Dorkbot: hunting zombies in Latin America

Pablo Ramos (@ramospablo)
Security Researcher

ESET


eset


10
adidas
AFA


eset
GIRA
ANTIVIRUS
eset

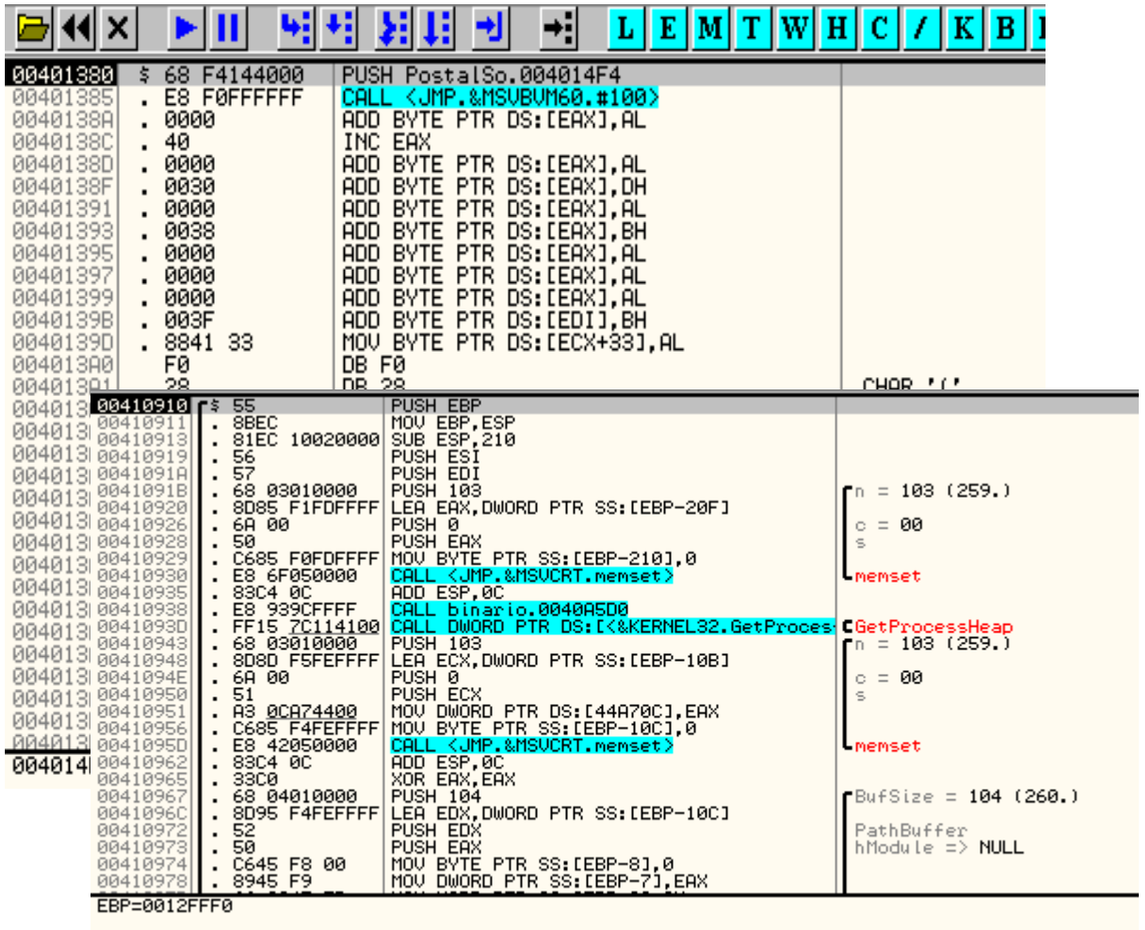
Dorkbot

(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).

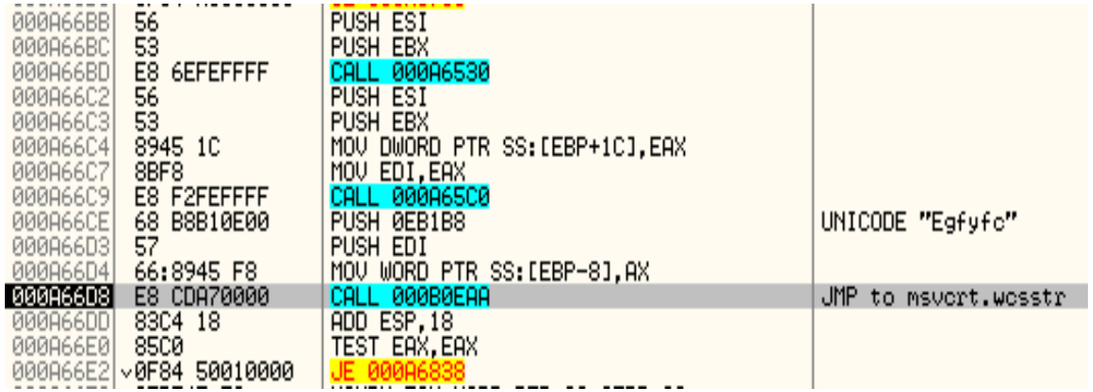
Signature	Date	Propagation techniques	Description
Win32/Dorkbot.A	April 4th, 2011	Autorun.inf, **LNK Spread**	First Dorkbot variant, not so widely spreaded
Win32/Dorkbot.B	May 16th, 2011	Includes Social Network spreading (**Facebook**, **Twitter**, etc)	Most used malware variant. Includes different versions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



