

Ethical Hacking

Malware, Botnets y Cibercrimen

Federico Pacheco



@FedeQuark



www.federicopacheco.com.ar



info@federicopacheco.com.ar

Virus (Biología)

- Agente submicroscópico acelular que se multiplica en células de otros organismos
- 1899: primer virus conocido (Beijerinck)
- Partes
 - Material genético (ADN o de ARN)
 - Cubierta proteica que protege a estos genes (cápside)
 - Bicapa lipídica (en algunos)
- Propagación
 - Organismos que los transmiten
 - Insectos
 - Aire
 - Agua



Malware

- Concepto: Software que ejecuta acciones maliciosas
- Clasificaciones principales
 - Por método de propagación
 - Virus, Troyanos, Gusanos, Adware y Spyware
 - Por funcionalidad
 - Keylogger, Password stealer, Rootkit, Ransomware, Bomba lógica, Botnet, etc.



Cronología

50s: primeras investigaciones de programas autorreplicables (John Von Neuman)

60s: desarrollo de juegos que "luchaban" por la memoria (Bell Labs)

70s: primeros programas autorreplicables para monitorear redes (Xerox PARC)

1971: primer código malicioso (Creeper) y primera removal tool (Reaper)

1983: primer virus moderno (Fred Cohen). Bautizados por Len Adleman.

1988: Gusano de Morris → Conciencia → Primeros antivirus

1991: primeros kits para construcción de virus

1992: virus Michelangelo es el primer virus popular

Salón de la fama

Michelangelo

Melissa

Slammer

Blaster

Klez

Bugbear

Chernobyl

I Love You

Sircam

Nimda

Código Rojo

Sobig

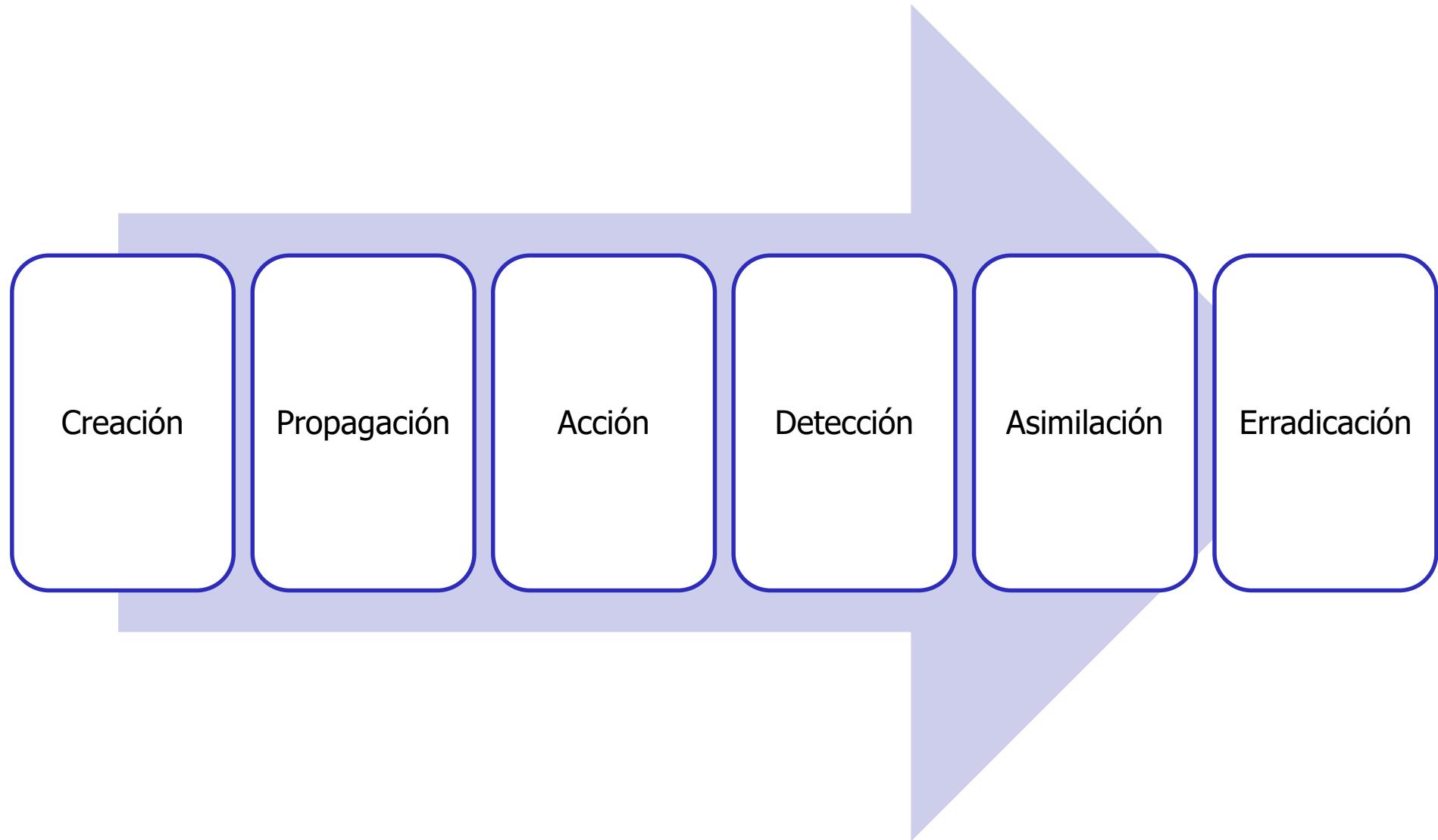
Sasser

Stuxnet

Flame

Duqu

Ciclo de vida del malware



Quine

- Programa que produce su código fuente como salida

- Ej. (Python)

```
s='s={0!r};print s.format(s)';print s.format(s)
```

- Ej. (C)

```
main(){char *c="main(){char *c=%c%c%;\nprintf(c,34,c,34);}\n";\nprintf(c,34,c,34);}
```

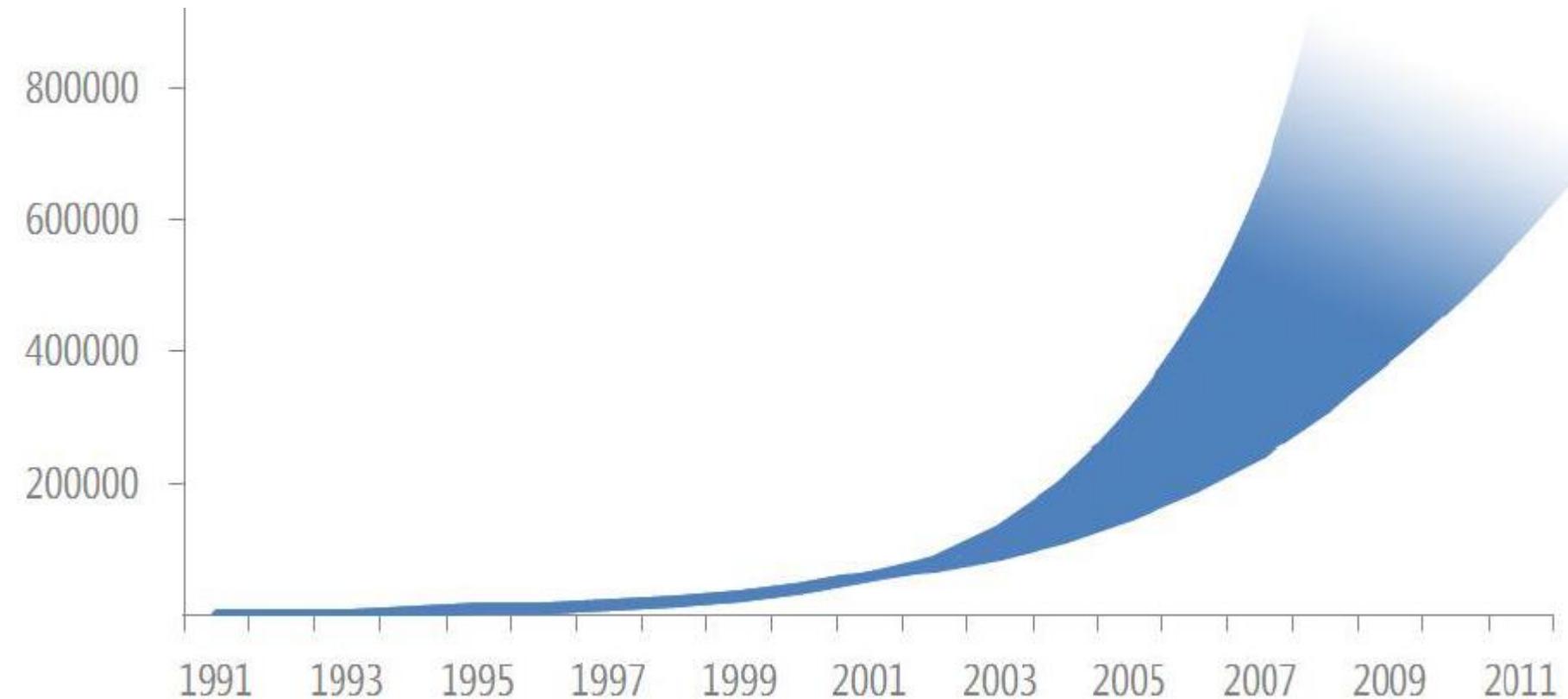
The screenshot shows a Java development environment with two windows. The top window is titled 'Quine.java' and contains the following Java code:

```
public class Quine
{
    public static void main( String[] args )
    {
        char q = 34;          // Quotation mark character
        String[] l = {         // Array of source code
            "public class Quine",
            "{",
            "    public static void main( String[] args )",
            "        "
        };
    }
}
```

The bottom window is titled 'Console' and shows the output of running the program:

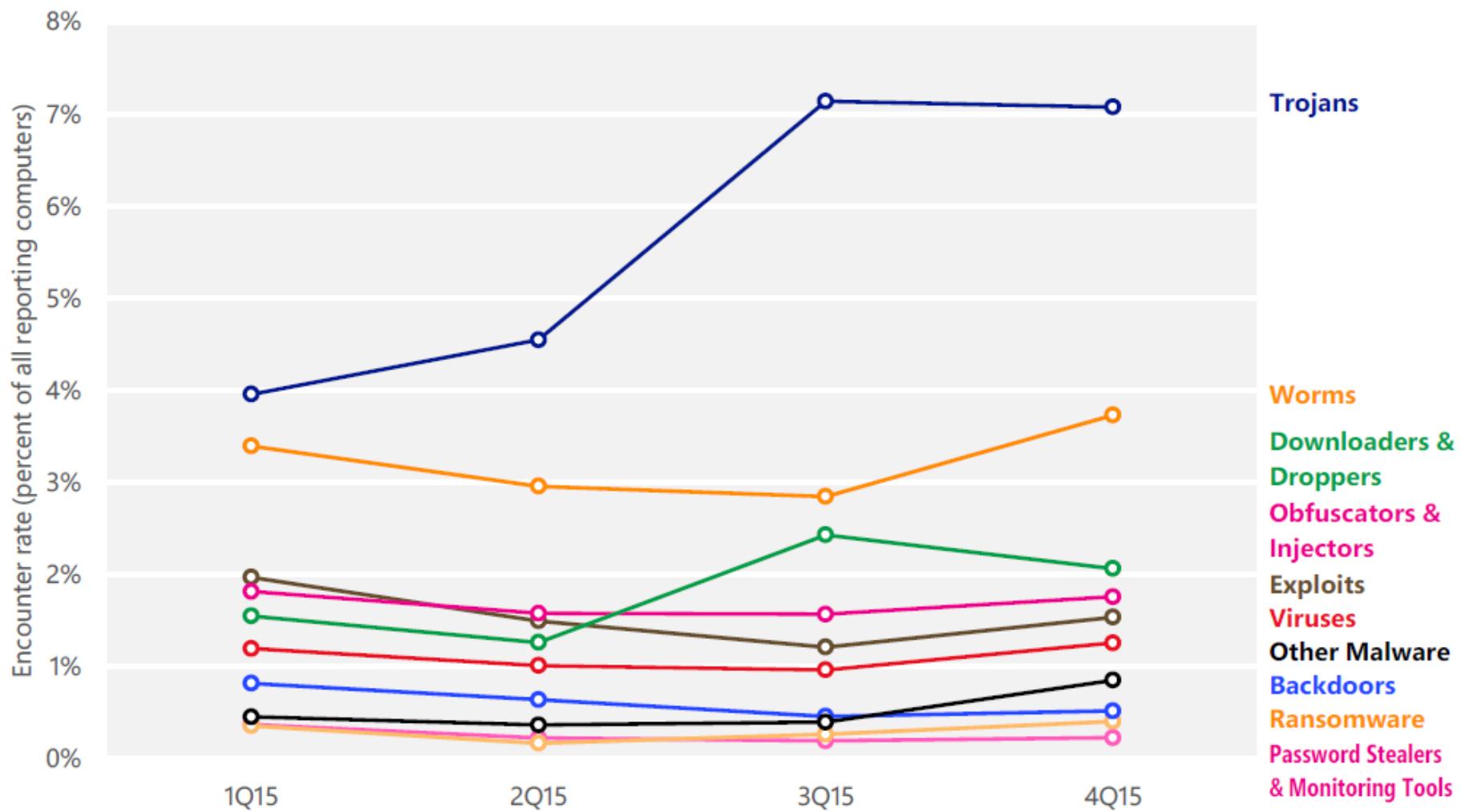
```
<terminated> Quine [Java Application] C:\Program Files\Java\jre6\bin\javaw.exe
public class Quine
{
    public static void main( String[] args )
    {
        char q = 34;          // Quotation mark character
        String[] l = {         // Array of source code
            "public class Quine",
            "{",
            "    public static void main( String[] args )",
            "        "
        };
    }
}
```

Cantidad de malware desde 1991



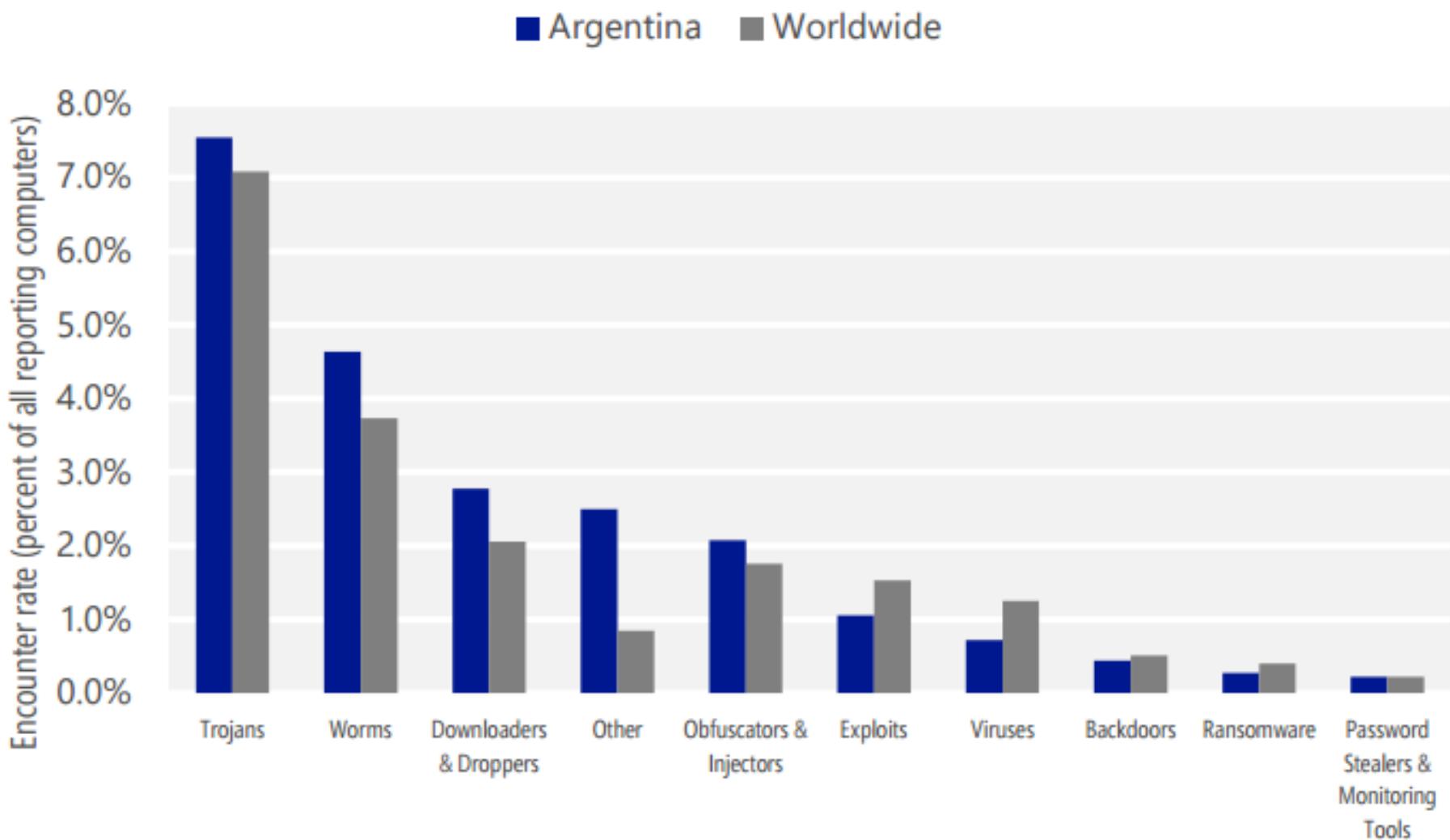
Fuente: Microsoft Security Intelligence Report

Malware por tipo



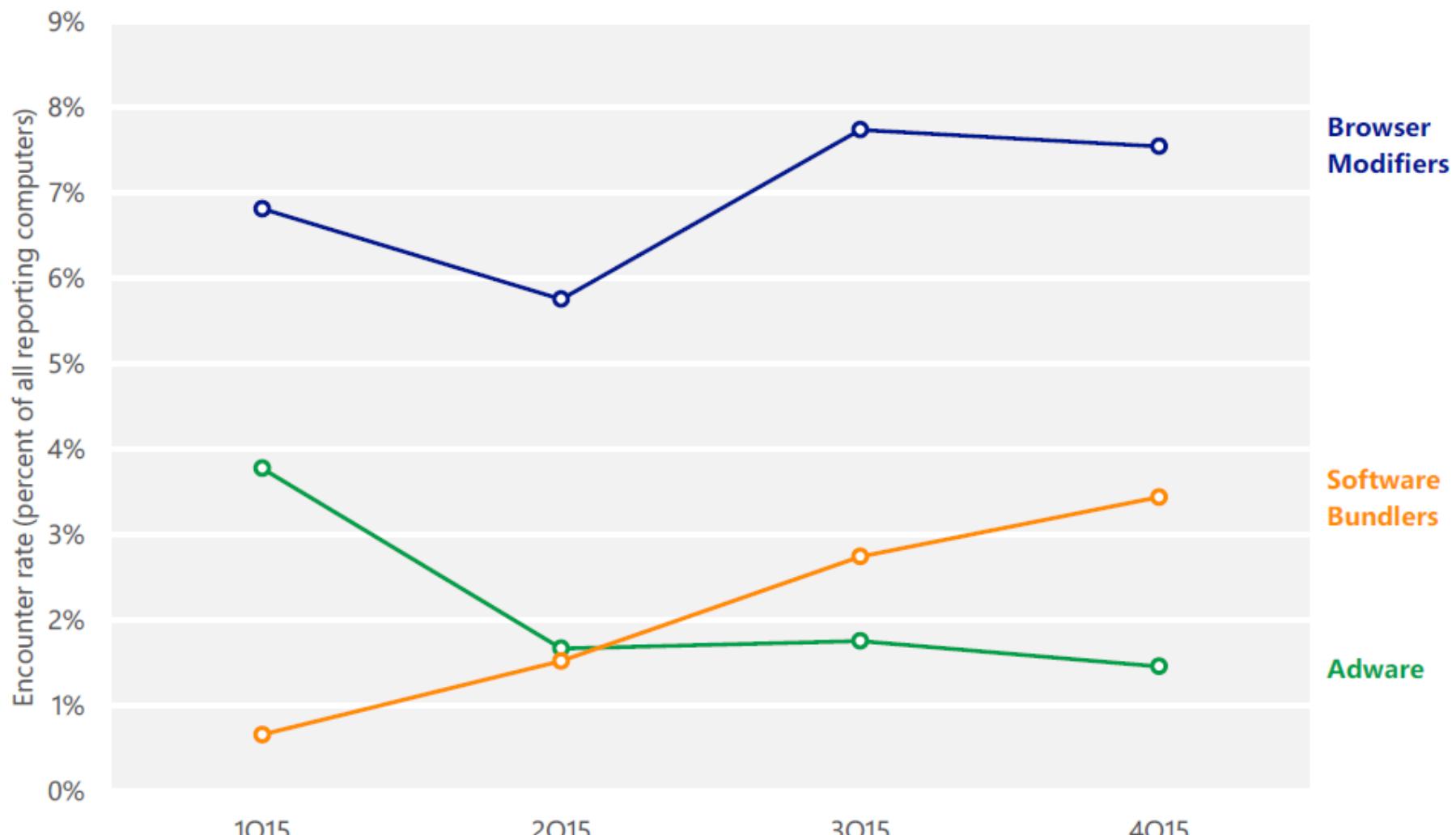
Fuente: Microsoft Security Intelligence Report

