The dark side of Online Advertising

Daniel Chechik, Rami Kogan

Trustwave®
Smart security on demand

YouTube
msn
DRUDGE REPORT
The Weather Channel
YAHOO!
TMZ
The Pirate Bay
THE HUFFINGTON POST
Daily Mail
POF
xfinity
REALTOR®
Answers.com®
{LIFE}BUZZ
dailymotion
YouPorn
Rotten Tomatoes™
Pornhub
Legacy.com®
Forbes

Few things in common

- Popular
- Free content
- Advertising
- Malicious

Malicious Advertising

Malvertising

Types

Trustwave®

Malvertising

Types

- Paid ads in search engines
- Deceptive downloads
- Drive-by downloads

Trustwave®
Smart security on demand

Malvertising

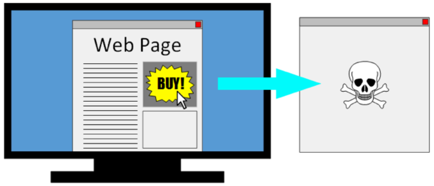
Types

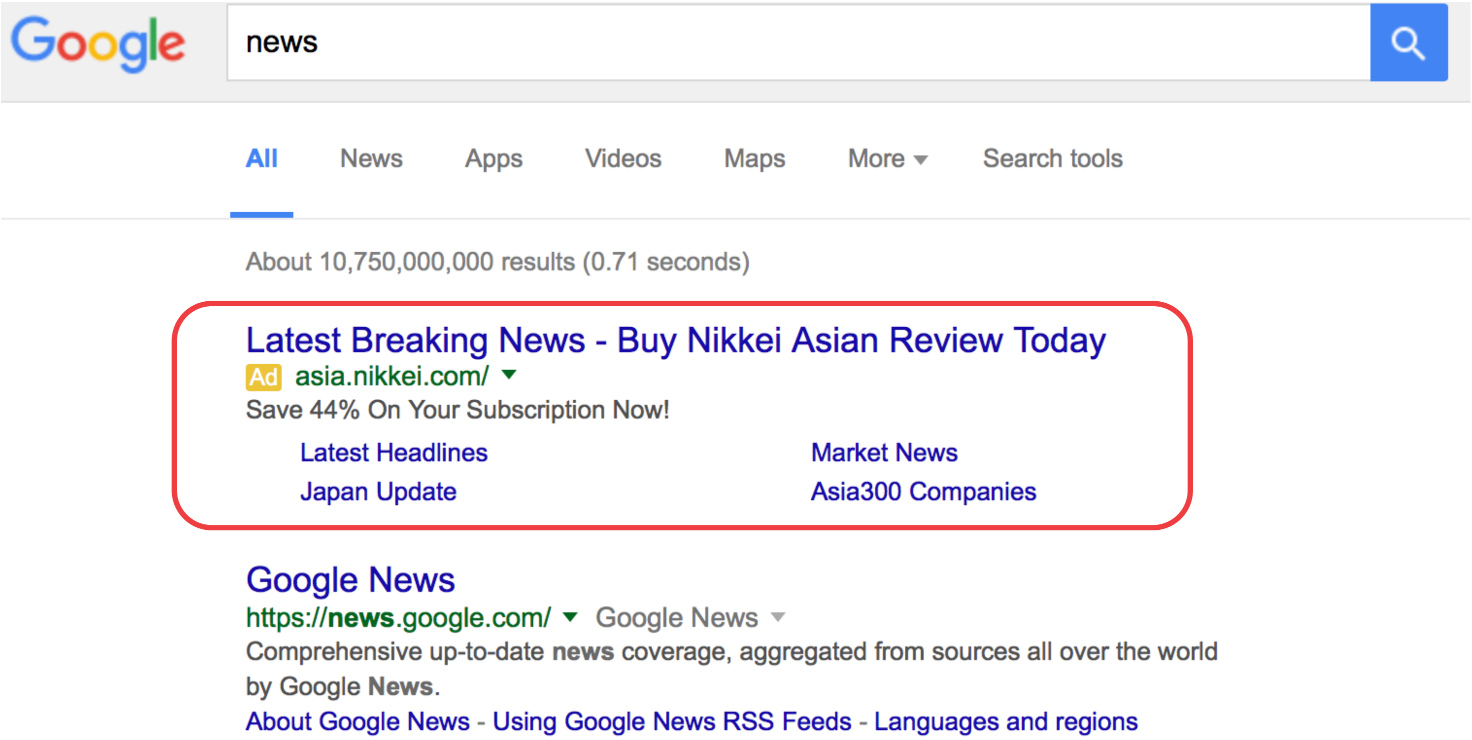
User Interaction	Drive By Downloads
Malicious paid ads in search engines	Malicious Flash
Deceptive downloads	Hidden iframes
	Pop unders

Trustwave®
Smart security on demand

User Interaction

Malicious ads in search engines





Google

news

All News Apps Videos Maps More ▾ Search tools

About 10,750,000,000 results (0.71 seconds)

Latest Breaking News - Buy Nikkei Asian Review Today
Ad asia.nikkei.com/ ▾
Save 44% On Your Subscription Now!

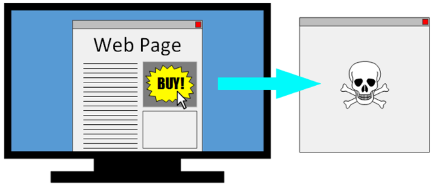
Latest Headlines	Market News
Japan Update	Asia300 Companies

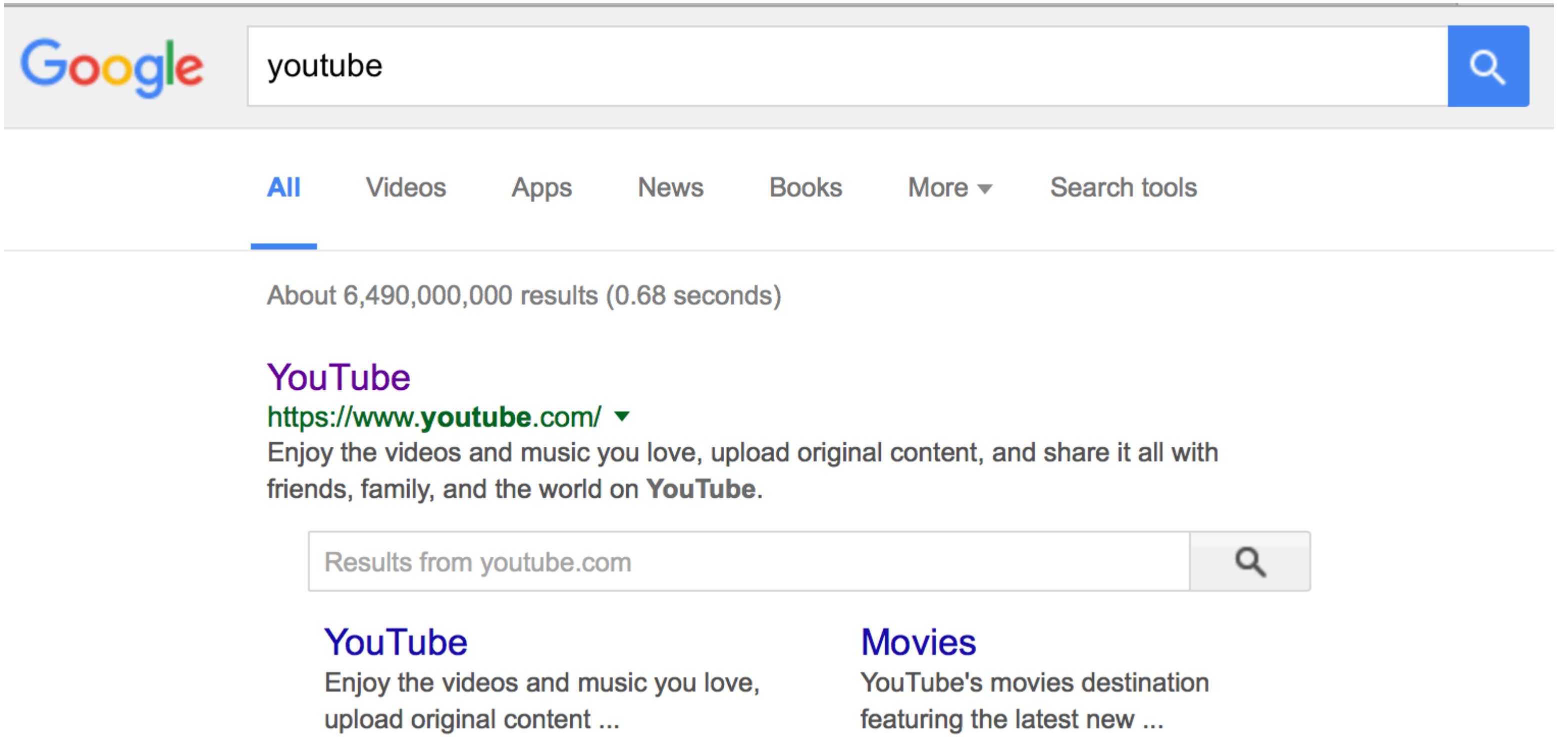
Google News
https://**news**.google.com/ ▾ Google News ▾
Comprehensive up-to-date **news** coverage, aggregated from sources all over the world by Google **News**.
About Google News - Using Google News RSS Feeds - Languages and regions

Trustwave®
Smart security on demand

User Interaction

Malicious ads in search engines





About 6,490,000,000 results (0.68 seconds)

YouTube
https://www.youtube.com/
Enjoy the videos and music you love, upload original content, and share it all with friends, family, and the world on **YouTube**.

Results from youtube.com

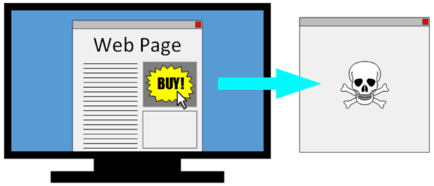
YouTube
Enjoy the videos and music you love, upload original content ...

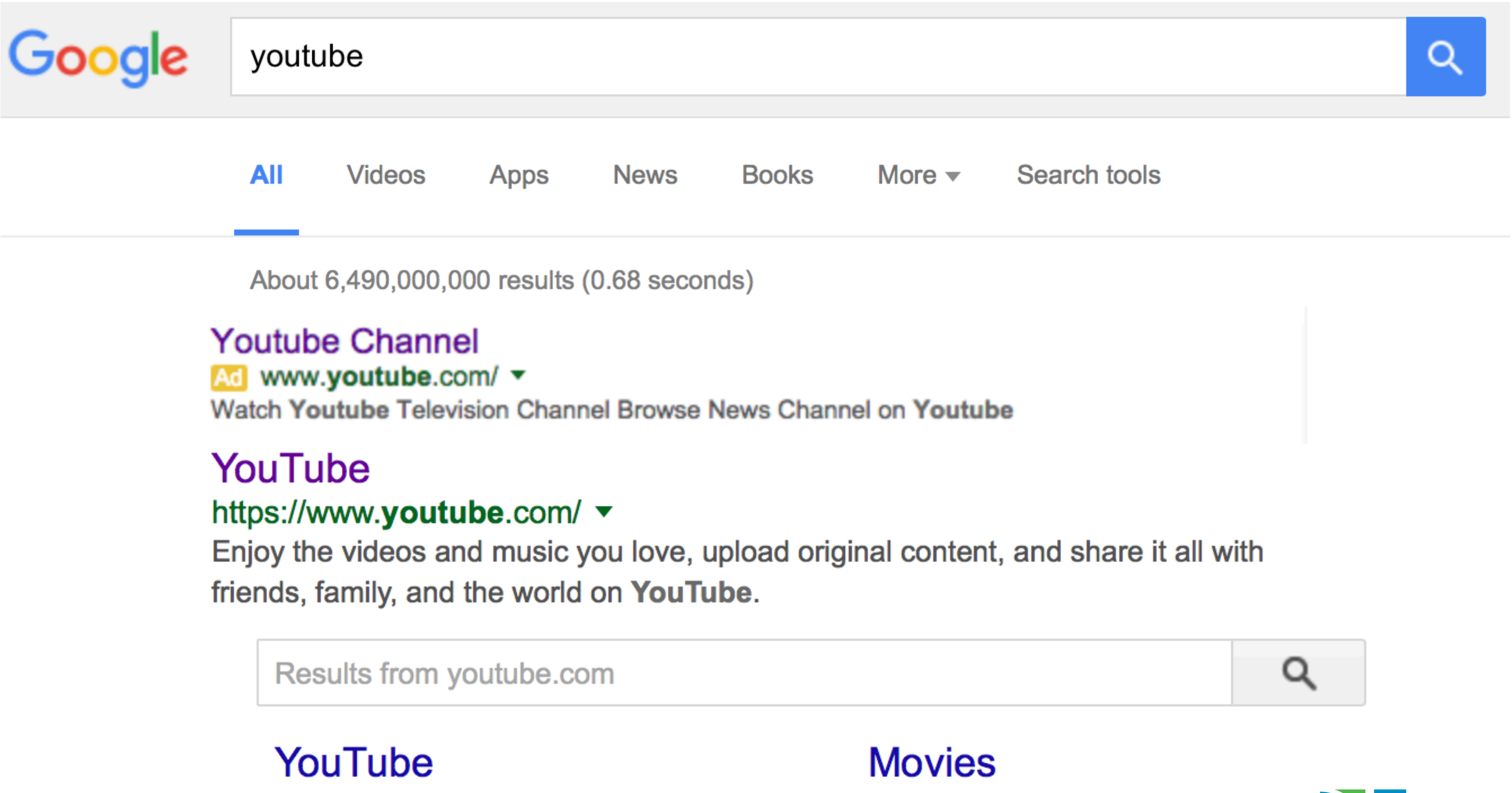
Movies
YouTube's movies destination featuring the latest new ...

Trustwave®
Smart security on demand

User Interaction

Malicious ads in search engines





About 6,490,000,000 results (0.68 seconds)

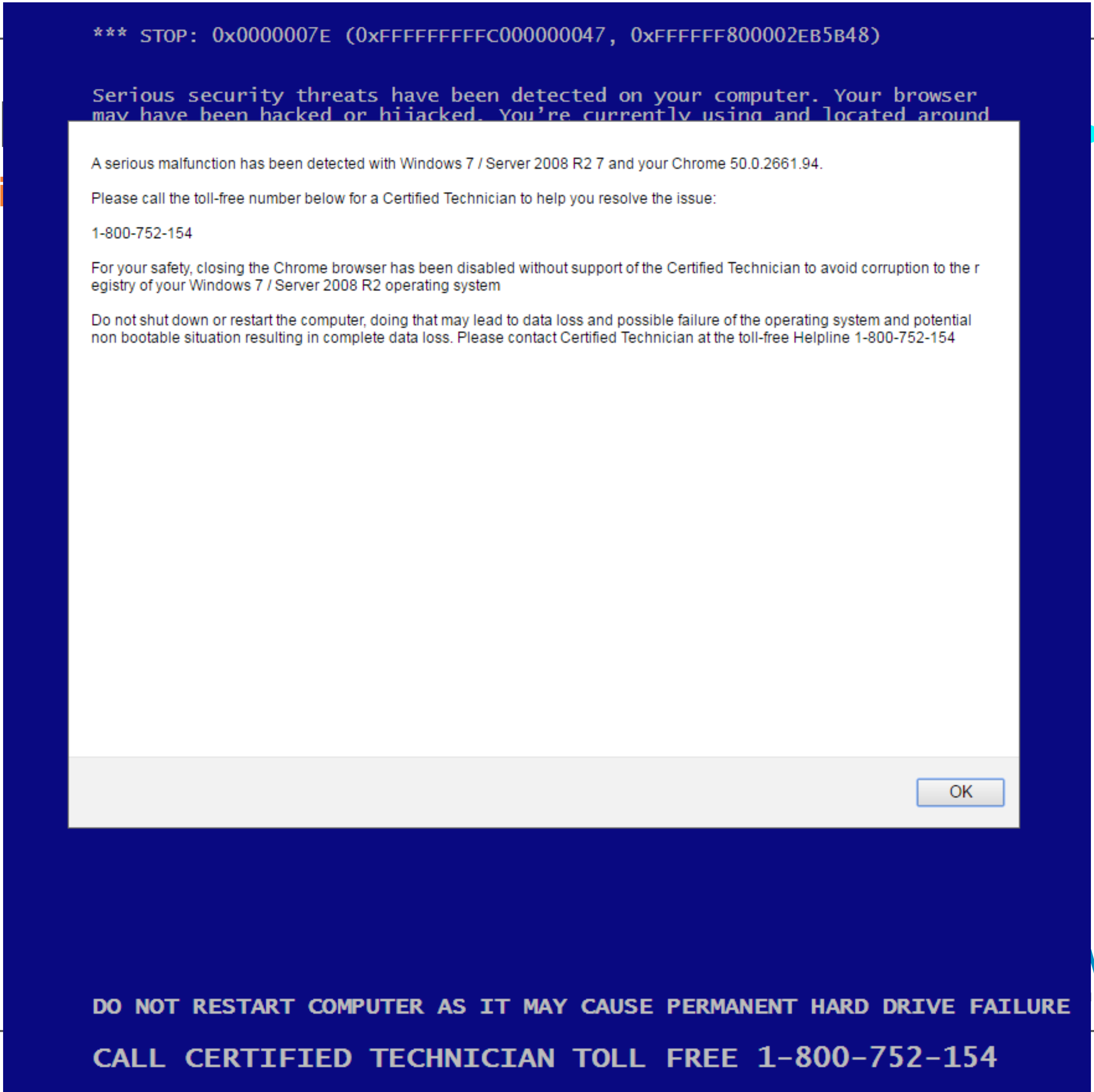
Youtube Channel
Ad www.**youtube**.com/
Watch **Youtube** Television Channel Browse News Channel on **Youtube**

YouTube
https://www.**youtube**.com/
Enjoy the videos and music you love, upload original content, and share it all with friends, family, and the world on **YouTube**.

Trustwave®
Smart security on demand

Use

Malici



```
*** STOP: 0x0000007E (0xFFFFFFFFC000000047, 0xFFFFFF800002EB5B48)
```

Serious security threats have been detected on your computer. Your browser may have been hacked or hijacked. You're currently using and located around

A serious malfunction has been detected with Windows 7 / Server 2008 R2 7 and your Chrome 50.0.2661.94.

Please call the toll-free number below for a Certified Technician to help you resolve the issue:

1-800-752-154

For your safety, closing the Chrome browser has been disabled without support of the Certified Technician to avoid corruption to the r egistry of your Windows 7 / Server 2008 R2 operating system

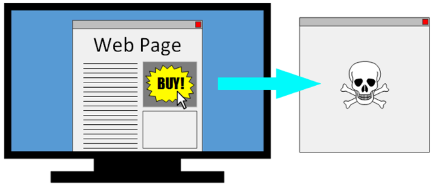
Do not shut down or restart the computer, doing that may lead to data loss and possible failure of the operating system and potential non bootable situation resulting in complete data loss. Please contact Certified Technician at the toll-free Helpline 1-800-752-154

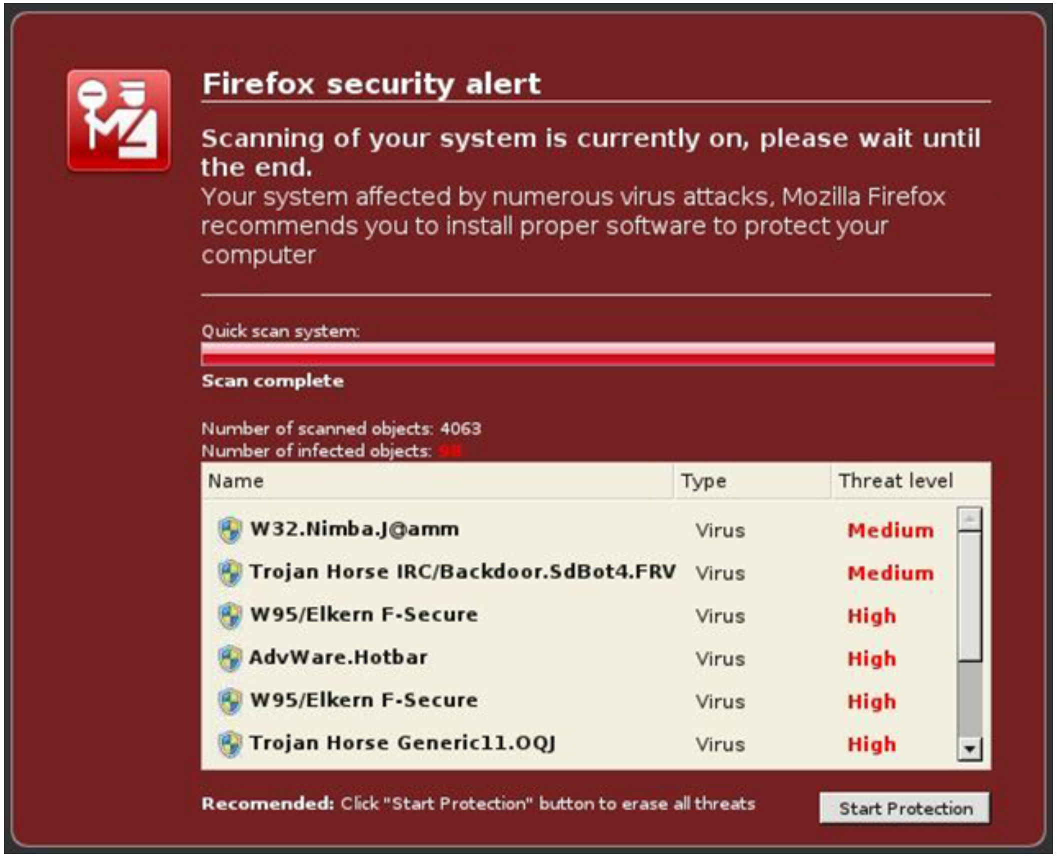
DO NOT RESTART COMPUTER AS IT MAY CAUSE PERMANENT HARD DRIVE FAILURE

CALL CERTIFIED TECHNICIAN TOLL FREE 1-800-752-154

User Interaction

Deceptive Downloads – Fake AV





Firefox security alert

Scanning of your system is currently on, please wait until the end.
Your system affected by numerous virus attacks, Mozilla Firefox recommends you to install proper software to protect your computer

Quick scan system:

Scan complete

Number of scanned objects: 4063
Number of infected objects: 98

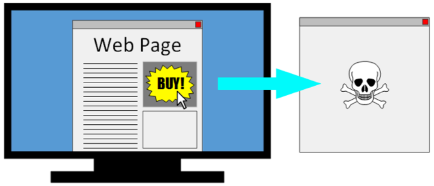
Name	Type	Threat level
W32.Nimba.J@amm	Virus	**Medium**
Trojan Horse IRC/Backdoor.SdBot4.FRV	Virus	**Medium**
W95/Elkern F-Secure	Virus	**High**
AdvWare.Hotbar	Virus	**High**
W95/Elkern F-Secure	Virus	**High**
Trojan Horse Generic11.OQJ	Virus	**High**