Process infection

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

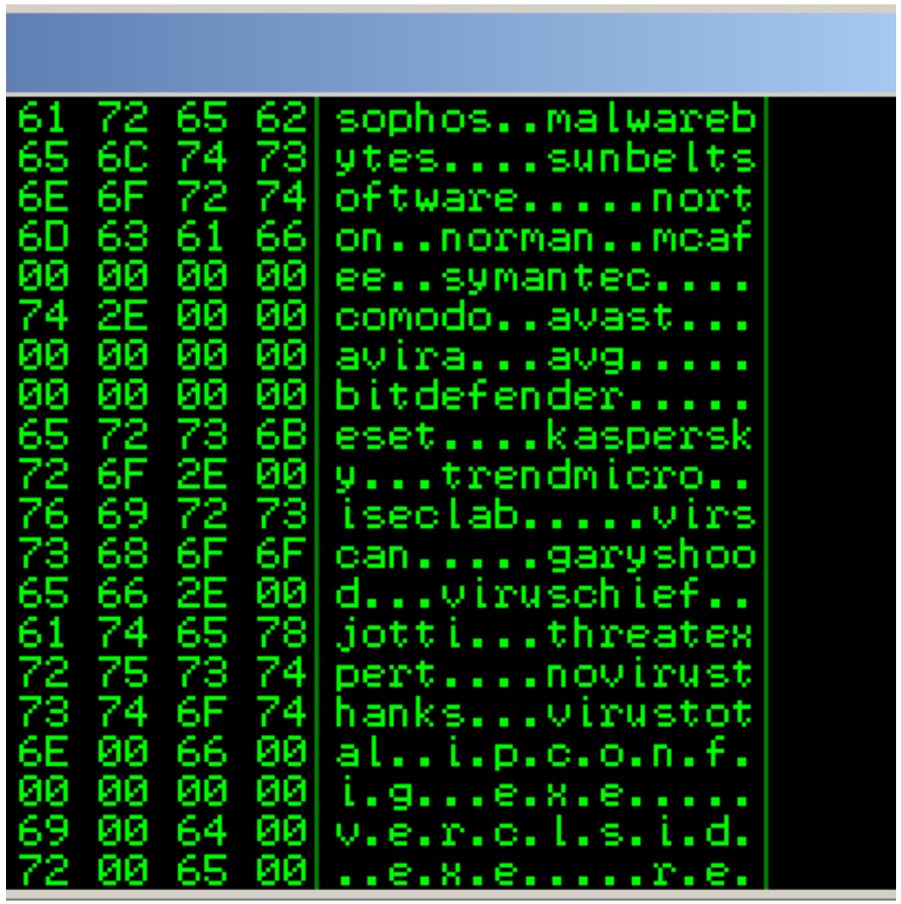
Hiding techniques



It hooks to *ZwQueryDirectoryFile* and *ZwEnumerateValueKey*.

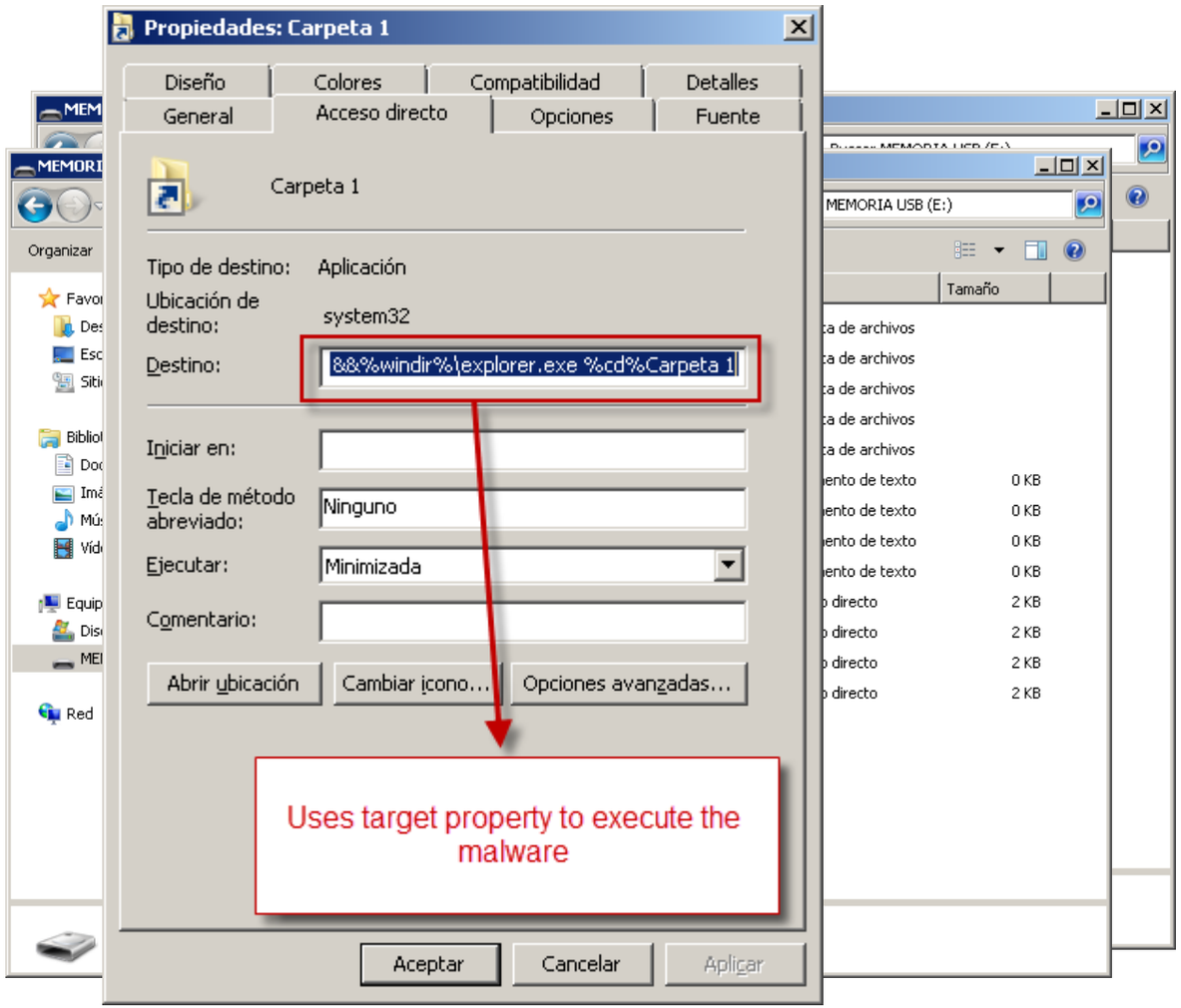
It tries to stay under the radar in an infected system. Why?

