERVICES



Heartland Payment Systems

130m HACKED

TJX Companies Inc.

94m HACKED

TRW

90m HACKED

RockYou Inc.

32m HACKED

US Dept of Veterans Affairs

26m STOLEN

HM Revenue & Customs

25m LOST

Sony Corporation

25m HACKED

GS Caltex

11m LOST

DAI Nippon Printing Company

9m FRAUD

Fidelity National Info Services

8m FRAUD

TD Ameritrade

6m HACKED

■1 million records lost, coloured by breach type

Source: Nathan YAU

CSI: Live - Security Training with Hands-On

- Instructors from Websense Security Labs
- 3-day security training with hands-on sessions
- Includes two attendees
- Offered twice annually

  (EMEA and NA locations)

websense® CSI SERVICES

© 2012 Websense, Inc.

CSI: Live – Proactive Security Reviews

websense

- Full policy and configuration evaluation
- Leverage industry, regional, and other standards
- Incorporate unique enterprise concerns
- Define and assess custom use case exercises
- Available Semi-annually

websense®
CSI SERVICES

© 2012 Websense, Inc.

CSI: Live – Custom Control Assessments

- Review submitted allow/deny lists
- For each URL, provides
  - Categorization
  - Security classification information
- Available Quarterly

websense®
CSI SERVICES

© 2012 Websense, Inc.

CSI: Summary

TRITON™

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

CyberSecurity Intelligence™ Services

websense

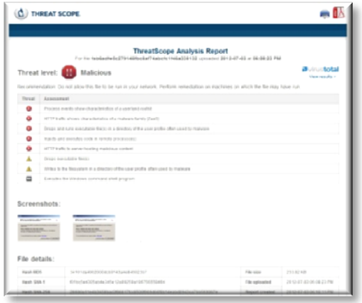
> *"It's becoming clear that many of these emerging threats cannot be defended against in-house, creating a shift in security posture toward being more proactive."*

IDC Senior Analyst Christine Liebert
IDC press release, Jan. 31, 2012,
http://www.idc.com/getdoc.jsp?containerId=prUS23290912

websense® CSI SERVICES

CSI: On-Demand

- ThreatScope malware analysis sandbox
- Priority access to research tools/services
- Video resources from research presentations & TAB events
- Online security training



THREAT SCOPE

ThreatScope Analysis Report

For file [illegible] uploaded [illegible] 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 (ZeuS)
●	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	[illegible]	File size	[illegible] KB
Hash SHA-1	[illegible]	File uploaded	[illegible]
Hash SHA-256	[illegible]	Report created	[illegible]

CSI: Live

- Direct access to Security Labs researchers
- Forensic investigation partner
- 3-day classes w/hands-on labs
- Regular security reviews
  - Customer Allow/Deny lists
  - Full security posture
- Includes **CSI: On-Demand**

© 2012 Websense, Inc.

CyberSecurity Intelligence™ Services

websense®

Blocking is Not Enough

On-Demand Resources

Live Researcher Access

websense® CSI SERVICES

© 2012 Websense, Inc.

Questions

http://securitylabs.websense.com/

© 2012 Websense, Inc.