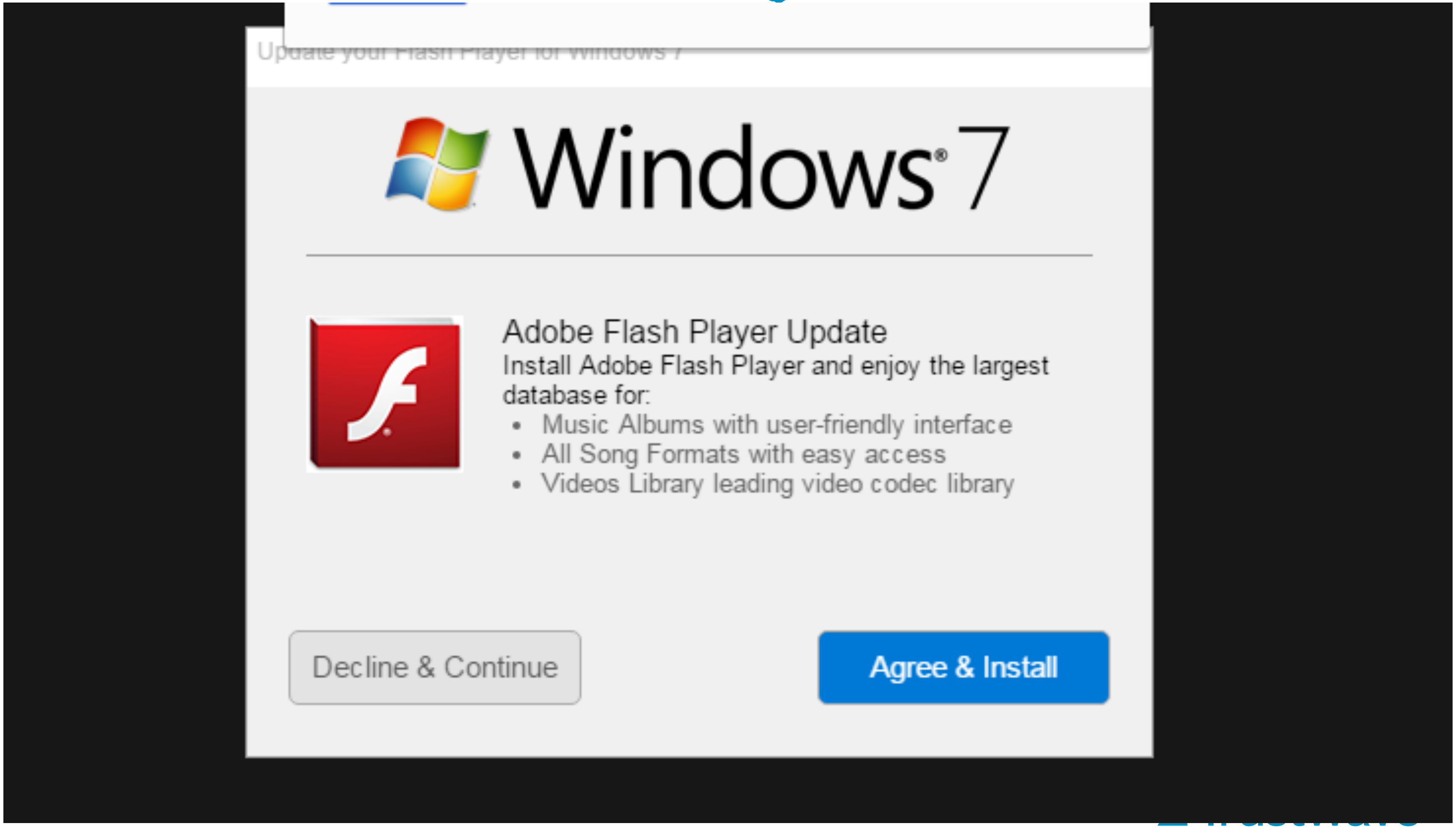
Recomended: Click "Start Protection" button to erase all threats

Trustwave®
Smart security on demand

User Interaction

Deceptive Downloads – Fake Plugin





Update your Flash Player for Windows 7

Adobe Flash Player Update

Install Adobe Flash Player and enjoy the largest database for:

- Music Albums with user-friendly interface
- All Song Formats with easy access
- Videos Library leading video codec library

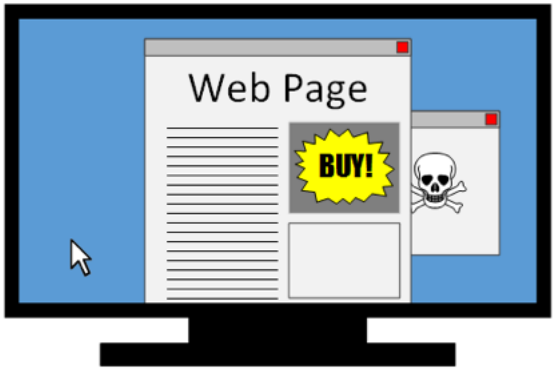
User Interaction

Trustwave®
Smart security on demand

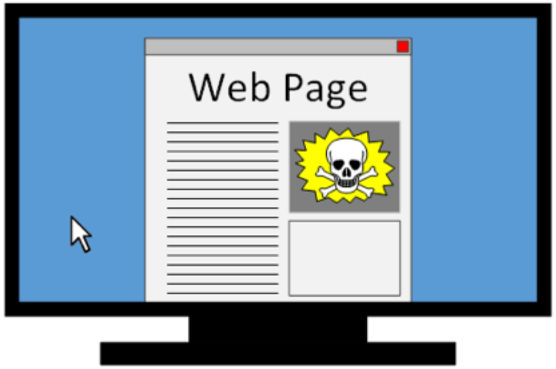
No User Interaction

Drive-By Downloads - The silent killer

- **Pop Under**



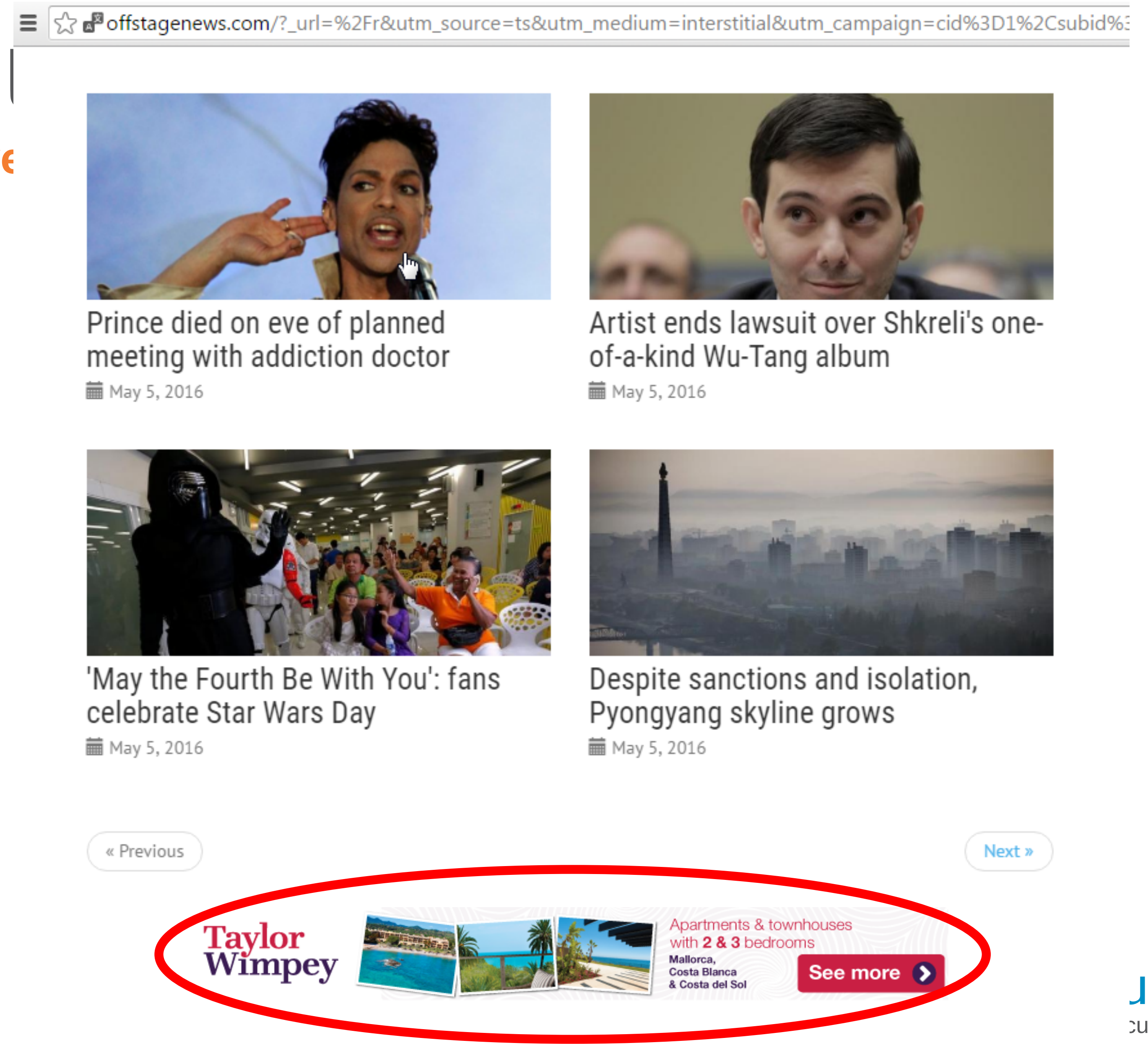
- **Iframe/Flash/JS**



Trustwave®
Smart security on demand

No

Drive



offstagenews.com/?_url=%2Fr&utm_source=ts&utm_medium=interstitial&utm_campaign=cid%3D1%2Csubid%3

Prince died on eve of planned meeting with addiction doctor
May 5, 2016

Artist ends lawsuit over Shkreli's one-of-a-kind Wu-Tang album
May 5, 2016

'May the Fourth Be With You': fans celebrate Star Wars Day
May 5, 2016

Despite sanctions and isolation, Pyongyang skyline grows
May 5, 2016

« Previous

Next »

Taylor Wimpey

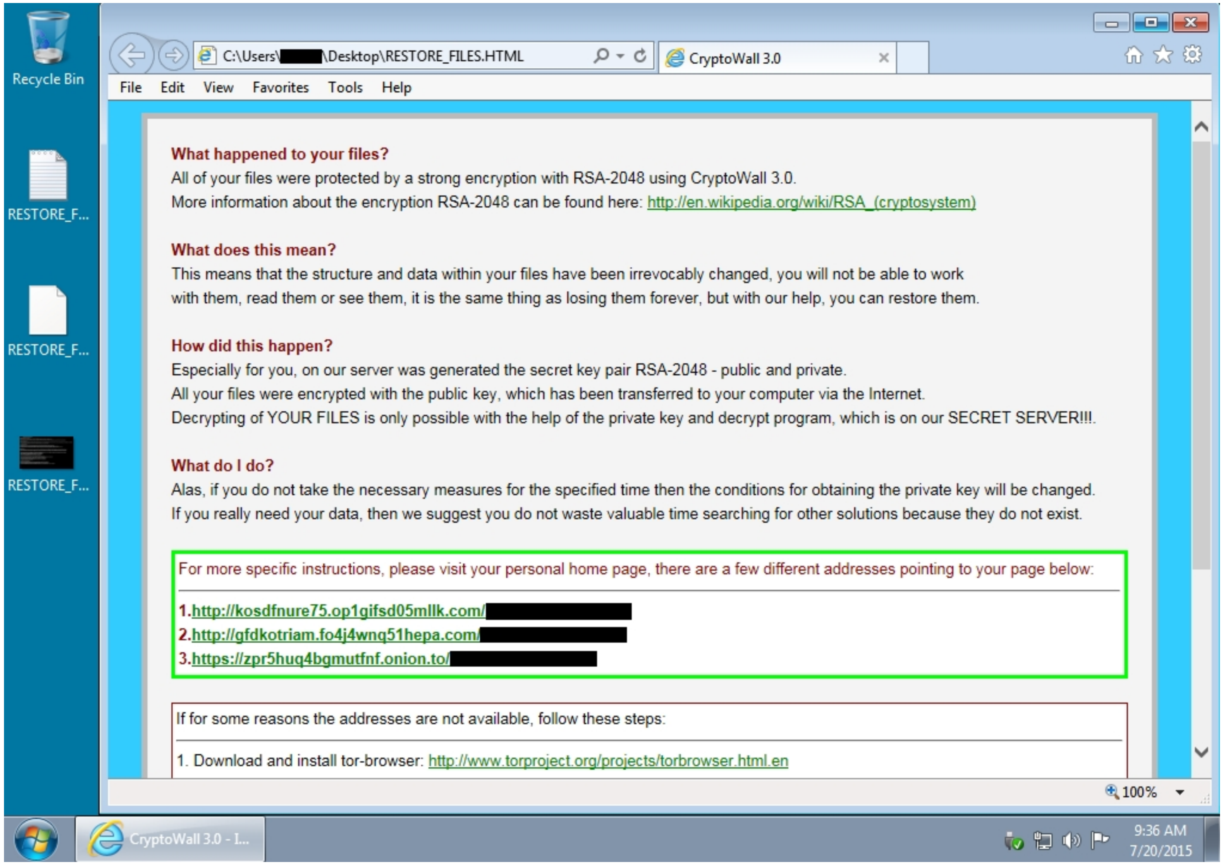
Apartments & townhouses with **2 & 3** bedrooms

Mallorca,
Costa Blanca
& Costa del Sol

See more

No User Interaction

Drive-By Downloads – The silent killer



What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0.
More information about the encryption 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 need 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.http://kosdfnure75.op1gifsd05mllk.com/[redacted]
2.http://gfdkotriam.fo4j4wnq51hepa.com/[redacted]
3.https://zpr5huq4bgmutfnf.onion.to/[redacted]

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

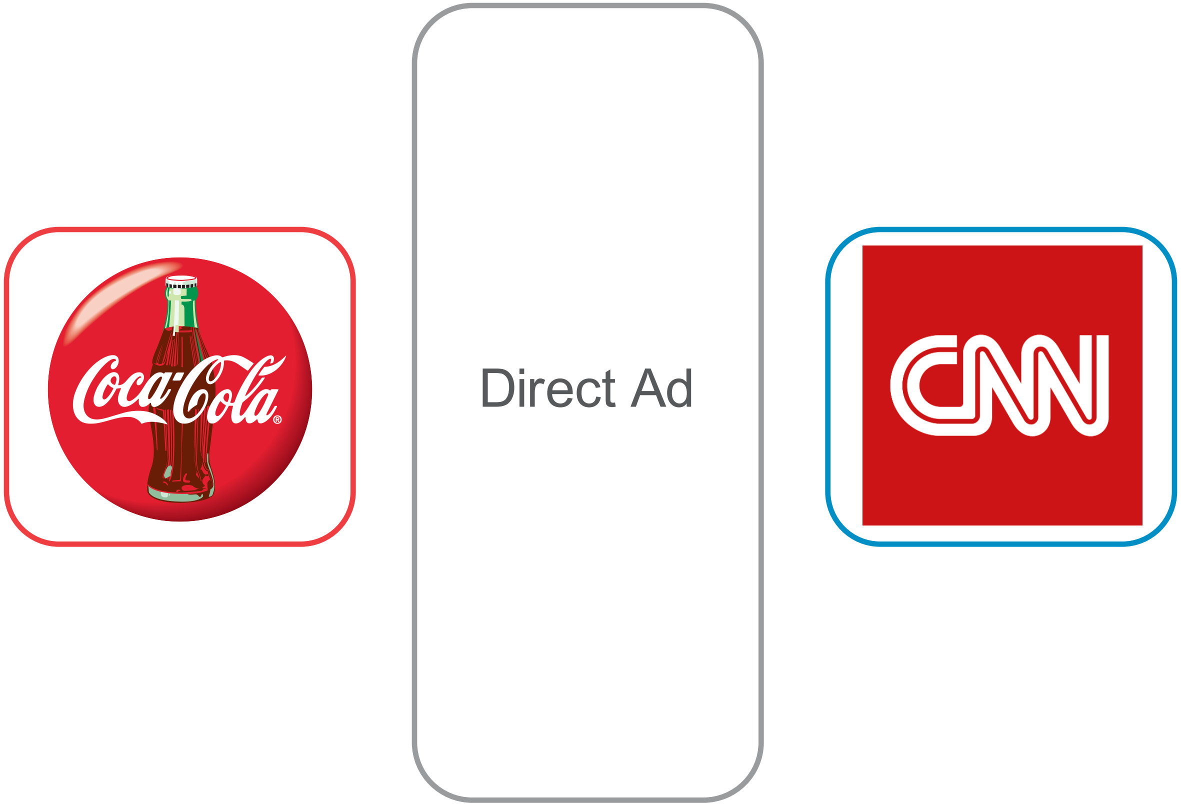
Trustwave®
Smart security on demand

How?