Malware en Argentina por tipo (2015)



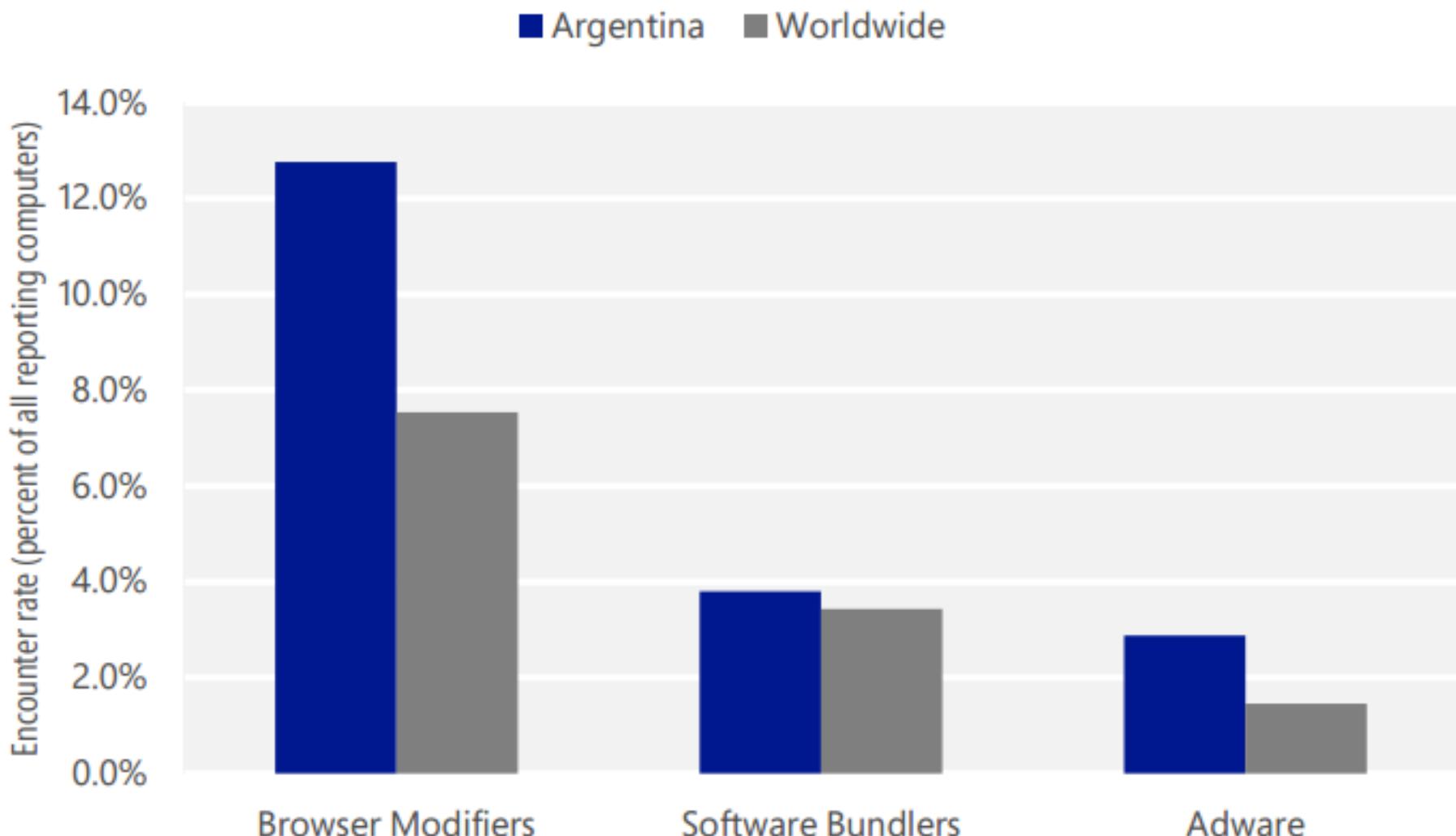
Fuente: Microsoft Security Intelligence Report

Software no deseado



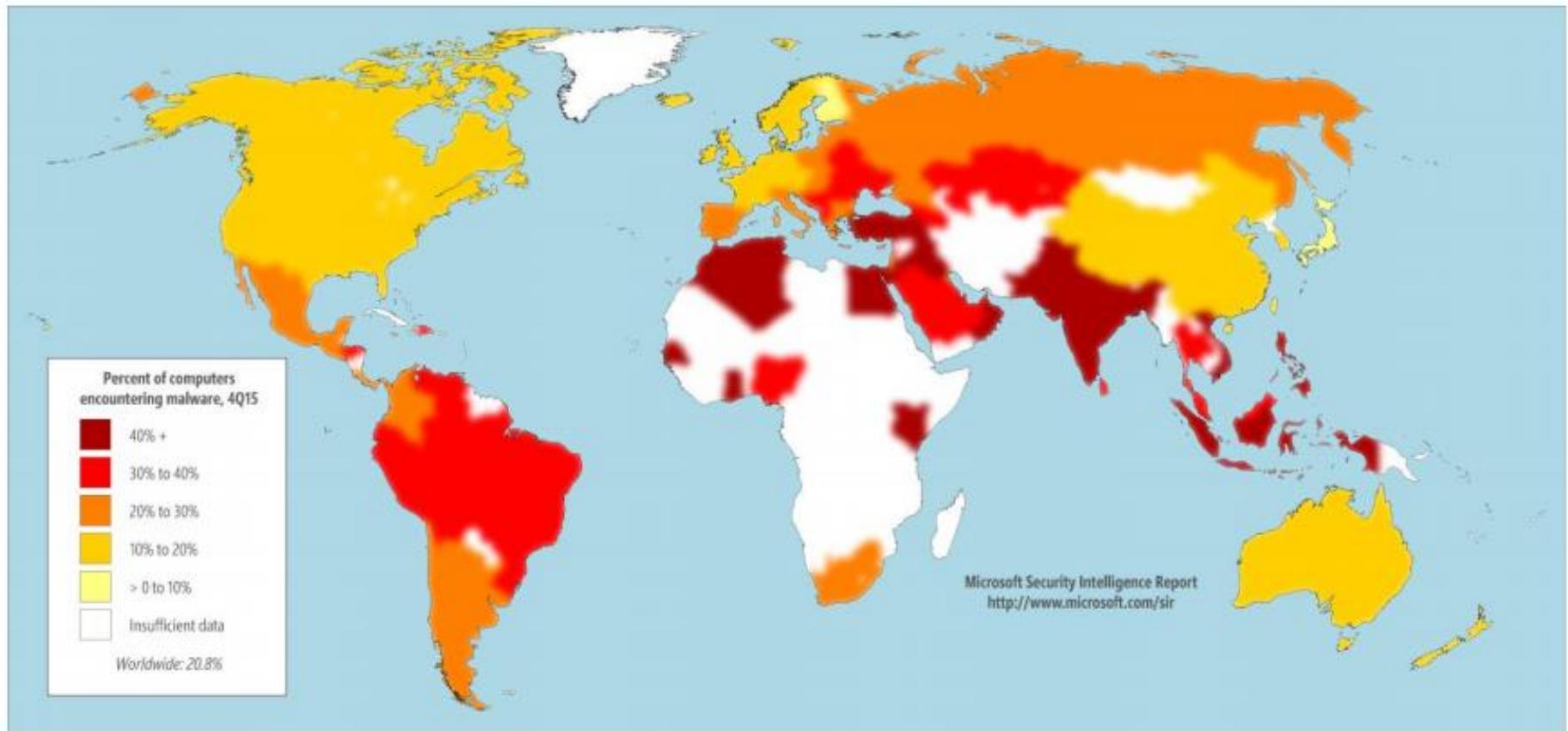
Fuente: Microsoft Security Intelligence Report

Software no deseado en Argentina (2015)



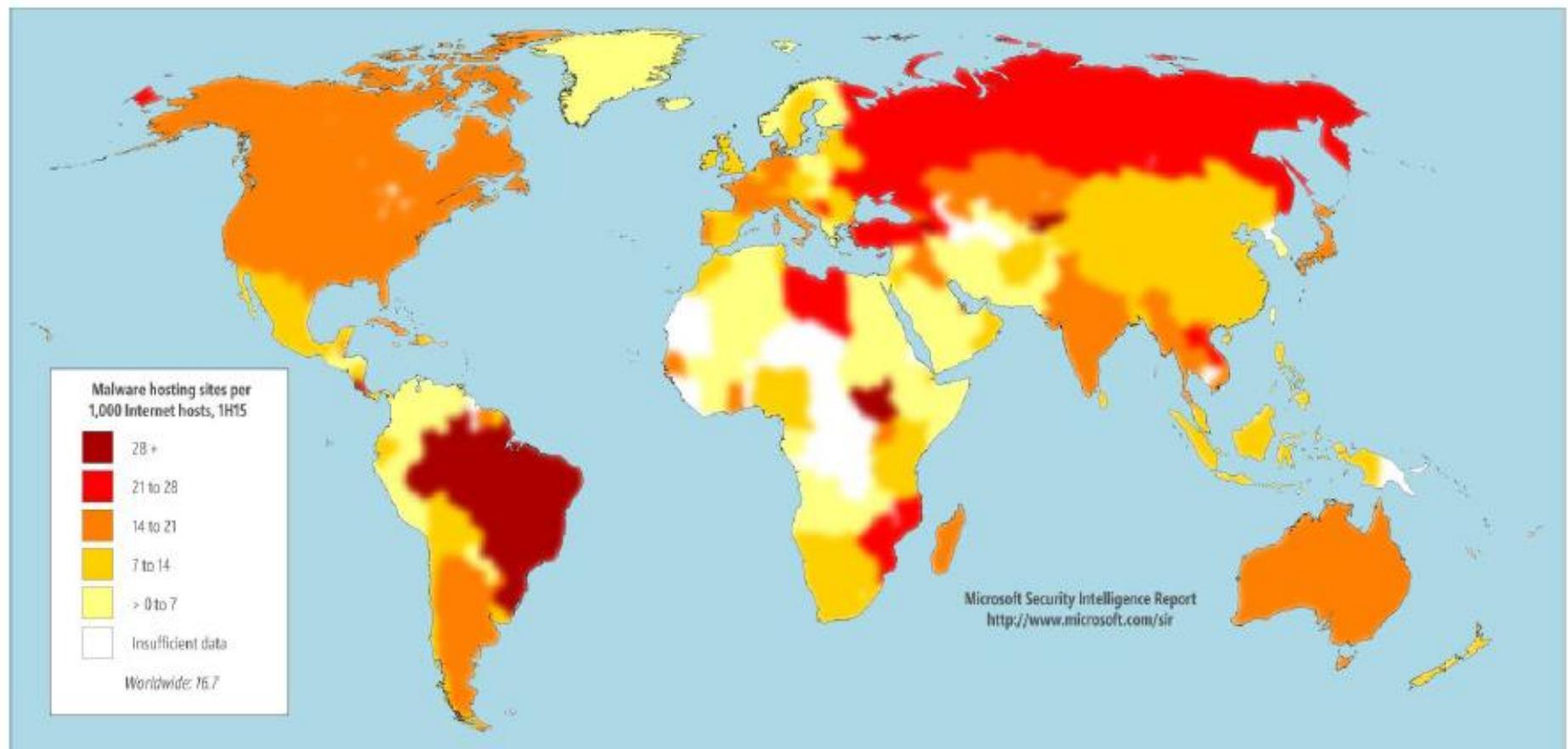
Fuente: Microsoft Security Intelligence Report

Malware detectado (2015)



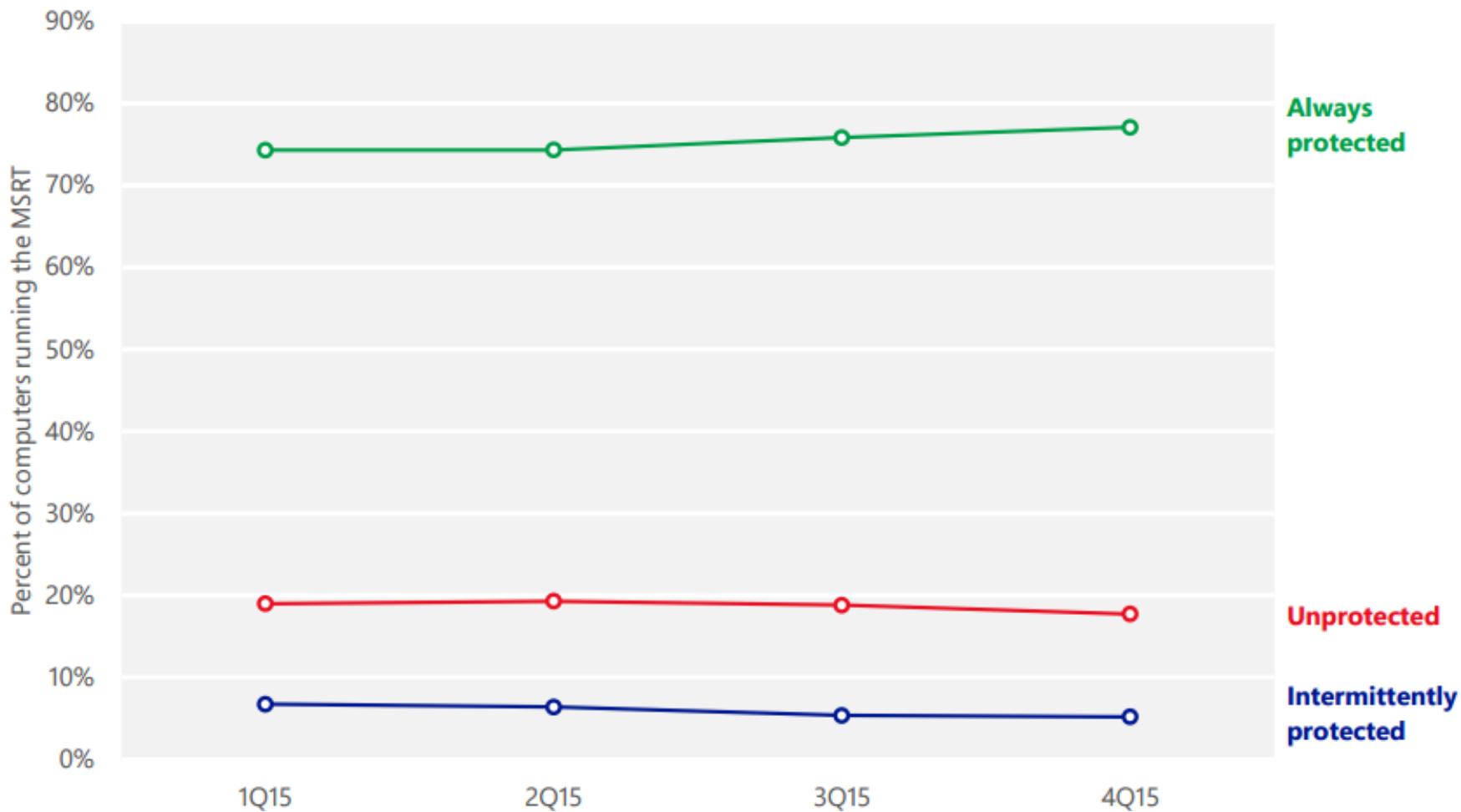
Fuente: Microsoft Security Intelligence Report

Sitios de distribución de malware



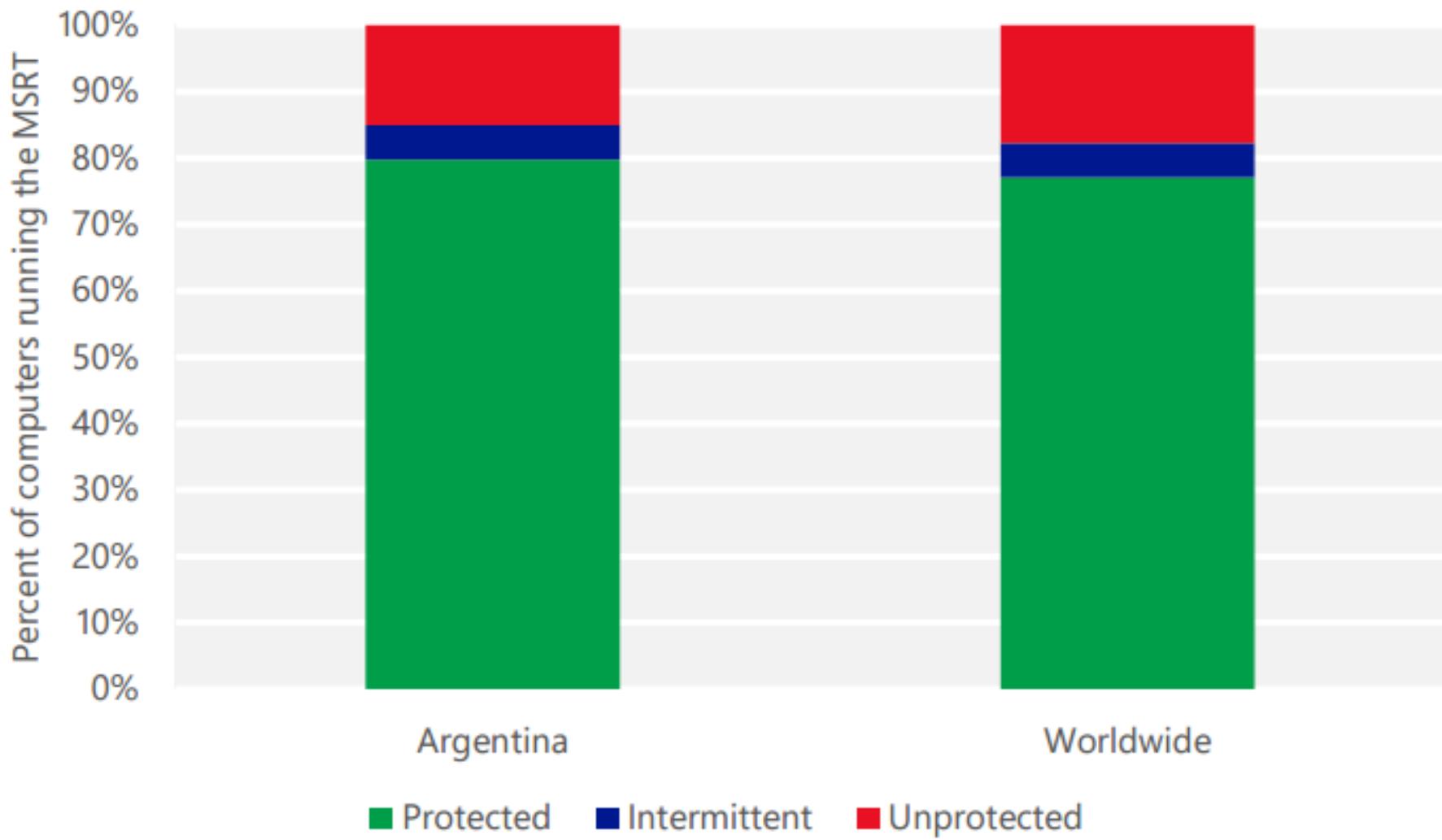
Fuente: Microsoft Security Intelligence Report

