

Software Antimalware

Adrián Gómez Lois

Contido

1. Obxectivos	3
2. Keyloggers	4-20
3. Software de xestión remota.....	21-35
4. Software antimalware.....	36-39
5. Análise antimalware live	40-42
6. Análise antimalware en sistemas activos e online.....	43-50
7. Conclusíóns	51

1. Obxectivos

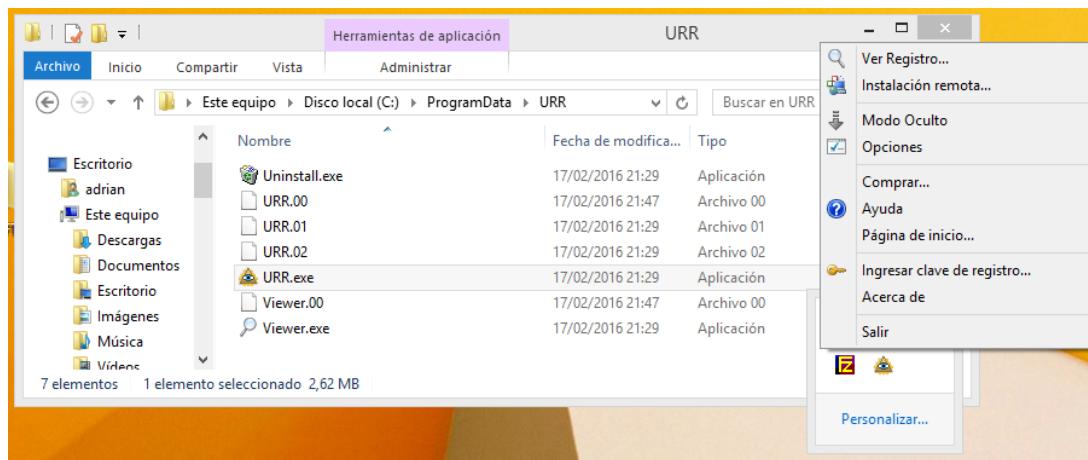
O que tentaremos conseguir con estas tarefas será poder compronder de que forma poden atacar os malwares, onde se poden hospedar dentro dun sistema informático, como detectalos e posteriormente eliminálos.

Verase como tomar control de forma remota doutros equipos e incluso como xerar un Keylogger e tentar ocultalo a través dunha imaxe, a finalidade destas prácticas puramente educativas.

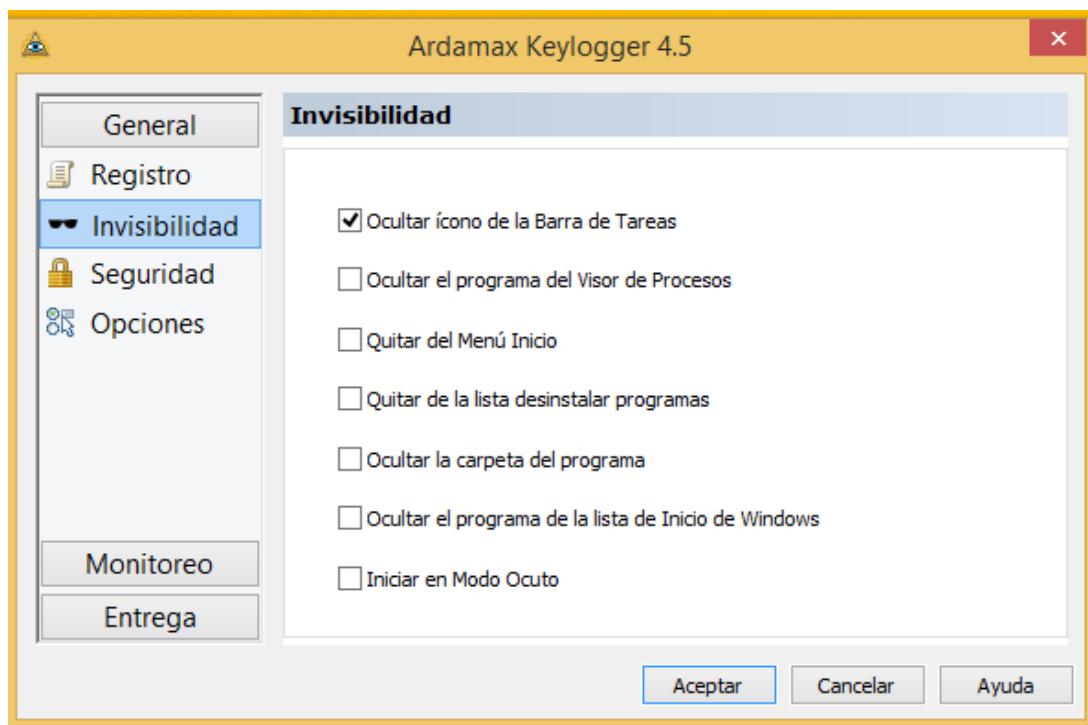
2. Keyloggers

Para esta práctica faremos uso de “Ardamax”, un keylogger xa reconocido que nos permitirá capturar as pulsacións de teclado entre outras cousas que veremos.

Despois de instalalo, vemos que se carga na área de notificacións de Windows, e que se instala na ruta “ProgramData\URR” ficheiro executable URR.exe (en cada instalación xenérase un nome distinto de 3 carácteres para este .exe). Este directorio por defecto está oculto en Windows.

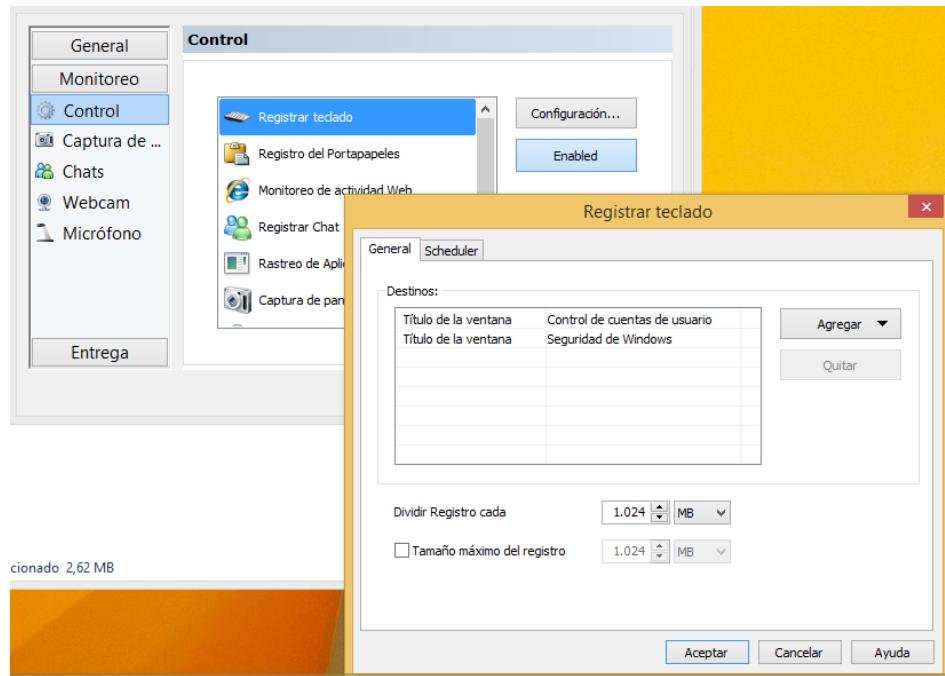


Si abrimos as opcións dos que este dispón, veremos varias bloques que encadran a outros bloques. Centrándose nos máis interesantes, temos a opción de ocultar o programa do Sistema de forma efectiva para o usuario final, pero non para un usuario avanzado, como veremos a posteriori.

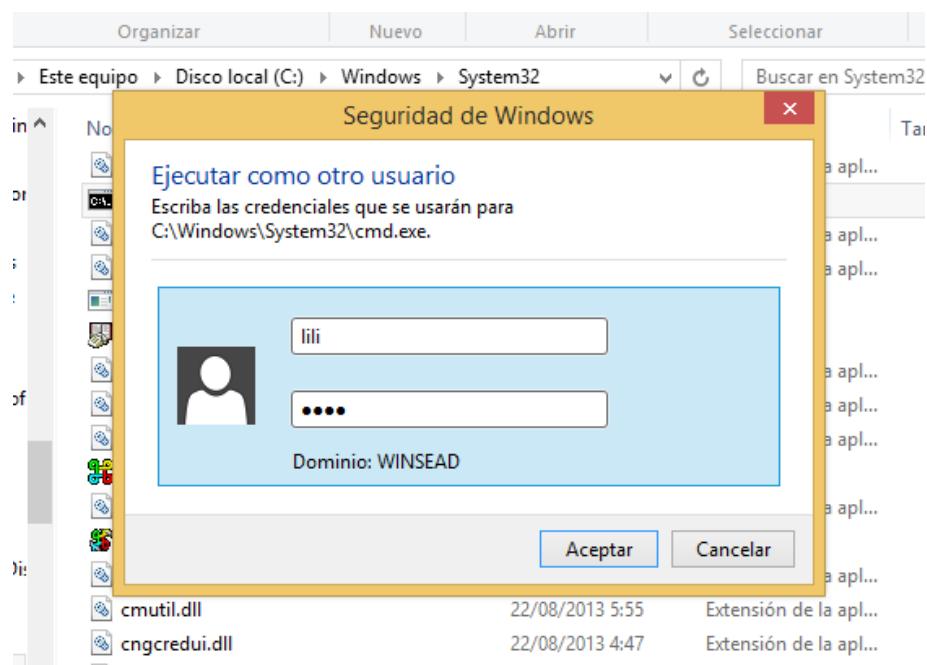


Na zona de monitoreo temos diversas opcións, dende registrar todas as pulsacións do teclado ata poder capturar os clics do rato, chats, rexistro de navegación web, tomar fotografías, capturar audio, rexistro do portapapeis, etc.

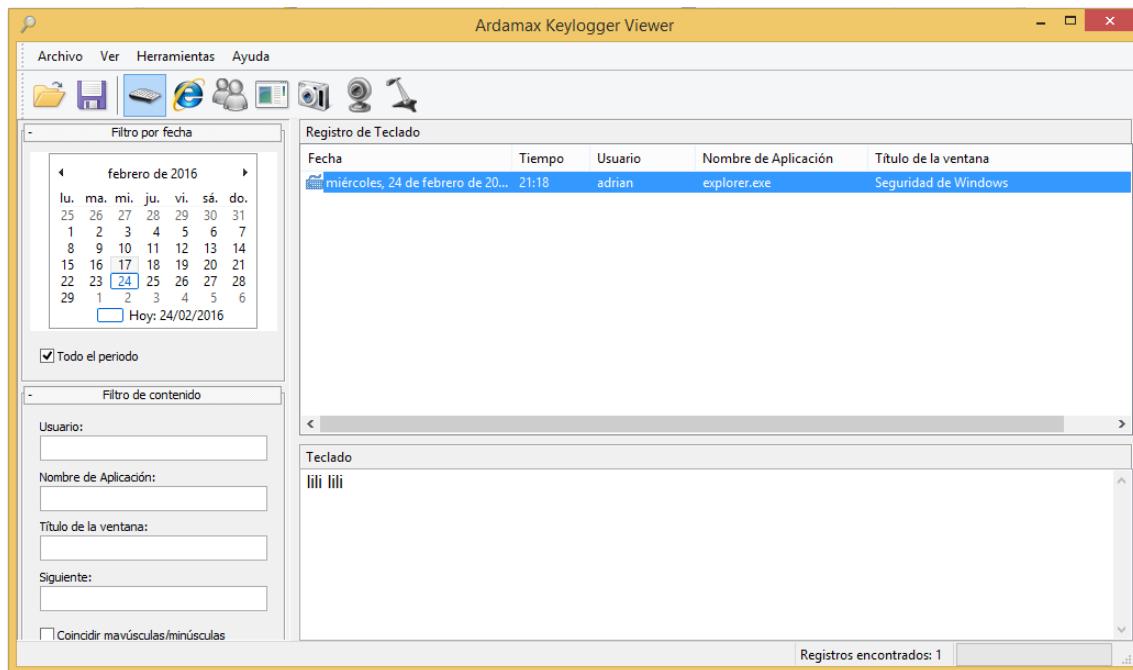
Neste caso e a modo de exemplo, vou capturar todas as pulsacións que se fagan no teclado pero soamente cando o título da ventana sexa “Seguridad de Windows”.



De este modo que cando quero executar algo con privilexios de unha maneira ou outra vou ter que executar unha ventana de UAC (User Account Control) para autenticar un usuario con privilexios.



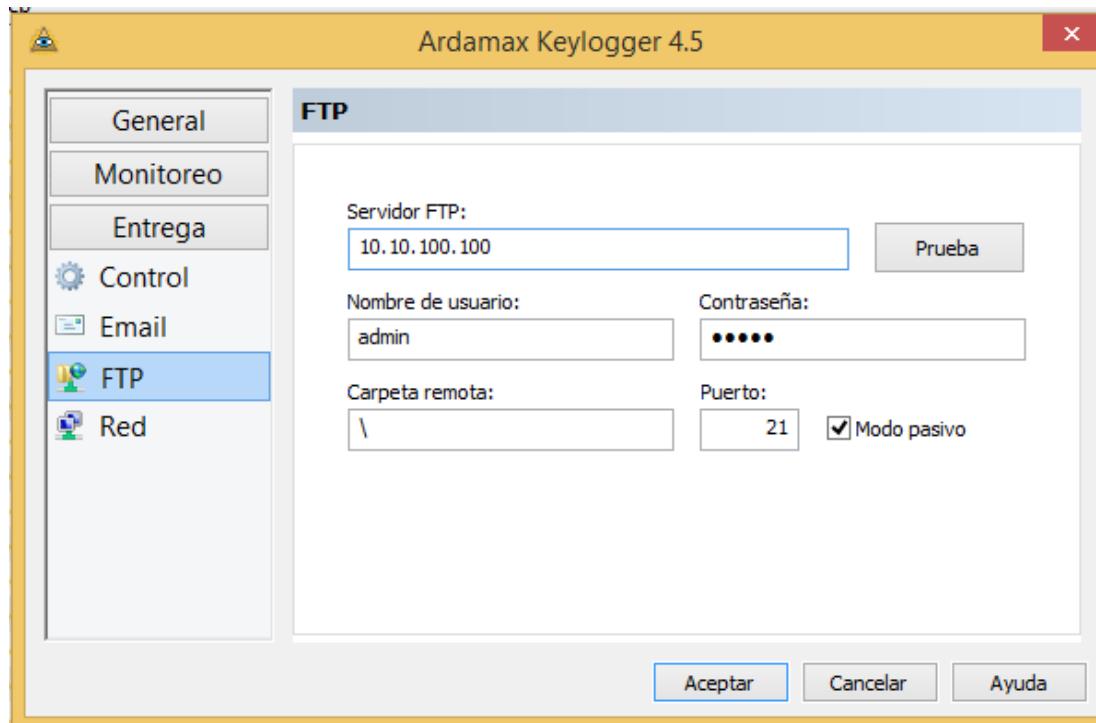
Mirando os rexistros de eventos capturados por ardamax, podemos comprobar como se rexistraron as pulsacións: "lili lili", correspondente ao usuario e contrasinal respectivamente.



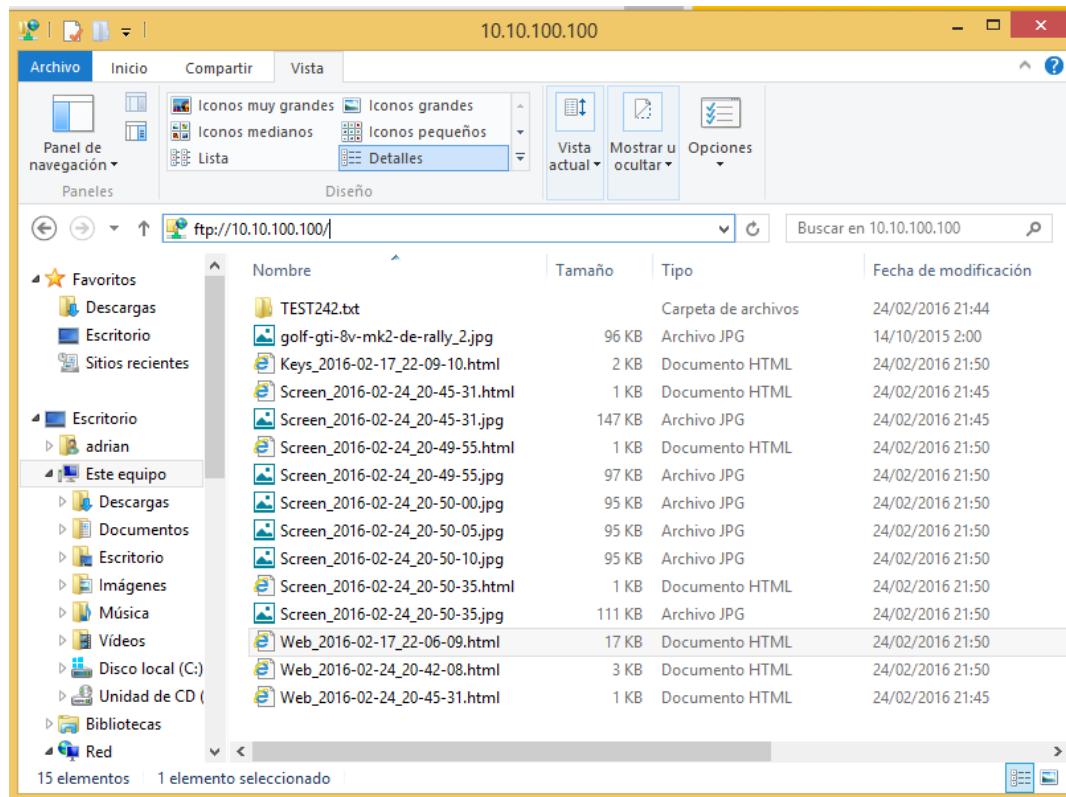
O ultimo punto de configuración de Ardamax e o control de envío de datos, hasta agora fixemos probas en local y comprobamos os rexistros no mesmo equipo, pero temos a opción de enviar estos eventos a un servidor SMTP, FTP ou por rede local.



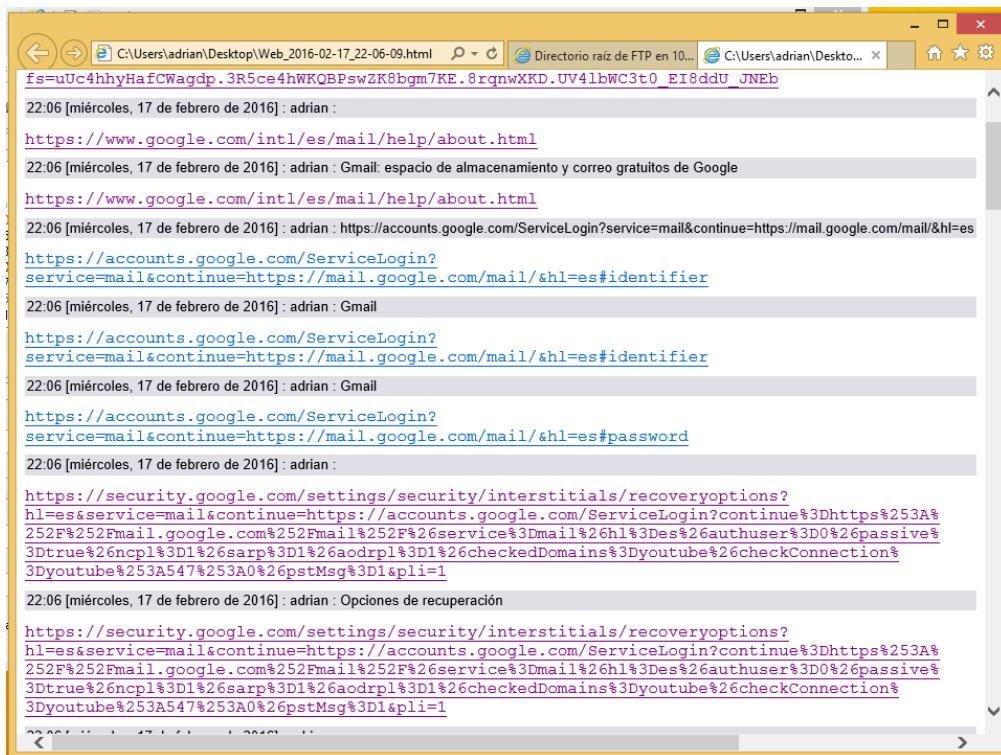
Como proba montouse un servidor FTP noutra maquina. E configurouse Ardamax cos parametros necesarios, para que poda mandar esta información o servidor FTP.



Aquí vemos como está enviando todas as capturas de pantalla, rexistros da nevagación web, e pulsacións de teclado (no configurado anteriormente polo “título da ventana”).



Proba dun ficheiro de navegación, no que se pode ver un inicio de sesión a Gmail.

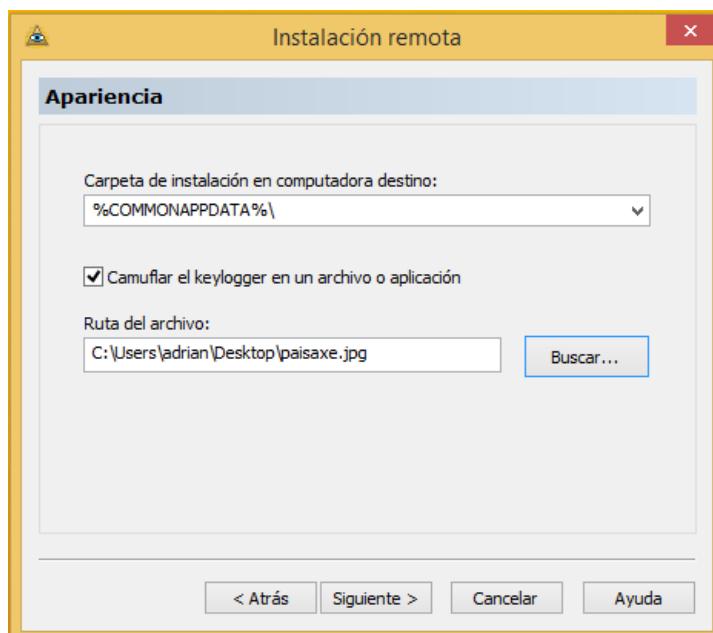


The screenshot shows a Windows taskbar at the top with several pinned icons. Below it is a browser window with the title 'C:\Users\adrian\Desktop\Web_2016-02-17_22-06-09.html'. The address bar contains a long URL starting with 'fs=uUc4hhyHafCWagdp...'. The main content area of the browser shows a scrollable list of URLs visited, primarily related to Google's ServiceLogin and Gmail services. The list includes:

- 22:06 [miércoles, 17 de febrero de 2016] : adrian :
- <https://www.google.com/intl/es/mail/help/about.html>
- 22:06 [miércoles, 17 de febrero de 2016] : adrian : Gmail: espacio de almacenamiento y correo gratuitos de Google
- <https://www.google.com/intl/es/mail/help/about.html>
- 22:06 [miércoles, 17 de febrero de 2016] : adrian : https://accounts.google.com/ServiceLogin?service=mail&continue=https://mail.google.com/mail/&hl=es
- <https://accounts.google.com/ServiceLogin?service=mail&continue=https://mail.google.com/mail/&hl=es#identifier>
- 22:06 [miércoles, 17 de febrero de 2016] : adrian : Gmail
- <https://accounts.google.com/ServiceLogin?service=mail&continue=https://mail.google.com/mail/&hl=es#identifier>
- 22:06 [miércoles, 17 de febrero de 2016] : adrian : Gmail
- <https://accounts.google.com/ServiceLogin?service=mail&continue=https://mail.google.com/mail/&hl=es#password>
- 22:06 [miércoles, 17 de febrero de 2016] : adrian :
- <https://security.google.com/settings/security/interstitials/recoveryoptions?hl=es&service=mail&continue=https://accounts.google.com/ServiceLogin?continue%3Dhttps%253A%252F%252Fmail.google.com%252Fmail%26service%3Dmail%26hl%3Des%26authuser%3D0%26passive%3Dtrue%26ncpl%3D1%26arp%3D1%26adrpl%3D1%26checkedDomains%3Dyoutube%26checkConnection%3Dyoutube%253A547%253A0%26pstMsg%3D1&pli=1>
- 22:06 [miércoles, 17 de febrero de 2016] : adrian : Opciones de recuperación
- <https://security.google.com/settings/security/interstitials/recoveryoptions?hl=es&service=mail&continue=https://accounts.google.com/ServiceLogin?continue%3Dhttps%253A%252F%252Fmail.google.com%252Fmail%26service%3Dmail%26hl%3Des%26authuser%3D0%26passive%3Dtrue%26ncpl%3D1%26arp%3D1%26adrpl%3D1%26checkedDomains%3Dyoutube%26checkConnection%3Dyoutube%253A547%253A0%26pstMsg%3D1&pli=1>

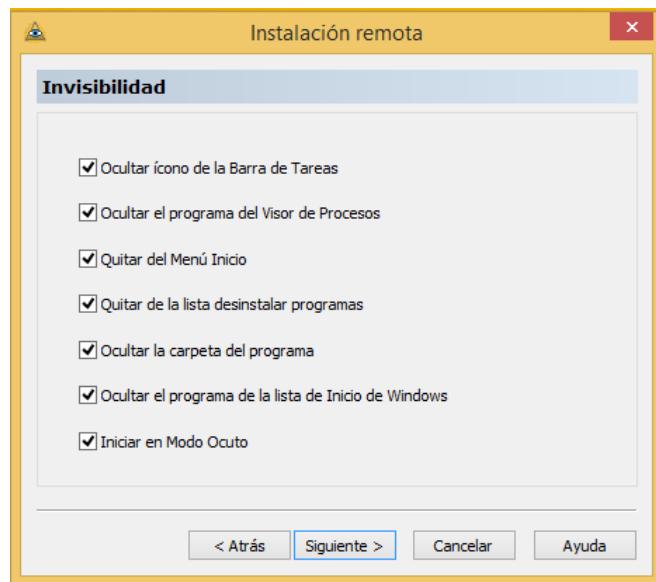
Chegados a iste punto, vamos **configurar Ardamax para unha instalación en remoto** de forma silenciosa (transparente ao usuario final) e que este a execute sin darse de conta de que realmente está executando un Keylogger e que este estase instalando de este modo de forma non lexitima.