Trustwave®

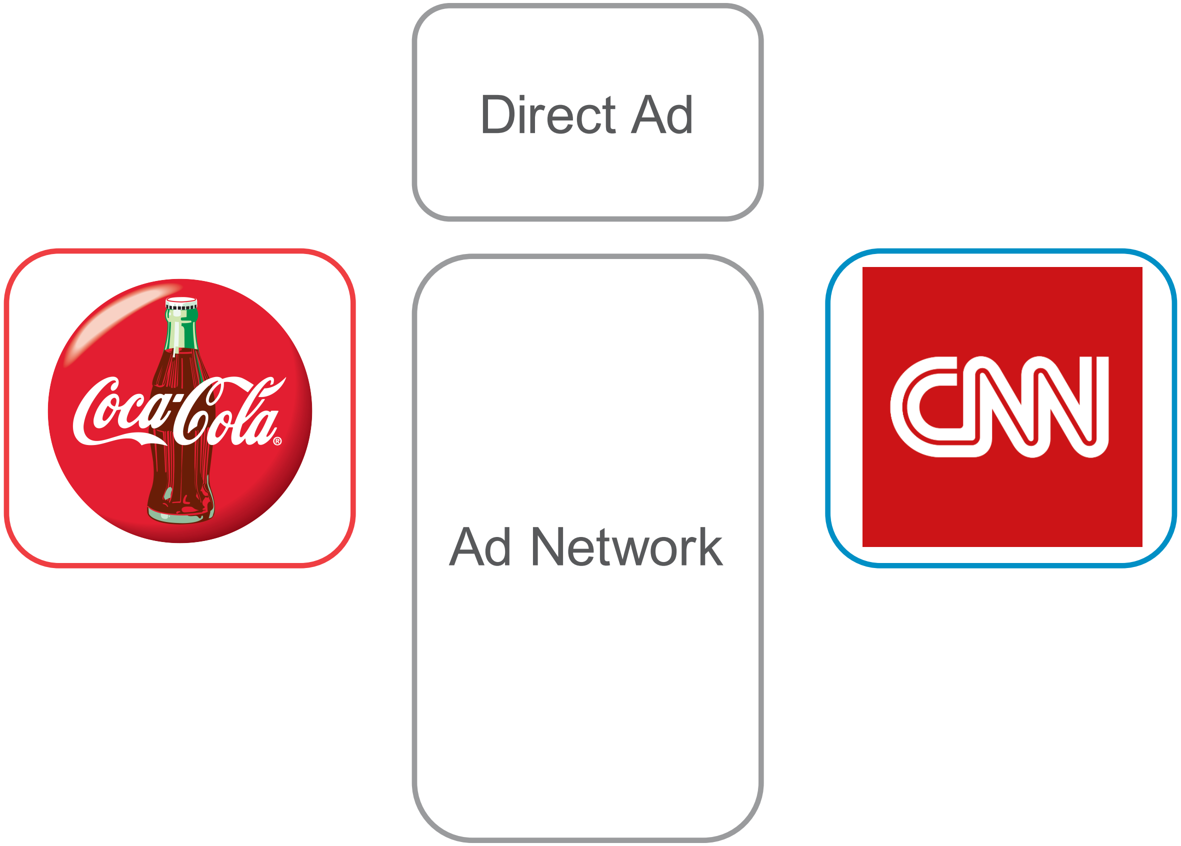
Advertising Eco-System

Direct Advertising



Advertising Eco-System

Advertising through Ad Agencies

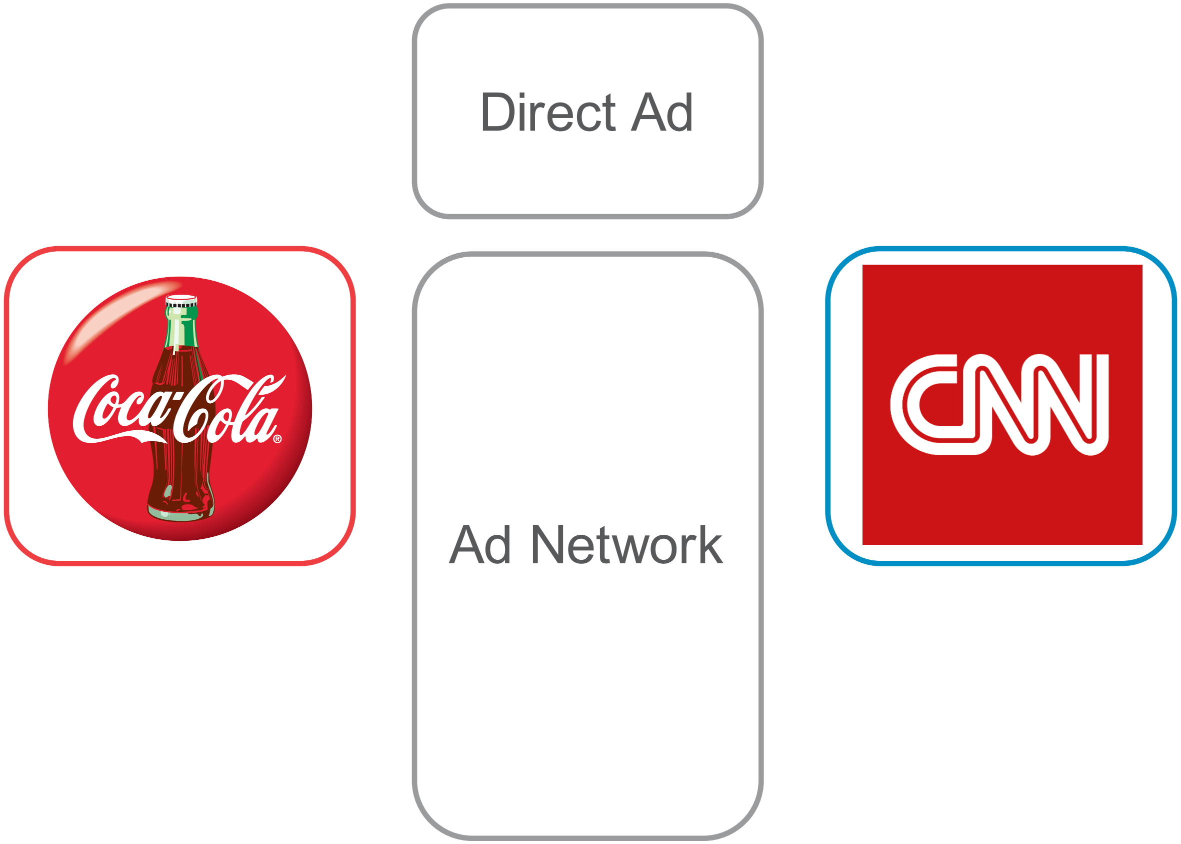


Direct Ad

Ad Network

Advertising Eco-System

Advertising through Ad Agencies

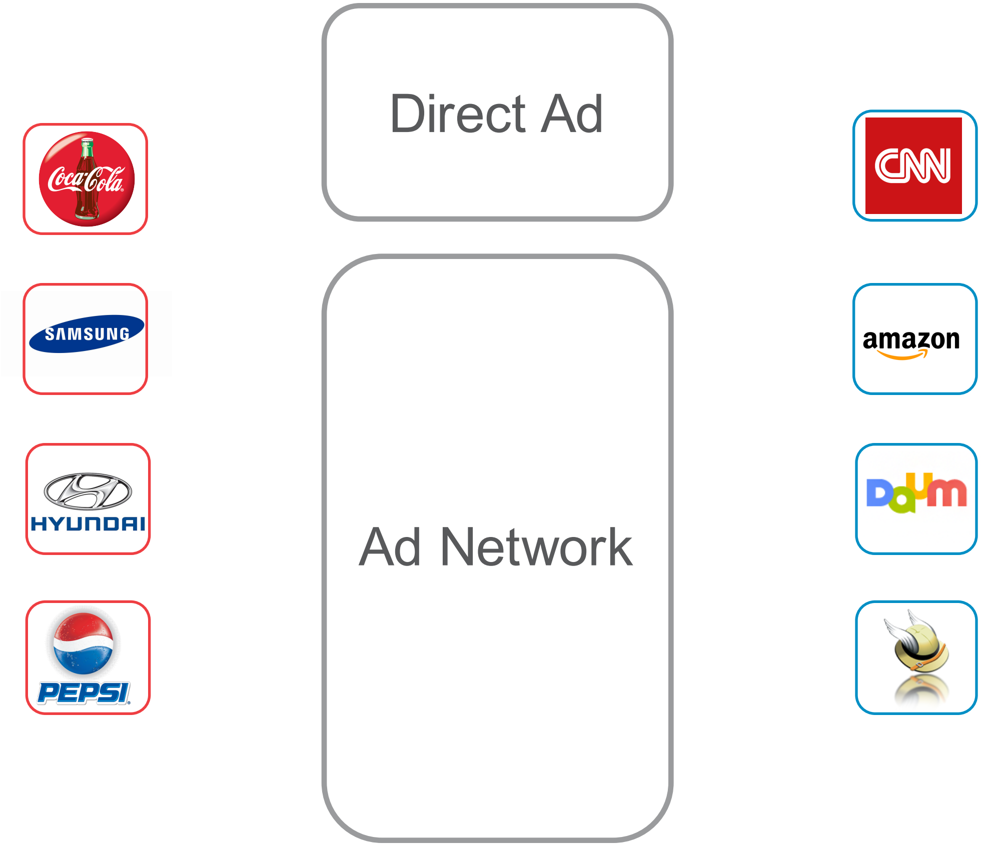


Direct Ad

Ad Network

Advertising Eco-System

Advertising through Ad Agencies

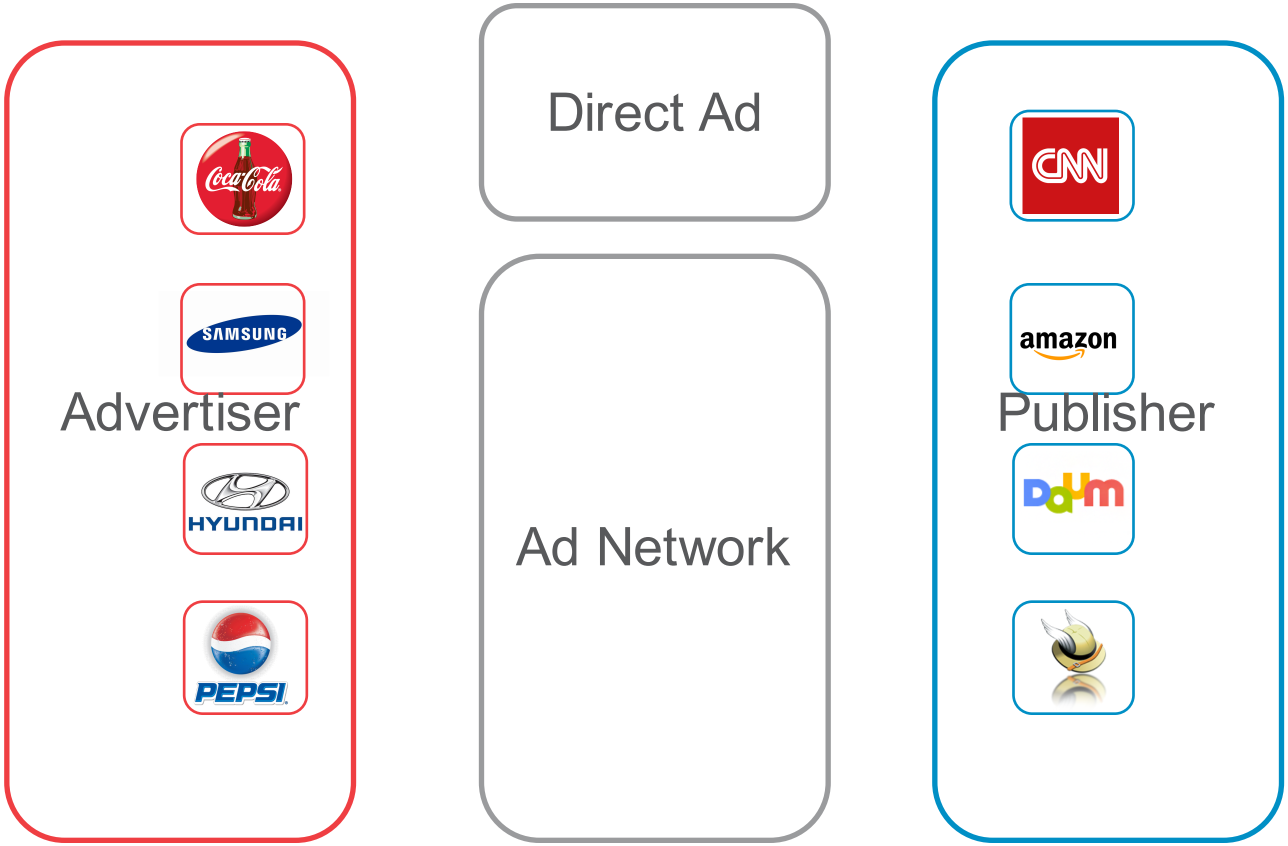


Direct Ad

Ad Network

Advertising Eco-System

Advertising through Ad Agencies



Advertiser

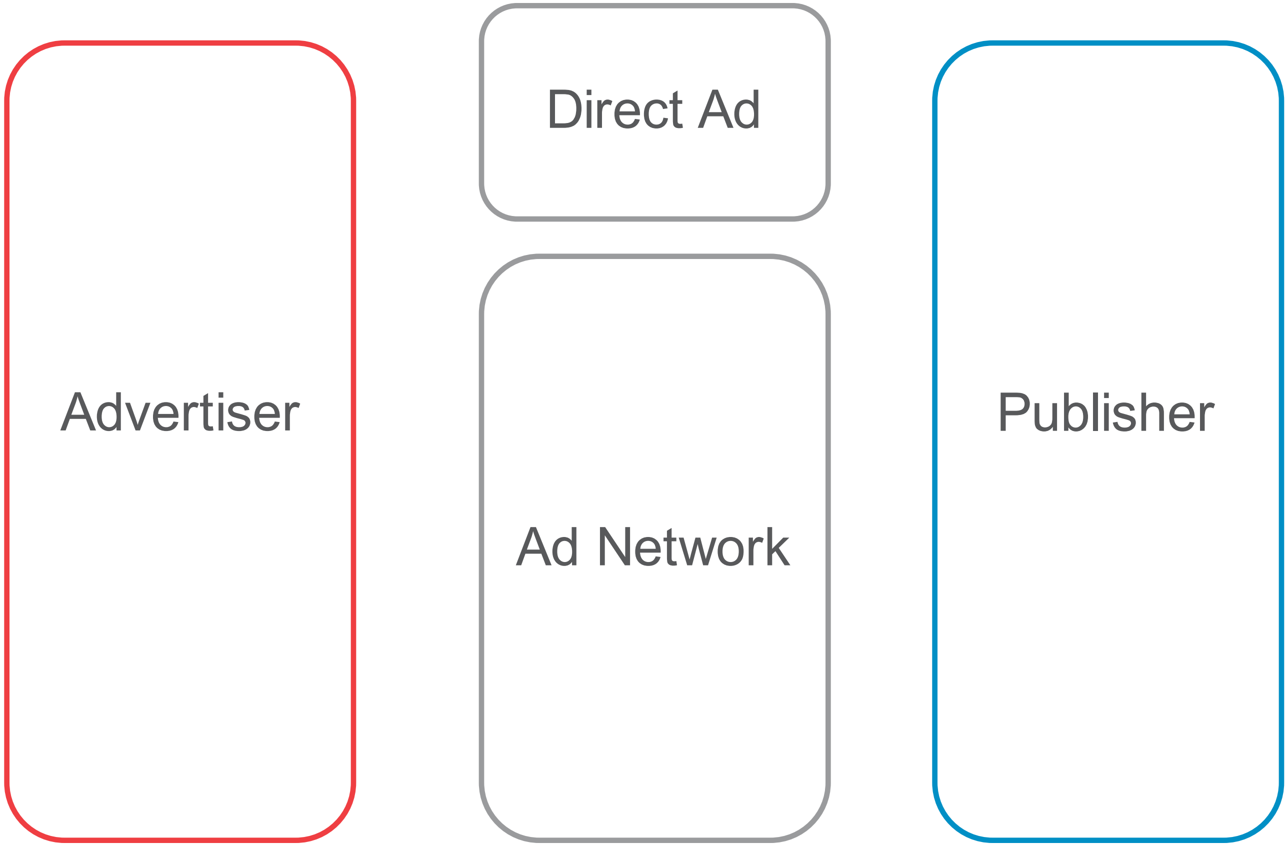
Direct Ad

Ad Network

Publisher

Advertising Eco-System

Advertising through Ad Agencies



Direct Ad

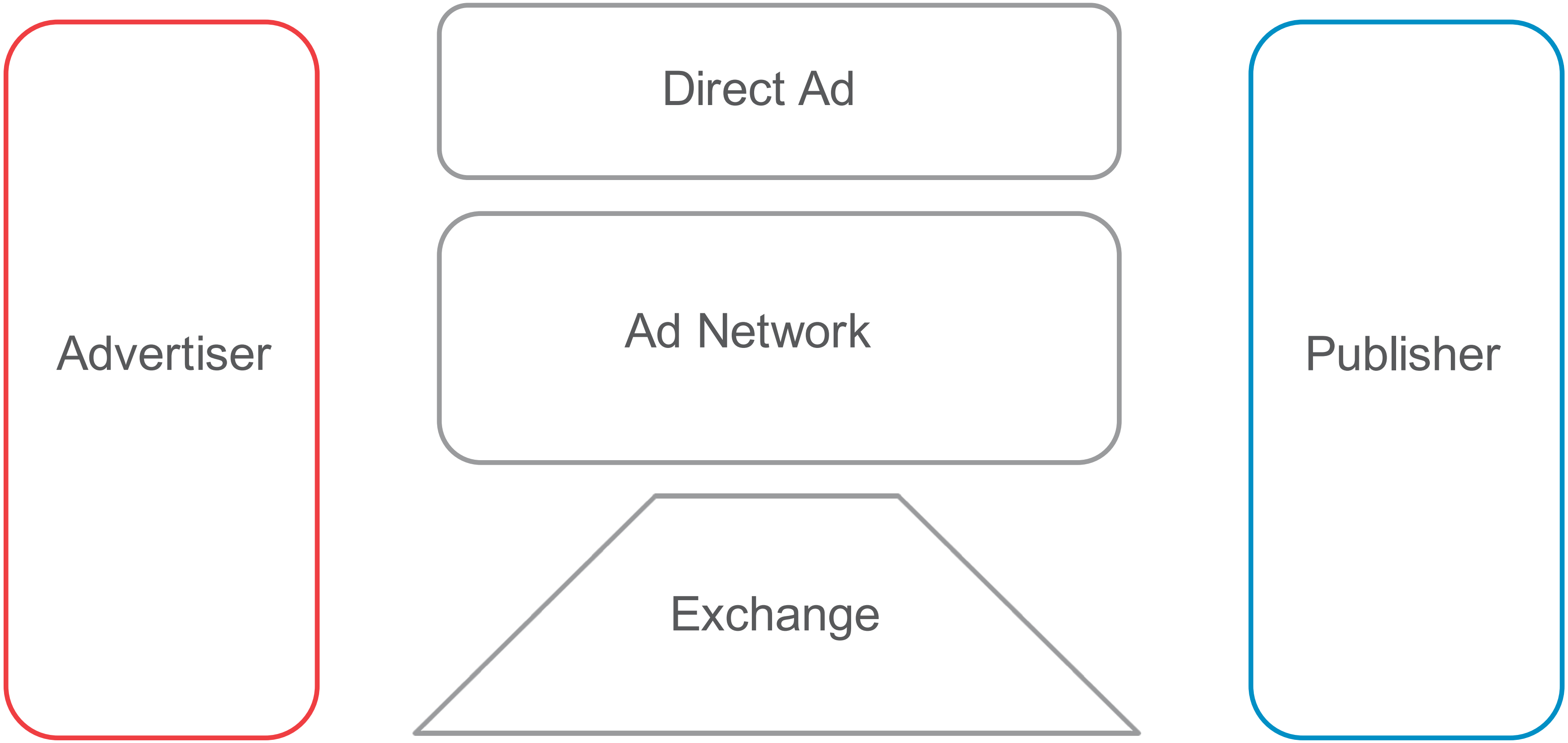
Advertiser

Ad Network

Publisher

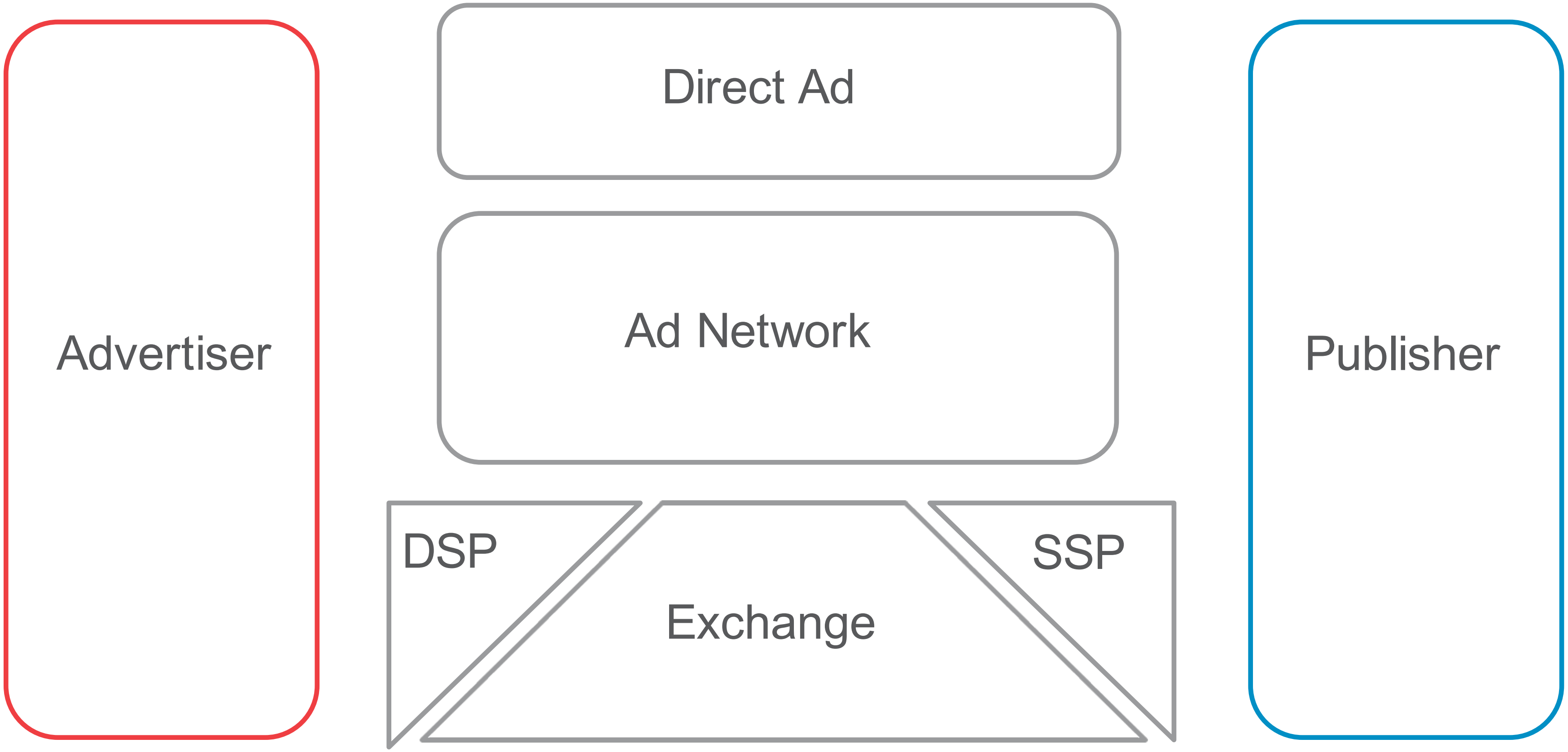
Advertising Eco-System

Exchange Services



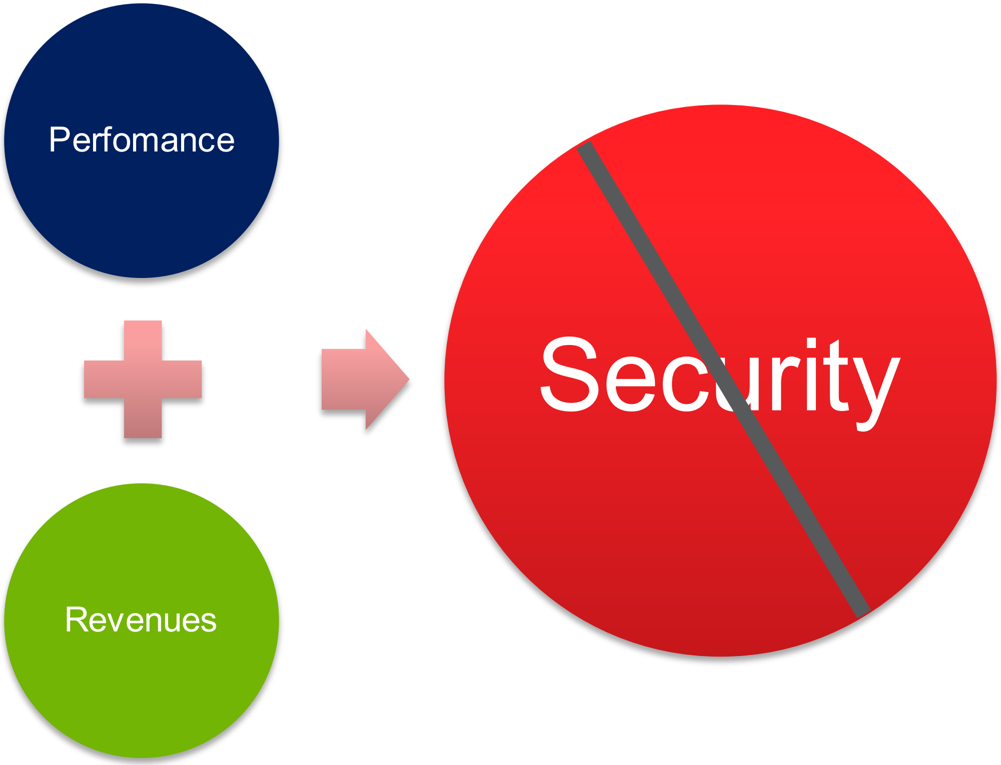
Advertising Eco-System

DSP and SSP



Malvertising

Online advertisement ecosystem – The Problem



Trustwave®
Smart security on demand

Malvertising

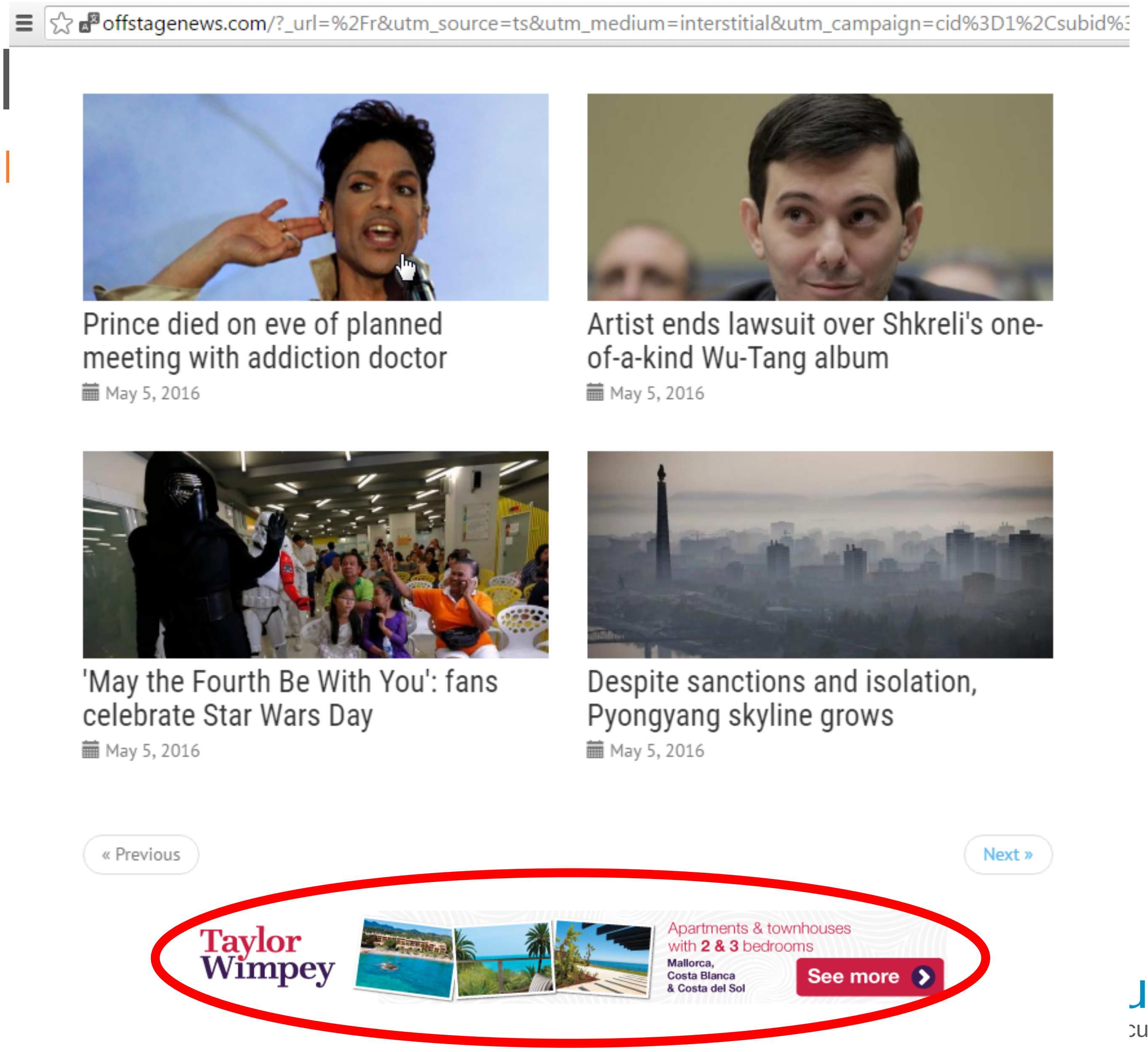
Online advertisement ecosystem – The Problem