Equipos protegidos (2015)



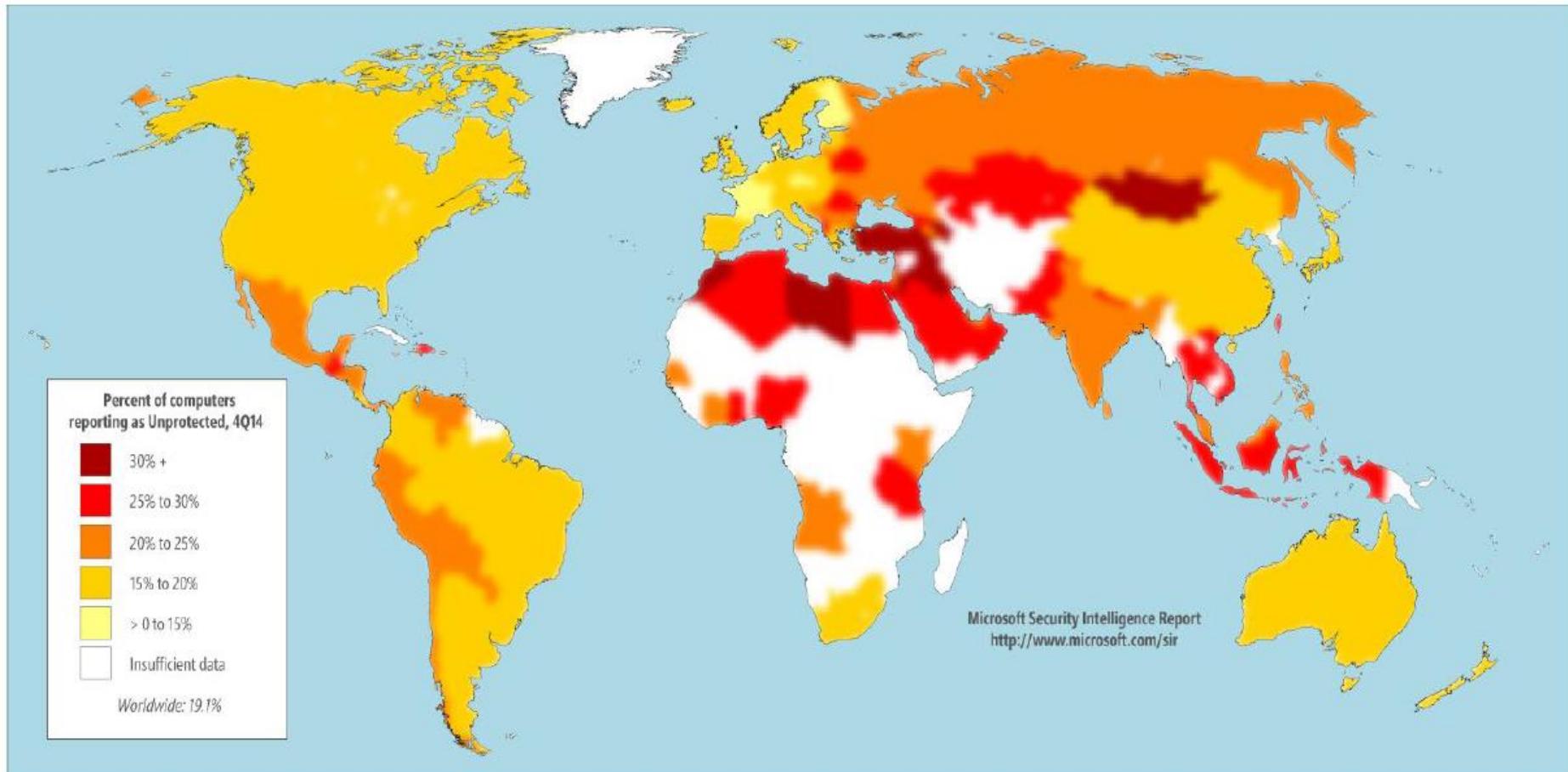
Fuente: Microsoft Security Intelligence Report

Equipos protegidos en Argentina (2015)



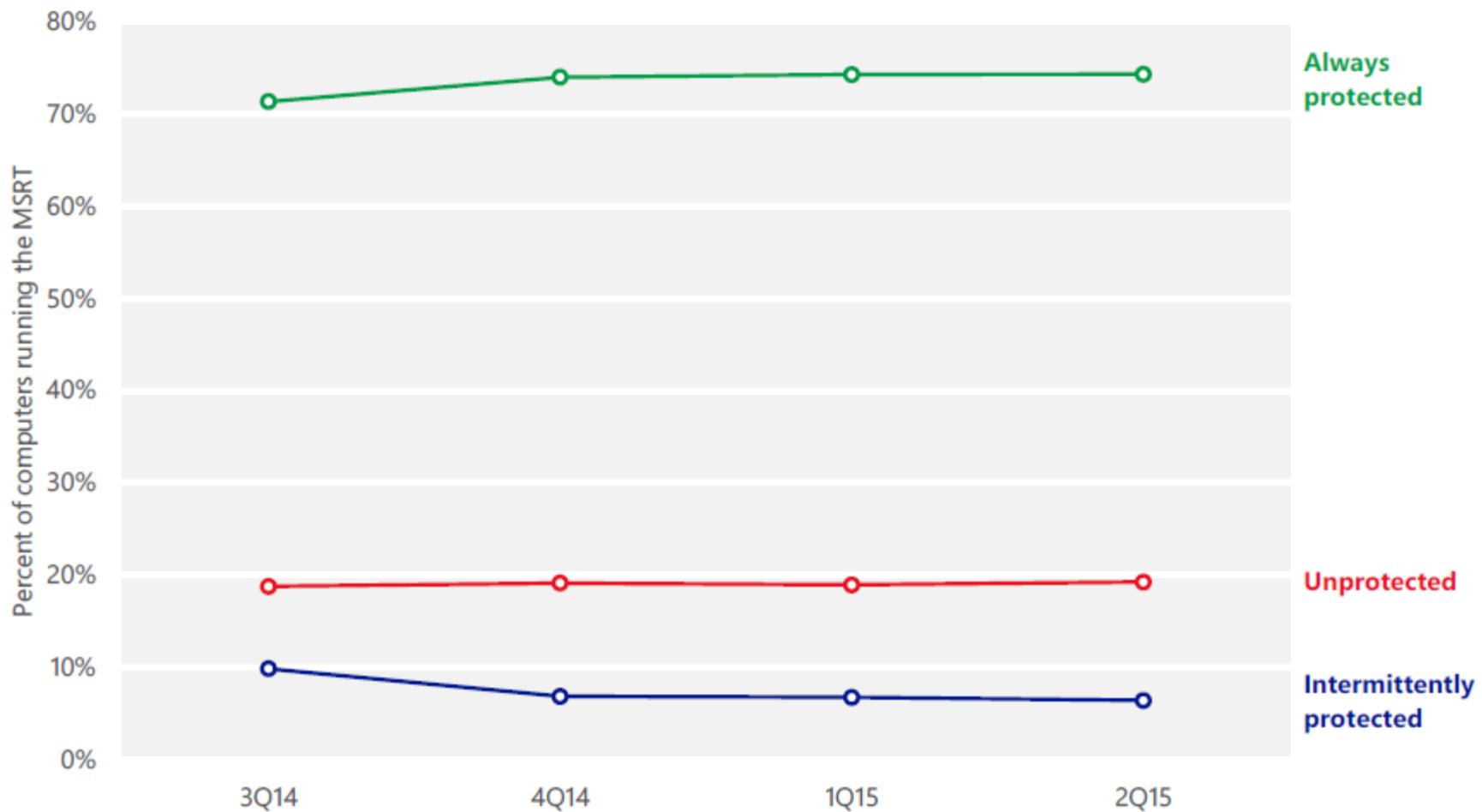
Fuente: Microsoft Security Intelligence Report

Equipos protegidos en el mundo



Fuente: Microsoft Security Intelligence Report

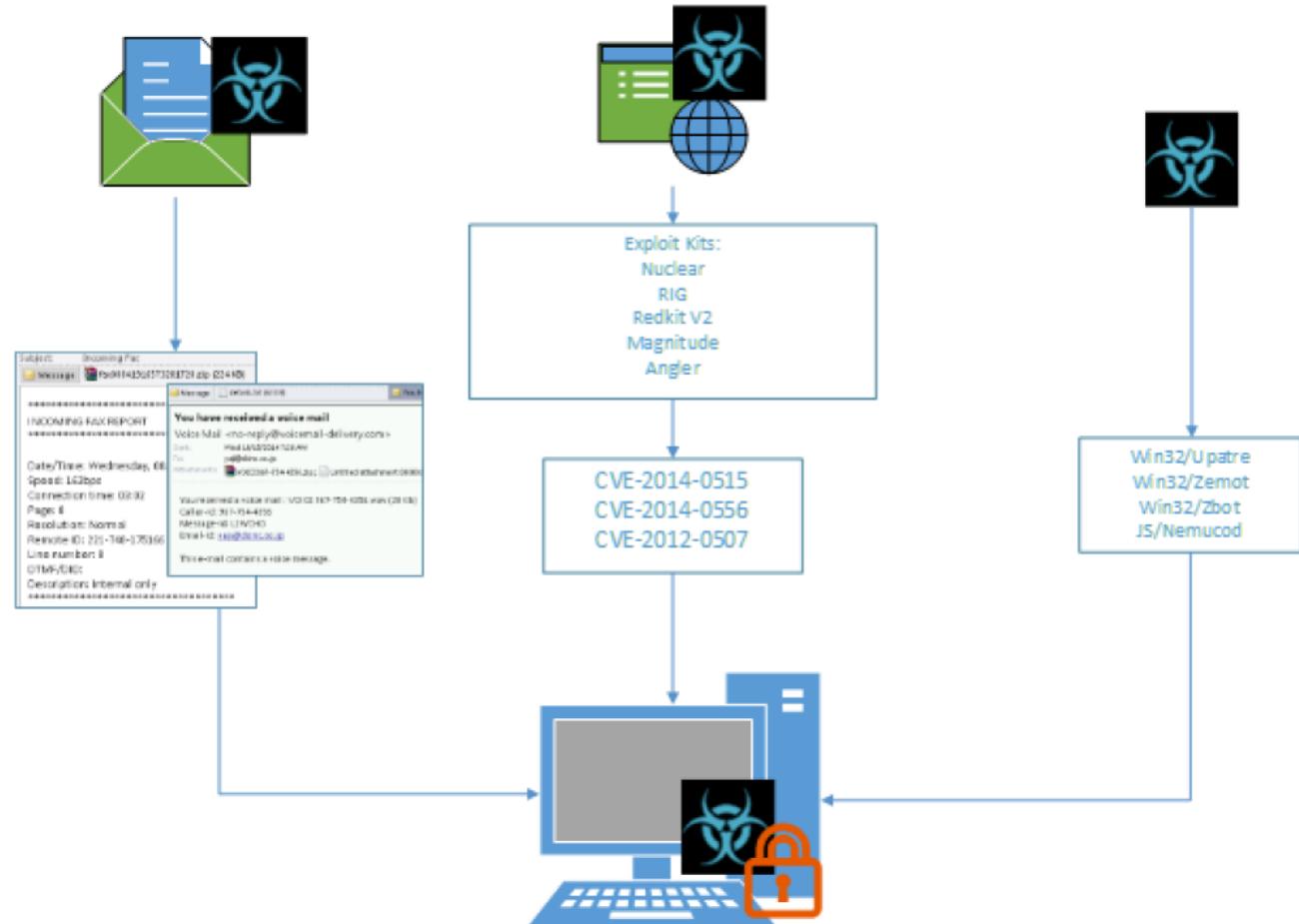
Equipos infectados según protección



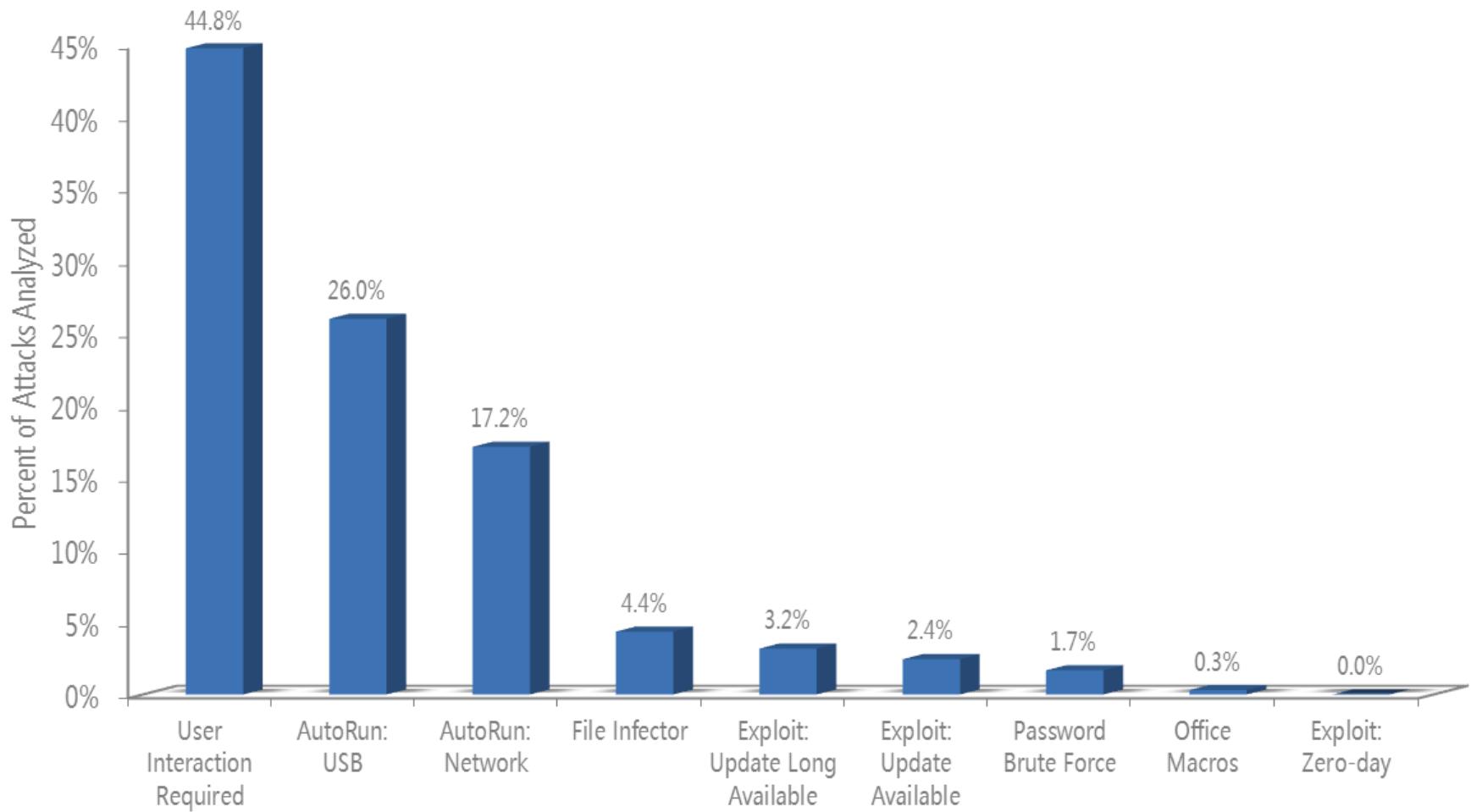
Fuente: Microsoft Security Intelligence Report

Medios de propagación

- Internet
 - Drive-by-download
 - Scam (troyanos)
 - Spam/email
 - Adware
 - Gusanos
- Medios extraíbles
 - Pendrives
 - Discos extraibles
 - Celulares
 - MP3 Players



Malware - Métodos de propagación



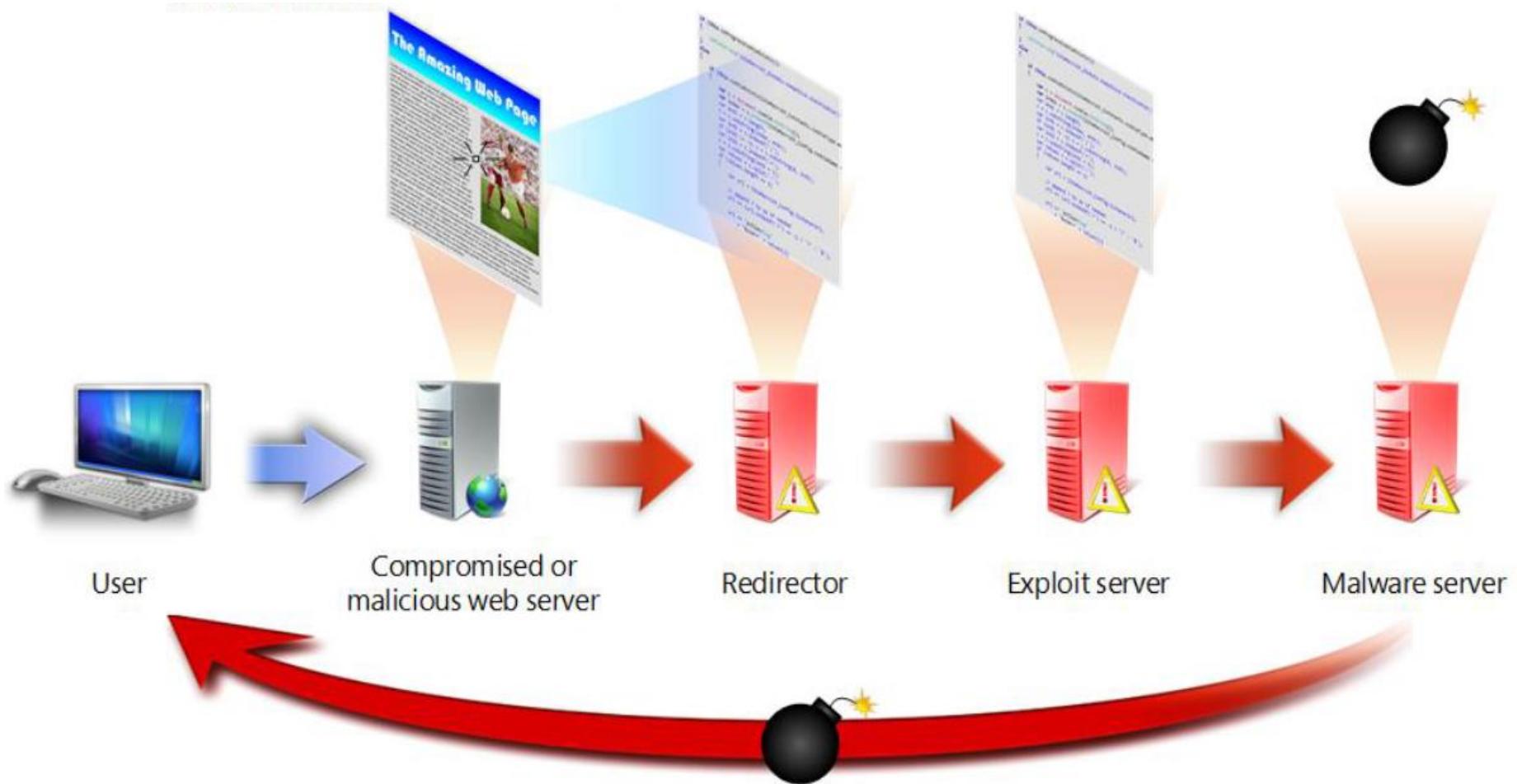
Fuente: Microsoft Security Intelligence Report

