proofpoint™

Essence of Advanced Persistent Threats in 15 Minutes

Wayne Huang, VP Engineering
email: whuang@proofpoint.com
twitter: @waynehuang

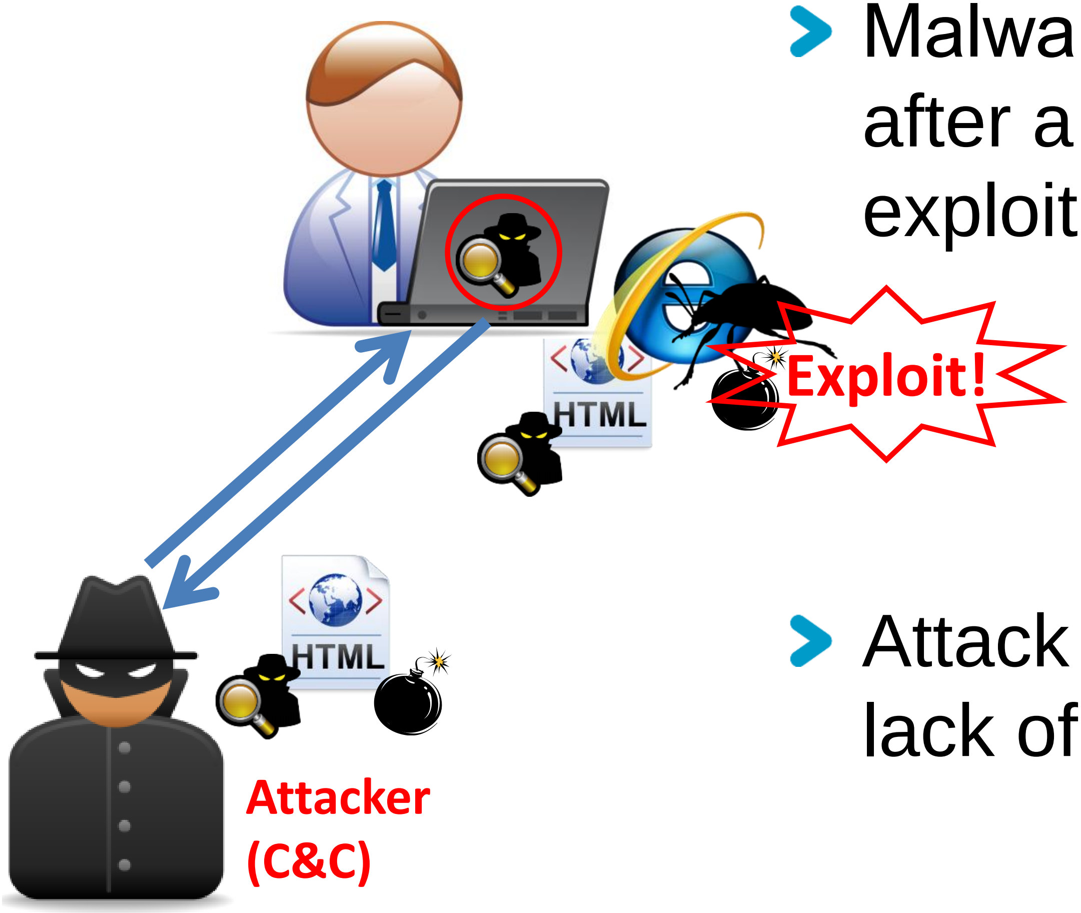
threat protection | compliance | archiving | secure communication

- Documents have lots of “bugs,” or “vulnerabilities”
- CVE-2013-3906
- Zeroday vulnerabilities

- Renderers [illegible]

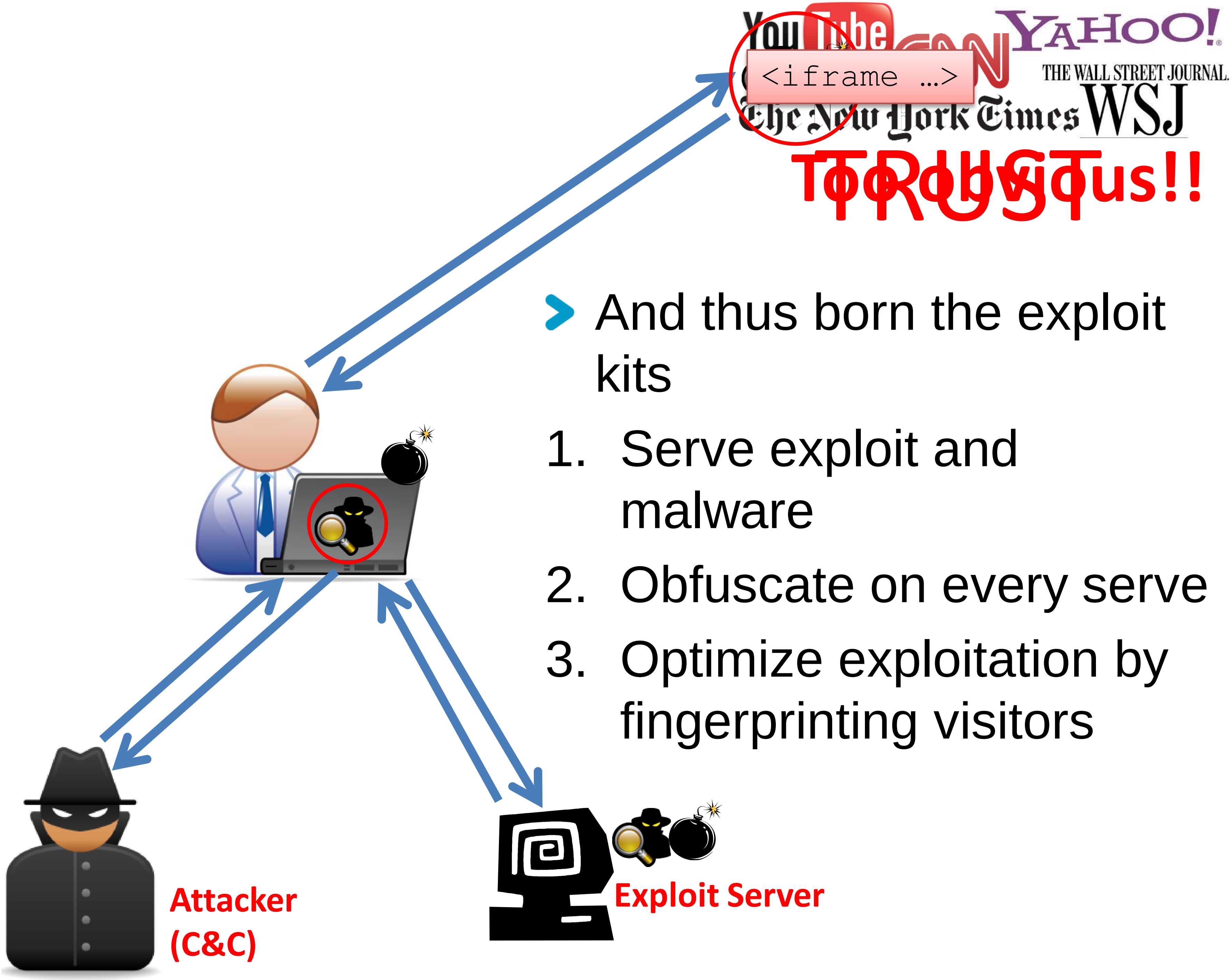
- HTML → Browsers
- PDF → PDF Reader, Foxit
- Word → MS Word
- PPT → MS Powerpoint
- Excel → MS Excel

“Documents” and “Renderers”



- Exploit: code to exploit a vulnerability
- Malware: What’s installed after a successful exploitation

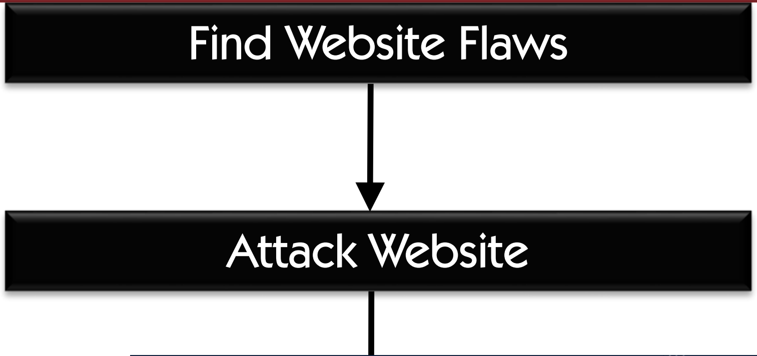
- Attack seldom works due to lack of TRUST



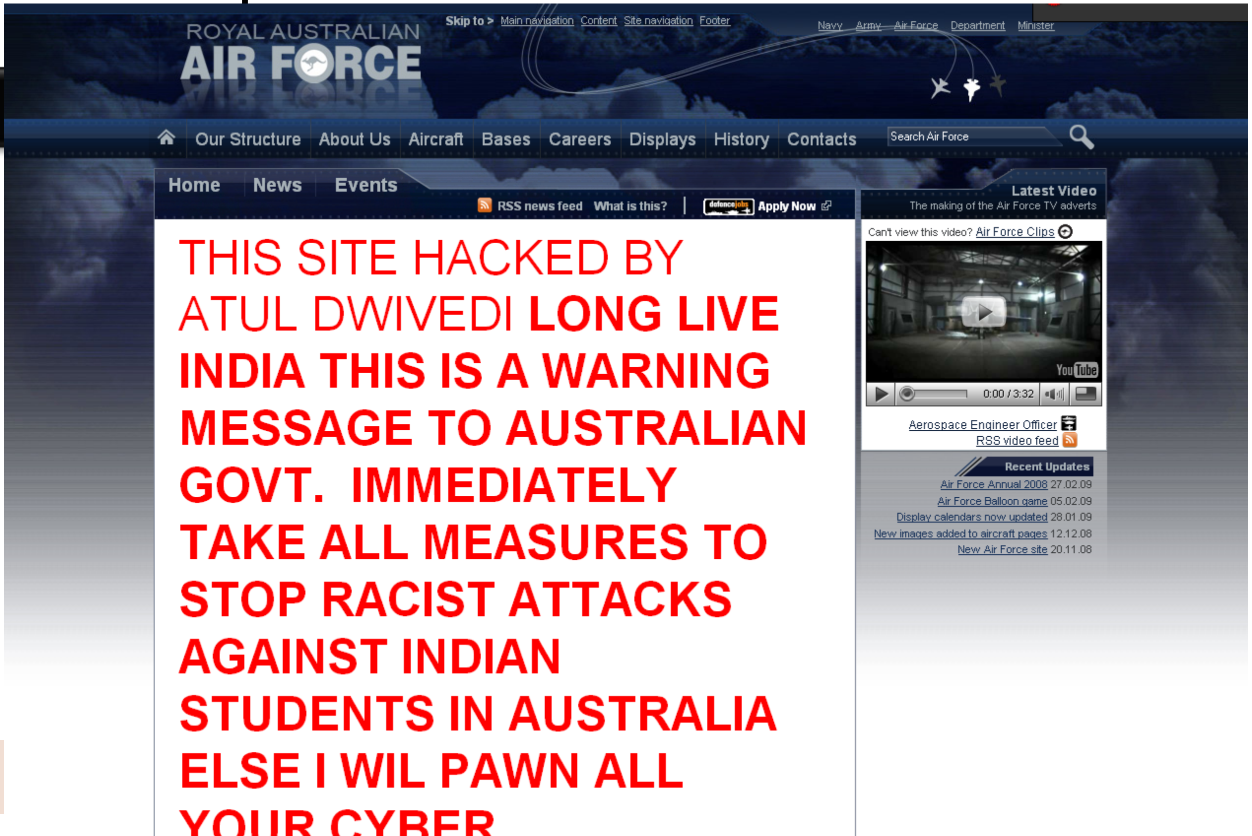
- And thus born the exploit kits

1. Serve exploit and malware
2. Obfuscate on every serve
3. Optimize exploitation by fingerprinting visitors

1990-1998: Deface Websites


Find Website Flaws

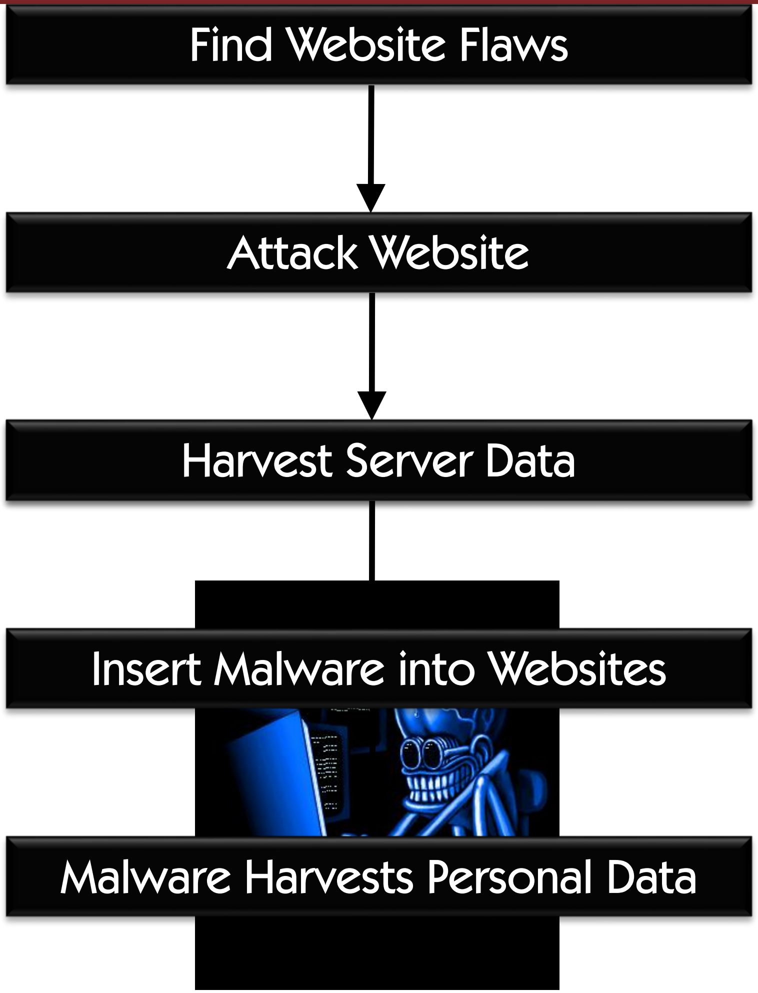
Attack Website


ROYAL AUSTRALIAN
AIR FORCE
Skip to > Main navigation Content Site navigation Footer
Navy Army Air Force Department Minister
Our Structure About Us Aircraft Bases Careers Displays History Contacts
Search Air Force
Home News Events
RSS news feed What is this?
defencejobs Apply Now
Latest Video
The making of the Air Force TV adverts
Can't view this video? Air Force Clips
0:00 / 3:32
YouTube
Aerospace Engineer Officer
RSS video feed
Recent Updates
Air Force Annual 2008 27.02.09
Air Force Balloon game 05.02.09
Display calendars now updated 28.01.09
New images added to aircraft pages 12.12.08
New Air Force site 20.11.08