- RTB takes less than 100 milliseconds
- DSPs ”fight” to respond faster
- Too fast to validate ads

Trustwave®
Smart security on demand

Mal

Sam



offstagenews.com/?_url=%2Fr&utm_source=ts&utm_medium=interstitial&utm_campaign=cid%3D1%2Csubid%3

Prince died on eve of planned meeting with addiction doctor

May 5, 2016

Artist ends lawsuit over Shkreli's one-of-a-kind Wu-Tang album

May 5, 2016

'May the Fourth Be With You': fans celebrate Star Wars Day

May 5, 2016

Despite sanctions and isolation, Pyongyang skyline grows

May 5, 2016

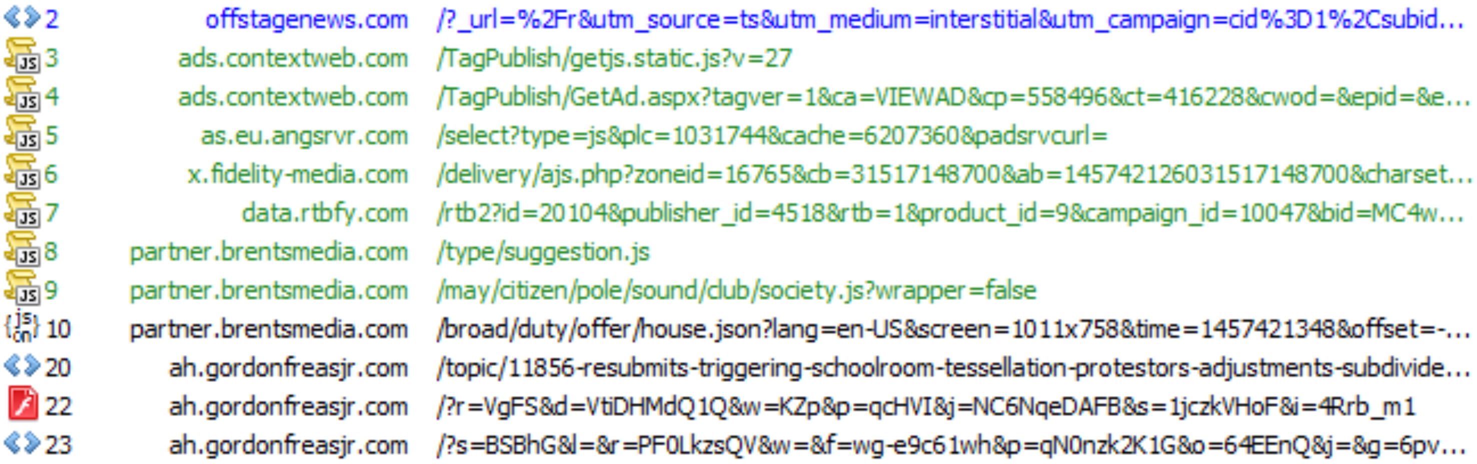
« Previous

Next »

Taylor Wimpey
Apartments & townhouses with 2 & 3 bedrooms
Mallorca, Costa Blanca & Costa del Sol
See more

Malvertising

Malvertising Infection Chain

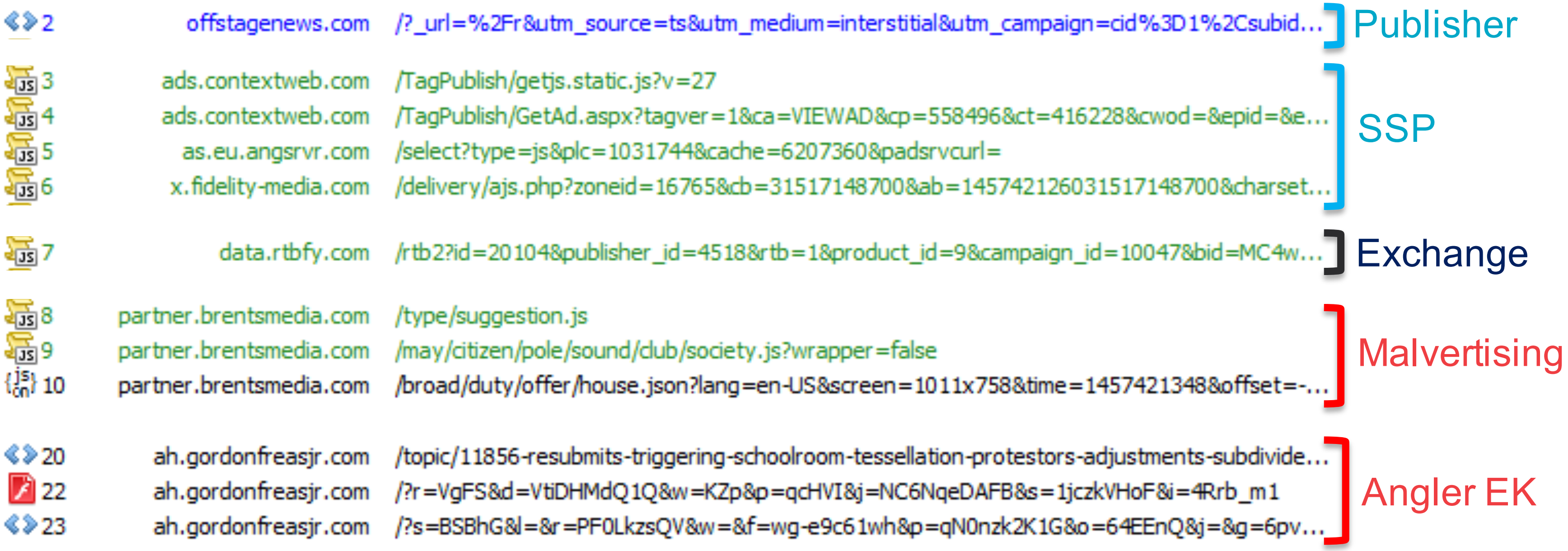


```
2   offstagenews.com          /?_url=%2Fr&utm_source=ts&utm_medium=interstitial&utm_campaign=cid%3D1%2Csubid...
3   ads.contextweb.com        /TagPublish/getjs.static.js?v=27
4   ads.contextweb.com        /TagPublish/GetAd.aspx?tagver=1&ca=VIEWAD&cp=558496&ct=416228&cwod=&epid=&e...
5   as.eu.angsrvr.com         /select?type=js&plc=1031744&cache=6207360&padsrvcurl=
6   x.fidelity-media.com      /delivery/ajs.php?zoneid=16765&cb=31517148700&ab=14574212603151714870 0&charset...
7   data.rtbfy.com            /rtb2?id=20104&publisher_id=4518&rtb=1&product_id=9&campaign_id=10047&bid=MC4w...
8   partner.brentsmedia.com   /type/suggestion.js
9   partner.brentsmedia.com   /may/citizen/pole/sound/club/society.js?wrapper=false
10  partner.brentsmedia.com   /broad/duty/offer/house.json?lang=en-US&screen=1011x758&time=1457421348&offset=-...
20  ah.gordonfreasjr.com      /topic/11856-resubmits-triggering-schoolroom-tessellation-protestors-adjustments-subdivide...
22  ah.gordonfreasjr.com      /?r=VgFS&d=VtiDHMdQ1Q&w=KZp&p=qcHVI&j=NC6NqeDAFB&s=1jczkVHoF&i=4Rrb_m1
23  ah.gordonfreasjr.com      /?s=BSBhG&l=&r=PF0LkzsQV&w=&f=wg-e9c61wh&p=qN0nzk2K1G&o=64EEnQ&j=&g=6pv...
```

Trustwave®
Smart security on demand

Malvertising

Infection Chain in



```
2          offstagenews.com  /?_url=%2Fr&utm_source=ts&utm_medium=interstitial&utm_campaign=cid%3D1%2Csubid...
3         ads.contextweb.com  /TagPublish/getjs.static.js?v=27
4         ads.contextweb.com  /TagPublish/GetAd.aspx?tagver=1&ca=VIEWAD&cp=558496&ct=416228&cwod=&epid=&e...
5           as.eu.angsrvr.com  /select?type=js&plc=1031744&cache=6207360&padsrvcurl=
6         x.fidelity-media.com  /delivery/ajs.php?zoneid=16765&cb=31517148700&ab=1457421260315171487008&charset...
7              data.rtbfy.com  /rtb2?id=20104&publisher_id=4518&rtb=1&product_id=9&campaign_id=10047&bid=MC4w...
8     partner.brentsmedia.com  /type/suggestion.js
9     partner.brentsmedia.com  /may/citizen/pole/sound/club/society.js?wrapper=false
10    partner.brentsmedia.com  /broad/duty/offer/house.json?lang=en-US&screen=1011x758&time=1457421348&offset=-...
20      ah.gordonfreasjr.com  /topic/11856-resubmits-triggering-schoolroom-tessellation-protestors-adjustments-subdivide...
22      ah.gordonfreasjr.com  /?r=VgFS&d=VtiDHMdQ1Q&w=KZp&p=qcHVI&j=NC6NqeDAFB&s=1jczkVHoF&i=4Rrb_m1
23      ah.gordonfreasjr.com  /?s=BSBhG&l=&r=PF0LkzsQV&w=&f=wg-e9c61wh&p=qN0nzk2K1G&o=64EEnQ&j=&g=6pv...
```

Publisher

SSP

Exchange

Malvertising

Angler EK

Trustwave®
Smart security on demand

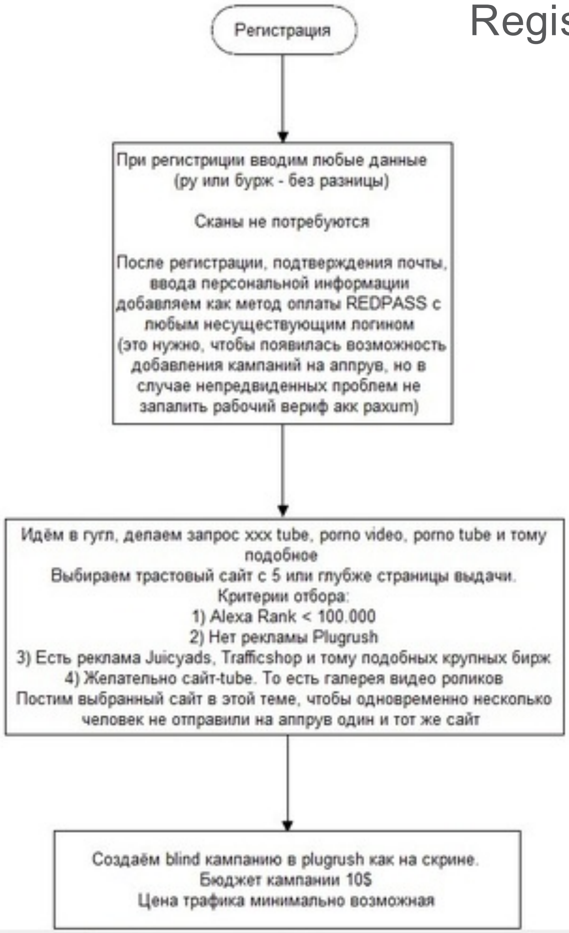
Malvertising Laundry

The standard flow

- A hacker signs up to an Ad network impersonates as a legit advertiser
- Spreading harmless ads for a while
- Choosing the right timing to enable the malicious code
- Every fixed number of views the malicious code is served
- Redirect to exploit kit

Trustwave®
Smart security on demand

Registration



Регистрация

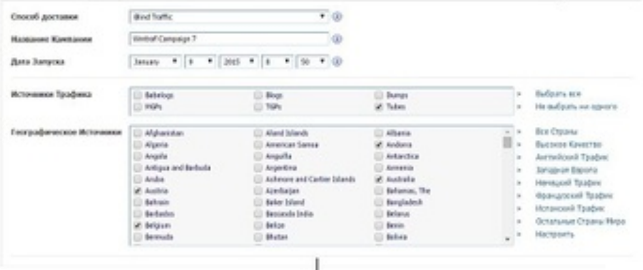
При регистриции вводим любые данные (ру или бурж - без разницы)

Сканы не потребуются

После регистрации, подтверждения почты, ввода персональной информации добавляем как метод оплаты REDPASS с любым несуществующим логином (это нужно, чтобы появилась возможность добавления кампаний на аппрув, но в случае непредвиденных проблем не запалить рабочий вериф акк paxum)

Идём в гугл, делаем запрос xxx tube, porno video, porno tube и тому подобное
Выбираем трастовый сайт с 5 или глубже страницы выдачи.
Критерии отбора:
1) Alexa Rank < 100.000
2) Нет рекламы Plugrush
3) Есть реклама Juicyads, Trafficshop и тому подобных крупных бирж
4) Желательно сайт-tube. То есть галерея видео роликов
Постим выбранный сайт в этой теме, чтобы одновременно несколько человек не отправили на аппрув один и тот же сайт

Создаём blind кампанию в plugrush как на скрине.
Бюджет кампании 10$
Цена трафика минимально возможная



Способ доставки: Blind Traffic
Название Кампании: Wintraf Campaign 7
Дата Запуска: January 6 2015 6 50

Источники Трафика: □ Babelogs □ Blogs □ Dumps □ MGPs □ TGPs ☑ Tubes
» Выбрать все
» Не выбрать ни одного

Географическое Источники: □ Afghanistan □ Aland Islands □ Albania □ Algeria □ American Samoa ☑ Andorra □ Angola □ Anguilla □ Antarctica □ Antigua and Barbuda □ Argentina □ Armenia □ Aruba □ Ashmore and Cartier Islands ☑ Australia ☑ Austria □ Azerbaijan □ Bahamas, The □ Bahrain □ Baker Island □ Bangladesh □ Barbados □ Bassas da India □ Belarus ☑ Belgium □ Belize □ Benin □ Bermuda □ Bhutan □ Bolivia
» Все Страны
» Высокое Качество
» Английский Трафик
» Западная Европа
» Немецкий Трафик
» Французский Трафик
» Испанский Трафик
» Остальные Страны Мира
» Настроить

Ждём аппрув, потом добавляем свой Paxum в аккаунт и оплачиваем кампанию.
Сливаем трафик на чужой сайт.

Register under any name (russian or american doesn’t matter). Choose to pay with REDPASS

Search for xxx site with no ads from Plugrush and with competitive advertisers

Set the minimum budget allowed for campaign: 10$

Wait for approval. Then you can add your Paxum account. The fun begins

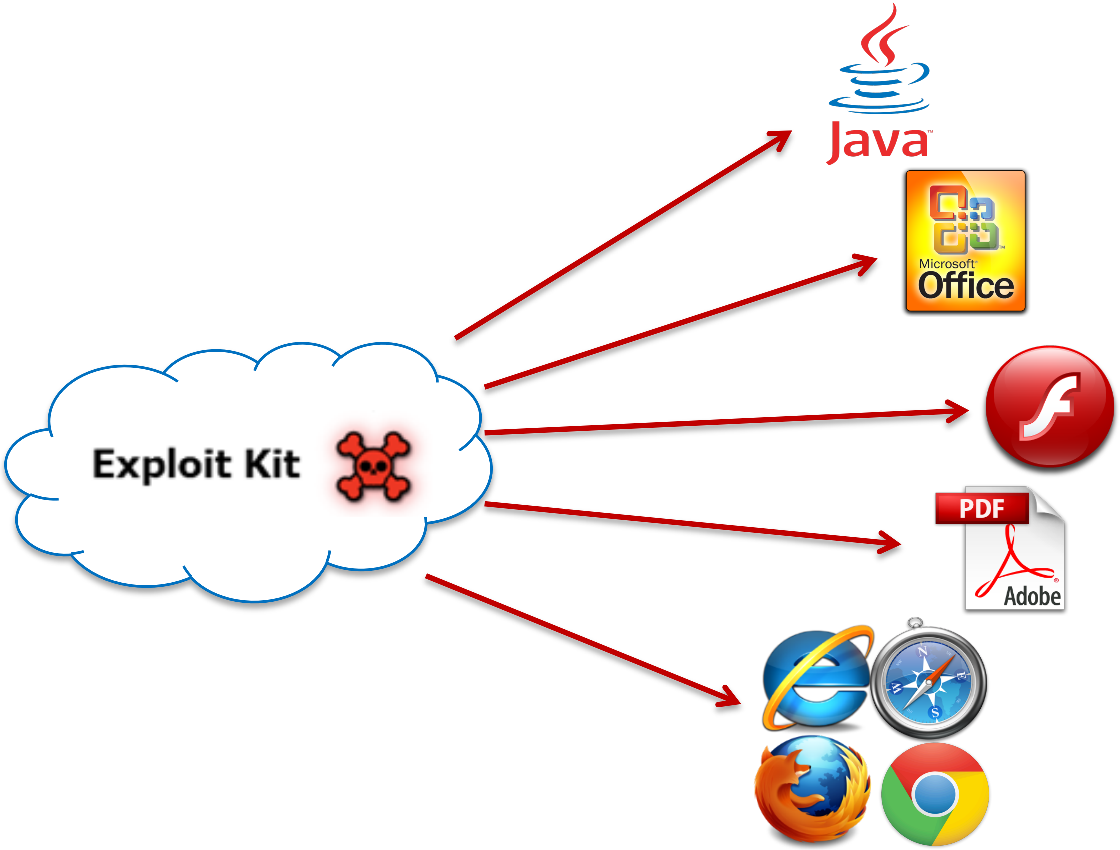
Who?

Exploit Kits

Exploit kits without traffic are like…

Trustwave®
Smart security on demand

Exploit Kits



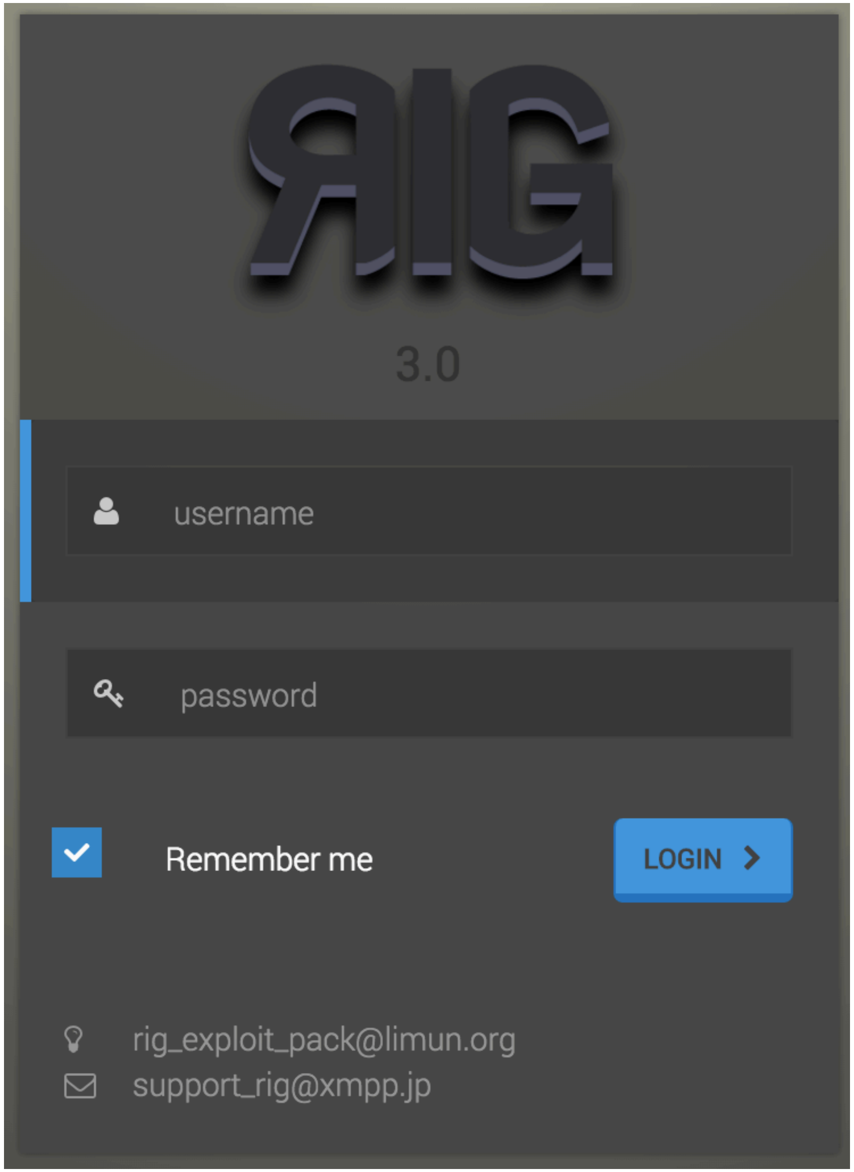
Trustwave®
Smart security on demand

Exploit Kits

Sources of traffic

- Compromised Web Sites
- SPAM

- Malvertising



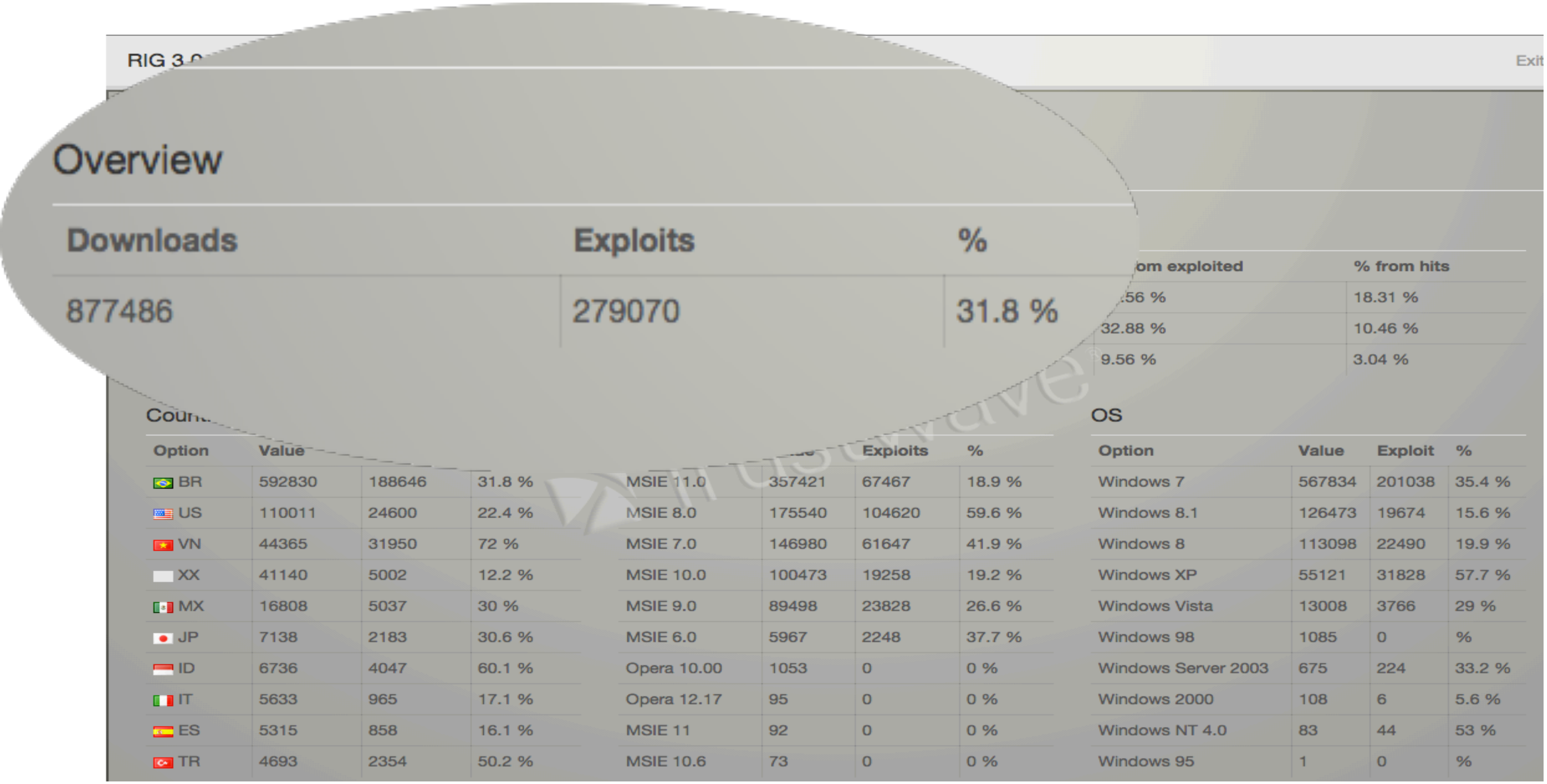
rig_exploit_pack@limun.org

support_rig@xmpp.jp

Trustwave®
Smart security on demand

Exploit Kits

Rig Exploit Kit Dashboard



Overview

Downloads	Exploits	%
877486	279070	31.8 %

om exploited	% from hits
.56 %	18.31 %
32.88 %	10.46 %
9.56 %	3.04 %

Coun

Option	Value		
BR	592830	188646	31.8 %
US	110011	24600	22.4 %
VN	44365	31950	72 %
XX	41140	5002	12.2 %
MX	16808	5037	30 %
JP	7138	2183	30.6 %
ID	6736	4047	60.1 %
IT	5633	965	17.1 %
ES	5315	858	16.1 %
TR	4693	2354	50.2 %