Drive-by-download

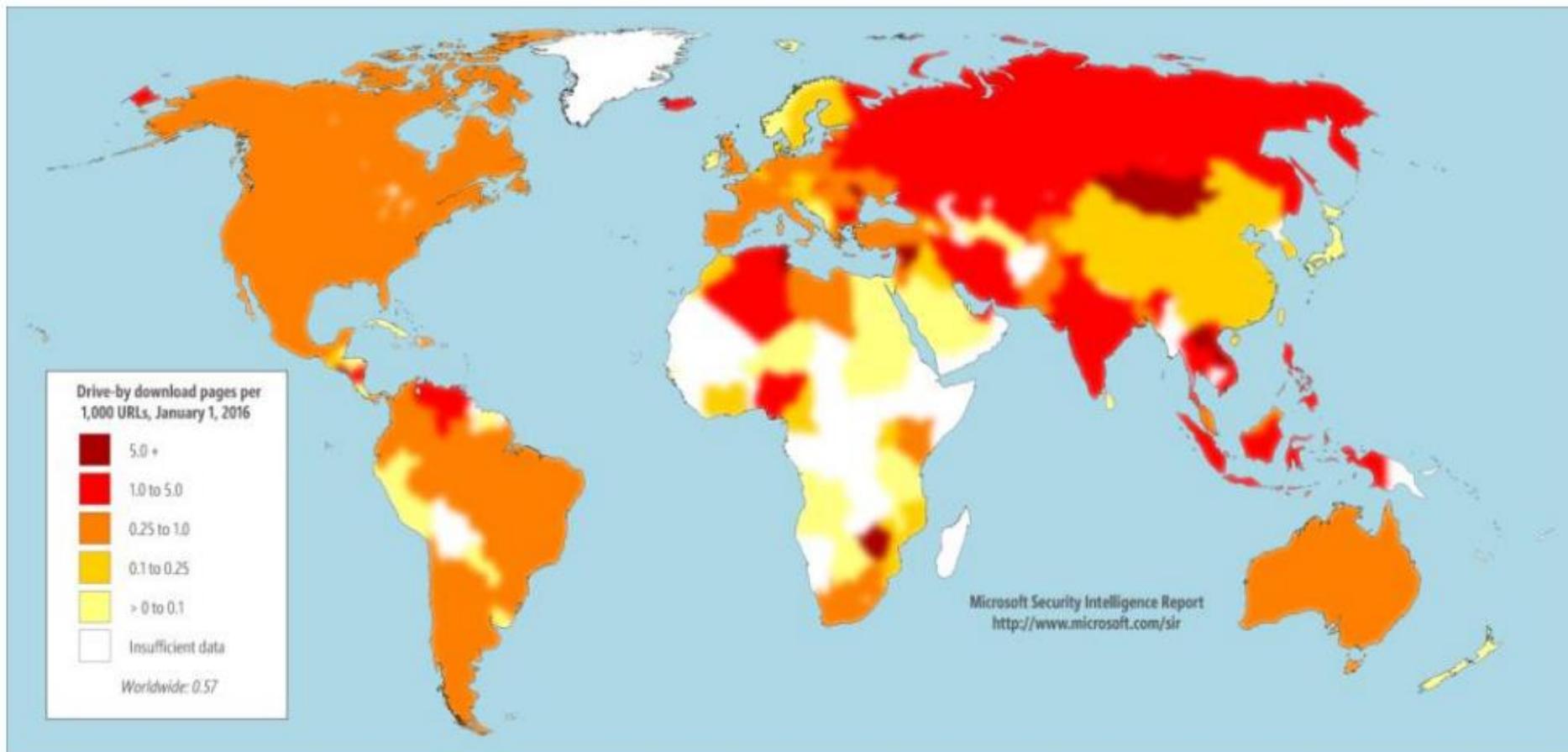
- Concepto: Infección de un equipo mediante la navegación en un sitio propio
 - Puede permitir la inserción de cookies
 - Permite determinar una contraseña válida si se registra
- Se utilizan técnicas de explotación de vulnerabilidades
 - Se comercializan kits y packs de explotación



Drive-by-download – Proceso detallado

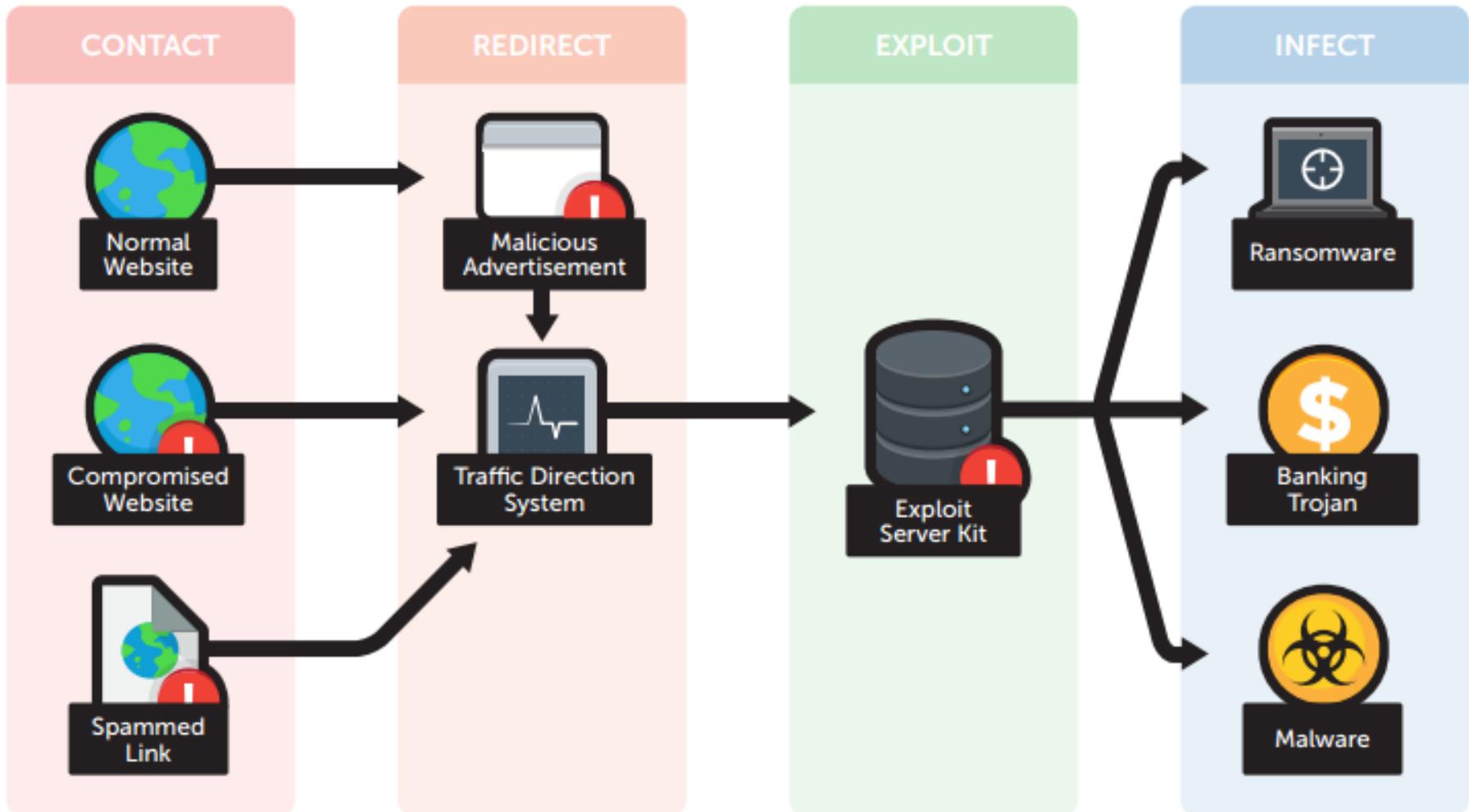


Sitios de Drive-by-Download (2015)



Fuente: Microsoft Security Intelligence Report

Infección por Exploit Kits



Técnicas de detección

- Firmas
 - Específicas o genéricas
 - Detección confiable
- Heurística
 - Análisis de comportamiento
 - Detección por probabilidades

00 55 50 58 30 00 00 00 00 00	UPX0
00 00 00 00 00 00 02 00 00 00	UPX1
00 00 00 00 00 80 00 00 E0	UPX2
00 00 70 00 00 00 70 01 00	3.91.UPX!
00 00 00 00 00 00 00 00 00 00	
E0 55 50 58 32 00 00 00 00 00	
00 00 04 00 00 00 70 00 00 00	
00 00 00 00 00 40 00 00 C0	
58 21 0D 09 02 08 B7 A3 E9	
01 00 C8 6B 00 00 00 8A 01	
AF FD 68 1C 05 00 00 68 02	
C0 FE 83 C4 0C 11 60 83 B9	
20 10 2A BB DD 67 BF 18 0A	



Análisis de malware

- Servicios de análisis online
- Sandbox local
- Análisis manual
- Software automatizado



Sysinspector

ESET SysInspector
BETA - Internal ESET Antivirus Lab tool now available for free!

Detail: Full Items Filtering: Fine (Risk Level 1-9) Find: Search

Status Section: Services

Running processes

Network Connections

Important Registry Entries

Standard Autostart

Winlogon Notify

Browser Helper Objects

Internet Explorer

Shell Open Commands

Network

Desktop

Shell Execute Hooks

Print Monitors

TypeLibs

Protocols

Services

Drivers

Critical files

System Information

File Details

About

Description

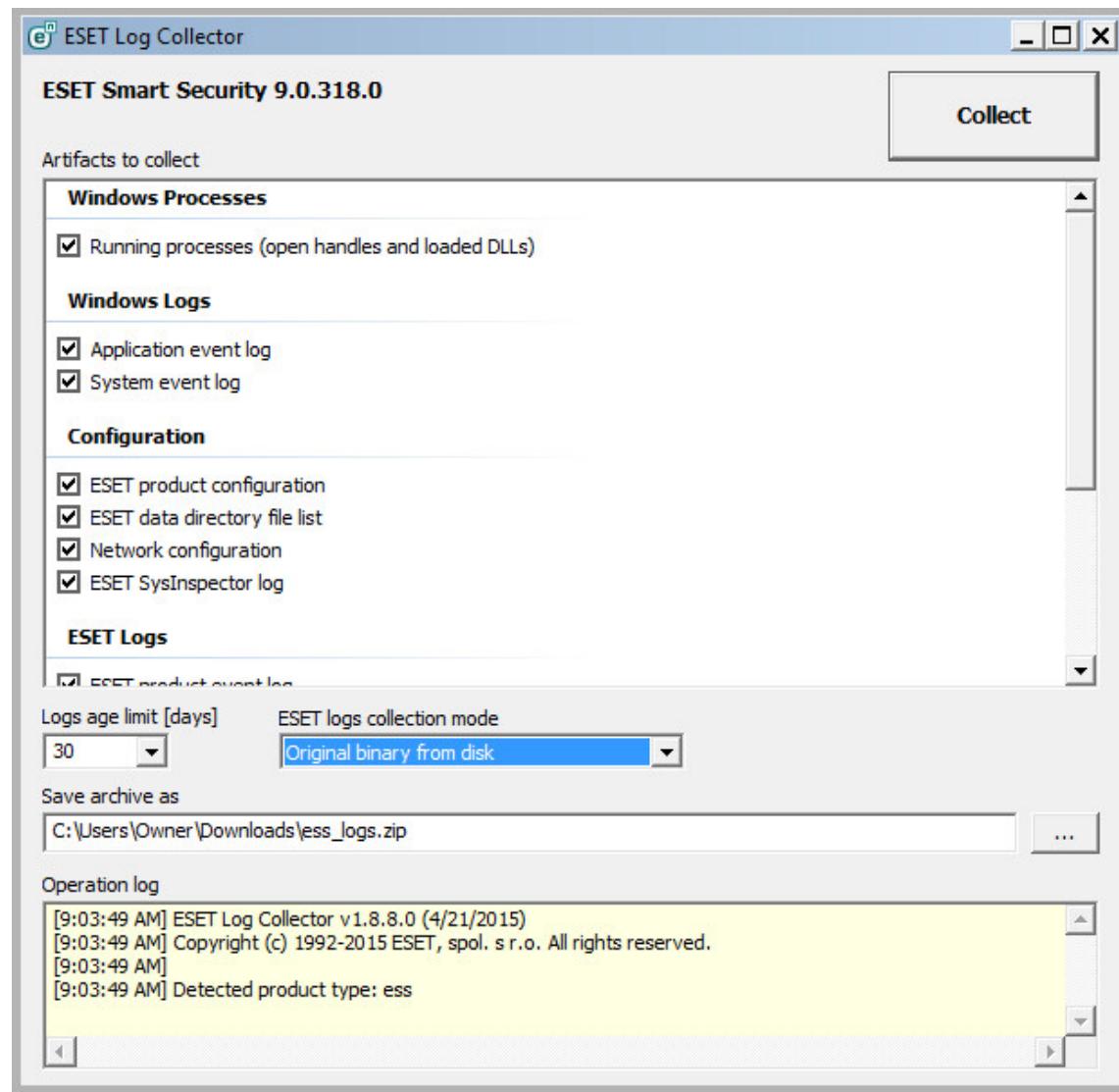
Path

rpcss.dll

c:\windows\system32\rpcss.dll

Internal Name	Product Name	FileVersion	Company Name	FileDescription	FileSize	SHA1	Creation Time	Last Write Time	Linked to
rpcss.dll	Microsoft® Windows® Operating System	6.0.6000.16386 (vista_rtm.061101-2205)	Microsoft Corporation	Distributed COM Services	545792	F195B9423DEC73E747FF84BE27A885108F5C1DB	2006/11/02 10:50	2006/11/02 11:46	Running processes -> svchost.exe -> c:\windows\system32\rpcss.dll

Log collector



Análisis de muestras – Virustotal



ViruTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

File

URL

Search

No file selected

Choose File

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow ViruTotal to share this file with the security community. See our [Privacy Policy](#) for details.

Scan it!

Análisis de muestras – Nodistribute

The screenshot shows a web browser window for the NoDistribute website (<https://nodistribute.com>). The interface includes a navigation bar with links for 'Login', 'Pricing', and 'About'. A message indicates '10 scans remaining'. Below the navigation is a banner featuring a blue gear icon and the text '100% FUD'.

Below the banner are four input fields: 'File' (with a file icon), 'URL' (with a link icon), 'Scan Watch' (with an eye icon), and 'Run-Time Scan' (with a double-headed arrow icon).

A large button labeled 'Seleccionar archivo' (Select file) is present, with the subtext 'Ningún archivo seleccionado' (No file selected). Below this is a blue button labeled 'Scan File'.

The main content area features a large cloud icon with an upward arrow and the text 'Scan A File'. Below this text is a explanatory message: 'Select your file in order to scan your file with over 35 anti-viruses. The results of the scans are never distributed.'

Análisis automatizado – Payload Security



PAYLOAD SECURITY

This webpage is a free malware analysis service powered by [Payload Security](#) that detects and analyzes unknown threats using a unique Hybrid Analysis technology.

 File

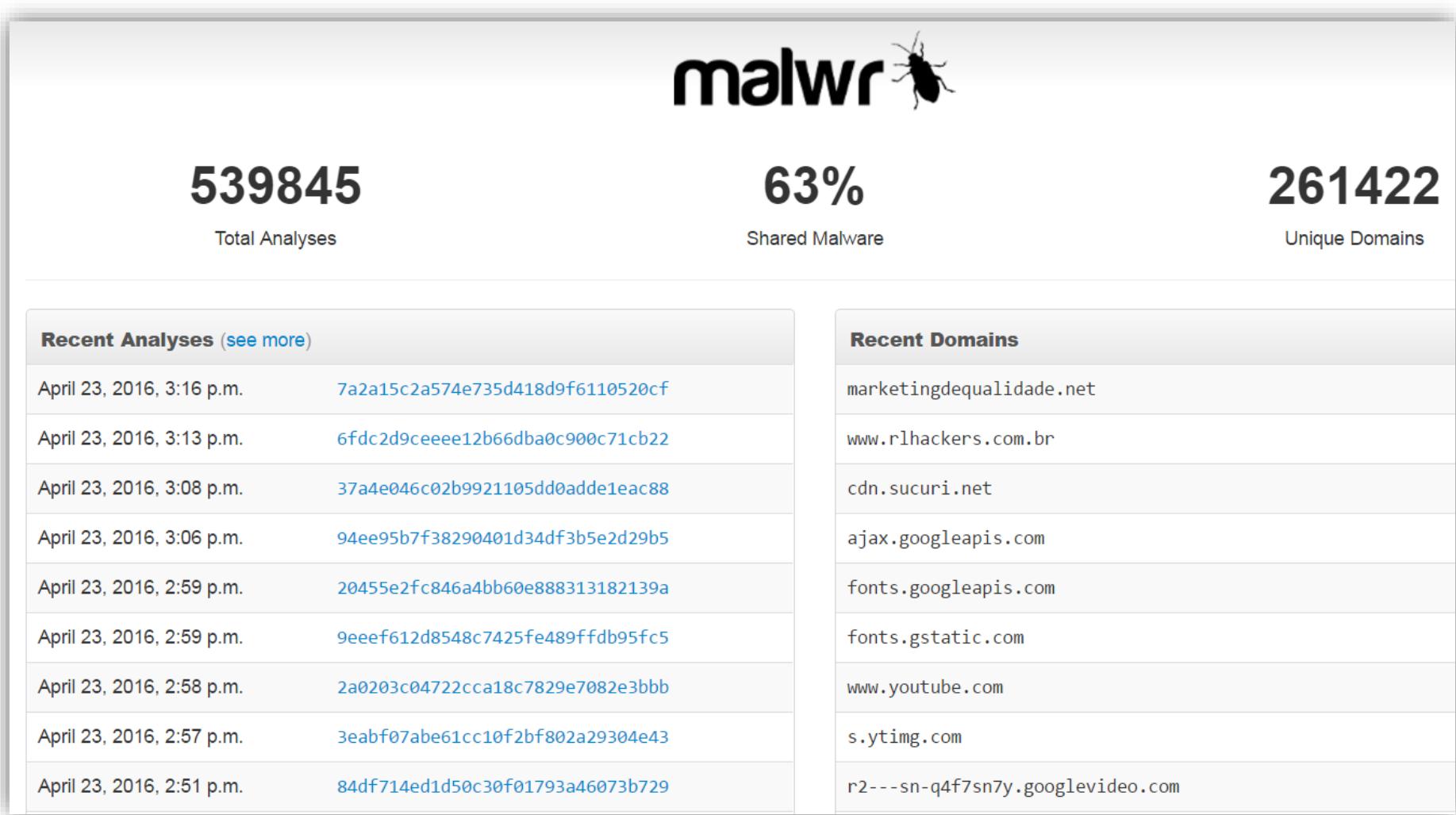
 Online File

Select file

This free malware analysis service is running **VxStream Sandbox v4.00** in the backend. Supporting PE, Office, PDF, APK files and more (e.g. EML). Maximum upload size is 100 MB.