THIS SITE HACKED BY ATUL DWIVEDI **LONG LIVE INDIA THIS IS A WARNING MESSAGE TO AUSTRALIAN GOVT. IMMEDIATELY TAKE ALL MEASURES TO STOP RACIST ATTACKS AGAINST INDIAN STUDENTS IN AUSTRALIA ELSE I WIL PAWN ALL YOUR CYBER**

1998-2006: Harvest Server Data

2007-2013: Harvest ~~Server~~ Endpoint Data



Find Website Flaws

Attack Website

Harvest Server Data

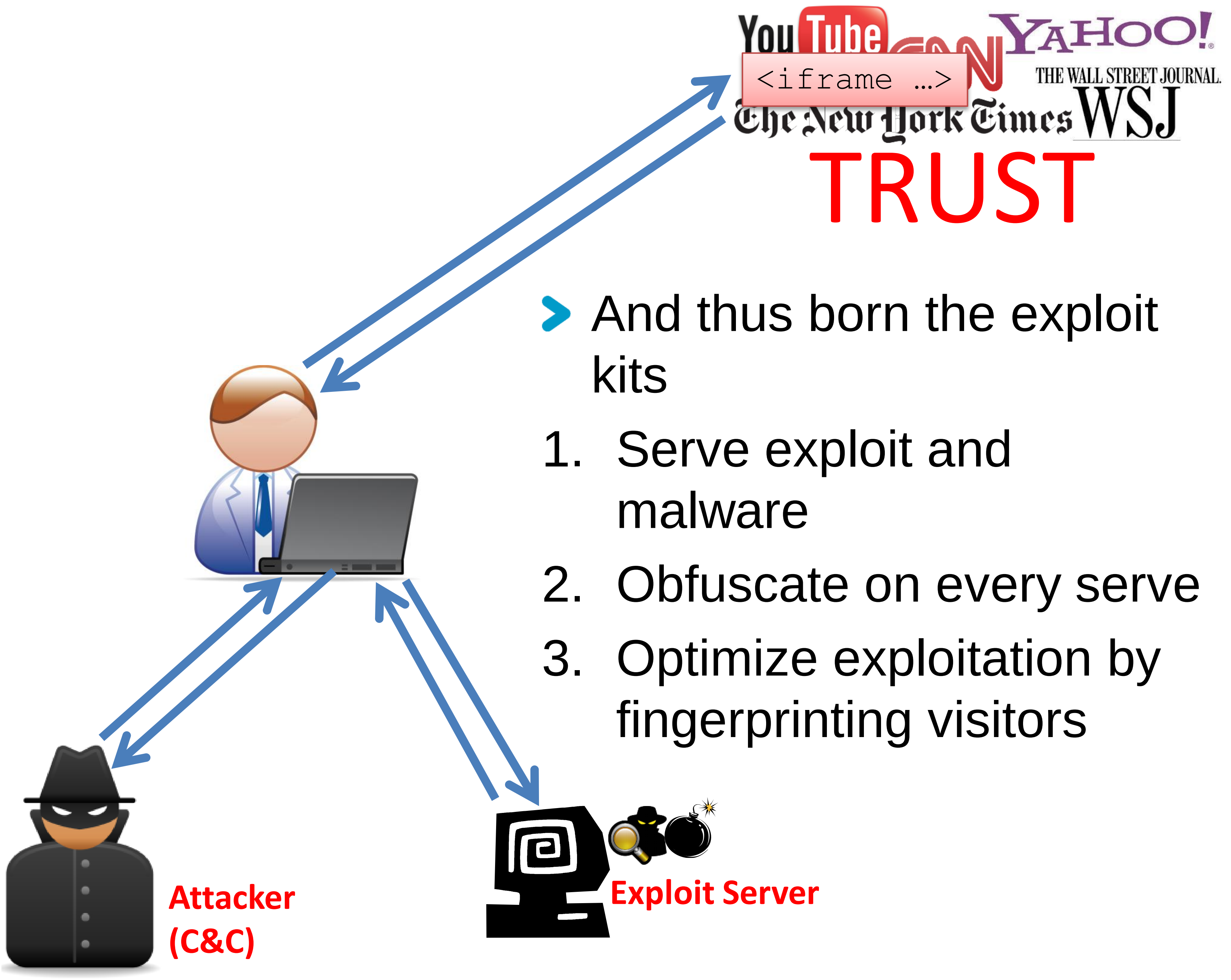
Insert Malware into Websites

Malware Harvests Personal Data

wayne@armorize.com @waynehuang

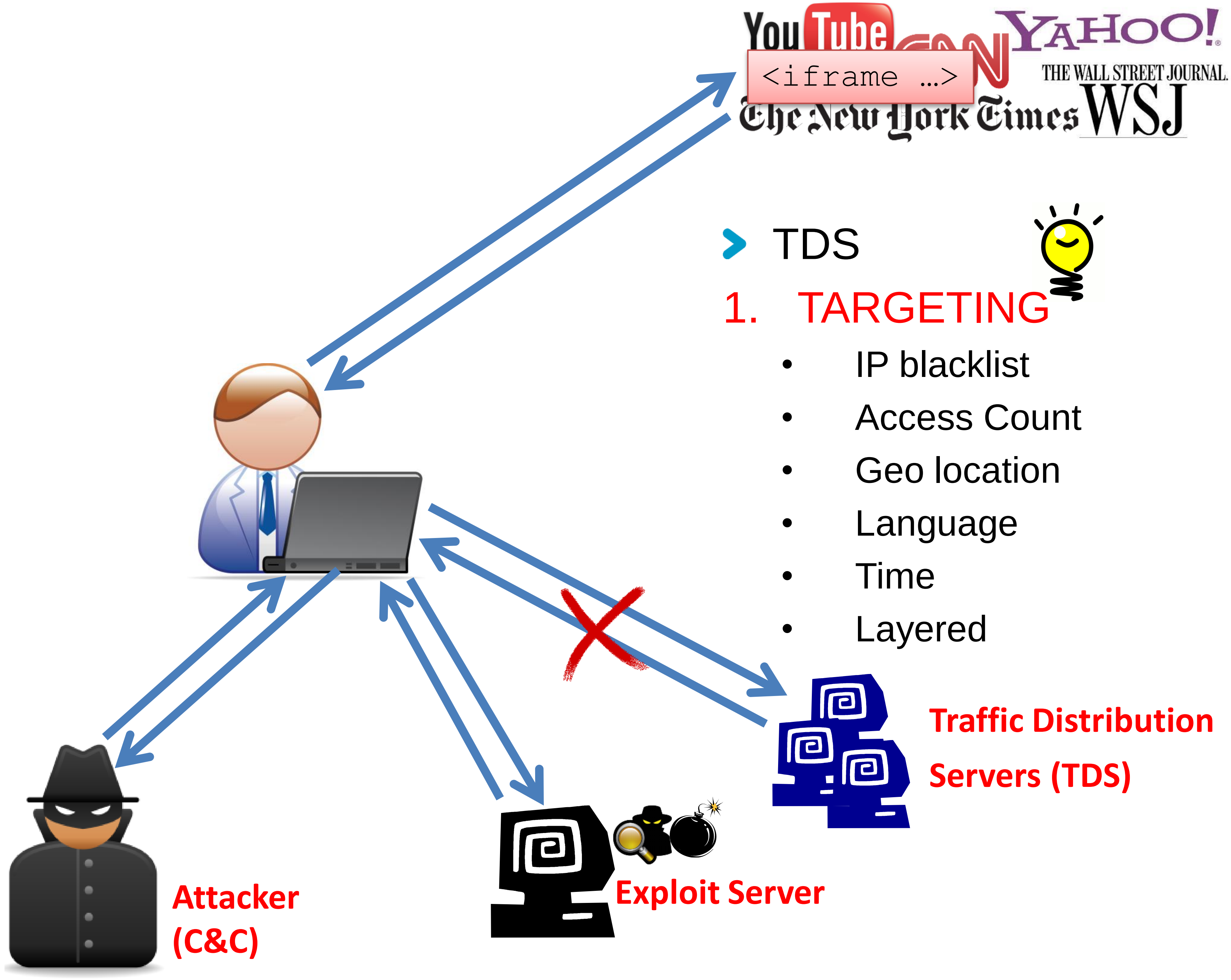
MySQL.com Spreading Fake Antivirus

- The Register: MySQL.com breach leaves visitors exposed to malware, September 26, 2011
- eWeek: Attackers Subvert MySQL.com With BlackHole Exploit Kit to Serve Malware, September 26, 2011
- Slashdot: Mysql.com Hacked, Made To Serve Malware, September 26, 2011
- Dark Reading: MySQL Site Compromised To Serve Up BlackHole Exploits, September 26, 2011
- Cnet: Hacked MySQL.com used to serve Windows malware, September 26, 2011
- ZDNet: MySQL.com hacked, redirects users to malware-laden sites, September 26, 2011
- PCWorld: MySQL.com Hacked to Serve Malware, September 27, 2011
- SC Magazine: MySQL.com hacked, September 27, 2011
- CIO: MySQL.com hacked to serve malware , September 27, 2011
- Krebs on Security: MySQL.com Sold for $3k, Serves Malware, September 26, 2011
- Threat Post: MySql.com Site Hacked, Was Serving Malware, September 26, 2011
- Computer World: MySQL.com hacked to serve malware, September 27, 2011
- Network World: MySQL.Com Website Hacked, September 26, 2011
- InfoWorld: MySQL.com hacked to serve malware, September 26, 2011
- ZDNet UK: Hackers place Windows malware on MySQL site, September 27, 2011
- Spam Fighter: Hackers Infiltrate MySQL.com for Pushing Malware, October 04, 2011
- THe H Security: MySQL.com hacked to serve malware, September 27, 2011
- Hack Illusion: Beware: Mysql.Com Infects Visitors With Malware, September 27, 2011
- Computing UK: MySql.com serves malware following hack, September 27, 2011
- Computerworld Australia: MySQL.com hacked to serve malware, September 27, 2011
- News4geeks: MySQL.com hacked to server malware, September 27, 2011
- OSNews: MySQL.com Hacked to Serve Malware, September 26, 2011
- Voice of Grey Hat: MYSQL.com Compromised & Giving Malware Warning, September 26, 2011
- Ars Technica: Hackers turn MySQL.com into malware launchpad, September 26, 2011
- BetaNews: mysql.com hacked and serving malware, stolen data sold on hacker forums, September 26, 2011
- Computer Weekly: MySQL.com hack serves up malware to site visitors, September 26, 2011
- Help Net Security: Mysql.com hacked, serving malware, September 26, 2011
- Naked Security: MySQL.com hacked for second time in a year, September 26, 2011
- SecurityWeek: MySQL.com Hacked: Cybercriminals Use Popular Open Source Site to Spread Malware, September 26, 2011
- TechWorld: MySQL.com hacked to serve malware, September 26, 2011