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

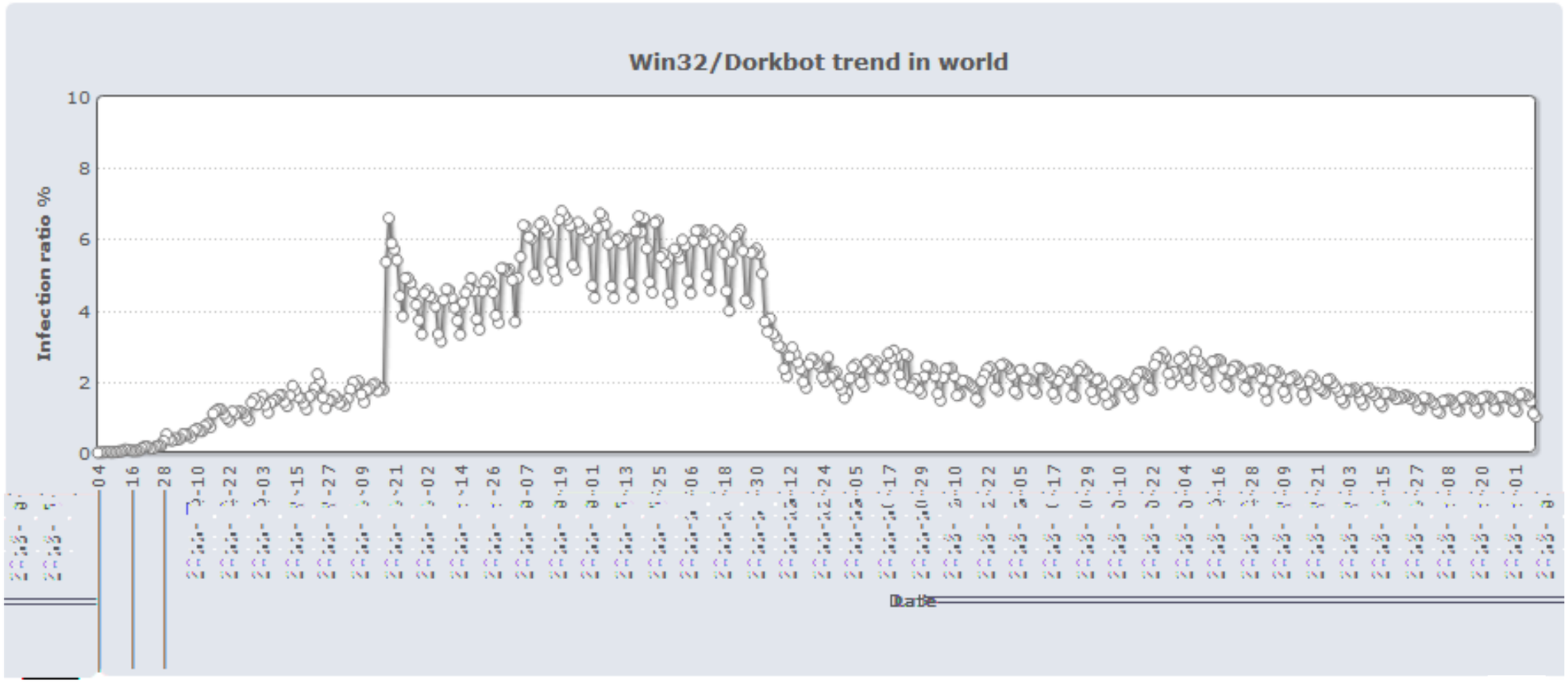
Using hooks to *DnsQuery_A* and *DnsQuery_W* it will prevent the infected computer to connect to many antivirus web sites.