Teremos que emascarar o Keylogger noutro arquivo. Por exemplo nunha imaxe .jpg.

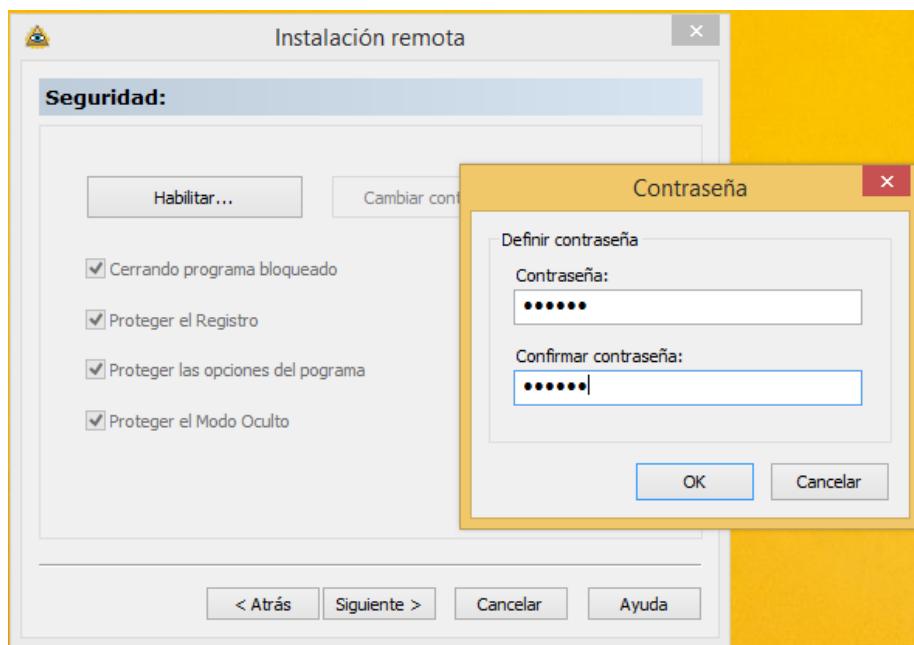


A partir de aquí este asistente irá preguntando configuración a configuración de igual forma que si o instalaramos na máquina remota, esto realmente o que fai e recopilar esta información da configuración para finalmente xenerar un ficheiro binario executable o cal xa estará preconfigurado cas opcións aquí postas.

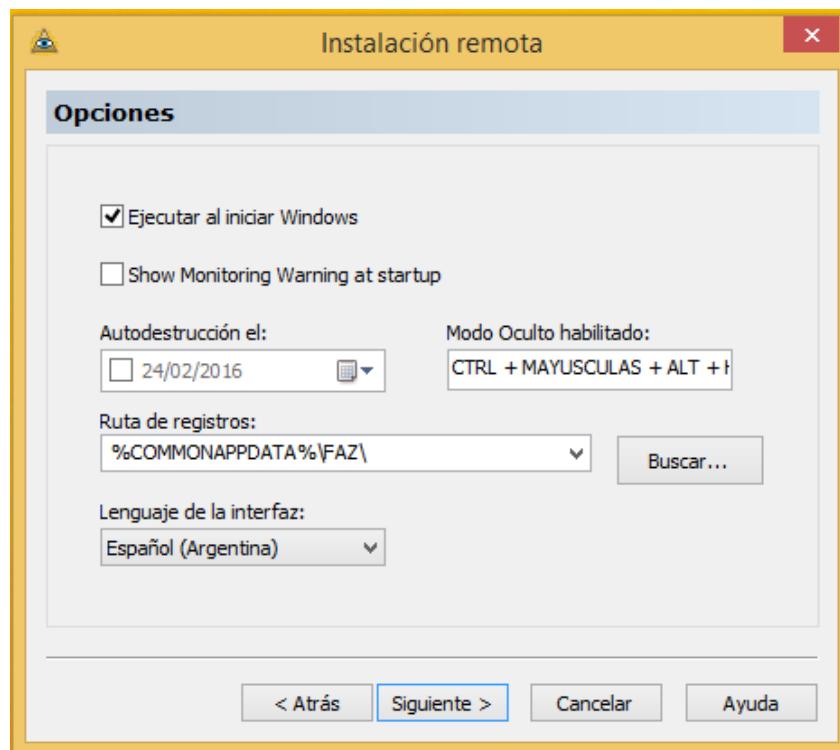
Neste caso e para que usuario non se de conta oculto todo posible rastro de fácil localización fora da vista do usuario remoto.



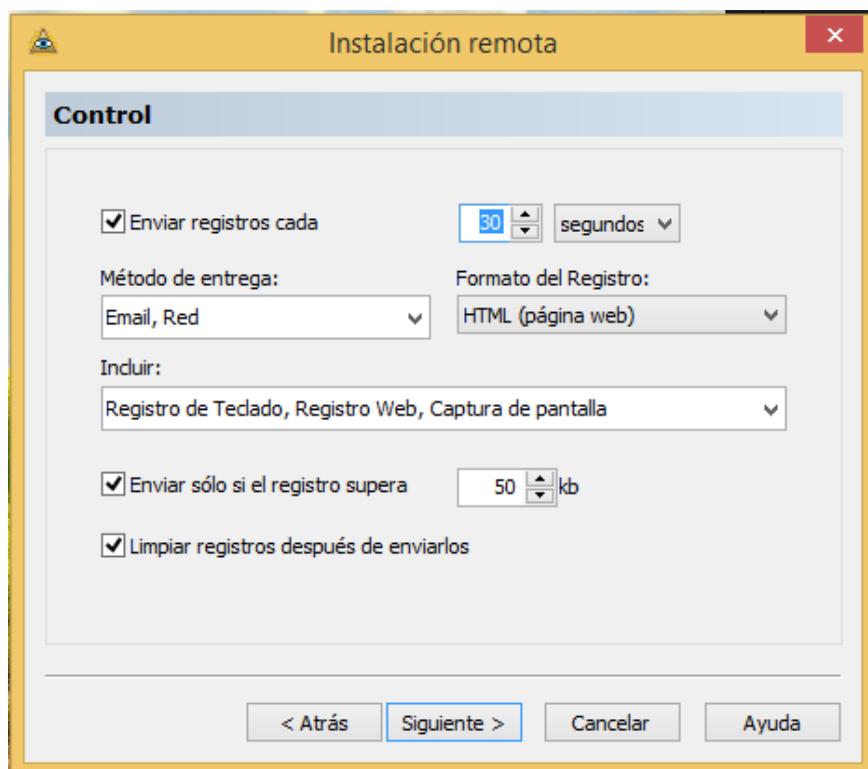
Establécese unha contrasinal para que usuario, no suposto de encontrar o Keylogger este non o poda abrir e desactivalo.



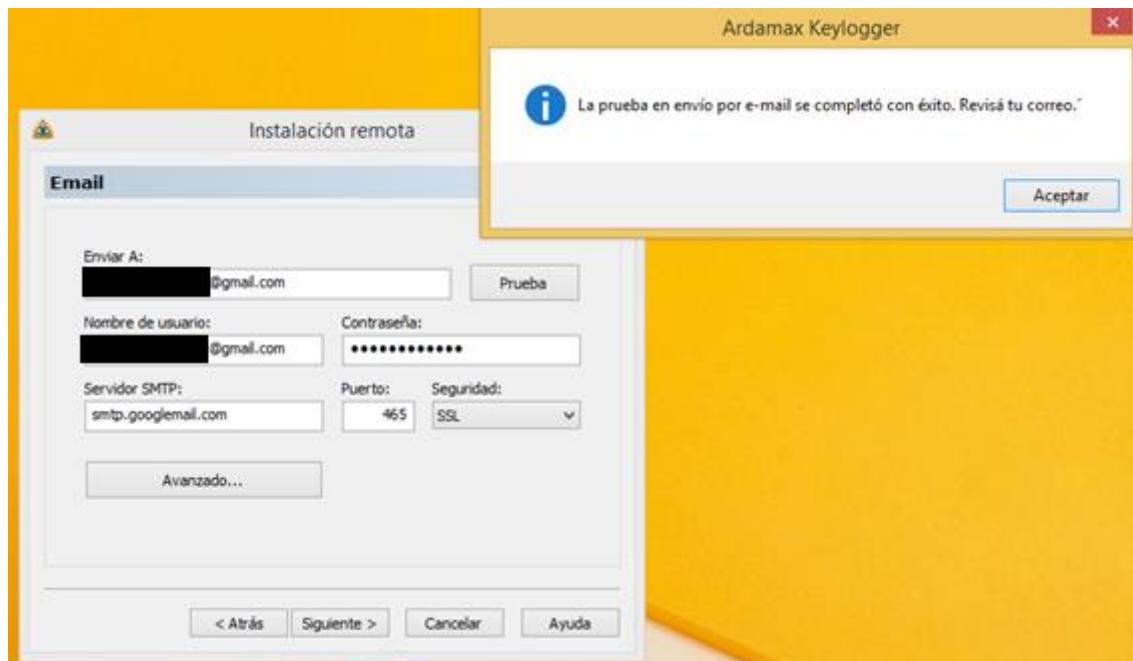
Configúrase a ruta a instalar e outros parámetros, así como que se execute de forma automática o iniciar o Sistema Windows.



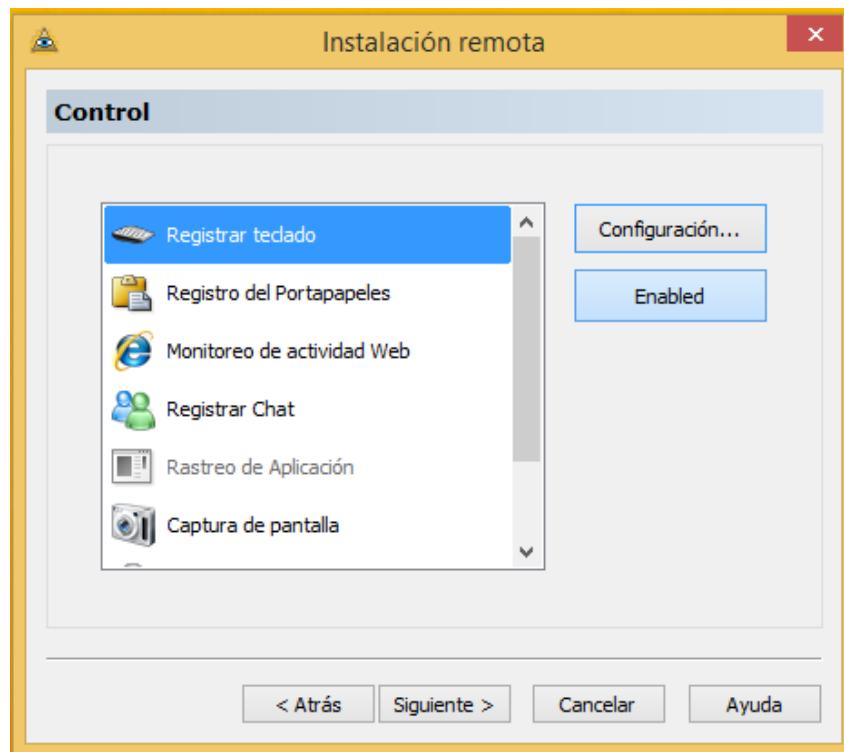
Neste caso emplearei un sistema de email vía SMTP e en rede, marcarase o que queremos que se nos envíe a esos métodos de entrada, cada cuanto tempo, etc.



Configuramos a Email, no caso de Gmail teremos que darlle acceso a aplicación mediante ista conta de correo. Neste exemplo creei unha conta Gmail baixo unha máquina virtual so para esta proba. (ainda que igualmente tapo dita conta).

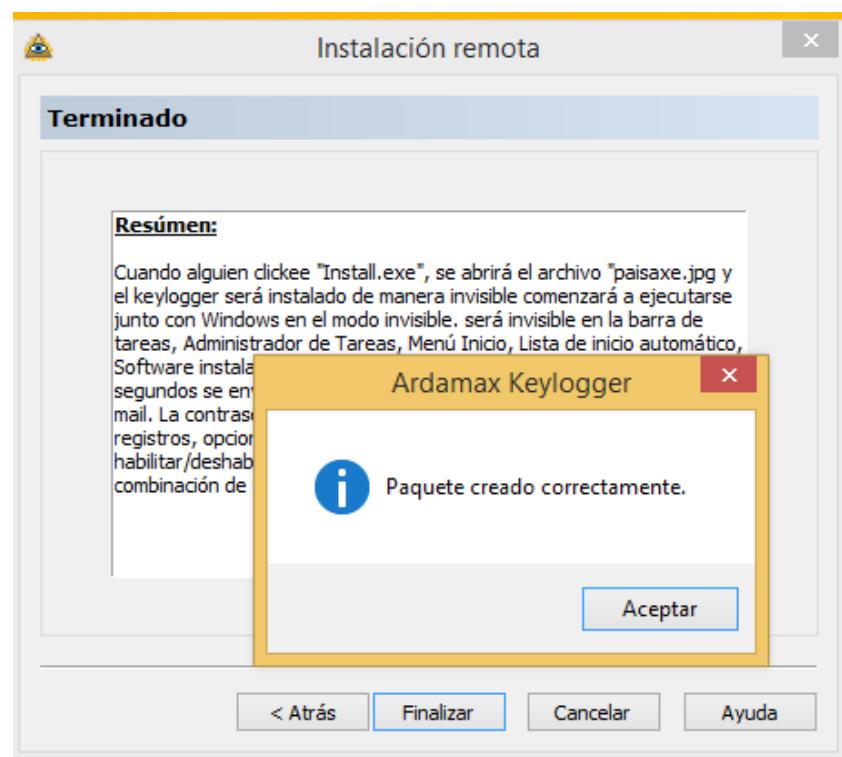


Configuramos a zona de control según as nosas necesidades ou igual que como se mostrou anteriormente.

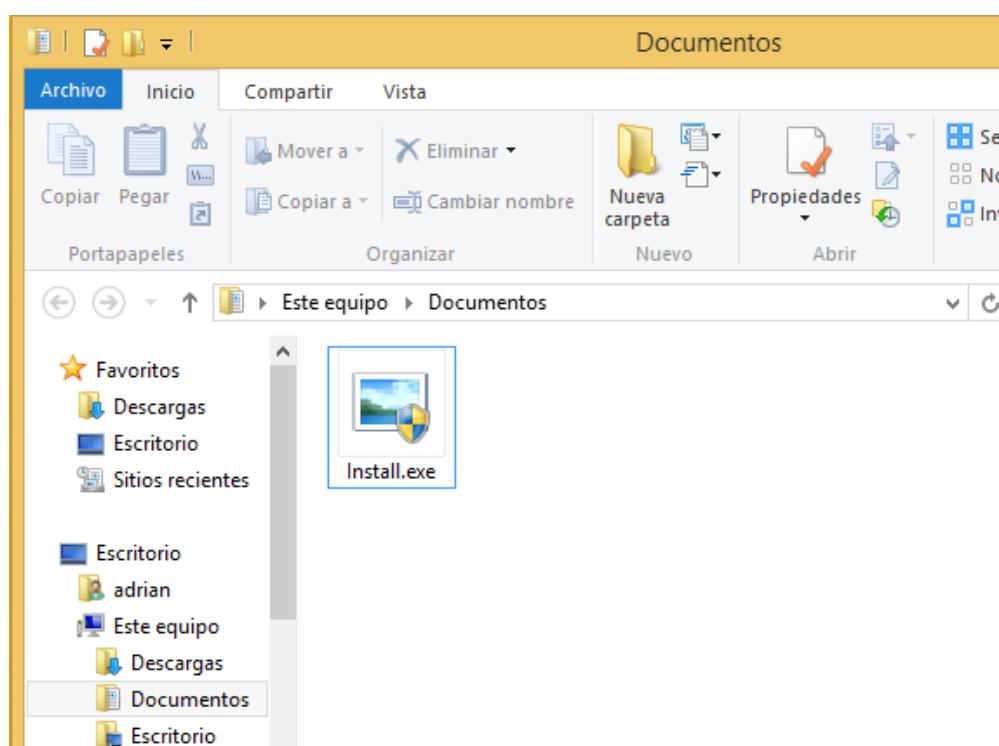


Ainda que non hay captura de pantalla do seguinte paso poderemos cargar un icono de para poder “camuflar” o Keylogger e que o usuario pense que realmente executa unha imaxe (paisaxe.jpg como cargamos anteriormente).

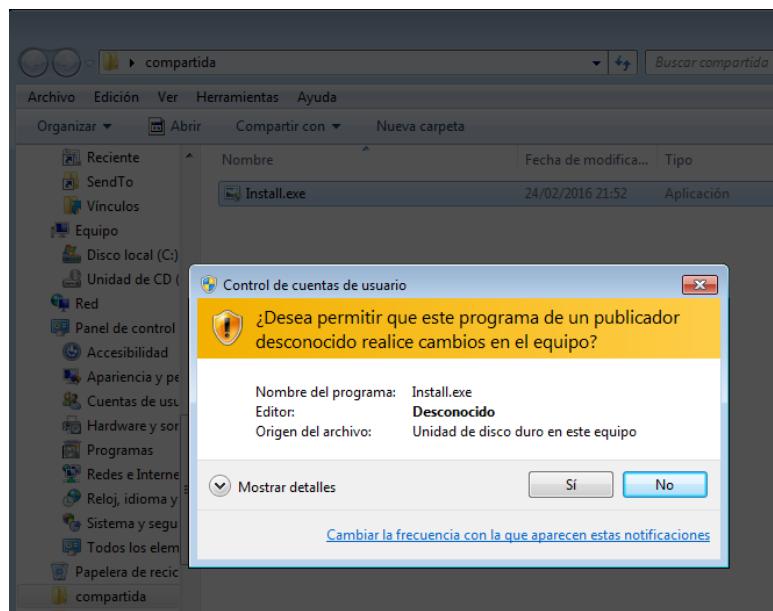
No ultimo paso finalizase o asistente correctamente.



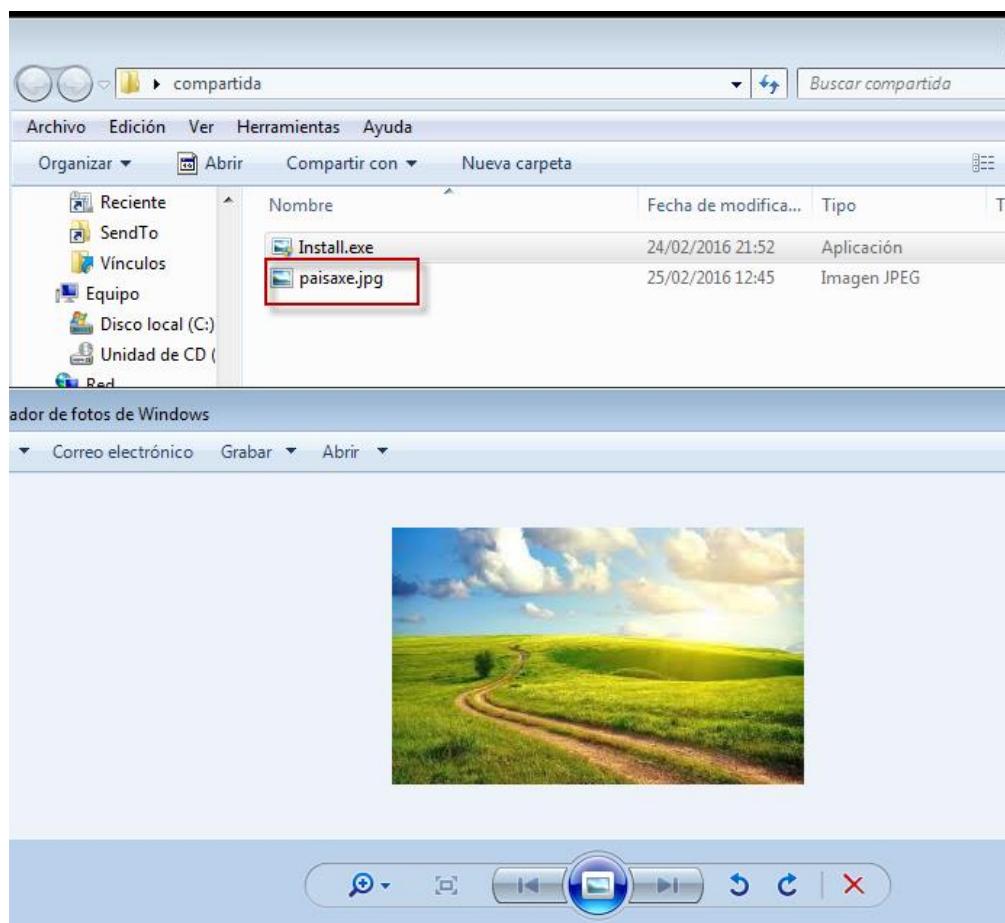
O tratarse de Windows 7 en adiante veremos un “escudo” no ícono, e o escudo de elevación de privilexios (UAC) para poder abrir unha imaxe o cal sería moi sospitoso sin mencionar que si mostramos as extensións de ficheiros veríamos un .exe.



UAC para abrir unha imaxe.

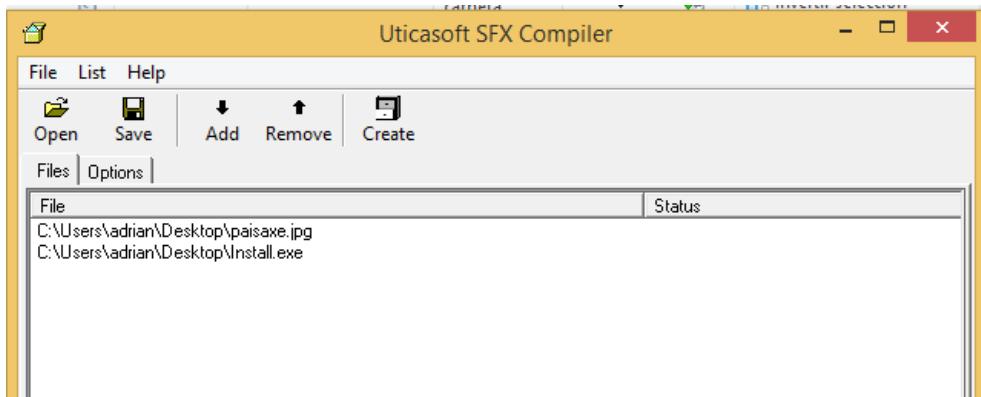


Outra cousa curiosa e que despois de abrir a imaxe unha soa vez (no equipo remoto) esta extraese do ficheiro .exe. O cal e más sospeitoso para o usuario final. Obviamente esto é simple e puramente didáctico para tentar de comprender o funcionamiento de ofuscación dun Keylogger neste caso.