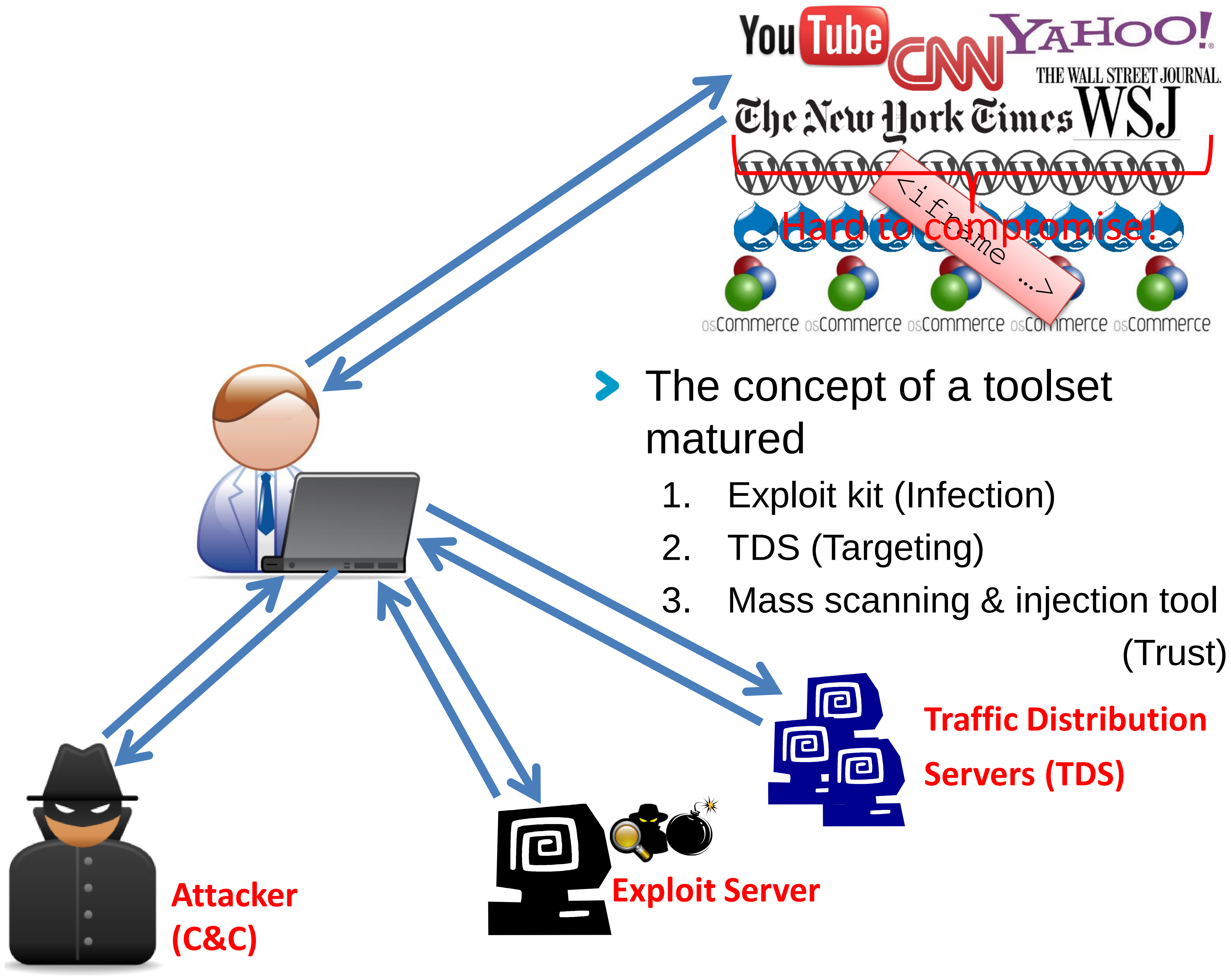
- And thus born the exploit kits

1. Serve exploit and malware
2. Obfuscate on every serve
3. Optimize exploitation by fingerprinting visitors



- TDS

1. TARGETING
   - IP blacklist
   - Access Count
   - Geo location
   - Language
   - Time
   - Layered



<iframe ...>

Hard to compromise!

- The concept of a toolset matured
  1. Exploit kit (Infection)
  2. TDS (Targeting)
  3. Mass scanning & injection tool (Trust)

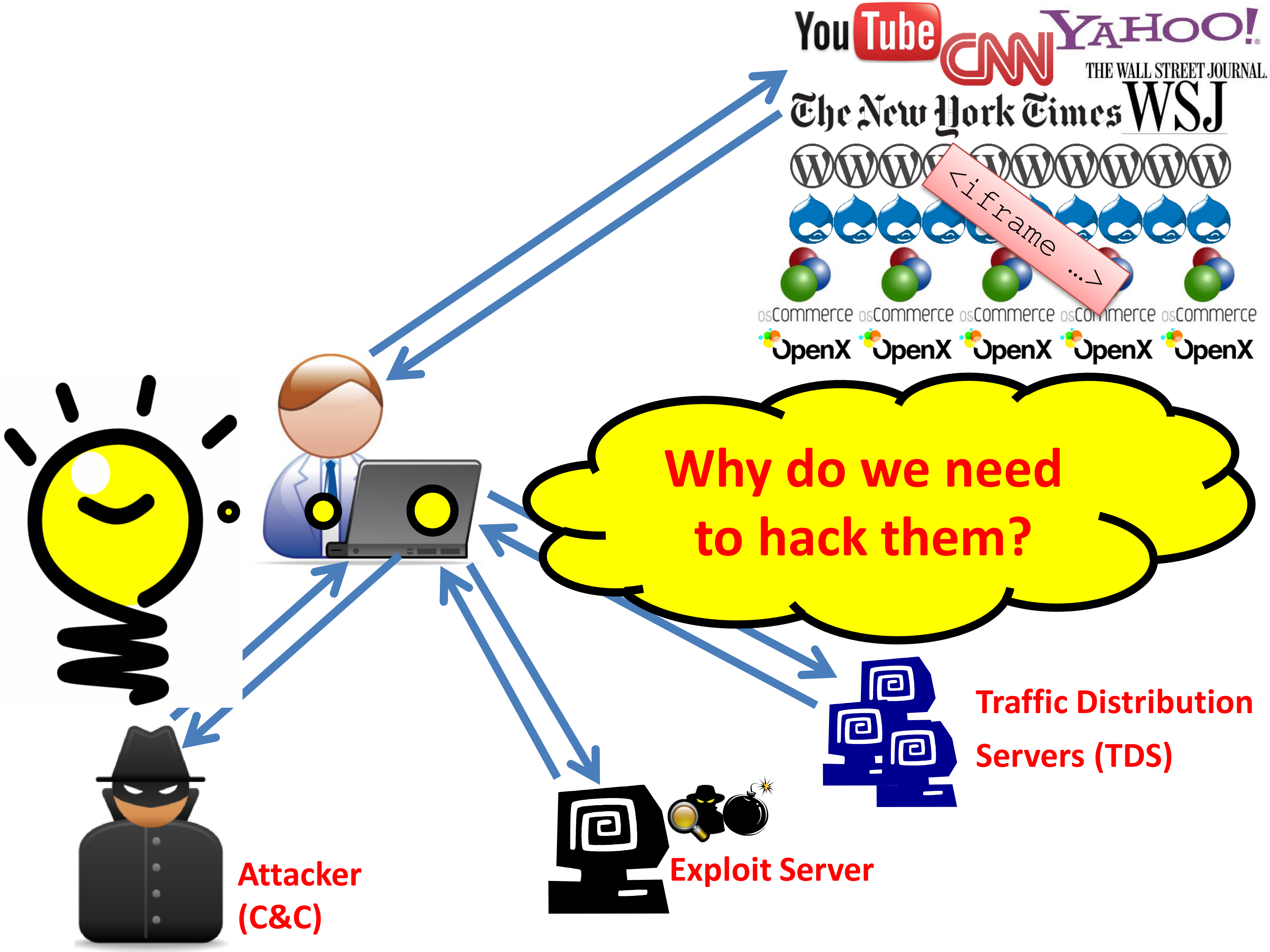
Traffic Distribution Servers (TDS)

Exploit Server

Attacker (C&C)

osCommerce Mass SQL Injection

- SPAMfighter: News, Armorize Unleash Massive Iframe Injection Assault, July 16, 2011
- CSO Online: Drive-by download infects more than 90,000 sites, Armorize warns, July 26, 2011
- Help Net Security: 90,000+ web pages compromised through iFrame injection, July 26, 2011
- TechNewsDaily: Massive Browser Attack Hits 90,000 Web Pages, July 26, 2011
- Threat Post: Massive iFrame Attack Hits More than 90,000 Pages, July 26, 2011
- CIO: E-Commerce Sites Based on Open Source Code Under Attack, July 28, 2011
- Computer World: E-commerce sites based on open source code under attack, July 28, 2011
- CSO Online: E-Commerce Sites Based on Open Source Code Under Attack, July 28, 2011
- InfoWorld: OS Commerce-based sites under attack, July 28, 2011
- Network World: E-commerce sites based on open source code under attack, July 28, 2011
- Practical Ecommerce: osCommerce 2.2 Websites Targeted by Mass Injection Attack, 143,000 Pages Hit, July 28, 2011
- ZDNet: 90,000+ pages compromised in mass iFrame injection attack, July 28, 2011
- PC World: E-commerce sites based on open source code under attack, July 29, 2011
- Rrockefeller News: Websites Programmed By Open Source Software Attacked By Malware, July 29, 2011
- CRN: iFrame Attack Infects More Than 300,000 osCommerce Sites, July 29, 2011
- Help Net Security: Mass iFrame injection attack now counts millions of compromised web pages, Auguest 1, 2011
- Kriterium: iFrame Attack Infects More Than 300,000 osCommerce Sites, Auguest 1, 2011
- Linux Today: E-commerce sites based on open source code under attack, Auguest 1, 2011
- SC Magazine: Mass injection campaign affects 3.8 million pages, Auguest 1, 2011
- Softpedia: Number of osCommerce Infected Pages Raises to Millions in Under a Week, Auguest 1, 2011
- The Tech Herald: osCommerce-based mass injection now 3.79 million pages strong, Auguest 1, 2011
- AVG: Massive iframe attack hits more than 100,000 web sites, Auguest 2, 2011
- HK Cert: Mass Injection Attacks Targeting osCommerce Vulnerabilities, Auguest 2, 2011
- The Register: Malware attack spreads to 5 million pages (and counting), Auguest 2, 2011
- The H Security: Millions of osCommerce stores hacked, Auguest 3, 2011
- Anti-Malware: Malware attack targets unpatched osCommerce websites, Auguest 4, 2011
- Threat Post: Massive Injection Campaign Affecting More Than Six Million Pages, Auguest 4, 2011
- KrebsonSecurity: Is That a Virus in Your Shopping Cart?, Auguest 5, 2011
- Spam Fighter: Armorize Unleash Massive Iframe Injection Assault, Auguest 5, 2011
- PCWorld: Speedy Malware Infects More than 6 Million Web Pages, Auguest 6, 2011
- Spam Fighter: Armorize Unleash Massive Iframe Injection Assault, Auguest 7, 2011
- CIO: New malware infects more than six million web pages, Auguest 8, 2011
- eWeek: Malware Wave Infects Six Million e-Commerce Pages, Auguest 8, 2011
- Ihotdesk: Malware reaches 6m pages in two weeks, Auguest 8, 2011
- PC Magazine: Millions of e-commerce Sites Hacked to Serve Malware, Auguest 8, 2011
- Tech World: Willysy malware infects millions of e-commerce sites, Auguest 8, 2011
- Dark Reading: 'Willysy' osCommerce Injection Attack Affects More Than 8 Million Pages, Auguest 9, 2011
- iss Source: Malware Feeds Off Slow Patching, Auguest 10, 2011
- Chameleon Web Services : osCommerce Virus Problems, Auguest 11, 2011
- USA TODAY: Millions of Web pages are hacker landmines, Auguest 11, 2011
- The Register: Attack targeting open-source web app keeps growing, Auguset 13, 2011