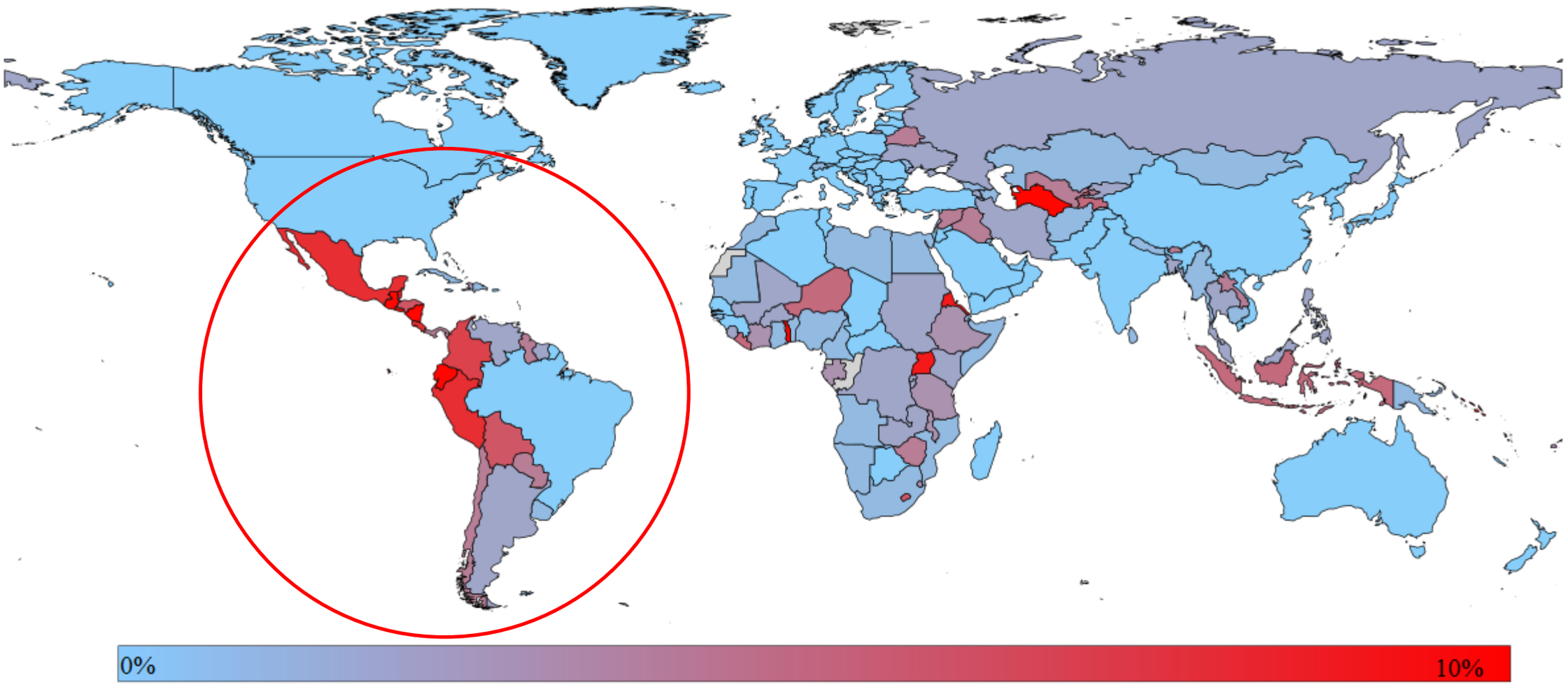


LNK spreading

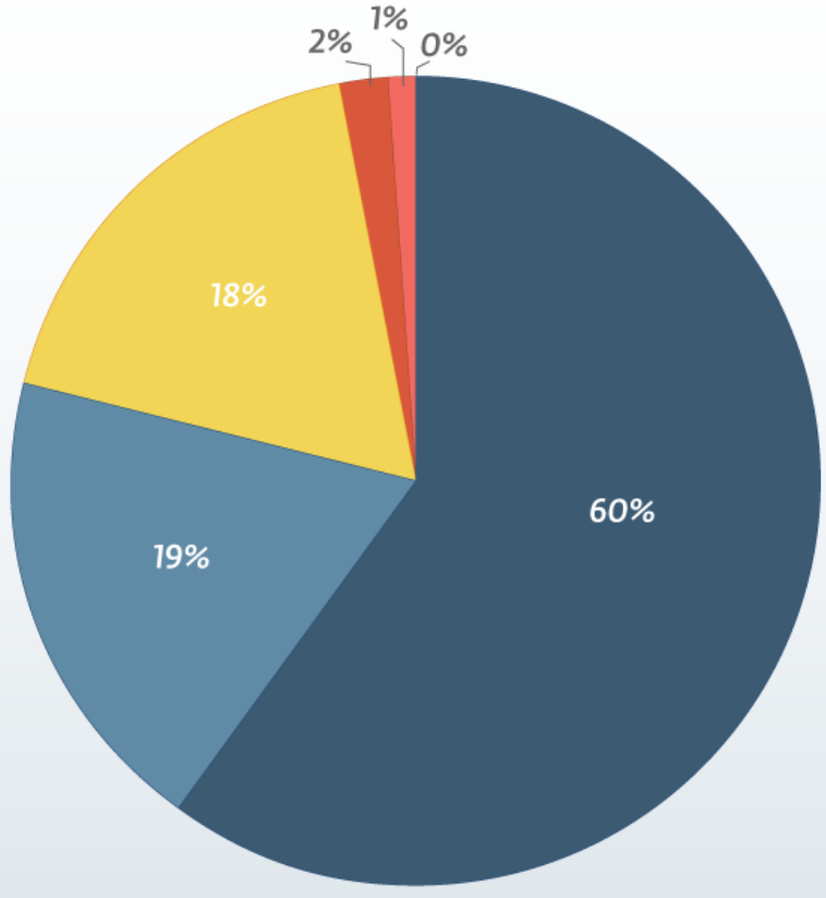
%windir%\system32\cmd.exe /c "start %cd%RECYCLER\<nombre_malware>.exe &&%windir%\explorer.exe %cd%Folder1

