KNOCK KNOCK... WHO'S THERE? ADMIN ADMIN AND GET IN!

An overview of the CMS brute forcing malware landscape

Anna Shirokova | Veronica Valeros

Cognitive Threat Analytics @AnnaBandicoot
Cognitive Threat Analytics @verovaleros
WHO WE ARE

ANNA

• Threat Researcher
  Cognitive Threat Analytics,
  Prague, Czechia

VERONICA

• Threat Researcher
  Cognitive Threat Analytics,
  Prague, Czechia
• Co-founder of MatesLab
  Hackerspace in Argentina
• Core member of Security
  Without Borders (@swborders)
WHAT DO WE DO?
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

\(~5\% \text{ of the Internet websites built with } \text{WordPress}\)
AUTHENTICATION METHOD

/wp-login.php
/xmlrpc.php

/administrator/index.php
` ?option=com login

/?q=user
/?q=user/login
/xmlrpc.php
VERTICAL BRUTE FORCE ATTACK
HORIZONTAL BRUTE FORCE ATTACK
BRUTE FORCING MALWARE
OVERVIEW
WHAT HAPPENED IN 2009?
2012 Stantinko

Stantinko  Teddy Bear Surfing Out of Sight

- 74.6% Search Parser
- 20.4% Brutplugin
- 3% Get HDD serial number
- 1.7% Plugin Installers remover
- 0.3% Radmin, Facebook bot & Zaxar cleaner
2013
FortDisco

https://www.arbornetworks.com/blog/asert/fort-disco-bruteforce-campaign/
2013
FortDisco

FortDisco

Blackhole EK

Stealrat botnet

Styx EK

https://www.arbornetworks.com/blog/asert/fort-disco-bruteforce-campaign/
2014
Mayhem

Mayhem

FortDisco

2015 Aethra

https://www.wordfence.com/blog/2015/12/aethera-botnet-attacks-wordpress-sites/
Infection Overview

https://www.researchgate.net/publication/299585015_Make_It_Count_an_Analysis_of_a_Brute-forcing_Botnet
2015
Troldesh

ВНИМАНИЕ!
Все важные файлы на всех дисках вашего компьютера были зашифрованы.
Подробности вы можете прочитать в файлах README.txt, которые можно найти на любом из дисков.

ATTENTION!
All the important files on your disks were encrypted.
The details can be found in README.txt files which you can find on any of your disks.
WHAT HAPPENED IN 2016?

https://www.wordfence.com/blog/2017/01/wordpress-botnet-monetization/
SIMPLE AUTOMATED WORKS
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/file/b19e0a4855ce7af346ae67a2479a3826d54909793f923bf48498394e2c02dfb0/analysis/

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

**File information**

<table>
<thead>
<tr>
<th>Identification</th>
<th>Details</th>
<th>Content</th>
<th>Analyses</th>
<th>Submissions</th>
<th>ITW</th>
<th>Behaviour</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-05-01 15:28:22</td>
<td>2/46</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013-05-01 19:54:10</td>
<td>2/46</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013-05-04 03:51:01</td>
<td>4/46</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013-05-04 08:00:49</td>
<td>3/46</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


2013-05-04 15:06:02  3/46  Eset  7.0.17.0  20130501
2013-05-05 02:47:35  3/44  ESET-NOD32  -  8285  20130501
2013-05-05 04:37:02  3/46  F-Prot  4.7.1.166  20130501
2013-05-05 09:41:07  3/46  F-Secure  11.0.19020.35  20130501
2013-05-05 09:41:07  3/46  Fortinet  5.0.43.0  20130501
MODULAR BOTNET

- backdoor
- downloader
- web crawler
- brute forcer
URL PATTERN OF THE INFECTED TORRENTS

GiliSoft Movie DVD Creator v6 x64 x86 download torrent

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 melakasankanandukunganUntukMerakam 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

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

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)
CRAWLER MODULE
http://www.bing.com/search?q=makers%20manage%20manual
<table>
<thead>
<tr>
<th>p,k,c,a</th>
<th>r,j,g,q</th>
<th>t,e,d,o</th>
<th>f,c,m,t</th>
</tr>
</thead>
<tbody>
<tr>
<td>g,g,k,o</td>
<td>d,p,b,r</td>
<td>k,n,q,b</td>
<td>k,o,j,l</td>
</tr>
<tr>
<td>n,q,j,i</td>
<td>g,d,j,e</td>
<td>e,k,s,m</td>
<td>l,l,j,l</td>
</tr>
<tr>
<td>p,p,o,c</td>
<td>o,c,l,l</td>
<td>f,h,b,s</td>
<td>r,c,s,h</td>
</tr>
<tr>
<td>p,l,b,b</td>
<td>q,i,d,t</td>
<td>o,i,k,e</td>
<td>l,h,t,b</td>
</tr>
<tr>
<td>g,g,k,q</td>
<td>d,d,g,p</td>
<td>d,j,b,a</td>
<td>j,f,h,m</td>
</tr>
<tr>
<td>g,l,i,g</td>
<td>g,q,b,t</td>
<td>g,i,o,l</td>
<td>d,k,l,m</td>
</tr>
<tr>
<td>t,c,g,p</td>
<td>n,t,m,k</td>
<td>j,s,j,i</td>
<td>e,k,o,e</td>
</tr>
<tr>
<td>c,g,h,d</td>
<td>r,i,e,b</td>
<td>g,e,n,t</td>
<td>e,q,d,i</td>
</tr>
</tbody>
</table>
WORDPRESS FRAMEWORK CHECK

http://[domain_name]/wp-login.php
BRUTE FORCE MODULE
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]
&pwn=magic&wp-submit=Log+In&testcookie=1
NOT 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>
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>
TOP 20 PASSWORDS TRIED