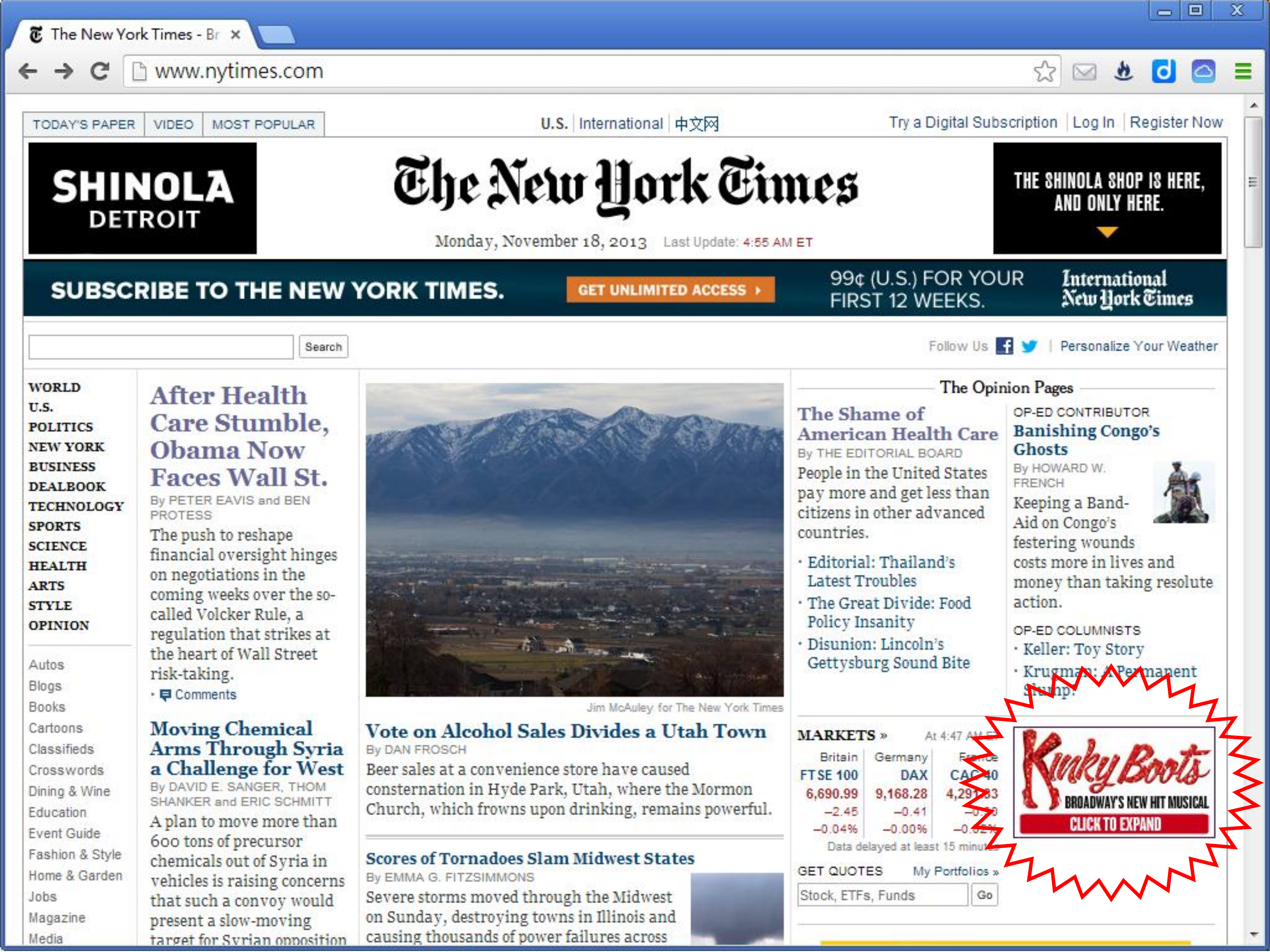
YouTube
CNN
YAHOO!
THE WALL STREET JOURNAL.
WSJ
The New York Times
<iframe …>
osCommerce osCommerce osCommerce osCommerce osCommerce
OpenX OpenX OpenX OpenX OpenX

Why do we need to hack them?

Traffic Distribution Servers (TDS)

Exploit Server

Attacker (C&C)



TODAY'S PAPER | VIDEO | MOST POPULAR

U.S. | International | 中文网

Try a Digital Subscription | Log In | Register Now

The New York Times

Monday, November 18, 2013 Last Update: 4:55 AM ET

Search

Follow Us | Personalize Your Weather

WORLD
U.S.
POLITICS
NEW YORK
BUSINESS
DEALBOOK
TECHNOLOGY
SPORTS
SCIENCE
HEALTH
ARTS
STYLE
OPINION

Autos
Blogs
Books
Cartoons
Classifieds
Crosswords
Dining & Wine
Education
Event Guide
Fashion & Style
Home & Garden
Jobs
Magazine
Media

After Health Care Stumble, Obama Now Faces Wall St.

By PETER EAVIS and BEN PROTESS

The push to reshape financial oversight hinges on negotiations in the coming weeks over the so-called Volcker Rule, a regulation that strikes at the heart of Wall Street risk-taking.

- Comments

Moving Chemical Arms Through Syria a Challenge for West

By DAVID E. SANGER, THOM SHANKER and ERIC SCHMITT

A plan to move more than 600 tons of precursor chemicals out of Syria in vehicles is raising concerns that such a convoy would present a slow-moving target for Syrian opposition

Jim McAuley for The New York Times

Vote on Alcohol Sales Divides a Utah Town

By DAN FROSCH

Beer sales at a convenience store have caused consternation in Hyde Park, Utah, where the Mormon Church, which frowns upon drinking, remains powerful.

Scores of Tornadoes Slam Midwest States

By EMMA G. FITZSIMMONS

Severe storms moved through the Midwest on Sunday, destroying towns in Illinois and causing thousands of power failures across

The Opinion Pages

The Shame of American Health Care

By THE EDITORIAL BOARD

People in the United States pay more and get less than citizens in other advanced countries.

- Editorial: Thailand's Latest Troubles
- The Great Divide: Food Policy Insanity
- Disunion: Lincoln's Gettysburg Sound Bite

OP-ED CONTRIBUTOR

Banishing Congo's Ghosts

By HOWARD W. FRENCH

Keeping a Band-Aid on Congo's festering wounds costs more in lives and money than taking resolute action.

OP-ED COLUMNISTS

- Keller: Toy Story
- Krugman: A Permanent Slump?

MARKETS » At 4:47 AM ET

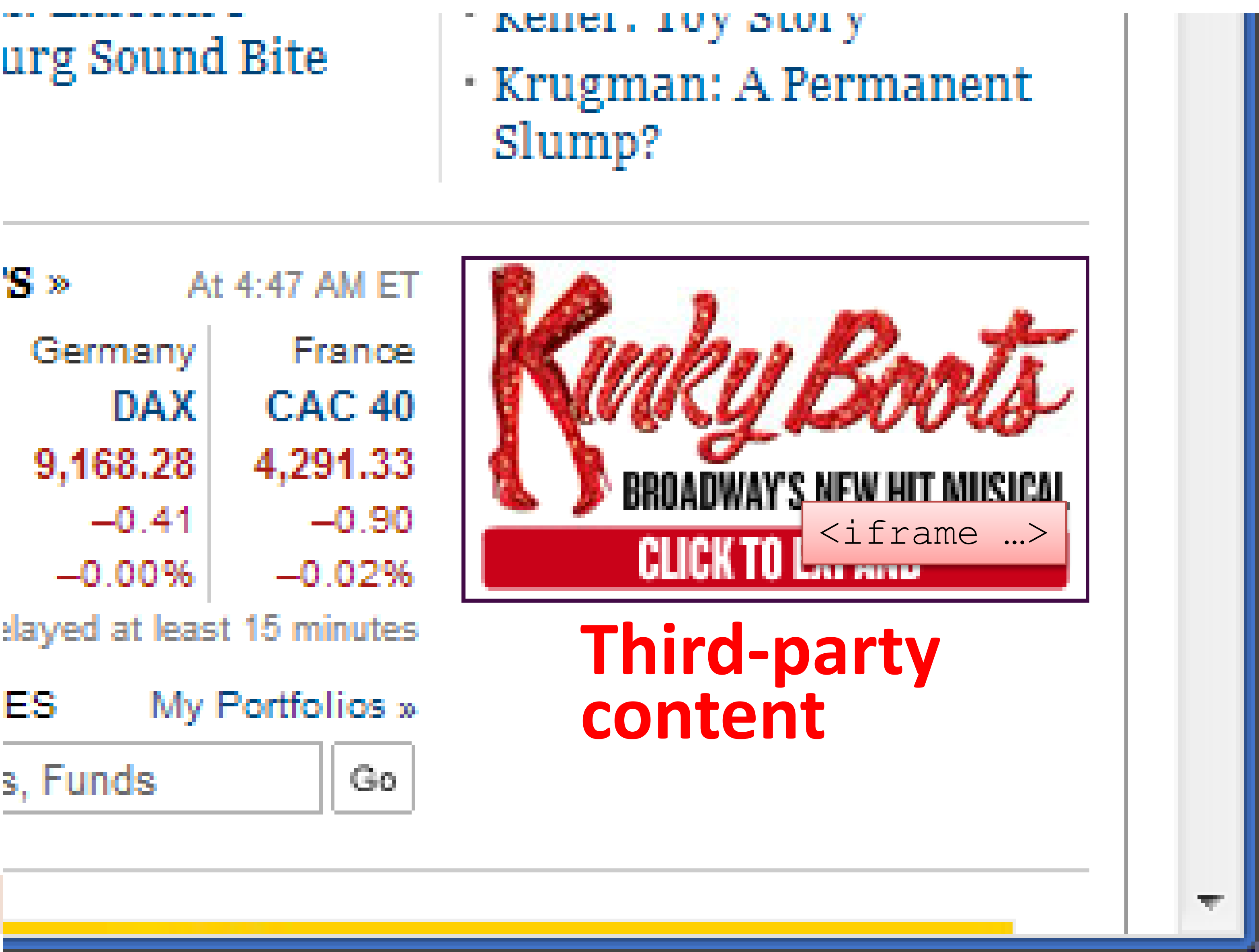
Britain	Germany	France
FTSE 100	DAX	CAC 40
6,690.99	9,168.28	4,291.33
−2.45	−0.41	−0.90
−0.04%	−0.00%	−0.02%

Data delayed at least 15 minutes

GET QUOTES My Portfolios »

Stock, ETFs, Funds Go

Submit Ad Containing IFrame to Exploit Kit?



urg Sound Bite

- Keller: Toy Story
- Krugman: A Permanent Slump?

'S » At 4:47 AM ET

Germany	France
DAX	CAC 40
9,168.28	4,291.33
–0.41	–0.90
–0.00%	–0.02%

elayed at least 15 minutes

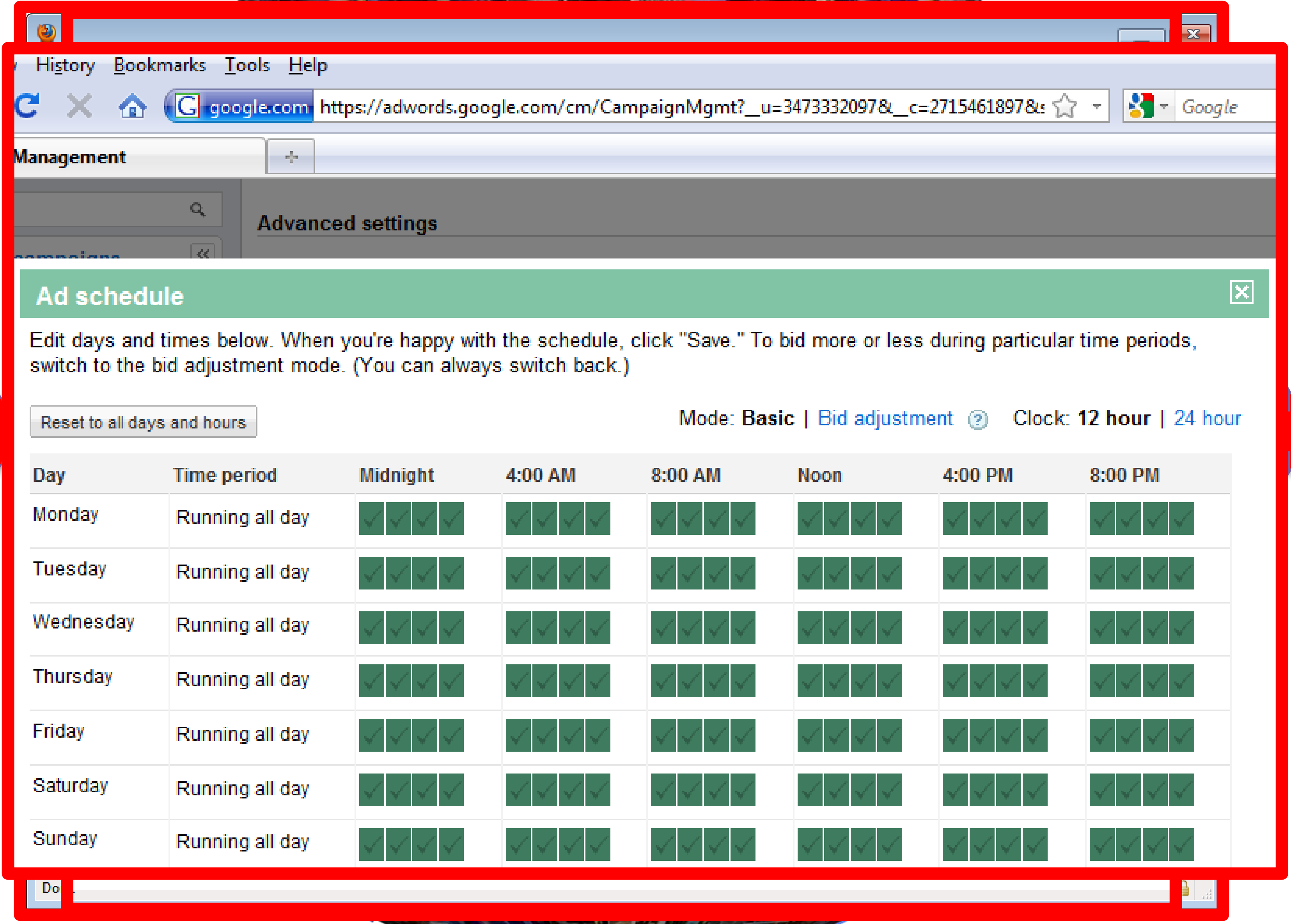
ES My Portfolios »

s, Funds Go

<iframe …>

Third-party content

ADVERTISERS


History Bookmarks Tools Help
google.com https://adwords.google.com/cm/CampaignMgmt?__u=3473332097&__c=2715461897&
Google
Management
Advanced settings

Ad schedule

Edit days and times below. When you're happy with the schedule, click "Save." To bid more or less during particular time periods, switch to the bid adjustment mode. (You can always switch back.)

