FIVE DAYS IN THE LIFE OF A CMS BRUTE FORCING MALWARE

Anna Shirokova

Cognitive Threat Analytics

@**AnnaBandicoot**

Veronica Valeros

Cognitive Threat Analytics

@**verovaleros**

WHO WE ARE?

Anna

- Threat Researcher Cognitive Threat Analytics, Prague, Czech Republic

Veronica

- Threat Researcher Cognitive Threat Analytics, Prague, Czech Republic
- Co-founder of MatesLab Hackerspace in Argentina
- Core member of Security Without Borders (@swborders)

ACKNOWLEDGEMENT

Sebastian García:

http://ar.linkedin.com/in/sebagarcia
https://www.researchgate.net/profile/Sebastian_Garcia6
https://stratosphereips.org/category/dataset.html
@eldracote

WHAT THIS TALK IS ABOUT?

WHAT THIS TALK IS NOT ABOUT?

POPULAR TARGET

~5% of the Internet websites built with WordPress

AUTHENTICATION METHOD

/wp-login.php

/xmlrpc.php

/administrator/index.php

` ?option=com login

/?q=user

/?q=user/login

/xmlrpc.php

BRUTE FORCING ATTACK

Trying different credentials until the correct one found

SIMPLE AUTOMATED WORKS

SATHURBOT

rosencraft #1

Members
12 posts
OFFLINE

Posted 28 June 2013 - 09:41 PM

My girlfriend downloaded and ran this file "x264 Video Codecs XP-Win7.exe" on her windows 7 computer. She got it from a torrent and the file results the following on virus total scan

https://www.virustotal.com/it/file/b19e0a4855ce7af346ae67a2479a3826d54909793f923bf48498394e2c02dfb0/analysis/

I am sure that is not a "safe" file to run on a windows computer.

File information

Identification | Details | Content | Analyses | Submissions | ITW | Behaviour | Comments

2013-05-01 15:28:22	2/46	ByteHero	-	1.0.0.1	20130425
2013-05-01 19:54:10	2/46	CAT-QuickHeal	-	12.00	20130430
2013-05-04 03:51:01	4/46	ClamAV	-	0.97.3.0	20130501
2013-05-04 08:00:49	3/46	Commtouch	-	5.4.1.7	20130501
2013-05-04 08:25:05	3/46	Comodo	-	16126	20130501
2013-05-05 02:47:35	3/44	DrWeb	BackDoor.HydraLoader.origin		
2013-05-05 04:37:02	3/46	ESET-NOD32	-	8285	20130501
2013-05-05 09:41:07	3/46	F-Prot	-	4.7.1.166	20130501
		F-Secure	-	11.0.19020.35	20130501
		Fortinet	-	5.0.43.0	20130501

Download file | Re-scan file | Close

MODULAR BOTNET

- backdoor
- downloader
- web crawler
- brute forcer

URL PATTERN OF THE INFECTED TORRENTS

www.verrolyne.co.uk/gilisoft-movie-dvd-creator-v6-x64-x86-download-torrent/

Apps | Reverse | tools | Home | Splunk 6.6.1 | linux | python | reading list | git | blogs | reg/search/stuff | CTA Performance-... | C&C Servers - Cybe... | spreadsheets | Other Bookmarks

Home / Uncategorized / GiliSoft Movie DVD Creator v6 x64 x86 download torrent

August 11, 2017

Share Ratio

GiliSoft Movie DVD Creator v6 x64 x86 download torrent

Download

Like us on Facebook:

Introduction:

The program can be converted and created types DVD disc, download DVD movie Creator is offered in full news. Make your drive can be almost any video format such as AVI, WMV, MPEG and others.

After the project is completedFor the video DVD Creator, it can be easily written to the carrier and then seen on the standard player in front of the TV, and can be seen on the computer, nothing will be forbidden -) Among other things, he melaksanakandukunganUntukMerakam ISO image after the addition The video you can crop,Add a watermark, add text and perform other similar operations.

Developer: Gili Mekka

License: Freeware

English

Size: MB

Operating System: Windows

How to Install:

» September 2017

» August 2017

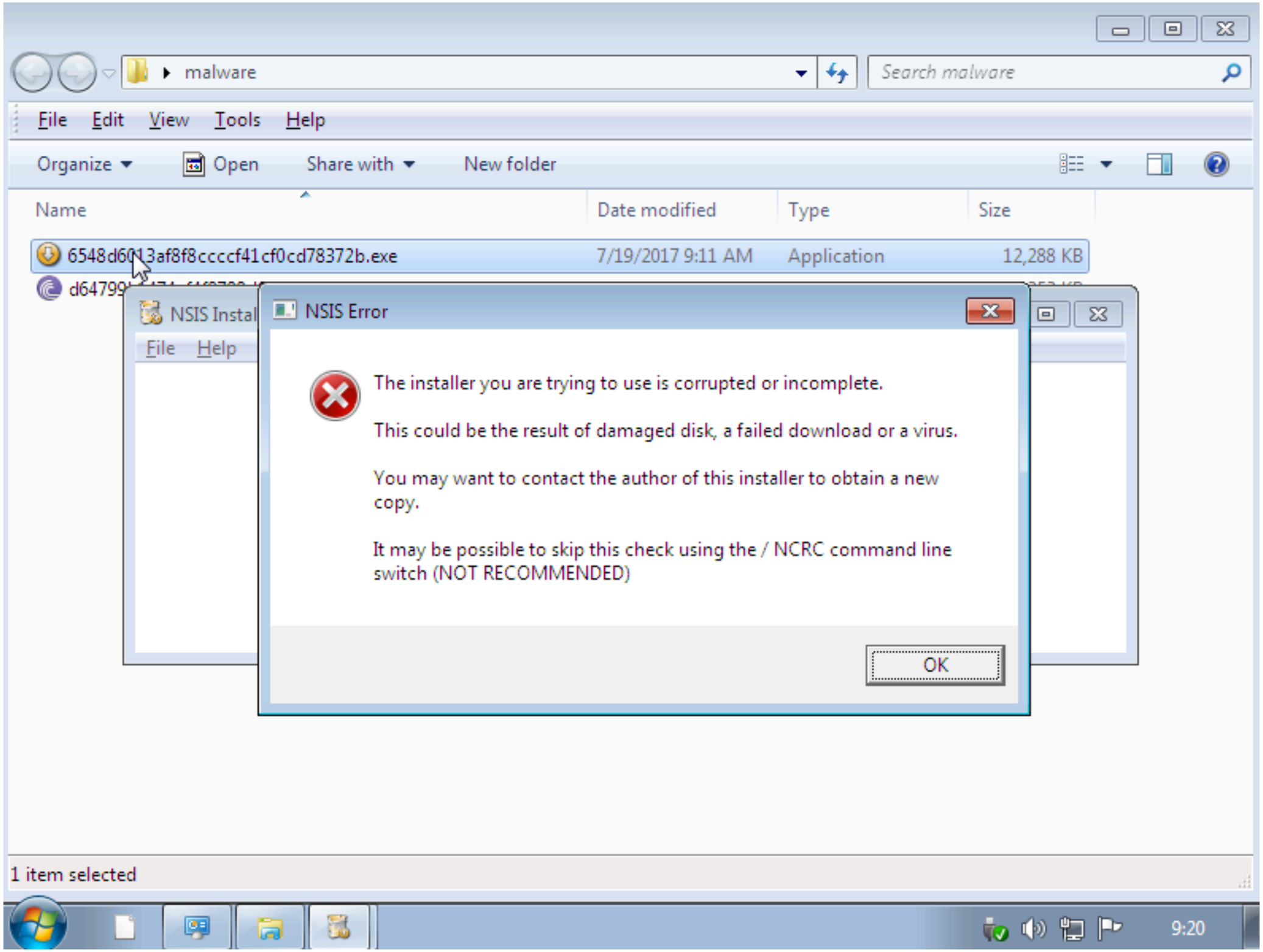
» July 2017

Search ... Search

Verrolyne Training Ltd
Get the Spirit of Achievement

www.verrolyne.co.uk/?30a227f6f31889a92c7be5f1b50fb5e4=127dca8d070bbb

INFECTION


malware
Search malware
File Edit View Tools Help
Organize
Open
Share with
New folder
Name
Date modified
Type
Size
6548d6013af8f8ccccf41cf0cd78372b.exe
7/19/2017 9:11 AM
Application
12,288 KB
NSIS Instal
File Help
NSIS Error
The installer you are trying to use is corrupted or incomplete.
This could be the result of damaged disk, a failed download or a virus.
You may want to contact the author of this installer to obtain a new copy.
It may be possible to skip this check using the / NCRC command line switch (NOT RECOMMENDED)
OK
1 item selected
9:20

CRAWLER

SEARCH ENGINES QUERY

http://www.bing.com/search?q=**makers**%20**manage**%20**manual**

abuse (42) access (18) account (18) ads (21) adsense (21) age (21) american (24) amp (87) analytics (18) android (69)
apple (18) apps (30) army (21) barbara (33) beauty (210) best (39) bridal (48) business (18) buy (21) center (21)
children (15) click (21) com (39) contouring (39) data (123) denied (30) development (18) difference (18)
download (36) drive (18) education (27) email (24) expert (18) face (15) facebook (27) flawless (42) food (30) game (27)
glowing (45) google (111) guide (48) hair (24) help (21) home (21) homeland (30) images (39)
information (21) ios (18) iphone (24) kardashian (42) keep (48) kim (33) law (18) leadership (27) learning (60)
library (21) list (27) makeup (75) marketing (24) natural (24) news (18) offensive (30) online (21) organic (66)
page (27) pass (15) please (27) posts (42) practice (87) private (78) products (24) report (162)
research (24) results (21) review (15) rmt (36) rodriguez (39) rt (36) sacred (33) safe (33) scam (27) search (30) security (18)
services (24) skin (57) smartphone (36) social (18) storm (27) strategic (36) support (24) tips (60) tutorial (27)
uploaded (21) users (18) validity (18) video (51) wars (30) web (21) website (18) wedding (45)

abuse (30) ads (31) adsense (27) adwords (24) age (54) amp (69) analytics (18) android (45) apk (15) app (21)
apple (18) army (21) barbara (36) beauty (195) best (24) block (18) body (15) book (18) bridal (42) car (21)
care (18) celebrity (18) com (21) community (15) contact (18) contour (42) data (162) denied (21) design (27)
developers (18) download (36) error (15) face (24) flawless (39) food (27) glowing (45)
google (103) guide (45) hair (45) health (18) help (49) highlight (21) homeland (36)
images (48) improve (18) information (42) international (18) iphone (36) kardashian (48) keep (18)
kim (57) leadership (24) learning (33) life (18) makeup (78) management (27) natural (27)
offensive (33) org (18) organic (72) page (42) pass (21) please (39) posts (24) practice (63)
private (66) products (24) reasons (21) report (135) results (16) reviews (21) rmt (21) rodriguez (30)
rt (21) sacred (36) safe (16) scam (48) school (24) search (21) security (39) site (21) skin (93)
smartphones (27) social (21) storm (24) strategic (21) student (21) support (27) tips (33) turn (18) tutorials (21)
university (21) uploaded (24) users (21) videos (42) wars (45) website (33) wedding (45) wikipedia (15)