 Learn more about the [standalone version](#) or purchase a [private webservice](#).

Análisis automatizado – malwr



Análisis automatizado – Varios



Comodo Instant Malware Analysis

Automated Analysis System

If you have a suspicious file, please submit it online by using the form below. Our system will scan it and report back its findings.

File to scan: Ningún archivo seleccionado

I agree with the [Terms and Conditions](#)

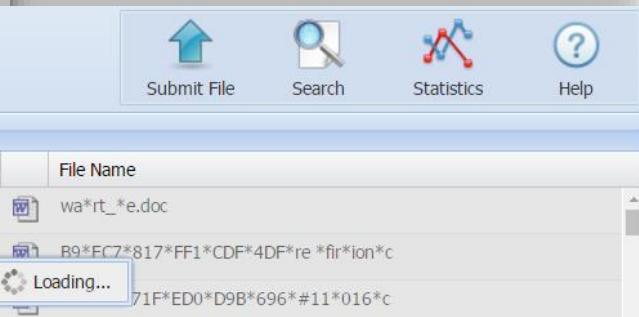
Upload File

Date	Result	File Name
2016/03/04	APT-Malicious!	wa*rt_*e.doc
2016/03/03	CVE-2014-1761	B9*EC7*817*FF1*CDF*4DF*re *fir*ion*c
2016/03/03	APT-Malicious!	71F*ED0*D9B*696*#11*016*c Loading...
2016/03/03	CVE-2014-1761	57*89E*DF9*1F8*E27*3E0*yme*Inv*e.doc

XecScan Rapid APT Identification Service

History

Submit File Search Statistics Help



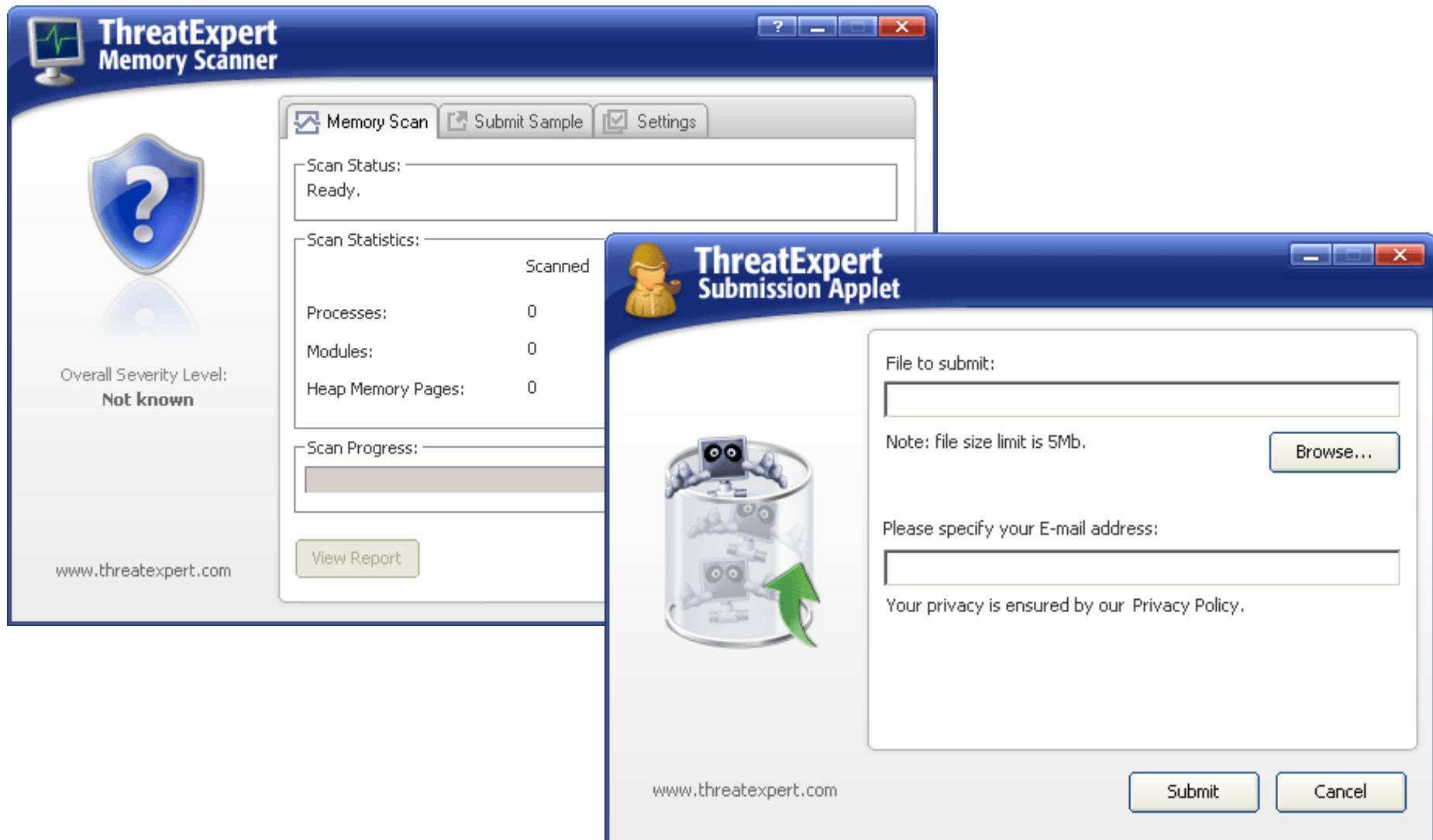
MASTIFF Online Free Documentation FAQ Terms of Service Contact 1986 , 1 - 25

MASTIFF Online is a free web service offered by KoreLogic Inc. as an extension of the [MASTIFF static analysis framework](#). The MASTIFF framework executes programs that analyze unknown or malicious files enabling individuals to quickly dissect and examine the true nature of files.

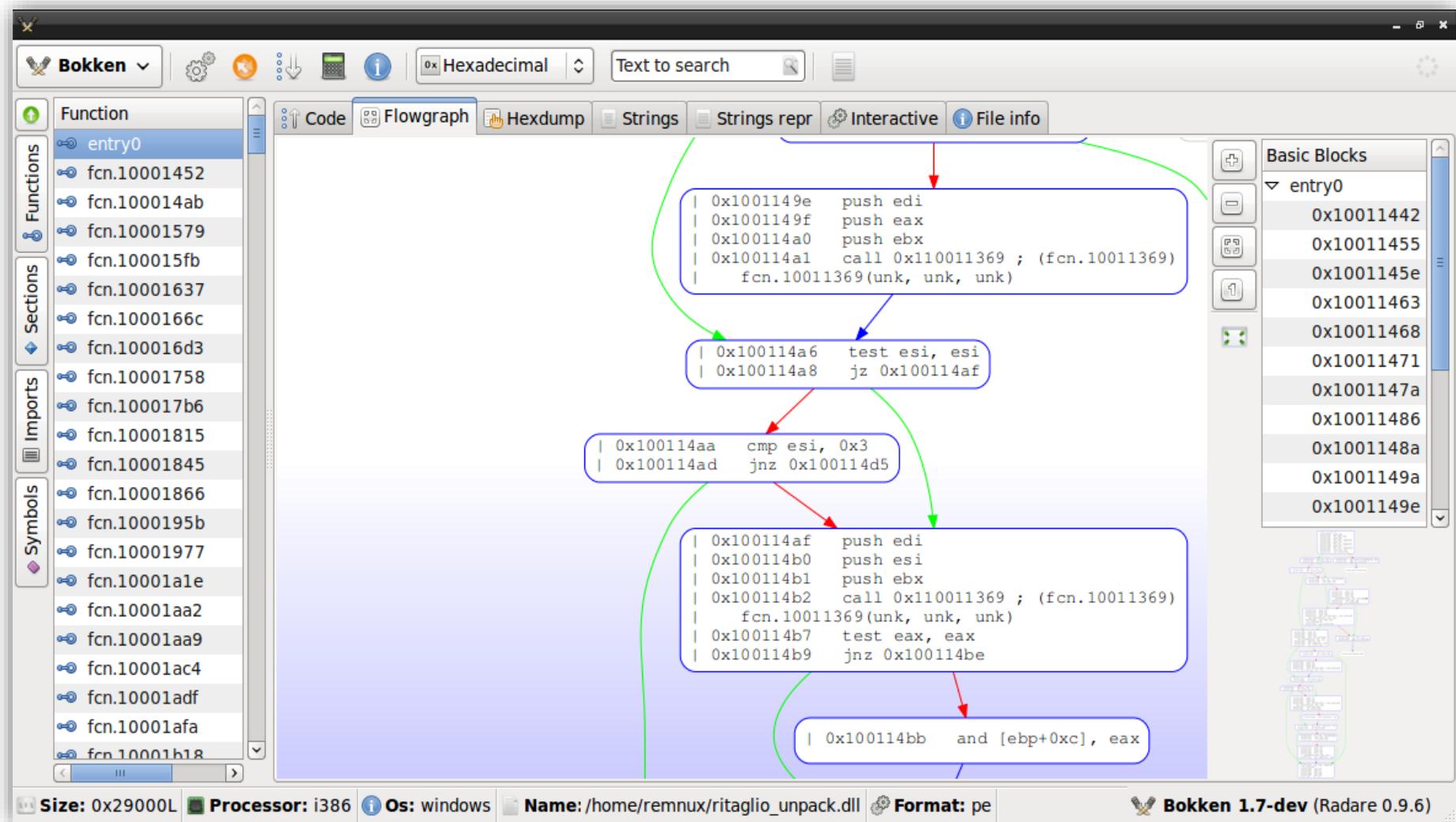
Upload Sample Search : Reload

Status	Sample	Bytes	MD5 Hash	Uploaded
✓	New_order_list.exe	766K	d3e2fdbf41a80d97257b0a5851da253a	2016-04-25 17:03:34
✓	BL.doc	123K	046ad4860496dd4eacccf24919de887ceb	2016-04-25 16:57:45
✓	UTHSCSA-20160425.doc	126K	995328103f5486a54cc99aab44b3fb21	2016-04-25 13:39:14
✓	STANDING-LETTER-OF-INSTRUCTION[1].PDF	538K	1ee02c02d06bfbd1dad8bbe7f85471eb9	2016-04-25 12:38:24
✓	VCTO25042016_XXXYXqjLnAfQAVavL9chXvwcRAm2ku7.exe	448K	3f6739a7dc801b6f9f243b8c8f9b3969	2016-04-25 11:44:24
✓	evtdiag.exe	64K	24d76abbcc0a10e4977ea28b33c879248	2016-04-25 09:51:39
✓	nroff_b.exe	24K	1d0e79feb6d7ed23eb1bf7f257ce4fee	2016-04-25 08:48:11
✓	Factuur_00891884-937473.pdf.exe	756K	9e30f43f2257e4c34ec4f2f141d2288d	2016-04-25 07:46:41
✓	Shot It v1.6.exe	1.4M	29bdbcf271f4e3be37cf853d49b78e5c	2016-04-25 06:21:26
✓	PianoInteractivo.exe	86K	7e058f9c5093695ccf8e2067499ff46e	2016-04-25 06:08:56
✓	explor.vbs	172K	fb6ec58c6c23d9063f79df16ed2b60c4	2016-04-25 02:22:51
✓	IMG054503502016-JPG.scr	104K	aa33ffc2f02379ce602e5a0aa7815466	2016-04-25 00:35:08

Herramientas varias



Bokken GUI



GUI para Pyew (malware analysis tool) y Radare (Reverse Engineering Framework)

Linux Distro: REMnux



Troyanización de sistemas

- Implica el control total o parcial del sistema remoto
- No se requiere crear troyanos desde cero
- Existen troyanos gratuitos y comerciales
- Se deben configurar diversos parámetros en función del objetivo



Troyano XtremeRAT

Xtreme RAT 3.6 Private [Servidores online (1)]

Arquivo Opções Idiomas Sobre

Nome do servidor	País	CAM	Versão	Ping (ms)	Janela ativa
Servers (1)					
Server_KENDER...	Spain	3.6 Pri...		0	Recortes

Gerenciador de arquivos (Server_KENDER-PC^kender(EAC2FE39))

Arquivos Procurar arquivos Transferências

Nome	Tamanho	Atributo	Tipo	Data de modificação
AutoPlay Me...		D	Diretório	21/02/2013 17:55:02
Mi música		DHS	Diretório	21/02/2013 16:05:24
Mis imágenes		DHS	Diretório	21/02/2013 16:05:24
Mis vídeos		DHS	Diretório	21/02/2013 16:05:24
desktop.ini	402 bytes	AHS	Opciones...	21/02/2013 16:05:40
safecoders....	22,1 KB	A	Imagen ...	24/02/2013 15:18:28

Dados do servidor

Server_KENDER-P...
Spain
127.0.0.1 / 127.0....
KENDER-PC / kend...

Troyano DarkComet

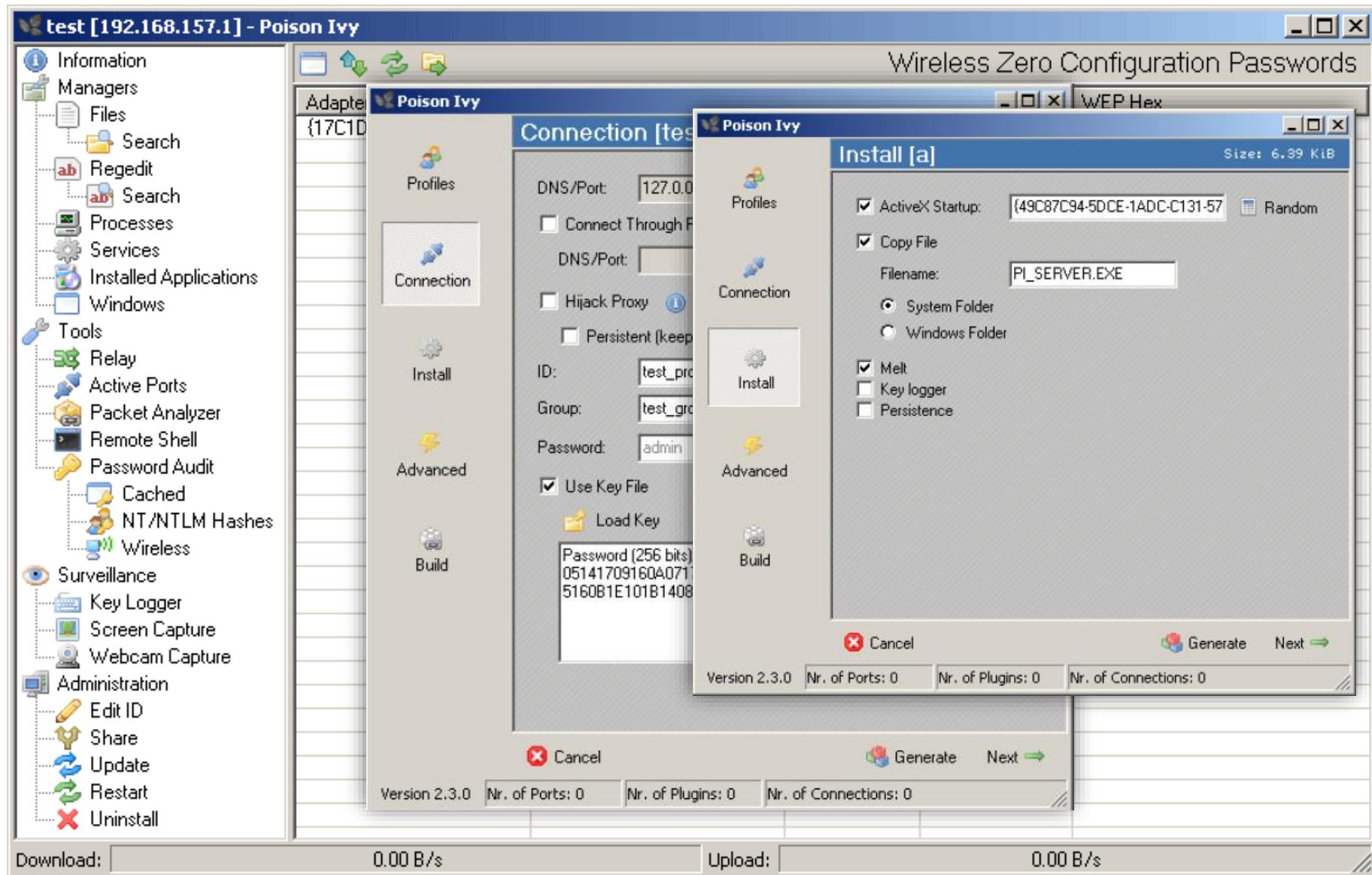
DarkComet-RAT v4.0 - [Online Users : 14]

	ID	IP Wan/[La...]	Computer ...	OS	RAM	Language/Country	A.	C.	P
	Unclassed users								
	Vexna	46.153.14...	ABU_MAD...	Windows ...	0.00 Bytes...	ÇáÚÑÈiÉ (çáóú...	x	x	3
	Vexna	94.59.91....	MS / M Shafi	Windows ...	325.51 MiB...	English (United St...	x		2
	Vexna	94.59.22....	AL-8F715...	Windows ...	459.71 MiB...	Arabic (U.A.E.) A...	x	x	5
	Vexna	46.44.119...	USER-0AE...	Windows ...	428.11 MiB...	ÇáÚÑÈiÉ (çáóú...	x	x	4
	Vexna	217.164.2...	H...			English (United St...	x	x	3
	Vexna	86.97.175...	U...			English (United St...	x	x	2
	Vexna	2.90.103....	A...			English (United St...	x	x	3
	Vexna	188.55.11...	A...	Windows ...	450.02 MiB...	ÇáÚÑÈiÉ (çáóú...	x		5
	Vexna	119.155.1...	KRN-BDBD...	Windows ...	359.15 MiB...	English (United Ki...	x		4
	Vexna	188.249.8...	ßiEäÈÇÖñ...	Windows ...	1.12 GiB/1....	ÇáÚÑÈiÉ (çáóú...	x.	x	4
	Vexna	188.54.10...	03F32919...	Windows ...	306.89 MiB...	ÇáÚÑÈiÉ (çáóú...	x	x	3
	Vexna	476.45.80...	ACCD_14...	Windows ...	225.20 MiB...	ÇáÚÑÈiÉ (çáóú...			2

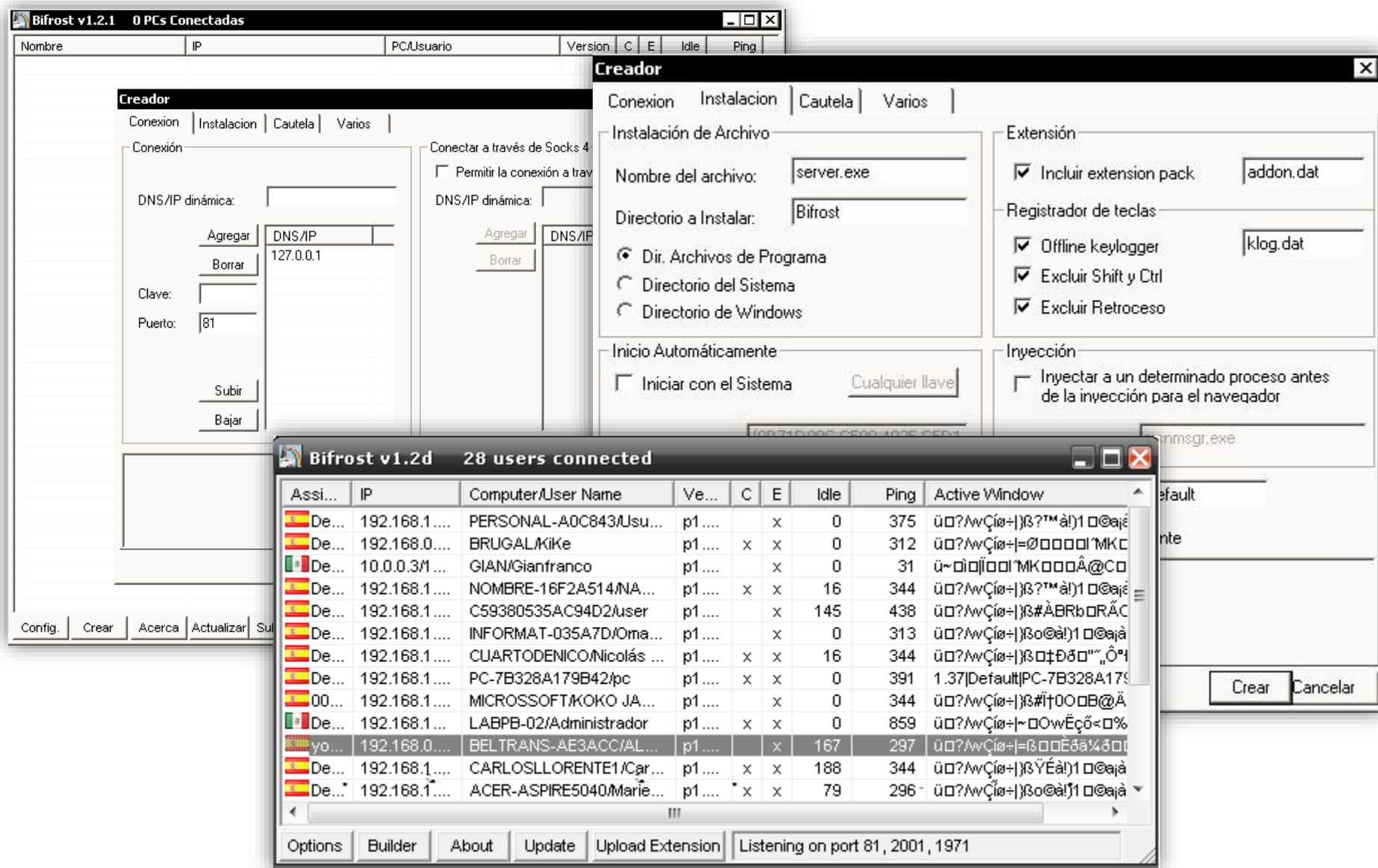
DARKCOMET
REMOTE ADMINISTRATION TOOL

Connections On Connect Edit Server Settings Users logs Sockets/Net

Troyano Poison Ivy



Troyano Bifrost



Troyano ProSpyRAT (\$)

ProSpy RAT V2 - 13 usuarios conectados

Menu Difundir Herramientas Utilidades ?