Reset to all days and hours

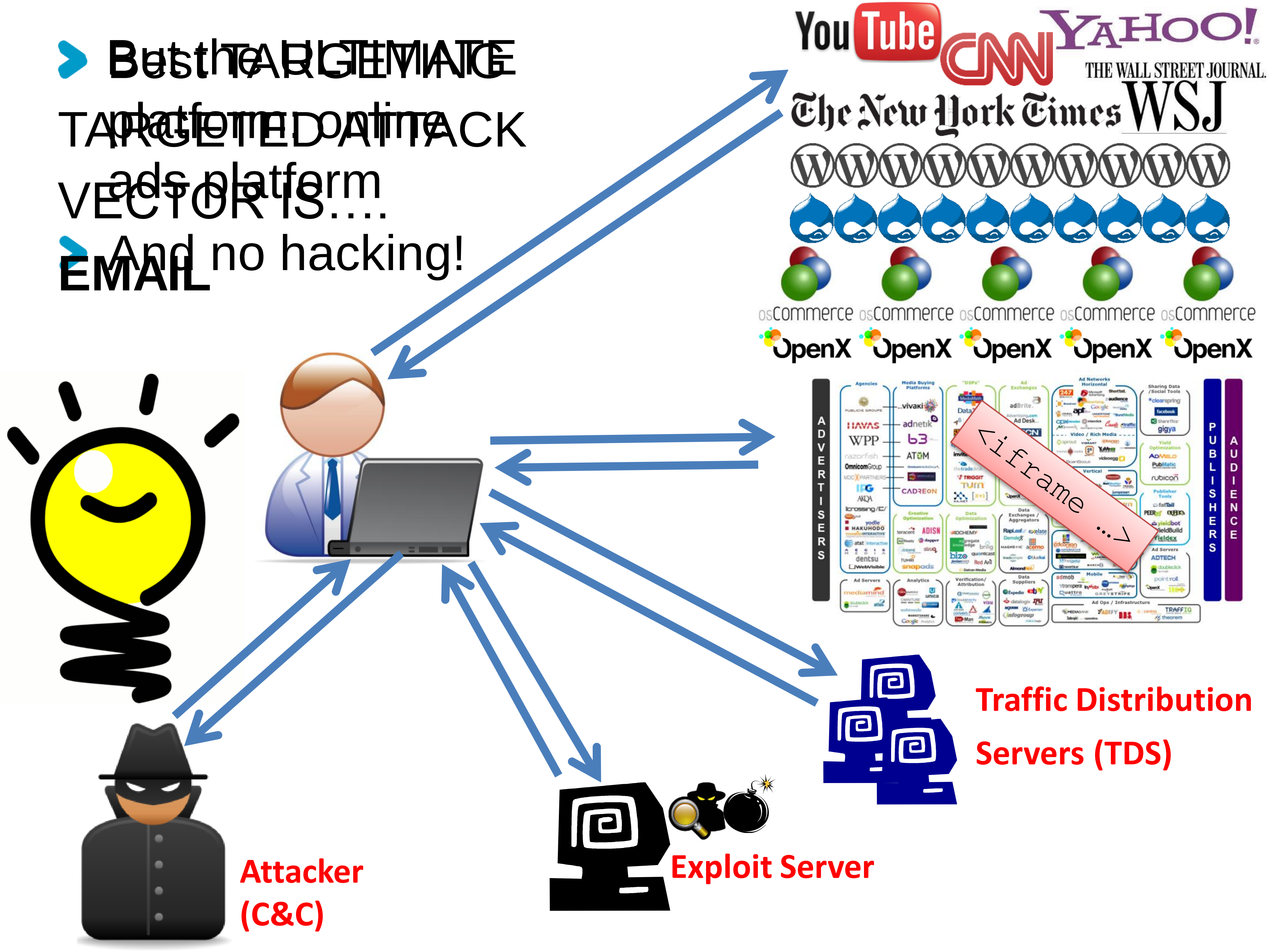
Mode: **Basic** | Bid adjustment Clock: **12 hour** | 24 hour

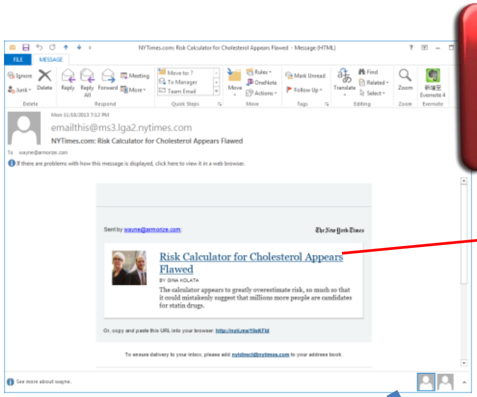
Day	Time period	Midnight	4:00 AM	8:00 AM	Noon	4:00 PM	8:00 PM
Monday	Running all day	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓
Tuesday	Running all day	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓
Wednesday	Running all day	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓
Thursday	Running all day	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓
Friday	Running all day	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓
Saturday	Running all day	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓
Sunday	Running all day	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓

AUDIENCE

Best TARGETED ATTACK VECTOR IS…. EMAIL

- But the LEGITIMATE platform: online ads platform
- And no hacking!





Mon 11/18/2013 7:12 PM

emailthis@ms3.lga2.nytimes.com

NYTimes.com: Risk Calculator for Cholesterol Appears Flawed

To wayne@armorize.com

If there are problems with how this message is displayed, click here to view it in a web browser.

Sent by wayne@armorize.com:

The New York Times

Risk Calculator for Cholesterol Appears Flawed

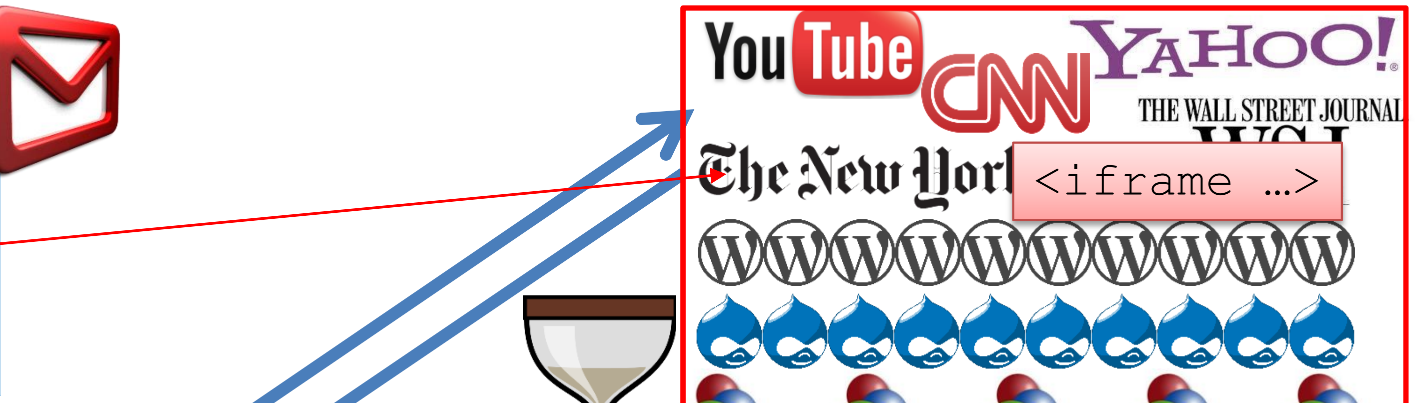
BY GINA KOLATA

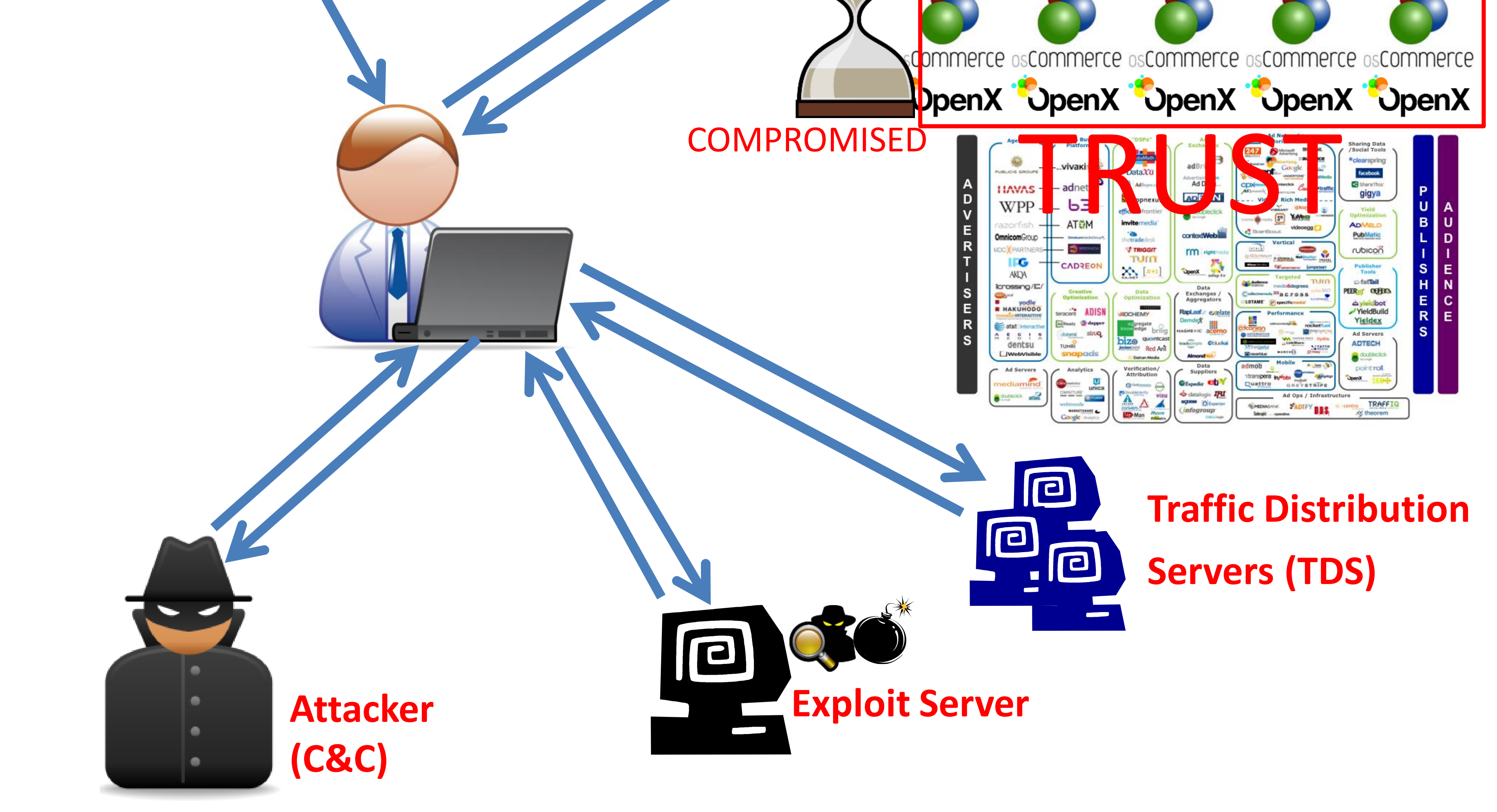
The calculator appears to greatly overestimate risk, so much so that it could mistakenly suggest that millions more people are candidates for statin drugs.

Or, copy and paste this URL into your browser: http://nyti.ms/19sKFld

To ensure delivery to your inbox, please add nytdirect@nytimes.com to your address book.

See more about wayne.

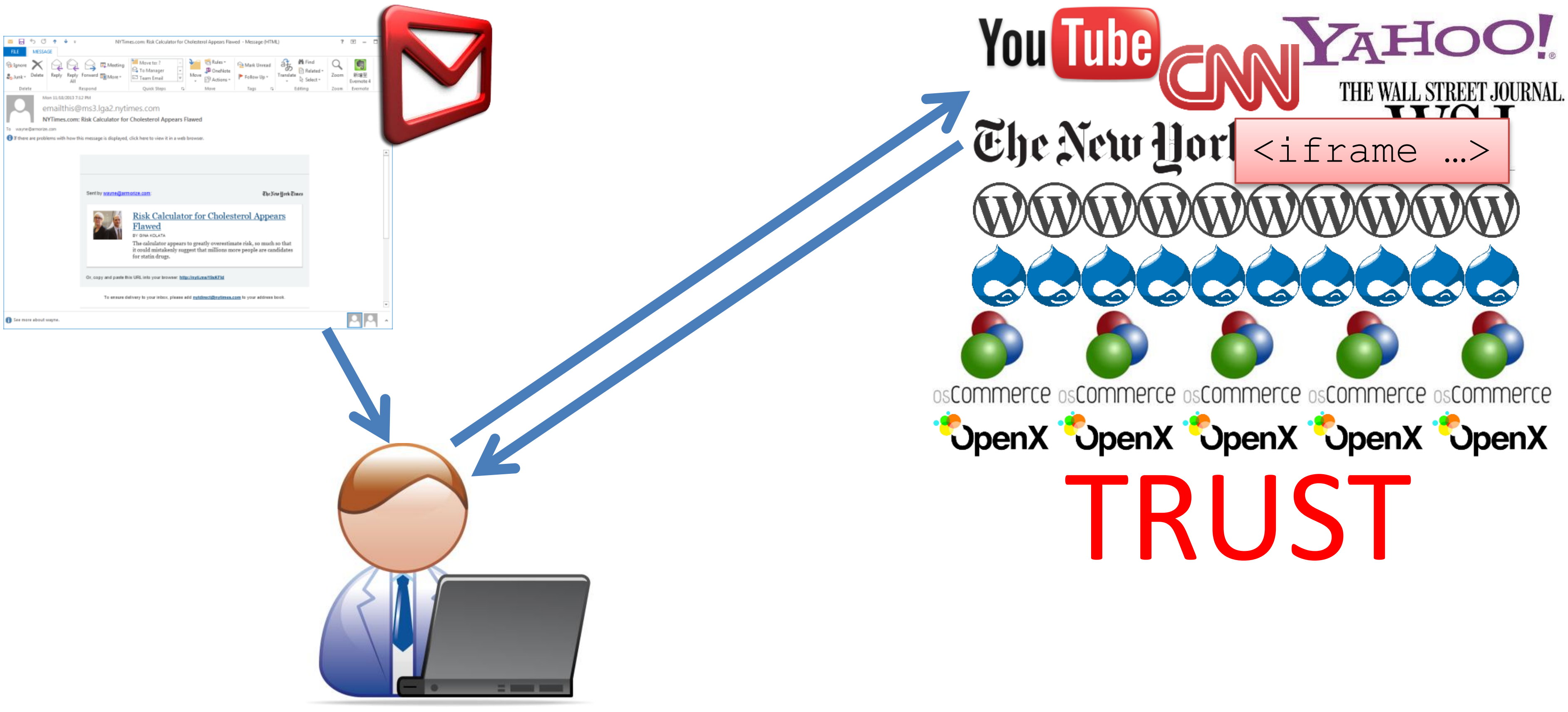




Traffic Distribution Servers (TDS)

Exploit Server

Attacker (C&C)



NYTimes.com: Risk Calculator for Cholesterol Appears Flawed - Message (HTML)

Mon 11/18/2013 7:12 PM

emailthis@ms3.lga2.nytimes.com

NYTimes.com: Risk Calculator for Cholesterol Appears Flawed

To wayne@armorize.com

If there are problems with how this message is displayed, click here to view it in a web browser.