p,k,c,a	r,j,g,q	t,e,d,o	f,c,m,t
g,g,k,o	d,p,b,r	k,n,q,b	k,o,j,l
n,q,j,i	g,d,j,e	e,k,s,m	l,l,j,l
p,p,o,c	o,c,l,l	f,h,b,s	r,c,s,h
p,l,b,b	q,i,d,t	o,i,k,e	l,h,t,b
g,g,k,q	d,d,g,p	d,j,b,a	j,f,h,m
o,l,i,g	g,q,b,t	g,i,o,l	d,k,l,m
t,c,g,p	n,t,m,k	j,s,j,i	e,k,o,e
c,g,h,d	r,i,e,b	g,e,n,t	e,q,d,i

WORDPRESS FRAMEWORK CHECK

http://[domain_name]/wp-login.php

BRUTE FORCE MODULE

ATTACK WITH XML-RPC

```
POST /xmlrpc.php HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Content-Length: 231
Host: www.venuscursos[REDACTED].com.br

<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
  <methodName>wp.getUsersBlogs</methodName>
  <params>
   <param><value>venuscursos[REDACTED]</value></param>
   <param><value>magic</value></param>
  </params>
</methodCall>
```

STANDARD CREDENTIAL'S COMBO

User name[domain_name]Password

POST /wp-login.php HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Content-Length: 232
Host: www.sanat[REDACTED].org

log=sanat[REDACTED]
&**pwd=magic**&wp-submit=Log+In&testcookie=1

NON STANDARD CREDENTIAL'S COMBO

User name[special_name]Password

```
POST /xmlrpc.php HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Content-Length: 227
Host: www.vodokanal[REDACTED].ru

<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
  <methodName>wp.getUsersBlogs</methodName>
  <params>
   <param><value>vdknl2017admin</value></param>
   <param><value>swimming</value></param>
  </params>
</methodCall>
```

ENUMERATION SCAN

Requesting numerical user IDs to reveal usernames

MORE THAN ONE TRY & PASSWORD

TIME:02:17:11.265496

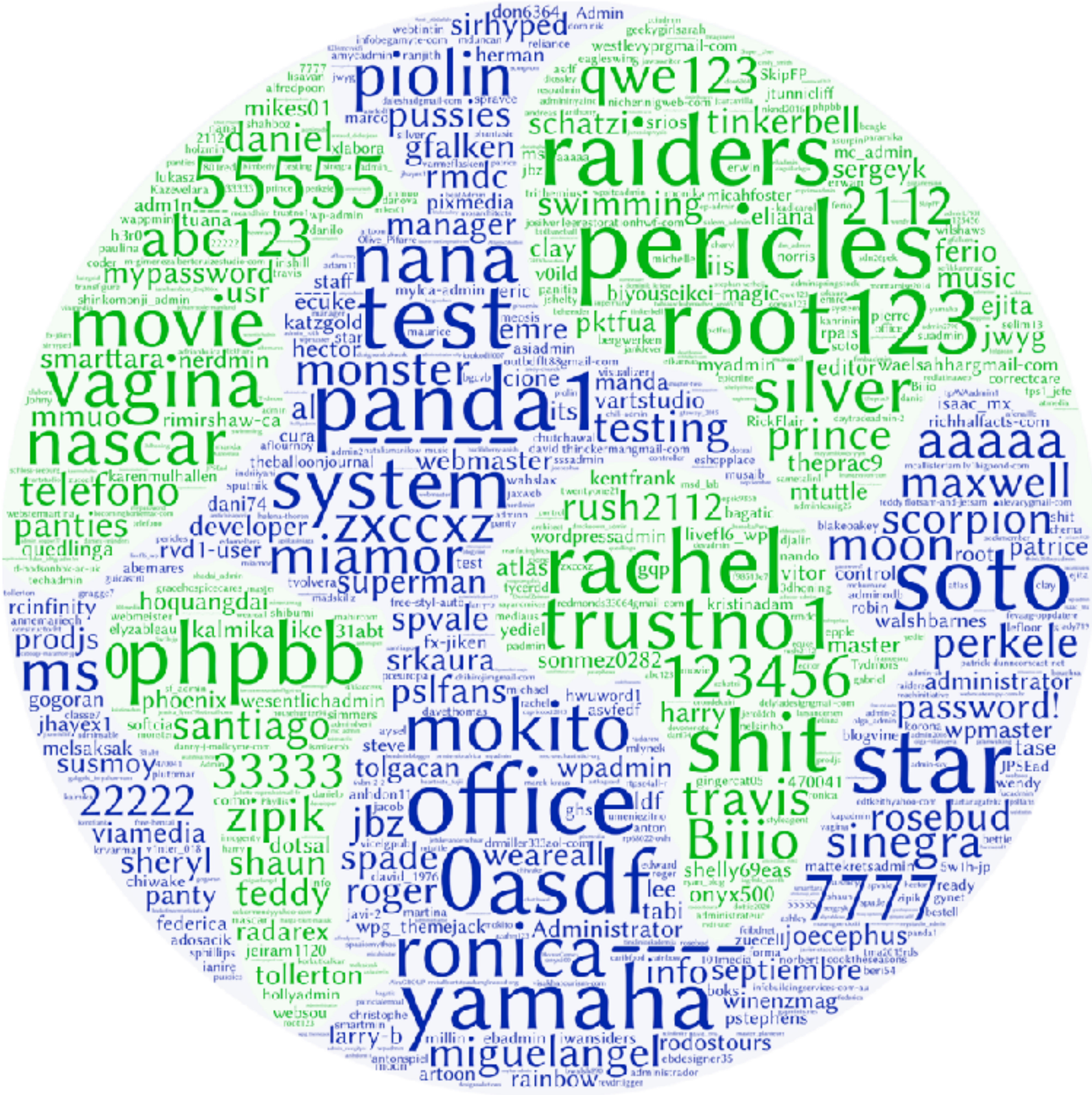
```
POST /xmlrpc.php HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Content-Length: 226
Host: www.raduapostol[REDACTED].ro

<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
 <methodName>wp.getUsersBlogs</methodName>
 <params>
  <param><value>raduapostol[REDACTED]</value></param>
  <param><value>mokito</value></param>
 </params>
</methodCall>
```