		Exploits	%
MSIE 11.0	357421	67467	18.9 %
MSIE 8.0	175540	104620	59.6 %
MSIE 7.0	146980	61647	41.9 %
MSIE 10.0	100473	19258	19.2 %
MSIE 9.0	89498	23828	26.6 %
MSIE 6.0	5967	2248	37.7 %
Opera 10.00	1053	0	0 %
Opera 12.17	95	0	0 %
MSIE 11	92	0	0 %
MSIE 10.6	73	0	0 %

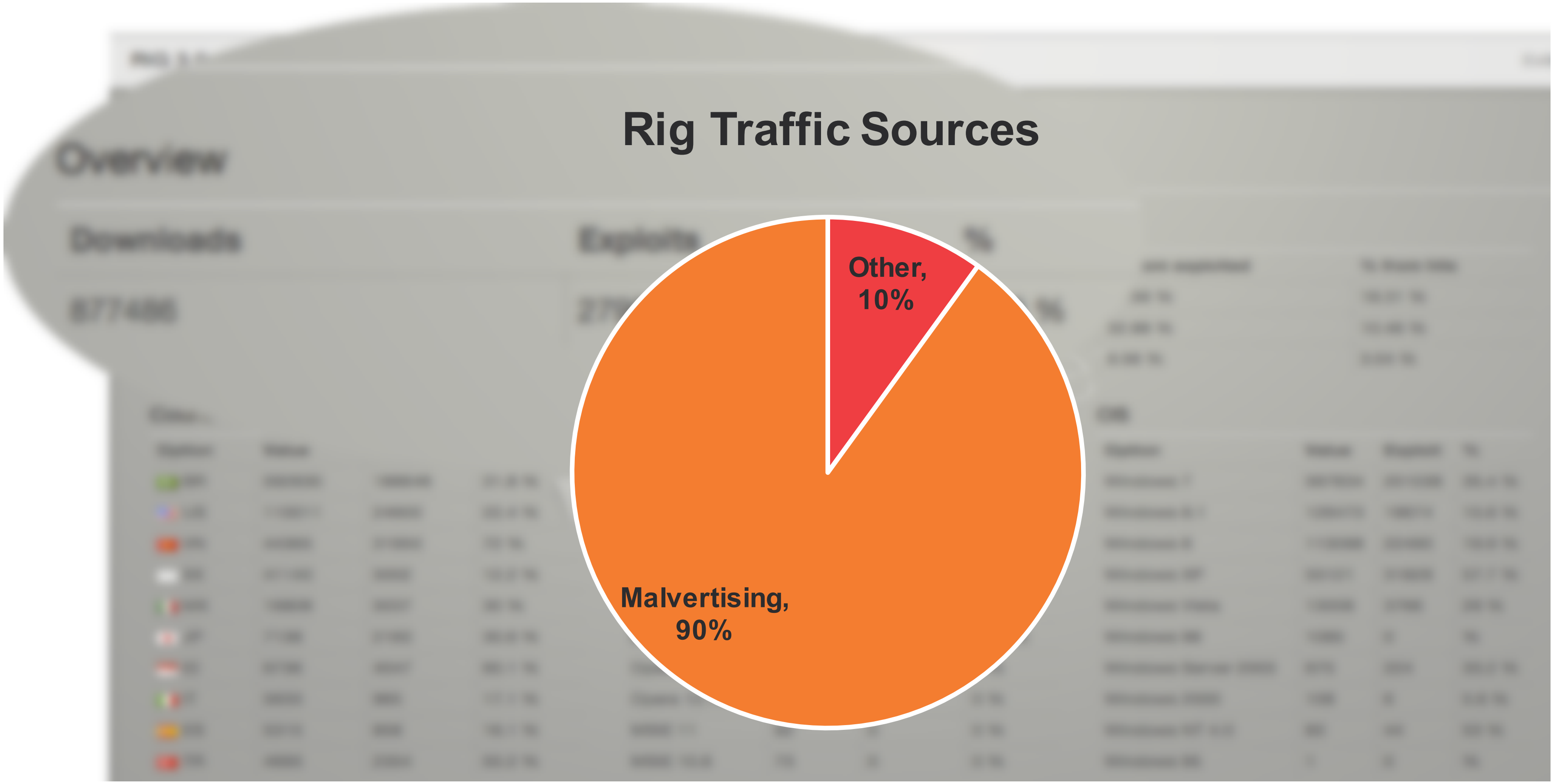
OS

Option	Value	Exploit	%
Windows 7	567834	201038	35.4 %
Windows 8.1	126473	19674	15.6 %
Windows 8	113098	22490	19.9 %
Windows XP	55121	31828	57.7 %
Windows Vista	13008	3766	29 %
Windows 98	1085	0	%
Windows Server 2003	675	224	33.2 %
Windows 2000	108	6	5.6 %
Windows NT 4.0	83	44	53 %
Windows 95	1	0	%

Trustwave®
Smart security on demand

Exploit Kits

Rig Exploit Kit Dashboard



Trustwave®
Smart security on demand

Why?

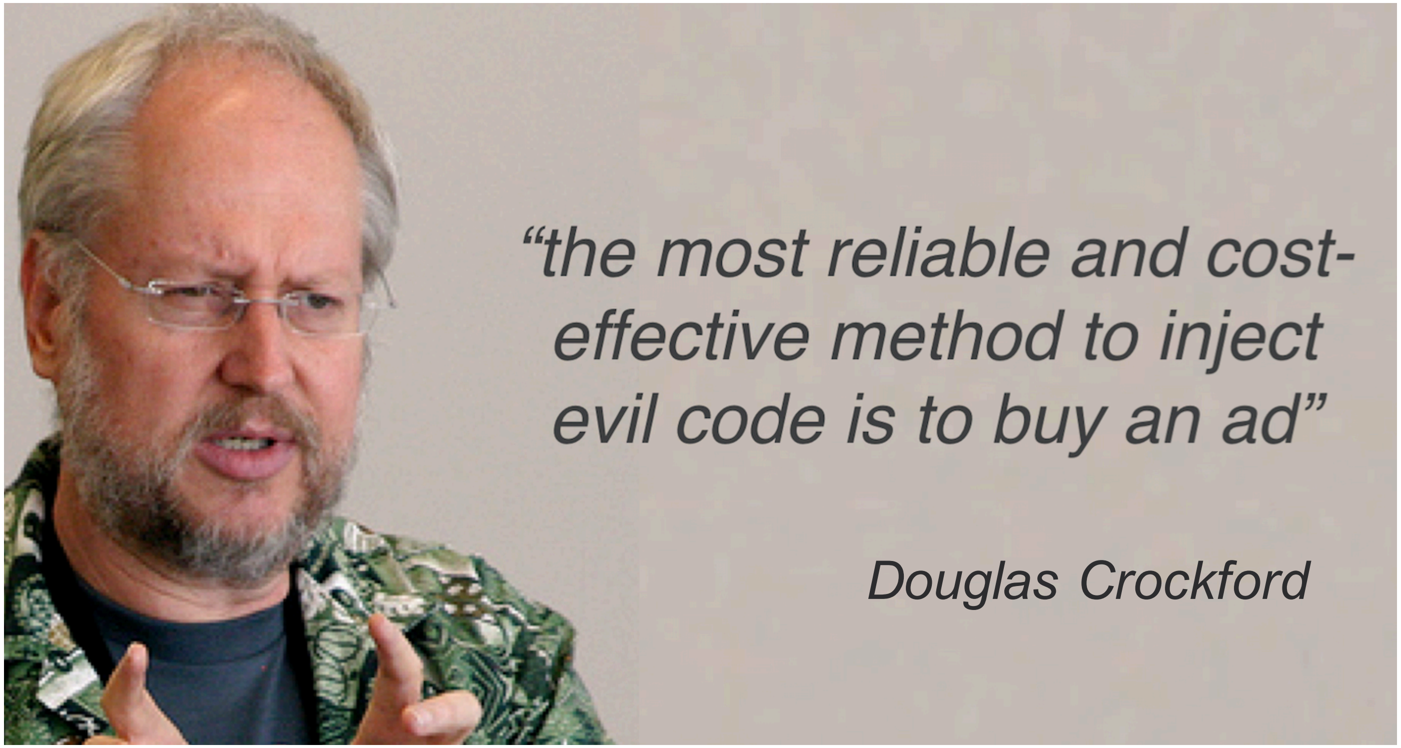
OR IN OTHER WORDS…

IF THE BAD GUYS CAN DO IT

SO CAN WE

Trustwave®

Reaching Vulnerable Machines



“the most reliable and cost-effective method to inject evil code is to buy an ad”

Douglas Crockford

Trustwave®
Smart security on demand

Reaching Vulnerable Machines

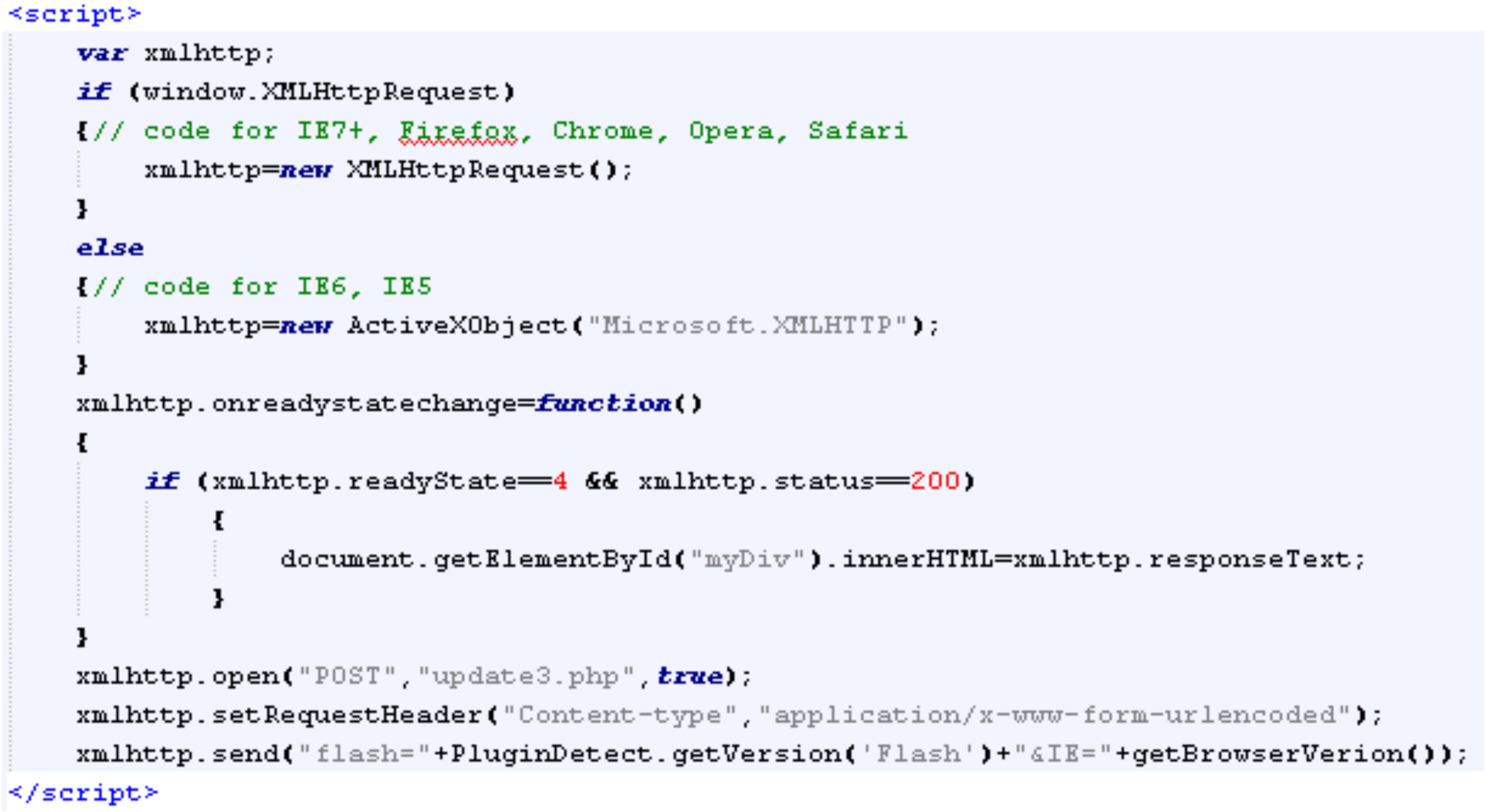
Task List

- Building a landing page
- Choosing Ad companies
- Bypassing “Security” checks of the Ad companies
- Running a campaign and analyzing the results
- Finding the best ROI taken by cybercriminals

Trustwave®
Smart security on demand

Building a Landing Page

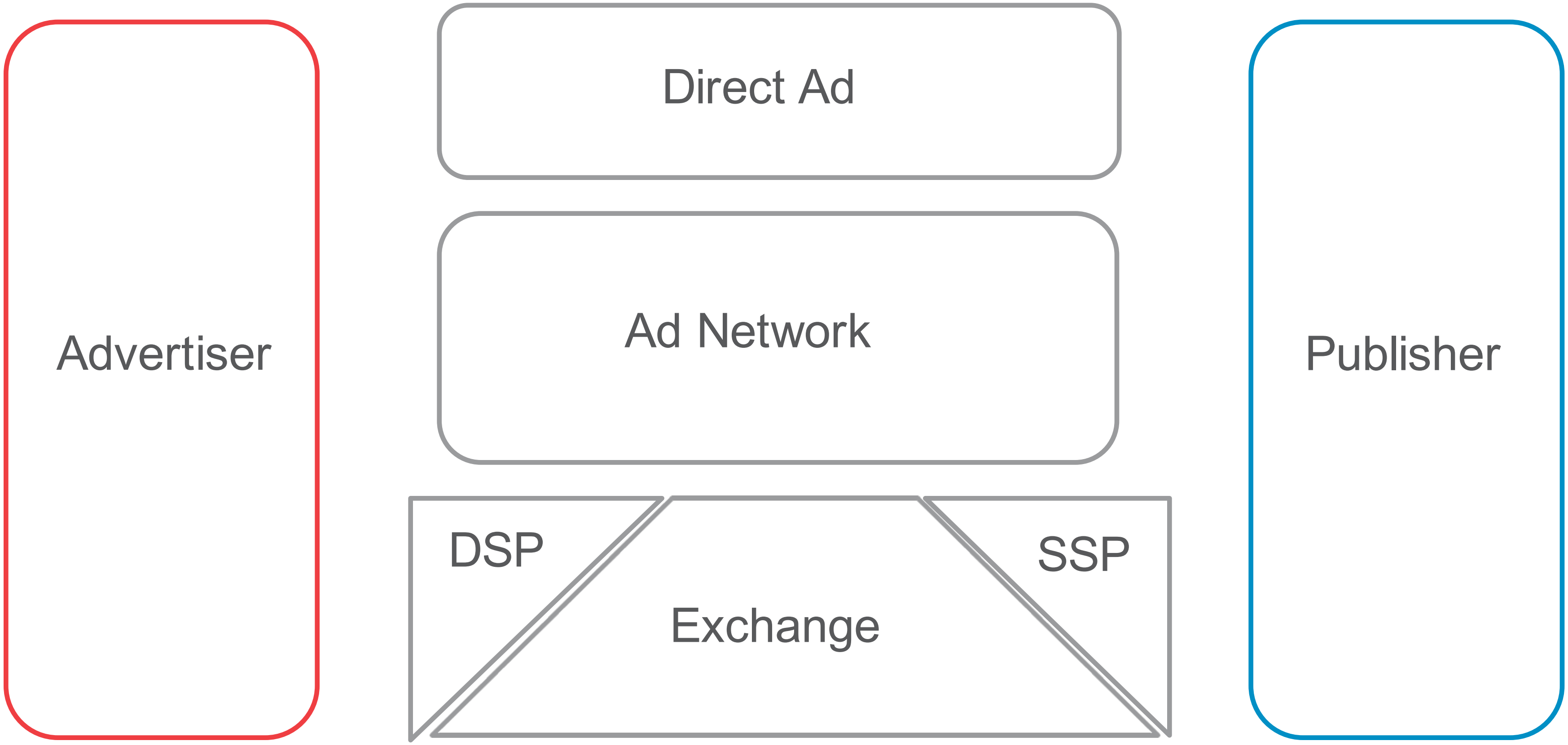
Looking for vulnerable Flash Player



```
<script>
    var xmlhttp;
    if (window.XMLHttpRequest)
    {// code for IE7+, Firefox, Chrome, Opera, Safari
        xmlhttp=new XMLHttpRequest();
    }
    else
    {// code for IE6, IE5
        xmlhttp=new ActiveXObject("Microsoft.XMLHTTP");
    }
    xmlhttp.onreadystatechange=function()
    {
        if (xmlhttp.readyState==4 && xmlhttp.status==200)
            {
                document.getElementById("myDiv").innerHTML=xmlhttp.responseText;
            }
    }
    xmlhttp.open("POST","update3.php",true);
    xmlhttp.setRequestHeader("Content-type","application/x-www-form-urlencoded");
    xmlhttp.send("flash="+PluginDetect.getVersion('Flash')+"&IE="+getBrowserVerion());
</script>
```