Dorkbot in Latin America


Win32/Dorkbot trend in world
Infection ratio %
10
8
6
4
2
0
Date


0%
10%

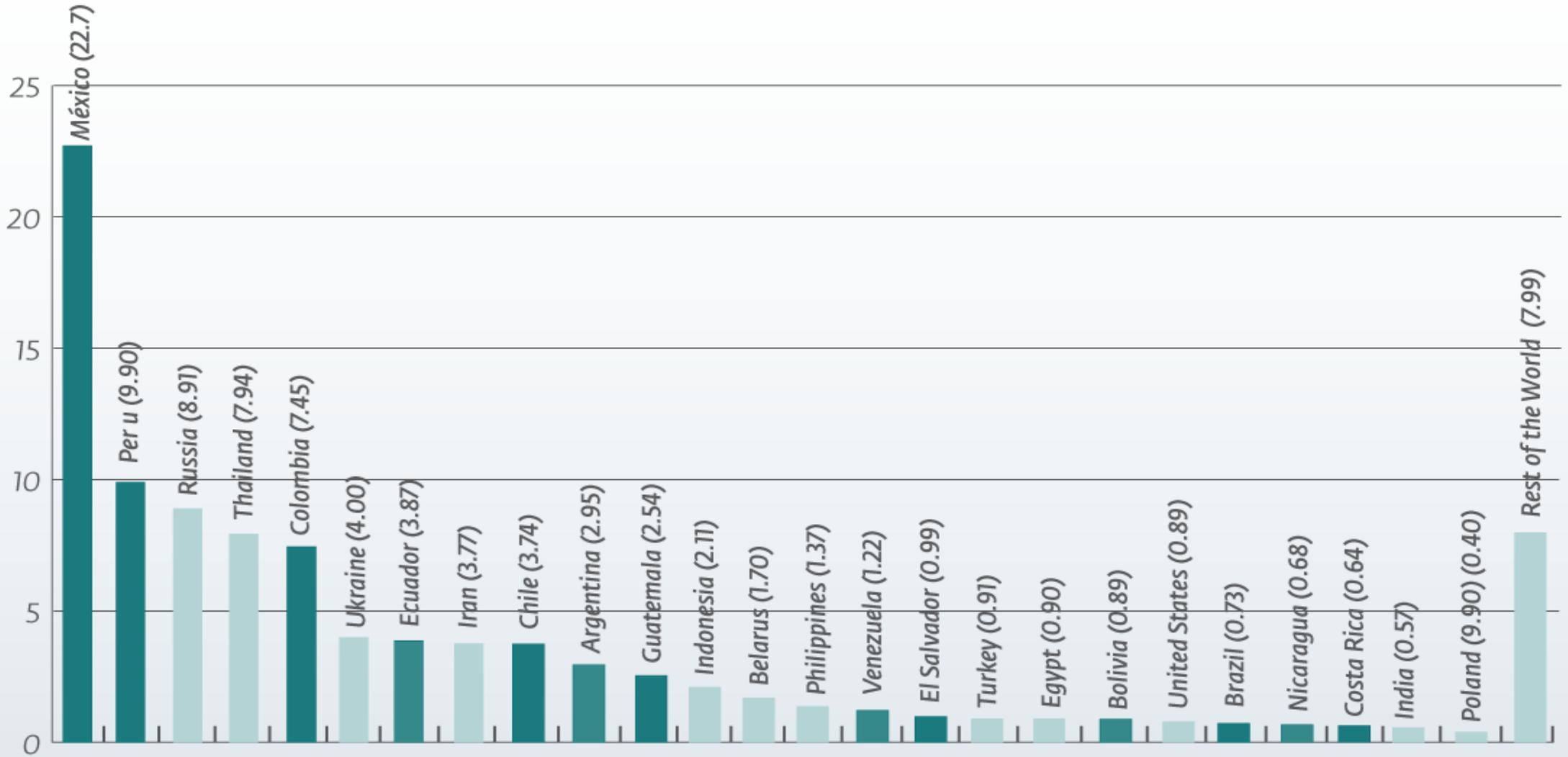
Detection by region



References

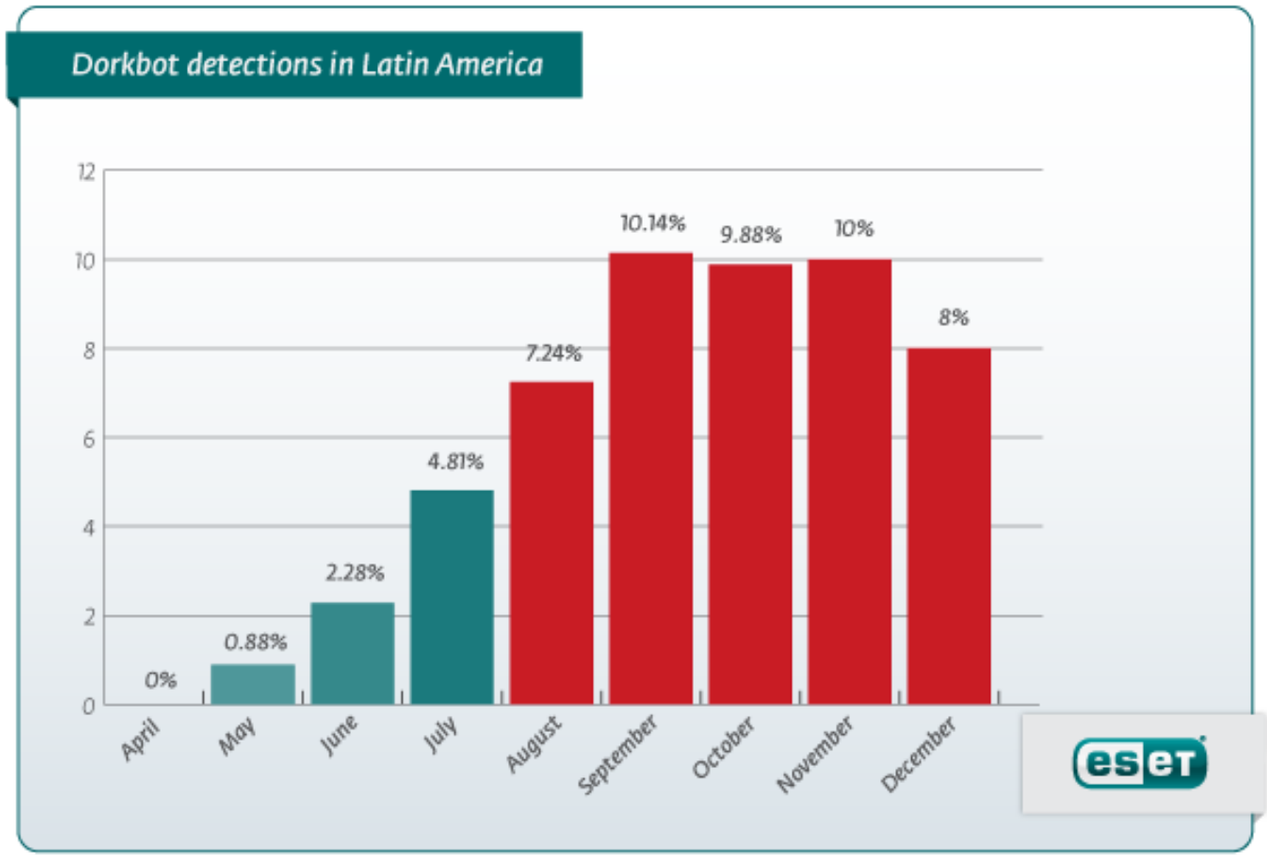
- Latin America & Caribbean
- Asia
- Europe
- Africa
- North America
- Oceania

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.



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

De: COM [mailto:noreply@sonico.com]
Enviado el: lunes, 06 de febrero de 2012 1:35

ideas

!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 deas.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 asi enviarnos al siguiente correo premio .cl

Descargar Formulario

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

Todos los Derechos Reservado

Ver más

Ver más

Recibiste una Postal Terra

Noticias te informa:

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

erra-NA 012-360-084

s mejores deseos que te han enviado, haz click en el siguiente nara:

com/PostalesTerra-NA012-360-084

oblema con el enlace, también puedes recuperarla desde aqui:

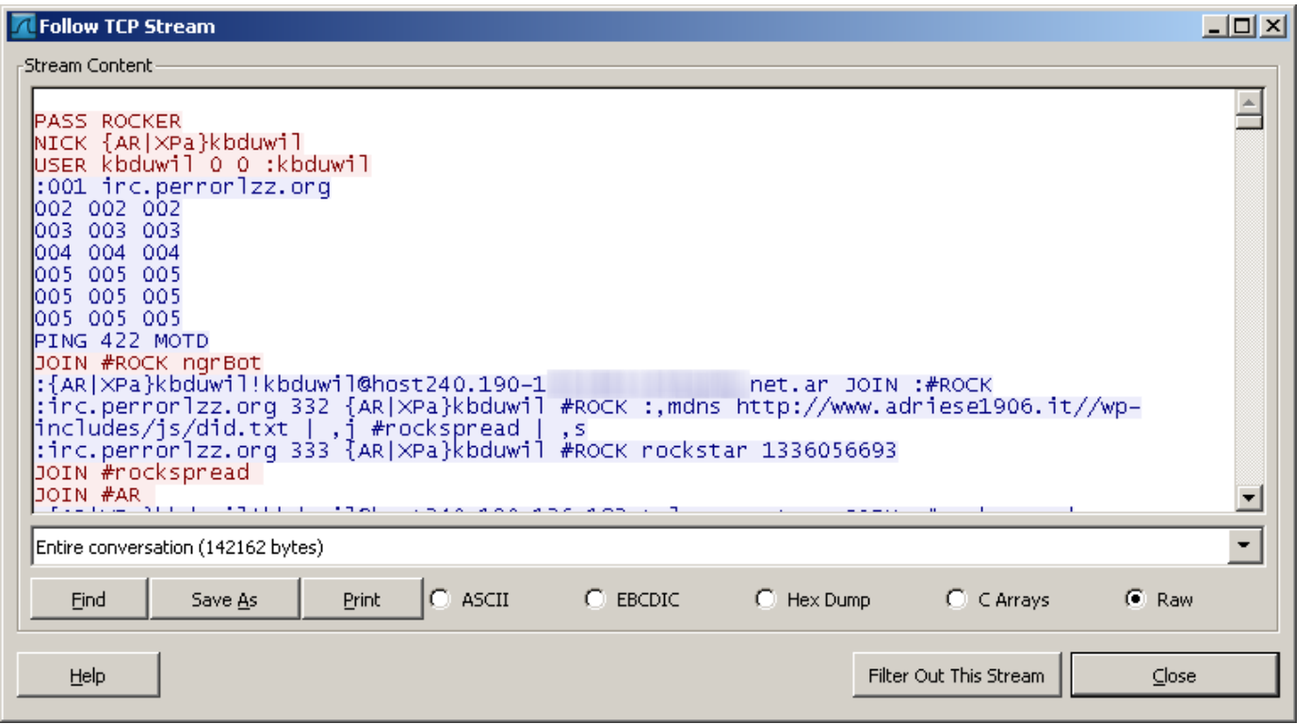
www.terra.com/PostalesTerra

UN MENSAJE MULTIMEDIA (MMS)

e han enviado un mensaje multimedia a través de nuestra portal ovistar.cl, el mensaje multimedia (MMS) sera borrado a los 10 ias.