TIME:06:15:32.848090

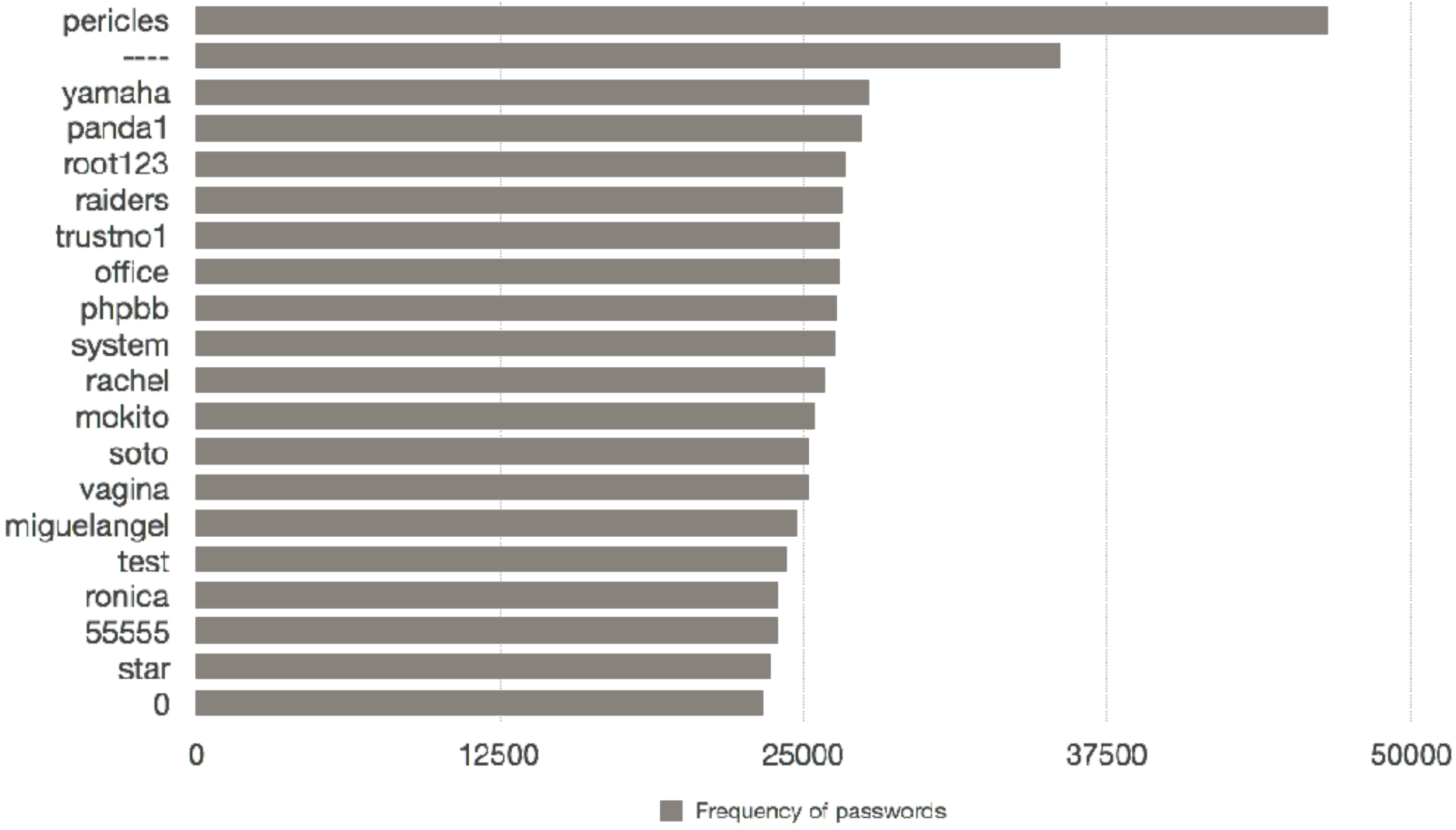
```
POST /xmlrpc.php HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Content-Length: 226
Host: www.raduapostol[REDACTED].ro

<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
 <methodName>wp.getUsersBlogs</methodName>
 <params>
  <param><value>raduapostol[REDACTED]</value></param>
  <param><value>system</value></param>
 </params>
</methodCall>
```