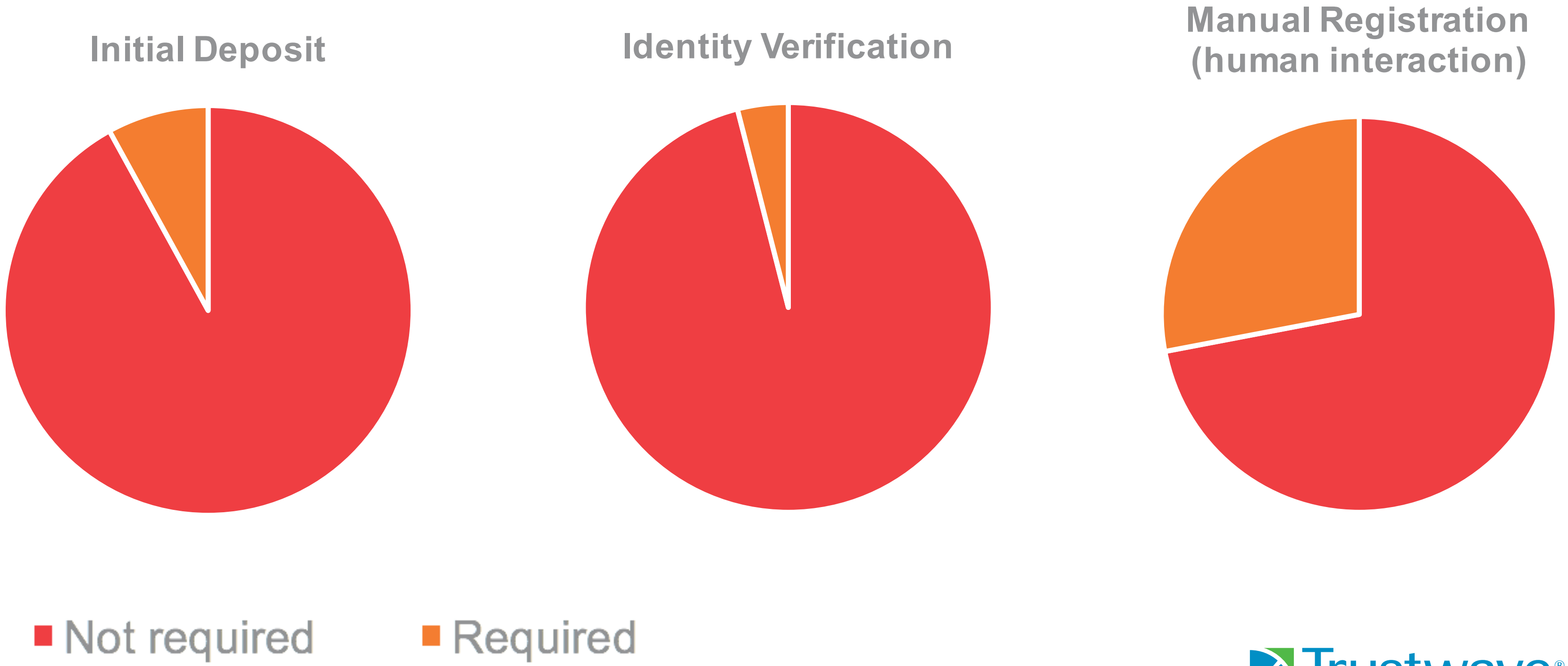
Trustwave®
Smart security on demand

Picking the right Ad company



Trustwave®
Smart security on demand

Picking the right Ad company



Trustwave®
Smart security on demand

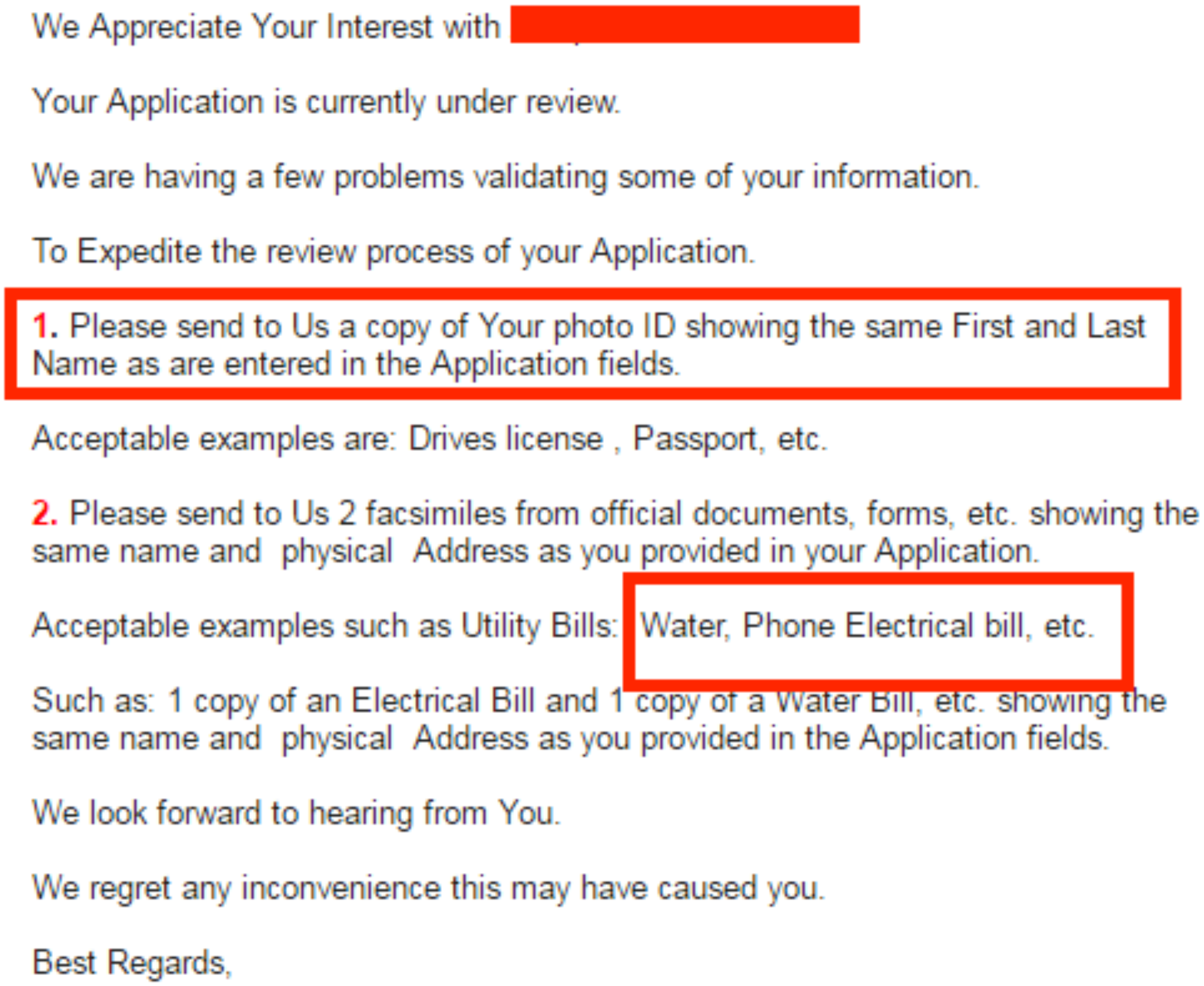
Bypassing Security Checks

Identity Verification

- Domain of the proposed banner *vs* domain of the company
  - Use hacked domain accounts (or buy already hacked) in some domain registrars
  - Generate subdomain in one of the accounts
  - Create a banner with a copied logo and a text from the original site
  - Host the banner on the subdomain
  - Approach an ad network and pretend to represent abused company

Bypassing Security checks

Request for identifying documents



We Appreciate Your Interest with [redacted]

Your Application is currently under review.

We are having a few problems validating some of your information.

To Expedite the review process of your Application.

1. Please send to Us a copy of Your photo ID showing the same First and Last Name as are entered in the Application fields.

Acceptable examples are: Drives license , Passport, etc.

2. Please send to Us 2 facsimiles from official documents, forms, etc. showing the same name and physical Address as you provided in your Application.

Acceptable examples such as Utility Bills: Water, Phone Electrical bill, etc.

Such as: 1 copy of an Electrical Bill and 1 copy of a Water Bill, etc. showing the same name and physical Address as you provided in the Application fields.

We look forward to hearing from You.

We regret any inconvenience this may have caused you.

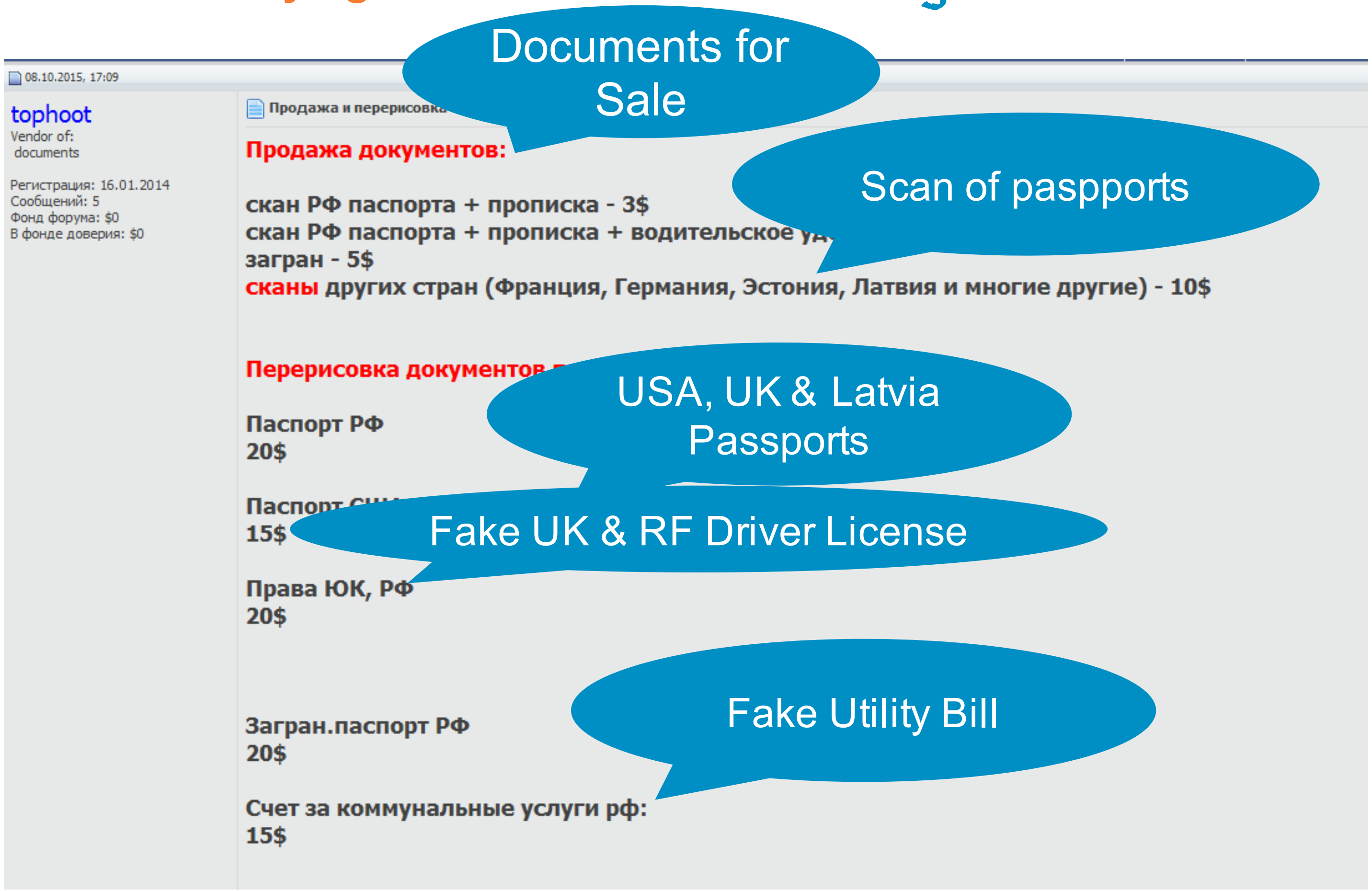
Best Regards,

the company

Trustwave®
Smart security on demand

Bypassing Security checks

Request for identifying documents – The underground to the rescue!!



08.10.2015, 17:09

tophoot
Vendor of:
documents

Регистрация: 16.01.2014
Сообщений: 5
Фонд форума: $0
В фонде доверия: $0

Продажа и перерисовка

Продажа документов:

скан РФ паспорта + прописка - 3$
скан РФ паспорта + прописка + водительское уд
загран - 5$
сканы других стран (Франция, Германия, Эстония, Латвия и многие другие) - 10$

Перерисовка документов п

Паспорт РФ
20$

Паспорт США
15$

Права ЮК, РФ
20$

Загран.паспорт РФ
20$

Счет за коммунальные услуги рф:
15$

Documents for Sale

Scan of paspports

USA, UK & Latvia Passports

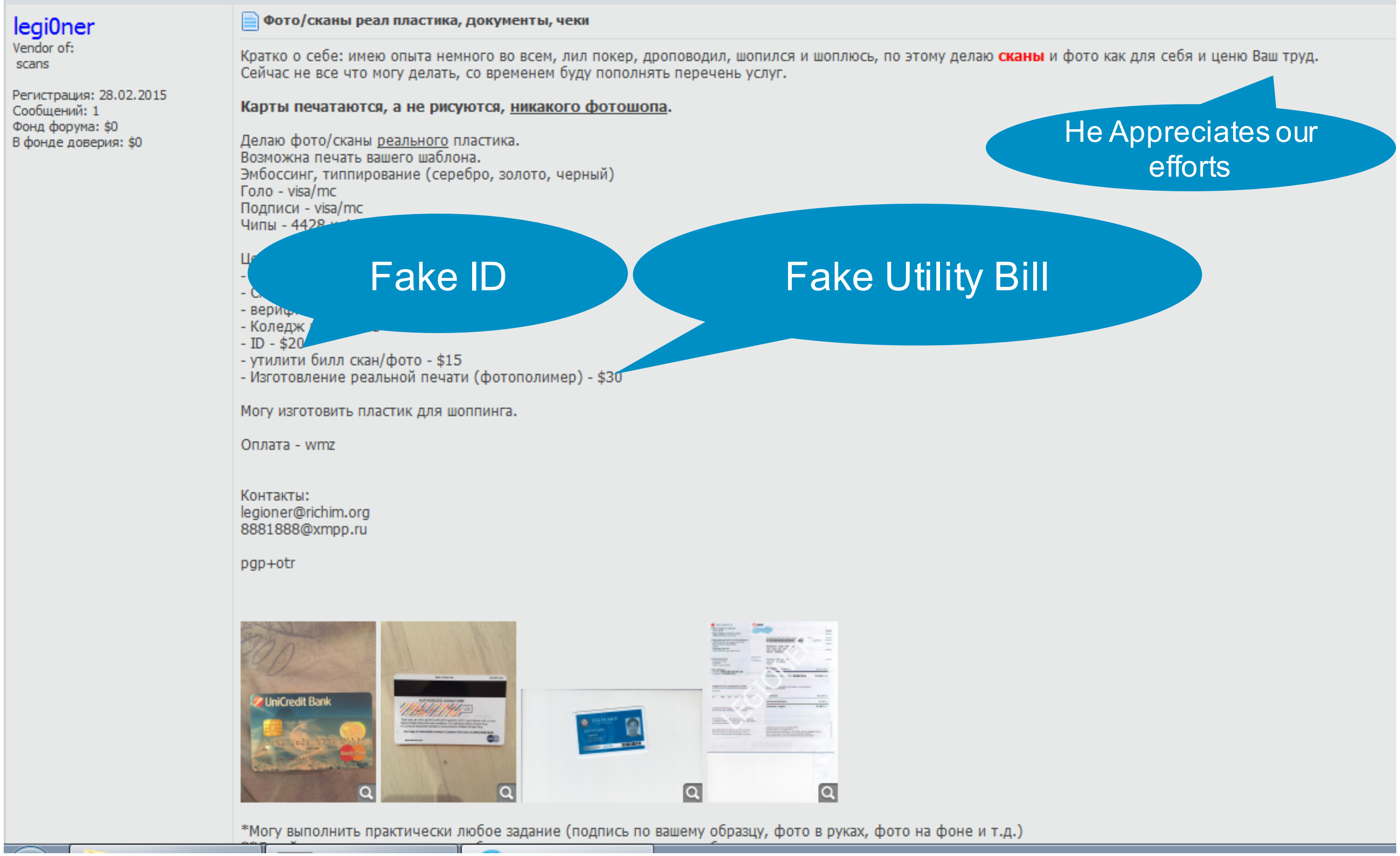
Fake UK & RF Driver License

Fake Utility Bill

Trustwave®
Smart security on demand

Bypassing Security checks

Request for identifying documents – The underground to the rescue!!



legi0ner
Vendor of:
scans

Регистрация: 28.02.2015
Сообщений: 1
Фонд форума: $0
В фонде доверия: $0

Фото/сканы реал пластика, документы, чеки

Кратко о себе: имею опыта немного во всем, лил покер, дроповодил, шопился и шоплюсь, по этому делаю **сканы** и фото как для себя и ценю Ваш труд.
Сейчас не все что могу делать, со временем буду пополнять перечень услуг.

Карты печатаются, а не рисуются, никакого фотошопа.

Делаю фото/сканы реального пластика.
Возможна печать вашего шаблона.
Эмбоссинг, типпирование (серебро, золото, черный)
Голо - visa/mc
Подписи - visa/mc
Чипы - 4428

Ц
-
- С
- вериф
- Коледж
- ID - $20
- утилити билл скан/фото - $15
- Изготовление реальной печати (фотополимер) - $30

Могу изготовить пластик для шоппинга.

Оплата - wmz

Контакты:
legioner@richim.org
8881888@xmpp.ru

pgp+otr

*Могу выполнить практически любое задание (подпись по вашему образцу, фото в руках, фото на фоне и т.д.)

He Appreciates our efforts

Fake ID

Fake Utility Bill

Trustwave®
Smart security on demand

First Experience as Advertisers

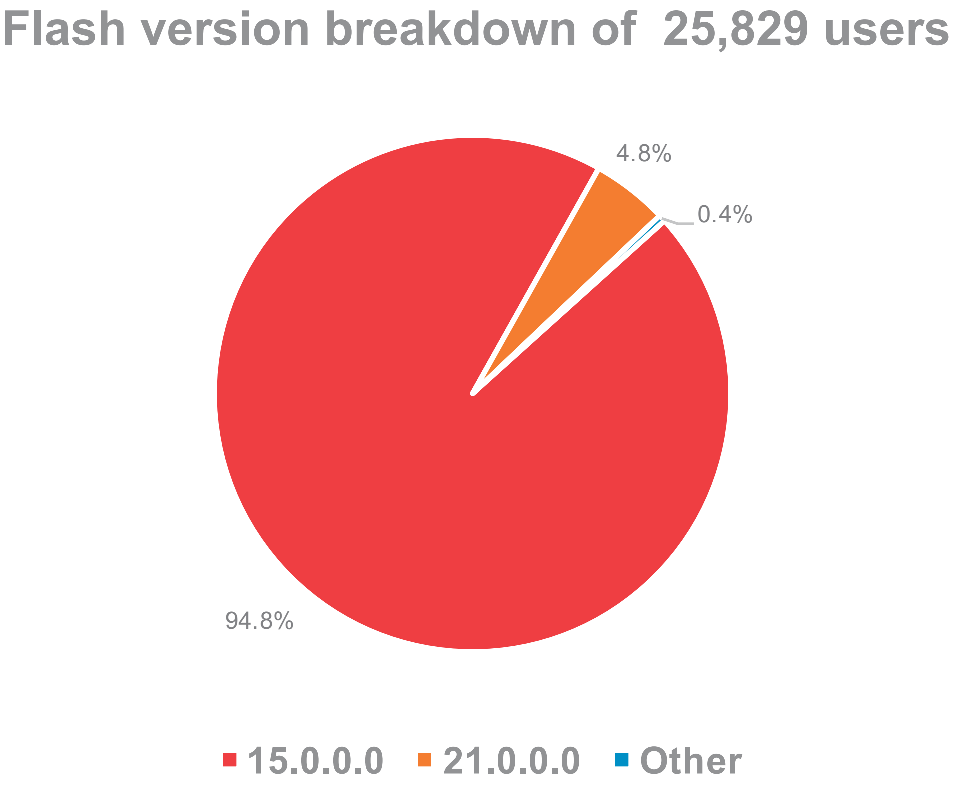
Campaign Results

- Budget: $4.00
- Campaign Time: 8 hours
- Total Clicks (according to the Ad company): 20,000
- Total Click (according to our records): 25,831

Trustwave®
Smart security on demand

First Experience as Advertisers

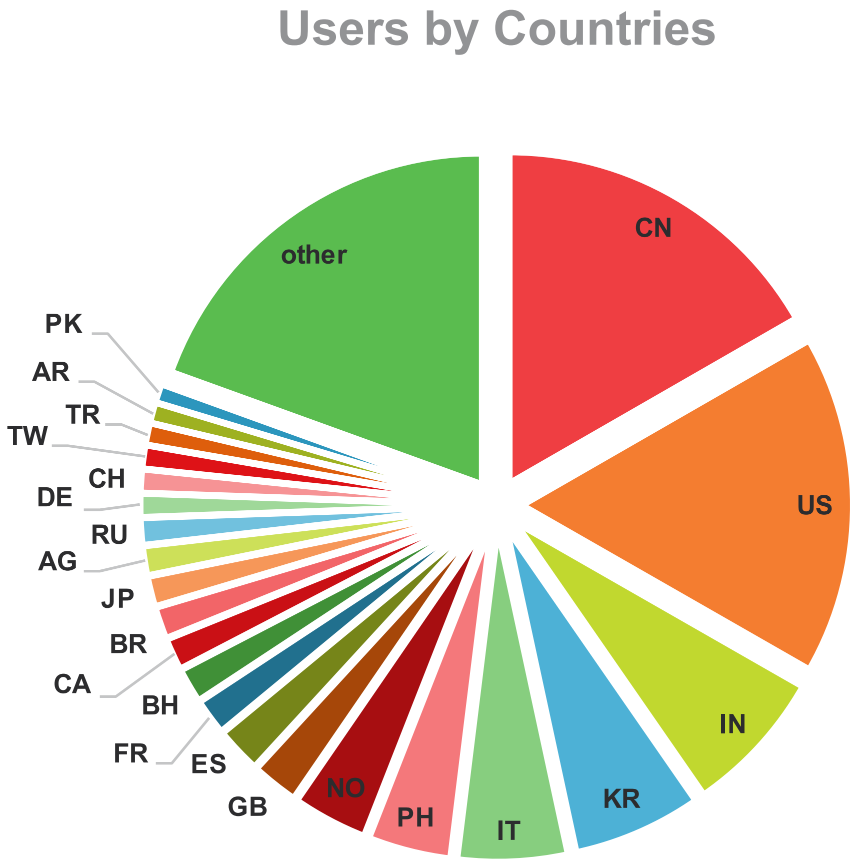
Campaign Results



Trustwave®
Smart security on demand

First Experience as Advertisers

Campaign Results



Trustwave®
Smart security on demand

Ad-Clicker & Malvertising

Bedep Malware in Action

- <LIVE DEMO>

Trustwave®
Smart security on demand

Ad-Clicker & Malvertising

Bedep Malware over 1 month period

- Approximately 300,000 advertising impressions
- The machine was attacked 2500 by exploits delivered by malvertising
- 0.83 % of the advertising were malware

Smart security on demand

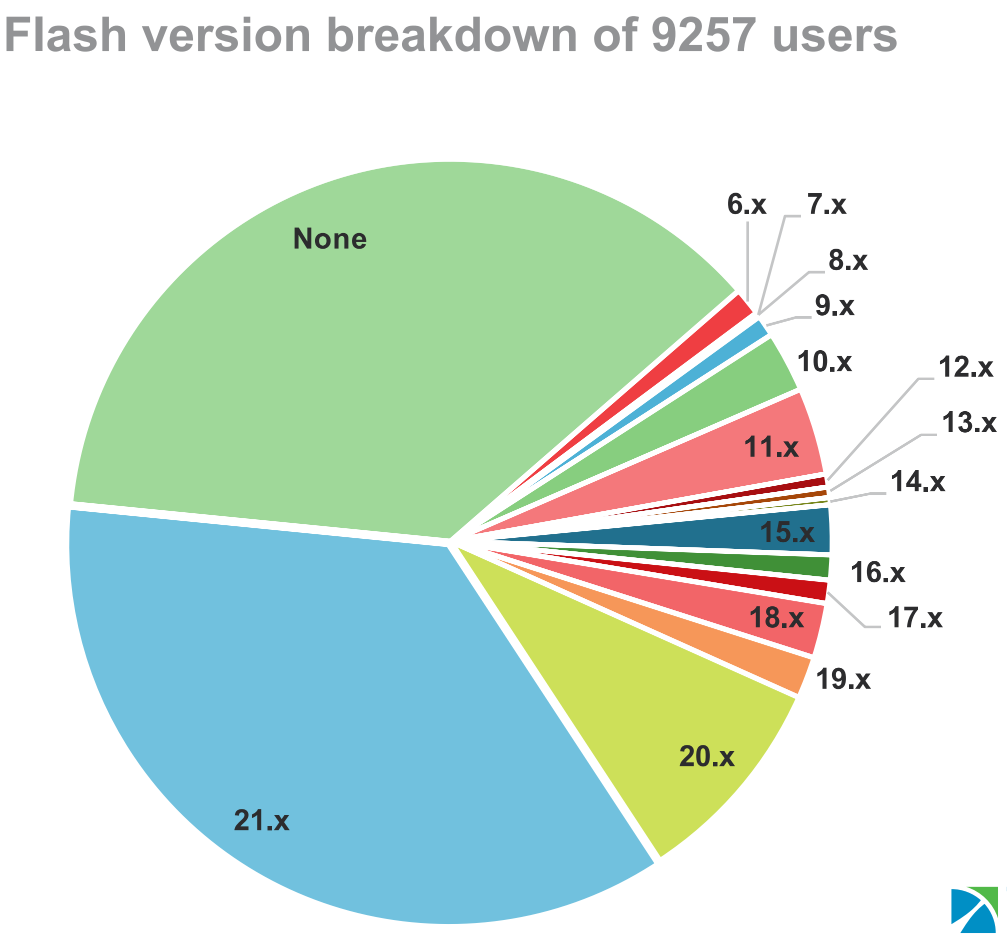
Second Experience as Advertisers

A different Ad network

- Budget: $5.00
- Campaign Time: 10 hours
- Total Clicks (according to the Ad company): 9,999
- Total Click (according to our records): 9,265

