GUÍA DE SEGURIDAD
(CCN-STIC-423)

INDICADORES DE COMPROMISO (IOC)

OCTUBRE 2015

Edita:
GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA
© Editor y Centro Criptológico Nacional, 2013
NIPO:002-15-026-5
Fecha de Edición: octubre 2015
Andrés Méndez Barco ha participado en la elaboración del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el **Centro Criptológico Nacional** puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Junio de 2013

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. Las mafias utilizan cada vez más a ciberdelincuentes con el objeto de lucrarse económicamente. También, cada vez más, algunos gobiernos emplean expertos en seguridad de la información para provocar daños o robar información de empresas o gobiernos rivales.
2. En este contexto, las ciberamenazas son cada vez más elaboradas, más desarrolladas ex profeso y orientadas a ataques u objetivos muy concretos.
3. Esto provoca que defenderse de los ciberataques sea cada vez más complejo, sobre todo cuando un ataque no es globalizado, sino muy dirigido, lo que impide que las herramientas de protección habituales o los protocolos de actuación sean tan eficientes como se espera, ya que por norma general no se han enfrentado antes con ese ciberataque en concreto.
4. En este entorno es necesario contar con herramientas y protocolos que permitan detectar y responder frente a este tipo de amenazas.

2. OBJETO

5. La presente guía persigue el objetivo de presentar al lector las herramientas existentes para identificar indicadores de compromiso, así como los pasos que se deben dar para actuar frente a amenazas desconocidas. También se mostrará al lector los pasos necesarios para compartir estos ficheros de inteligencia en la plataforma disponible REYES (Repositorio común y estructurado de amenazas y código dañino), así como los pasos de creación y exportación de manera manual.

3. ALCANCE

6. El Responsable de Seguridad, determinará el alcance de su aplicación, considerando la Política de Seguridad de la Organización y las amenazas a las que está expuesta la misma.

4. DEFINICIONES

7. Antes de comenzar con la descripción de las herramientas y su uso, se darán unas nociones básicas sobre los conceptos que se van a usar en esta guía.

4.1. AMENAZA AVANZADA PERSISTENTE

8. Una Amenaza Avanzada Persistente (*Advanced Persistent Threat* – APT) es un tipo de ataque sofisticado, que se ejecuta durante un largo periodo de tiempo y está dirigido específicamente a una Organización.
9. Tienen como objetivo extraer información confidencial o clasificada y/o reducir la capacidad operativa de la Organización atacada.
10. Se llaman así por:

    - **Amenaza**: suponen una amenaza para la Organización, ya que el atacante está muy motivado a robar información o reducir la capacidad operativa de la Organización.

- **Avanzada**: el atacante tiene una alta capacidad que le permite poder llevar a cabo el ataque, aprovechando las vulnerabilidades de la Organización, incluso encontrando nuevas vulnerabilidades no documentadas o utilizando varios vectores de ataque (a través de Internet, mediante ingeniería social, etc.). Es capaz de evadir los sistemas de protección tradicionales (firewalls, antivirus, etc.). Puede hacerse con el control absoluto del sistema comprometido.
- **Persistente**: el ataque se produce durante un largo periodo de tiempo (se puede estar hablando de años) en el que se va consiguiendo información y acceso paulatino a los sistemas.

11. No se considera como una APT el hecho de que se detecte código dañino en un sistema sin que tenga como objetivo el robo de información sensible.

4.2. INDICADOR DE COMPROMISO

12. Los códigos dañinos (virus, troyanos, etc.) realizan modificaciones en los sistemas para acceder a espacios del sistema no autorizados, de mayor nivel, para hacerse con el control de ciertas funciones, etc.
13. Cada código dañino realiza esta tarea de una forma determinada y los hay que son capaces de realizar cambios en su forma de actuar para dificultar a las herramientas de detección su presencia en el sistema. Por ese motivo, cada vez que un proveedor de seguridad (fabricante de antivirus, firewalls, etc.) identifica un nuevo código dañino, lo analiza, interpreta su patrón de ataque y genera una firma para que su herramienta de detección sea capaz de identificarlo, detenerlo e, incluso, anularlo.
14. Pero existen muchas maneras de desarrollar un código dañino y muchas maneras también de atacar un sistema. Por ese motivo, cuando un atacante desarrolla una APT, utiliza un código a medida, para que las herramientas de detección no sean capaces de identificarlo ni detenerlo.
15. No obstante, el código dañino siempre realiza cambios en el sistema orientados a aumentar sus privilegios en el mismo, y es en ese momento cuando se pueden interpretar esas modificaciones que realiza en el sistema como indicadores de que el sistema ha sido comprometido. Es lo que se conoce como Indicador de Compromiso (*Indicator of Compromise* – IOC).
16. Por lo tanto, los indicadores de compromiso sirven para identificar si un sistema ha sido comprometido (a modo de herramienta forense), o si se está intentando comprometerlo.

5. ESTÁNDARES PARA LA DEFINICIÓN DE IOC

17. Existen diversas iniciativas para definir cómo se deben documentar los indicadores de compromiso:
    - *Incident Object Description and Exchange Format* (**IODEF**)[1], creado por miembros del *IETF Extended Incident Handling* (INCH) *Working Group*, que forman parte del *IETF Security Area*.
    - *Open Indicators of Compromise* (**OpenIOC**)[2], creado por la empresa de seguridad MANDIANT.

[1] http://www.ietf.org/rfc/rfc5070.txt
[2] http://www.openioc.org

- *Cyber Observable eXpression* (**CybOX**)[3], creado por miembros del MITRE[4].

18. Después de analizar las distintas soluciones, el Centro Criptológico Nacional (CCN) ha optado por emplear el estándar OpenIOC. Se trata de un estándar abierto, de uso gratuito y cuyas herramientas de trabajo esenciales son también gratuitas. Por lo tanto, cada vez que se haga referencia en esta guía a un IOC, siempre se estará hablando de un IOC que sigue el estándar OpenIOC.

6. REYES

19. REYES (REpositorio común Y EStructurado de amenazas y código dañino) está basado en la tecnología MISP (*Código dañino Information Sharing Platform*)[5].
20. REYES es un sistema ya funcional y utilizable por las organizaciones para implementar una plataforma para el intercambio de ciberinteligencia. Puesto que su principal funcionalidad es el intercambio de información, la herramienta está especialmente ideada para ofrecer diversas formas de intercambio y exportación de información entre distintas organizaciones confiables que internamente generan ciberinteligencia. Los usuarios del sistema tienen por tanto la oportunidad de facilitar y consumir elementos de ciberinteligencia.
21. Inicialmente fue desarrollada en el marco de las fuerzas armadas belgas (www.mil.be) pero desde 2012 se ha facilitado abiertamente a la comunidad con una licencia de código abierto y participan en su desarrollo y mejora diversos equipos de respuesta a incidentes como NATO NCIRC[6], CIRCL[7], y CERT-EU[8].
22. Este sistema está adquiriendo bastante popularidad entre distintos equipo de respuesta a incidentes que tienen relación con el NATO NCIRC y actualmente el CIRCL (CSIRT[9] nacional de Luxemburgo) ha implementado una plataforma de intercambio de ciberinteligencia[10] con MISP en la que participan varios CSIRT nacionales europeos y algunos privados.
23. El sistema ofrece una base de datos centralizada de eventos de ciberseguridad en un formato estructurado compatible con iniciativas como OpenIOC o STIX[11], y con funcionalidades como correlación de eventos en base a sus atributos, importación y exportación de estos eventos en distintos formatos (XML[12], texto plano, OpenIOC, YARA, STIX, CSV[13], etc.).
24. Como plataforma de intercambio, el sistema está diseñado para ofrecer distintas capacidades de interrelación entre las distintas entidades que colaborarían en una instancia REYES y también entre distintas instancias REYES.

[3] http://cybox.mitre.org
[4] http://www.mitre.org
[5] http://www.misp-project.org/
[6] Nato Computer Incident Response Capability
[7] Computer Incident Response Center Luxemburg
[8] Computer Emergency Response Team. European Union
[9] Computer Security Incident Response Team
[10] http://www.circl.lu/services/misp-malware-information-sharing-platform/
[11] Structured Threat Information eXpresion
[12] eXtensible Markup Language
[13] Comma Separated Values

25. En una instancia de REYES, una organización colaboradora puede disponer de múltiples usuarios con distintos niveles de privilegios de visibilidad de la información y con registro de sus actividades. Igualmente a nivel de organizaciones también se pueden implementar distintos niveles de visibilidad.
26. Entre distintas instancias de REYES (distintas comunidades) es posible establecer relaciones en las que se establezcan limitaciones como distintos niveles de visibilidad de información, dirección en que se puede realizar la transferencia de información.

7. CREACIÓN DE UN IOC

27. OpenIOC ha definido un formato de fichero, con extensión ".IOC", que contiene un esquema XML extensible para describir las características técnicas que identifican a una amenaza, una metodología de ataque u otra evidencia de compromiso.
28. Por lo tanto, cuando en esta guía se haga referencia a un IOC, se estará hablando tanto de los indicadores de un compromiso como del fichero ".IOC" en el que se representan siguiendo el estándar OpenIOC.
29. Se entiende que, de alguna manera y previamente, el lector de esta guía ha identificado ya cuáles son los indicadores de un compromiso. Gracias a ello puede proceder a documentar cómo se comporta el código dañino mediante el estándar OpenIOC. Si desea conocer una herramienta para identificar situaciones anómalas en un sistema, consulte el apartado 9. (IDENTIFICACIÓN DE SITUACIONES ANÓMALAS EN UN SISTEMA) de la presente guía.

7.1. INSTALACIÓN DE MANDIANT IOC EDITOR

30. Una vez identificados los elementos que se consideran como indicadores de un compromiso, la forma de documentarlos siguiendo el estándar OpenIOC es mediante la herramienta *IOC Editor* (IOCe) de Mandiant.
31. Esta herramienta está desarrollada para plataformas Windows y es de uso gratuito. Se puede obtener desde: https://www.fireeye.com/services/freeware/ioc-editor.html
32. NOTA: Se ha utilizado IOCe versión 2.2 de 4 de diciembre de 2012, para la elaboración de esta guía.
33. Mediante IOCe es posible definir todos los elementos que compondrían un compromiso, como pueden ser rutas de directorios, nombres de ficheros, firmas MD5, claves del registro de Windows, nombres de dominio, direcciones IP, etc.
34. A continuación se explicará cómo instalar IOCe y utilizarlo para crear un primer IOC que identifique un sistema comprometido por un virus imaginario en Windows XP.
35. Este virus tendría el siguiente comportamiento:
    - Genera un fichero ejecutable, que puede llamarse msdr.exe o mshk.exe;
    - Almacena dicho fichero en la carpeta C:\WINDOWS;
    - Genera una librería que empieza por "lib", seguida por números y con extensión .dll en el directorio *C:\WINDOWS\SYSTEM*;
    - Almacena el nombre del ejecutable en el registro de Windows para que se ejecute como *MSDriver* cada vez que se arranque del sistema, en `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`;

- El ejecutable se encuentra en ejecución, cargado en memoria.

36. La aplicación IOCe dispone de un instalador, por lo que su instalación es muy sencilla. Esta aplicación puede instalarse en cualquier equipo, pero es preferible que se instale en un equipo que no haya sido comprometido o que no sea en un equipo del que se tiene sospecha que haya podido ser comprometido.

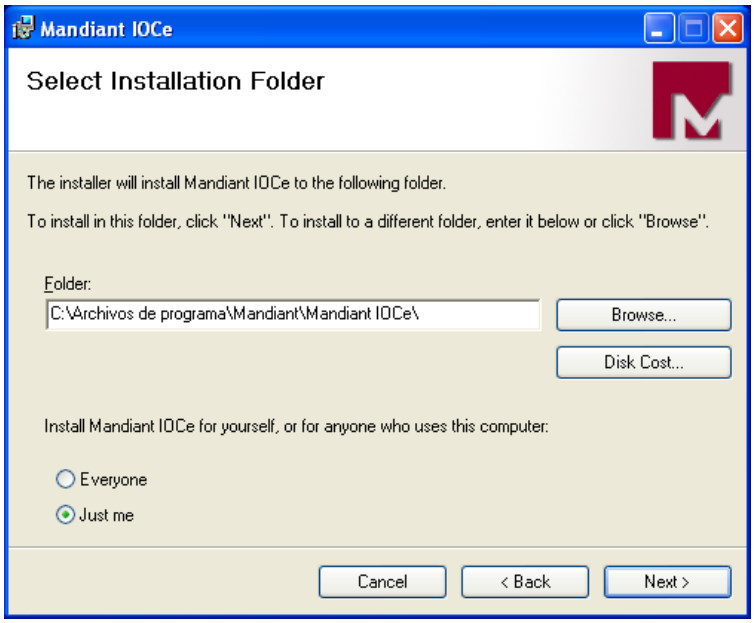


Figura 1. Instalación de Mandiant IOC Editor

37. Lo primero que pedirá la aplicación es el directorio donde trabajar con los ficheros ".IOC". Una opción es crear una carpeta "IOC" dentro de "C:\", por ejemplo, y seleccionarla para tal fin.

Figura 2. Selección del directorio de trabajo

38. Al estar la carpeta vacía, aparecerá una ventana temporalmente indicando que no hay ningún fichero ".IOC" a cargar, y se cerrará dicha ventana automáticamente.

39. Para crear un nuevo ".IOC" se debe ejecutar *File* → *New* → *Indicator*.

7.2. DESCRIPCIÓN DEL IOC

40. Lo primero será introducir la información del IOC a generar, rellenando los siguientes campos:
    - *Name*: nombre del IOC.
    - *Author*: nombre del creador del IOC.
    - *Description*: detalle de la amenaza que este IOC será capaz de detectar.
41. NOTA: las tildes pueden dar problemas, por lo que es aconsejable no utilizarlas.
42. En la zona derecha se pueden añadir más detalles de la amenaza. Para ello bastará con que pulsar con el botón derecho bajo la columna "Type" y seleccionar una de las opciones que se ofrecen, como "Add Category", para especificar una categoría en la que se encuentre la amenaza, que en el caso del ejemplo será "Virus".