pericles
raiders
root123
test
panda1
office
yamaha
0asdf
ronica
system
nana
piolin
mokito
phpbb
shit
soto
star
rachel
trustno1
123456
7777
nascar
vagina
movie
55555
abc123
telefono
qwe123
2112
silver
zxccxz
miamor
maxwell
aaaaa
scorpion
moon
perkele
sinegra
rosebud
travis
Biiio
33333
22222
zipik
santiago
ms
sirhyped
pussies
gfalken
rmdc
manager
monster
webmaster
testing
prince
swimming
tinkerbell
schatzi
daniel
mikes01
mypassword
smarttara
nerdmin
mmuo
panties
quedlinga
developer
superman
hoquangdai
kalmika
spvale
srkaura
pslfans
phoenix
tolgacan
miguelangel
roger
spade
sheryl
shaun
teddy
radarex
tollerton
septiembre
info
joecephus
weareall
wpadmin
Administrator
password!
administrator
rush2112
music
ferio
ejita
jwyg
manda
vartstudio
theprac9
mtuttle
kentfrank
hector
katzgold
staff
herman
pixmedia
clay
eliana
sergeyk
mc_admin

TOP 20 PASSWORDS TRIED



TRIES TO BRUTE FORCE

QUORA:

GET http://www.quora.com/wp-login.php

GIPHY:

GET http://giphy.com/wp-login.php

SNAPCHAT:

GET http://snapchat.com/wp-login.php

TWITTER:

GET http://twitter.com/wp-login.php

SOUNDCLOUD:

GET http://soundcloud.com/wp-login.php

SHOPIFY:

GET http://www.shopify.com/wp-login.php

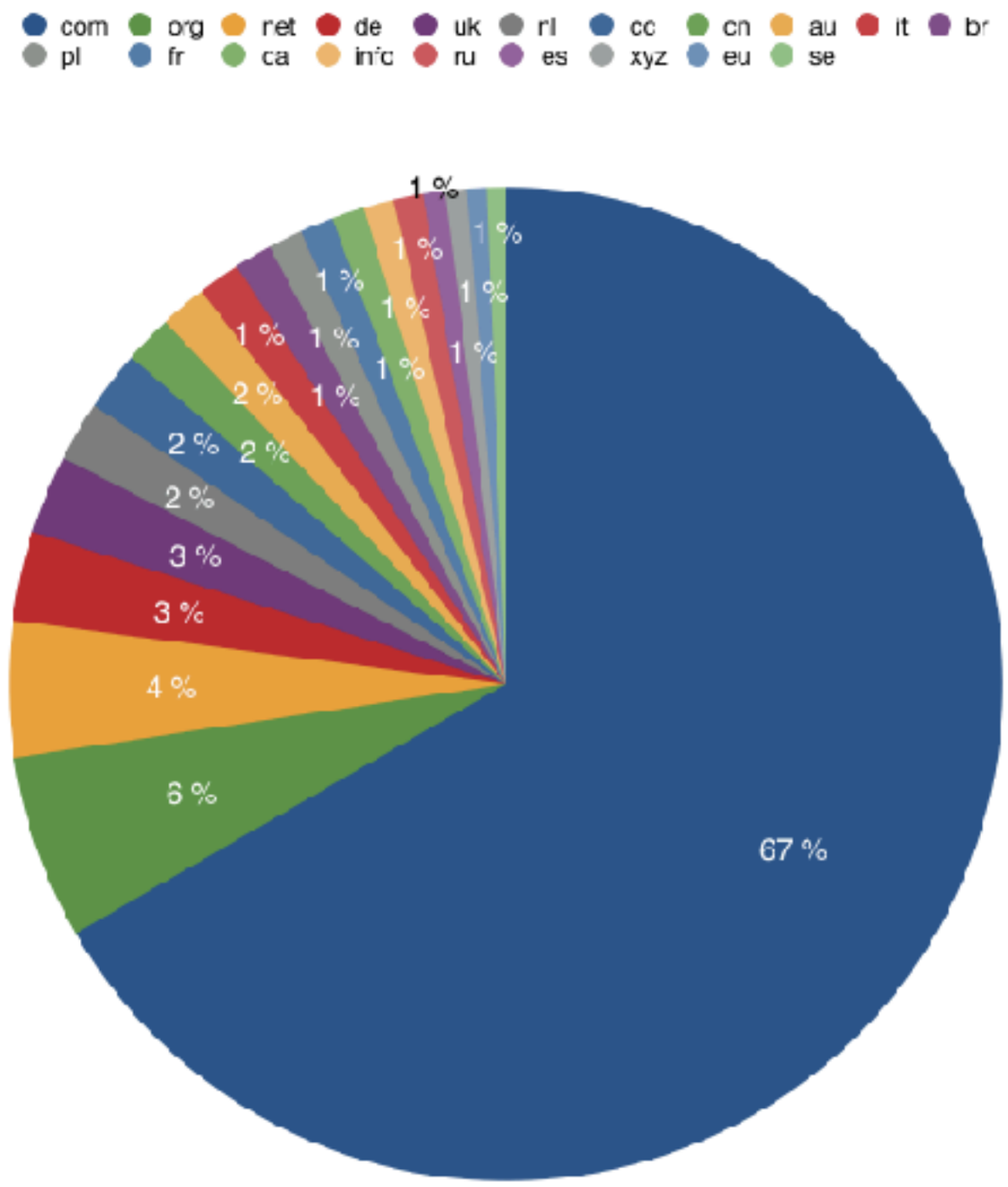
MOST COMMON TLDS TARGETED

gTLD

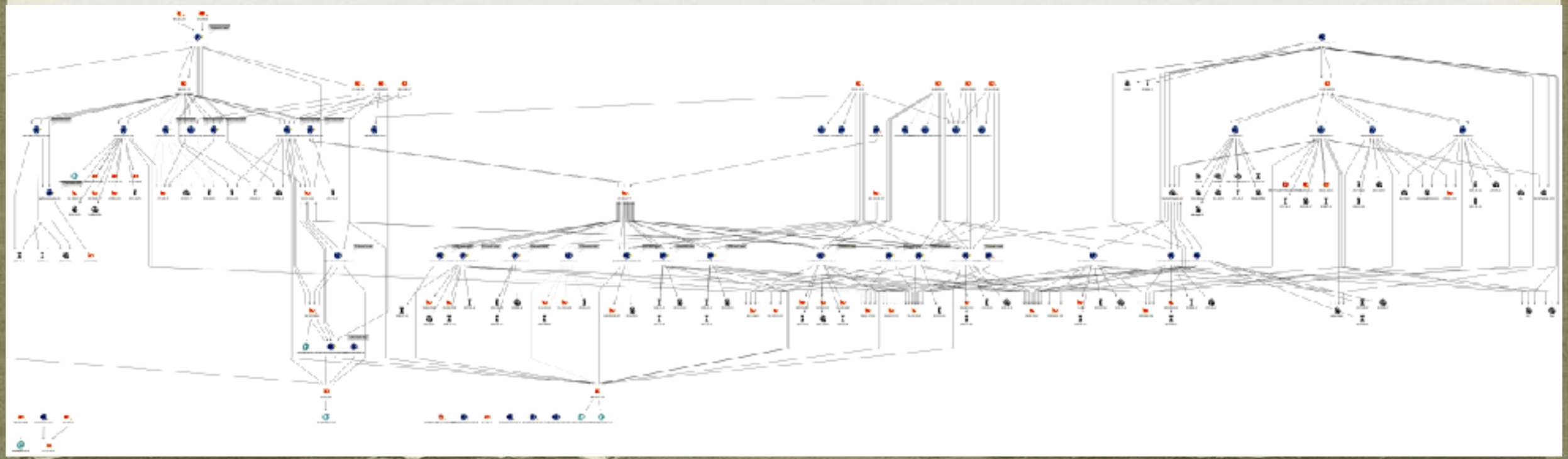
com	1552601
org	139582
net	102798
info	23288
xyz	16076
eu	14732

ccTLD

de	68078
uk	59681
nl	45528
cc	45419
cn	36527
au	35410
it	32400
br	28158
pl	26216
fr	25319
ca	24766
ru	21802
es	17372
se	14284



INFRASTRUCTURE



DIFFERENT VERSIONS

2015

SHA-256:
28f1cb771de05473b0c1cc2c21f3c437dc50cc6ab3c4c15ceefb21ea6e6b95fa

URL:
asdas2qw2aswasasdasd.in/wordpress.php?g=4bc87ed0379a11e5acf3080027535333&b=0&v=1

2016

SHA-256: -

URL:
edasdfdfwedzsczxczxcawaw1.xyz/wordpress.php?g=5f64c9690c7911e68d7c00155d0a1117&b=0&v=1