Trustwave®
Smart security on demand

Second Experience as Advertisers



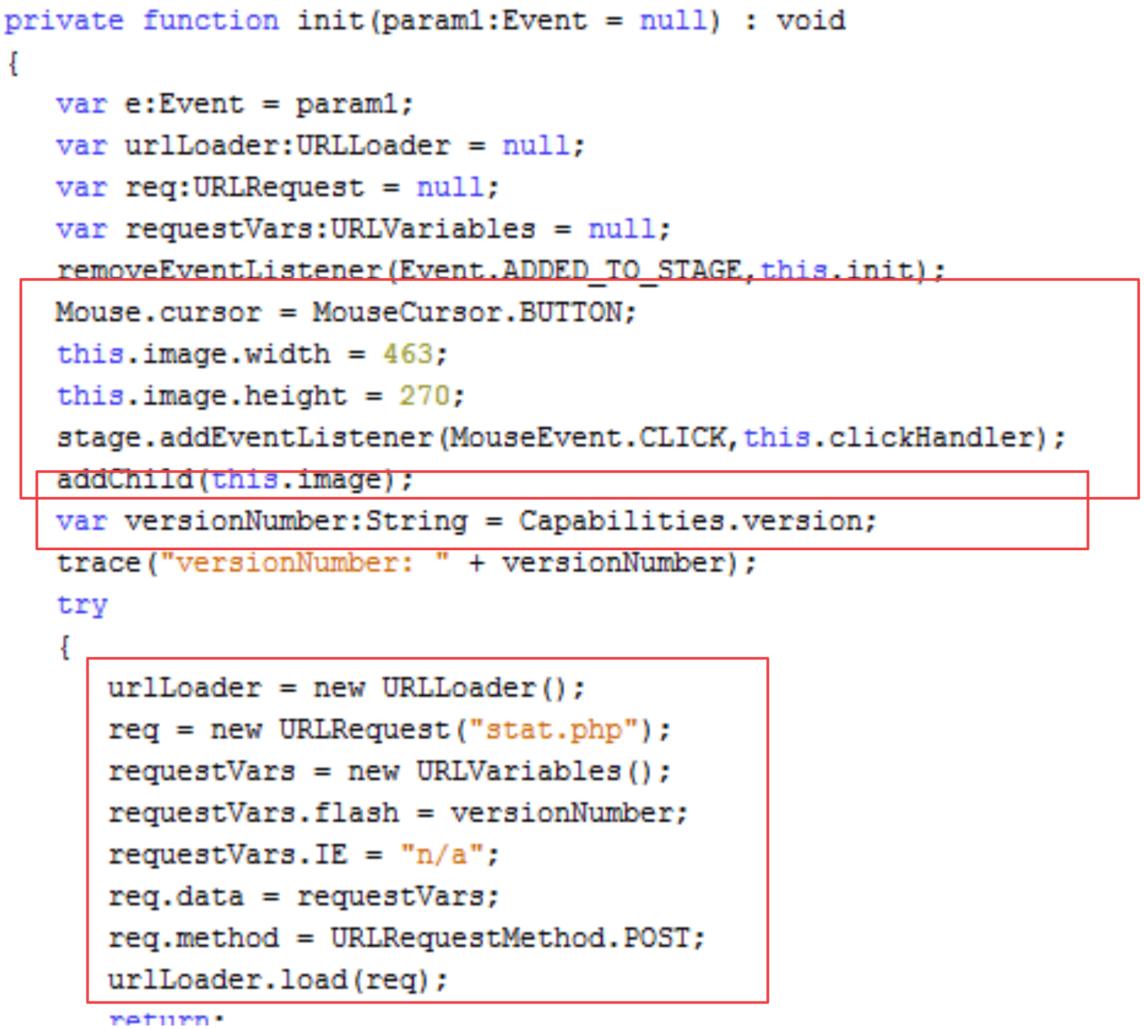
Trustwave®
Smart security on demand

What we've learned so far

- Every campaign inserted automatically into pending status
- Changing the campaign parameters enforce system approval
- Mostly cosmetic checks, such as URL validity and visually
- After approval, no validation upon changing the landing page itself

Trustwave®
Smart security on demand

Flash Based Landing Page



```
private function init(param1:Event = null) : void
{
   var e:Event = param1;
   var urlLoader:URLLoader = null;
   var req:URLRequest = null;
   var requestVars:URLVariables = null;
   removeEventListener(Event.ADDED_TO_STAGE,this.init);
   Mouse.cursor = MouseCursor.BUTTON;
   this.image.width = 463;
   this.image.height = 270;
   stage.addEventListener(MouseEvent.CLICK,this.clickHandler);
   addChild(this.image);
   var versionNumber:String = Capabilities.version;
   trace("versionNumber: " + versionNumber);
   try
   {
      urlLoader = new URLLoader();
      req = new URLRequest("stat.php");
      requestVars = new URLVariables();
      requestVars.flash = versionNumber;
      requestVars.IE = "n/a";
      req.data = requestVars;
      req.method = URLRequestMethod.POST;
      urlLoader.load(req);
      return;
```

Smart security on demand

Third Experience as Advertiser

Campaign Results

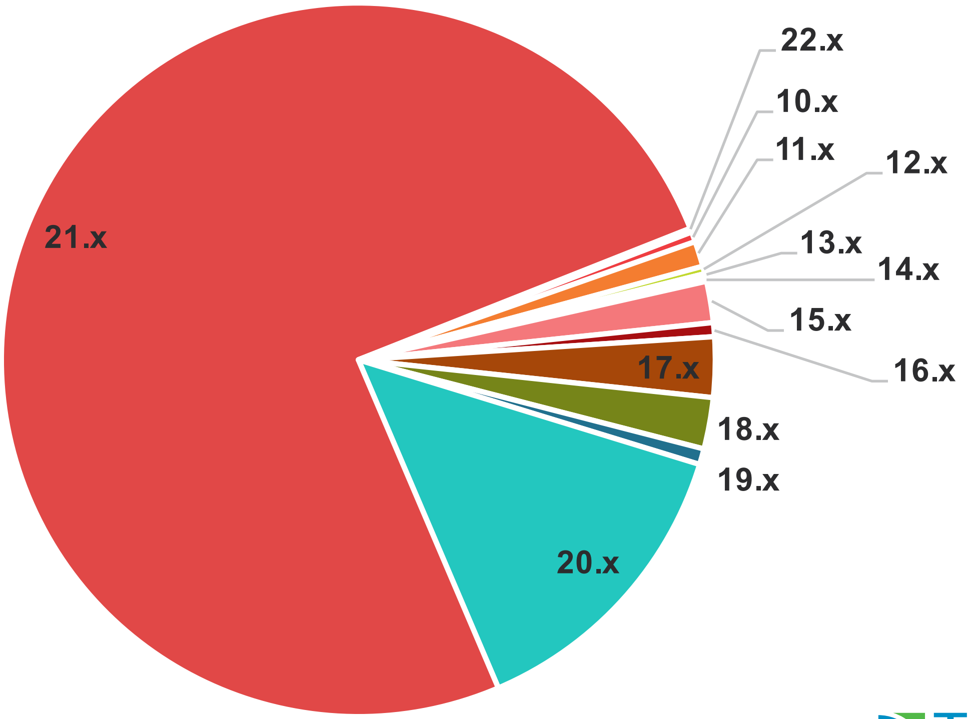
- Budget: $5.00
- IE Filter
- Campaign Time: 6 hours
- Total Clicks (according to the Ad company): 6250
- Total Click (according to our records): 4,818

Trustwave®
Smart security on demand

Third Experience as Advertiser

Campaign Results

Flash version breakdown of 3,419 users

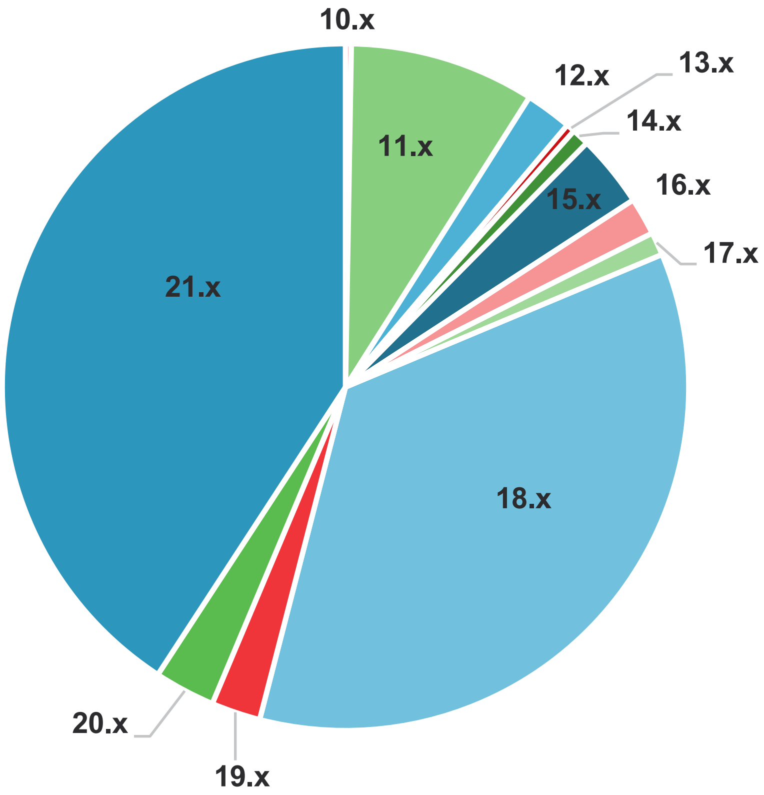


Trustwave® Smart security on demand

Third Experience as Advertiser

Campaign Results

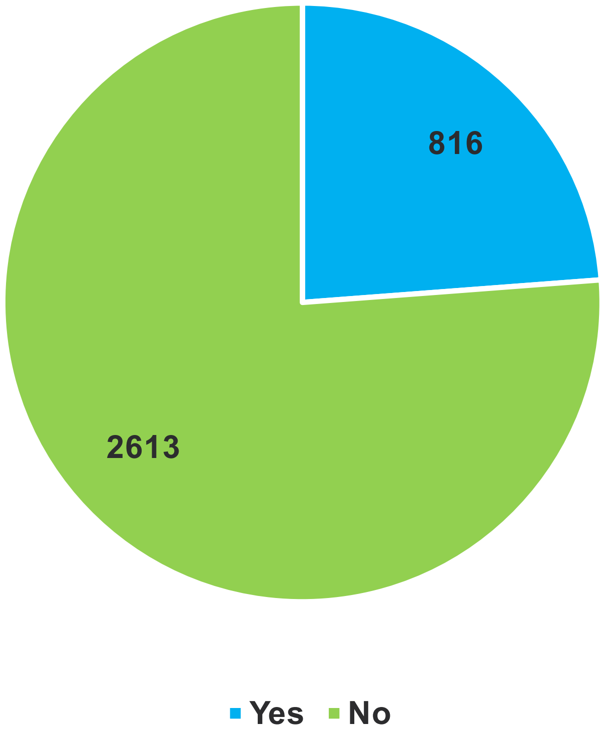
Flash Versions Breakdown of 4,818 Users



Trustwave®
Smart security on demand

Arm Landing Page With Exploit

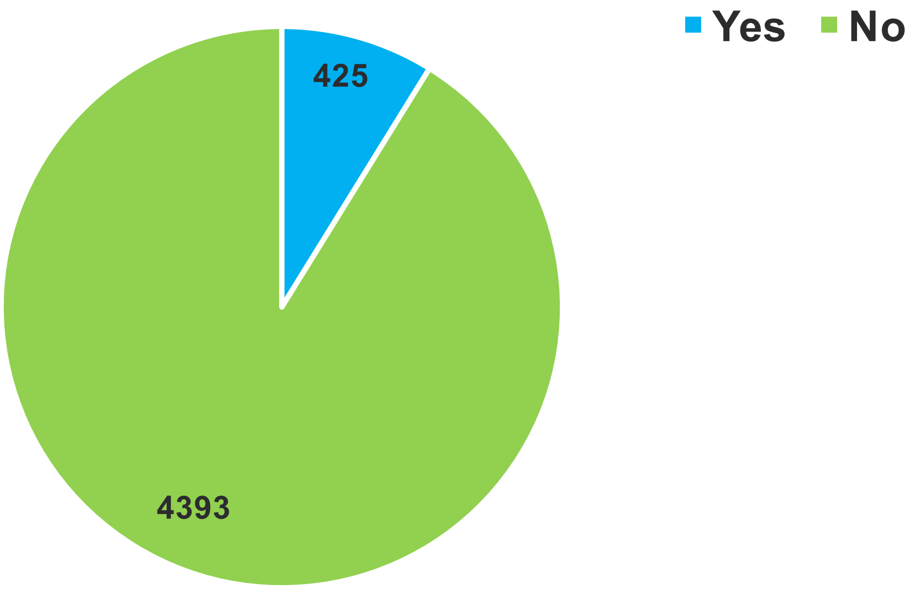
Machines Running Vulnerable Flash



Trustwave®
Smart security on demand

Arm Landing Page With Exploit

Machines Running Vulnerable Flash



Trustwave®
Smart security on demand

LIVE DEMO

Trustwave®
Smart security on demand

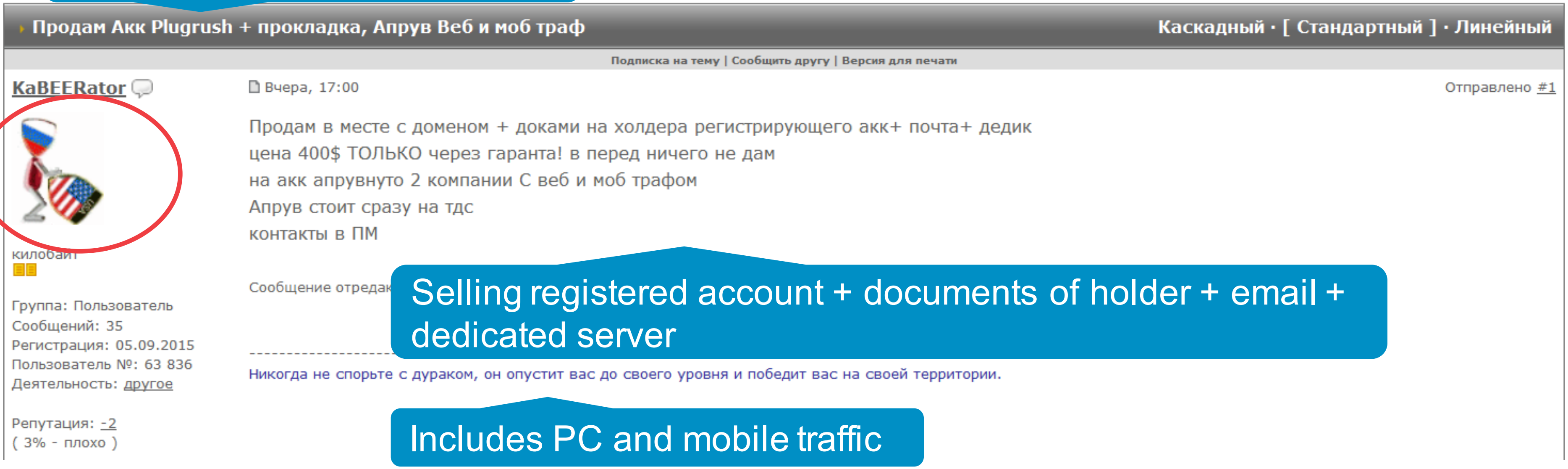
Underground

Trustwave®

Underground Gives its Alternatives

Ad Networks Accounts For Sale

PlugRush account for sale



Продам Акк Plugrush + прокладка, Апрув Веб и моб траф

Каскадный · [Стандартный] · Линейный

Подписка на тему | Сообщить другу | Версия для печати

KaBEERator

Вчера, 17:00

Отправлено #1

Продам в месте с доменом + доками на холдера регистрирующего акк+ почта+ дедик
цена 400$ ТОЛЬКО через гаранта! в перед ничего не дам
на акк апрувнуто 2 компании С веб и моб трафом
Апрув стоит сразу на тдс
контакты в ПМ

килобайт

Сообщение отредак

Группа: Пользователь
Сообщений: 35
Регистрация: 05.09.2015
Пользователь №: 63 836
Деятельность: другое

Репутация: -2
(3% - плохо)

Никогда не спорьте с дураком, он опустит вас до своего уровня и победит вас на своей территории.

Selling registered account + documents of holder + email + dedicated server

Includes PC and mobile traffic

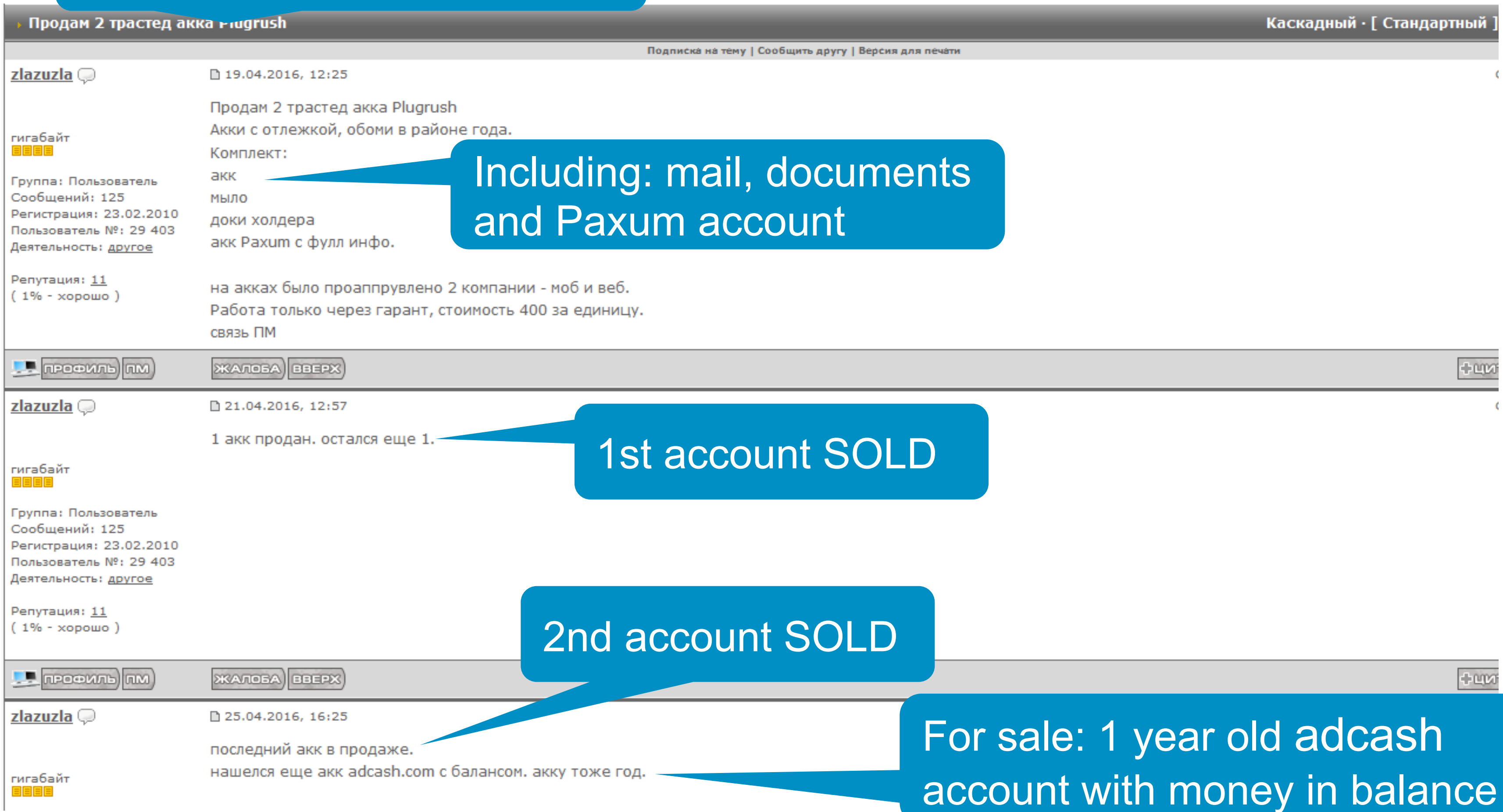
Price: $400

Trustwave®
Smart security on demand

Underground Gives its Alternatives

2 PlugRush accounts for sale

A… Sale



Продам 2 трастед акка Plugrush

Каскадный · [Стандартный]

Подписка на тему | Сообщить другу | Версия для печати

zlazuzla

гигабайт

Группа: Пользователь
Сообщений: 125
Регистрация: 23.02.2010
Пользователь №: 29 403
Деятельность: другое

Репутация: 11
(1% - хорошо)

19.04.2016, 12:25

Продам 2 трастед акка Plugrush
Акки с отлежкой, обоми в районе года.
Комплект:
акк
мыло
доки холдера
акк Paxum с фулл инфо.

на акках было проаппрувлено 2 компании - моб и веб.
Работа только через гарант, стоимость 400 за единицу.
связь ПМ

zlazuzla

гигабайт

Группа: Пользователь
Сообщений: 125
Регистрация: 23.02.2010
Пользователь №: 29 403
Деятельность: другое

Репутация: 11
(1% - хорошо)

21.04.2016, 12:57

1 акк продан. остался еще 1.

zlazuzla

гигабайт

25.04.2016, 16:25

последний акк в продаже.
нашелся еще акк adcash.com с балансом. акку тоже год.