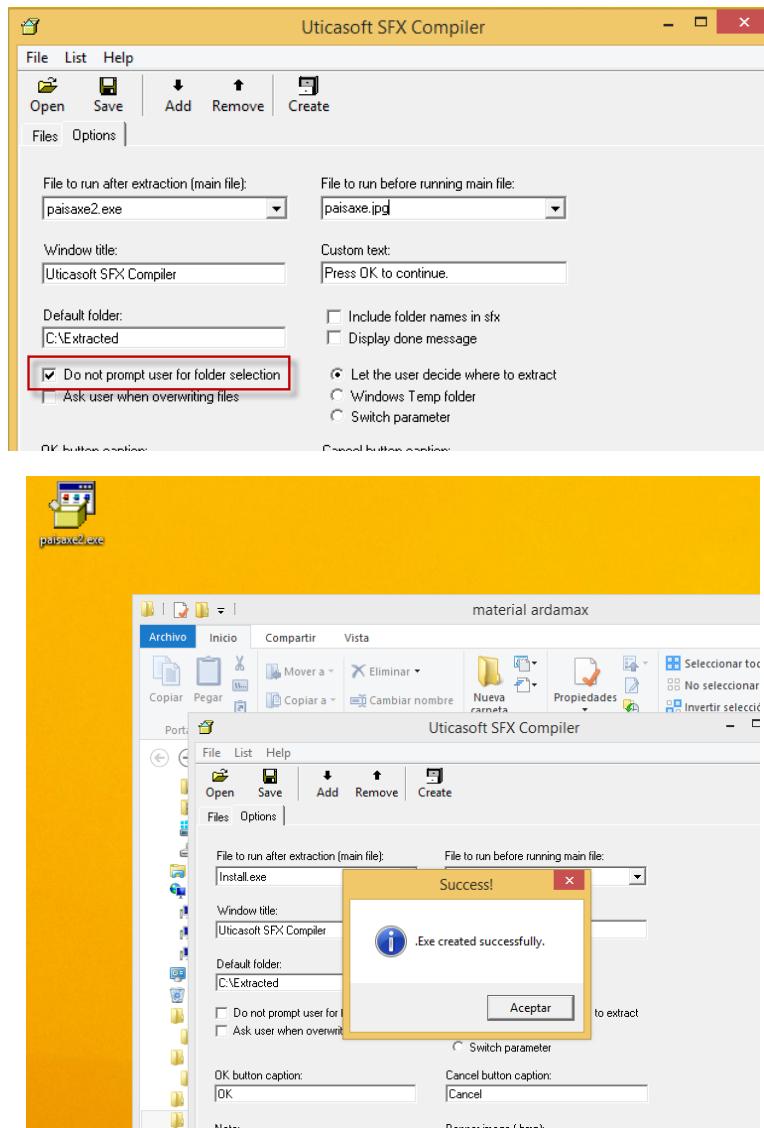


Ainda que o propio Ardamax permíteme enmascarar o seu executable nunha imaxe. Seguindo a práctica veremos como facer esto con SFX Compiler e con Resource Hacker.

Agregamos o binario executable xerado por Ardamax e a imaxe .jpg.

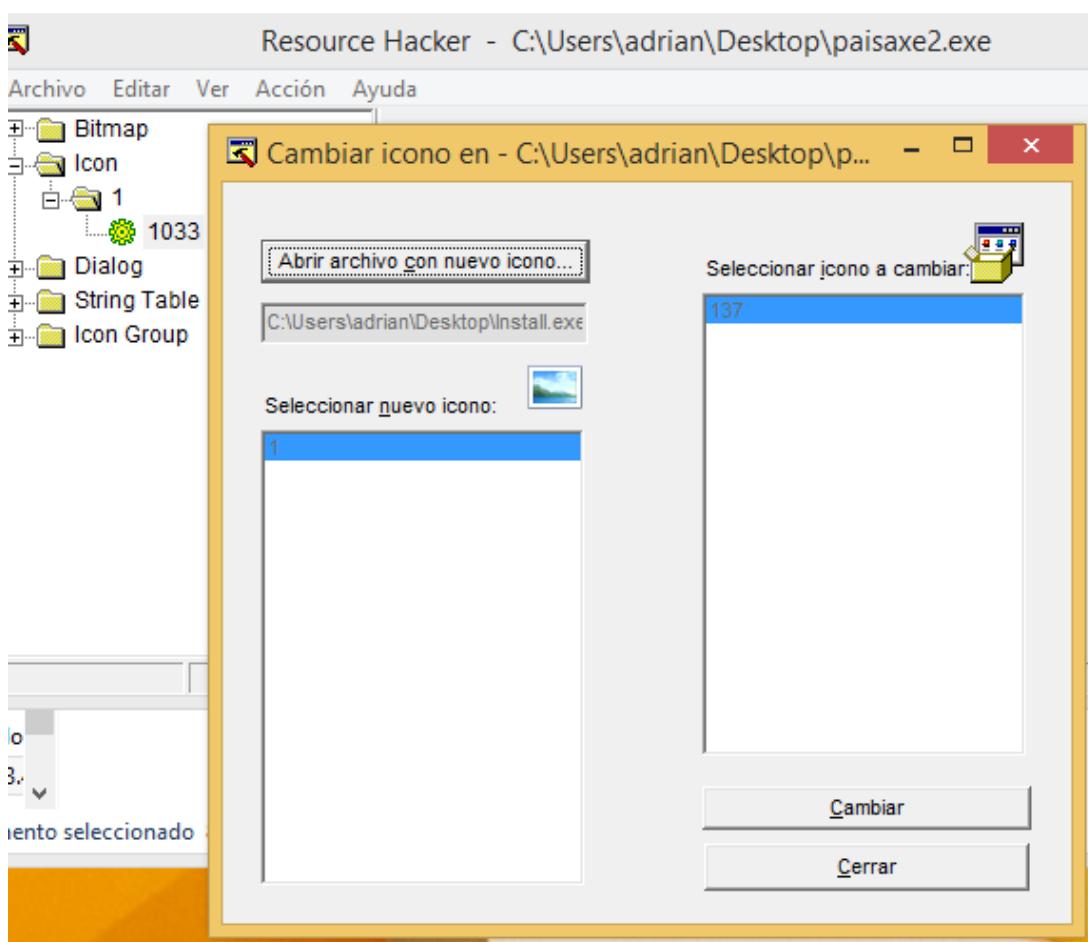
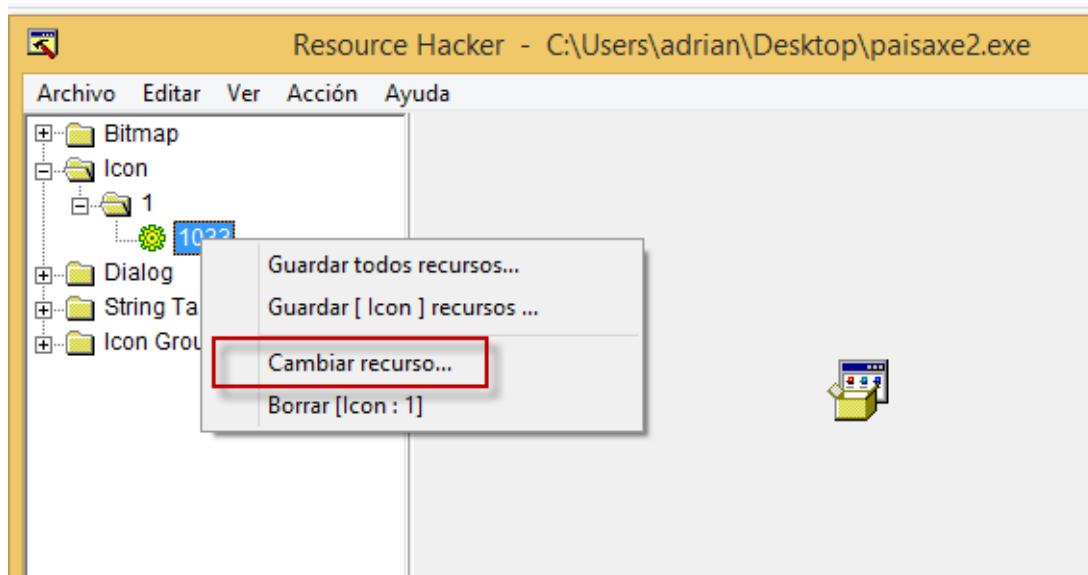


Configurámos o ficheiro executable e o ficheiro que queremos que se mostre de cara o usuario. E procemos a enmascaralo.



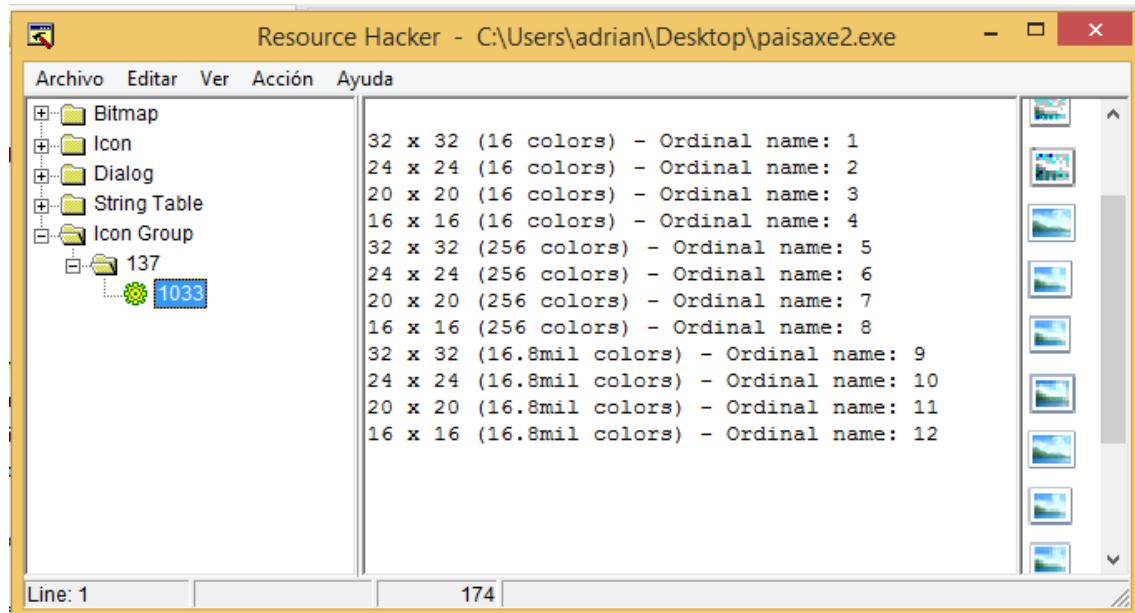
Agora só nos queda cambiar o ícono de por un ícono de imaxe, de maneira que se vexa máis “creible e lexítimo” ao usuario.

Con Resource hacker cambiamos recursos de binarios ou librerías polo que teríamos que encontrar a clave que apunta o ícono e cambialo.



Deixo unha referencia deste aplicativo do meu blog:

<http://www.zonasystem.com/2013/01/editar-ficheros-dll-y-exe-con-resource.html>



Despois de este paréntesis seguimos. Unha vez o usuario execute esa imaxe no seu equipo, según como o configuramos anteriormente Ardamax empezarán a chegar correos dos rexistros do que houberamos configurado que capturase.

Neste exemplo vense os correos e os adxuntos de capturas de pantalla e rexistros de historial, etc.

Búsqueda Imágenes Maps Play YouTube Noticias Gmail Drive Más » Cuenta | Configuración | Ayuda | Cerrar sesión

Gmail™ Buscar mensaje Buscar en la Web Mostrar opciones de búsqueda Create a filtro

Redactar correo Archivar Marcar como spam Eliminar Más acciones... Ir Actualizar 1 - 36 de 36

<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:20
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:19
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:18
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:17
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:16
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:15
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:14
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:12
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:11
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:06
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:05
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:05
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:04
<input type="checkbox"/>	yo	Registros de "adrián" - Encontrará el Registro adjunto a esta carta.	13:03

Recibidos (19) Destacados ★ Enviados Borradores Todos Spam Papelera Contactos Etiquetas Personal Registros Editar etiquetas

Búsqueda Imágenes Maps Play YouTube Noticias Gmail Drive Más »

Gmail by Google Buscar mensaje Buscar en la Web Mostrar opciones de Create un filtro

Redactar correo Recibidos (17) « Volver a Recibidos Archivar Marcar como spam Eliminar Más acciones... ▾

Destacados Envíados Borradores Todos Spam Papelera Contactos Etiquetas Personal Registros Editar etiquetas

Registros de "adrian" Recibidos

Para [REDACTED] @gmail.com > @gmail.com

Responder | Responder a todos | Reenviar | Imprimir | Eliminar | Mostrar original

Encontrará el Registro adjunto a esta carta.

12 archivos adjuntos — Explorar y descargar todos los archivos adjuntos Ver todas las imágenes

Screen_2016-02-25_13-16-14.jpg
106K Ver Explorar y descargar

Screen_2016-02-25_13-16-19.jpg
106K Ver Explorar y descargar

Screen_2016-02-25_13-16-24.jpg
32K Ver Explorar y descargar

Gmail - Registros de "adrian"

https://mail.google.com/mail/u/0/h/f3y4vdwkkkis/?view=att&th=1531857a76a401c8&attid=0.1&disp=in - Windows Internet Explorer

Favoritos Sitios sugeridos Galería de Web Slice

https://mail-attachment.googleusercontent.com/attachment/u/0/?view=att&th=1531857a76a401c8&attid=0.1&disp=in

miércoles, 24 de febrero de 2016 [21:30] URR.exe: Instal %COMMONAPPDATA%

miércoles, 24 de febrero de 2016 [21:47] iexplore.exe: ico Bing images - Internet Explorer

ico de img.jpg

Keys_2016-02-24_21-30-38.html
1K Ver Explorar y descargar

Keys_2016-02-25_12-54-22.html
8K Ver Explorar y descargar

Keys_2016-02-25_12-56-37.html
1K Ver Explorar y descargar

Keys_2016-02-25_12-56-39.html
1K Ver Explorar y descargar

Keys_2016-02-25_12-58-36.html
1K Ver Explorar y descargar

Ainda que esto estaría fora do exercicio e posto que o comprobei non está de más añadilo a este traballo.

Con Wireshark podemos capturar tráficos SMTP e FTP, entre moitos outros.

No caso de que o usuario que de forma non lícita ten o keylogger instalado no seu equipo e sospeite de algo, poderá monitorear o tráfico local da sua rede e ver o seguinte.

Vemos como hay envíos dende o equipo local en momentos concretos de tempo a unha dirección IP externa con unha conexión segura (TLS - Transport Layer Security) conexión usada por protocolo HTTPS(port: 443) e o tráfico é unha petición SMTP. Claramente vemos as peticións mandadas dende unha máquina a un servidor externo de correo, e todo forma non lícita o usuario.

```

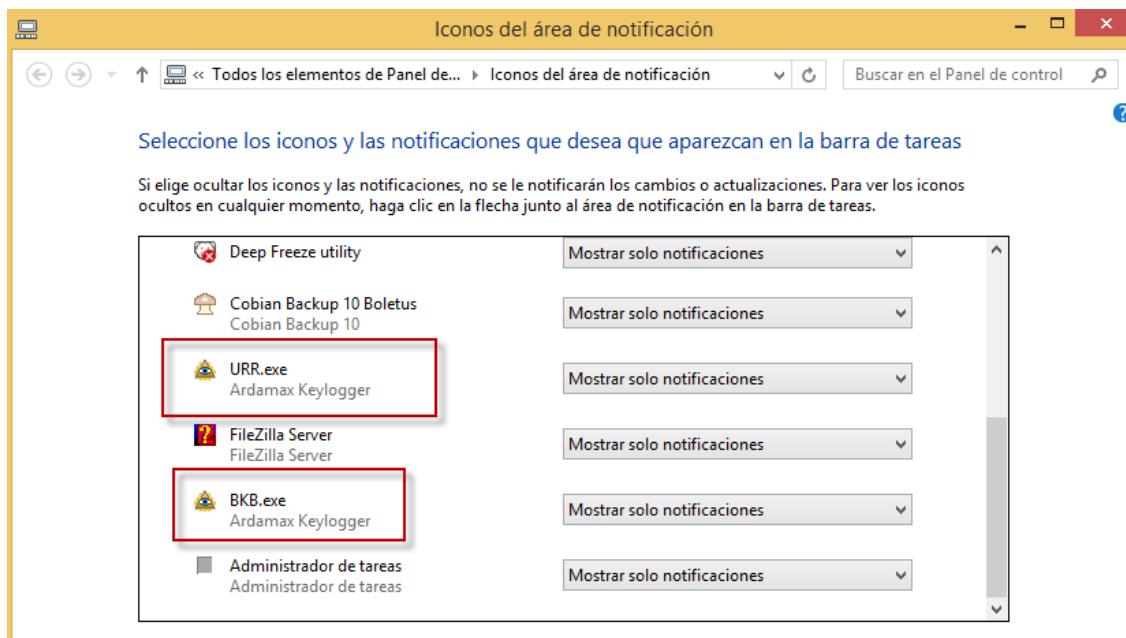
200 1... 74.125.195.16      10.0.2.15          TCP      60 465 → 49591 [ACK] Seq=4456 Ack=340537 Win=65535 Len=0
201 1... 10.0.2.15          74.125.195.16    TLSv1   6928 Application Data, Application Data
202 1... 74.125.195.16      10.0.2.15          TCP      60 465 → 49591 [ACK] Seq=4456 Ack=343457 Win=65535 Len=0
203 1... 74.125.195.16      10.0.2.15          TCP      60 465 → 49591 [ACK] Seq=4456 Ack=346377 Win=65535 Len=0
204 1... 74.125.195.16      10.0.2.15          TCP      60 465 → 49591 [ACK] Seq=4456 Ack=347411 Win=65535 Len=0
205 1... 10.0.2.15          74.125.195.16    TLSv1   6928 Application Data, Application Data
206 1... 74.125.195.16      10.0.2.15          TCP      60 465 → 49591 [ACK] Seq=4456 Ack=350331 Win=65535 Len=0

Length: 32
Encrypted Application Data: a0883777bdef1b300fabe...db1da82489ed45f8560cb3b3d...
TLSv1 Record Layer: Application Data Protocol: smtp
Content Type: Application Data (23)
Version: TLS 1.0 (0x0301)
Length: 6832
Encrypted Application Data: 15b4547461ad83fc...15a461ed6e26ac43d18487f01af2b35...

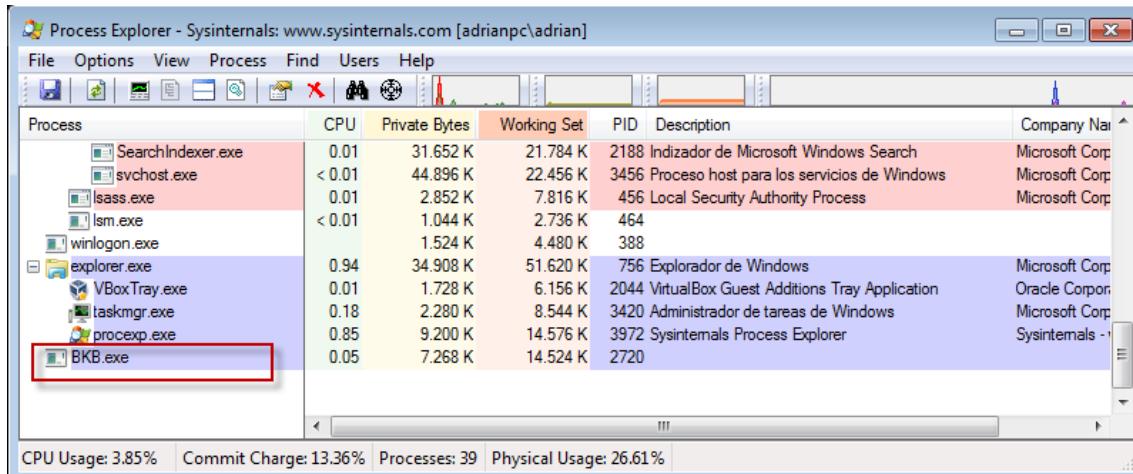
0050 cb 3b 3d cd 4d c2 e0 18  ec 83 52 17 03 01 1a b0 .;=.M.... .R.....
0060 15 b4 54 74 61 ad 83 fc  d1 5a 46 1e d6 e2 6a c4 ..Tta.... .ZF....j.
0070 3d 18 48 7f 01 af 2b 35  c5 33 05 84 c0 8b f6 1d =.H...+5 .3..... .
0080 e8 19 65 a7 72 62 1f 95  42 2f ba 90 9e 6a b5 2f ..e.rb.. B/...j./
0090 b3 9c b1 4d 95 c8 57 13  31 90 51 f0 d3 d0 4c f5 ...M..N. 1.0...1


```

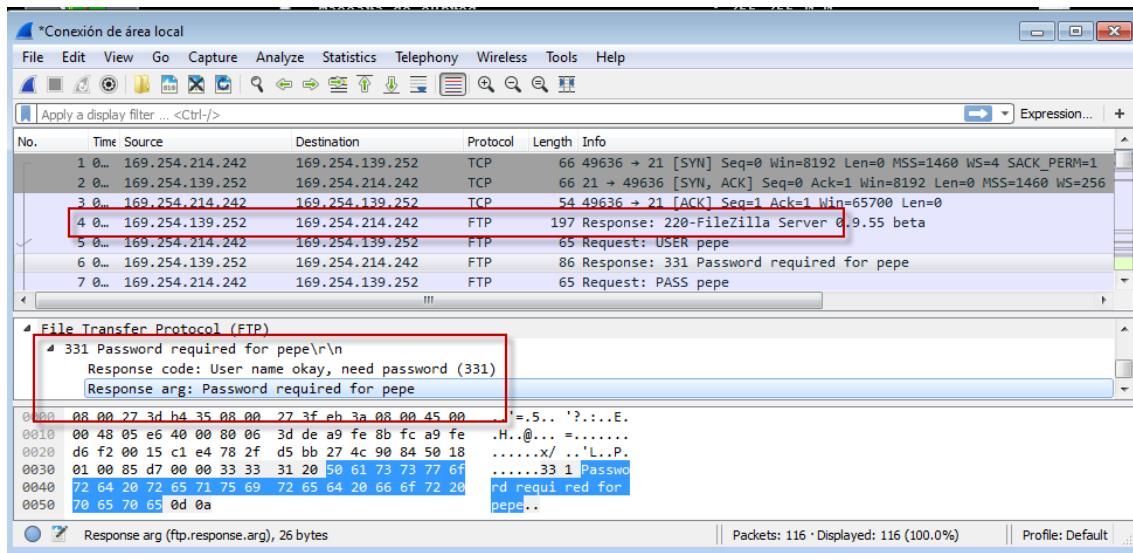
Outro detalle sería mirar a área de notificacións, ainda que se oculta, si entramos un pouco máis en detalle vemos esto.



Con velo na área de notificacións vemos que está instalado un Keylogger no equipo pero si temos a duda de si se está executando. Pois efectivamente con Process Explorer podemos ver que os ficheiros de execución coinciden e se están executando.



Por último comentar que tamen se fixo monitoreo do tráfico de FTP, no que se puideron capturar o usuario e o contrasinal do usuario FTP, así como tamen saber que na máquina local mandábanse peticións cada certo tempo a este servidor de forma non lexítima.