Conexion Herramientas Seleccionar Accesos directos

Conexiones Ventanas No-ip Registros Estado PS Online

Vista conexiones

Informacion Miniaturas

20:19:23: [DESKTOP-7787]: Juegos de Modo Escuchando en puerto 3000

ID	IP	PC/USUARIO	PAIS	SO	VER	PRIV...	ESTADO/VENTANA ACTIVA
MI_PC	192.168.1.10	Sistema		WIN XP	2.0.2	Admin	Juegos de moda para chicas - Juegos internet gratis
DAVID-FD671F66B-1476	192.168.1.10	Administrador de archivos		Win 7	2.0.2	Admin	My Shared Folder
VAIO-2804	192.168.1.10	Captura de pantalla		Win Vista	2.0.2	Admin	Twitter / Mis Tweets, retuiteados - Google Chrome
REGINATO-5900	192.168.1.10	Captura de camara		Win 7	2.0.2	Admin	(2) Facebook - Google Chrome
USUARIO-PC-1166	192.168.1.10	Captura entrada de audio/microfono		Win 7	2.0.2	User	Canal de [REDACTED] - YouTube
WN764-PC-9...	192.168.1.10	Keylogger		Win XP	2.0.2	Admin	Spider
DESKTOP-7787	192.168.1.10	Shell remota		Win XP	2.0.2	Admin	vivaerobus.com
HECTOR-PC-...	192.168.1.10	Enviar teclas					
FLIAYRAUS..._5957	192.168.1.10	Ultimas ventanas activas					
EQUIPO ANTES	192.168.1.10	Administrar MSN messenger					
PRUEBA_4	192.168.1.10	Administrar portapapeles					
TRABAJO2	192.168.1.10	Bromas					
USUARIO-577	192.168.1.10	Contraseñas					

Información de sistema
Procesos activos
Ventanas activas
Aplicaciones instaladas

ProSpy RAT V2 - 14 usuarios conectados

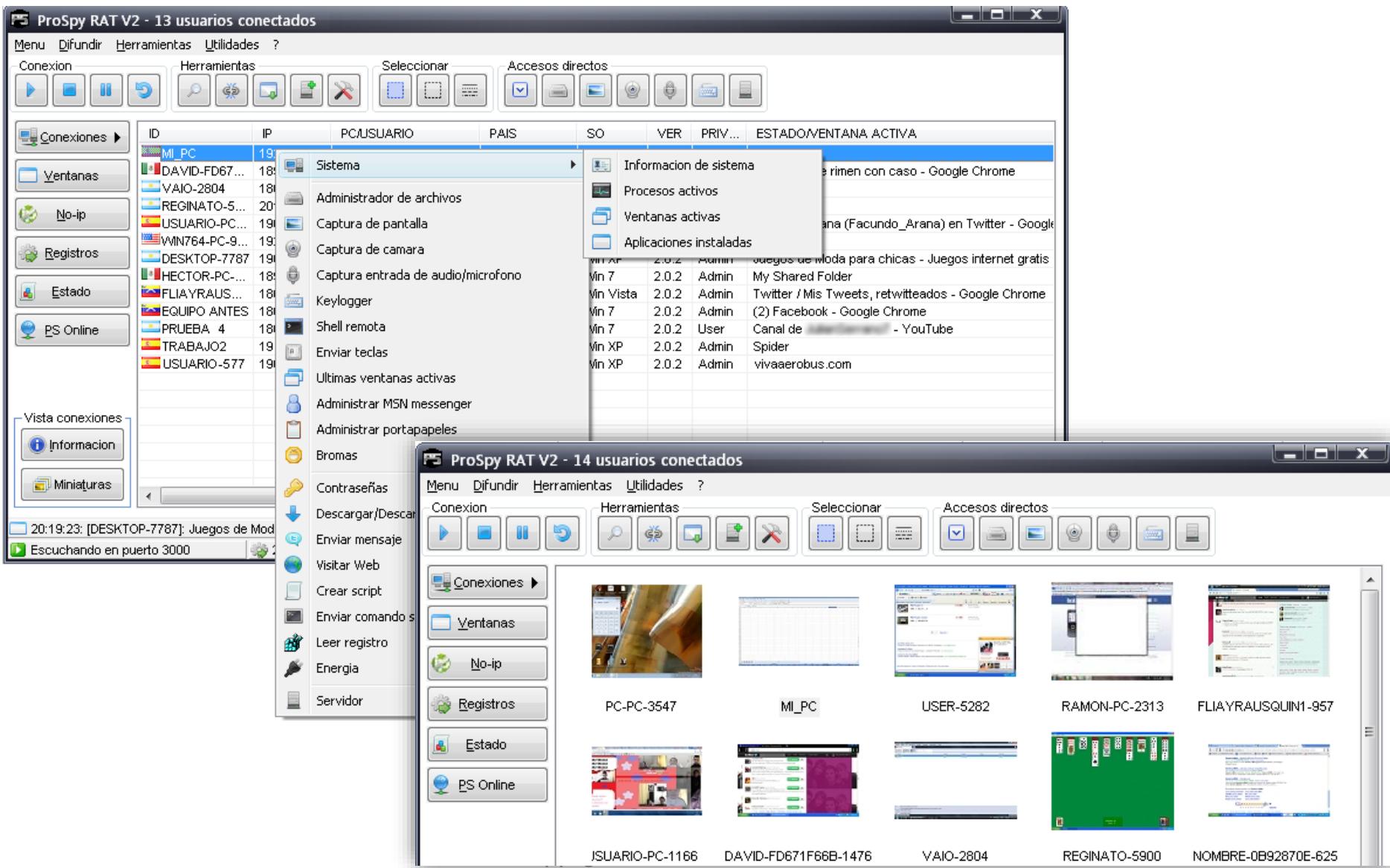
Menu Difundir Herramientas Utilidades ?

Conexion Herramientas Seleccionar Accesos directos

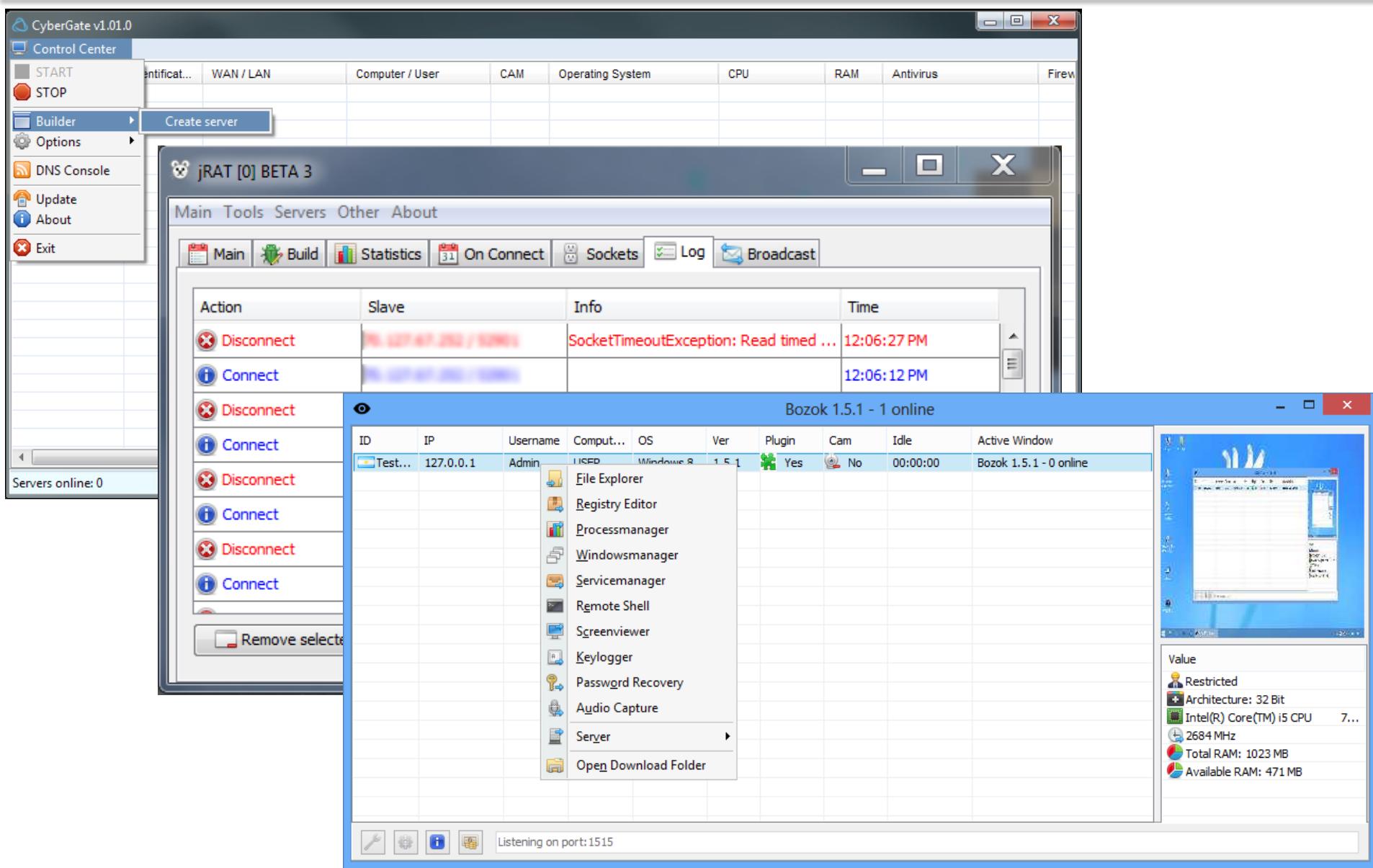
Conexiones Ventanas No-ip Registros Estado PS Online

PC-PC-3547 MI_PC USER-5282 RAMON-PC-2313 FLIAYRAUSQUIN1-957

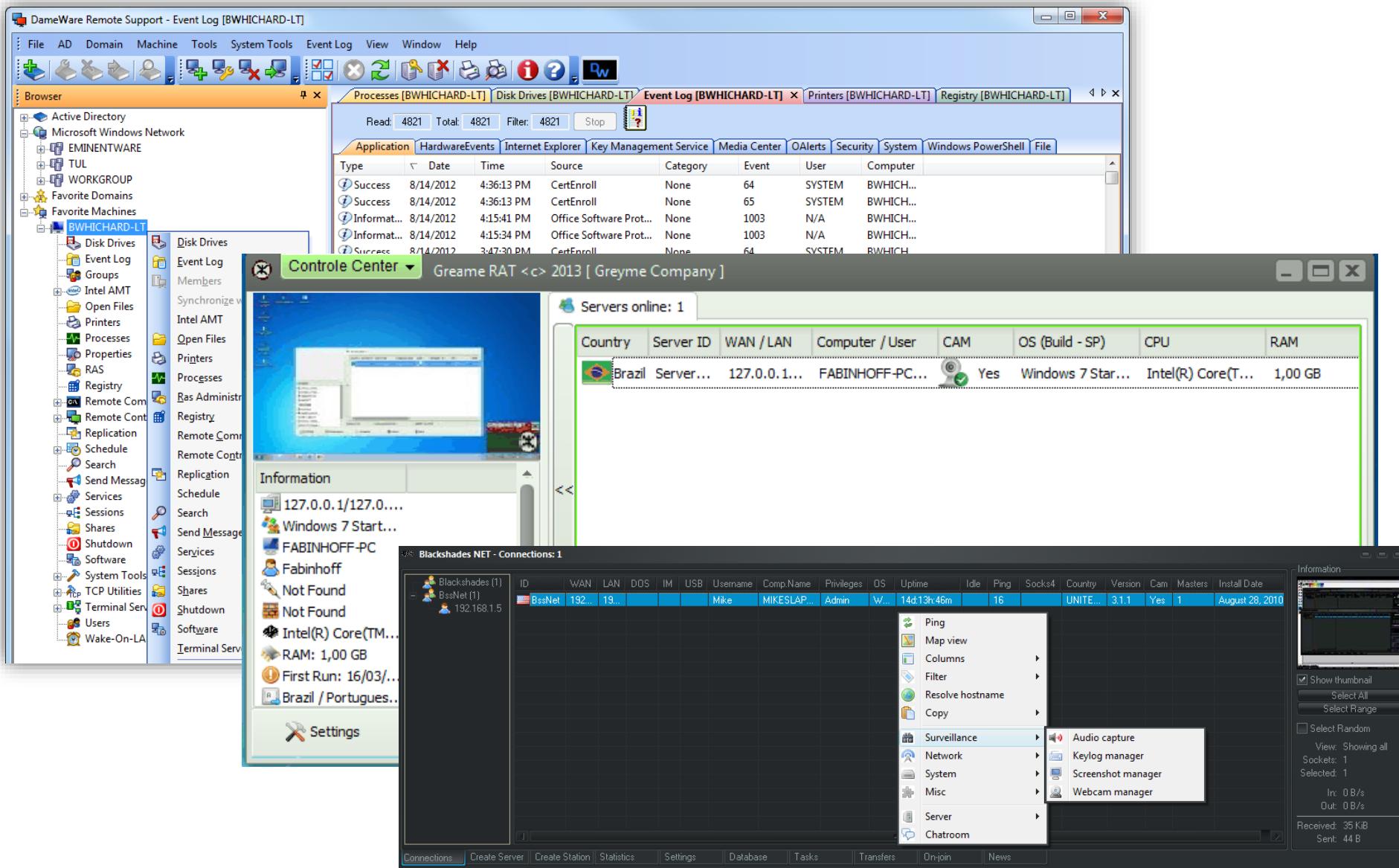
ISUARIO-PC-1166 DAVID-FD671F66B-1476 VAIO-2804 REGINATO-5900 NOMBRE-0B92870E-625



Troyanos varios



Troyanos varios (II)



Troyanos varios (III)

Spy-Net 2.6

Arquivo Opções Sobre START

Localização	Identificação	Computador / Usuário	CAM	Sistema Operacional	CPU
Brazil	vitima_EC6B9EBD	1. SEVEN-PC/SEVEN	X Não	Windows 7 Ultimate (Build: 7...)	Intel(R) Core(TM...
Brazil	vitima_D8ACE693	1. MICRO-COCOSBAR/Client...	Sim	Windows XP Professional (...)	AMD Sempron(t...
Brazil	vitima_1494E768				
Brazil	vitima_90DCC329				
Brazil	vitima_36362073				
Brazil	vitima_4CC00104				
Brazil	vitima_EC697257				
Brazil	vitima_8C418D33				
Brazil	vitima_5C451133				
Brazil	vitima_0EB75768				
Brazil	vitima_B4E893B3				
Brazil	vitima_64627DAA				
Brazil	vitima_6C9ADD39				
Italy	vitima_C0970FE8				
Brazil	vitima_14E86E33				
Brazil	vitima_748000F4				
Brazil	vitima_E8AFDBA5				
Brazil	vitima_401D0F2D				
Brazil	vitima_64CEA4E0				
Brazil	vitima_E0F212C7				
Brazil	vitima_20B2F667				
Brazil	vitima_E8DCED9F				
Brazil	vitima_CC355B07				

jSpy 0.31 - [Connections: 1]

Sessions On-Connect Commands Installed Plugins Configuration Builder

#	ID	IP	Port	PC Name	OS	MAC Addr.	Version
0	Fabinhoff	127.0.0.1:49363	49363	FB-PC	Windows 7	08-00-27-93-4...	0.31

Sessions selected: 1

- Networking
- Surveillance
- Fun Functions
- File Explorer
- Remote Chat
- CMD/Terminal
- Inject Jar (into memory)
- Session Information
- Plugins
- Maintenance

Screen Capture Webcam Capture Live Keylogger Offline Keylogger

J SPY

PussyRAT 0.33 [Guest: 1]

File Edit Theme Help

Connections Build Listen On-Connect Plugins

(Online: 1) (Peak: 1)

[22:49:26] Welcome to j Spy 0.31.
[22:50:28] Built server to: C:\User...
[22:51:04] Listening to 3175.
[22:51:04] [Server]: Initiated Server
[22:51:04] [Server]: New session:

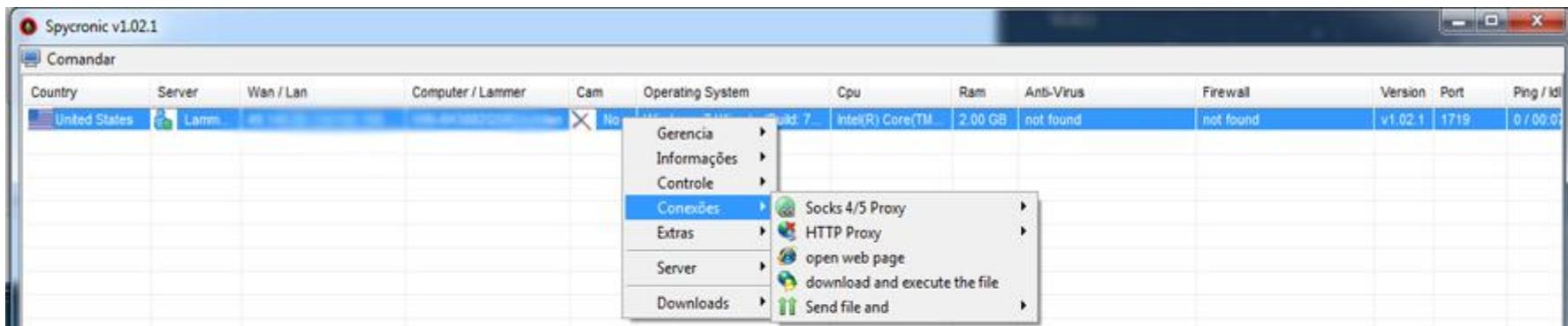
[08:39:04] Welcome Guest, PussyRAT 0.33 launched, begin your session by heading to the "Listen" tab.
[08:39:07] Listening to 3175.
[08:39:07] [Server]: Server Started.
[08:39:07] [Server]: New session: 127.0.0.1:51413

Session Preview

PUSSY RAT

Get Chunk: 0
Get Chunk: 1
Get Chunk: 2

Troyanos varios (IV)



A screenshot of the ::Lost@Door v 8.0.1 Fix+ interface. At the top, there's a header with tabs: Hosts Names, AntiVirus, O.System, Wan|IP, Webcam, and Active Window. The Active Window tab is selected, showing the path ..::Lost@Door v 8.0.1 Fix+. Below the header is a sub-header with tabs: Lammers online, D-Dos, and Remote Control. The D-Dos tab is selected, displaying the 'D-Doser' tool. The D-Doser window has fields for Target (www.*****.com), Message (1337), and Delay per sec (20). It also has buttons for Fire !!!, Stop, and Lock. The status bar shows Nbrs Of hits : 0 and Status: Disconnected. To the right of the D-Doser window is a remote desktop session showing a Windows XP desktop with various icons and windows. At the bottom of the main window, there are sections for Informations (User Name: a, Computer Name: M, O.System: Microsoft Windows XP, Processor: Intel(R) Pentium(R) D CPU), and a connection status message: Connection Established with Final. There are also status bars at the very bottom: Build Server, Public User: [a], Connected Server(s) [1], Connection Established with Final, and @Unique_Oussamie.