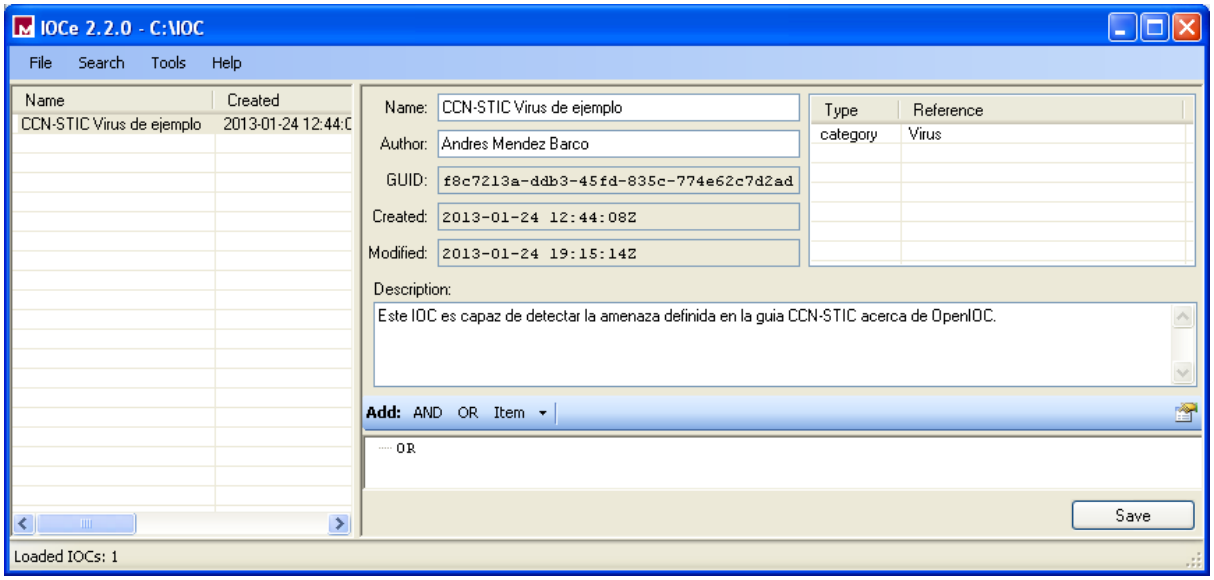


Figura 3. Datos básicos del primer IOC

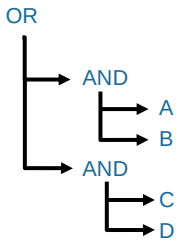
7.3. DEFINICIÓN DE INDICADORES DE COMPROMISO

43. Habitualmente, cuando un código dañino infecta un sistema se suele almacenar como uno o varios ficheros, con uno de los nombres posibles que lleva prefijados, con un nombre aleatorio o siguiendo cierto patrón.
44. IOCe permite modelar los indicadores al comportamiento del código dañino, de forma que se puede recoger esa casuística de varios nombres posibles gracias a la funcionalidad que tiene de crear múltiples árboles con condicionantes Y (AND) y O (OR).
45. La forma de identificar el fichero ejecutable de este virus sería de la siguiente forma:
    - Fichero msdr.exe
    - En la carpeta C:\WINDOWS

    ó

- Fichero mshk.exe
- En la carpeta C:\WINDOWS

46. Esto se representaría del siguiente modo: A and B or C and D
47. O lo que es lo mismo: (A and B) or (C and D)
48. La representación gráfica sería:



49. Para representarlo en el IOC se empieza por crear el primer AND pulsando en el botón "AND".
50. Ahora, el AND que se ha creado estará seleccionado. Para especificar el nombre del fichero se pulsa en el desplegable junto al botón "Item". Mostrará todos los tipos de elementos que soporta el IOC, y se selecciona *FileItem → File Name*.
51. A continuación se introduce el primer posible nombre del fichero ejecutable y se pulsa *Enter*. Se completará automáticamente mostrando "File Name contains msdr.exe".
52. Dado que se ignora si la unidad donde se ha instalado el sistema operativo puede haber sido *C:* u otra, no se usará la letra de la unidad para definir la ruta del ejecutable malicioso. Para especificar entonces la ruta del fichero sin su unidad se selecciona *Item → FileItem → File Path*.
53. Una vez definido esto se puede crear el otro AND. Es posible hacerlo también pulsando en el árbol que se está creando con el botón derecho del ratón, entrando en el menú "Add Logic".
54. No hay problema si en algún momento se crea algo en alguna rama incorrecta, pues arrastrándolo con el ratón se puede colocar donde corresponda.
55. Algo parecido ocurre si el elemento creado no fuera el correcto. Se puede cambiar su tipo pulsando sobre él con el botón derecho del ratón y seleccionando "Change Term".
56. Si ha habido un error en el valor introducido, se puede editar pulsando dos veces en el mismo.

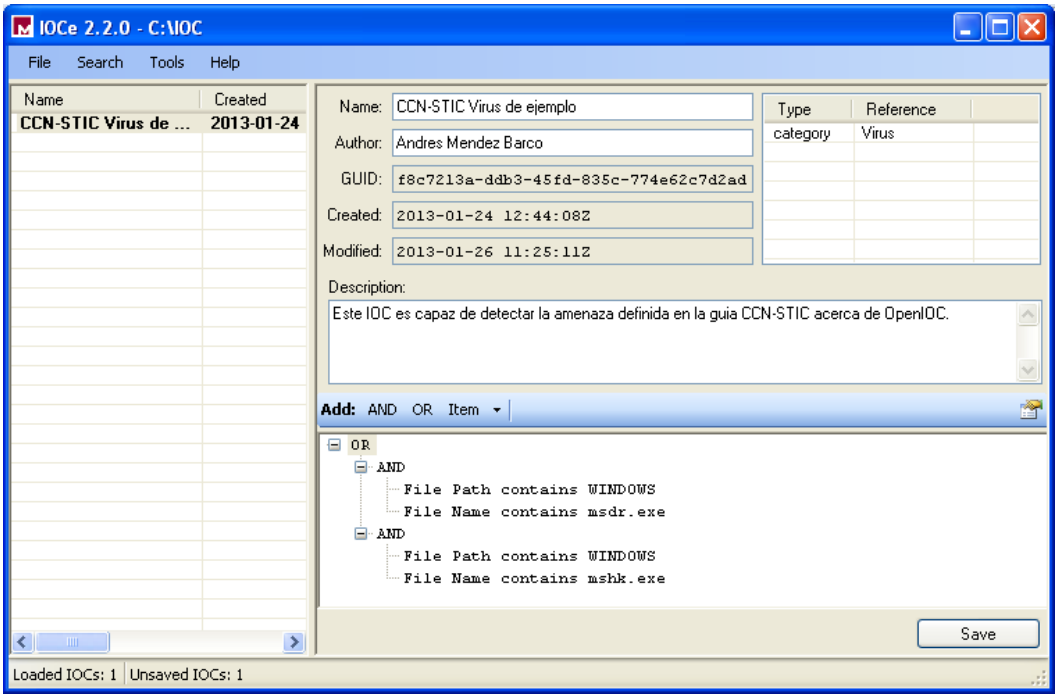


Figura 4. Primeros indicadores de compromiso en el IOC

57. Por defecto, IOCe introduce los valores definidos con la condición "contains" (contiene), es decir, que busque la cadena de texto introducida en el nombre del fichero y en el nombre del directorio. Como son valores exactos, se debe cambiar el "contains" por "is" (es). Esto se hace pulsando con el botón derecho del ratón sobre los elementos y seleccionando *Change Condition* → *is*. Esto se debe hacer para todos los valores introducidos hasta el momento.

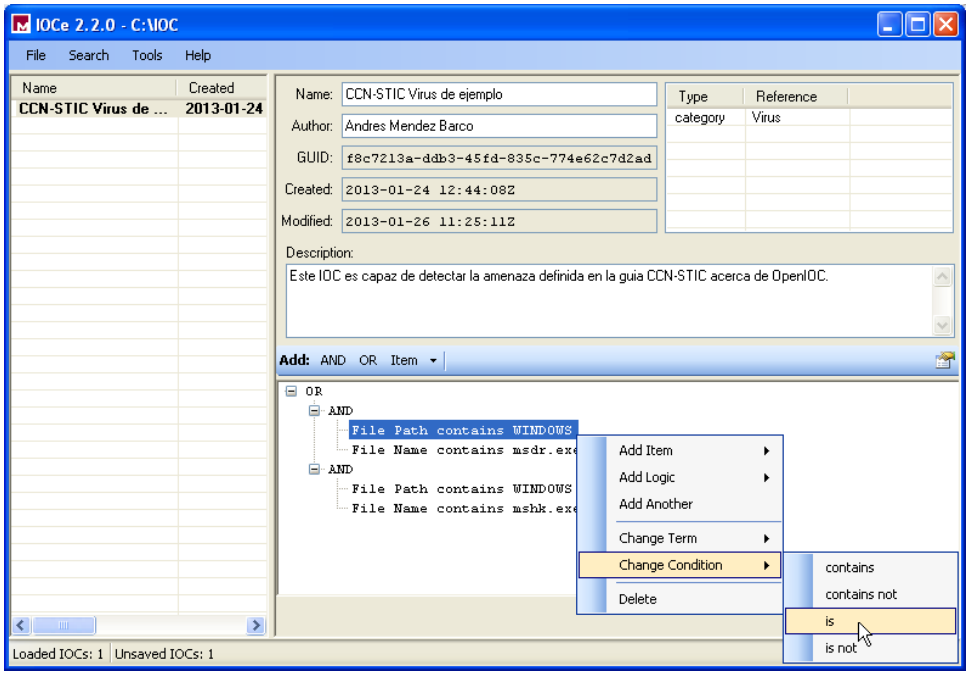


Figura 5. Cambio de la condición de un indicador en el IOC

58. A continuación, para buscar el indicador de la librería que empieza por "lib", seguida por números y con extensión .dll en el directorio *C:\WINDOWS\SYSTEM*, se añaden otros elementos bajo el "OR", como serán el nombre, la extensión y la ruta. Como todos deben darse al mismo tiempo, deben estar dentro de un "AND".

59. Dado que la librería aparece junto con uno de los ejecutables antes vistos, se deberá incluir ambos ejecutables dentro de un "OR", para que pueda ser uno u otro, a la vez que la librería.

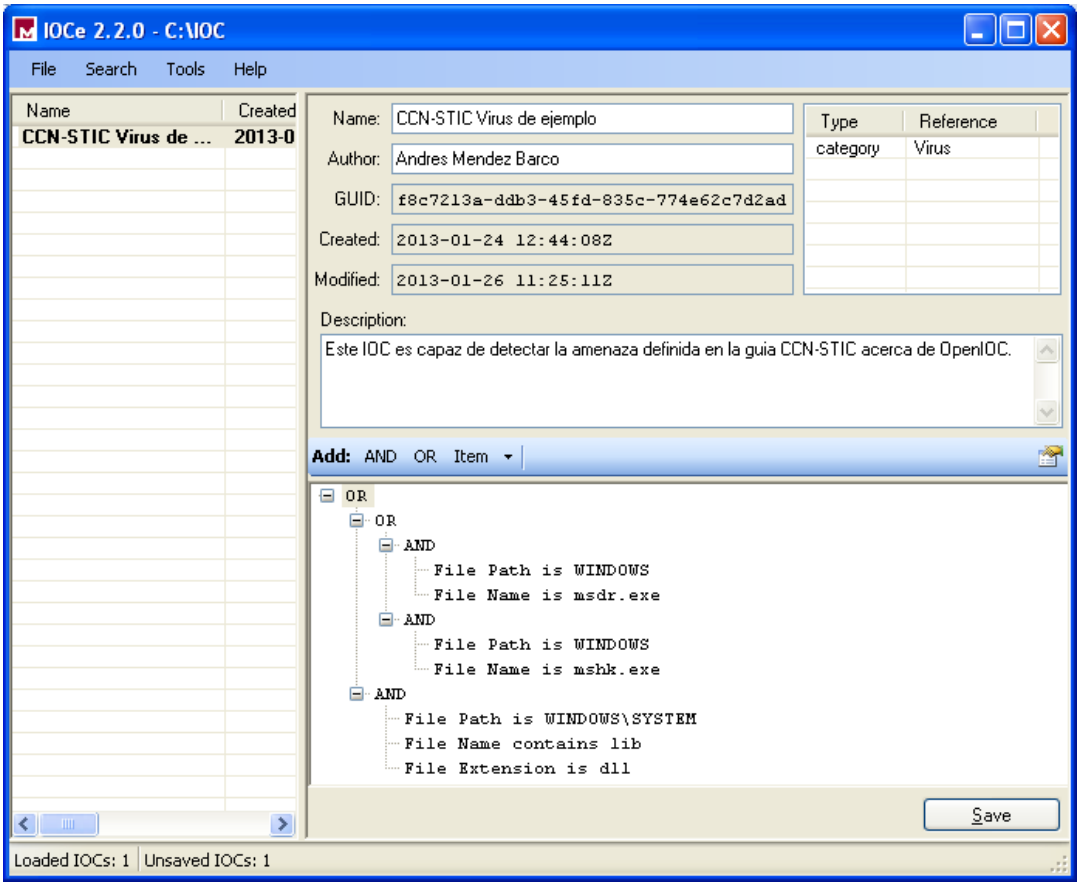


Figura 6. Ajuste de la lógica de los elementos

60. En siguiente lugar se define el indicador de compromiso que se encuentra en el registro de Windows. Para ello se creará otro grupo de elementos dentro de un "AND". Se empezará por especificar la ruta de la clave mediante *Item → RegistryItem → Registry Path*, introduciendo a continuación:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