Outros Keylogger gratuitos:

Keylogger Free

<http://www.key-logger-free.com>

Kmint Keylogger

<http://www.kmint21.com/keylogger>

Refog free keylogger

<https://es.refog.com/free-keylogger>

Danusoft Free Keylogger

<http://www.filesriver.com/app/275/danusoft-free-keylogger>

Real Free Keylogger

<http://www.filesriver.com/app/274/real-free-keylogger>

Revealer Keylogger free

<http://www.logixoft.com/es-es/index>

Outros Keyloggers de pago e más sofisticados:

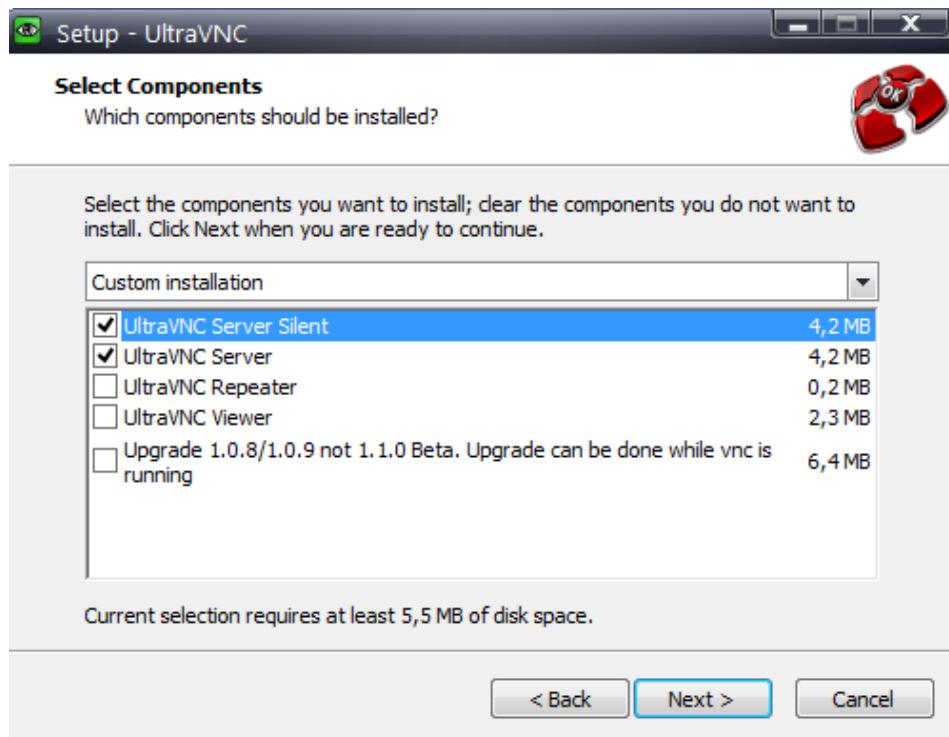
2016 Best Keyloggers & Monitoring Software Review

Ranking	TOP	2	3	4	5	6	7	8	9	10
										
	Spytech SpyAgent	All In One Keylogger	Ardamax Keylogger	PC Pandora	Elite Keylogger	Actual Keylogger	Refog Personal Monitor	Micro Keylogger	WebWatcher	Refog Free Keylogger
	Review ↗	Review ↗	Review ↗	Review ↗	Review ↗					
	Download	Download	Download	Download	Download					
	\$69.95	\$69.95	\$48.97	\$69.95	\$79	\$59.95	\$69.95	\$79.95	\$99.95	Free

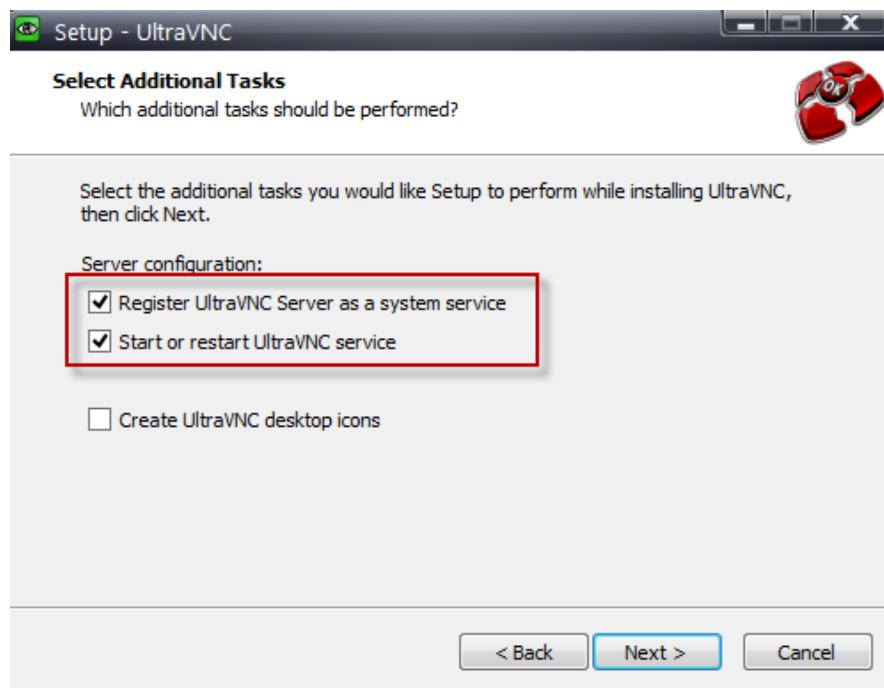
3. Software de xestión remota

Instalaremos un aplicativo que funciona baixo unha arquitectura cliente-servidor basado nas conexións VNC (Virtual Network Computing).

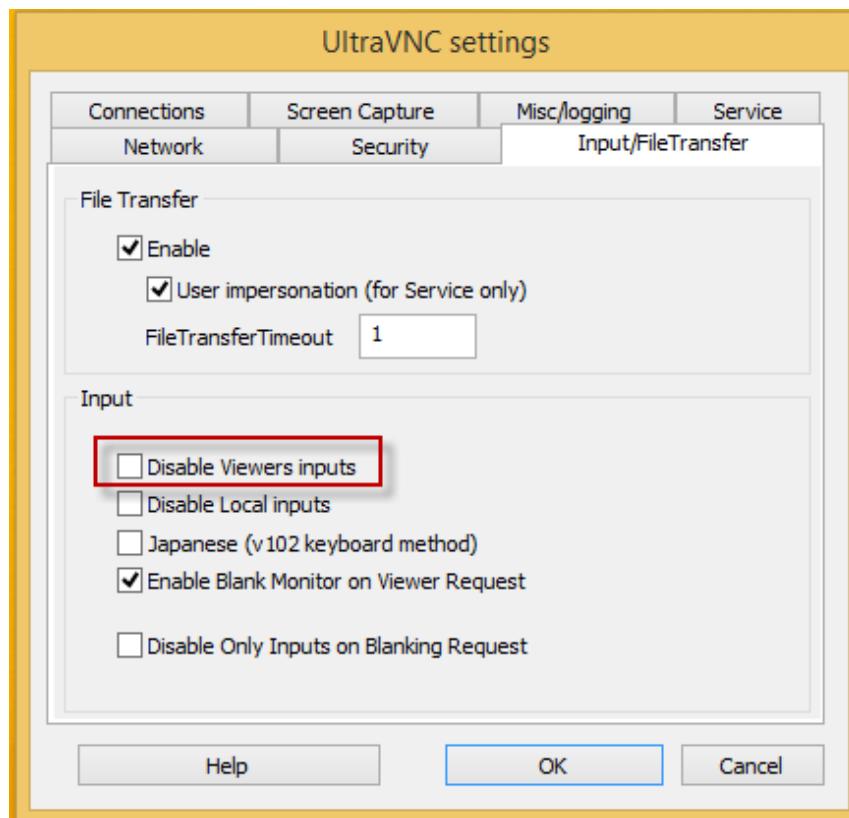
Neste caso instalaremos UltraVNC server en modo silent (de forma que sileciosa de modo que ó usuario non se percaate).



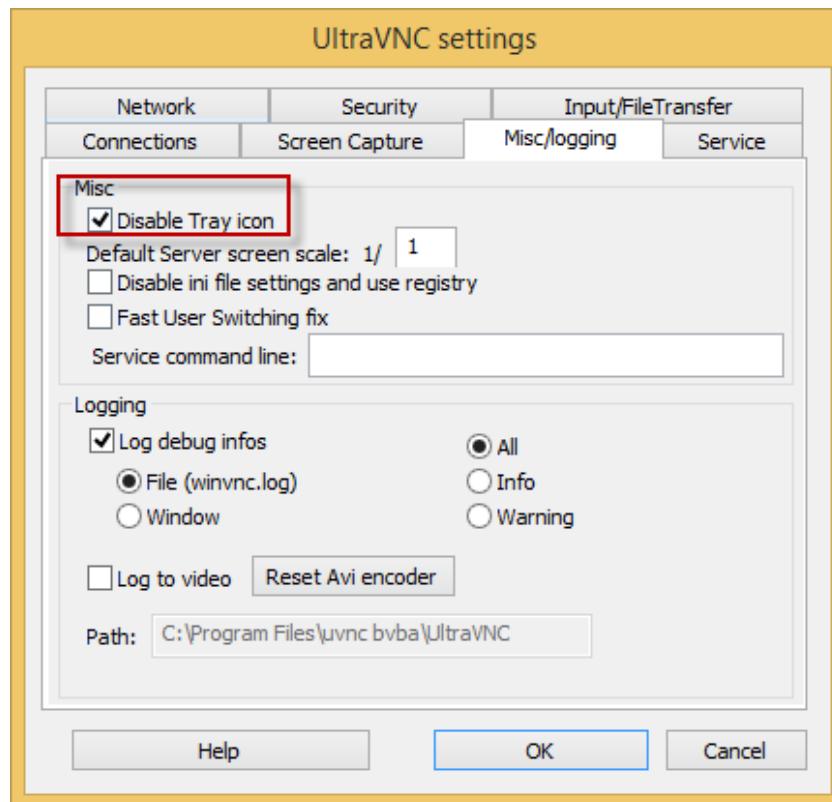
Rexistramos UltraVNC como un servizo do Sistema.



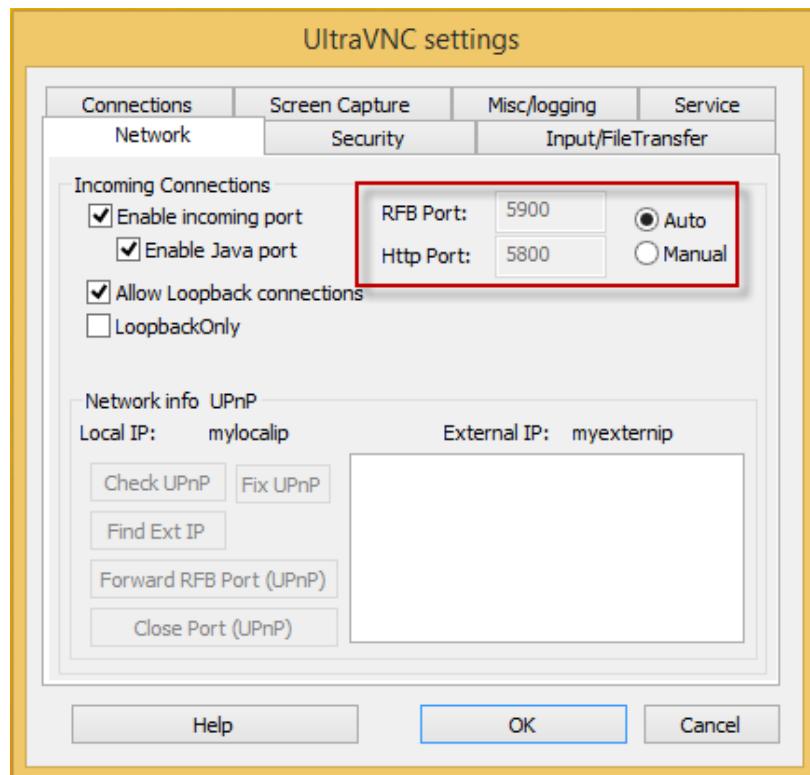
Na configuración de UltraVNC desabilitamos as notificacións de conexión, de modo que usuario non vexa si nos estamos conectando ou non.



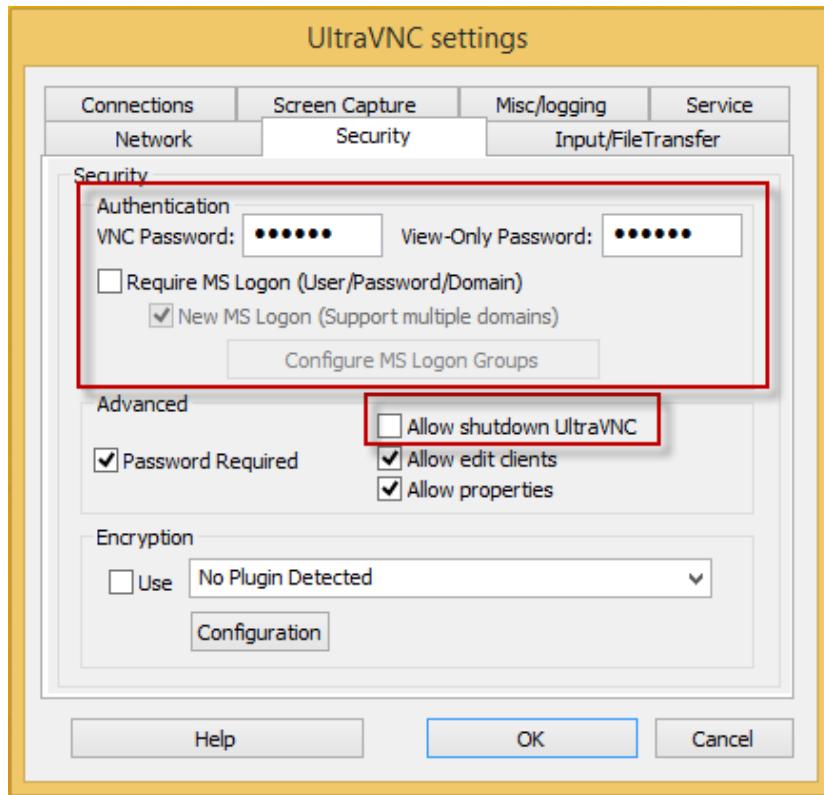
E desactivamos o ícono da barra de tarefas de Windows.



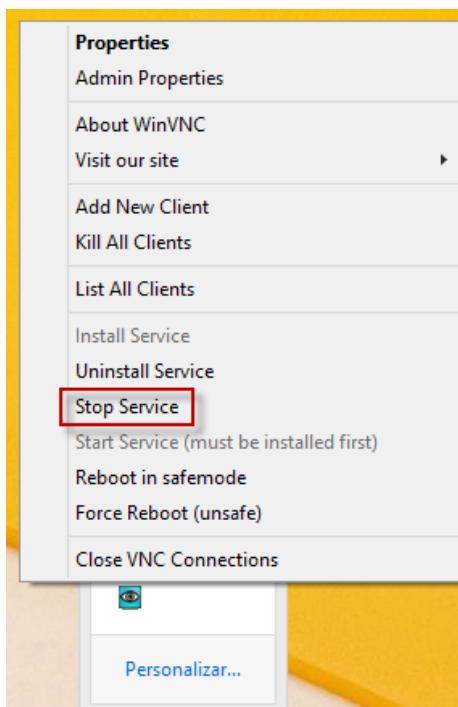
Fixarémonos que podemos especificar puertos de forma manual tanto para conexions locais a través dun viewer vnc ou por conexión HTTP con plugin de Java a través do navegador web (como veremos más adiante).



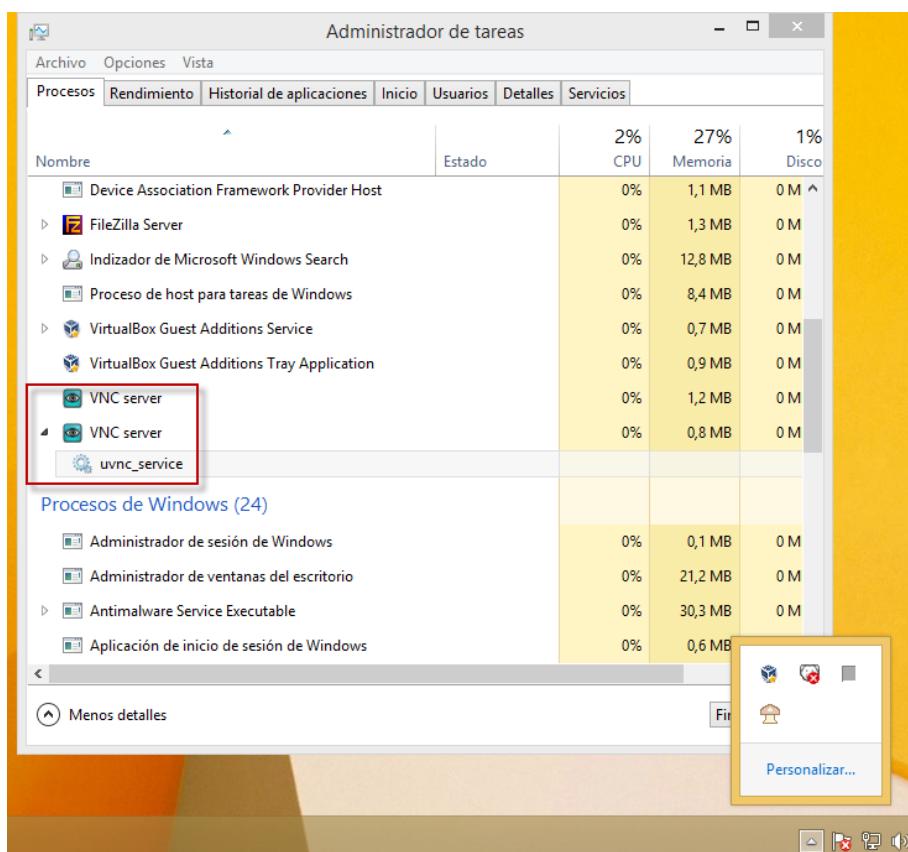
Establecemos unha password e desabilitamos que os usuarios clients que teñen instalado o servidor non poidan desactivar o UltraVNC.



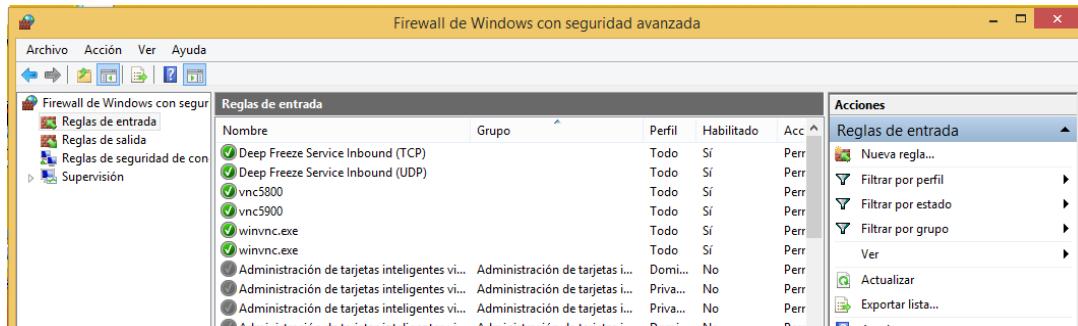
Para aplicar os cambios teremos que reiniciar o servizo de UltraVNC.



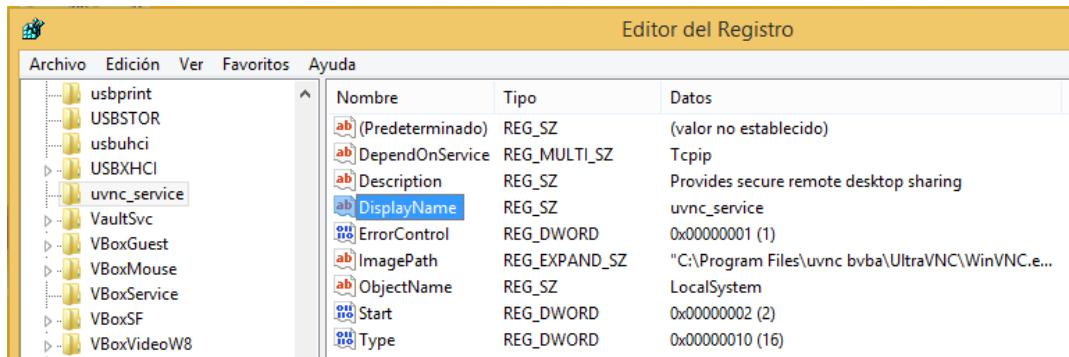
Ainda que se oculte, se o usuario e un pouco hábil podere ver no administrador de tarefas de Windows como hay un proceso VNC_server que depende dun servizo.



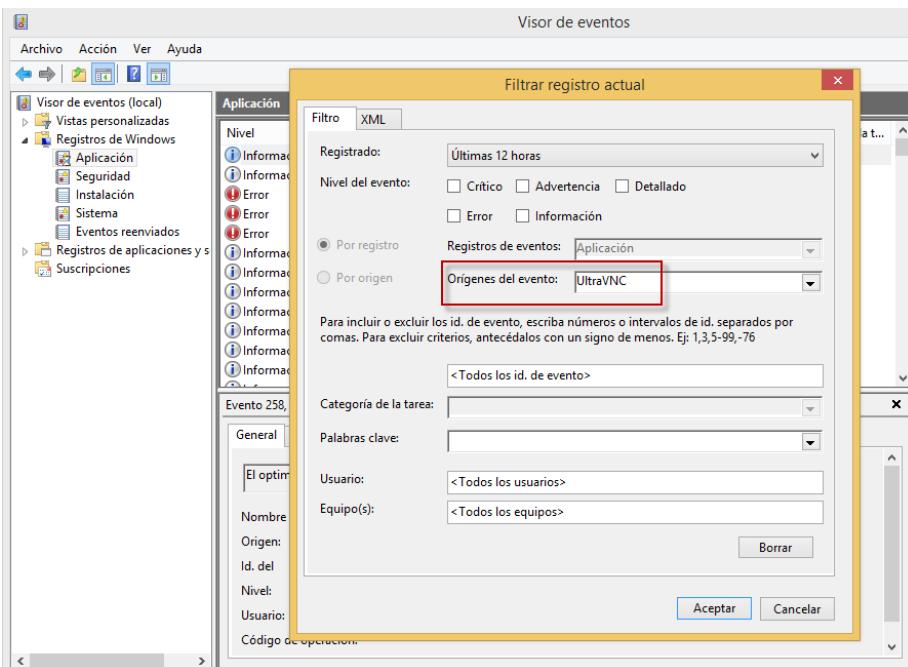
Ainda que por defecto UltraVNC xa preconfigure o firewall de Windows, e abre os puestos por defecto necesarios para el (RFB: 5900 e HTTP: 5800) podemos igualmente crear novas excepcións para poder especificar os novos portos establecidos de forma manual, se fose o caso.



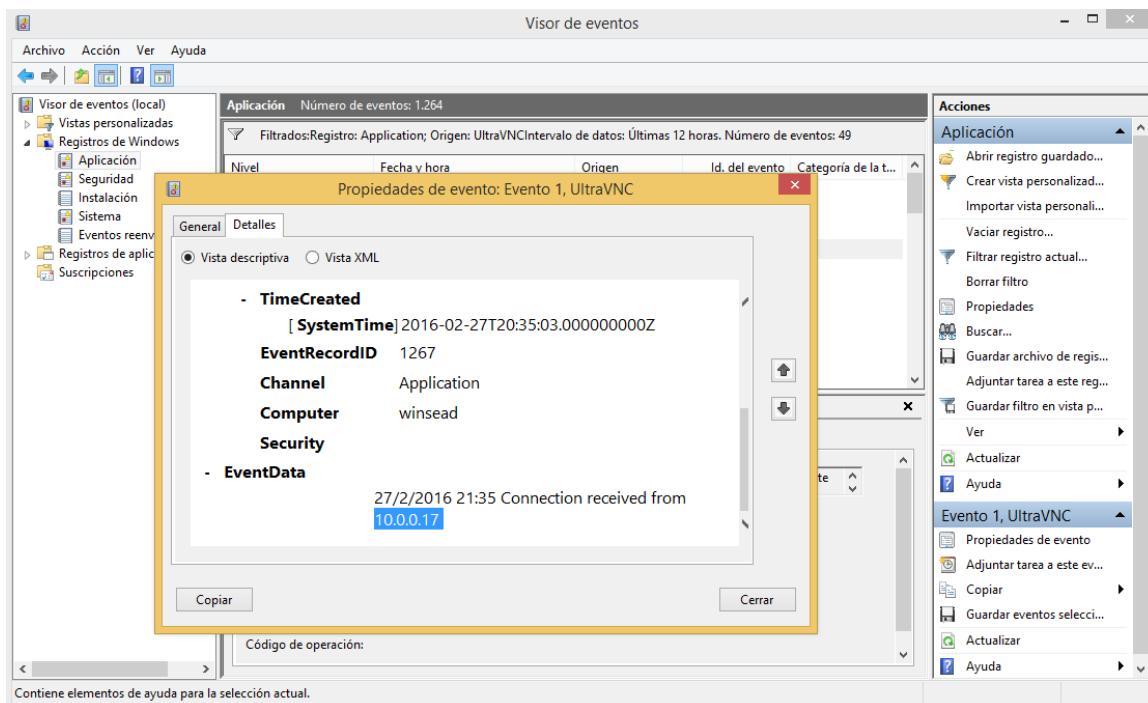
Saber tamén que todo aplicativo que se instala no sistema ten a sua ruta de configuración do rexistro, e que poderíamos incluso cambiar certos parámetros para poder ofuscalo ainda un pouco máis, por exemplo neste caso, o nome do servizo.



Saber tamen que toda aplicación instalada no sistema e que teña conexións e auditada por defecto, polo que podemos ter control de que se conecta a cuando ao noso equipo.