Sent by wayne@armorize.com:

The New York Times

Risk Calculator for Cholesterol Appears Flawed

BY GINA KOLATA

The calculator appears to greatly overestimate risk, so much so that it could mistakenly suggest that millions more people are candidates for statin drugs.

Or, copy and paste this URL into your browser: http://nyti.ms/19xKFId

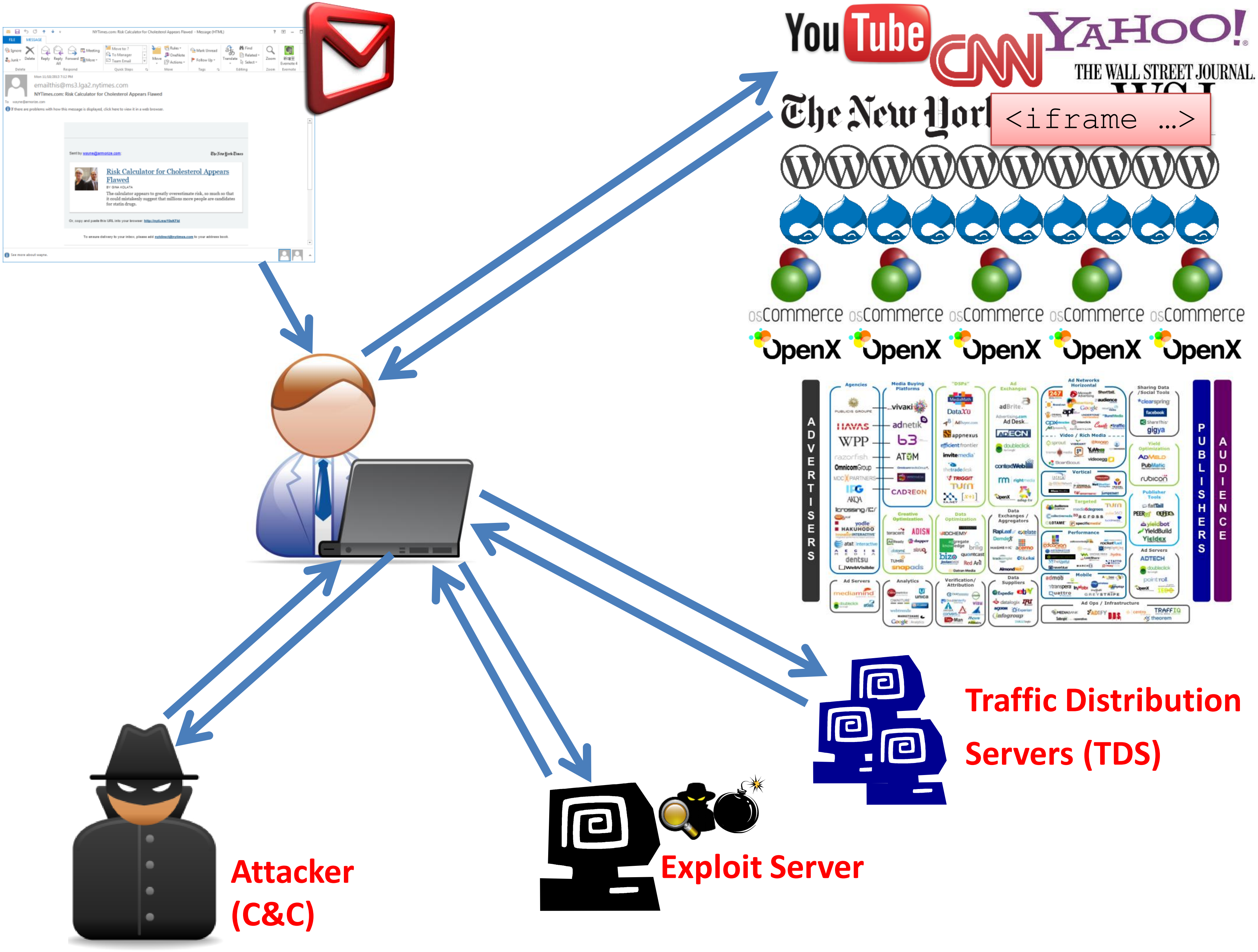
To ensure delivery to your inbox, please add nytdirect@nytimes.com to your address book.

See more about wayne.

<iframe …>

TRUST

- At send time, everything is LEGITIMATE
- Nothing what-so-ever is malicious
- There’s nothing to detect
- If exploit pack targets well, then even at click-time, detection is difficult



NYTimes.com: Risk Calculator for Cholesterol Appears Flawed - Message (HTML)

Mon 11/18/2013 7:12 PM

emailthis@ms3.lga2.nytimes.com

NYTimes.com: Risk Calculator for Cholesterol Appears Flawed

To wayne@armorize.com

If there are problems with how this message is displayed, click here to view it in a web browser.

Sent by wayne@armorize.com:

The New York Times

Risk Calculator for Cholesterol Appears Flawed

BY GINA KOLATA

The calculator appears to greatly overestimate risk, so much so that it could mistakenly suggest that millions more people are candidates for statin drugs.

Or, copy and paste this URL into your browser: http://nyti.ms/19xKFld

To ensure delivery to your inbox, please add nytdirect@nytimes.com to your address book.

See more about wayne.

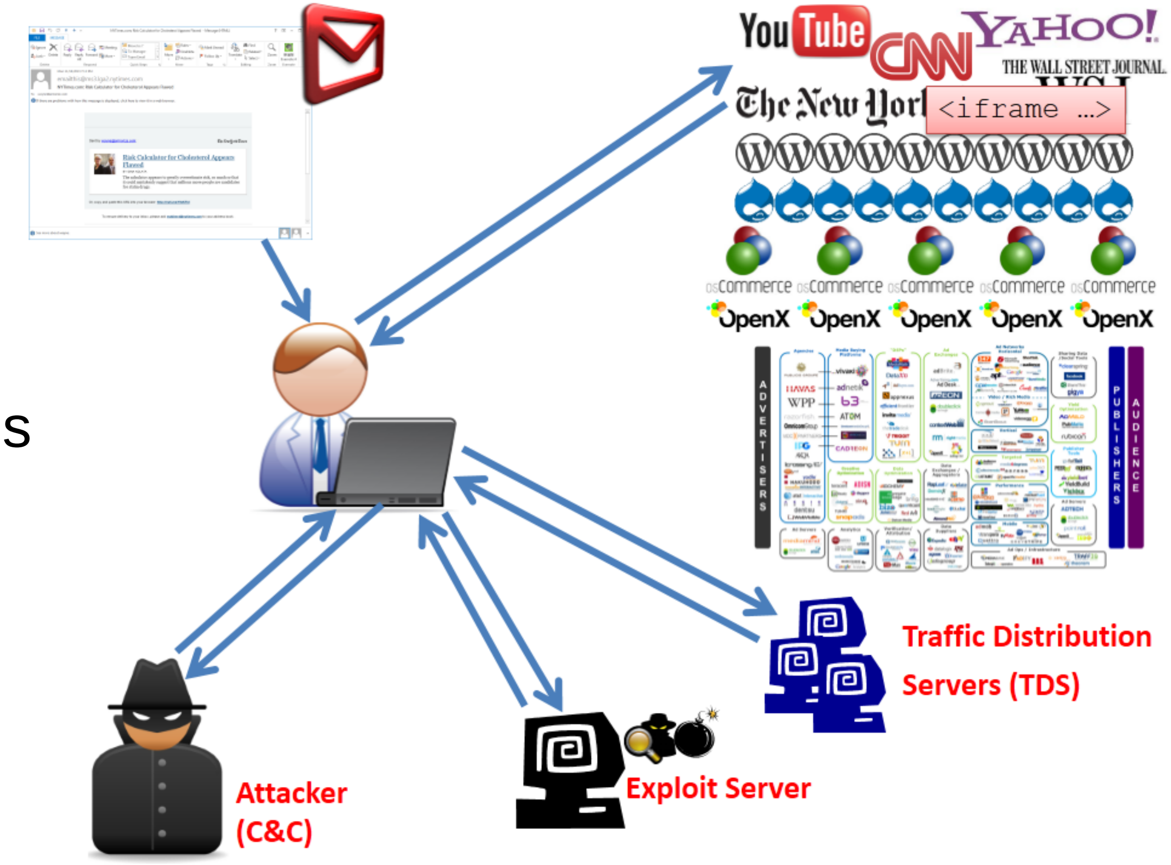
Traffic Distribution Servers (TDS)

Exploit Server

Attacker (C&C)

Modern Exploitation Toolset

- Mass Infection Tools
  - Wordpress
  - Joomla
  - OpenX
  - osCommerce
- Webshells
  - Scheduled injection and removal of iframes
- TDSs
- Exploit packs
- Malware
- C&C



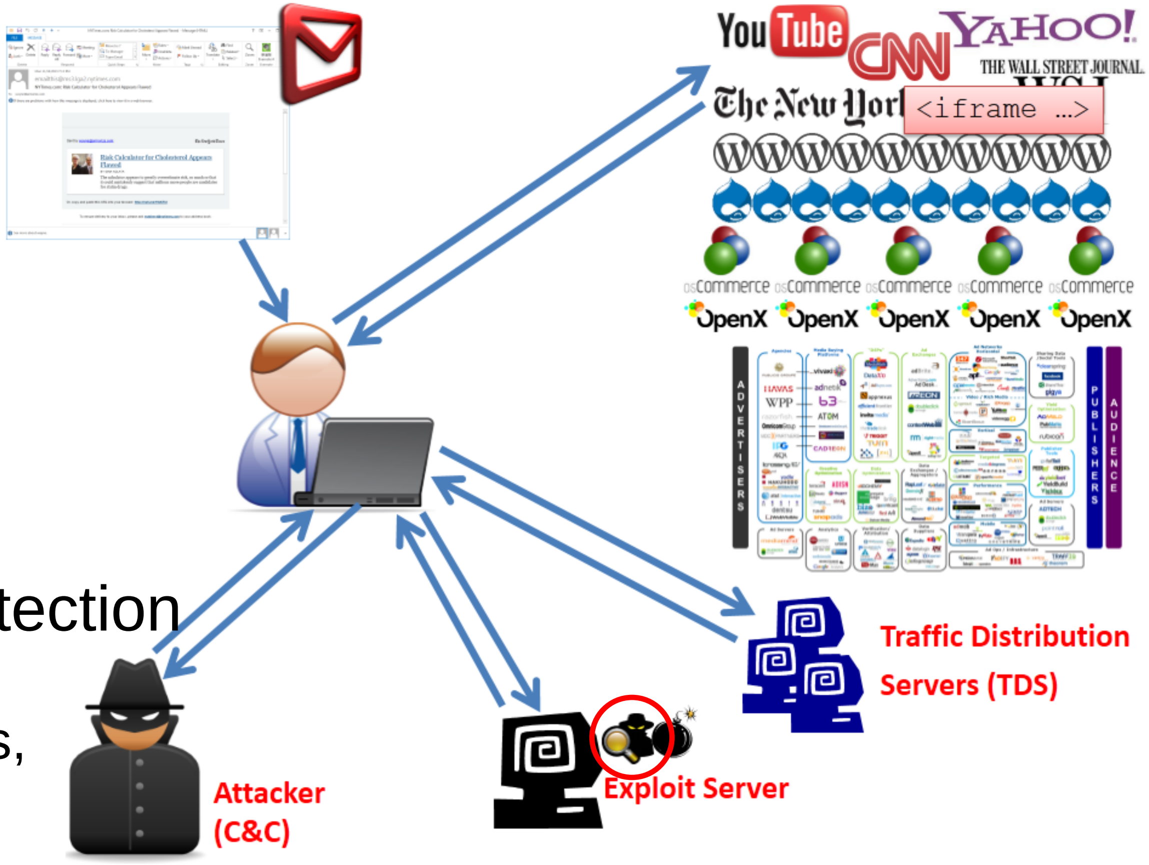
Traffic Distribution Servers (TDS)