61. La ruta exacta contendrá el nombre del valor, es decir, se representará como:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
\MSDriver
```

62. Por ese motivo se ajusta la condición a "contains".

63. Ahora se especifica la clave buscada con *Item → RegistryItem → Registry Value Name*, introduciendo el valor "MSDriver", con la condición ajustada a "is".

64. Por último hay que especificar el texto de la clave. Como el nombre del ejecutable puede ser uno de dos (msdr.exe o mshk.exe), habrá que crear una nueva rama lógica mediante

un "OR". Dentro se especifica el valor con *Item* → *RegistryItem* → *Registry Text*, introduciendo el valor "msdr.exe". Se ajusta la condición a "is" y se repite el proceso para el otro nombre del ejecutable.

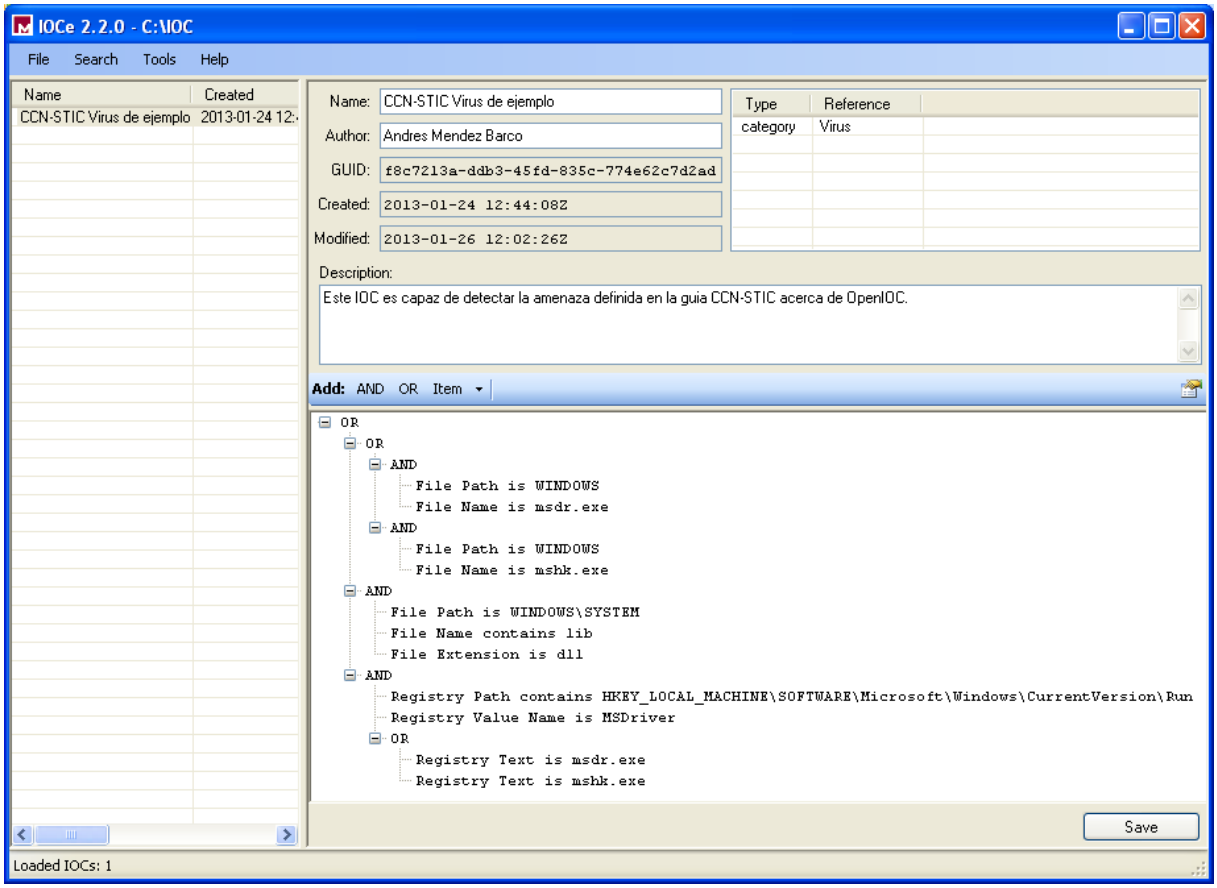


Figura 7. Adición de elementos del registro al IOC

65. Finalmente sólo queda especificar el nombre del proceso que reside en memoria. Ello se hace mediante *Item* → *ProcessItem* → *Process Name*. El valor será "MSDriver". Como puede ser uno de los dos nombres, se han de poner los valores entre "OR".

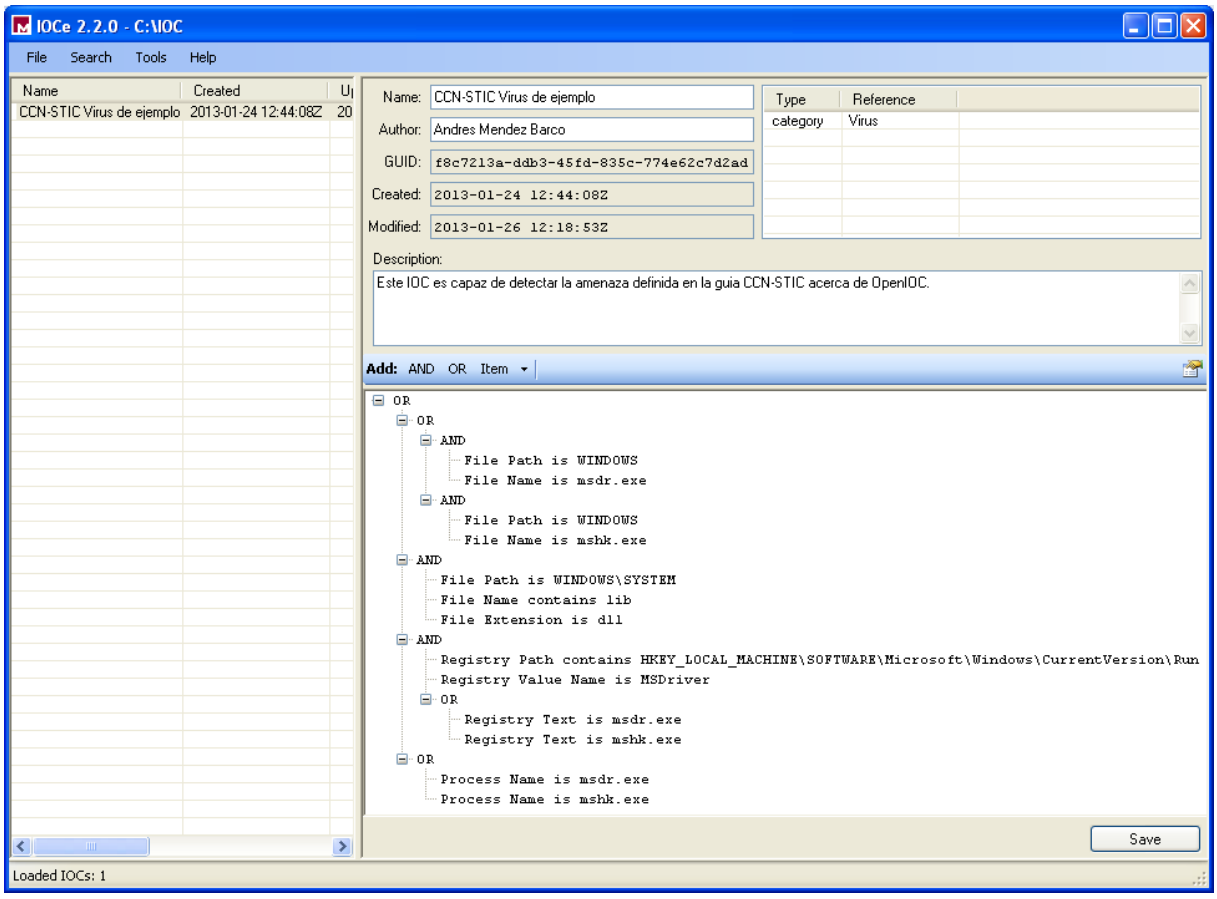


Figura 8. IOC resultante

66. Si en algún momento se quiere ver con más detalle alguno de los indicadores de compromiso definidos, o introducir un comentario sobre alguno de los indicadores, es posible hacerlo pulsando en el botón que aparece a la derecha, “Properties”. Se abrirá una nueva zona a la derecha que mostrará los detalles del indicador seleccionado. En el campo “Comment” se podrá introducir el comentario que se desee, a modo de recordatorio del porqué de algún elemento o valor, por ejemplo.

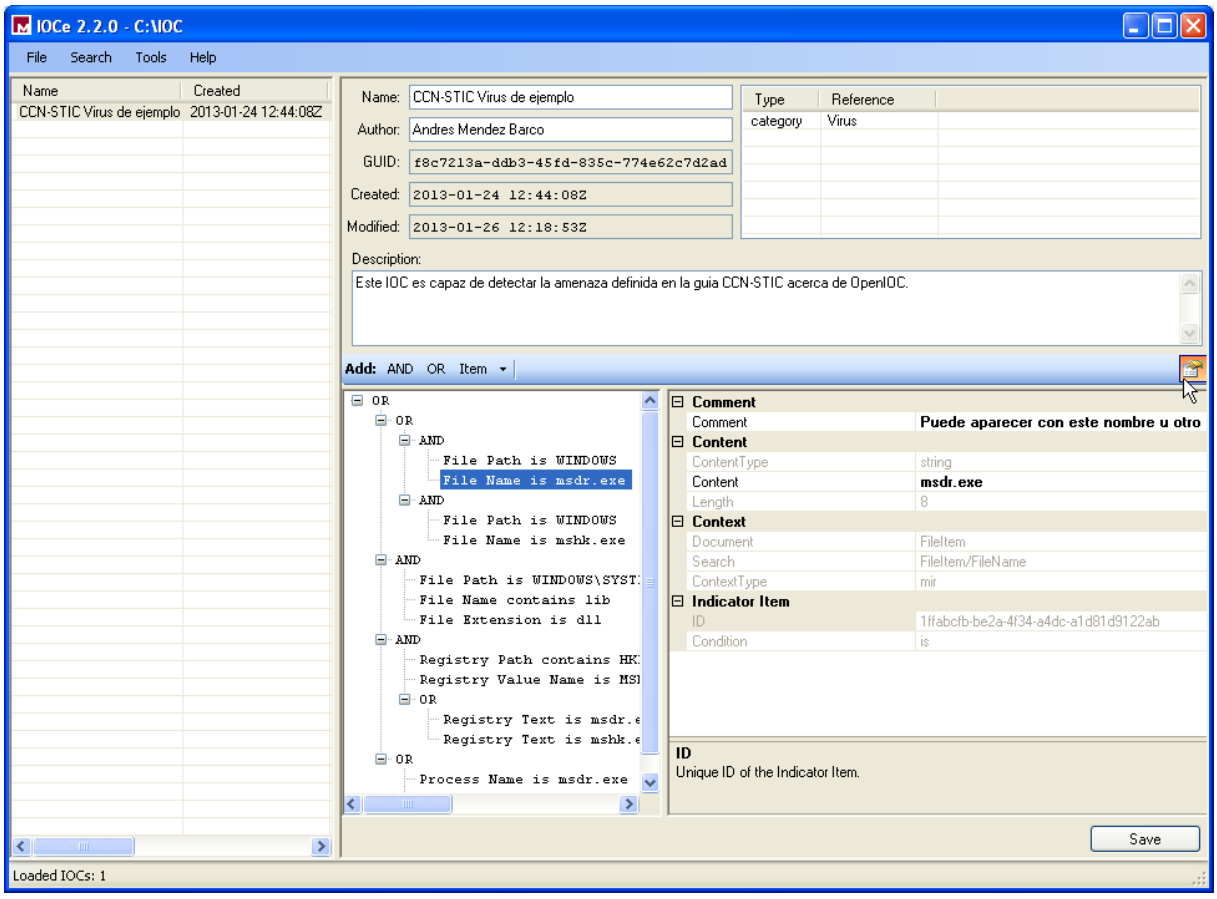


Figura 9. Introducción de un comentario en un IOC

67. Para guardar el IOC creado, pulse en "Save". Se guardará en el directorio seleccionado inicialmente, con el nombre de fichero que muestra en el campo "GUID" y la extensión ".ioc". En este ejemplo el fichero resultante es f8c7213a-ddb3-45fd-835c-774e62c7d2ad.ioc.

68. Por defecto, todos los indicadores creados cuelgan de una raíz que es "OR", lo que significa que si se identifica cualquiera de estos indicadores en el análisis a un sistema (tienen que darse las condiciones dentro de cada subrama "OR" o "AND" de las que se han definido), se generará un aviso indicando que, para este código dañino, se ha encontrado alguno de los indicadores de que el sistema ha sido comprometido.

69. Con esto, se ha visto sólo algunos de los múltiples elementos que se pueden añadir como indicadores de compromiso, aunque se ha explicado todo lo que se puede hacer con ellos. Por lo tanto, habiendo entendido estas bases, si se desea se pueden definir unos IOC tan complejos como sea preciso.

7.3.1. POSIBLES INDICADORES DE COMPROMISO A DEFINIR

70. Para conocer todos los elementos que se pueden definir, más de 500, se recomienda visitar http://schemas.mandiant.com/, donde se pueden encontrar los esquemas XML de todos los elementos que pueden emplearse (se recomienda consultar sólo aquellos marcados con el status "current", que corresponden a la última versión).

7.4. GESTIÓN DE FICHEROS IOC

71. Conviene tener todos los ficheros .IOC en una misma carpeta ya que de ese modo se pueden gestionar fácilmente desde el IOCe.

72. Una vez cargado el directorio con los IOC en el IOCe, éstos aparecerán a la izquierda. Para trabajar con ellos bastará con seleccionar el que se desee.

7.4.1. BÚSQUEDA DE UN IOC

73. En caso de tener muchos ficheros .IOC, para buscar alguno en concreto por su contenido, se puede hacer desde el IOCe mediante el menú *Search* → *Search for Keyword*.

7.4.2. BORRADO DE UN IOC

74. Para borrar un fichero .IOC, desde el propio IOCe se selecciona en el listado de la izquierda, pulsando con el botón derecho del ratón sobre él y seleccionando "Delete Indicator".

7.4.3. COMPARACIÓN DE DOS IOC

75. Si en alguna ocasión se tienen dos ficheros IOC y se duda de sean iguales o muy parecidos, se debe recurrir a la funcionalidad de comparación del contenido del IOC del IOCe, accesible mediante el menú *Tools* → *Compare Two IOCs*.

76. Esta acción abrirá una nueva ventana a la que se deben arrastrar los IOC cargados previamente en el IOCe. Una vez arrastrados, la herramienta los compara automáticamente, marcando en rojo aquello que es diferente.

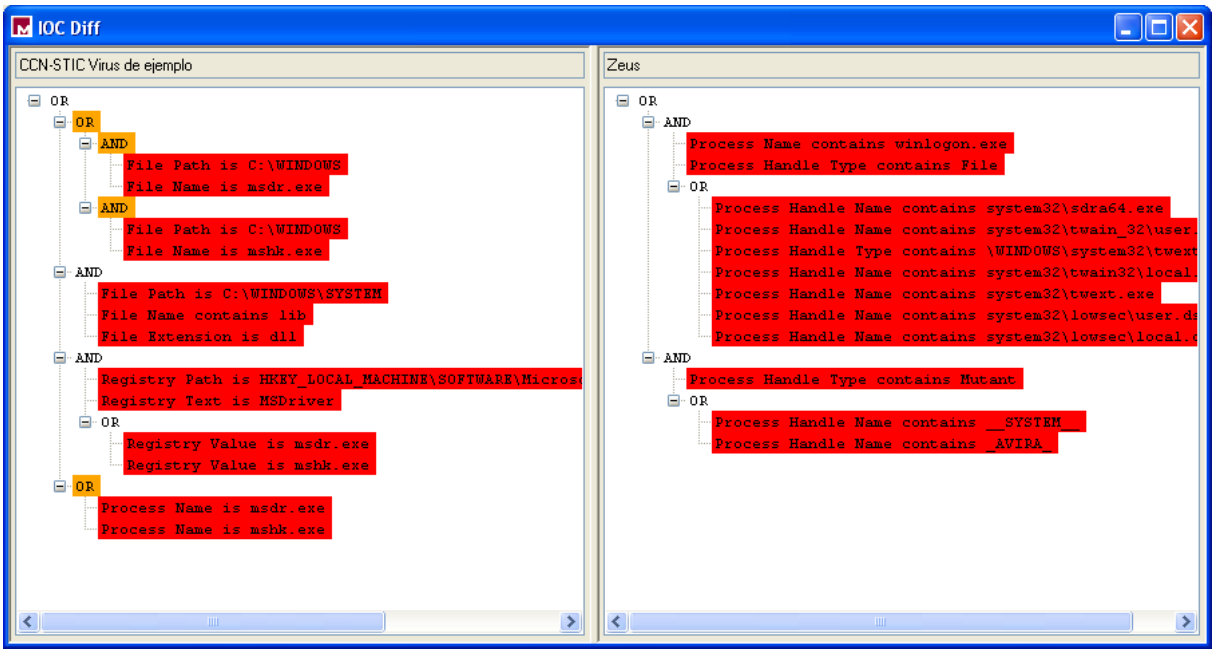


Figura 10. Comparación de dos ficheros IOC

8. IDENTIFICACIÓN DE IOC EN UN SISTEMA

77. Una vez se tienen los ficheros .IOC, que contienen los indicadores de compromiso a buscar en un sistema para saber si ha sido comprometido, llega el momento de analizar los sistemas a la búsqueda de dichos indicadores.

8.1. INSTALACIÓN DE MANDIANT IOC FINDER

78. Lo primero que se necesitará será una herramienta que extraiga de un sistema toda la información relevante que permita revelar si ha sido comprometido. Posteriormente, será necesaria otra herramienta que compare la información extraída del sistema con los indicadores de compromiso conocidos (definidos en ficheros .IOC).

79. Para hacer ambas cosas siguiendo el estándar OpenIOC con una misma herramienta, se hace uso del *IOC Finder* (IOCf) de Mandiant.

80. Esta herramienta está desarrollada para plataformas Windows y es de uso gratuito. Se puede obtener desde: https://www.fireeye.com/services/freeware/ioc-finder.html/

81. NOTA: Se ha utilizado el *IOC Finder* versión 1.0, de 31 de octubre de 2011, para elaborar esta guía.

82. La aplicación viene comprimida en un ZIP y bastará con descomprimirla para poder ejecutarla. Dado que se utilizará inicialmente esta herramienta para analizar un equipo que se sospecha comprometido, se recomienda ejecutar la aplicación en el equipo comprometido **desde una memoria USB**, para evitar alterar el sistema en análisis.

83. De cara también a que las evidencias generadas no alteren el sistema, por defecto se recomienda almacenarlas en la propia memoria USB. Para valorar la capacidad que deberá tener dicha memoria USB, las evidencias que se pueden obtener de un Windows XP Service Pack 3 recién instalado ocupan 228 Mb. Por lo tanto, se recomienda emplear una memoria USB con una capacidad mínima de 2Gb.

84. Existen dos directorios en el ZIP, x64 (para analizar sistemas con arquitectura de 64 bits) y x86 (para analizar sistemas con arquitectura de 32 bits). Bastará con copiar el fichero *mandiant_ioc_finder.exe* de la arquitectura del sistema a analizar a la memoria USB.

85. Dado que dicha memoria USB será introducida en un sistema posiblemente comprometido, es aconsejable que si posteriormente se conecta ésta a otro sistema, éste disponga de un antivirus que analice las unidades extraíbles, para evitar contagios.

86. En la memoria USB también se deberá copiar la carpeta con todos los ficheros .IOC de que se disponga, para poder realizar desde el USB tanto la recolección de evidencias como su posterior análisis.

8.2. RECOLECCIÓN DE EVIDENCIAS DE COMPROMISO

87. Se proceder a conectar la memoria USB preparada con el *IOC Finder* en el equipo del que se sospecha ha sido comprometido. Con permisos de administrador, se lanza una consola de MS-DOS: *Inicio* → *Ejecutar* → *cmd*

88. Se accede a la unidad del USB y se ejecuta la herramienta *IOC Finder*:

```
G:\> mandiant_ioc_finder.exe collect
```

89. La herramienta procederá a extraer información tanto volátil como no volátil del sistema de la unidad definida por *Windows %SYSTEMDRIVE%* (la unidad donde esté instalado

el sistema operativo) que sirva para identificar posteriormente si ha sido comprometido. Toda la información que extraiga se almacena en ficheros XML, uno por cada tipo de información (procesos en memoria, logs del sistema, cookies, etc.).

90. Dado que no se ha especificado ninguna ruta concreta, la herramienta almacenará dicha información en la memoria USB. Para ello creará un directorio "audits" en la misma ruta donde se encontrara el ejecutable *mandiant_ioc_finder.exe*. Dentro de ese directorio creará otro con el nombre del sistema analizado, por ejemplo "wxp_ejemplo". Dentro de ese directorio, creará otro compuesto por el año+mes+día+hora+minuto+segundo en que se lanzó la recolección. Por lo tanto, se guardarán las evidencias en:

```
G:\audits\WXP_EJEMPLO\20130125003948\
```

91. La colección de ficheros se almacena conforme al *MIR* (*MANDIANT Incident Response*) *Agent Local Data Collection*, es decir, la colección de datos generados por un agente local para la respuesta ante incidentes de Mandiant.

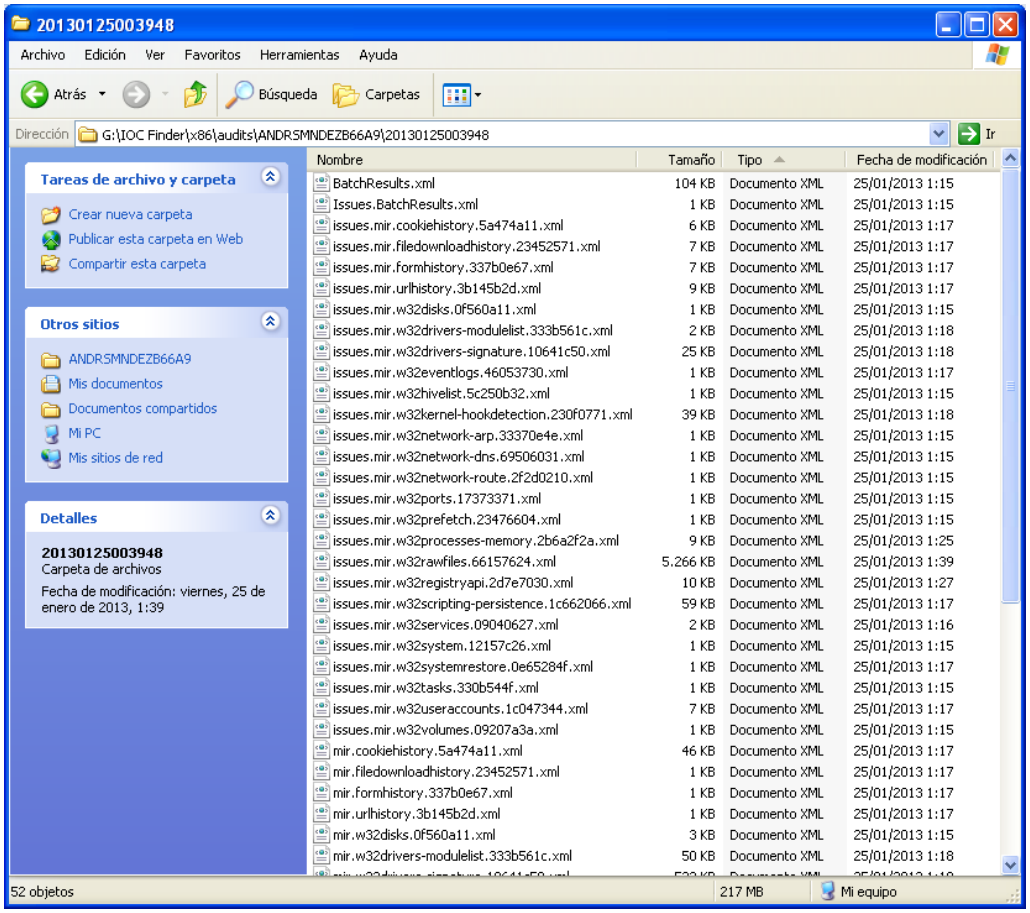


Figura 11. Ficheros de evidencias recopiladas por *IOC Finder*

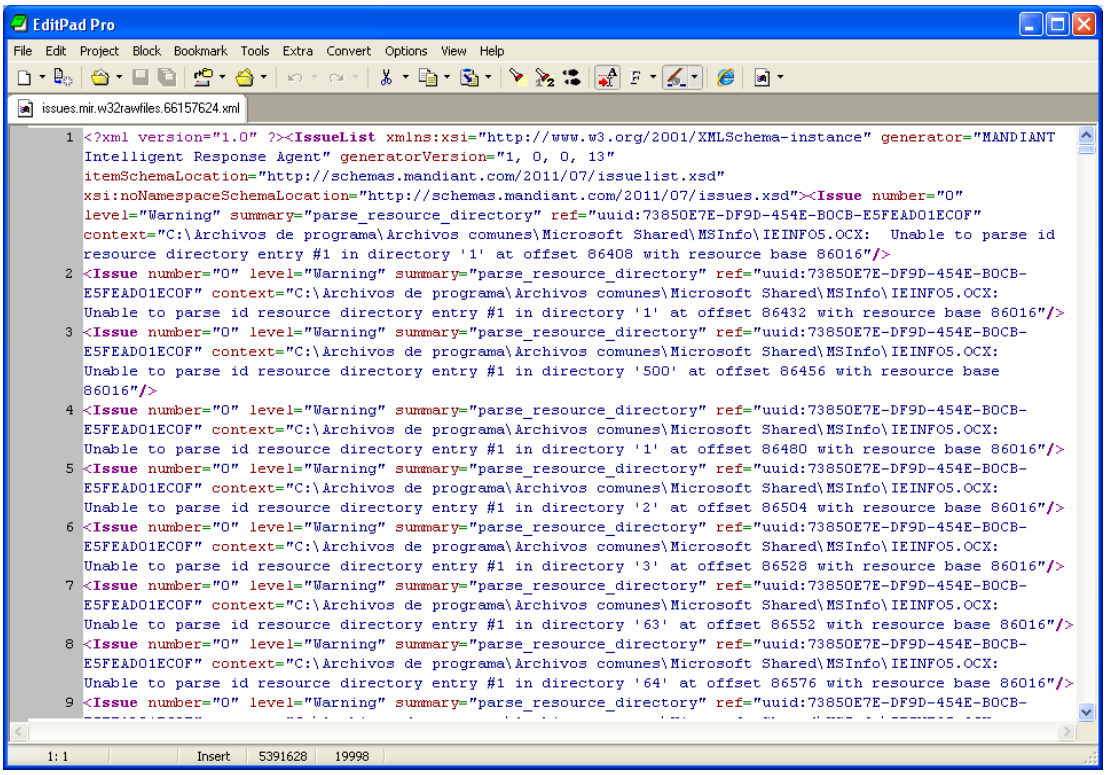


Figura 12. Contenido de uno de los ficheros de evidencias recopiladas por *IOC Finder*

92. Durante la recolección de evidencias no se recomienda utilizar el sistema. La duración de la recolección dependerá de la complejidad del sistema. Para disponer de un orden de magnitud, el tiempo que se requiere en obtener las evidencias de un sistema Windows XP Service Pack 3 recién instalado en un equipo de buenas prestaciones es de 26 minutos. Por norma general, en equipos en explotación la recopilación puede tardar varias horas.

93. Si se quiere almacenar las evidencias en otra ruta, por ejemplo "G:\evidencias" se indicará al ejecutar el *IOC Finder* mediante la opción "–o":

```
G:\> mandiant_ioc_finder.exe collect -o G:\evidencias
```

94. Para obtener las evidencias de otra unidad o de varias, por ejemplo "C:\" y "D:\", se ejecutará:

```
G:\> mandiant_ioc_finder.exe collect -d C: -d D:
```

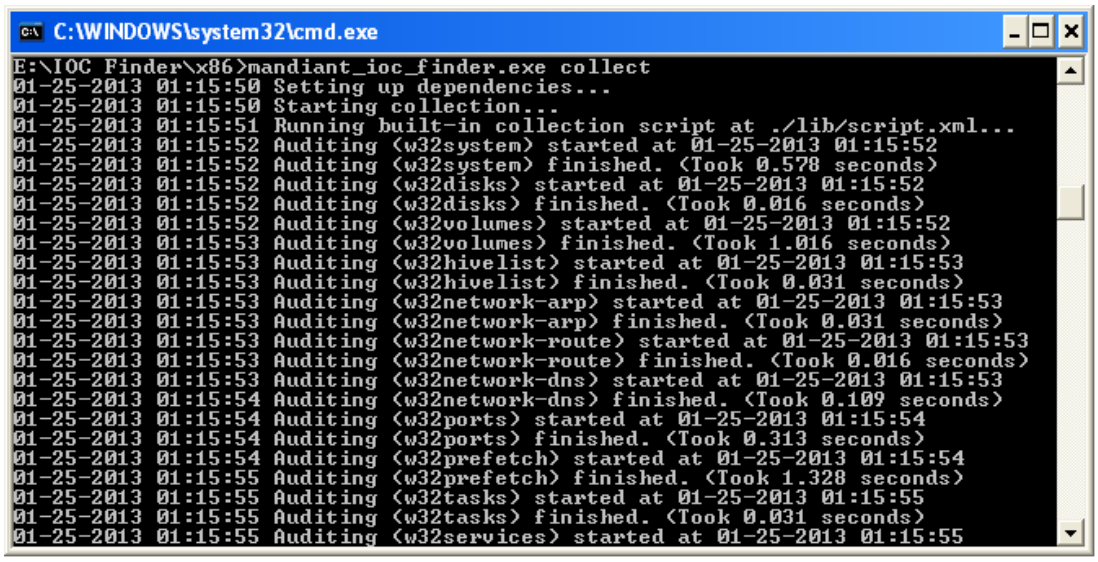


Figura 13. Ejecución del IOC Finder en modo de recolección de evidencias

95. Para detener la recolección, basta con pulsar *CTRL+C*. En ese caso se habrá generado un directorio dentro de "audits" llamado "tmp+año+mes+día+hora+minuto+segundo" con la información que llevaba recopilada hasta ese momento la herramienta.

8.3. ANÁLISIS DE EVIDENCIAS DE COMPROMISO

96. Una vez que el *IOC Finder* ha extraído las evidencias de un sistema, se deben analizar éstas para tratar de encontrar en ellas indicadores de compromiso. El resultado del análisis se pude almacenar tanto en formato HTML[14] o en un documento Word (en formato XML).

8.3.1. INFORME DE ANÁLISIS EN FORMATO HTML

97. El informe en HTML se genera de la siguiente forma desde la memoria USB preparada previamente:

```
G:\> mandiant_ioc_finder.exe report -i IOC -t html
```

98. Con el parámetro "-i" se indica la carpeta que contiene los ficheros IOC (en el ejemplo, en la misma ruta que el ejecutable). Con el parámetro "-t" se indica que el formato del informe sea HTML.

[14] HyperText Markup Language

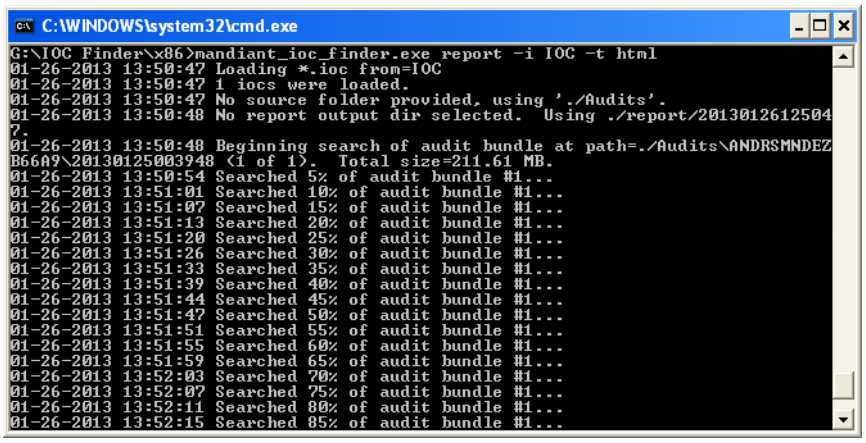


Figura 14. Ejecución del IOC Finder en modo de identificación de evidencias

99. Si identifica algún indicador de compromiso en el sistema analizado, *IOC Finder* lo mostrará de la siguiente forma: <fecha de la recolección>, <hostname o IP>, <IOC detectado>.

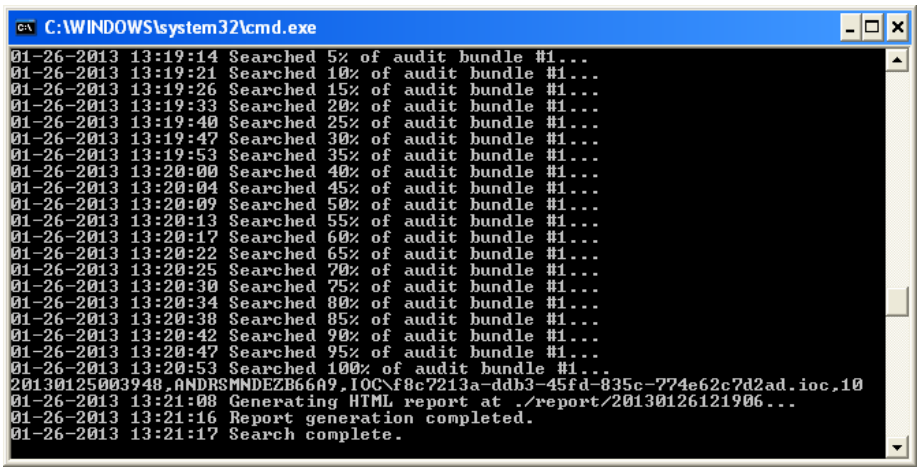


Figura 15. Detección de IOC en un sistema analizado

100. Dado que no se especificó ningún directorio de salida para el informe, el *IOC Finder* generará automáticamente la carpeta "report" en la misma ruta donde se haya ejecutado. Dentro de dicha carpeta se creará otra compuesta por el año+mes+día+hora+minuto+segundo en que se lanzó la generación del informe, donde se encontrará el fichero "index.html".

101. Si la recolección de evidencias estuviera en otro directorio, por ejemplo dentro de "G:\evidencias" (y ahí, a su vez, se encontrarían organizados por hosts, al igual que en el directorio por defecto "audits"), se indicaría con el parámetro "-s":

```
G:\> mandiant_ioc_finder.exe report -i IOC -t html -s G:\evidencias
```

102. El informe en HTML dispone, a la izquierda, de un menú para ver los resultados ordenados por sistemas ("View by Hosts") o por IOC ("View by Indicator").

103. En la vista por Host aparecerán aquellos sistemas (con su IP) donde se haya identificado alguno de los indicadores del IOC y, dentro de éste, los IOC donde haya habido algún positivo en un indicador.

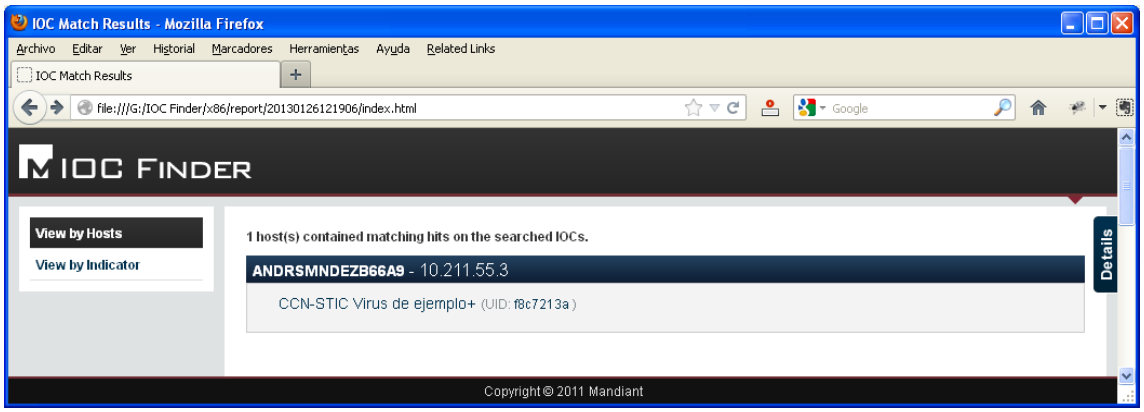


Figura 16. Sistema que ha dado positivo en un IOC

104. Al pulsar en el IOC, se desplegarán los indicadores identificados, agrupados por el fichero XML donde se haya identificado. Como cada fichero XML es de un conjunto de elementos del sistema, esto permite ver la información agrupada. En el ejemplo aparece agrupado por:

- Procesos en memoria: mir.w32**processes-memory**.2b6a2f2a.xml
- Ficheros del sistema: mir.w32**rawfiles**.66157624.xml
- Registro de Windows: mir.w32**registryapi**.2d7e7030.xml

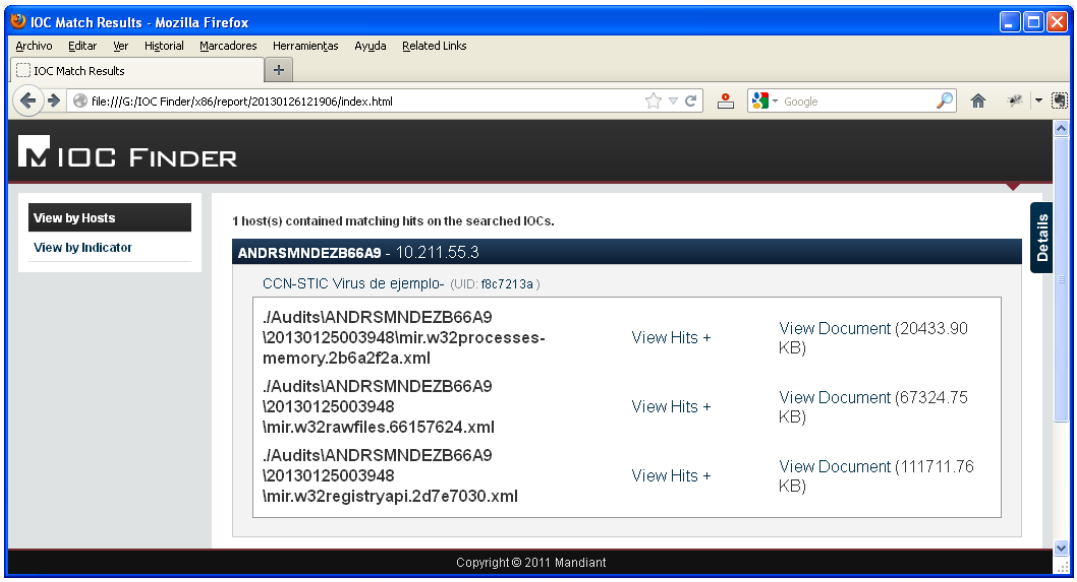


Figura 17. Elementos del sistema donde se han detectado positivos

105. Pulsando “View Hits +”, se mostrará exactamente qué es lo que se ha identificado como un indicador en dicho fichero de evidencias.

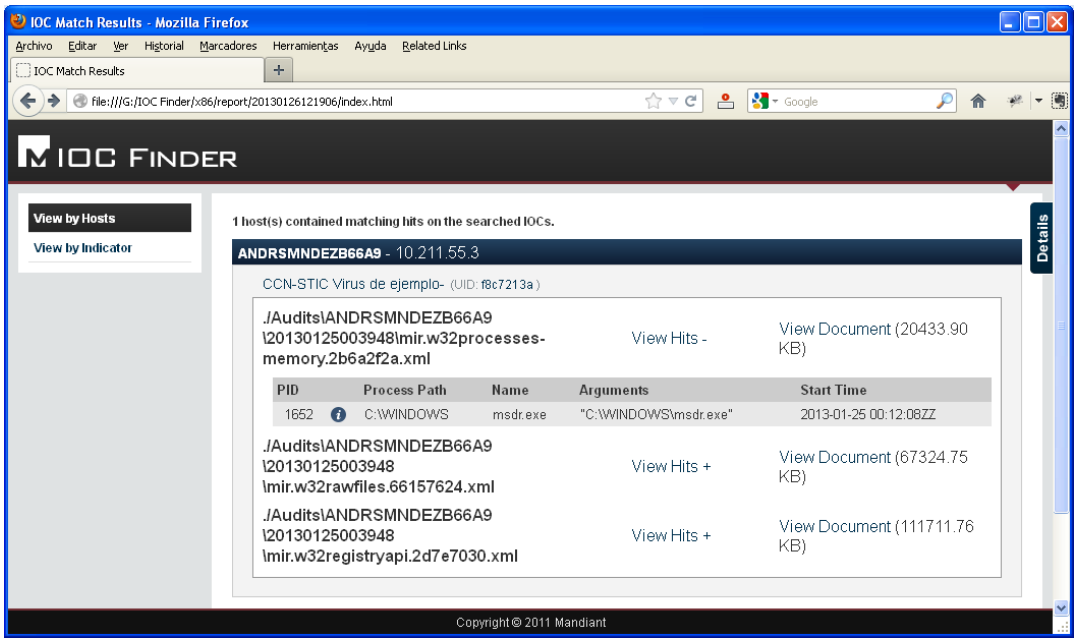


Figura 18. Indicador identificado en el sistema

106. Pulsando en  se despliega la pestaña "Details", donde se muestran más detalles sobre el indicador. En función del tipo de indicador del que se trate (un proceso, un fichero, etc.), así mostrará la información referente al mismo que obtuvo en el momento de la recolección.

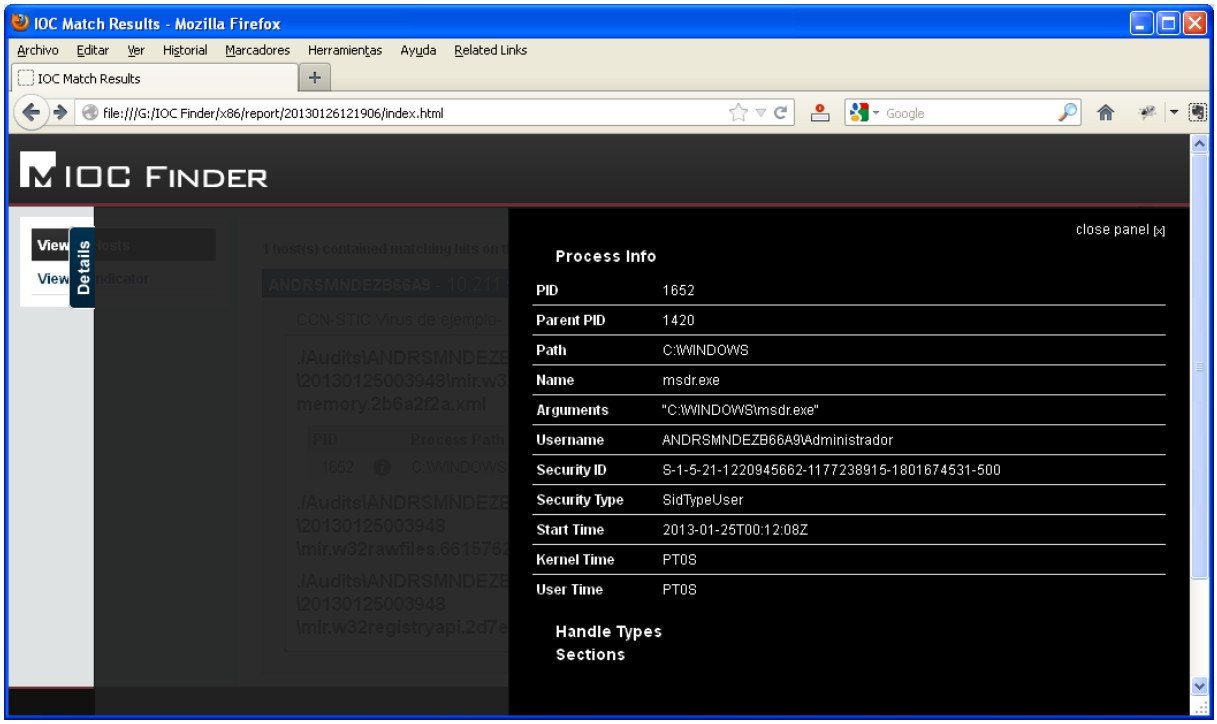


Figura 19. Detalles del indicador identificado en el sistema

107. Para obtener más detalles, en la zona inferior de la pestaña "Details", según el tipo de indicador del que se trate, pueden aparecer secciones con más detalle pulsando en ellas, como es el caso de "Handle Types" del ejemplo mostrado.

8.3.2. INFORME DE ANÁLISIS EN FORMATO WORD

108. Para obtener el informe resultante como un documento Word (en formato XML), se establece el parámetro "-t" como "doc":