Including: mail, documents and Paxum account

1st account SOLD

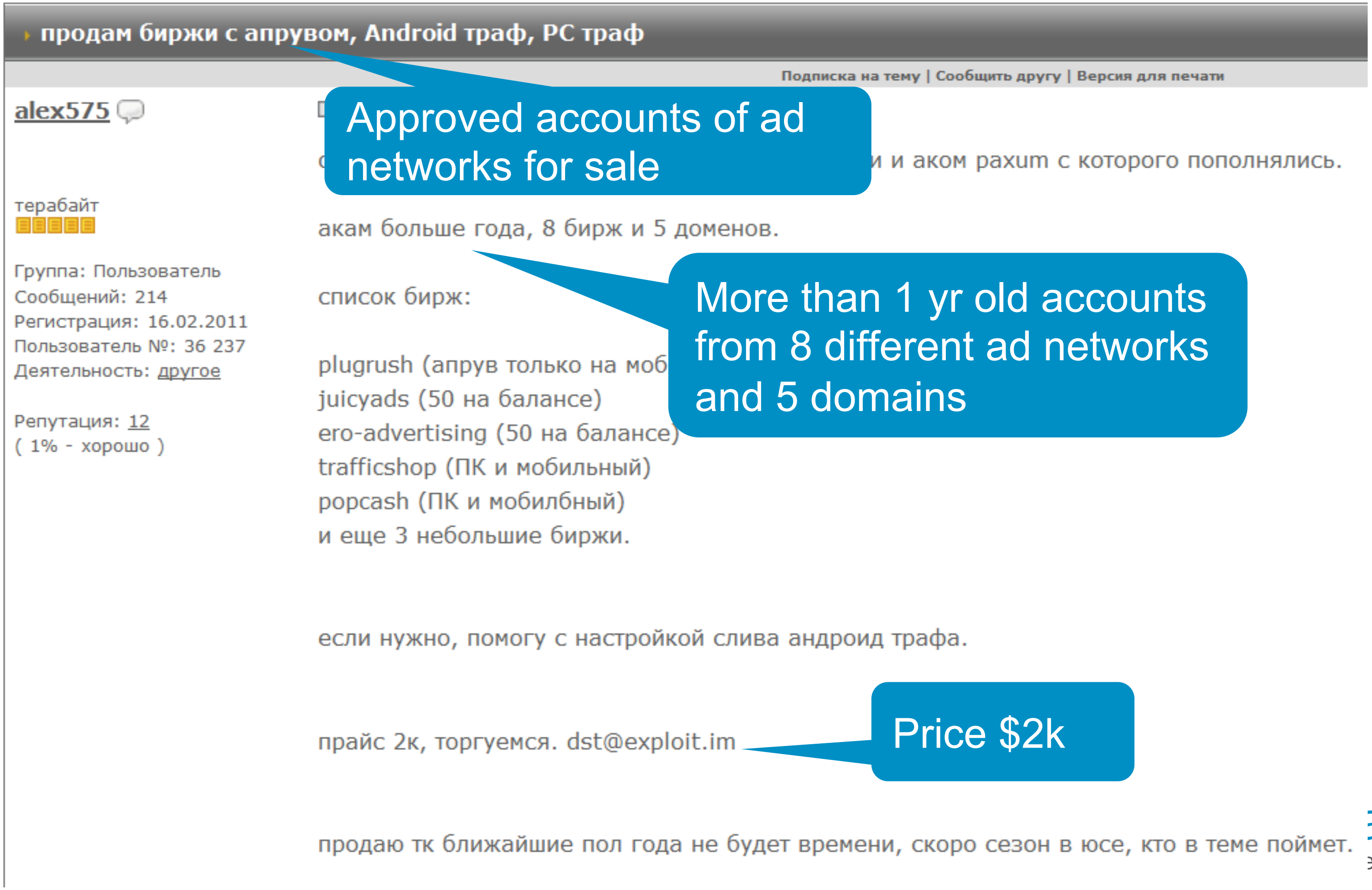
2nd account SOLD

For sale: 1 year old adcash account with money in balance

Trustwave®
Smart security on demand

The Underground Gives its Alternatives

Ad Networks Accounts For Sale



продам биржи с апрувом, Android траф, PC траф

Подписка на тему | Сообщить другу | Версия для печати

alex575

терабайт

Группа: Пользователь
Сообщений: 214
Регистрация: 16.02.2011
Пользователь №: 36 237
Деятельность: другое

Репутация: 12
(1% - хорошо)

и и аком paxum с которого пополнялись.

акам больше года, 8 бирж и 5 доменов.

список бирж:

plugrush (апрув только на моб
juicyads (50 на балансе)
ero-advertising (50 на балансе)
trafficshop (ПК и мобильный)
popcash (ПК и мобилбный)
и еще 3 небольшие биржи.

если нужно, помогу с настройкой слива андроид трафа.

прайс 2к, торгуемся. dst@exploit.im

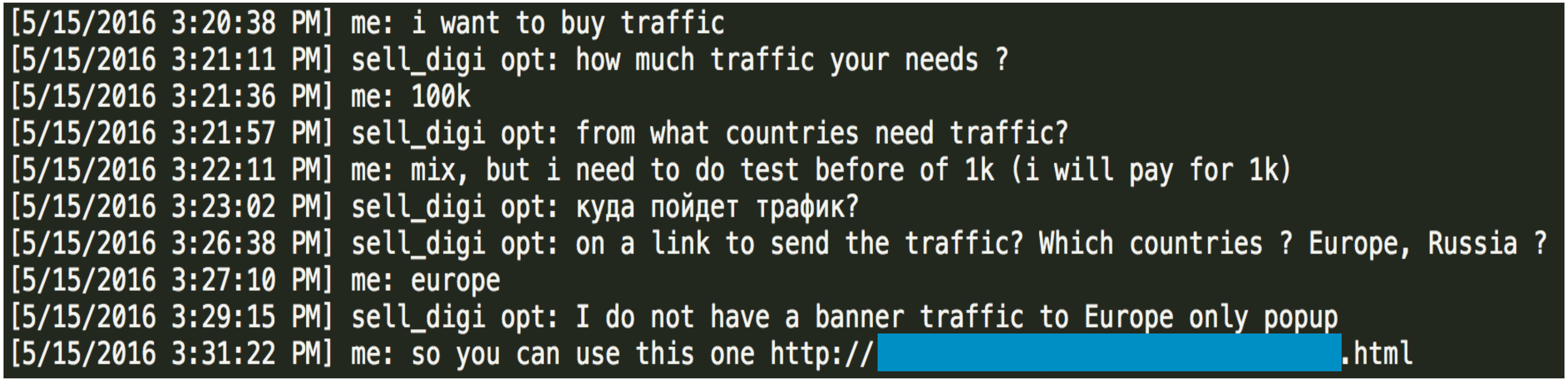
продаю тк ближайшие пол года не будет времени, скоро сезон в юсе, кто в теме поймет.

Approved accounts of ad networks for sale

More than 1 yr old accounts from 8 different ad networks and 5 domains

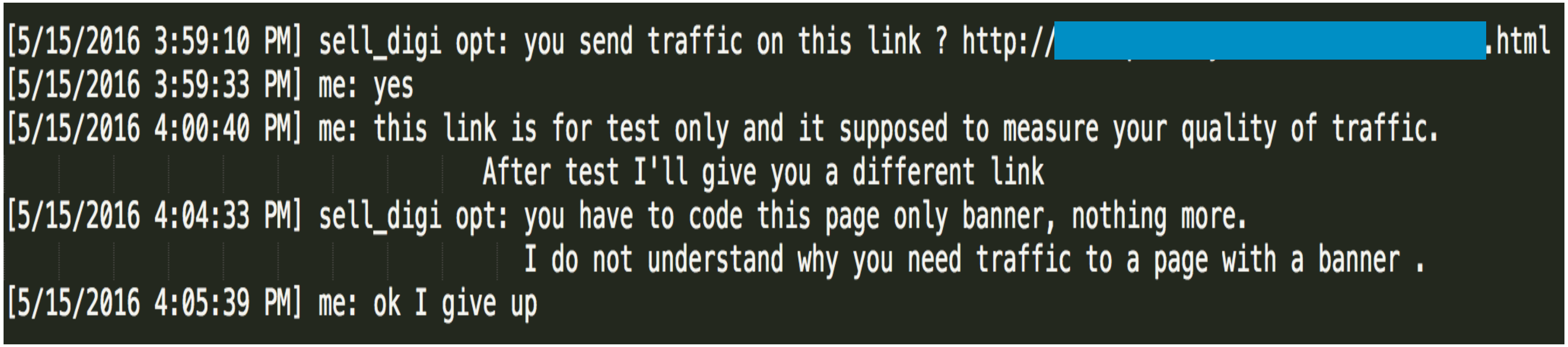
Price $2k

Buying Traffic



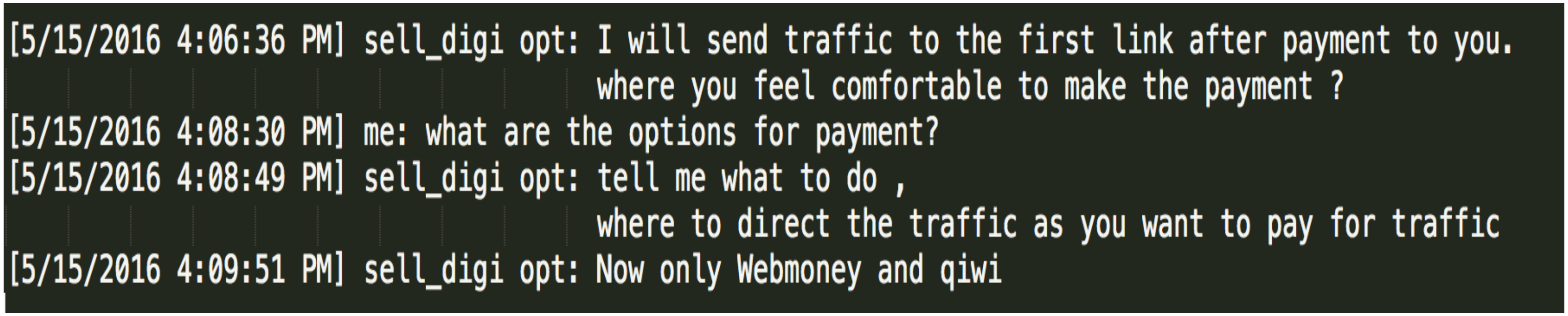
```
[5/15/2016 3:20:38 PM] me: i want to buy traffic
[5/15/2016 3:21:11 PM] sell_digi opt: how much traffic your needs ?
[5/15/2016 3:21:36 PM] me: 100k
[5/15/2016 3:21:57 PM] sell_digi opt: from what countries need traffic?
[5/15/2016 3:22:11 PM] me: mix, but i need to do test before of 1k (i will pay for 1k)
[5/15/2016 3:23:02 PM] sell_digi opt: куда пойдет трафик?
[5/15/2016 3:26:38 PM] sell_digi opt: on a link to send the traffic? Which countries ? Europe, Russia ?
[5/15/2016 3:27:10 PM] me: europe
[5/15/2016 3:29:15 PM] sell_digi opt: I do not have a banner traffic to Europe only popup
[5/15/2016 3:31:22 PM] me: so you can use this one http://[redacted].html
```

Buying Traffic



```
[5/15/2016 3:59:10 PM] sell_digi opt: you send traffic on this link ? http://[redacted].html
[5/15/2016 3:59:33 PM] me: yes
[5/15/2016 4:00:40 PM] me: this link is for test only and it supposed to measure your quality of traffic.
                              After test I'll give you a different link
[5/15/2016 4:04:33 PM] sell_digi opt: you have to code this page only banner, nothing more.
                                 I do not understand why you need traffic to a page with a banner .
[5/15/2016 4:05:39 PM] me: ok I give up
```

Buying Traffic



```
[5/15/2016 4:06:36 PM] sell_digi opt: I will send traffic to the first link after payment to you.
                                      where you feel comfortable to make the payment ?
[5/15/2016 4:08:30 PM] me: what are the options for payment?
[5/15/2016 4:08:49 PM] sell_digi opt: tell me what to do ,
                                      where to direct the traffic as you want to pay for traffic
[5/15/2016 4:09:51 PM] sell_digi opt: Now only Webmoney and qiwi
```

Experience With Underground Traffic

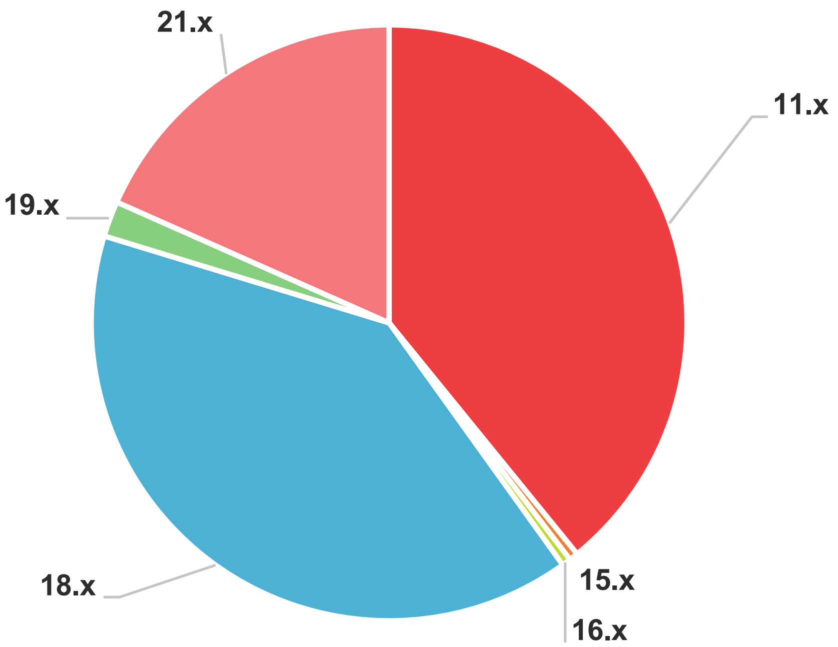
Campaign Results (A different Ad network)

- Budget: $6.00
- Campaign Time: 3 hours
- Total clicks according to agreement: 3,000
- Total clicks actual number: 2,742

Trustwave®
Smart security on demand

Underground Traffic

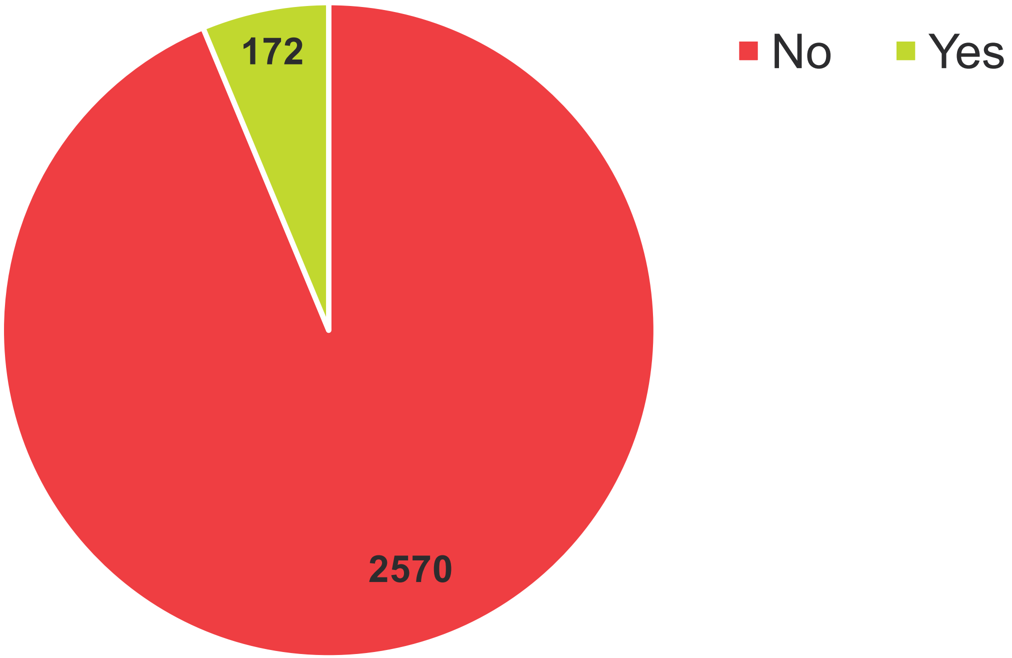
Flash Versions Breakdown of 206 IE Users



Trustwave®
Smart security on demand

Underground Traffic

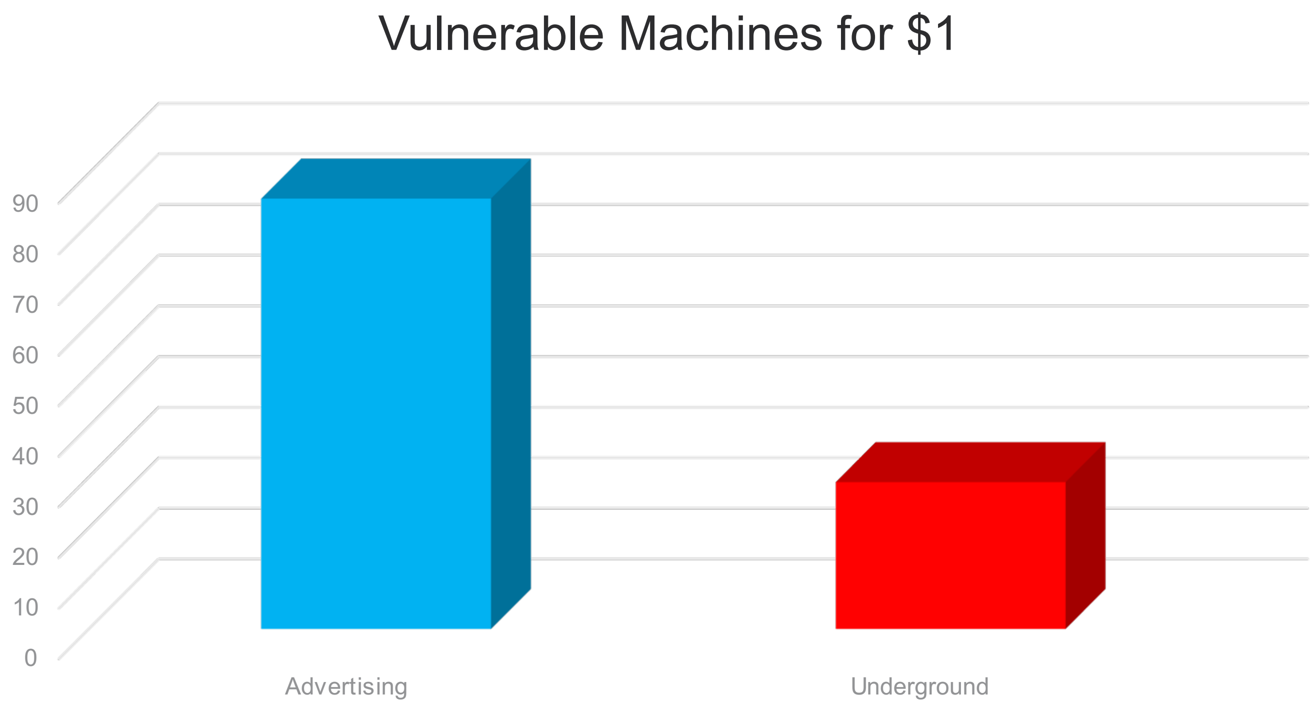
Amount of Vulnerable Machines



Trustwave®
Smart security on demand

Campaigns Summary

Advertising VS. Underground



Trustwave®
Smart security on demand

Perspectives

Trustwave®

The Online Advertising Market Perspective

A wake up call

- IAB: Malvertising is costing the American marketing and media industry: $1.1 billion
- IAB: Out of $1.1 b, $780m is lost because of ad blocking
- IAB: a "call to action” asking industry leaders to step in and contribute to fight corruption in the digital advertising supply chain ecosystem
- AdWords & DoubleClick will block Flash by June 30th

Trustwave®
Smart security on demand

The Online Advertising Market Perspective

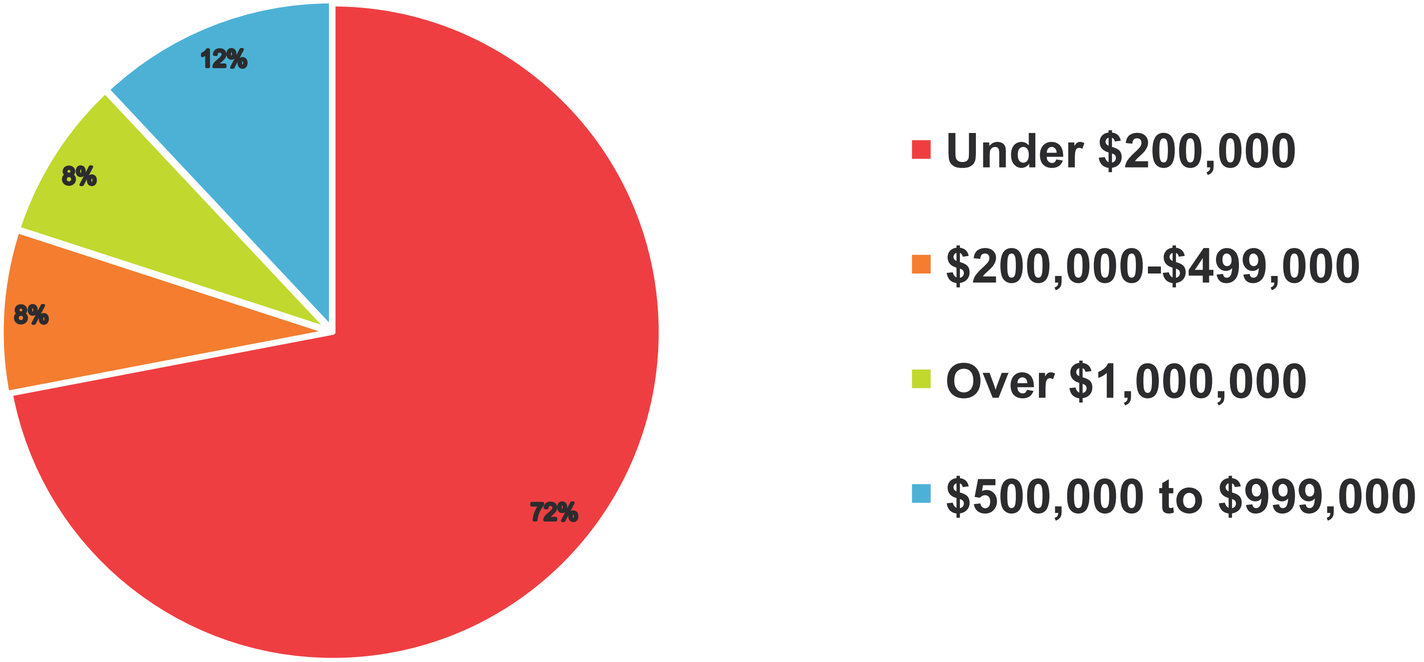
A wake up call

- IAB: Malvertising is costing the American marketing and media industry: $1.1 billion
- IAB: Out of $1.1 b, $780m is lost because of ad blocking

Trustwave®
Smart security on demand

The Online Advertising Market Perspective

Publishers losses because of ad blockers



Trustwave®
Smart security on demand

Web Users' Perspective

Ad blocking is the name of the game

- According to KPMG's survey in UK:
  - 60% of 16-24 year-olds in UK plan to make use of ad blocking in the next six months
  - 55% of people earning more than £55,000 are using or are planning to use ad blocking in the next six months

- According to IAB UK:
  - 22% of British adults online are currently using ad blocking

- Mobile operator Three to introduce adblocking across its UK and Italian networks

Trustwave®
Smart security on demand

Publishers' Perspective

Bad reputation

- Less visitors
- Bad reputation within search engine = down the result list
- Income disaster

Trustwave®
Smart security on demand

Browsers' Perspectives

- Google Chrome: "HTML5 by Default" by 4th Q of 2016
- Microsoft's Edge will pause Flash ads on the upcoming updates
- Opera featured last March a native ad blocker
- "Brave" is a new browser which automatically blocks ads

Trustwave®
Smart security on demand

Web Criminal's Perspective

Trustwave®
Smart security on demand

Reduction of Attack Surface

Staying safe is in your hands

- Plugins – Click to Play
- Use the most advanced browsers like Chrome and Edge
- Keep your browser and its plugins constantly updated

Trustwave®
Smart security on demand

Q&A