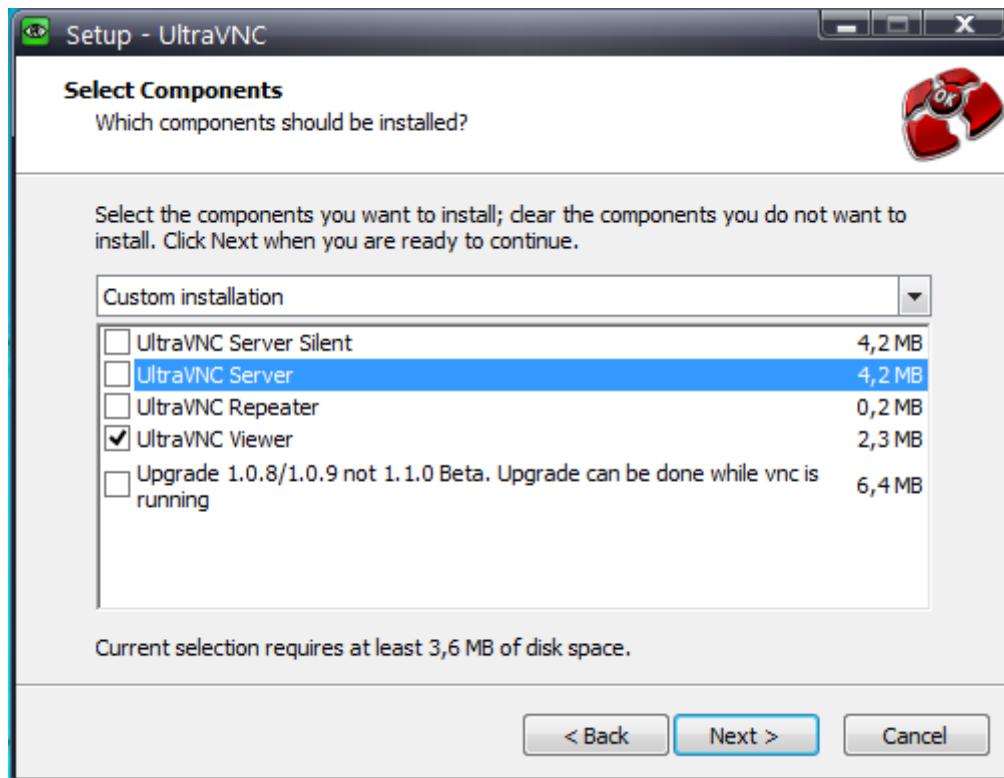


Cemos que unha dirección 10.0.0.17 conectouse a fecha e hora que se mostra na captura.

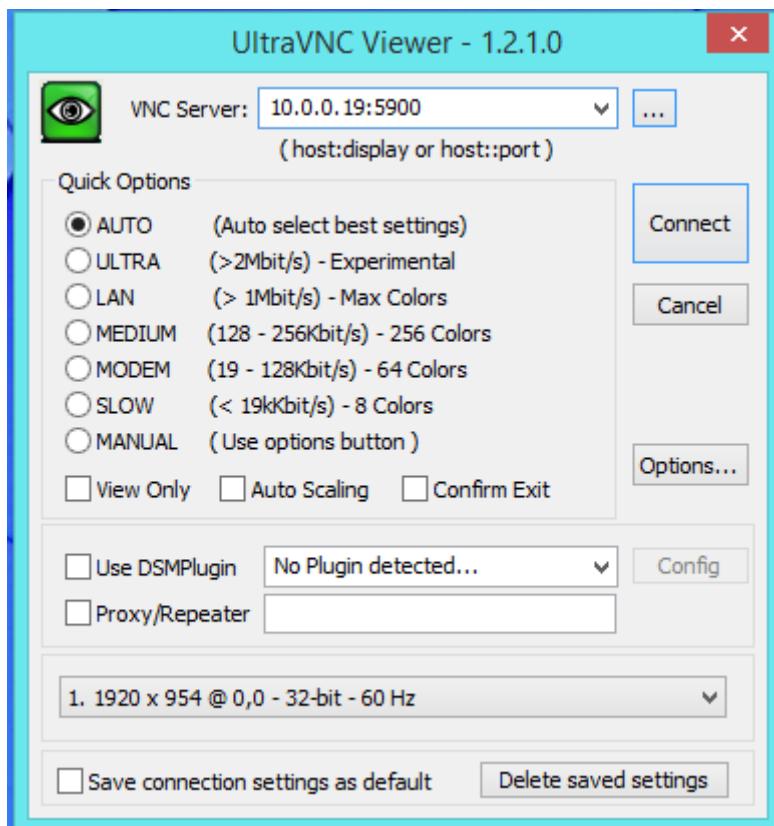


Agora instalaremos o UltraVNC Viewer, o aplicativo polo cal nos conectaremos o servidor.

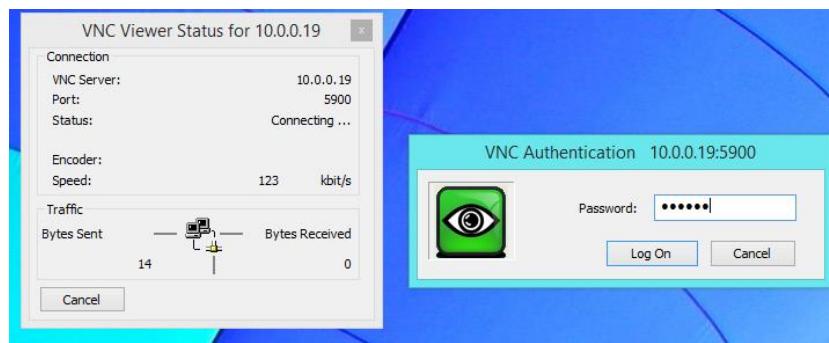
Instalamos o complement Viewer.



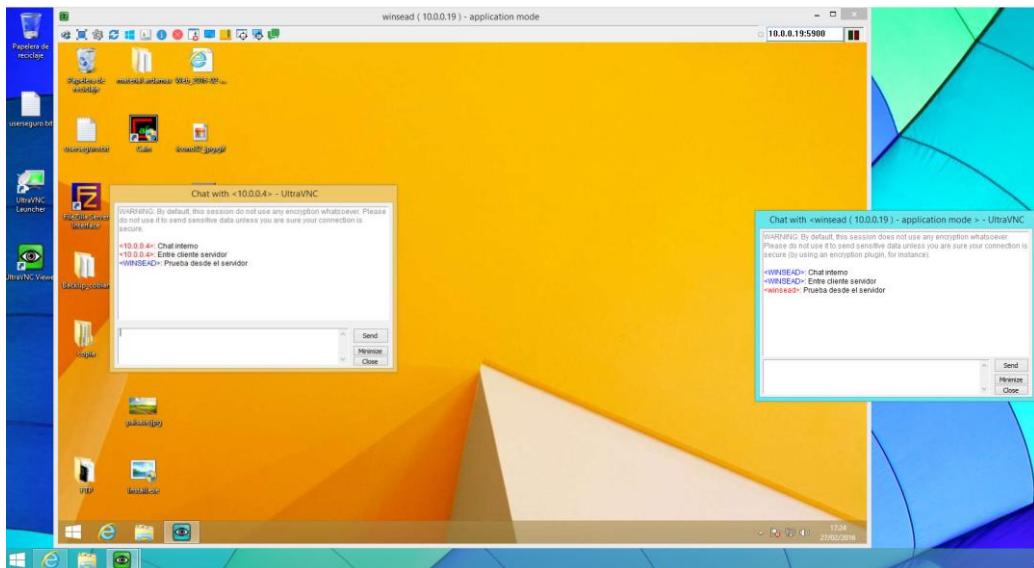
E simplemente poñendo a dirección IP ou nome de equipo remoto sería suficiente, neste caso especifiquei o porto, ainda que se si usan os portos por defecto no sería necesario especificalo.



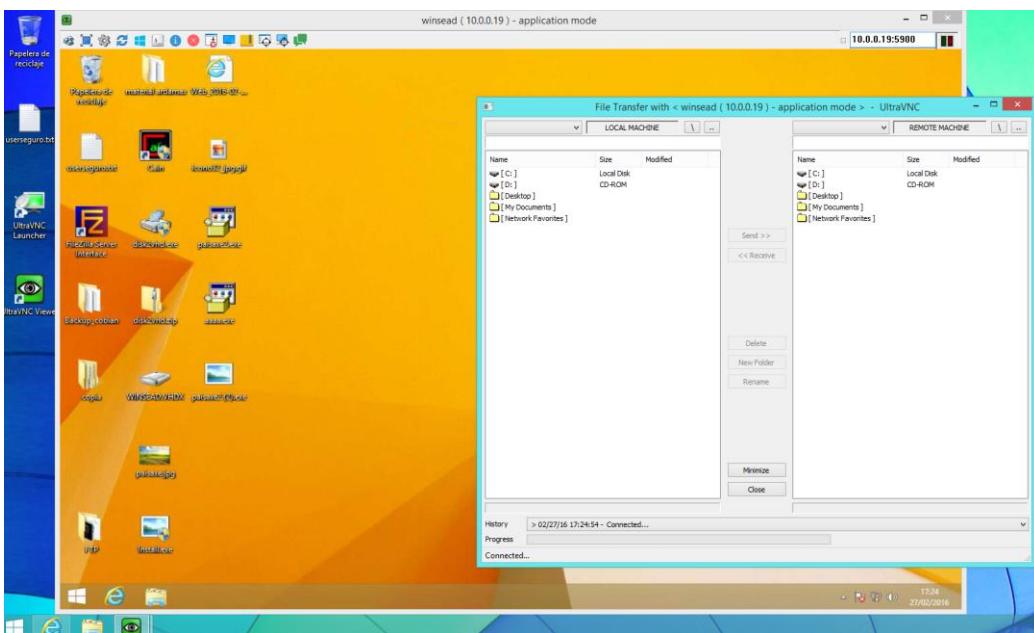
Pediranos a contrasinal que establecésemos.



E teremos conexión por VNC co outro equipo remoto, como vemos dentro do aplicativo do visor temos algunas funcionalidades, como son un chat interno entre o cliente e o servidor. Para poder escribirse co usuario no caso de ser un soporte técnico.

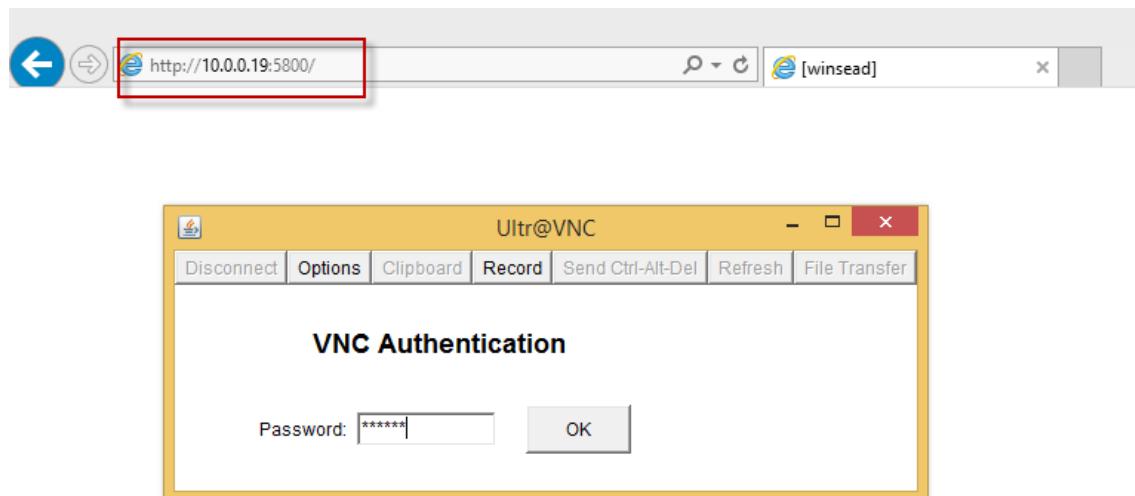


Así tamen como transferir archivos entre os equipos cliente-servidor.

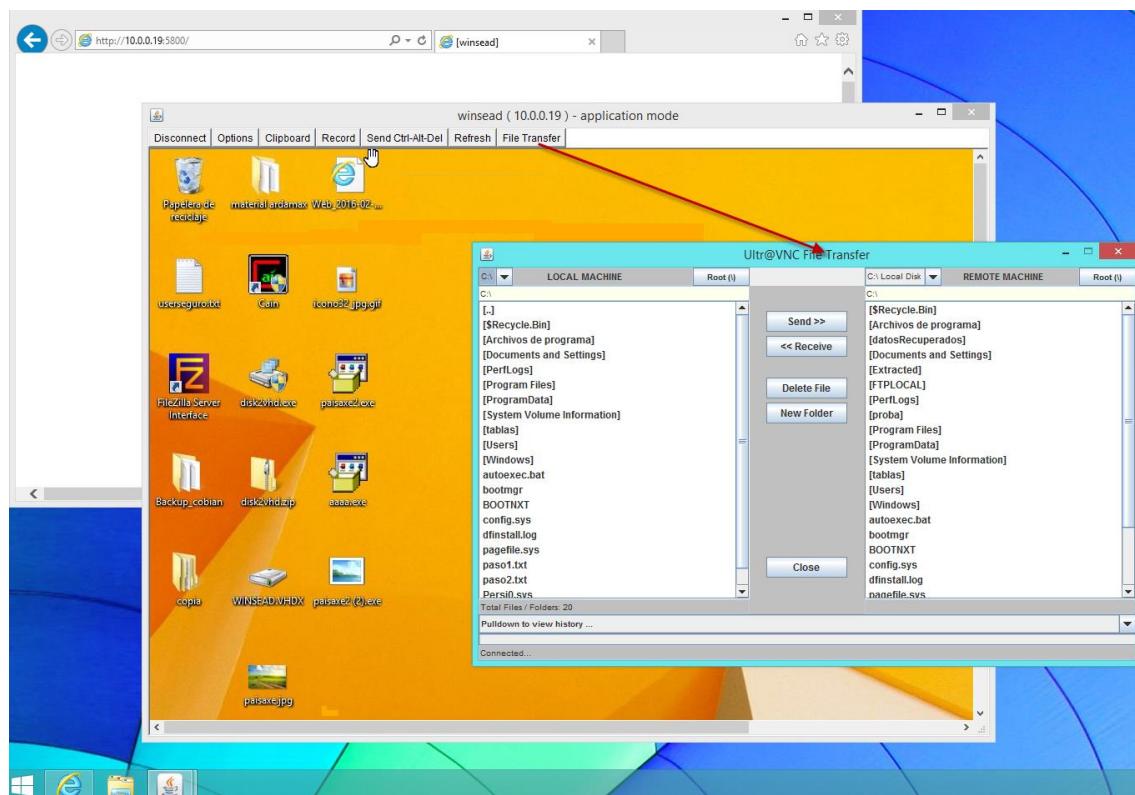


Outra forma de acceder sería co plugin de Java como complemento do navegador web. E acceder mediante HTTP polo porto 5800 (por defecto).

Pedirános autenticación establecida anteriormente no servidor.



De igual modo podemos transferir ficheiros.



A modo detalle, poderáse ver os portos de escoita do VNC.

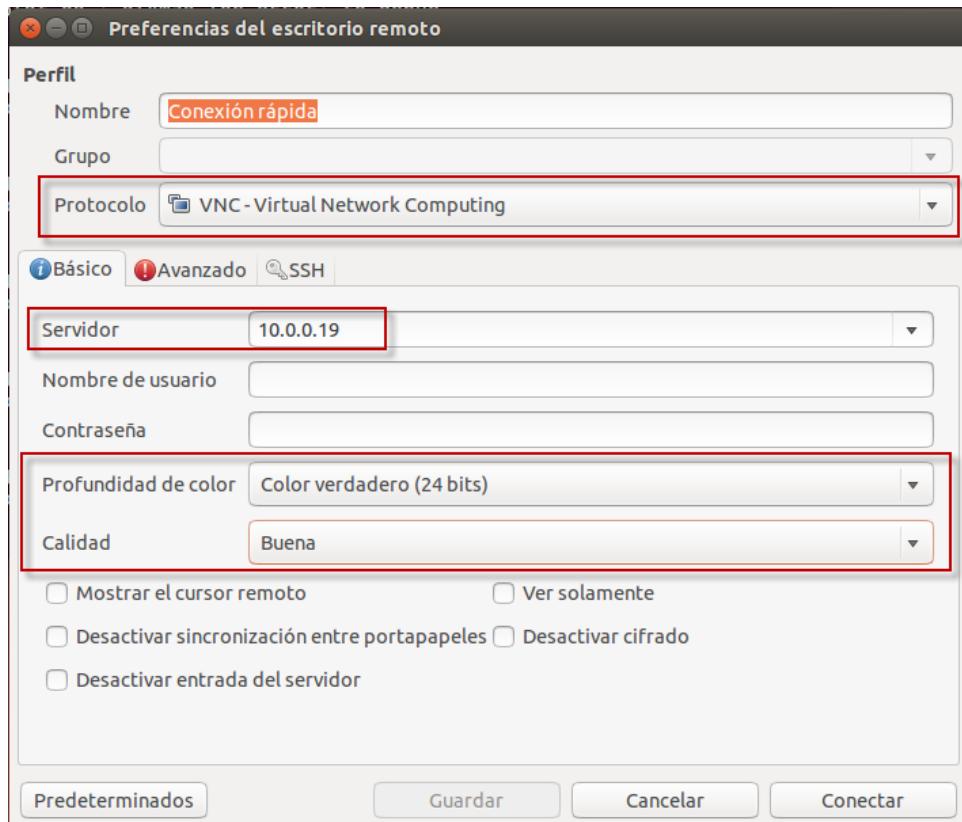
```
C:\Windows\system32>netstat -a -b
Conexiones activas

Proto Dirección local      Dirección remota        Estado
TCP   0.0.0.0:21           winsead:0             LISTENING
[FileZilla Server.exe]     TCP   0.0.0.0:135          winsead:0             LISTENING
RpcSs [svchost.exe]
TCP   0.0.0.0:445          winsead:0             LISTENING
No se puede obtener información de propiedad
TCP   0.0.0.0:2869          winsead:0             LISTENING
No se puede obtener información de propiedad
TCP   0.0.0.0:3389          winsead:0             LISTENING
CryptSvc [svchost.exe]
TCP   0.0.0.0:5357          winsead:0             LISTENING
No se puede obtener información de propiedad
TCP   0.0.0.0:5800          winsead:0             LISTENING
[WinUNC.exe]    TCP   0.0.0.0:5900          winsead:0             LISTENING
[WinUNC.exe]    TCP   0.0.0.0:49152         winsead:0             LISTENING
[wininit.exe]   TCP   0.0.0.0:49153         winsead:0             LISTENING
EventLog
```

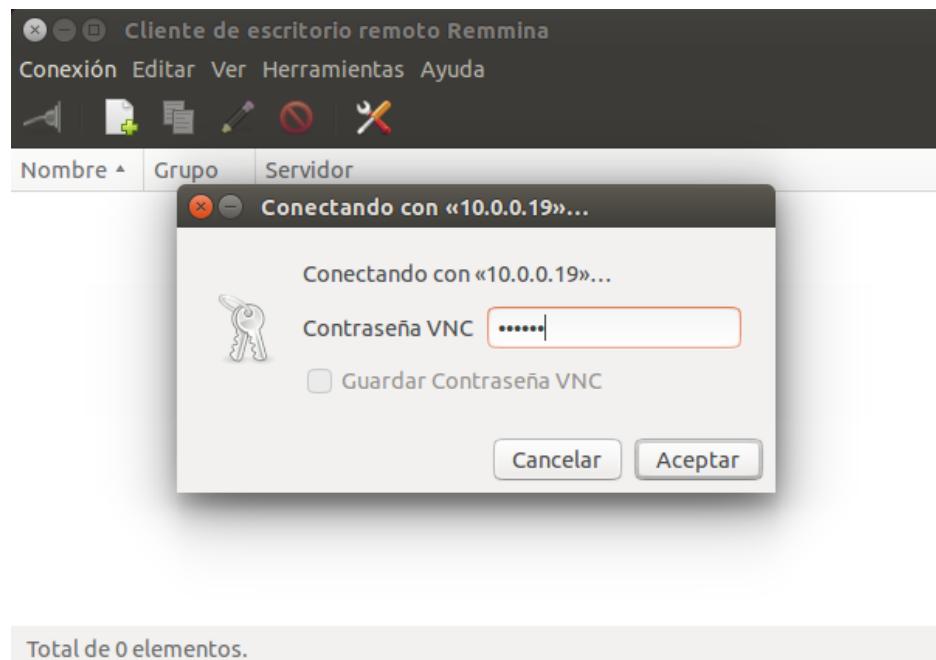
Esto todo en Windows, pero no caso de un sistema Linux sería similar xa que VNC e digamos un estándar universal que pode funcionar en calquera contorna.

Conexión dende un Ubuntu a servidor Windows. Podemos facer uso do aplicativo por defecto que este incorpora instalado como e: Remmina.

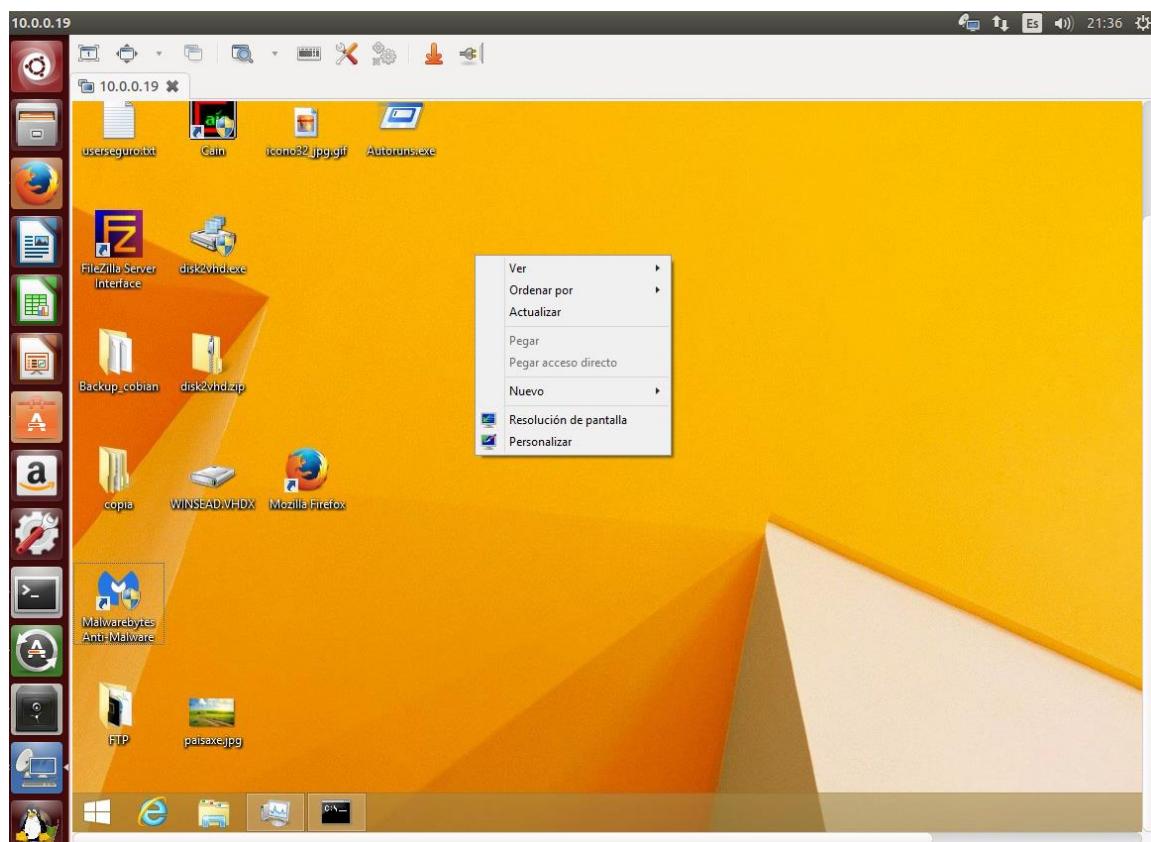
E IMPORTANTE que a configuración de profundidade de cor esté a un cor verdadeiro de 24bits.



Pediranos autenticación establecida no servidor VNC de Windows.



Conexión establecida dende un Ubuntu con Remmina como visor a un servidor VNC de Windows.



Faremos o mesmo co plugin de Java para Firefox sobre Ubuntu, de modo que non teremos que facer uso de ningún visor externo, simplemente co navegador e un plugin poderemos establecer a conexión o equipo remoto.

Neste punto tiven certas dificultades a hora de instalar dito plugin no navegador polo que deixarei a sentencia de comandos empregada.

Instalación de Java (JRE) e plugin do navegador web en Firefox.