```
G:\> mandiant_ioc_finder.exe report -i IOC -t doc
```

109. En ese caso, el informe resultante se guardará en la misma ruta donde se encuentre el *IOC Finder*, con nombre "report-[año+mes+día+hora+minuto+segundo en que se lanzó la generación del informe].doc.xml", que se podrá abrir con Microsoft Word.

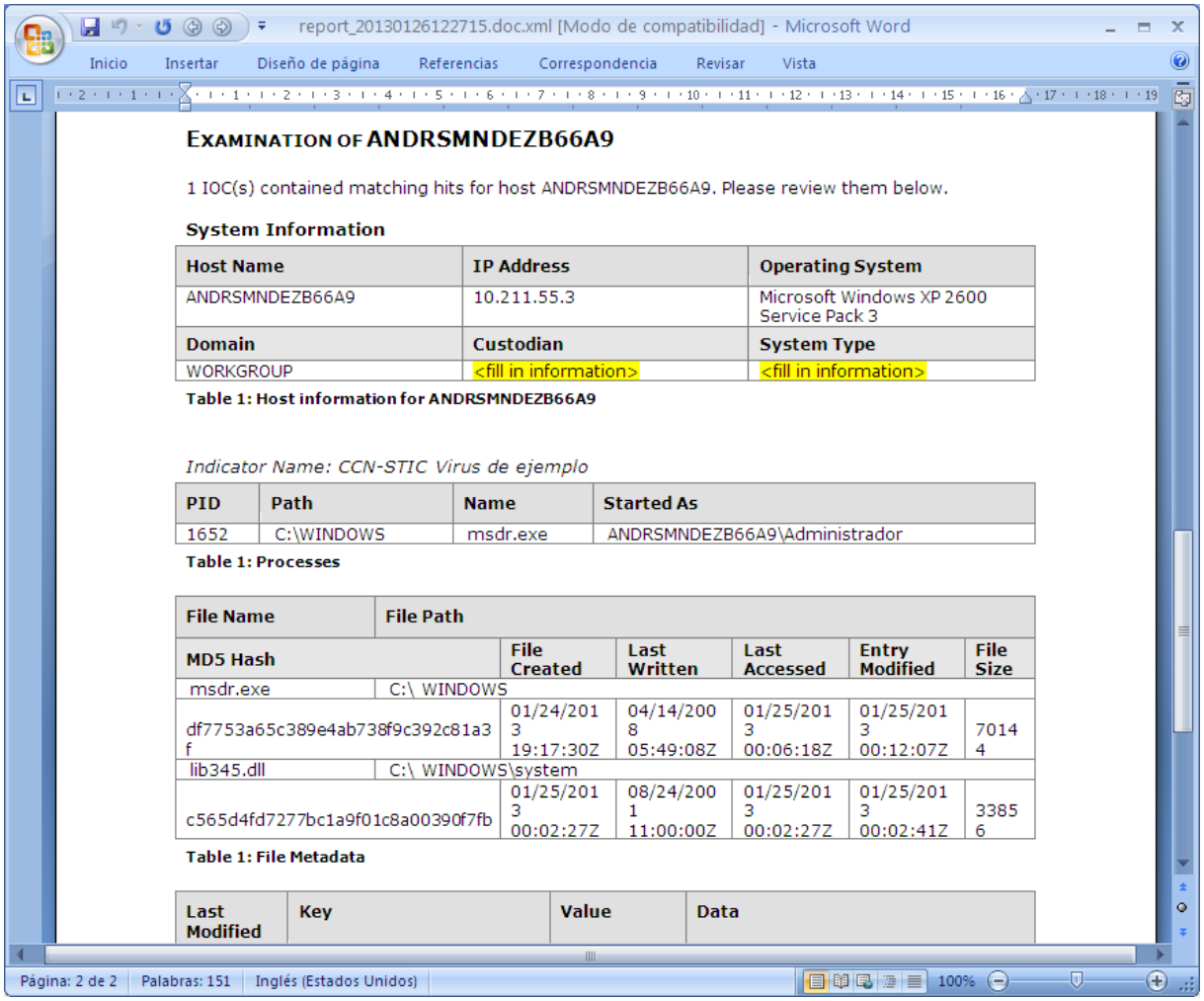


Figura 20. Ejemplo de un informe del IOC Finder en formato Word

110. El informe en formato Word es más ejecutivo y contiene menos información que el del formato HTML.

9. IDENTIFICACIÓN DE SITUACIONES ANÓMALAS EN UN SISTEMA

111. Existen diversas herramientas que permiten identificar situaciones anómalas en un sistema, que pueden denotar la existencia de código dañino o que el sistema haya sido comprometido. Una de estas herramientas, desarrollada por Mandiant y compatible con OpenIOC, es *Redline*.

112. Para poder aprovechar mejor las funcionalidades de los IOC y facilitar la detección de indicadores de compromiso, se explicará el uso de *Redline*. Un uso habitual de *Redline*, en combinación con las otras herramientas de Mandiant ya explicadas, sería algo similar a lo siguiente:

- Un usuario aprecia un comportamiento anómalo en su sistema, por lo que avisa a los responsables del mantenimiento de los sistemas;
- Éstos seguirán el protocolo establecido, que incluirá, en base al comportamiento identificado y que haga sospechar que el equipo ha sido comprometido, la ejecución de un agente de *Redline* en el equipo supuestamente comprometido para la recolección de evidencias;
- El resultado de la recolección será analizado en otro equipo mediante *Redline*;
- En base a los resultados del análisis, si se identifica que el equipo ha sido comprometido (en este paso se pueden haber utilizado más herramientas de análisis, si así lo establece el protocolo), se identificarán indicadores del compromiso y se plasmarán en un fichero .IOC mediante el *IOC Editor*;
- Ahora, con el fichero .IOC, se podrá generar mediante *Redline* un agente específico para buscar dichos indicadores, de forma que sea posible analizar el resto de equipos de la red que pudieran haber sido comprometidos también;
- Se analizará el resto de equipos de la red que pudieran haber sido comprometidos también, para comprobar el nivel del ataque y proceder a su limpieza.

113. Mandiant *Redline* permite buscar síntomas de actividad maliciosa en sistemas mediante el análisis de la memoria y los ficheros, pudiendo realizar análisis con mayor nivel de detalle incluyendo conexiones de red. *Redline* se puede ejecutar en el sistema sin necesidad de instalar nada en el mismo, evitando alterarlo. Es capaz de analizar los procesos en funcionamiento y los drivers en uso a un nivel inferior del que trabajan los *rootkits*[15] y otros tipos de código dañino, evitando sus técnicas de ocultación.

114. *Redline* se centra más en el análisis de la memoria que en el análisis del disco duro porque:

- En los equipos de sobremesa y servidores, la cantidad de memoria del sistema siempre es inferior a la capacidad de almacenamiento en el disco duro, lo que conlleva un análisis más rápido;
- Un código dañino debe estar en la memoria del sistema (del usuario o del kernel) para funcionar.

115. *Redline* es capaz de proporcionar un indicador de riesgo de código dañino o *Malware Risk Index* (MRI), para ayudar al investigador a centrarse en aquellos elementos del sistema que tengan más probabilidad de ser un código dañino.

116. Esta aplicación puede utilizarse para:

- Generar un agente que extraiga la información relevante del sistema para un análisis posterior, sin necesidad de instalar ni *Redline* ni dicho agente en el sistema posiblemente comprometido;

[15] Herramienta de código dañino que permite ocultar actividades ilegítimas en un sistema pudiendo el atacante actuar con nivel de privilegios de administrador

- Analizar las evidencias recolectadas previamente por un agente o por el *IOC Finder* y buscar en ellas indicadores de compromiso.

117. En ambos casos se debe instalar *Redline* en un equipo distinto del supuestamente comprometido.

118. Esta herramienta está desarrollada para plataformas Windows y es de uso gratuito. Se puede obtener desde: https://www.fireeye.com/services/freeware/redline.html

119. NOTA: Se ha utilizado *Redline* versión 1.7, de noviembre de 2012[16], para la elaboración de esta guía.