Exploit Server

Attacker (C&C)

The Modern Exploit Pack

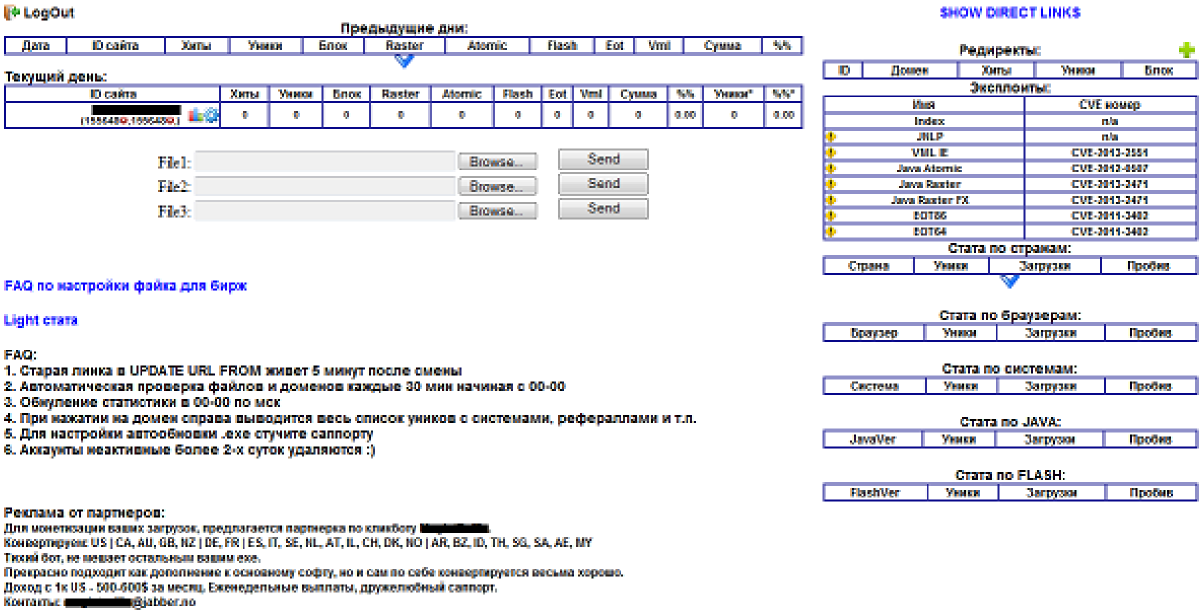
- Exploit pack features:
  - Targeting
    - IP blacklist
    - Access Count
    - Geo location
    - Language
    - Time
  - Obfuscation
  - Newest exploits
- Obfuscation of the dropper
- Techniques that make non-sandbox detection more difficult
  - IDS, emulated browsers, crawlers



proofpoint

Magnitude (Popads / DeathTouch EK)

- Widely used since March
- Obfuscation of the dropper (single-byte XOR)
- Mostly for email and malvertising attacks
- CVE-2011-3402 (IE)
  CVE-2012-0507 (Java)
  CVE-2013-2463 (Java)
  CVE-2013-0634 (Flash)
  CVE-2013-2551 (IE6-10)



LogOut

Предыдущие дни:

Дата	ID сайта	Хиты	Уники	Блок	Raster	Atomic	Flash	Eot	Vml	Сумма	%%

Текущий день:

ID сайта	Хиты	Уники	Блок	Raster	Atomic	Flash	Eot	Vml	Сумма	%%	Уники*	%%*
[redacted] (1556480,1556480)	0	0	0	0	0	0	0	0	0	0.00	0	0.00

File1: Browse... Send
File2: Browse... Send
File3: Browse... Send

FAQ по настройки файла для бирж

Light стата

FAQ:
1. Старая линка в UPDATE URL FROM живет 5 минут после смены
2. Автоматическая проверка файлов и доменов каждые 30 мин начиная с 00-00
3. Обнуление статистики в 00-00 по мск
4. При нажатии на домен справа выводится весь список уников с системами, рефераллами и т.п.
5. Для настройки автообновки .exe стучите саппорту
6. Аккаунты неактивные более 2-х суток удаляются :)

Реклама от партнеров:
Для монетизации ваших загрузок, предлагается партнерка по кликботу [redacted].
Конвертируем: US | CA, AU, GB, NZ | DE, FR | ES, IT, SE, NL, AT, IL, CH, DK, NO | AR, BZ, ID, TH, SG, SA, AE, MY
Тихий бот, не мешает остальным вашим exe.
Прекрасно подходит как дополнение к основному софту, но и сам по себе конвертируется весьма хорошо.
Доход с 1к US - 500-600$ за месяц. Еженедельные выплаты, дружелюбный саппорт.
Контакты: [redacted]@jabber.no

SHOW DIRECT LINKS

Редиректы:

ID	Домен	Хиты	Уники	Блок

Эксплоиты:

Имя	CVE номер
Index	n/a
JNLP	n/a
VML IE	CVE-2013-2551
Java Atomic	CVE-2012-0507
Java Raster	CVE-2013-2471
Java Raster FX	CVE-2013-2471
EOT86	CVE-2011-3402
EOT64	CVE-2011-3402

Стата по странам:

Страна	Уники	Загрузки	Пробив

Стата по браузерам:

Браузер	Уники	Загрузки	Пробив

Стата по системам:

Система	Уники	Загрузки	Пробив

Стата по JAVA:

JavaVer	Уники	Загрузки	Пробив

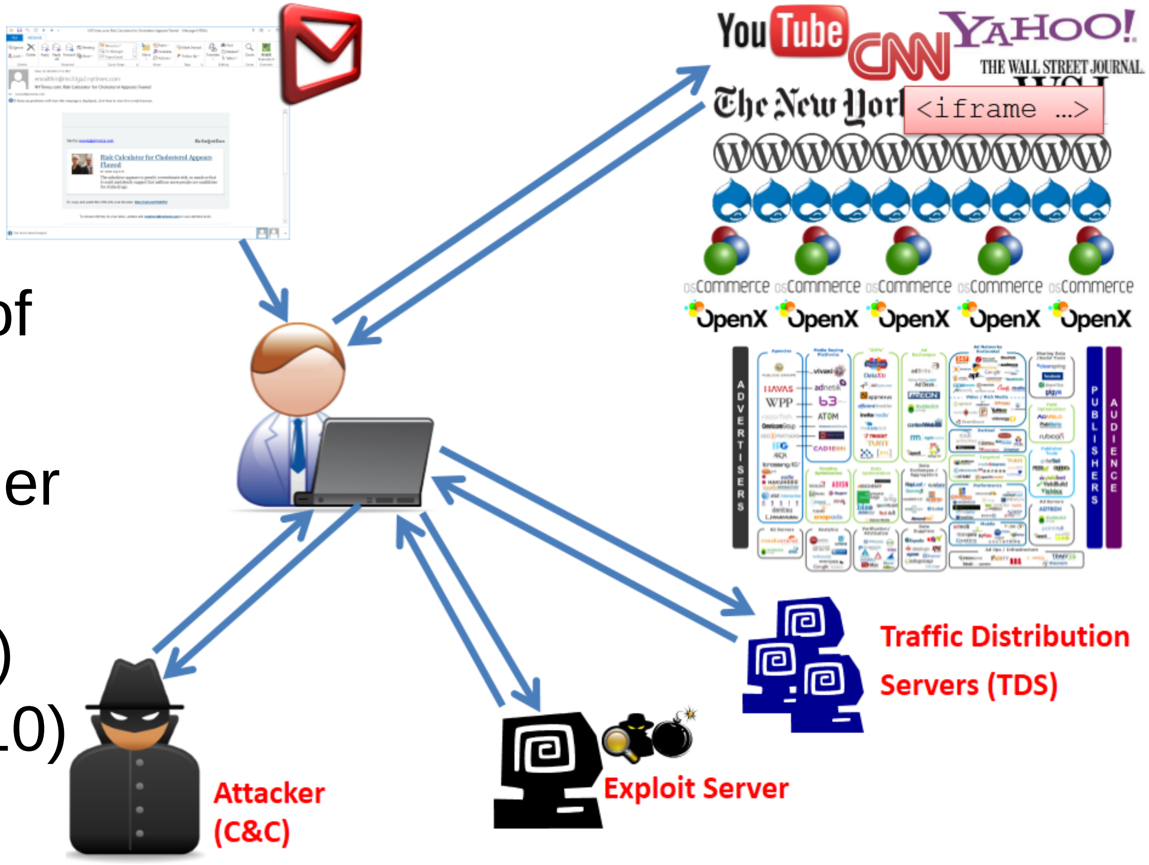
Стата по FLASH:

FlashVer	Уники	Загрузки	Пробив

(screenshot from: kahusecurity.com)

Neutrino

- Replaces BlackHole 2.0
- Widely used since Jan
- Obfuscation of the dropper (4-byte XOR)
- AJAX-based retrieval of javascript
- Harder for IDS and other emulators to detect
- CVE-2012-1723 (Java) CVE-2013-2551 (IE6-10)



Conclusion 1

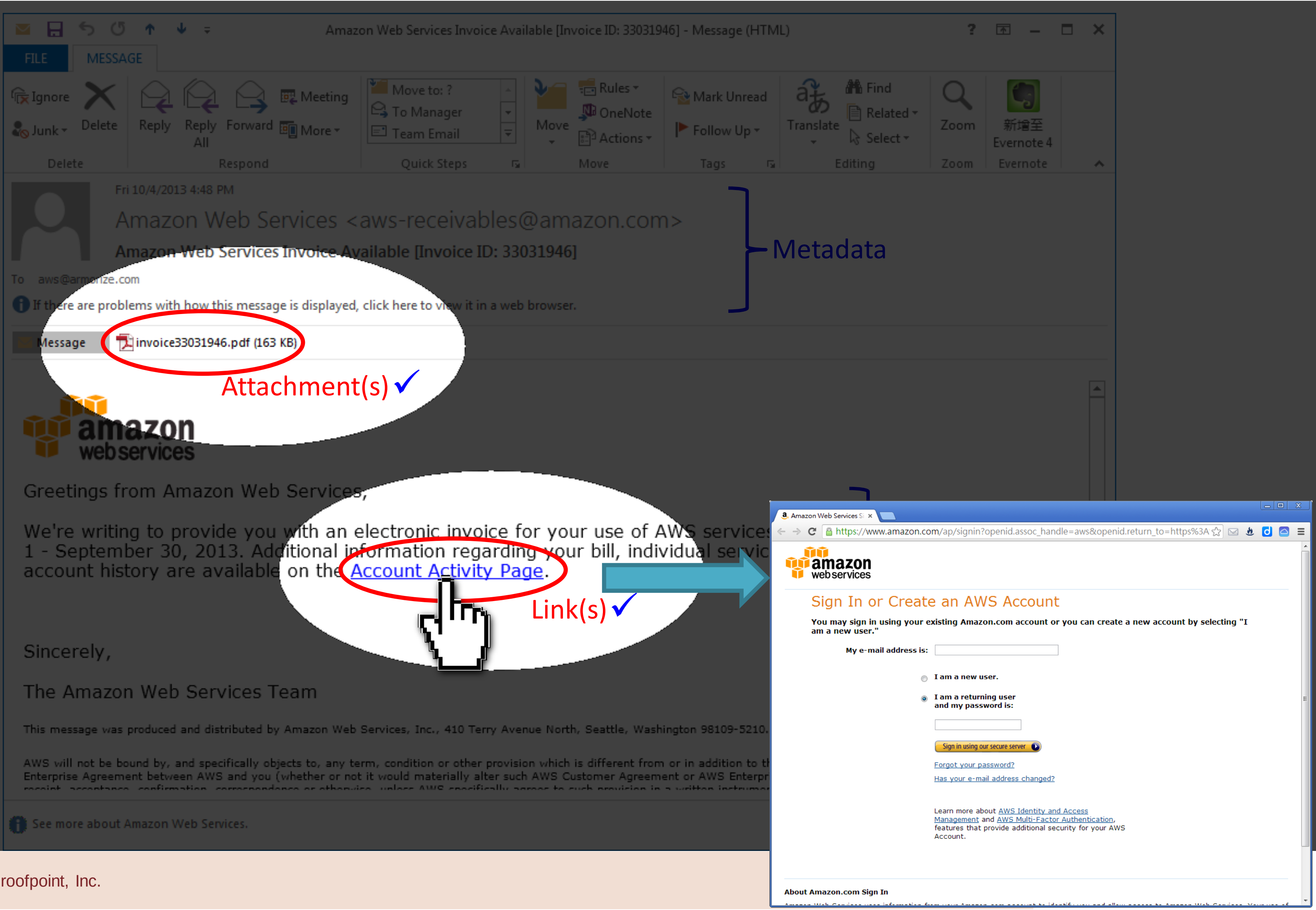
- Modern exploit packs are used for:
  - Email-based APT attacks
    - Watering hole timing attacks
  - Mass infections
  - Malvertising

- Harder and harder for traditional technologies to detect

- Follows BlackHole 2.0’s model, offered as a service

- Used as a part of the attacker’s toolset

Advanced Email Threats: Attack Vectors



Amazon Web Services Invoice Available [Invoice ID: 33031946] - Message (HTML)

Fri 10/4/2013 4:48 PM

Amazon Web Services <aws-receivables@amazon.com>

Amazon Web Services Invoice Available [Invoice ID: 33031946]

To aws@armorize.com

If there are problems with how this message is displayed, click here to view it in a web browser.