Añadimos os repositorios de Java:

```
sudo add-apt-repository ppa:webupd8team/java
```

Actualizamos os repositorios:

```
sudo apt-get update
```

Instalamos a Versión 8 de Java:

```
sudo apt-get install oracle-java8-installer
```

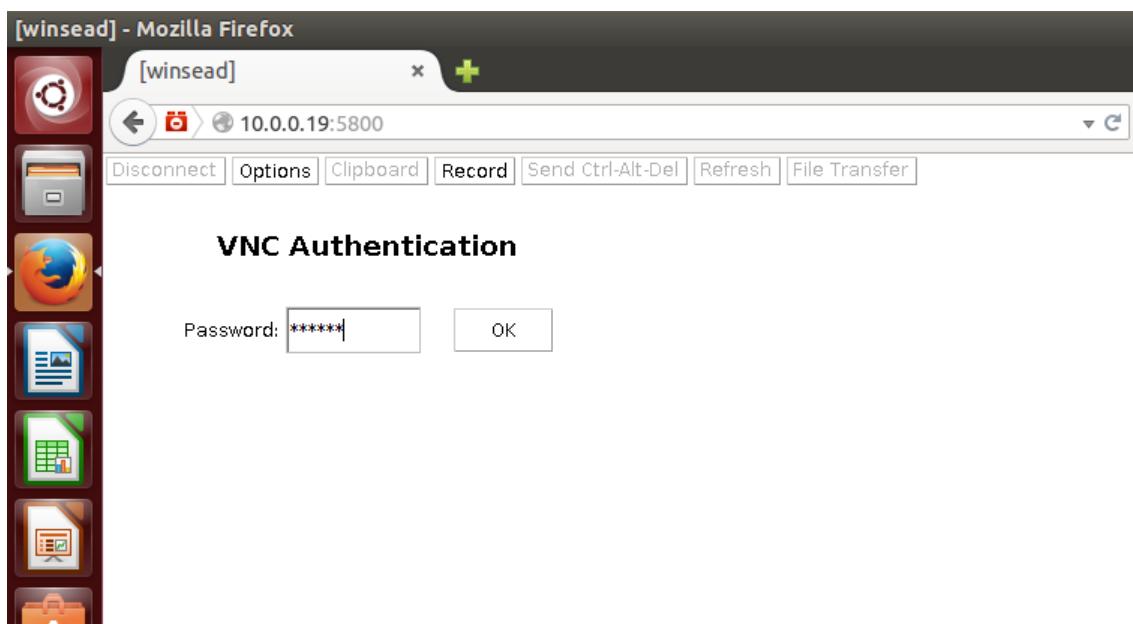
Creamos o directorio de plugins:

```
mkdir -p ./mozilla/plugins
```

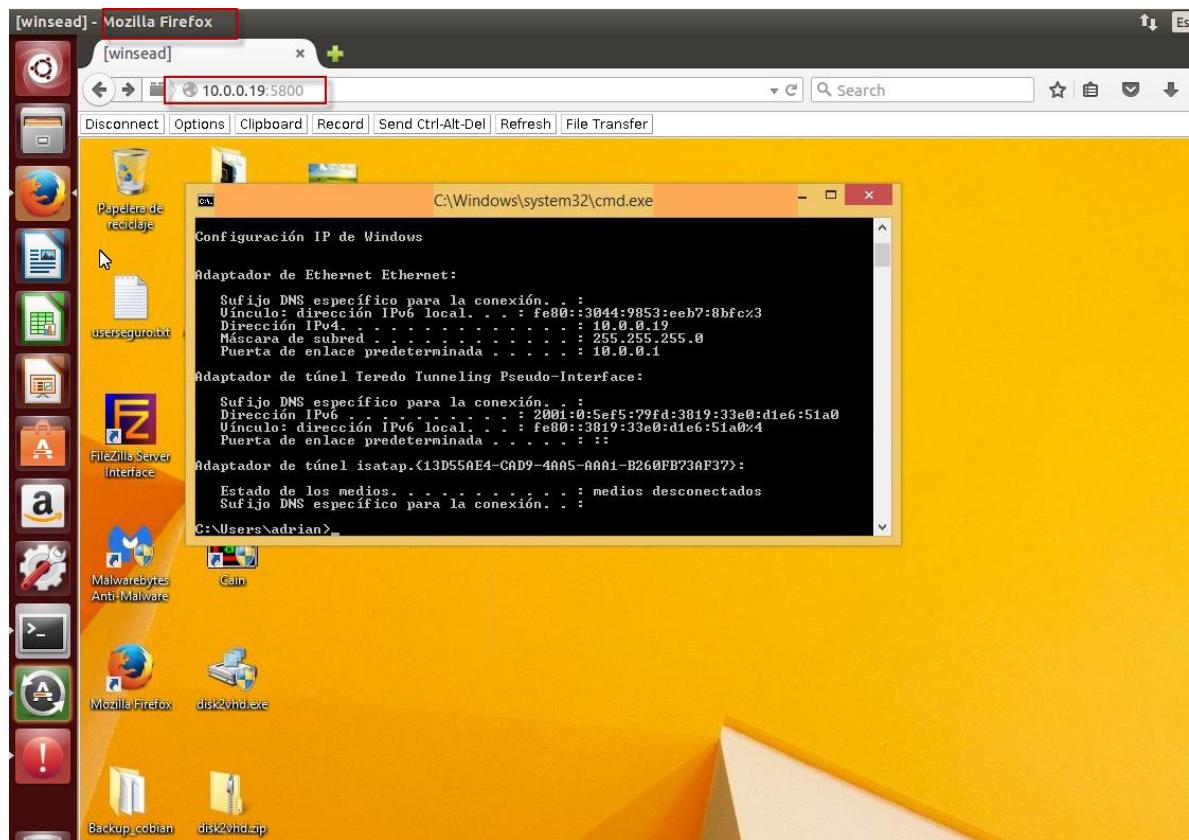
Creamos un enlace simbólico no directorio de Firefox:

```
ln -s /usr/lib/jvm/jre1.7.0/lib/i386/libnpjp2.so ./mozilla/plugins
```

Pediranos autenticación para a conexión.

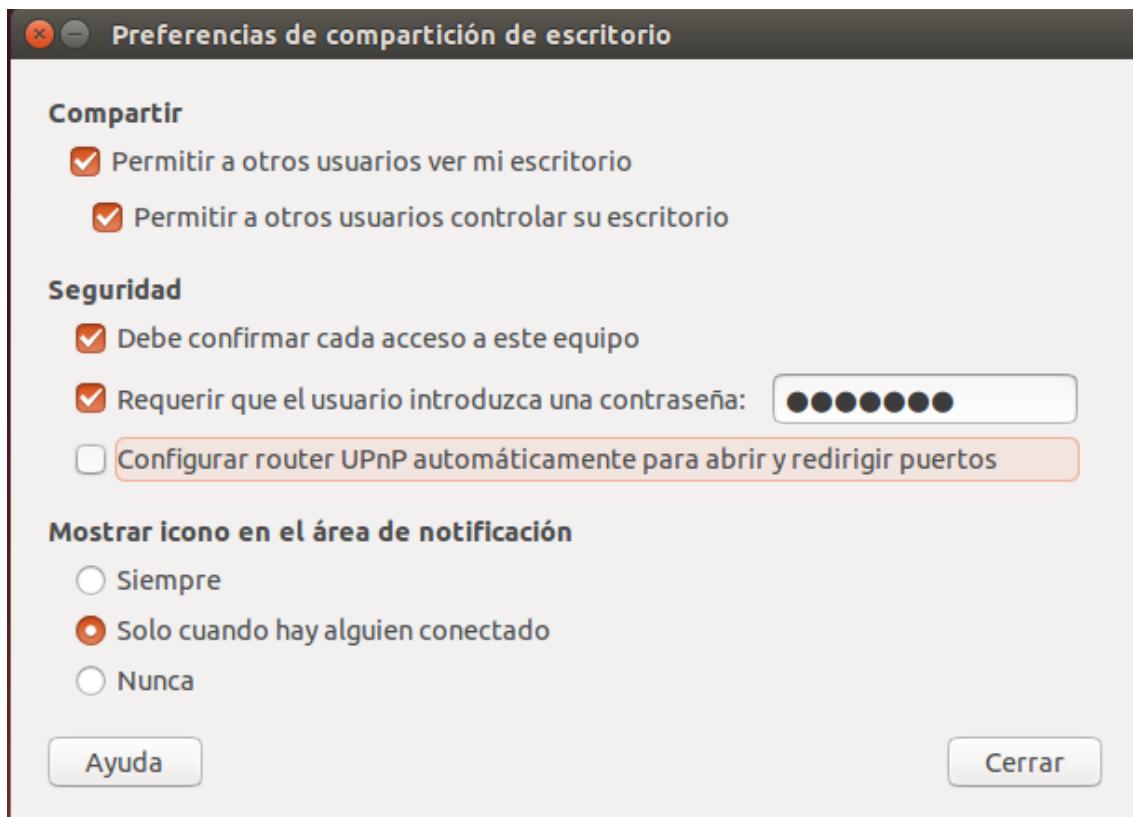


Conexión establecida desde un Ubuntu a un Windows mediante o plugin de Java a través del navegador Web.



Agora probaremos a poñer como **servidor VNC a un Sistema Linux**, concretamente un Ubuntu.

Este por defecto, disón dunha función de compartición de escritorio, a cal e moi sinxela de configurar como se pod ever na seguinte captura.



Temos a opción de instalar TightVNC (similar a UltraVNC) para Ubuntu si o quixeramos facer por terminal.

Instalación do VNC Server:

```
apt-get install tightvncserver
```

Creación de un servidor gráfico:

```
tightvncserver :1 -geometry 800x600 -depth 24
```

Destrucción de un servidor gráfico VNC:

```
tightvncserver -kill :1
```

No caso de ter un cliente de visualización para outro Ubuntu:

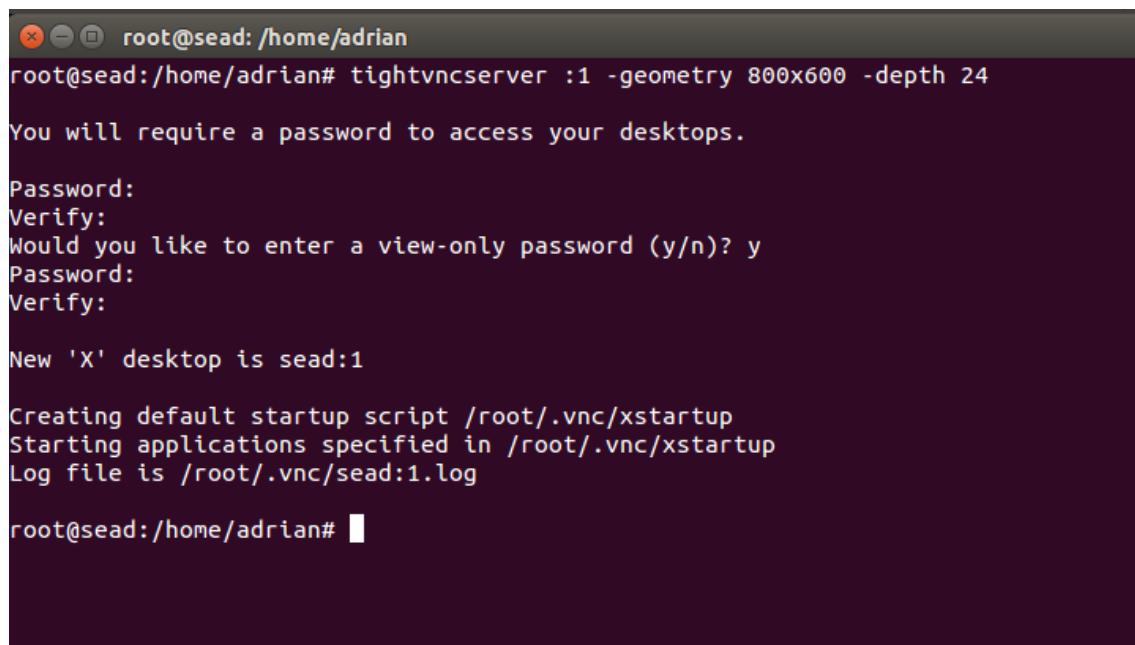
Instalación del cliente VNC:

```
apt-get install xtightvncviewer
```

No caso que queremos habilitar a función de servidor de conexión para aceptar peticions polo 5800 a través de HTTP:

Instalación do tightvnc-java:

```
apt-get install tightvnc-java
```



```

root@sead:/home/adrian# tightvncserver :1 -geometry 800x600 -depth 24
You will require a password to access your desktops.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:

New 'X' desktop is sead:1

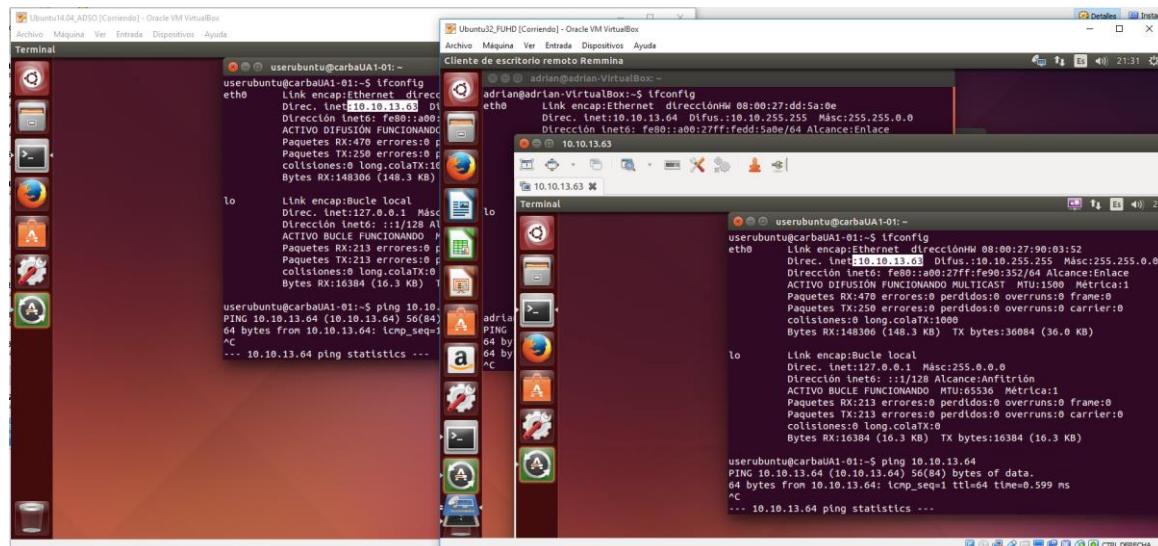
Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/sead:1.log

root@sead:/home/adrian#

```

Conexión entre dous Ubuntu a través de Remina e de compartición de escritorio por parte do Ubuntu servidor VNC.

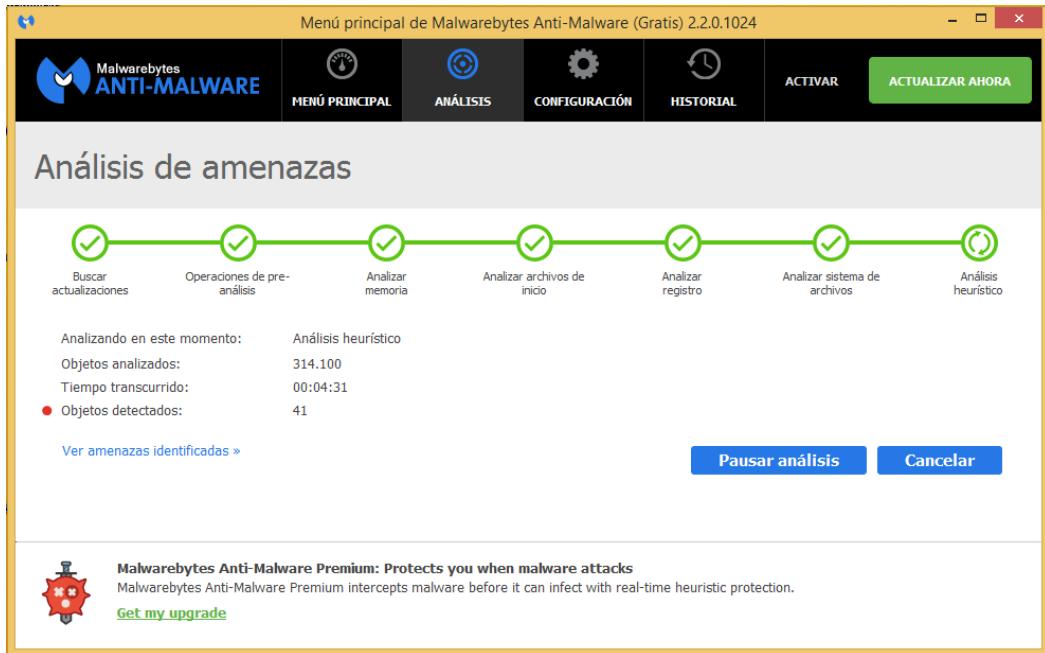
Nota: Pode observarse un cambio de IPs dende un punto a outro desde exercicio, debido os cambios de redes (en clases e particular) nas máquinas virtuais.



4. Software antimalware

Existen multitude de software antimalware, pero entre os máis populares e gratuitos (en certas funcionalidades básicas) e Malwarebytes Anti-Malware.

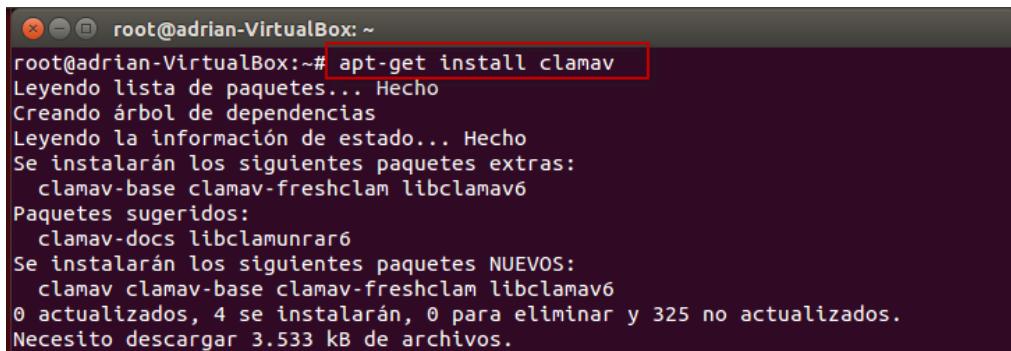
Escaneando o equipo no que temos instalado o Keylogger, aproveitando o ejercicio anterior. Vemos que se detectaron 41 obxectos infectados.



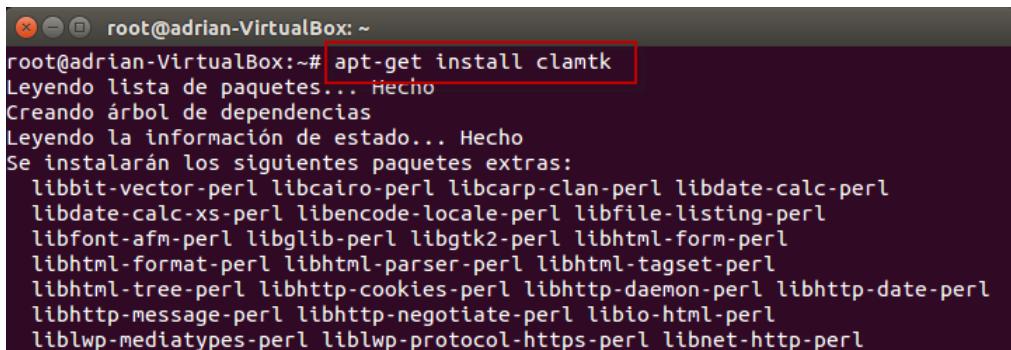
Podemos ver no resultado do analise como está paisaxe.jpg (que é realmente o keylogger enmascarado) detectao como ameza así como "Cain" (outro software instalado noutro temario), etc.

Amenaza	Categoría	Tipo	Ubicación
PUP.Optional.ArdamaxKeyLogger	Programas potencialmente no deseados	Archivo	C:\Users\adrian\Desktop\install.exe
PUP.Optional.ArdamaxKeyLogger	Programas potencialmente no deseados	Archivo	C:\Users\adrian\Desktop\paisaxe2 (2).exe
PUP.Optional.ArdamaxKeyLogger	Programas potencialmente no deseados	Archivo	C:\Users\adrian\Desktop\paisaxe2.exe
HackTool.Cain	Malware	Archivo	C:\Program Files\Cain\Abel.exe
HackTool.Cain	Malware	Archivo	C:\Program Files\Cain\Abel64.exe
PUP.Optional.PasswordTool.Cain	Programas potencialmente no deseados	Archivo	C:\Program Files\Cain\Cain.exe
PUP.Optional.ArdamaxKeyLogger	Programas potencialmente no deseados	Archivo	C:\Users\adrian\Documents\install.exe
Trojan STRGen	Malware	Valor del registro	HKLM\SOFTWARE\Microsoft\...ENTVERSION\RUN\BKB Start
Trojan STRGen	Malware	Archivo	C:\ProgramData\OYYVII\BKB.exe
Trojan STRGen	Malware	Valor del registro	HKU\S-1-5-21-1366977006-13...3-1795099234-1001\SOFTWARE
Trojan STRGen	Malware	Proceso	C:\ProgramData\OYYVII\BKB.exe

No caso de Linux (Ubuntu) dispomos de de antivirus como poden ser, ClamAv e Clamtk en modo gráfico. Instalaremos ambas e probarémolas.

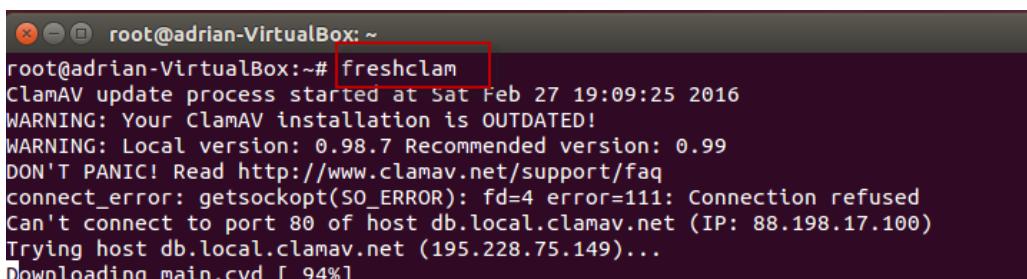


```
root@adrian-VirtualBox:~# apt-get install clamav
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  clamav-base clamav-freshclam libclamav6
Paquetes sugeridos:
  clamav-docs libclamunrar6
Se instalarán los siguientes paquetes NUEVOS:
  clamav clamav-base clamav-freshclam libclamav6
0 actualizados, 4 se instalarán, 0 para eliminar y 325 no actualizados.
Necesito descargar 3.533 kB de archivos.
```



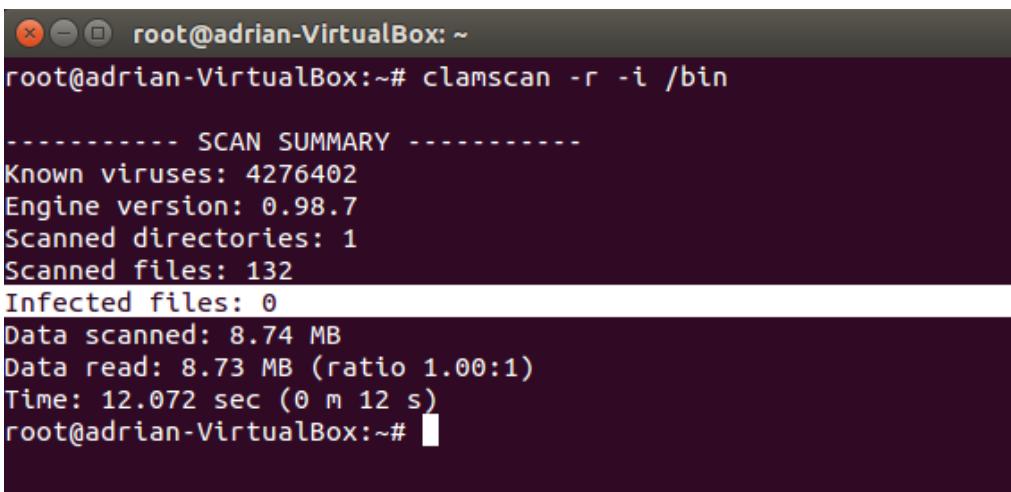
```
root@adrian-VirtualBox:~# apt-get install clamtk
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  libbit-vector-perl libcairo-perl libcarp-clan-perl libdate-calc-perl
  libdate-calc-xs-perl libencode-locale-perl libfile-listing-perl
  libfont-afm-perl libglib-perl libgtk2-perl libhtml-form-perl
  libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl
  libhtml-tree-perl libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl
  libhttp-message-perl libhttp-negotiate-perl libio-html-perl
  liblwp-mediatypes-perl liblwp-protocol-https-perl libnet-http-perl
```

Actualizamos a base datos dos antivirus de forma Online con freshclam dende root.



```
root@adrian-VirtualBox:~# freshclam
ClamAV update process started at Sat Feb 27 19:09:25 2016
WARNING: Your ClamAV installation is OUTDATED!
WARNING: Local version: 0.98.7 Recommended version: 0.99
DON'T PANIC! Read http://www.clamav.net/support/faq
connect_error: getsockopt(SO_ERROR): fd=4 error=111: Connection refused
Can't connect to port 80 of host db.local.clamav.net (IP: 88.198.17.100)
Trying host db.local.clamav.net (195.228.75.149)...
Downloading main.cvd [ 94%]
```

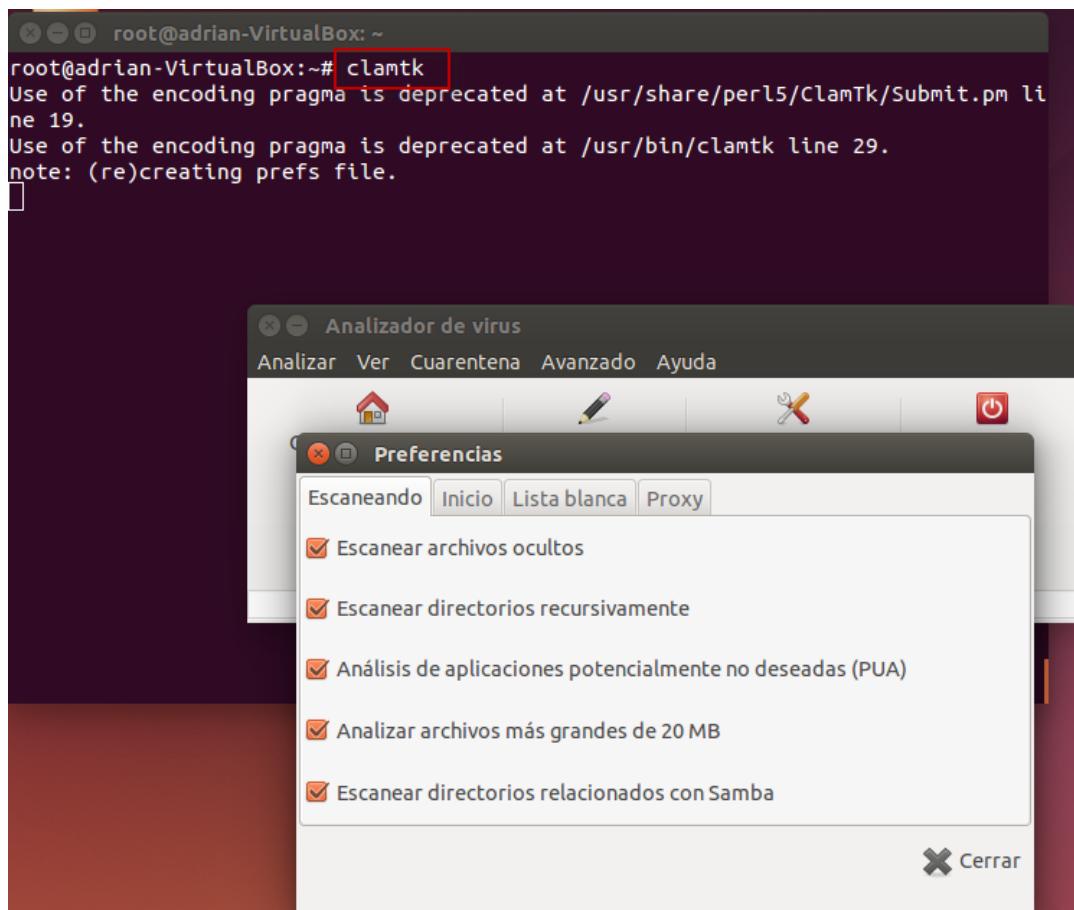
Facemos un escaneo do directorio /bin, -r de forma recursiva, -i que so nos mostre os ficheiros infectados. Neste caso parece que estamos limpos.