9.1. INSTALACIÓN DE MANDIANT REDLINE

120. La instalación de *Redline* requiere el framework Microsoft .Net v4.0, por lo que el programa redirigirá inicialmente, si dicho framework no se encuentra instalado, a la dirección web desde donde descargarlo.

121. La aplicación dispone de un instalador, por lo que su instalación es muy sencilla.

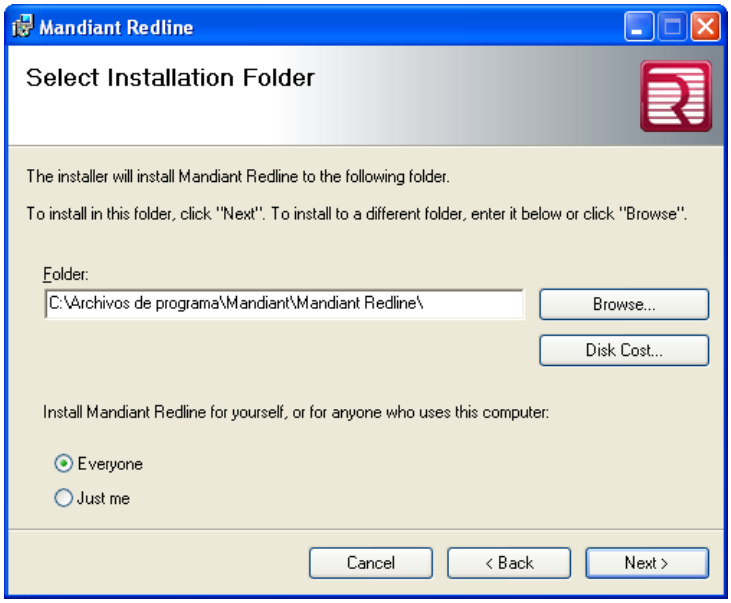


Figura 21. Instalación de Mandiant *Redline*

122. Una vez instalado *Redline* se debe actualizar su *whitelist*. La *whitelist* consiste en un listado de hashes (funciones resumen) de DLLs[17] y ejecutables confiables, obtenidos de *Microsoft Windows Server Update Service* y la *National Software Reference Library*. Se puede descargar la última versión de la *whitelist* desde la misma página desde la que se descargó *Redline*.

123. La *whitelist* está comprimida en un fichero .ZIP, que al descomprimirlo es un .TXT. Una vez ejecutado *Redline*, se deberá pulsar en su logotipo que se encuentra arriba a la izquierda.

[16] Versión actual Redline 1.14 de 12 de junio de 2015
[17] Dynamic Link Library Biblioteca de enlace dinámico.

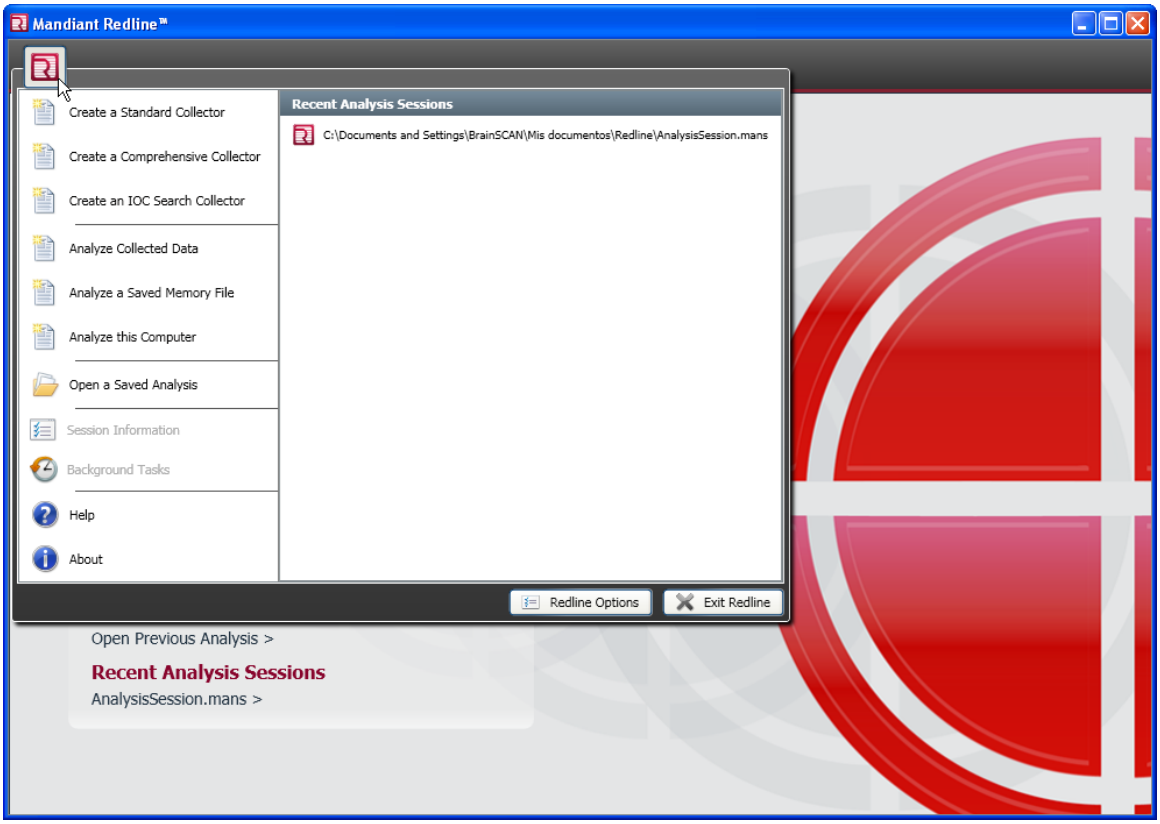


Figura 22. Configuración de *Redline*

124. Pulsando en "Redline Options" se accede a una nueva pantalla. Dentro del menú "General Configuration", se selecciona "Whitelist Management".

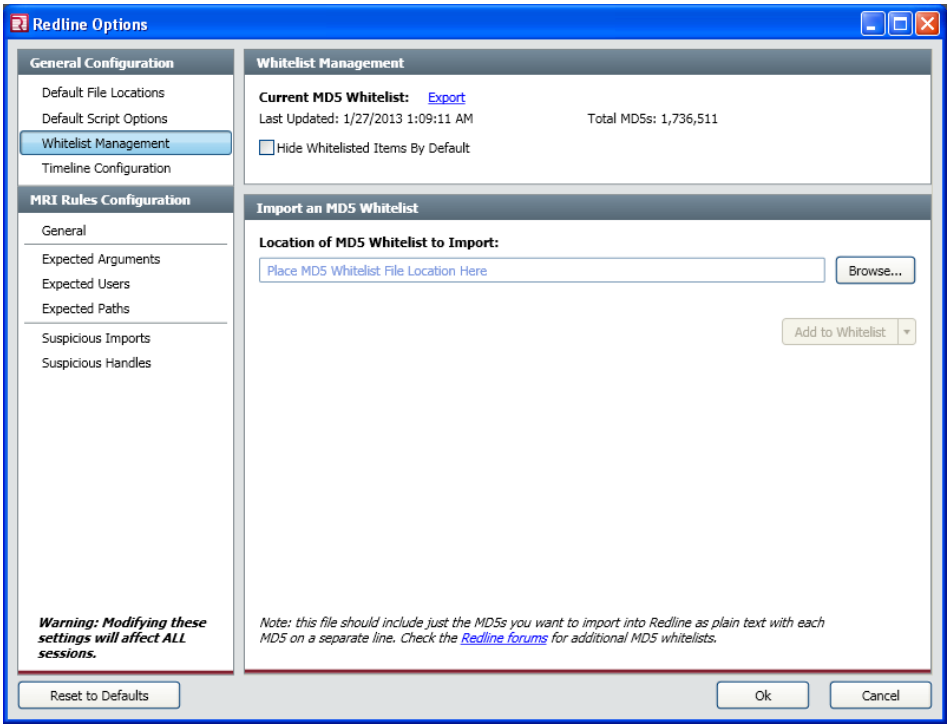


Figura 23. Actualización de la whitelist de Redline

125. A continuación, hay que pulsar en "Browse", seleccionar el fichero .TXT descomprimido y pulsar "Abrir". Se habilitará un botón que indica "Add to Whitelist", aunque se deberá pulsar en el desplegable a la derecha y seleccionar "Replace Whitelist", para reemplazar la lista blanca actual por la nueva que es más completa y está más actualizada.

126. Otro elemento a configurar es el antivirus, si es que el sistema donde se ha instalado *Redline* y donde se van a realizar los análisis de las evidencias de los sistemas posiblemente comprometidos dispone de uno (ya se recomendó anteriormente que se disponga de un antivirus en el equipo de análisis).

127. Durante el análisis que *Redline* es capaz de hacer de las evidencias, puede extraer código dañino de las imágenes de la memoria, y lo almacena en un espacio temporal. Este espacio temporal (una vez que *Redline* obtiene el código dañino lo almacena en un fichero ZIP protegido mediante contraseña) se puede ver mediante *General Configuration → Default File Locations → Default Unsafe Acquisition Staging Location*. Es necesario configurar el antivirus para que excluya ese directorio de su análisis en tiempo real y bajo demanda. También, para evitar la posible ejecución fortuita de un código dañino que hubiera en ese directorio, se puede configurar una Política de Restricción de Software[18] (*AppLocker* si utiliza Windows 7) para evitar la ejecución de aplicaciones en ese directorio.

128. El equipo donde se analicen las evidencias, aunque éstas sean cargadas desde una memoria USB, necesitará, como mínimo, el espacio que dicho análisis ocupa en la memoria USB libre en el disco duro. En la siguiente pantalla de configuración de *Redline* se pueden ver los directorios donde trabaja de manera temporal la herramienta, "Default Audit Location" y "Default Acquisition Location", por lo que si se necesitase utilizar una unidad diferente a la estándar (que será *C:\Documents and Settings\[nombre de usuario]\Configuración local\Temp*) se deberá modificar en esta pantalla.

[18] Consultar la guía CCN-STIC-503A "Seguridad en Windows 2003 Server (Controlador de Dominio)", apartado 11.1.

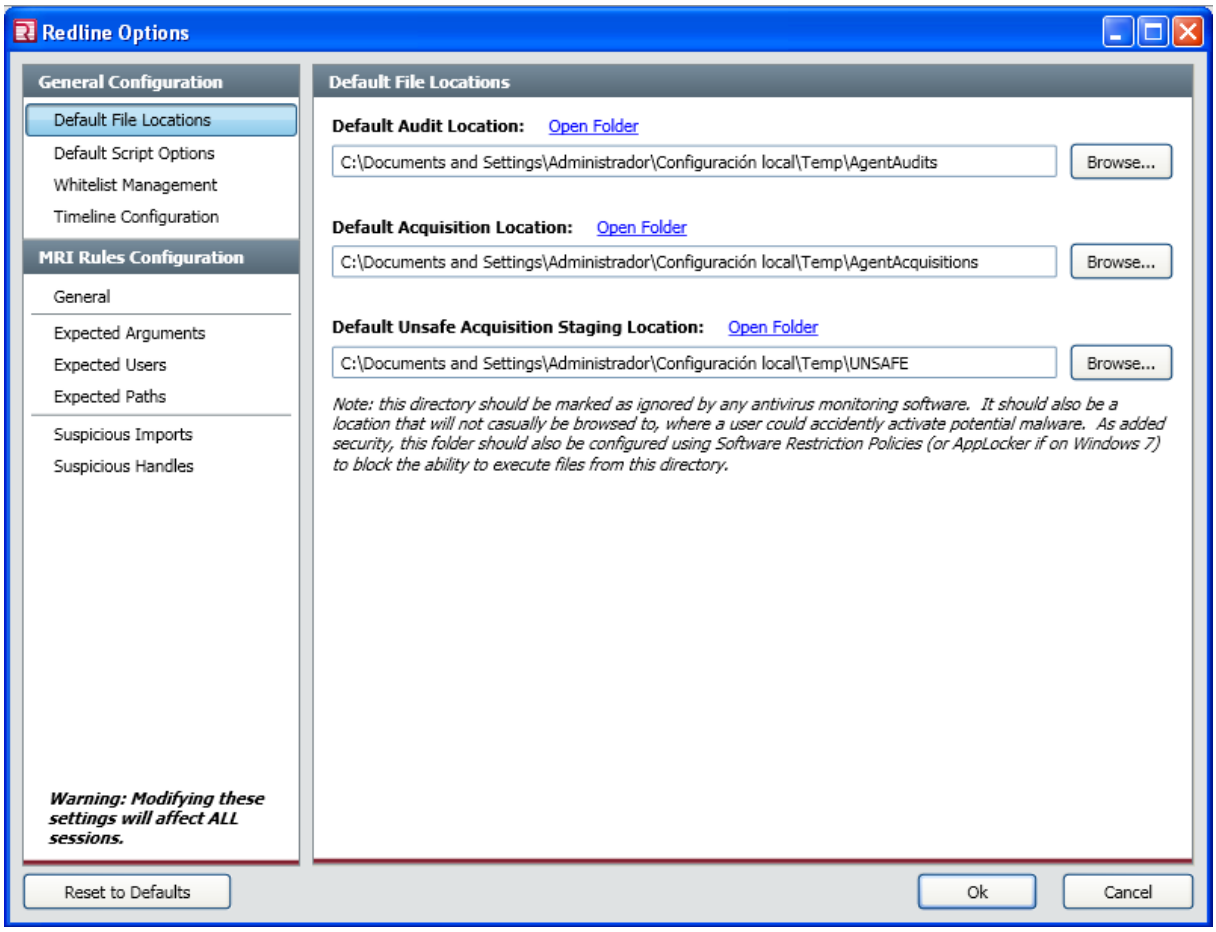


Figura 24. Configuración de directorios temporales *Redline*

129. Para conocer o ajustar los elementos que *Redline* utiliza a la hora de establecer el MRI, consulte, dentro de "Redline Options", el menú "MRI Rules Configuration".

9.2. RECOLECCIÓN DE EVIDENCIAS DE COMPROMISO

130. *Redline* es capaz de recolectar evidencias de un compromiso, de forma semejante a como lo hace *IOC Finder*. Como añadidura, es capaz de especificar en cada caso cuánta información y de qué tipo se quiere recopilar, en función del tipo de análisis posterior que se quiera realizar.

131. En los siguientes apartados se explican las formas de configurar un agente de recolección de evidencias, en función del tipo de análisis posterior que se quiera realizar.