Message | invoice33031946.pdf (163 KB)

Greetings from Amazon Web Services,

We're writing to provide you with an electronic invoice for your use of AWS services
1 - September 30, 2013. Additional information regarding your bill, individual servic
account history are available on the Account Activity Page.

Sincerely,

The Amazon Web Services Team

This message was produced and distributed by Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, Washington 98109-5210.

AWS will not be bound by, and specifically objects to, any term, condition or other provision which is different from or in addition to th
Enterprise Agreement between AWS and you (whether or not it would materially alter such AWS Customer Agreement or AWS Enterpr

See more about Amazon Web Services.

Amazon Web Services Si

https://www.amazon.com/ap/signin?openid.assoc_handle=aws&openid.return_to=https%3A

Sign In or Create an AWS Account

You may sign in using your existing Amazon.com account or you can create a new account by selecting "I am a new user."

My e-mail address is: ____

○ **I am a new user.**

● **I am a returning user and my password is:** ____

Sign in using our secure server

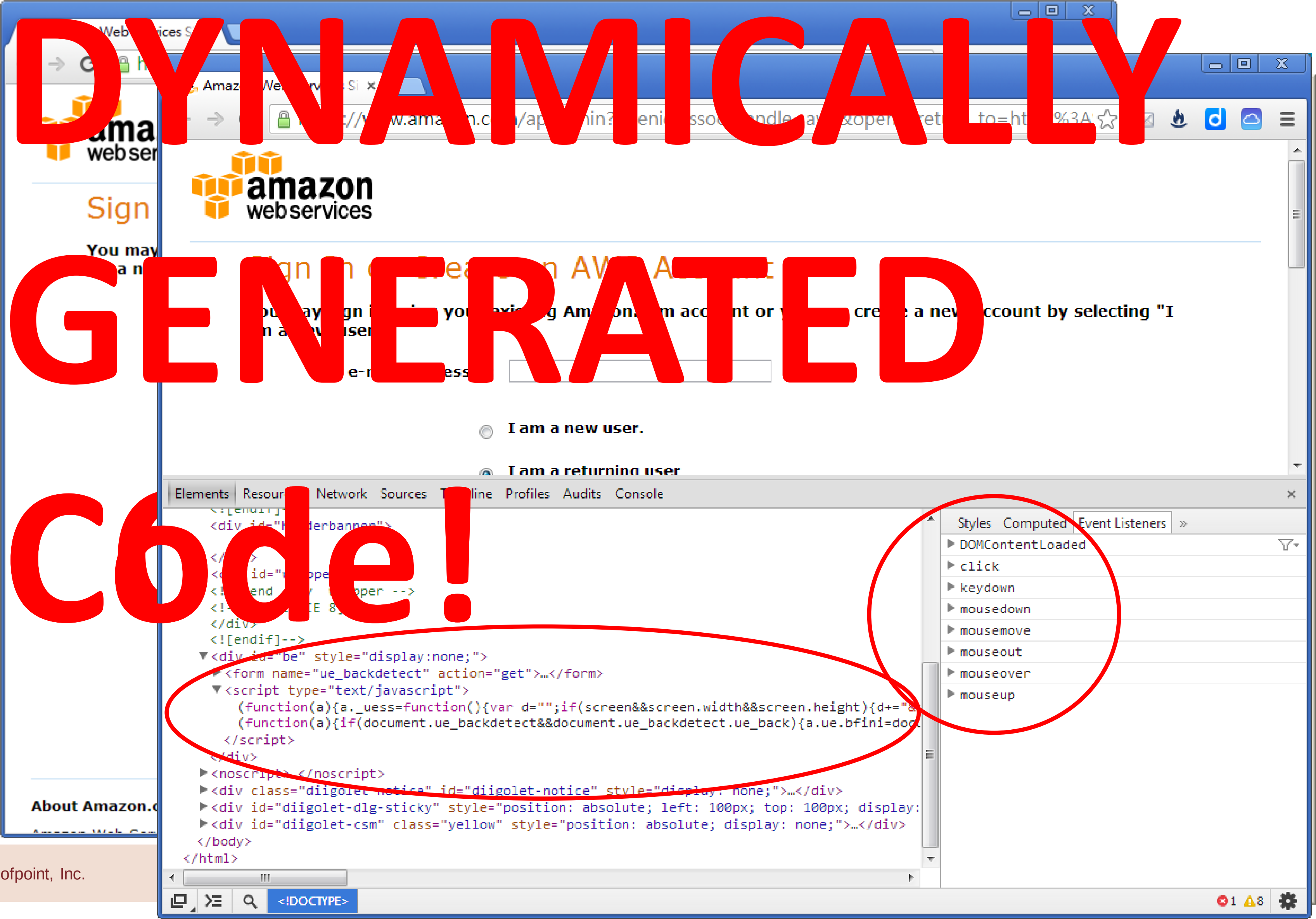
Forgot your password?

Has your e-mail address changed?

Learn more about AWS Identity and Access Management and AWS Multi-Factor Authentication, features that provide additional security for your AWS Account.

About Amazon.com Sign In

Scan against more detection vectors



DYNAMICALLY GENERATED C0de!

Sign In or Create an AWS Account

You may sign in using your existing Amazon.com account or you can create a new account by selecting "I am a new user."

My e-mail address is:

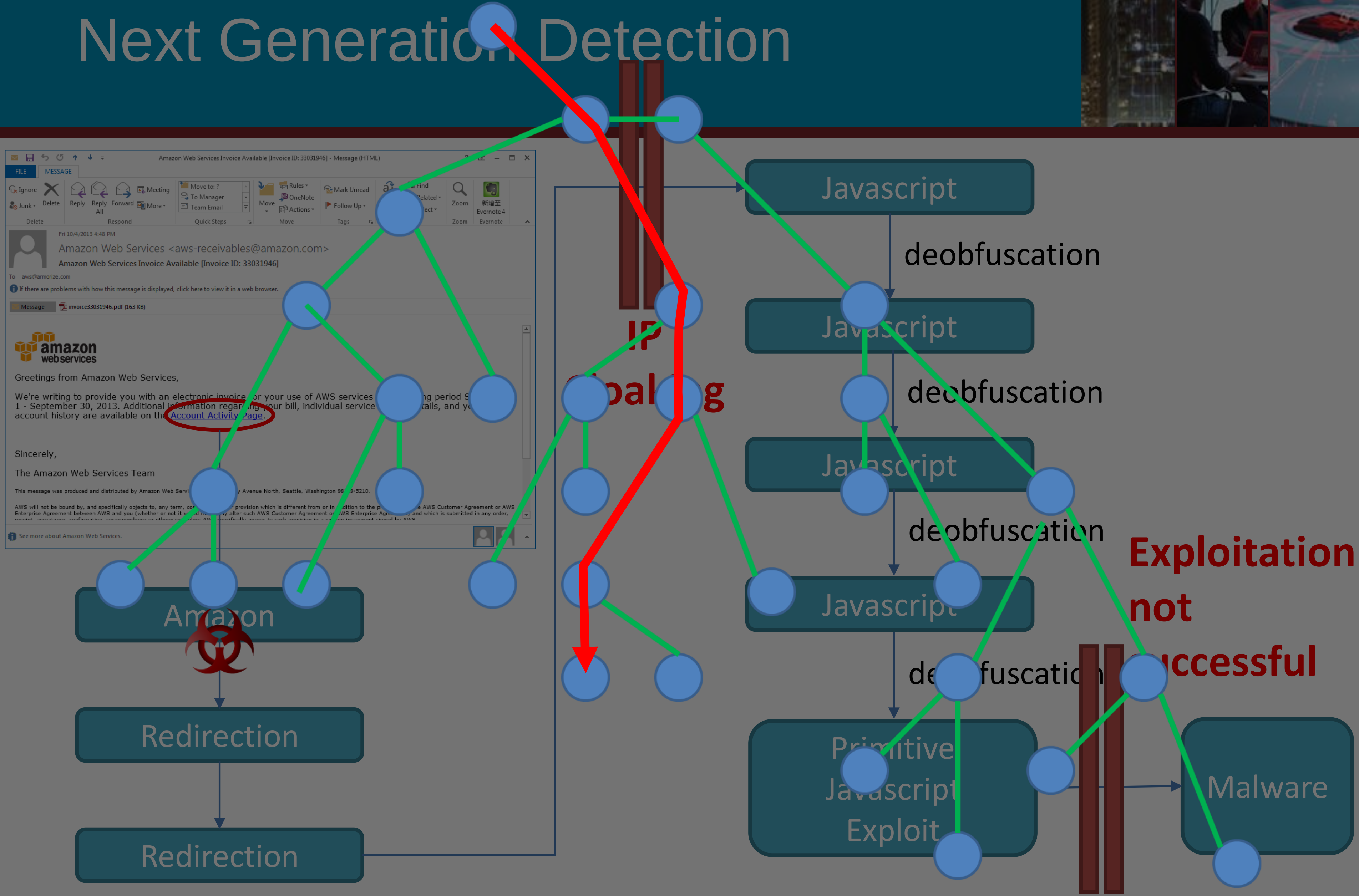
○ I am a new user.

● I am a returning user

```
<![endif]-->
<div id="headerbanner">
</div>
<div id="wrapper">
<!-- end of wrapper -->
<!--[if IE 8]>
</div>
<![endif]-->
▼<div id="be" style="display:none;">
  ▶<form name="ue_backdetect" action="get">…</form>
  ▼<script type="text/javascript">
      (function(a){a._uess=function(){var d="";if(screen&&screen.width&&screen.height){d+="&
      (function(a){if(document.ue_backdetect&&document.ue_backdetect.ue_back){a.ue.bfini=doc
    </script>
  </div>
▶<noscript>…</noscript>
▶<div class="diigolet notice" id="diigolet-notice" style="display: none;">…</div>
▶<div id="diigolet-dlg-sticky" style="position: absolute; left: 100px; top: 100px; display:
▶<div id="diigolet-csm" class="yellow" style="position: absolute; display: none;">…</div>
</body>
</html>
```

```
▶ DOMContentLoaded
▶ click
▶ keydown
▶ mousedown
▶ mousemove
▶ mouseout
▶ mouseover
▶ mouseup
```

Next Generation Detection



Amazon Web Services Invoice Available [Invoice ID: 33031946] - Message (HTML)

Fri 10/4/2013 4:48 PM

Amazon Web Services <aws-receivables@amazon.com>

Amazon Web Services Invoice Available [Invoice ID: 33031946]

To aws@armorize.com

If there are problems with how this message is displayed, click here to view it in a web browser.

invoice33031946.pdf (163 KB)

Greetings from Amazon Web Services,

We're writing to provide you with an electronic invoice for your use of AWS services [illegible] ng period S 1 - September 30, 2013. Additional information regarding your bill, individual service [illegible] tails, and yo account history are available on the Account Activity Page.

Sincerely,

The Amazon Web Services Team

This message was produced and distributed by Amazon Web Servi [illegible] y Avenue North, Seattle, Washington 98 [illegible] 9-5210.

AWS will not be bound by, and specifically objects to, any term, co [illegible] provision which is different from or in addition to the p [illegible] e AWS Customer Agreement or AWS Enterprise Agreement between AWS and you (whether or not it w [illegible] ly alter such AWS Customer Agreement or AWS Enterprise Agre [illegible] and which is submitted in any order,

See more about Amazon Web Services.

Amazon

Redirection

Redirection

IP cloaking

Javascript

deobfuscation

Javascript

deobfuscation

Javascript

deobfuscation

Javascript

deobfuscation

Primitive Javascript Exploit

Exploitation not successful

Malware

Conclusion 2

- For every vulnerability, there is usually __1__ number of different implementations
- Even traditional antivirus has every exploit’s signature
- All we need to do, is match against the final code
  - Dynamically generated code
- And apply behavioral analysis for the zerodays

proofpoint™

Q&A

threat protection | compliance | archiving | secure communication

Contact us at:
sales@proofpoint.com

408-517-4710
www.proofpoint.com

For more Information

2014 Targeted Attacks Study
THE NEW ART OF WAR
How to Detect, Predict and Eliminate Advanced Targeted Threats
INSIDE:
Survey Results
Analysis
Expert Commentary
proofpoint
ISMG

For More Information,
Contact us at:
sales@proofpoint.com

408-517-4710
www.proofpoint.com

The New Art of War: 2014 Targeted Attacks Study

How to Detect, Predict and Eliminate Advanced Targeted Threats

This 2014 Targeted Attacks Study looks at the specific threats organizations face today; where traditional security approaches are failing; and what advanced tools organizations are investing in over the year ahead..
In this study, you'll receive a comprehensive overview of survey results and expert analysis on:

- The common threats organizations face
- Where to bolster traditional defenses
- How to protect employees from targeted attacks

Visit the link below to download this report, compliments of Proofpoint:

http://www.proofpoint.com/id/2014-targeted-attacks-study/index.php?id=1