- pericles
- yamaha
- panda1
- root123
- raiders
- trustno1
- office
- phpbb
- system
- rachel
- mokito
- soto
- vagina
- miguelangel
- test
- ronica
- 55555
- star
- 0

Frequency of passwords
TRIES TO BRUTE FORCE

QUORA:

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

<table>
<thead>
<tr>
<th>Domain</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>com</td>
<td>1552601</td>
</tr>
<tr>
<td>org</td>
<td>139582</td>
</tr>
<tr>
<td>net</td>
<td>102798</td>
</tr>
<tr>
<td>info</td>
<td>23288</td>
</tr>
<tr>
<td>xyz</td>
<td>16076</td>
</tr>
<tr>
<td>eu</td>
<td>14732</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>de</td>
<td>68078</td>
</tr>
<tr>
<td>uk</td>
<td>59681</td>
</tr>
<tr>
<td>nl</td>
<td>45528</td>
</tr>
<tr>
<td>cc</td>
<td>45419</td>
</tr>
<tr>
<td>cn</td>
<td>36527</td>
</tr>
<tr>
<td>au</td>
<td>35410</td>
</tr>
<tr>
<td>it</td>
<td>32400</td>
</tr>
<tr>
<td>br</td>
<td>28158</td>
</tr>
<tr>
<td>pl</td>
<td>26216</td>
</tr>
<tr>
<td>fr</td>
<td>25319</td>
</tr>
<tr>
<td>ca</td>
<td>24766</td>
</tr>
<tr>
<td>ru</td>
<td>21802</td>
</tr>
<tr>
<td>es</td>
<td>17372</td>
</tr>
<tr>
<td>se</td>
<td>14284</td>
</tr>
</tbody>
</table>
FROM V.1 TO V.3

2015
SHA-256: 28f1cb771de05473b0c1cc2c21f3c437dc50cc6ab3c4c15ceefb21ea6e6b95fa
URL: asdas2qw2aswasasdasd.asdasd.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

FROM V.1 TO V.3

2015
SHA-256: 28f1cb771de05473b0c1cc2c21f3c437dc50cc6ab3c4c15ceefb21ea6e6b95fa
URL: asdas2qw2aswasasdasd.asdasd.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

Email
listama7653@yahoo.com (registrant, admin, tech)

Name
Listma Huistma (registrant, admin, tech)

- Street: Chernjakovskogo 12 35 (registrant, admin, tech)
- City: Kiev (registrant, admin, tech)
- State: Kiev (registrant, admin, tech)
- Postal: 0010052 (registrant, admin, tech)
- Country: UA (registrant, admin, tech)
DOMAINS

FORCE

asdkjnasdiu3kadsomiljsdforce.xyz
forcedsharedtraktor.live
newforceddomainsherenow.club
justanotherforceddomain.xyz

MASTER

zeusgreekmaster.xyz
apollogreekmaster.xyz
jhasdkjanskidjnahsmaster.xyz
jhasdkjanskidjnahsmaster.info

SLAVE

uromatalieslave.space
mrsleslemmiwinkstwo.xyz
artemisoslave.xyz
crazynfuckingslavemudak.xyz

BOOM

boomboomboomway.xyz
badaboommail.xyz
badaboomsharetracker.xyz
**OTHER**
edasdfwedzxcxcawaw1.xyz
mozilladownloadshare.space.xyz
jhkabmasdjmsdu7gjaysgddasd.xyz
asxdq2saxadsdawdq2sasaddfsdfsfsf4ssfuckk.xyz
asxdq2saxadsdawdq2sasaddfsdfsfsf4ssfuckk.xyz
kjaskdhkaudhsnkq3uhaksjndkud3asd.s.xyz
updateserviceshared.space.xyz
adq3asdasda3adfkunssssss.space
khkhasd89u8ojaodsijdkjaksd.link
kjhasdkjhkuhk2qwskjakjshdkjh123kjs2.in
asdas2qw2aswasasdasd.asd.in
kjanskduhi8asdasdkjdkn.in

**TORRENT TRACKERS**
megafreecontentdelivery.com
megafreesharetracker.club
blablablablabla.traffic.xyz
webdatasource.traffic.xyz
happynewyear.traffic.xyz
webtraffic.success.xyz
freemplemediatracker.xyz
sharetorrentsonline.tracker.xyz
coolfastcheaptracker.link
coolfastcheaptracker.xyz
meganeewblablablan.in
WHY SHOULD YOU CARE?
WHAT DID WE LEARN?

- CMS are being brute forced since the beginning
- Still successful due the weak passwords used
- Important component in malware ecosystem
- Brute force attacks are not well researched
- Brute forcing methodology is the same across malware
- Hard to measure the successful rate of this type of attacks
FUTURE WORK

- Measure the success rate
- How often the password changed
- Follow the hack
QUESTIONS?

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

Anna Shirokova
ashiroko@cisco.com
@AnnaBandicoot

Veronica Valeros
vvaleros@cisco.com
@verovaleros
THANK YOU!