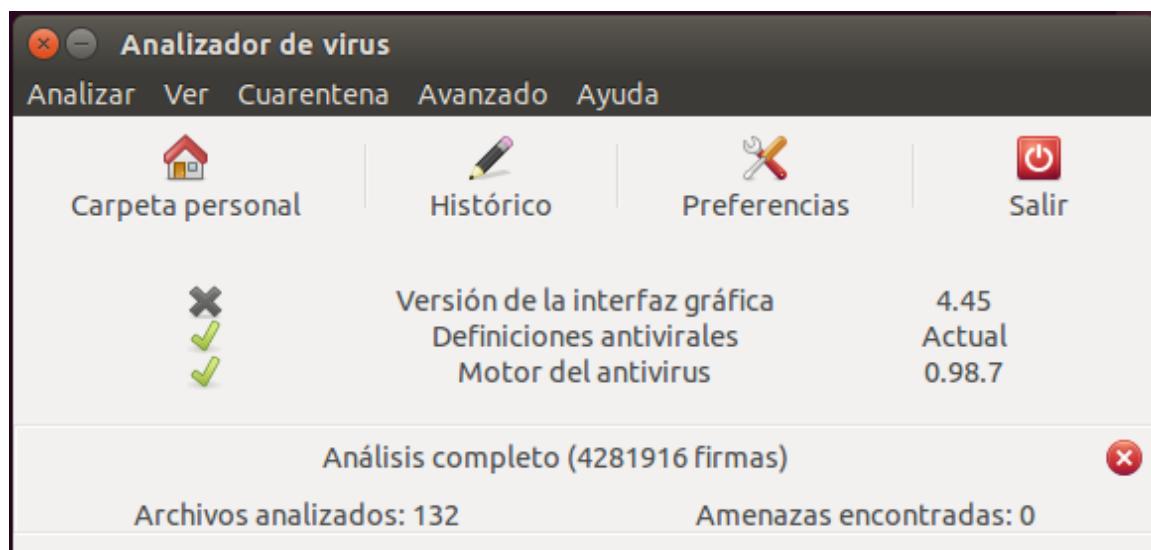
```
root@adrian-VirtualBox:~# clamscan -r -i /bin
----- SCAN SUMMARY -----
Known viruses: 4276402
Engine version: 0.98.7
Scanned directories: 1
Scanned files: 132
Infected files: 0
Data scanned: 8.74 MB
Data read: 8.73 MB (ratio 1.00:1)
Time: 12.072 sec (0 m 12 s)
root@adrian-VirtualBox:~#
```

```
root@adrian-VirtualBox: ~
/home/adrian/.local/share/recently-used.xbel: OK
/home/adrian/.local/share/evolution/tasks/system/tasks.ics: OK
/home/adrian/.local/share/evolution/calendar/system/calendar.ics: OK
/home/adrian/.local/share/unity-settings-daemon/input-sources-converted: Empty file
/home/adrian/.local/share/telepathy/mission-control/accounts.cfg: OK
/home/adrian/.local/share/unity-webapps/availableapps-v2.db: OK
/home/adrian/.local/share/.converted-launchers: Empty file
/home/adrian/.local/share/gsettings-data-convert: OK
/home/adrian/.remmina/remmina.pref: OK
/home/adrian/.compiz/session/10a4d5a3bbc8edc2b4144259783738440700000018690001: OK
/home/adrian/.xsession-errors: OK
/home/adrian/.dbus/session-bus/c4e2ff811945536087e893af55fb045d-0: OK
/home/adrian/.config/ibus/bus/c4e2ff811945536087e893af55fb045d-unix-0: OK
/home/adrian/.config/user-dirs.locale: OK
/home/adrian/.config/unity/first_run.stamp: Empty file
/home/adrian/.config/gtk-3.0/bookmarks: OK
/home/adrian/.config/dconf/user: OK
/home/adrian/.config/pulse/c4e2ff811945536087e893af55fb045d-stream-volumes.tdb: OK
/home/adrian/.config/pulse/c4e2ff811945536087e893af55fb045d-default-source: OK
/home/adrian/.config/pulse/cookie: OK
/home/adrian/.config/pulse/c4e2ff811945536087e893af55fb045d-card-database.tdb: OK
```

Executamos clamtk dende root, abrirase a interfaz gráfica. Seleccionamos as opcións de escaneo oportunas.



Como vemos seguimos limpos.

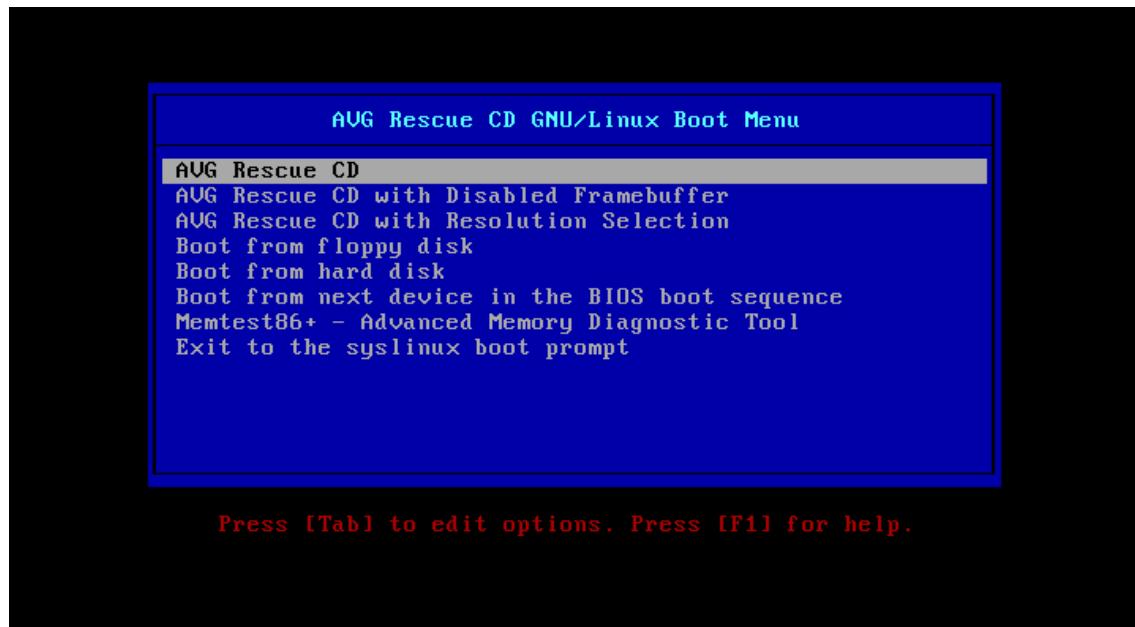


O intereseante disto e saber que se iniciamos un LiveUbuntu (cargado en memoria) con funcións de rede e acceso aos repositorios e instalamos por exemplo clamav. Montamos con "mount" o disco do sistema instalado no equipo sexa Linux ou Windows nunha zona do live e podémolo escanear con clamav.

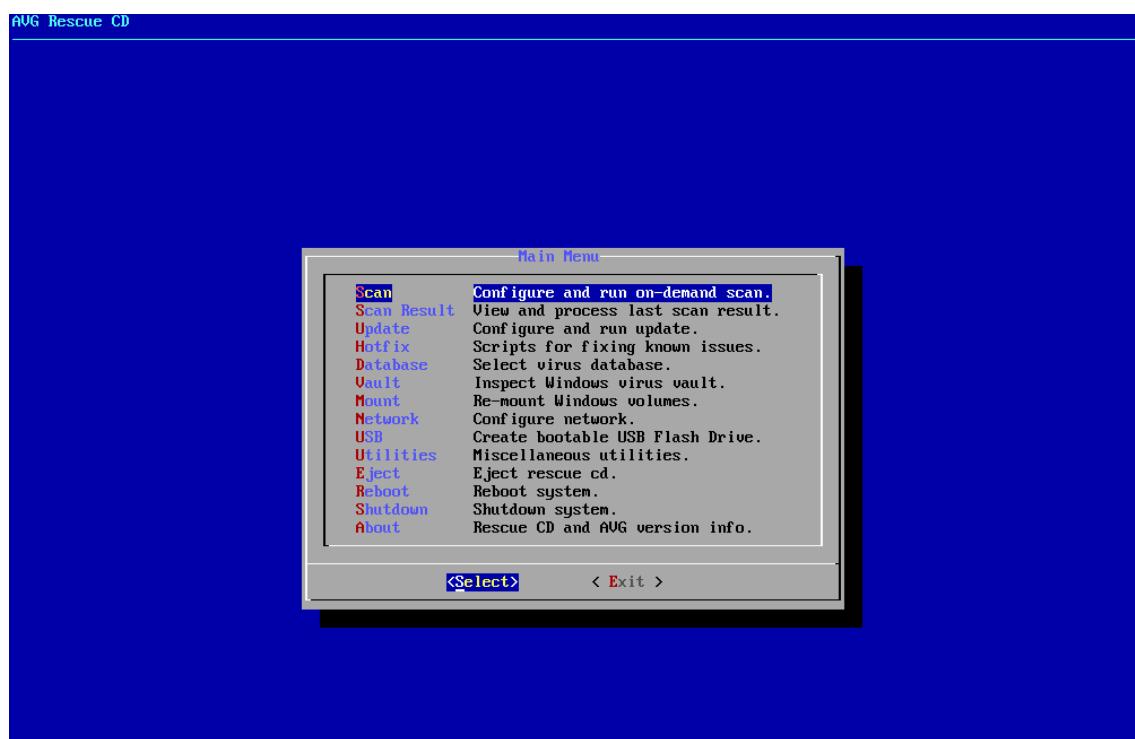
5. Análise antimalware live

No caso de que teñamos un malware o cal nos quite o safe mode e se poda cargar no arrinque do sistema. Faremos uso de utilidades antimalware Live's.

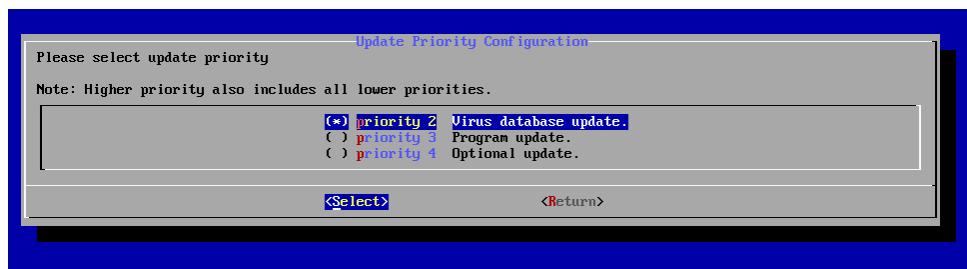
Neste caso probouse con AVG Rescue LiveCD.



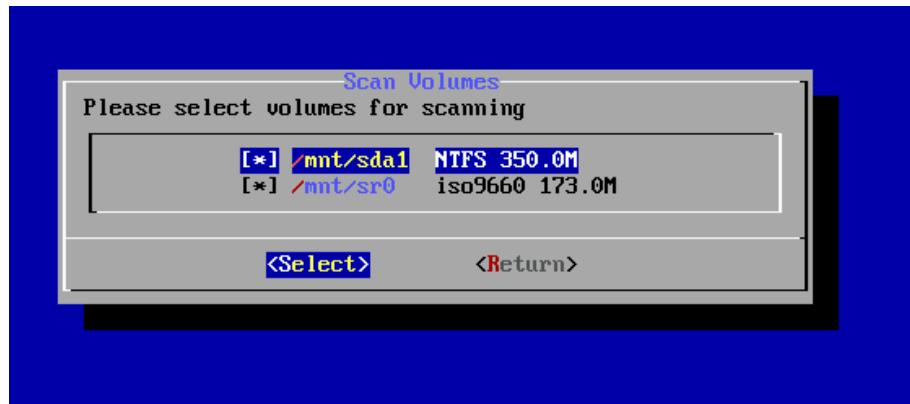
Permítenos varias opcións, podemos realizar un esqueno normal.



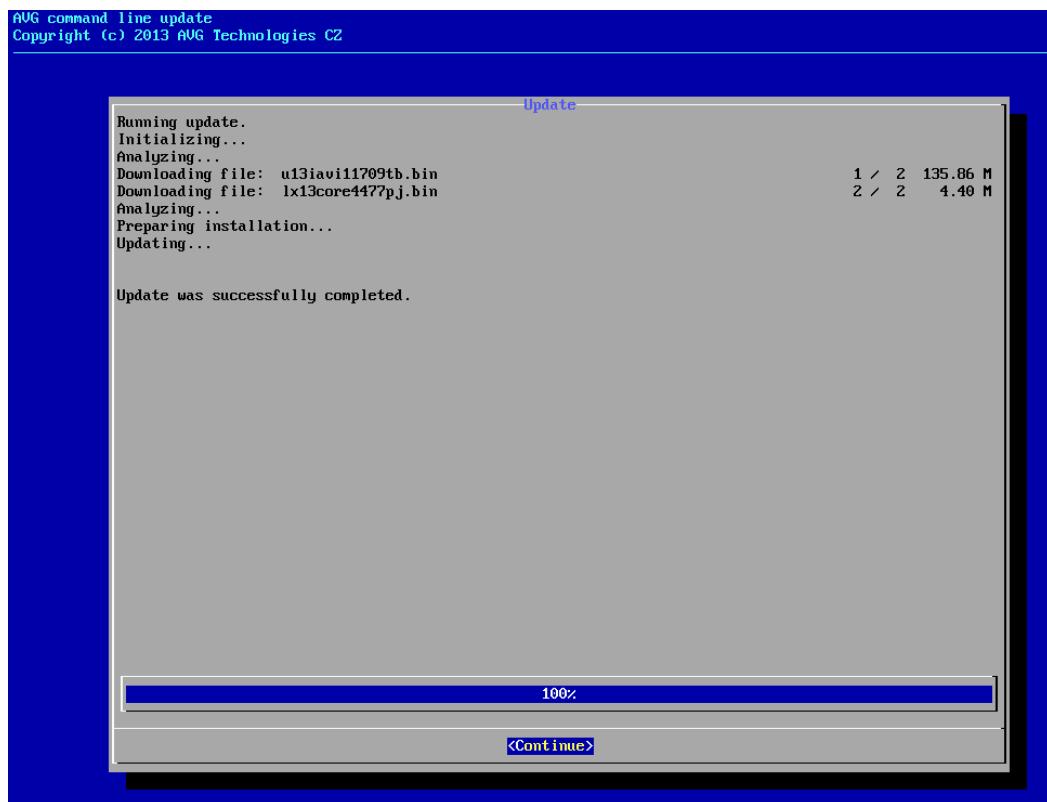
Eleximos a prioridade de actualización da base datos de virus.



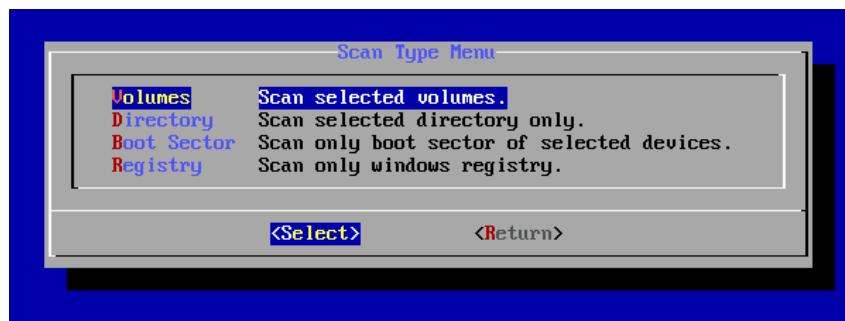
Seleccionamos sobre que volumen queremos realizar o escaneo.



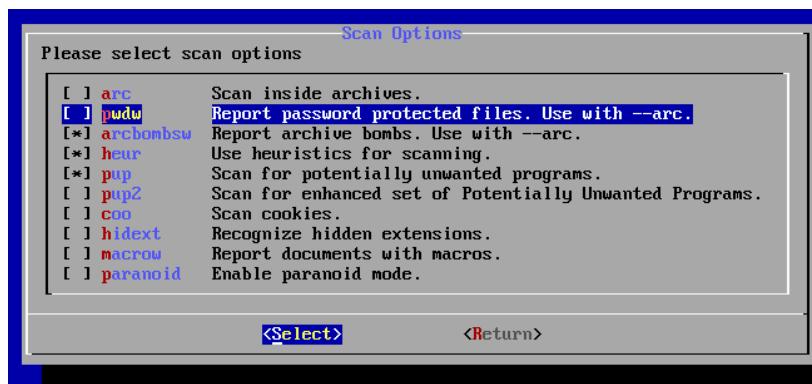
Actualizando a base datos.



Seleccionamos a zona a escanear, xa poden ser un volumen, directorios, rexistro de Windows ou sector de arrinque.



Podemos seleccionar de forma múltiple os tipos de escaneo que se levarán a cabo, podemos ser más concretos nas seleccións a esquerda.



Outras ferramentas antimalware Live's:

Trend Micro:

<http://www.trendmicro.com/ftp/products/rescuedisk/RescueDisk.exe>

F-Secure:

<http://download.f-secure.com/estore/rescue-cd-3.16-73600.iso>

Avira:

http://install.avira-update.com/package/rs_avira/unix/int/rescue-system.iso

Eset:

<http://descargas.eset.es/utilidades>

"ESET SysRescue Live"

Bitdefender:

http://download.bitdefender.com/rescue_cd

"BitDefenderRescueCD_v2.0.0_5_10_2010.iso"

Kaspersky:

<http://support.kaspersky.com/viruses/rescuedisk>

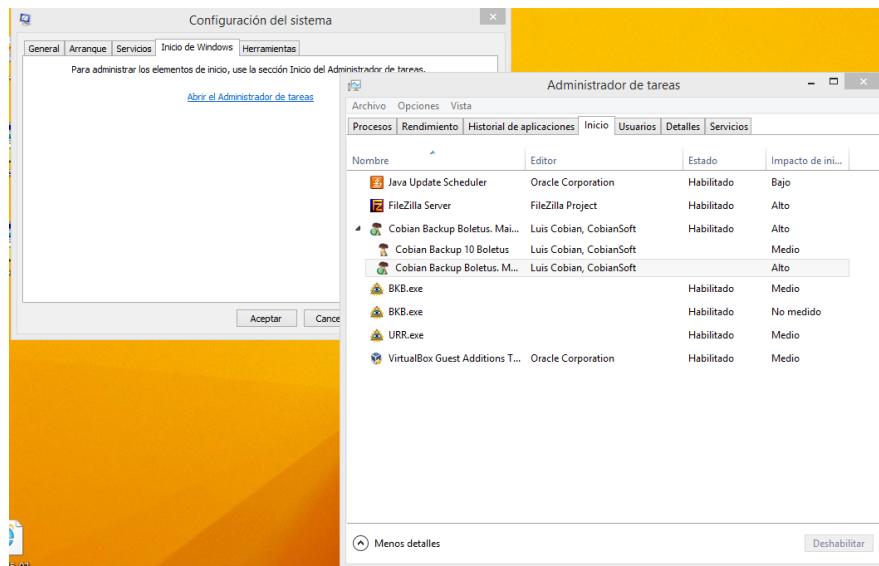
Comodo:

http://downloads.comodo.com/crd/download/setups/comodo_rescue_disk_2.0.261647.1.iso

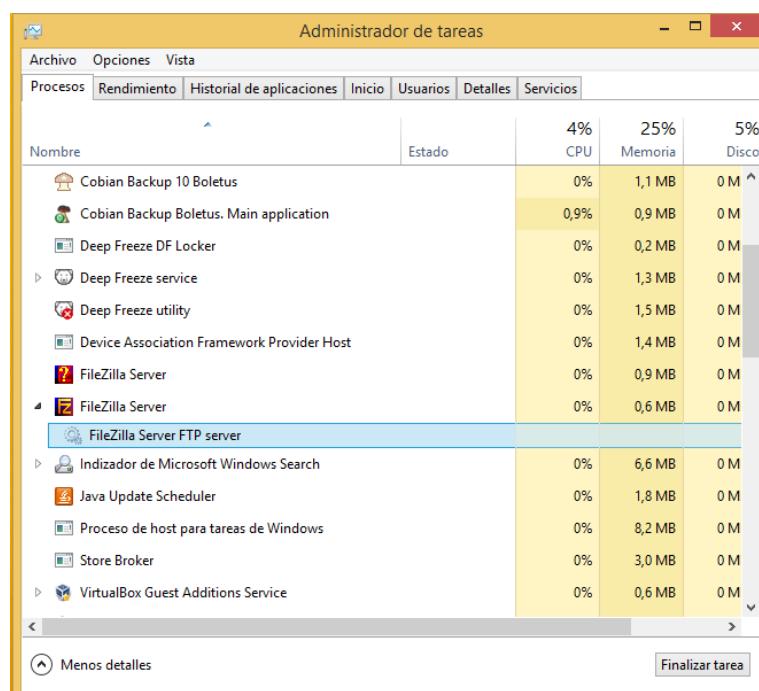
6. Análise antimalware en sistemas activos e online

Nesta tarefa veremos como detectar malware activo “latente” nun equipo local. Os pasos a seguir que deberíamos ir facendo para pouco a pouco entrar máis en profundidade no análisis do sistema, nesta caso nun sistema Windows.

O primeiro que debemos fazer é mirar os procesos de aplicación que se executan no inicio de Windows. Ahí podemos comprobar si se inicia algo non lexítimo ou usuario. (msconfig ou taskmgr “pestaña inicio”).



Tamén podemos observar o Administrador de tarefas o cal nos dice que procesos se están executando nese momento, o taskmgr de Windows 8/8.1/10 é máis sofisticado co de Windows XP/7. Un bo detalle é que mostran os servizos dependentes dun proceso.



Outras alternativas a msconfig e taskmgr por defecto de Windows, son “Autoruns” e “Process Explorer” as dúas de Sysinternals de Microsoft.

Autoruns é unha aplicación que nos mostra non so procesos de inicio, si non que moitas outras características.