Troyanos (V)

njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]

Scre	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	Hacked_C043E7A7	127.0.0.1	ZTHREAT	zuser	15-03-11		N/A	Win XP ProfessionalSP2 x86	No	0.7d	000ms	My Documents

Manager

- Run File
- Remote Desktop
- Remote Cam
- Microphone
- Get Passwords
- Keylogger
- Open Chat
- Server
- Open Folder

Xyat-RAT V5.0

Menu No-IP Update UPnP Port Scanner Check Port Xyat-Scanner FTP Crédit

Bot's Configurations Builder Port Ouvert Téléchargement/Upload

Status/Pays	Identifications	Adresse IP	OS	Version	Fenêtre Active	Ping

XYA

Trouver Server
ID: Trouver

Socket Status: Connecté | Port Connecté: 123

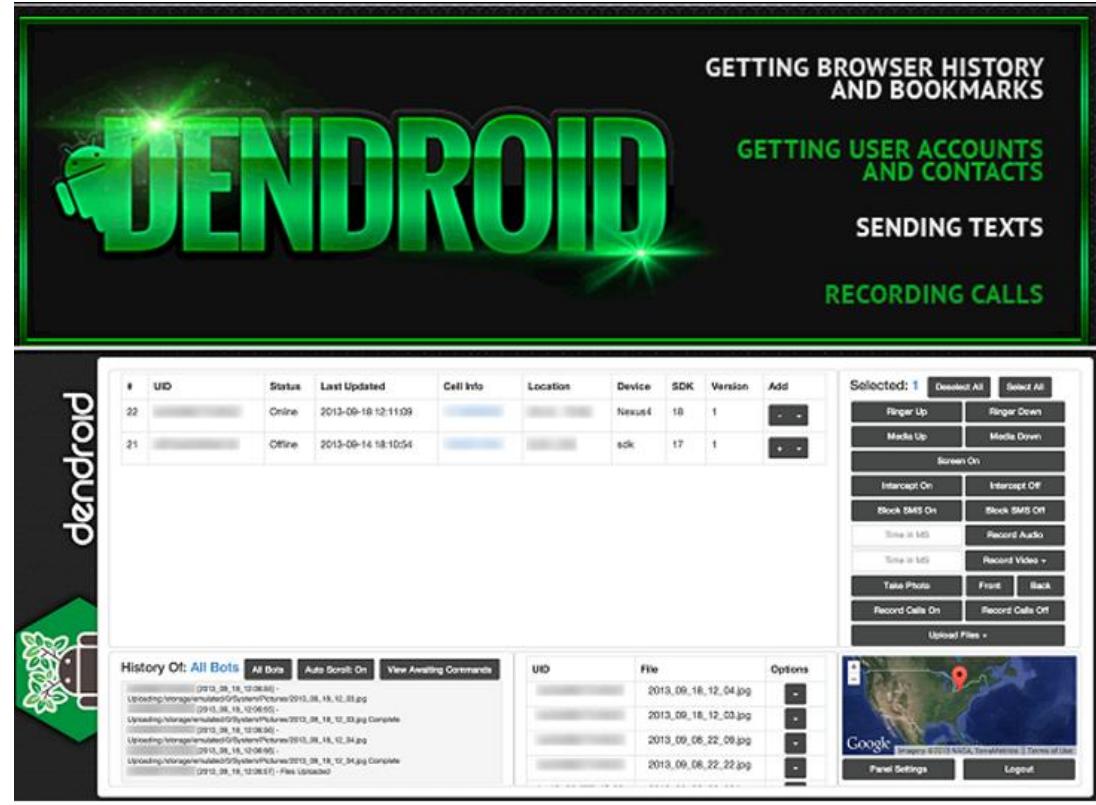
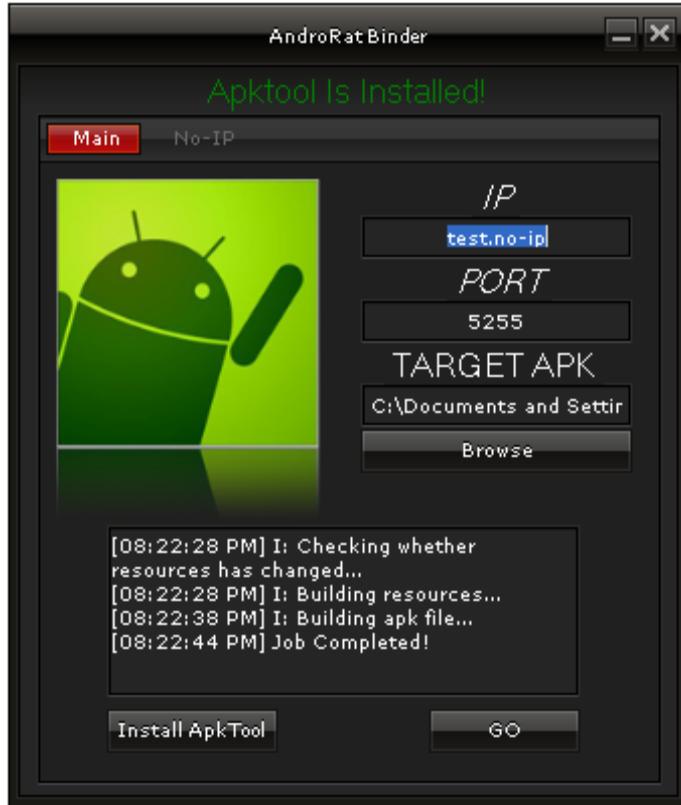
T V5.0

Selectionner Servers à Selectionner

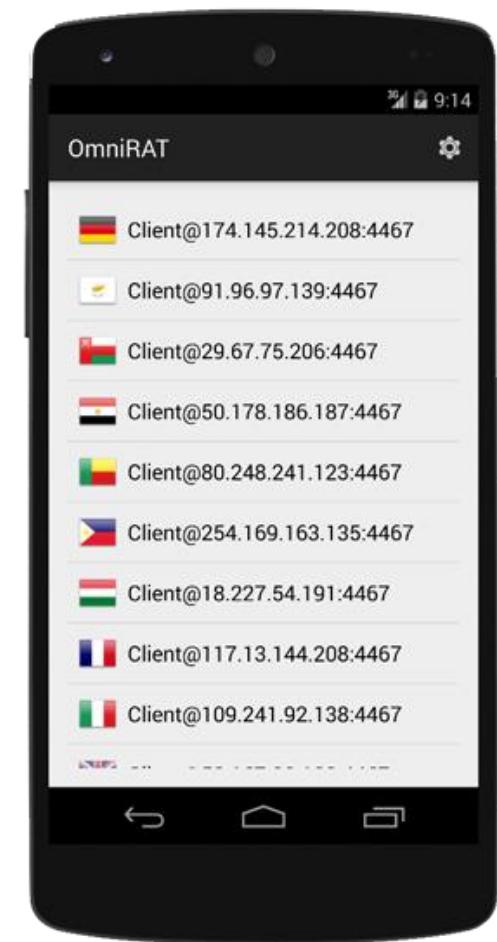
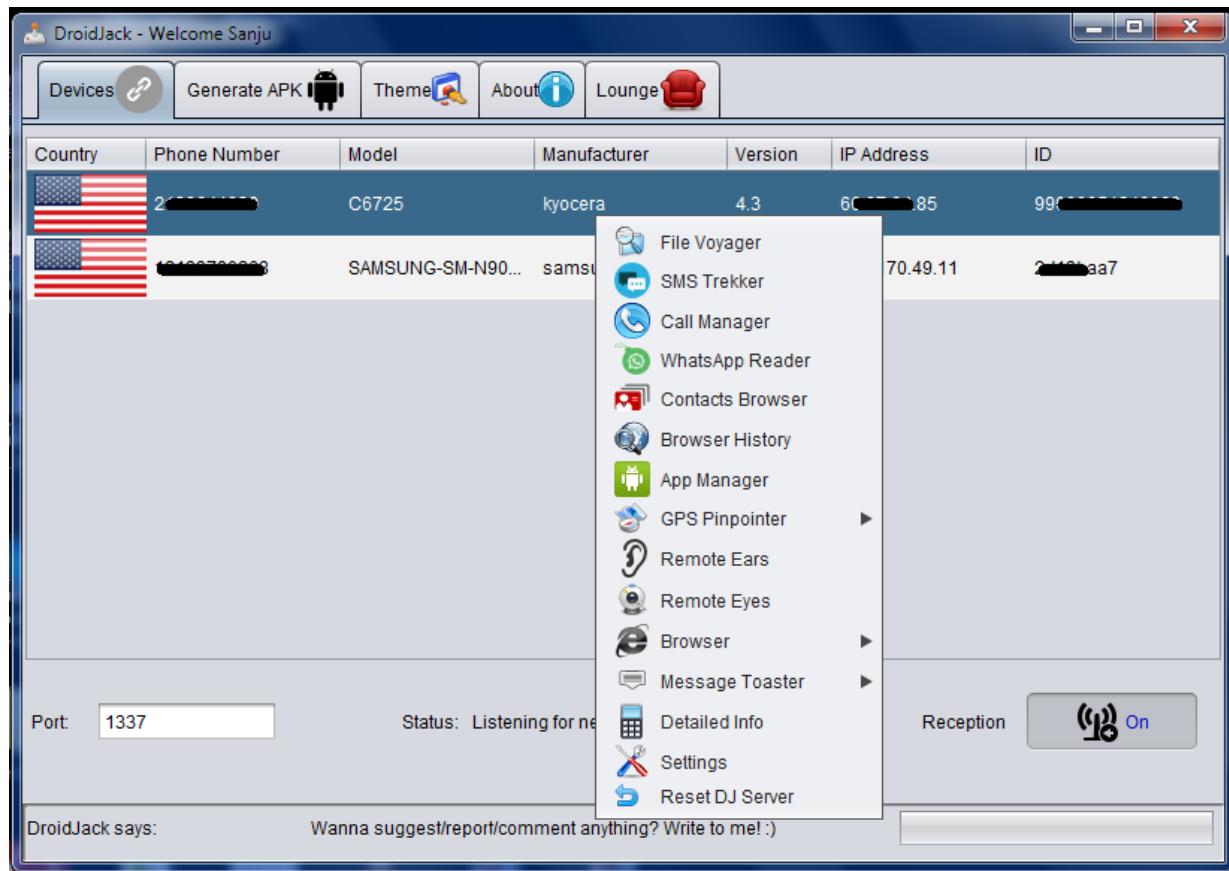
s: 0

Server
Ordinateur
Surveillance
Fonctions Spread
MapView
IP Grabber
Torrent Seeder
Malware Killer
WebSite Blocker
DDoS
Stealer Sécurité
Presse-Papier
Ouvrir URL
Télécharger + Exécuter
Envoyer Message
Script

Troyanos Android



Troyanos Android (\$)



Joiners / Binders

The image displays three software interfaces used for file joining and binding:

- Soprano Binder V3.0 Beta:** A window titled "Soprano Binder V3.0 Beta" showing a table of files. The columns are "Nombre", "Ruta", "Peso", "Llave Cry.", and "Encriptacion". Two files are listed: "a2AntiMalw..." (64,24 MB) and "server.exe" (280 KB). A context menu is open over the "server.exe" row, with options: "Agregar Archivo", "Encriptacion:" (with sub-options "XOR", "RC4", "CryptApi"), "Crear Servidor", "Borrar Todo", and "Borrar Seleccionado".
- JoDeDoR 5x1:** A window titled "JoDeDoR 5x1 v0.1" with the identifier "[c0d3d by m3m0_11]" and the URL "www.JodedorSoftware.tk". It features a large logo for "JoDeDoR 5x1 by m3m0_11". Below the logo are tabs: "Crypter", "Joiner", "Multi-Downloader" (selected), "EOF Writer", "Packer", and "About". In the "Multi-Downloader" section, there is a list of URLs: "www.JodedorSoftware.tk/File.exe", "www.Troyanosvirus.com.ar/File1.exe", and "www.Indetectables.net/Archivo.exe". A context menu is open over the first URL, listing various execution options: "Ejecución Normal y extraer en %System32%", "Inyección en IE", "Inyección en el MSN", "Ejecución Normal y extraer en %Windows%", "Ejecución Normal y extraer en %Temp%", "Ejecución Normal y extraer en %Archivos de Programa%", "Inyección en IE", "Inyección en svchost", "Inyección en ctfmon", "Inyección en el MSN", "Inyección en el Explorer", and "Inyección en mi mismo".
- Magic Binder v2:** A window titled "Magic Binder v2" with the identifier "[c0d3d by m3m0_11]". It shows two selected files: "C:\Users\Fabinhoff\Desktop\Test.exe" (File #1) and "C:\Users\Fabinhoff\Desktop\Test-2.exe" (File #2). At the bottom are buttons for "About" and "Binder".

Hook Analyser

```
C:\WINDOWS\system32\cmd.exe - HookAnalyser3.2.exe
[HOOK] ANALYSER
<Malware & Cyber Threat Intelligence>

beenude11986[@]gmail[dot]com
07/2015      Hook Analyser 3.2 (with Cyber Threat Intelligence)
Do Visit      www.BeenuArora.com & www.HookAnalyser.com
Usage - Interactive : HookAnalyser3.2.exe
For bugs and improvements - Please send an email

[*] Welcome to HookAnalyser Interactive Mode
[1] Spawn and Hook to Application
[2] Hook to a specific running process
[3] Perform Static Malware Analysis
[4] Application crash analysis
[5] Exe Extractor (from Process)
[6] Cyber Threat Intelligence (updated)
[7] Batch Malware Analysis

[-] Please enter your choice [1/2/3/4/5]

C:\WINDOWS\system32\cmd.exe
[HOOK] ANALYSER
Intelligence re-loaded

[1] ThreatIntel.exe -auto
[+] Please input your request/keywords on the following files
[--] Malicious websites feed = feeds -> url.txt
[--] Vulnerabilities feed = feeds -> rssurl.txt
[--] Gather Intel on a particular ip-address = feeds -> intelligence-ipdb.txt
[--] Gather intel on any keyword (ip/hash/etc...) = feeds -> keywords.txt
[--] Gather intel about keywords on Social Media (Twitter - for 2 mins) = feeds -> channels.txt

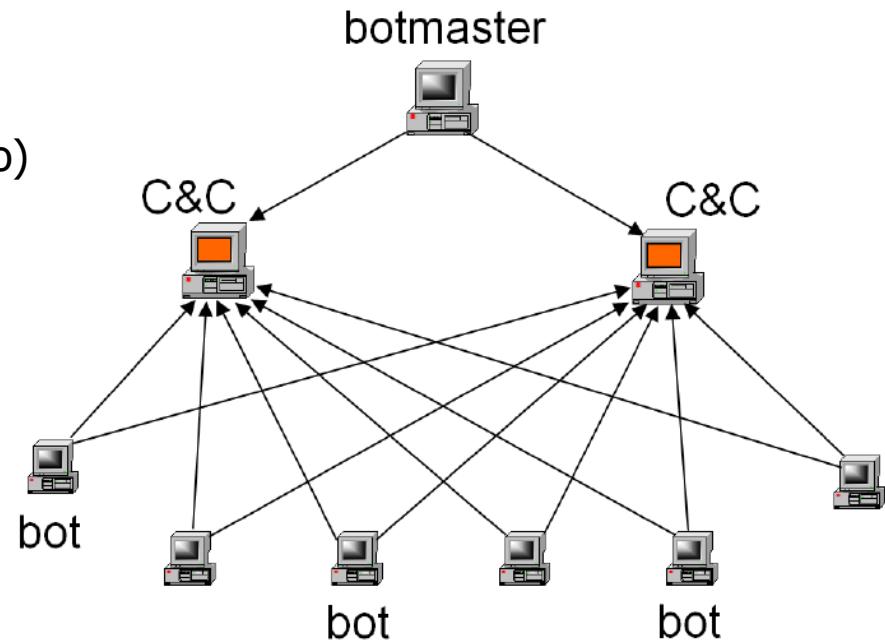
[2] ThreatIntel.exe -f FileName.txt
[INFO] Gather intel from a keywords file or PCAP file

[3] ThreatIntel.exe -t ChannelList.txt
[INFO] Gather intel about keywords on Social Media (Twitter - for unlimited time)

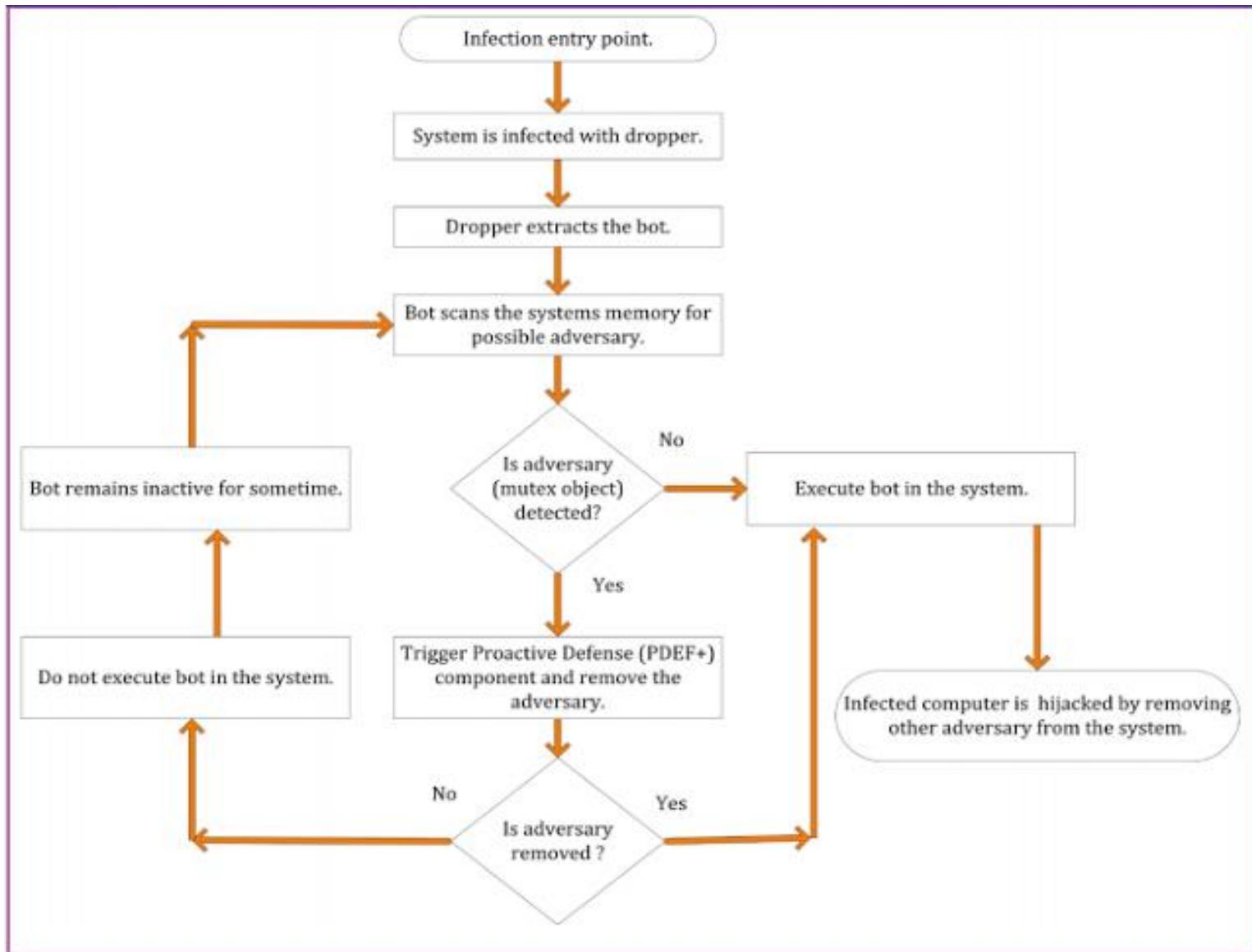
C:\Users\user\Desktop\Research\Hook Analyser 3.2>ThreatIntel.exe -auto_
```