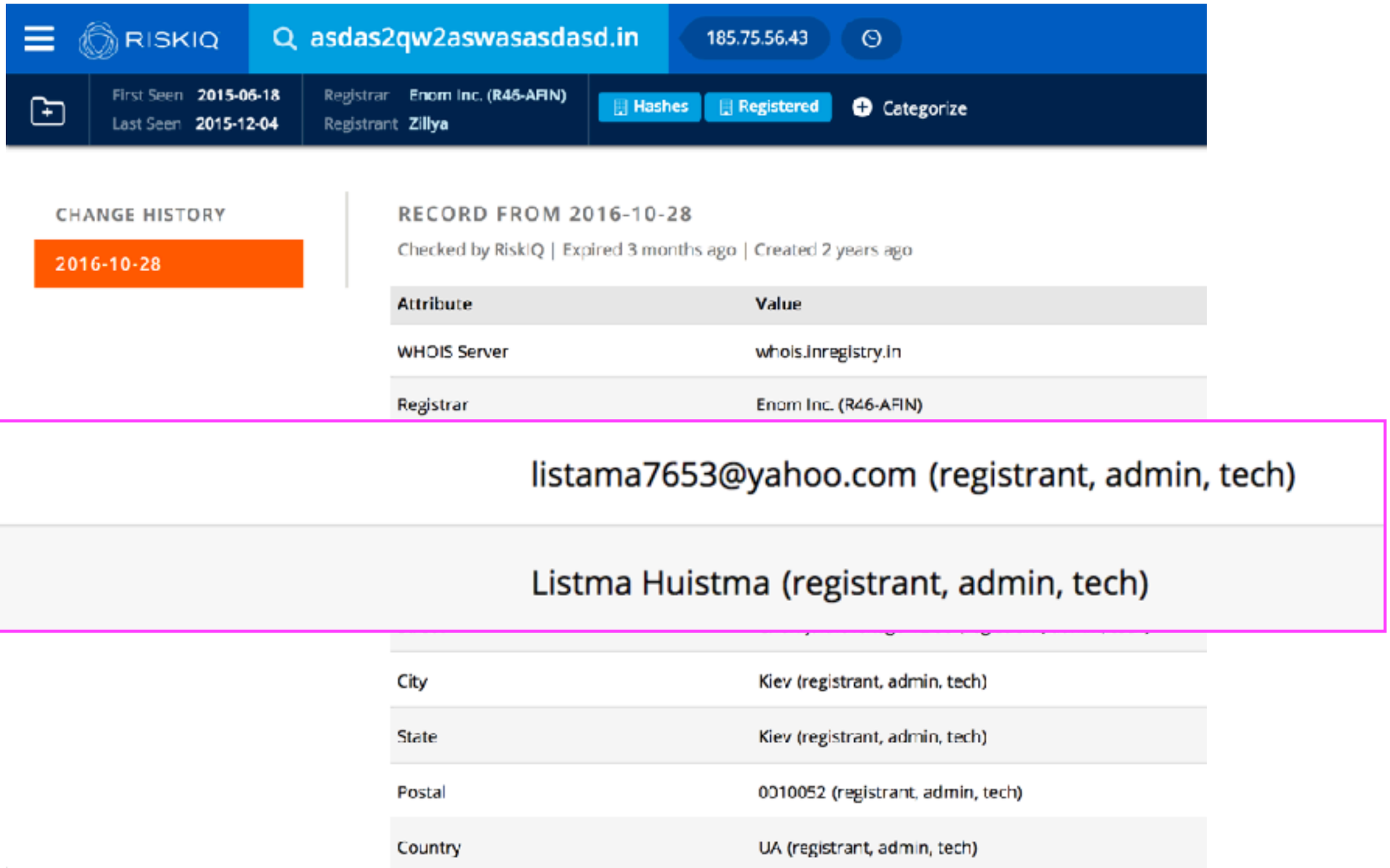
2017

SHA-256:
20ae9e5f8f26635c627afce5eaeeb749af459f55138c80f29da9d787ecc38f92

URL:
forcedsharetraktor.live/cocos/driver.php?g=e71847216cbc11e7b4e0080027e1e38a&v=3

LINKED EMAIL

URL:
asdas2qw2aswasasdasd.in/wordpress.php?g=4bc87ed0379a11e5acf3080027535333&b=0&v=1



CONNECTION SEQUENCE

1st C&C

forcedsharetraktor.live

217.23.6.215

2nd C&C

DNS TXT Record

zeusgreekmaster.xyz

3rd C&C

uromatalieslave.space

217.23.6.155

4th C&C

megafreecontentdelivery.club

Connectivity check

google.com

Crawling

Brute forcing

DOMAINS

FORCE

asdkjnasdiu3kadsomiljsd**force**.xyz
forcedsharedtraktor.live
new**forced**domainsherenow.club
justanother**forced**domain.xyz

MASTER

zeusgreek**master**.xyz
apollogreek**master**.xyz
jhasdkjanskdjnahsn**master**.xyz
jhasdkjanskdjnahsn**master**.info

SLAVE

uromatalie**slave**.space
mr**slave**lemmiwinkstwo.xyz
artemiso**slave**.xyz
crazyfucking**slave**mudak.xyz

BOOM

boom**boom**boomway.xyz
bada**boom**mail.xyz
bada**boom**sharetracker.xyz

DOMAINS

OTHER

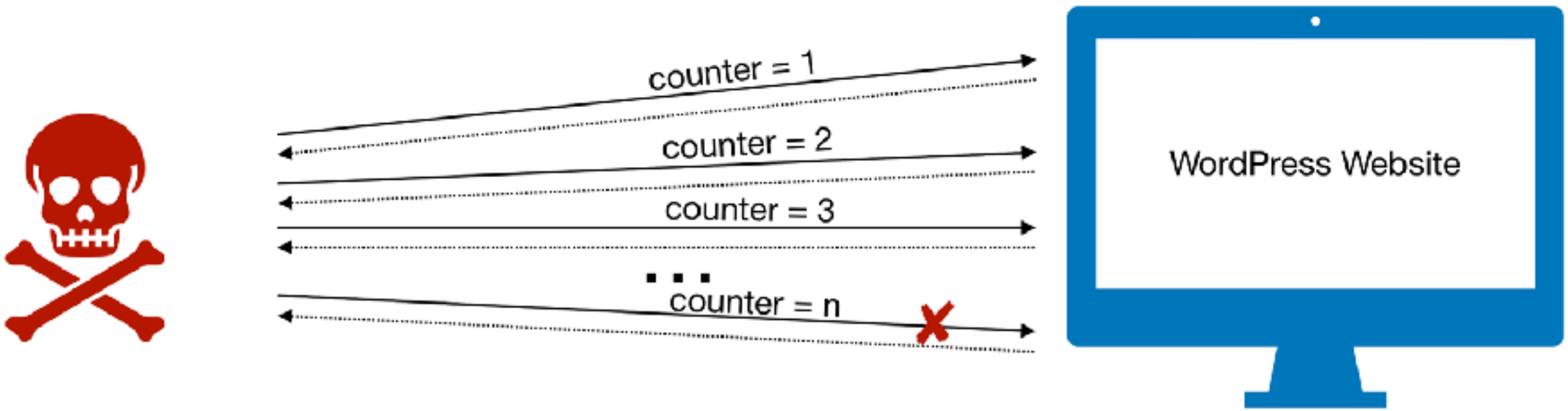
ed**asd**fdfwedzsczxczxcawaw1.xyz
mozilladownloadshare**space**.xyz
jhkabmasdjm2**asd**u7gjaysgdd**asd**.xyz
asxdq2sax**ads**dawdq2sasaddfsdfsf4ssfuckk.xyz
asxdq2sax**ads**dawdq2sasaddfsdfsf4ssfuck.xyz
kj**askd**hkaudhsnkq3uhaksjndkud3**asd**s.xyz
updateserviceshared**space**.xyz
adq3asd**asd**a3adfkunssssss.**space**
khkh**asd**89u8ojaodsijdkjaksd.link
kjh**askd**jhkuhk2qwskjakjshdkjh123kjs2.in
asdas2qw2aswasasd**asd**.in
kjanskduhi8**asd**askjdkn.in