Saber tamen que a clave de rexistro de Windows donde se almacenan as rutas de carga dos procesos de inicio e: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

Autoruns - Sysinternals: www.sysinternals.com						
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal	
HKLM\Software\Microsoft\Windows\CurrentVersion\Run	Cobian Backup 10	Cobian Backup Boletus. Ma... Luis Cobian, Cobian Soft	c:\program files\cobian bac...	23/09/2010 15:46		
FileZilla Server Interface	FileZilla Server	FileZilla Project	c:\program files\filezilla serv...	28/01/2016 17:28		
SunJavaUpdateSched	Java Update Scheduler	Oracle Corporation	c:\program files\common fil...	30/01/2016 3:57		
VBoxTray	VirtualBox Guest Additions ...	Oracle Corporation	c:\windows\system32\vbox...	02/10/2015 13:36		
HKCU\Software\Microsoft\Windows\CurrentVersion\Run	URR Start		c:\programdata\urr\urr.exe	12/11/2015 22:23		
HKLM\Software\Microsoft\Active Setup\Installed Components	Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files\windows m...	22/08/2013 4:13	
HKLM\Software\Classes\ShellEx\ContextMenuHandlers	7-Zip	7-Zip Shell Extension	Igor Pavlov	c:\program files\7-zip\7zip.dll	31/12/2015 15:25	
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers	7-Zip	7-Zip Shell Extension	Igor Pavlov	c:\program files\7-zip\7zip.dll	31/12/2015 15:25	
HKLM\Software\Classes\DragDropHandlers	7-Zip	7-Zip Shell Extension	Igor Pavlov	c:\program files\7-zip\7zip.dll	31/12/2015 15:25	
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers	7-Zip	7-Zip Shell Extension	Igor Pavlov	c:\program files\7-zip\7zip.dll	31/12/2015 15:25	
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	Java(tm) Plug-in SSV Helper	Java(TM) Platform SE binary	Oracle Corporation	c:\program files\java\jre1.8...	30/01/2016 3:07	
	Java(tm) Plug-in SSV Helper	Java(TM) Platform SE binary	Oracle Corporation	c:\program files\java\jre1.8...	30/01/2016 3:06	
Task Scheduler						
Microsoft\Windows\NetTrace\Gat...				c:\windows\system32\gath...	18/07/2013 16:53	
\Microsoft\Windows\Defender	Microsoft Malware Protectio...	Microsoft Corporation		c:\program files\windows d...	22/08/2013 4:43	
\Microsoft\Windows\Defender	Microsoft Malware Protectio...	Microsoft Corporation		c:\program files\windows d...	22/08/2013 4:43	

Procesos que se executan no inicio de login do usuario cos paths donde se cargan e o vendor do aplicativo, en caso de ver un proceso cun nome sospeitoso e sin vendor nunha ruta non moi común para o almacenamento de programas por defecto de Windows, poderemos sospeitar un pouco sobre ese proceso, neste caso observase o Keylogger Ardamax (URR).

Autoruns - Sysinternals: www.sysinternals.com						
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal	
HKLM\Software\Microsoft\Windows\CurrentVersion\Run	Cobian Backup 10	Cobian Backup Boletus. Ma... Luis Cobian, CobianSoft	c:\program files\cobian bac...	23/09/2010 15:46		
FileZilla Server Interface	FileZilla Server	FileZilla Project	c:\program files\filezilla serv...	28/01/2016 17:28		
SunJavaUpdateSched	Java Update Scheduler	Oracle Corporation	c:\program files\common fil...	30/01/2016 3:57		
VBoxTray	VirtualBox Guest Additions ...	Oracle Corporation	c:\windows\system32\vbox...	02/10/2015 13:36		
HKCU\Software\Microsoft\Windows\CurrentVersion\Run	URR Start		c:\programdata\urr\urr.exe	12/11/2015 22:23		
HKLM\Software\Microsoft\Active Setup\Installed Components	Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files\windows m...	22/08/2013 4:13	

Outra característica a destacar son os servizos de Windows empregados polas aplicacións, que ainda que temos a utilidade nativa do sistema (services.msc) e o novo administrador de tarefas que nos di os servizos que dependen dun proceso, esta característica de Autoruns e igualmente interesante.

Autoruns - Sysinternals: www.sysinternals.com

Autonun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\System\CurrentControlSet\Services\cbVSCService	Cobian Backup Boletus VS... Cobian Soft, Luis Cobian	c:\program files\cobian backup 10\cb...	08/02/2010 22:53		
HKLM\System\CurrentControlSet\Services\DFServ	Deep Freeze service Faronics Corporation	c:\program files\faronics\deep freeze\...	30/10/2015 10:27		
HKLM\System\CurrentControlSet\Services\FileZilla Server	FileZilla Server FileZilla Project	c:\program files\filezilla server\filezill...	28/01/2016 16:51		
HKLM\System\CurrentControlSet\Services\MBAMService	Malwarebytes Anti-Malware ... Malwarebytes	c:\program files\malwarebytes anti-mal...	03/09/2015 14:08		
HKLM\System\CurrentControlSet\Services\ModemMaintenance	El servicio de mantenimiento... Mozilla Foundation	c:\program files\mozilla maintenance s...	11/02/2016 2:36		
HKLM\System\CurrentControlSet\Services\pcapd	Allows to capture traffic on t... Riverbed Technology, Inc.	c:\program files\wincap\pcapd.exe	01/03/2013 2:28		
HKLM\System\CurrentControlSet\Services\uvnc_service	Provides secure remote des... UltraVNC	c:\program files\uvnc\bvba\ultravnc\w...	24/01/2016 23:42		
HKLM\System\CurrentControlSet\Services\VBoxService	Manages VM runtime inform... Oracle Corporation	c:\windows\system32\vboxservice.exe	02/10/2015 13:36		
HKLM\System\CurrentControlSet\Services\WdNisSvc	Ayuda a proteger contra int... Microsoft Corporation	c:\program files\windows defender\vis...	22/08/2013 4:11		
HKLM\System\CurrentControlSet\Services\WinDefend	Ayuda a proteger a los usu... Microsoft Corporation	c:\program files\windows defender\ms...	22/08/2013 5:02		

Outra sección interesante a de ver as tarefas programadas, moitos tipos de malware poden cargarse de forma programada ou por “disparadores” de accións do usuario.

Autoruns - Sysinternals: www.sysinternals.com

Autonun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
Task Scheduler\Microsoft\Windows\NetTrace\GatherNetworkInfo		c:\windows\system32\gath...	18/07/2013 16:53		
Task Scheduler\Microsoft\Windows\Windows Defender\Windows Defen...	Microsoft Malware Protectio... Microsoft Corporation	c:\program files\windows d...	22/08/2013 4:43		
Task Scheduler\Microsoft\Windows\Windows Defender\Windows Defen...	Microsoft Malware Protectio... Microsoft Corporation	c:\program files\windows d...	22/08/2013 4:43		
Task Scheduler\Microsoft\Windows\Windows Defender\Windows Defen...	Microsoft Malware Protectio... Microsoft Corporation	c:\program files\windows d...	22/08/2013 4:43		
Task Scheduler\Microsoft\Windows\Windows Defender\Windows Defen...	Microsoft Malware Protectio... Microsoft Corporation	c:\program files\windows d...	22/08/2013 4:43		

Tamén poderíamos consultar o programador de tarefas de Windows (taskschd.msc) no cal poderemos ver tamen profundamente as tarefas programadas.

Programador de tareas

Archivo Acción Ver Ayuda

Windows

Nombre	Estado	Desencadenadores	Hora próxima ejecución	Hora última ejecución
ScheduledDefrag	Listo		03/03/2016 10:55:01	

Acciones

- Defrag
- Crear tarea básica...
- Crear tarea...
- Importar tarea...
- Mostrar todas las tareas en ejecución
- Habilitar el historial de todas las tareas
- Nueva carpeta...
- Eliminar carpeta
- Ver
- Actualizar
- Ayuda

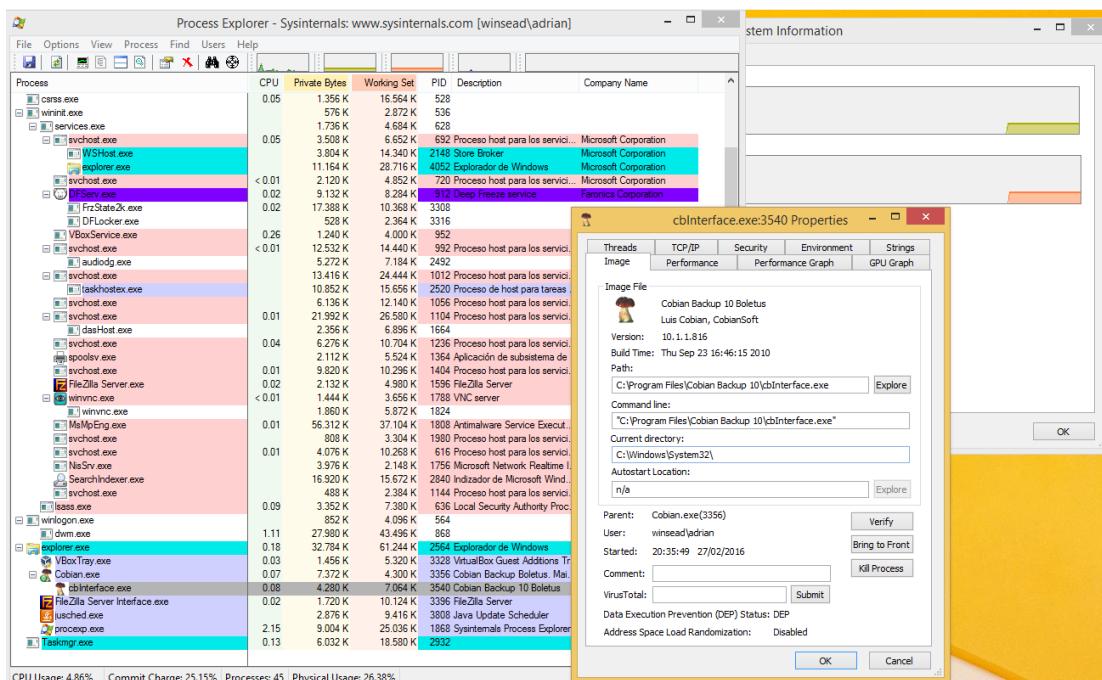
Elemento seleccionado

- Ejecutar
- Finalizar
- Deshabilitar
- Exportar...

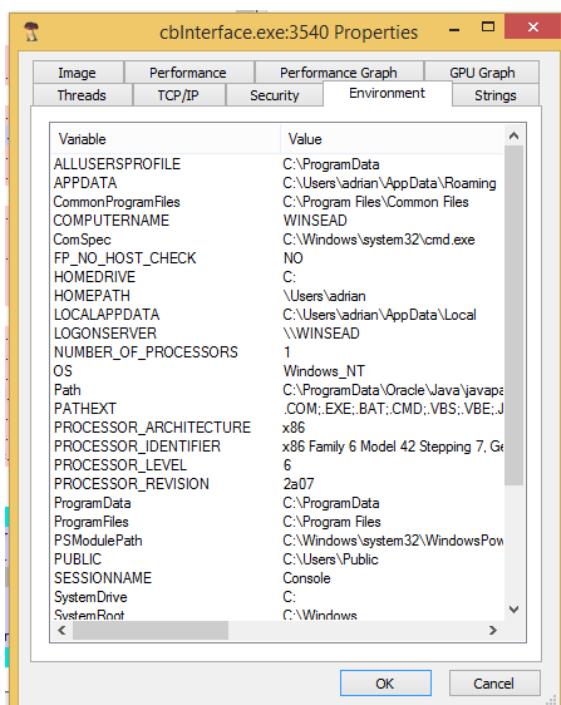
Unha alternativa o administrador de tarefas de Windows e Process Explorer. Utilidade moi útil para ver de forma xerárquica os procesos que se están execuntando e coñecer a suas dependencias.

Deixo unha ligazón o meu blog sobre esta ferramenta e sobre TaskInfo (a cal se falará nesta tarefa máis adiante):

<http://www.zonasytem.com/2010/04/system-explorer-un-administrador-de.html>



Variables e paths útiles para profundizar no funcionamento e interacción do proceso.



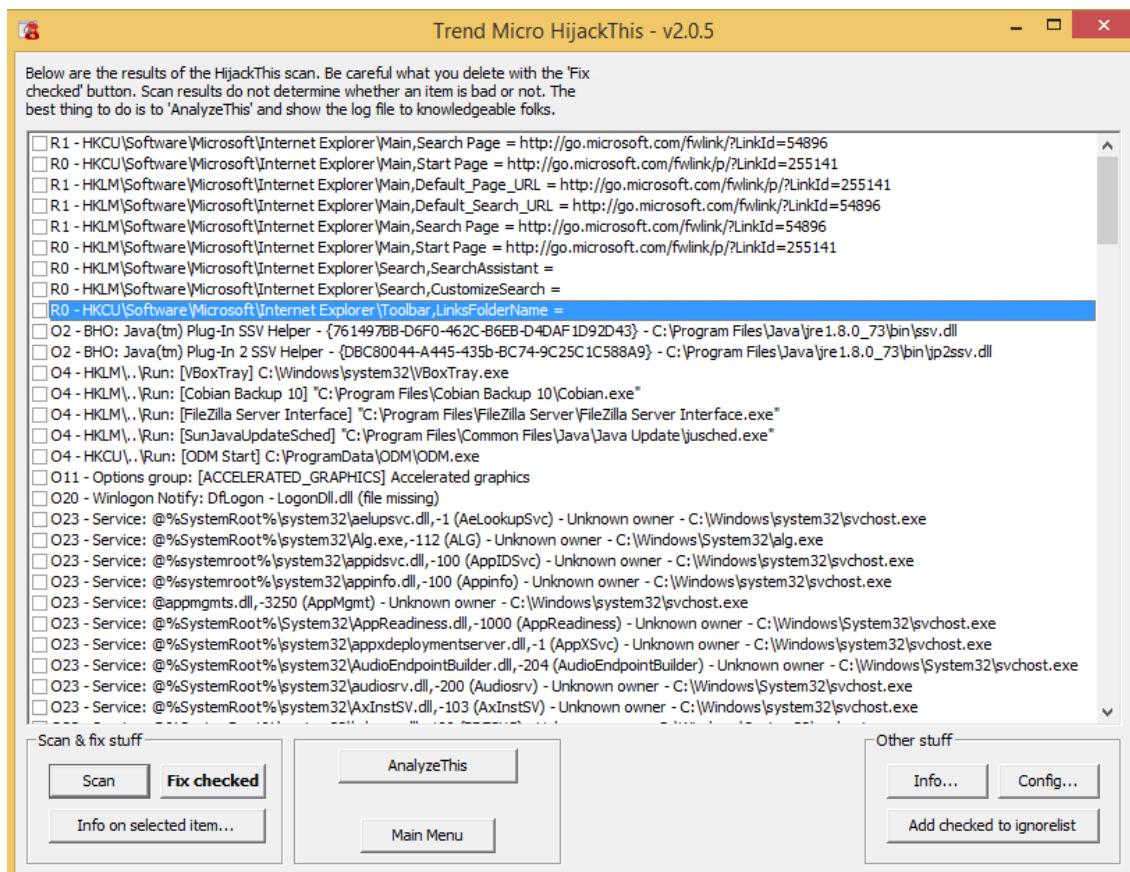
Unha utilidade interesante e HijackThis, analizaremos todo o sistema de forma rápida buscando posibles anomalías.

Sobretodo resulta útil para ver e tentar eliminar as molestas barras dos navegadores web (toolbars) así como PUP (Potentially Unwanted Program) aqueles programas que se instalan sin consentimento do usuario, software que resulta moi molesto e carga recursos innecesarios no equipo. Dito adware tamen se podría eliminar coa utilidade ben coñecida: AdwCleaner.

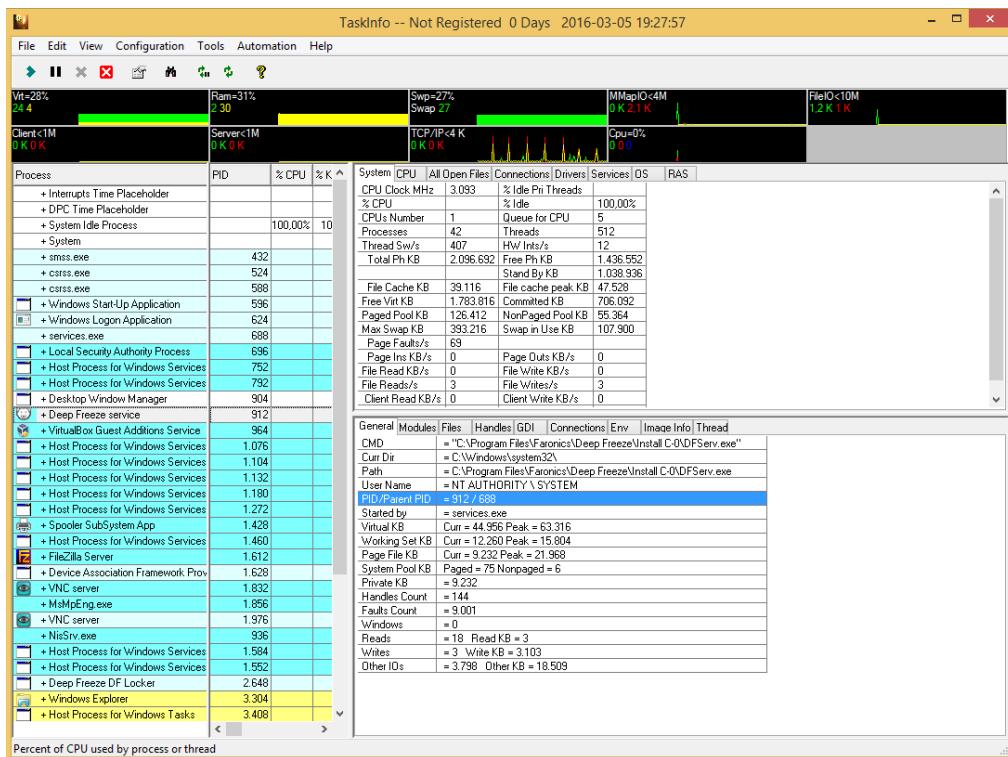
Si nos fixamos nos resultados que mostra un escaneo de HijackThis veremos que este uns números, estos números son códigos que indican de que tipo son as entradas mostradas.

Deixo unha ligazón o meu blog para máis info sobre como entender un log de HijackThis:

<http://www.zonasytem.com/2010/04/detectar-software-malicioso-del.html>



Outra utilidade monitoreo do sistema e que nos facilite o análise de este, é TaskInfo, unha utilidade que engloba un conxunto de ferramentas nunha mesma. Administrador de tarefas + información do sistema + monitor de recursos + dependencias e informaícon dos procesos.



Por outro lado temos o análise de malware de maneria Online, podendo subir un ficheiro ou escanear unha páxina web, e comprobar si está libres de ameazas..

Unha antivirus en liña que fai un barrido por múltiples antivirus dun arquivo ou web proporcionada e: virustotal.com

Comprobación dun website de exemplo: zonasystem.com, está libre de posibles ameazas.

The screenshot shows the VirusTotal analysis results for the URL <http://zonasystem.com>. The page displays a summary with the URL, detection count (0/67), and analysis date (2016-02-27 09:12:30 UTC). It also features a green 'Clean site' rating icon. Below this, the 'Analizador' section lists various antivirus engines and their results for the site, all showing 'Clean site'. At the bottom, there are tabs for 'Análisis', 'Información adicional', 'Comentarios', and 'Votos'.

Comprobando o ficheiro xerado polo Keylogger vemos que 37 de 54 antimalware, detectaron dito ficheiro como perigoso.

The screenshot shows the VirusTotal analysis interface. At the top, there's a navigation bar with links like 'Comunidad', 'Estadísticas', 'Documentación', 'FAQ', 'Acerca de...', 'Español', 'Únete a la comunidad', and 'Iniciar sesión'. Below the navigation is the 'virus total' logo. The main content area displays the following information:

- SHA256:** 7a75a5d73a458e04cf60250d3faee9664adcb29d3c239a25747200ead0fda
- Nombre:** Install.exe
- Detecciones:** 37 / 54
- Fecha de análisis:** 2016-02-27 20:03:49 UTC (hace 3 minutos)

To the right of the details is a color-coded threat level meter showing a red-to-green gradient with two smiley faces at the ends, both labeled '0'.

Below the details, there are tabs for 'Análisis' (selected), 'Detalles', 'Información adicional', 'Comentarios', 'Votos', and 'Información de comportamiento'. A table follows, listing various antivirus engines and their detection results:

Antivirus	Resultado	Actualización
AVG	Luhe.Fiha.A	20160227
AVware	Trojan.Win32.Ardamax.nbq (v)	20160227
Ad-Aware	Gen.Variant.FAKEAlert.105	20160227
AegisLab	Troj.W32.Gen	20160227
Agnitum	Riskware.Ardamax!	20160227
AhnLab-V3	Trojan/Win32.Agent	20160227
Antiy-AVL	RiskWare[Monitor:not-a-virus,HEUR]/Win32.Ardamax	20160227
Arcabit	Trnian FAkeAlert 105	20160227

Existen múltiples antivirus de escaneo online como poden ser: "ESET Online Scanner" e "F-Secure Online Scanner".

The screenshot shows the ESET Online Scanner website and its active scan window. The main page has a sidebar with links for 'Online Scanner', 'Online Scanner en su sitio', 'Nuevas Características', 'Beneficios', 'Requerimientos del Sistema', 'Ayuda', and 'Preguntas Frecuentes'. The main content area features the 'ESET Online Scanner' logo and a green banner with the text 'Utilice gratis nuestro antivirus online: ESET Online Scanner'. To the right, a large window titled 'ESET Online Scanner' shows the status of an analysis:

Análizando... (Step 3 of 4)

Analís del ordenador en curso...

Progress bar: 81%

Details:

- Objetivo: C:\Users\adrian\AppData\Local\Temp\DeepFreeze_C.exe
- Archivos analizados: 18136
- Archivos infectados: 15
- Duración total del análisis: 00:05:32

Resultados del análisis actual:

- Se han detectado amenazas
 - JS/Kryptik.AZM.Troyano
 - JS/Exploit.Agent.NLM.Troyano
 - JS/Iframe.LX.Troyano
 - una variante de Win32/KeyLogger.Ardamax.NBG aplicación
 - una variante de Win32/KeyLogger.Ardamax.NBP aplicación
 - ...

ESET

Ainda que foi un proceso que tardou en comparación con outros escáneres online diste tipo, este detectounos varias ameazas, entre elas a ferramente de Cain e o Keylogger instalado.

The screenshot shows the ESET Online Scanner interface. On the left, there's a sidebar with links like 'Online Scanner', 'Online Scanner en su sitio', 'Nuevas Características', 'Beneficios', 'Requerimientos del Sistema', 'Ayuda', and 'Preguntas Frecuentes'. The main content area has a green header 'ESET Online Scanner' and a sub-header 'Resultados del análisis'. It lists several threats found in the user's system, each with its location, type, and status (e.g., 'eliminado'). A large blue bar at the bottom contains the text 'Copiar información seleccionada' and 'Exportar a archivo de texto...'. The overall theme is dark with green highlights.

No caso de F-Secure o escaneo foi más rápido e ainda que nos detectou soamente 3 ameazas entre elas, o keylogger, non foi tan exhaustivo como ESET.

The screenshot shows the F-Secure Online Scanner interface. At the top, there are navigation links for 'Para el hogar', 'Para empresas (en Inglés)', and 'Para socios (en Inglés)'. Below that, there's a section titled 'Reiniciar el equipo' with the sub-instruction 'Reiniciale el equipo para limpiar todos los elementos perjudiciales.' Three threat items are listed under 'Limpiar al reiniciar': 'Application:W32/Generico...', 'Application:W32/Generico...', and 'Application:W32/Generico...'. Each item shows 'Archivos infectados: 1'. At the bottom, a large blue button says 'Reiniciar el equipo'. The background features a photograph of a person's hands typing on a keyboard.

Para finalizar estas tarefas relacionadas co análise e desinfección de malware, deixo unha ligazón onde fai un tempo redactara un artículo sobre un conxunto de ferramentas útiles para estes cometidos:

<http://www.zonasystem.com/2010/04/guia-para-dejar-tu-pc-limpio-de-virus-y.html>

7. Conclusóns

Con estas prácticas vimos que de forma sinxela pódese construir un Keylogger, emascaralo e distribuílo a outros equipos mediante correo electrónico, descargas na rede, etc. De modo que como vemos nunca se está plenamente seguro e protexido.

Podemos ver que calquera equipo pode ser administrado xa sea de forma local ou remota a través de Internet, e que esas conexións remotas visual e gráficamente do entorno do noso equipo poden ser ou non lexítimas o usuario final.

E importante tentar ter un pequeno control frente a unha posible ameza, saber os seus posibles riscos ou coñecer que pode estar facendo nun equipo informático e que opcións temos para poder eliminarla.