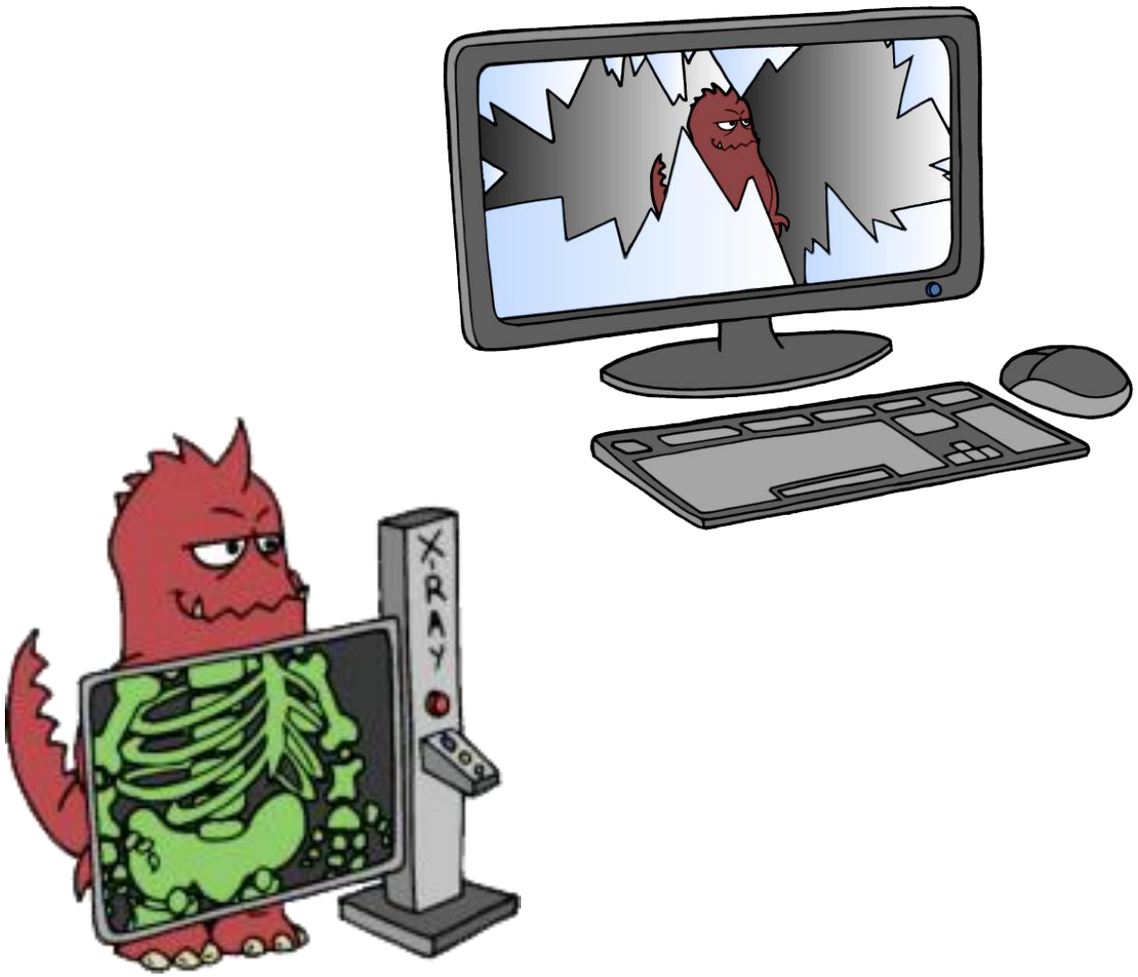
VER MENSAJE MULTIMEDIA

Este servicio es de Movistar.



Botnet tracking

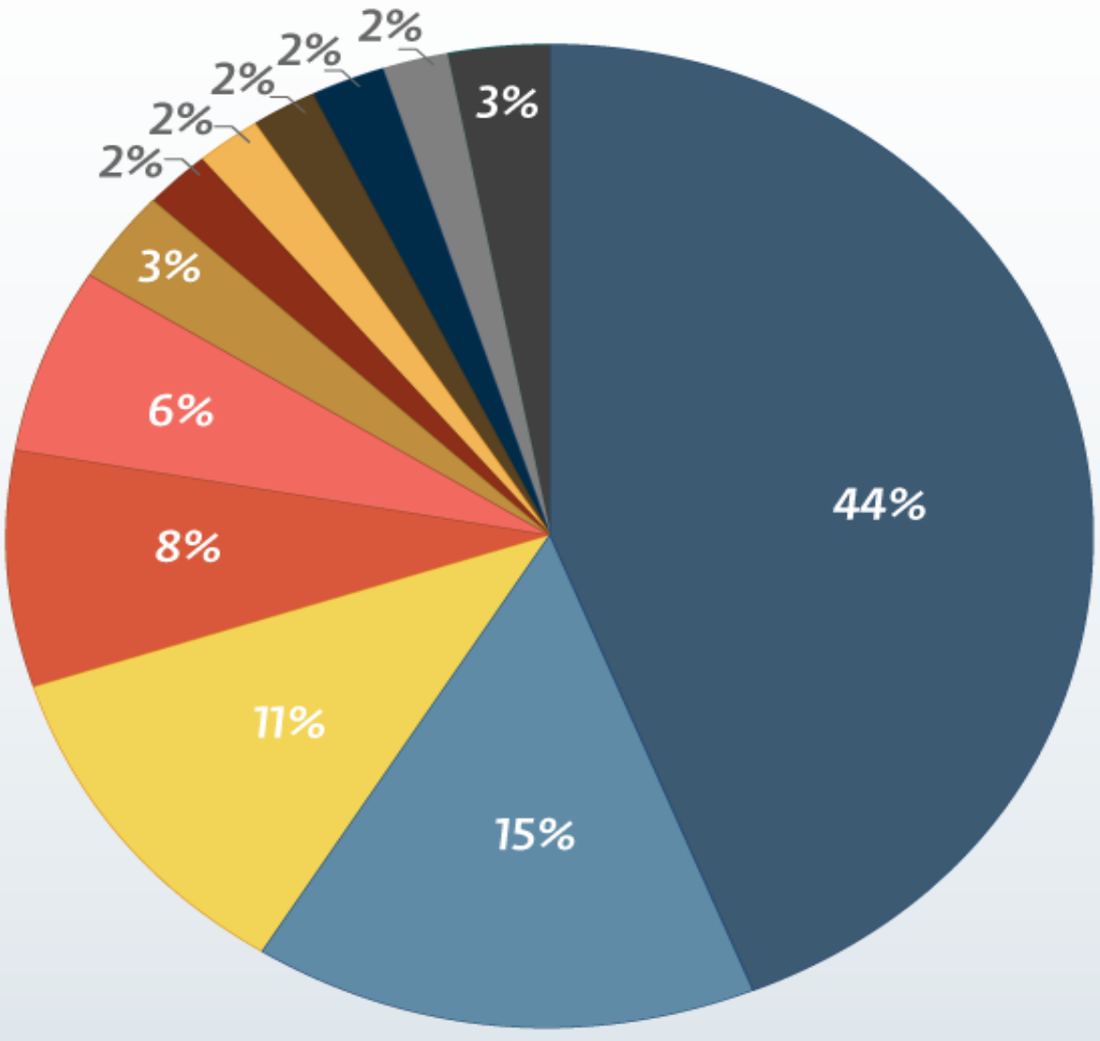
- Tracking cybercriminal campaigns, for more than 6 months.
- Viewing botnet activities and stats.
- Social Engineering techniques.
- Information stealing