TORRENT TRACKERS

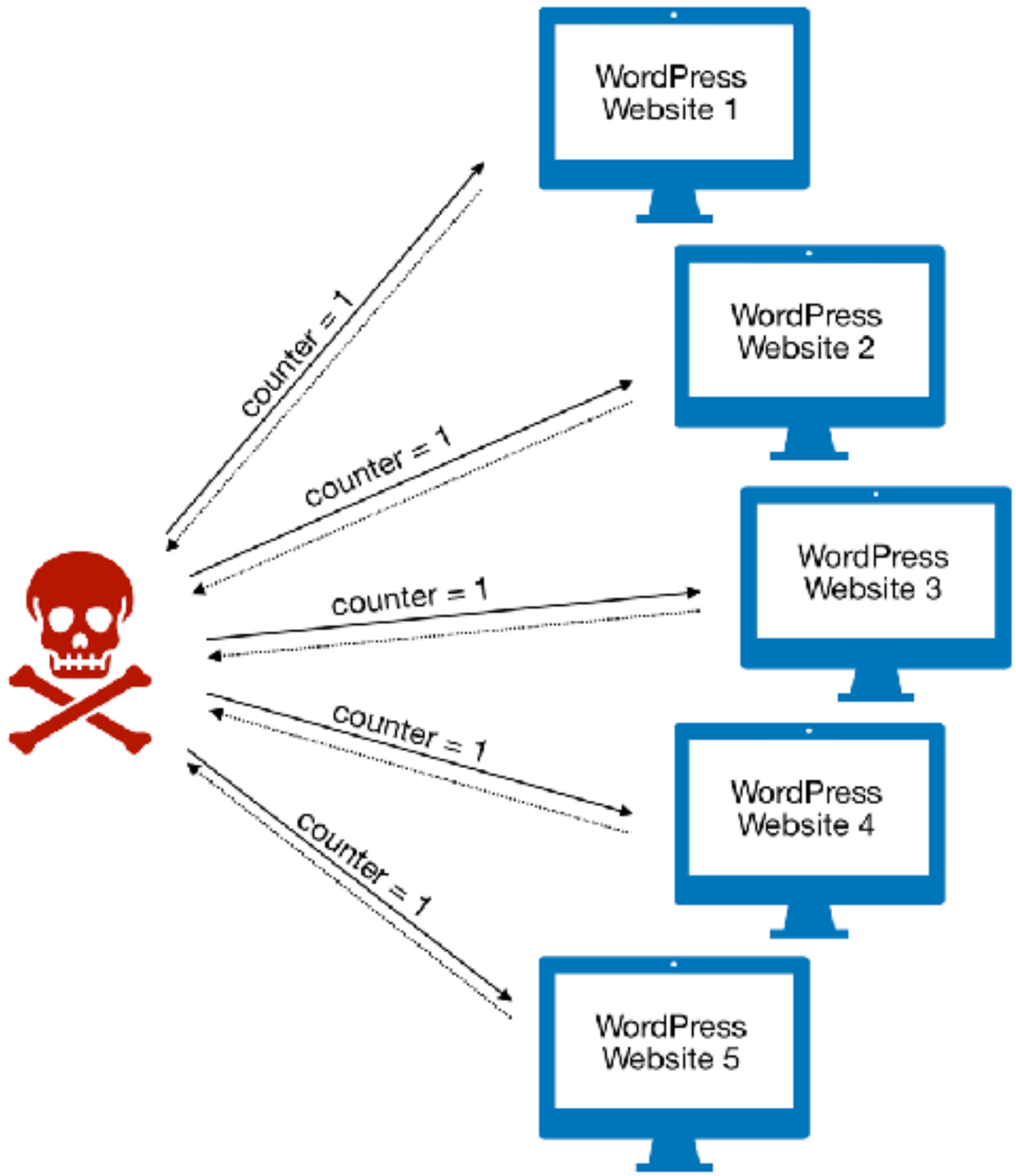
megafreecontentdelivery.com
megafreeshare**tracke**r.club
blablablablabla**traffic**.xyz
webdatasource**traffic**.xyz
happynewyear**traffic**.xyz
web**traffic**success.xyz
freemplemedia**tracker**.xyz
sharetorrentsonline**tracker**.xyz
coolfastcheap**tracker**.link
coolfastcheap**tracker**.xyz
meganewblablablan.in

DETECTION

VERTICAL BRUTE FORCING



HORIZONTAL BRUTE FORCING



WHY IT IS IMPORTANT?

QUESTIONS?

Sathurbot pcap

https://stratosphereips.org/category/dataset.html

Anna Shirokova

ashiroko@cisco.com

@AnnaBandicoot

Veronica Valeros

vvaleros@cisco.com

@verovaleros

THANK YOU!