Botnet

- Conjunto de equipos “zombie” controlados remotamente por un atacante
- Características
 - Se controlan desde un centro de comando y control (C&C)
 - Pueden coexistir clientes de distintas botnets en un equipo
 - A veces uno intenta bajar al otro
 - Existen para distintos S.O.
 - Suelen usar servicios de DNS dinámicos
 - Se interconectan por HTTP (a veces cifrado)
- Usos
 - Phishing
 - Contenido ilegal
 - DDoS
 - Spam



Botnet: Bots internals



Técnicas utilizadas por el malware

- Técnicas evasivas
 - AV Evasion
 - Crypters/Packers
 - Binders/Joiners
- Técnicas ofensivas
 - AV Killers
 - DoS



Evasión de payloads de Metasploit: SideScript

- Cifrado del shellcode con AES-128 bits
- Cambio aleatorio de nombres de variables y funciones
- Evasión de sandboxes mediante uso de hora local del host
- Inclusión de variables aleatorias antes de la función main()
- Si Cygwin está presente, utiliza strip para eliminar símbolos de depuración
- Si se usa peCloak, codifica las instrucciones de ensamblado en el último paso

```
root@kali:~/Downloads/SideStep-master# ./sidestep.py
./sidestep.py: line 25:
Name:          SideStep
Version:       0.1.0
Date:          3/30/2015
Author:         Josh Berry - josh.berry@codewatch.org
Github:        https://github.com/codewatchorg/sidestep

Description:   SideStep is yet another tool to bypass anti-virus software. The
               tool generates Metasploit payloads encrypted using the CryptoPP library (licens
               e included), and uses several other techniques to evade AV.

Software Requirements:
Metasploit Community 4.11.1 - Update 2015031001 (or later)
Ruby 2.x
Windows (7 or 8 should work)
Python 2.7.x
```

Evasión: Veil Framework

```
=====  
Veil-Evasion | [Version]: 2.4.0  
=====  
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework  
=====
```

Main Menu

24 payloads loaded

Available commands:

use	use a specific payload
info	information on a specific payload
list	list available payloads
update	update Veil to the latest version
clean	clean out payload folders
checkvt	check payload hashes vs. VirusTotal
exit	exit Veil

[>] Please enter a command: █



Evasión: Shelter

```
*****
* IAT Handler Stage *
*****  
  
Fetching IAT Pointers to Memory Manipulation APIs...  
  
0. VirtualAlloc --> IAT[45d190]  
1. VirtualAllocEx --> N/A  
2. VirtualProtect --> Not Allowed in Stealth Mode!  
3. VirtualProtectEx --> N/A  
4. HeapCreate/HeapAlloc --> IAT[45d16c]/IAT[45d1c4]  
5. LoadLibrary/GetProcAddress --> IAT[45d284]/IAT[45d2e4]  
6. GetModuleHandle/GetProcAddress --> IAT[45d2d8]/IAT[45d2e4]  
7. CreateFileMapping/MapViewOfFile --> IAT[45d28c]/IAT[45d290]  
  
Using Method --> 6  
  
*****  
* IAT Handler Obfuscation *  
*****  
  
Status: Binding the IAT Handler with Thread Context Aware Polymorphic code.  
Please wait...  
  
Code Generation Time Approx: 0.02 seconds.  
  
*****  
* PolyMorphic Junk Code *  
*****  
  
Type: Engine  
Generating: ~425 bytes of PolyMorphic Junk Code  
Please wait...  
Generated: 426 bytes  
Code Generation Time Approx: 0.02 seconds.
```

```
*****
* Payloads *
*****  
  
[1] Meterpreter_Reverse_TCP  
[2] Meterpreter_Reverse_HTTP  
[3] Meterpreter_Reverse_HTTPS  
[4] Meterpreter_Bind_TCP  
[5] Shell_Reverse_TCP  
[6] Shell_Bind_TCP  
[7] WinExec  
  
Use a listed payload or custom? <L/C/H>: L  
Select payload by index: 1  
  
*****  
* meterpreter_reverse_tcp *  
*****  
  
SET LHOST: 192.168.56.101  
SET LPORT: 4444  
  
*****  
* Payload Info *  
*****  
  
Payload: meterpreter_reverse_tcp  
Size: 281 bytes  
Reflective Loader: NO  
Encoded-Payload Handling: Enabled  
Handler Type: IAT  
  
*****  
* Encoding Stage *  
*****  
Encoding Payload: Done!
```

Evasión: PayDay

```
root@kali:~/payday# mkdir -p /root/payloads/windows
root@kali:~/payday# python payday.py --veil --msf --ip 192.168.56.101
[!] Generating MSF Payloads
[!] Generating : windows/meterpreter/reverse_tcp
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 299 bytes
Saved as: /root/payloads/windows/revmet.exe
```

Malware en PDFs

- El formato PDF es muy complejo y puede incluir código malicioso
 - Campos: header, objetos, table cross-reference (ubicar objetos) y trailer
 - Permite ejecutar scripts
 - Pueden incluir ofuscación: /JavaScript == /J#61vaScript
- Características
 - /OpenAction, /AA (Additional Action): especifica script o acción a ejecutar
 - /Names, /AcroForm, /Action: también puede especificar y lanzar acciones
 - /JavaScript: especifica el JavaScript a correr
 - /GoTo*: cambia la vista a un destino específico del mismo PDF o de otro
 - /Launch: lanza un programa o abre un documento
 - /URI: accede a un recurso por su URL
 - /SubmitForm, /GoToR: puede enviar datos a una URL
 - /RichMedia: usado para embeder Flash
 - /ObjStm: puede secundar objetos en Object Streams

PDF internals

⌘PDF-1.1

Header

```
1 0 obj
<<
/Type /Catalog
/Outlines 2 0 R
/Pages 3 0 R
>>
endobj
```

```
2 0 obj
<<
/Type /Outlines
/Count 0
>>
endobj
```

```
3 0 obj
<<
/Type /Pages
/Kids [4 0 R]
/Count 1
>>
endobj
```

```
4 0 obj
<<
/Type /Page
/Parent 3 0 R
/MediaBox [0 0 612 792]
/Contents 5 0 R
/Resources
<< /ProcSet 6 0 R
/Font << /F1 7 0 R >>
>>
>>
endobj
```

```
5 0 obj
<< /Length 67 >>
stream
BT
/F1 24 Tf
100 700 Td
(Hello World)Tj
ET
endstream
endobj
```

```
6 0 obj
[/PDF /Text]
endobj
```

```
7 0 obj
<<
/Type /Font
/Subtype /Type1
/Name /F1
/BaseFont /Helvetica
/Encoding /MacRomanEncoding
>>
endobj
```

Objetos

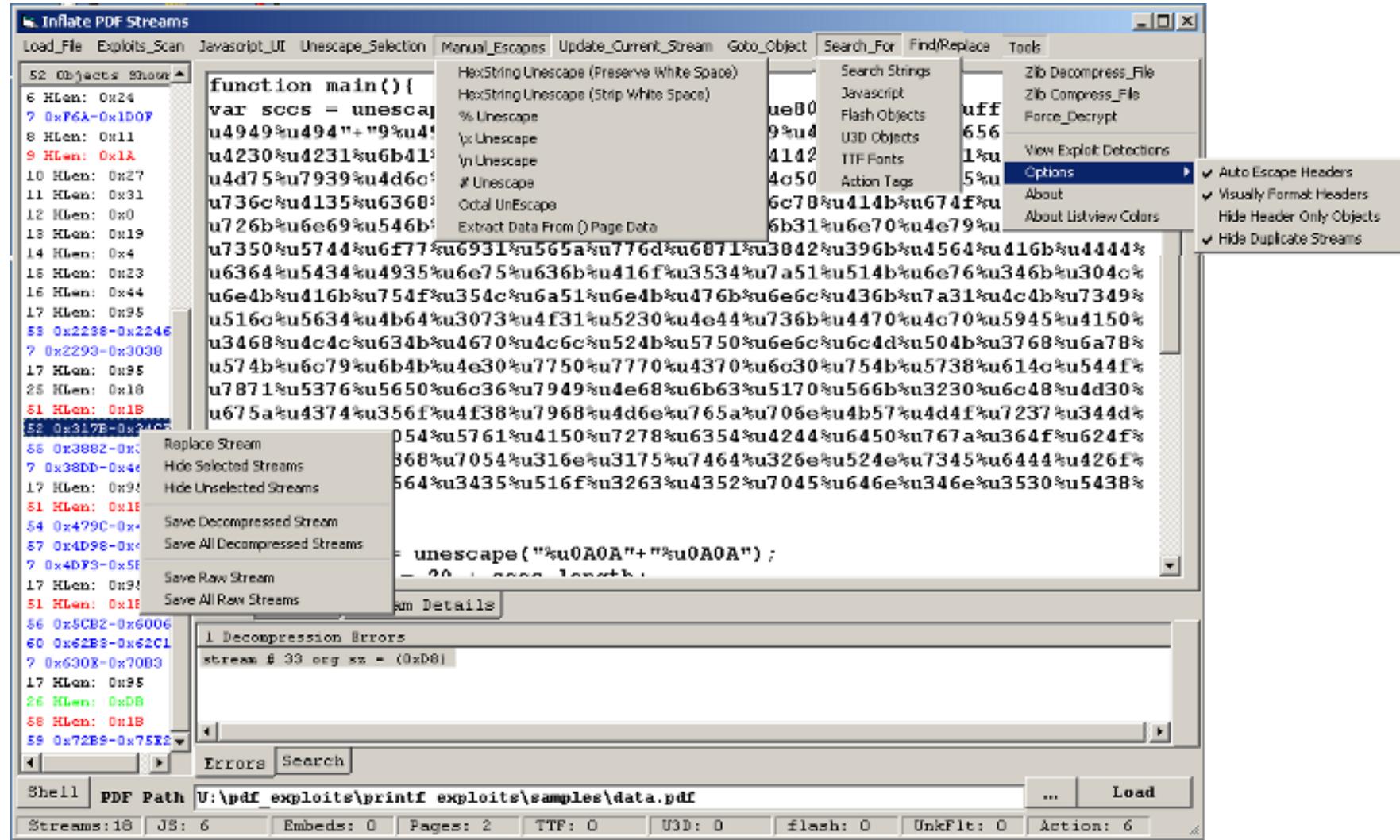
Tabla cross-reference

xref	0 8	0000000000 65535 f
	0000000012 00000 n	0000000089 00000 n
	0000000145 00000 n	0000000214 00000 n
	0000000381 00000 n	0000000485 00000 n
	0000000518 00000 n	

xref	trailer
/Size 8	<<
/Root 1 0 R	startxref
>>	642
	⌘EOF

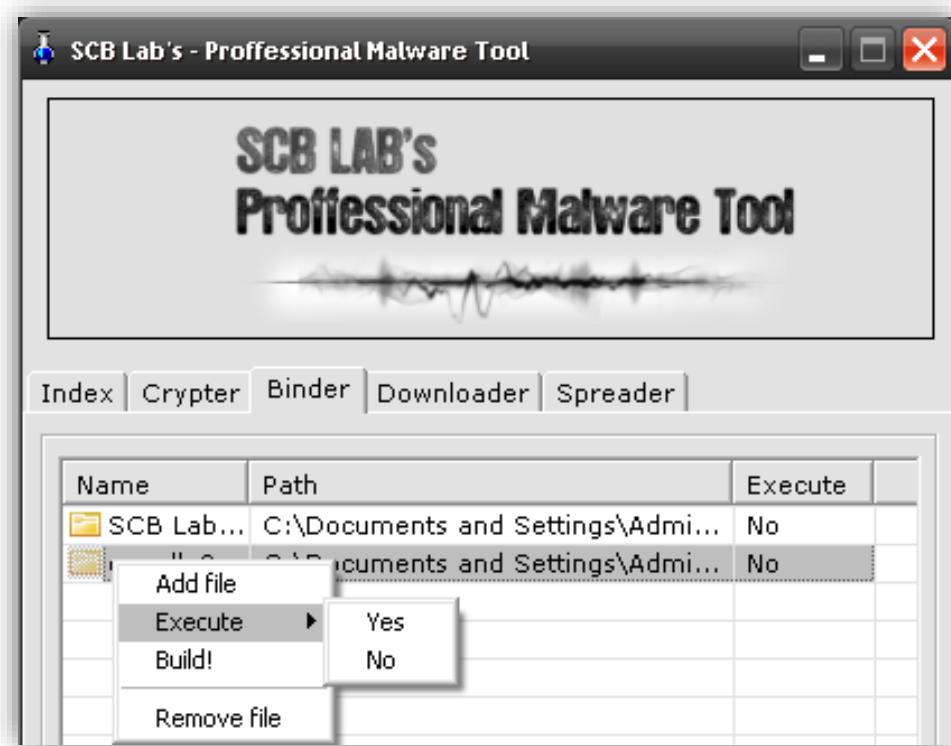
Trailer

PDF Stream Dumper

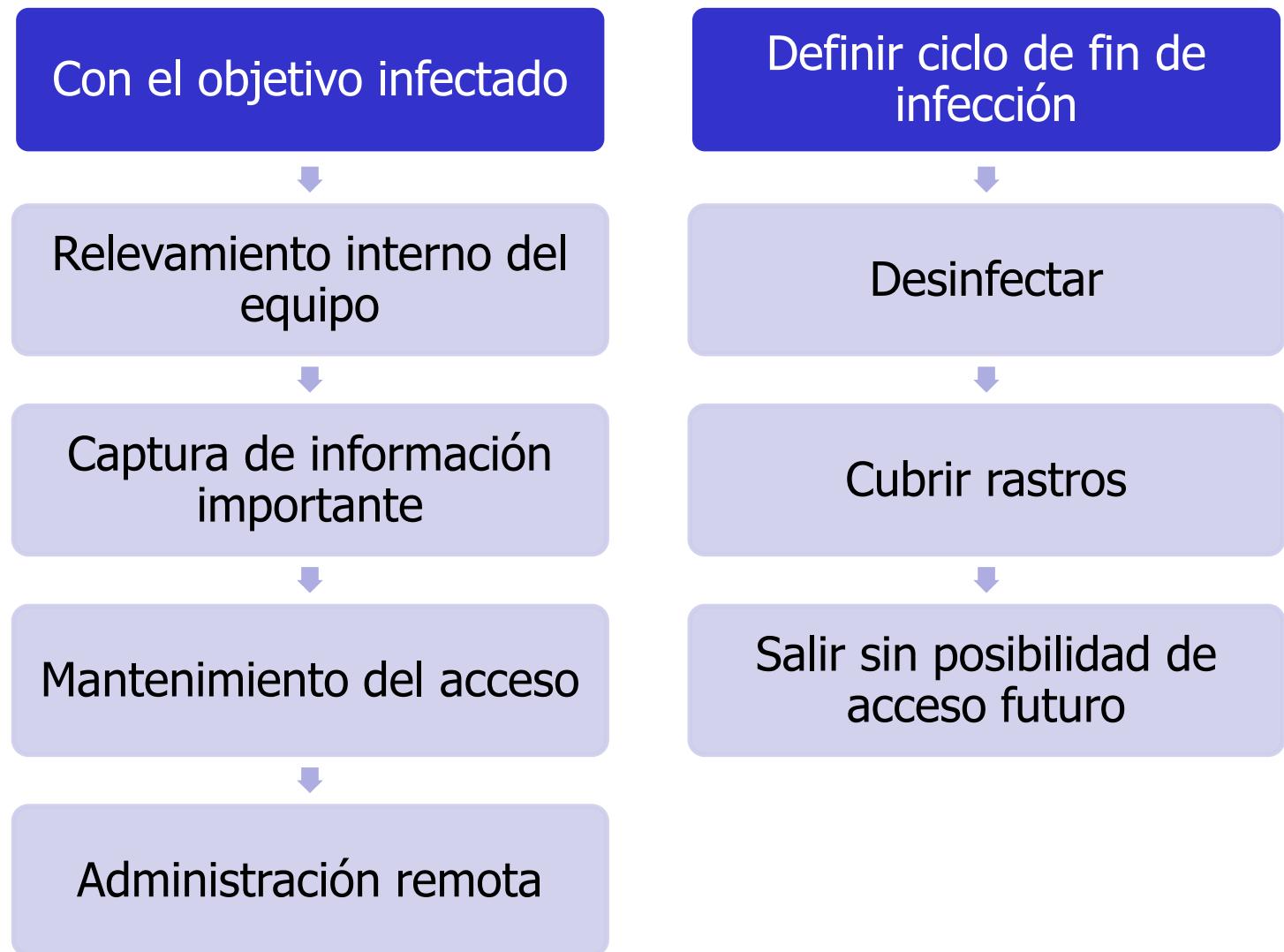


Anatomía de un ataque con malware

- Relevamiento del objetivo
 - Datos de red
 - S.O. con el máximo nivel de detalle
 - Software antivirus
 - Firewall personal
 - Otras aplicaciones
- Contacto con el objetivo
 - Acceso físico
 - Envío por email
 - Drive-by-download



Anatomía de un ataque con malware



Phishing

- Envío de mail masivo o dirigido para inducir al usuario a acceder a un sitio web
- El servidor contiene un sitio falso, controlado por el atacante
 - El usuario ingresa se loguea y sus datos son robados
 - Puede recargar la página llevando al sitio real
- Requerimientos
 - Listas de emails + análisis y filtrado de la base
 - Diseño de emails y sitios (snapshot de sitios reales)
 - Alojamiento: propio o sitios reales vulnerables
 - Envío de spam (botnets)
 - Sistema de lavado: dinero virtual a físico



¿Preguntas?

Federico Pacheco



@FedeQuark



www.federicopacheco.com.ar



info@federicopacheco.com.ar