Information analysis

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

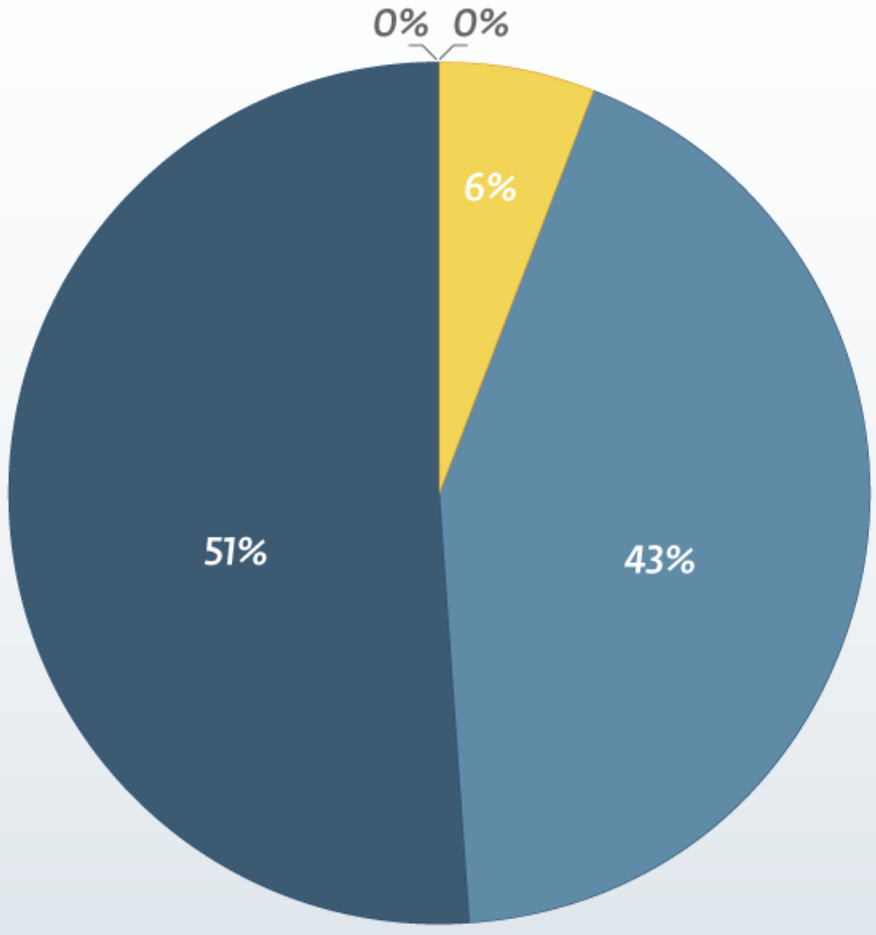
Bots reported by country



References

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

Affected OS

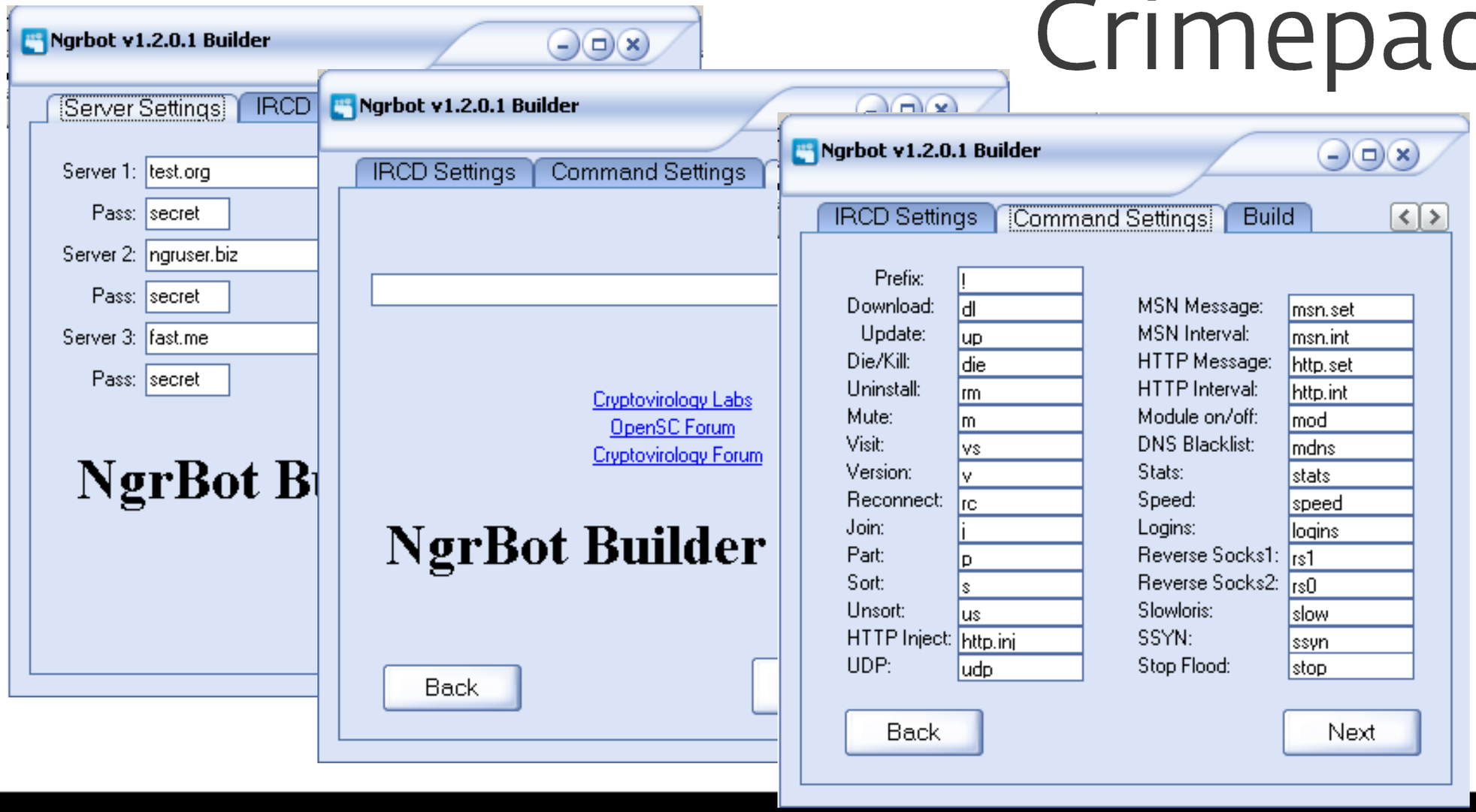


References

- 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

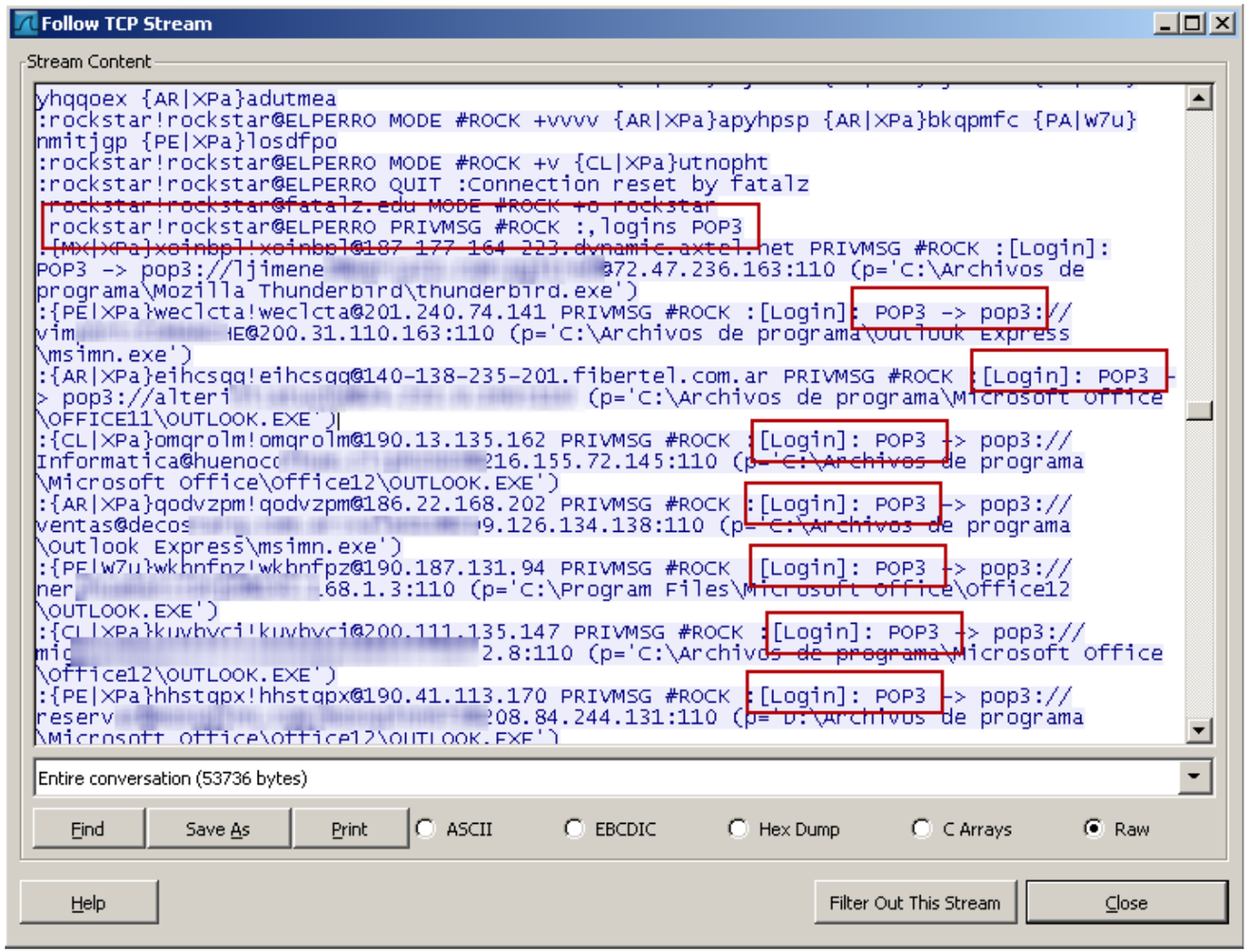
Crimepack


Ngrbot v1.2.0.1 Builder
Server Settings
IRCD
Server 1: test.org
Pass: secret
Server 2: ngruser.biz
Pass: secret
Server 3: fast.me
Pass: secret
NgrBot Bu
Ngrbot v1.2.0.1 Builder
IRCD Settings
Command Settings
Cryptovirology Labs
OpenSC Forum
Cryptovirology Forum
NgrBot Builder
Back
Ngrbot v1.2.0.1 Builder
IRCD Settings
Command Settings
Build
Prefix: !
Download: dl
Update: up
Die/Kill: die
Uninstall: rm
Mute: m
Visit: vs
Version: v
Reconnect: rc
Join: j
Part: p
Sort: s
Unsort: us
HTTP Inject: http.inj
UDP: udp
MSN Message: msn.set
MSN Interval: msn.int
HTTP Message: http.set
HTTP Interval: http.int
Module on/off: mod
DNS Blacklist: mdns
Stats: stats
Speed: speed
Logins: logins
Reverse Socks1: rs1
Reverse Socks2: rs0
Slowloris: slow
SSYN: ssyn
Stop Flood: stop
Back
Next

Social Engineering

Using social networks

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



Information stealing

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

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.


SECRET

What are we dealing with?

From Autorun to LNK

References

Dorkbot detections

INF/Autorun detections

Win32/Autorun detections

eset

Contact info:

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

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

Pablo Ramos
@ramospablo
pablo.ramos@eset.com