9.2.1. CREACIÓN DE UN RECOLECTOR DE DATOS ESTÁNDAR

132. Para generar un agente (*MIR Agent*) que recolecte los datos necesarios para que *Redline* pueda detectar situaciones anómalas en un sistema se utilizará la opción *Collect Data → Create a Standard Collector*.

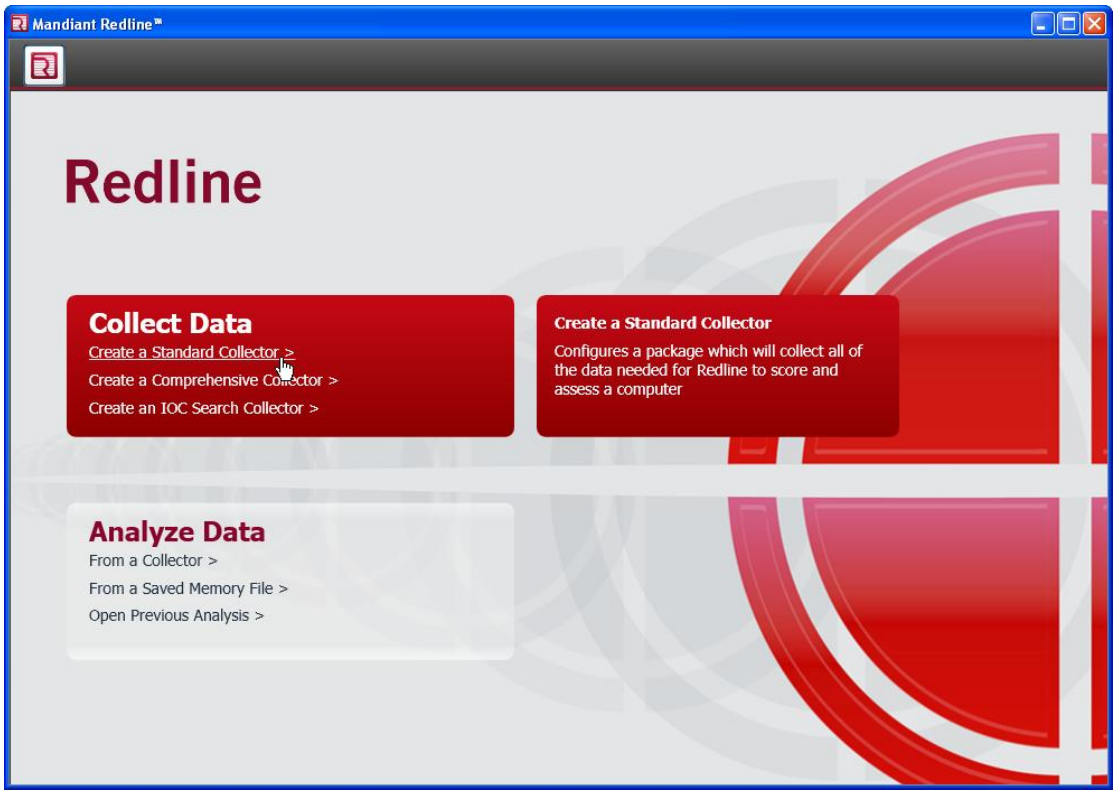


Figura 25. Opción para crear un agente de recolección estándar

133. Aparecerá una nueva ventana, desde la que es posible realizar distintas acciones.

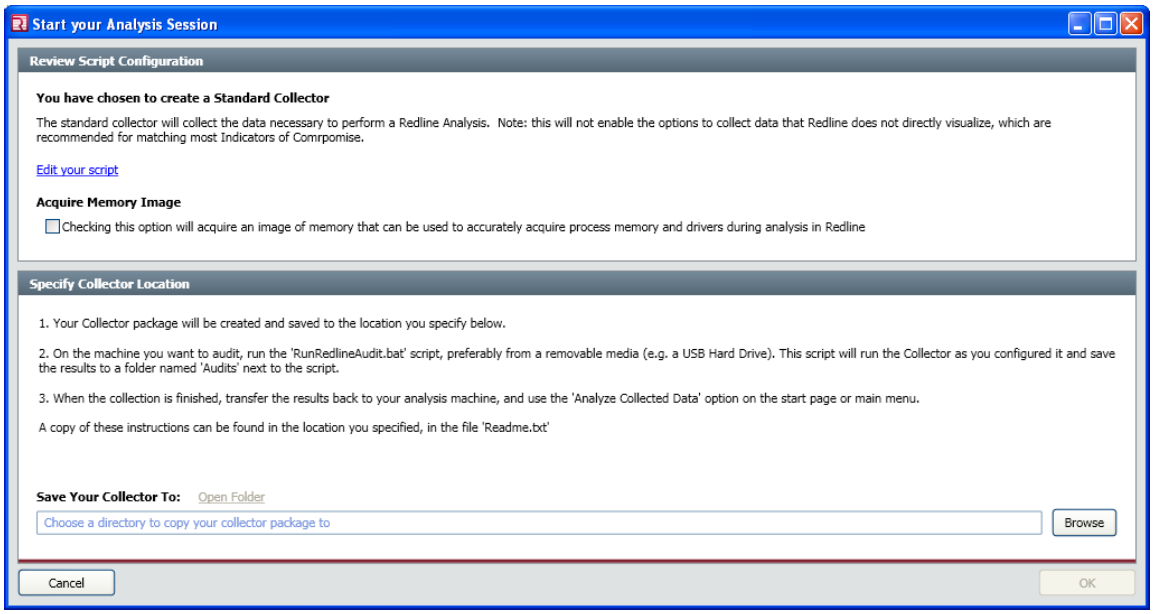


Figura 26. Ajustes del agente de recolección estándar

134. Por un lado se puede ajustar más todavía los elementos que interesa recopilar (aunque no debería ser necesario) para que luego *Redline* sea capaz de identificar situaciones anómalas. Para ello, pulse en "Edit your script". En la nueva ventana, aparecerá marcada la información que *Redline* necesita que se recopile del sistema cuando se analice por el

agente. A través de las distintas pestañas y casillas se podrá marcar o desmarcar lo que se considere relevante para el posterior análisis.

135. Marcando la casilla "Show Advanced Parameters" se podrán definir incluso más detalles.

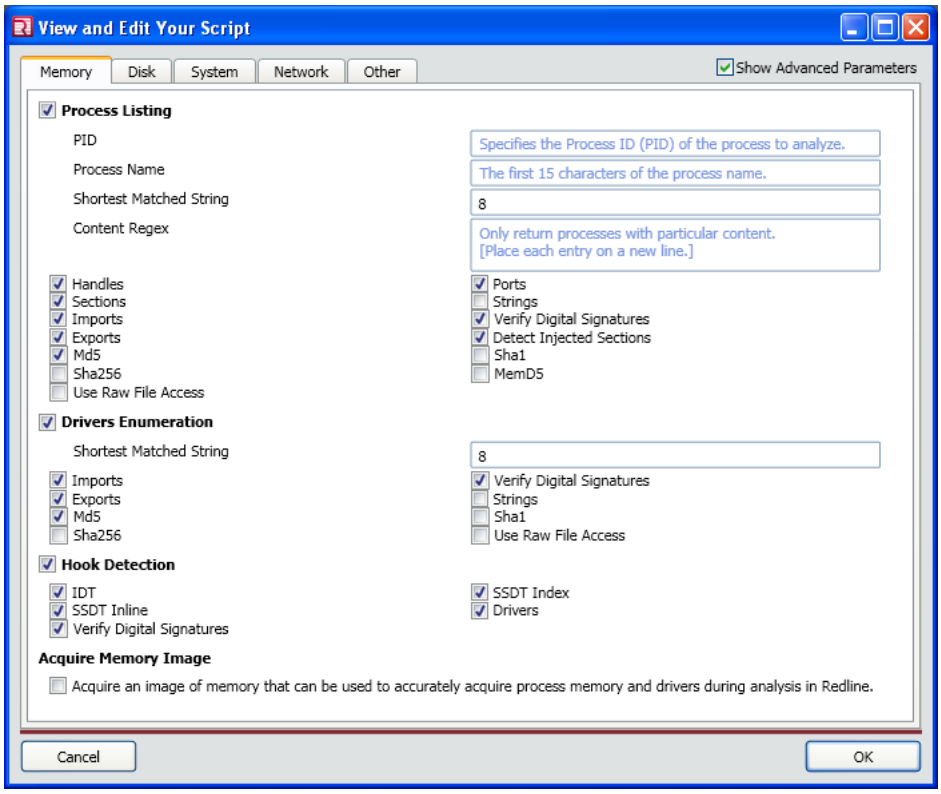


Figura 27. Edición del script del agente de recolección estándar

136. Una vez terminada la revisión o el ajuste de los datos a recopilar, pulse "OK".

137. En caso de querer que el agente obtenga una imagen de la memoria, para un posterior análisis más concienzudo, se deberá marcar la casilla bajo "Acquire Memory Image". Hay que tener en cuenta que esto generará un fichero tan grande como la memoria en uso del sistema a analizar, por lo que la unidad de almacenamiento de las evidencias tendrá que tener espacio libre suficiente.

138. Por otro lado hay que seleccionar en qué directorio vacío se va a guardar el agente, pulsando el botón "Browse". Se recomienda, al igual que en el caso del *IOC Finder*, que se almacene en una memoria USB, que será la que luego se conecte al equipo posiblemente comprometido.

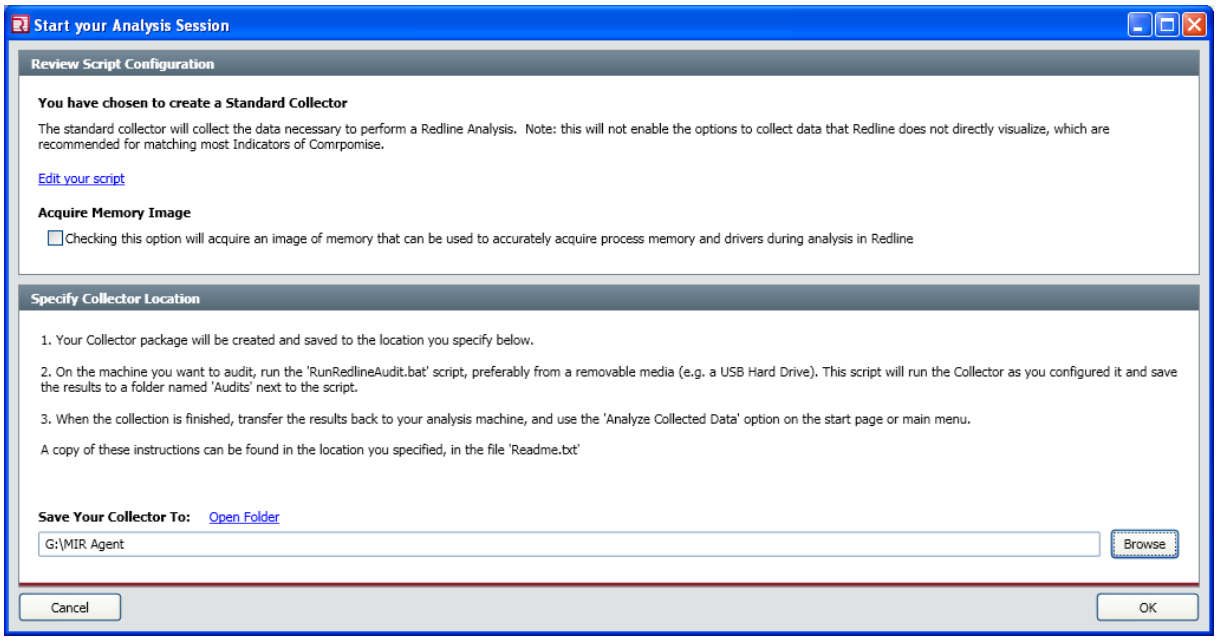


Figura 28. Terminando de configurar el agente de recolección estándar

139. Hecho todo esto bastará pulsar "OK" para que se generen los scripts y se copien los ejecutables al directorio indicado.

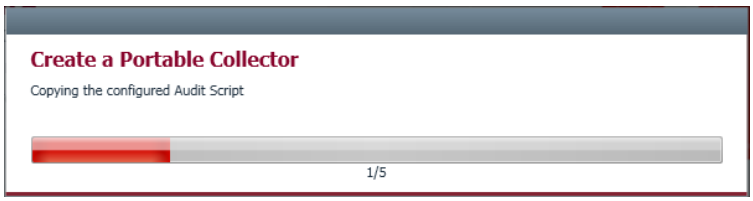


Figura 29. Copiándose el agente de recolección estándar a la memoria USB

140. Una vez se hayan terminado de copiar los datos a la memoria USB, aparecerá una ventana con unas instrucciones de uso.

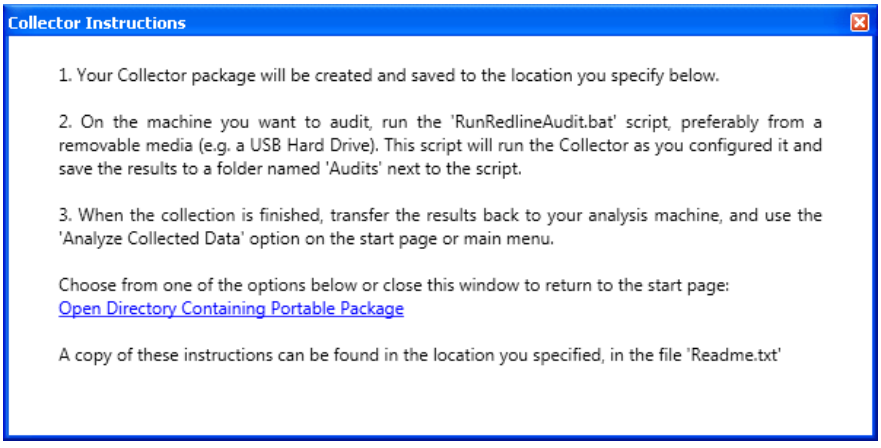


Figura 30. Instrucciones sobre de uso del agente de recolección estándar

141. Ahora que se dispone de una memoria USB con el agente de recolección estándar preparado, para ejecutarlo bastará conectar la memoria USB al equipo posiblemente comprometido, ir al directorio donde está el agente y ejecutar "RunRedlineAudit.bat". Esta acción abrirá una consola del sistema que recolectará toda la información pertinente y la almacenará en la ruta desde la que se ha ejecutado el agente, dentro de la carpeta "Audits". Al estar usando una memoria USB significa que se guardará en dicha memoria, de forma similar a cuando se usa el *IOC Finder*. Una vez que haya terminado de recolectar la información, se cerrará la consola.

9.2.2. CREACIÓN DE UN RECOLECTOR DE DATOS COMPLETO

142. Para generar un agente (*MIR Agent*) que recolecte los datos necesarios para que *Redline* pueda detectar situaciones anómalas y para que se puedan identificar indicadores de compromiso en un sistema, es emplea la opción *Collect Data* → *Create a Comprehensive Collector*.

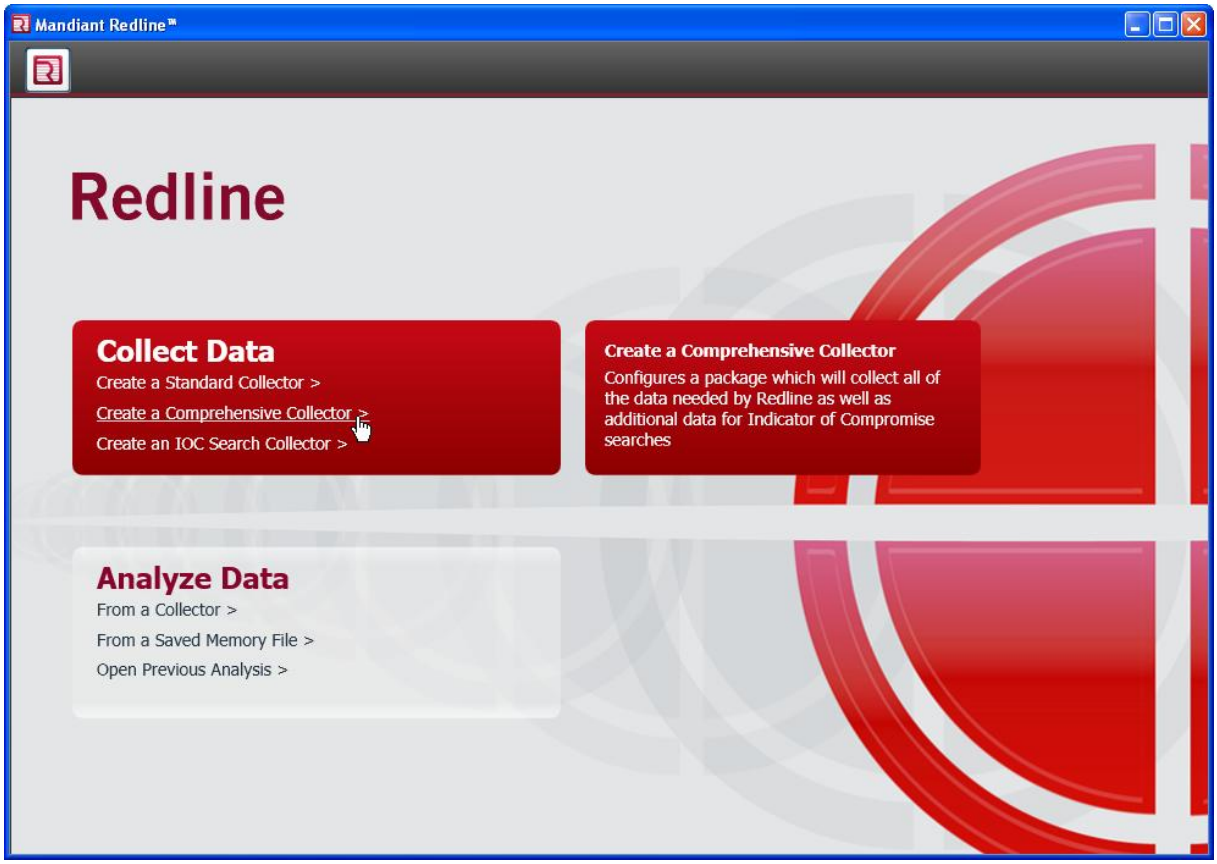


Figura 31. Opción para crear un agente de recolección completo

143. Aparecerá una nueva ventana, ofreciendo diversas opciones.

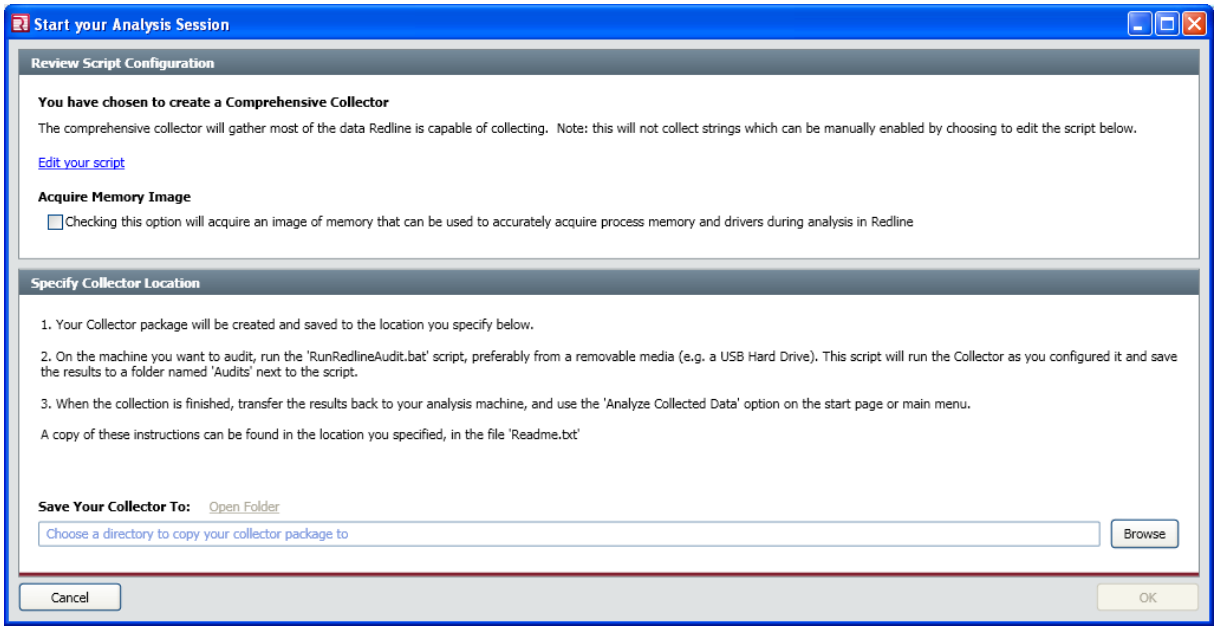


Figura 32. Ajustes del agente de recolección completo

144. Por un lado es posible ajustar más todavía los elementos que interesa recopilar (aunque no debería ser necesario, ya que por defecto están marcadas la mayoría de opciones). Para ello, se debe pulsar en "Edit your script". En la nueva ventana, aparecerá marcada la información que *Redline* necesita que se recopile del sistema, y la información que normalmente se necesita para ser analizado mediante un IOC. A través de las distintas pestañas y casillas se puede marcar o desmarcar lo que se considere relevante para un posterior análisis.

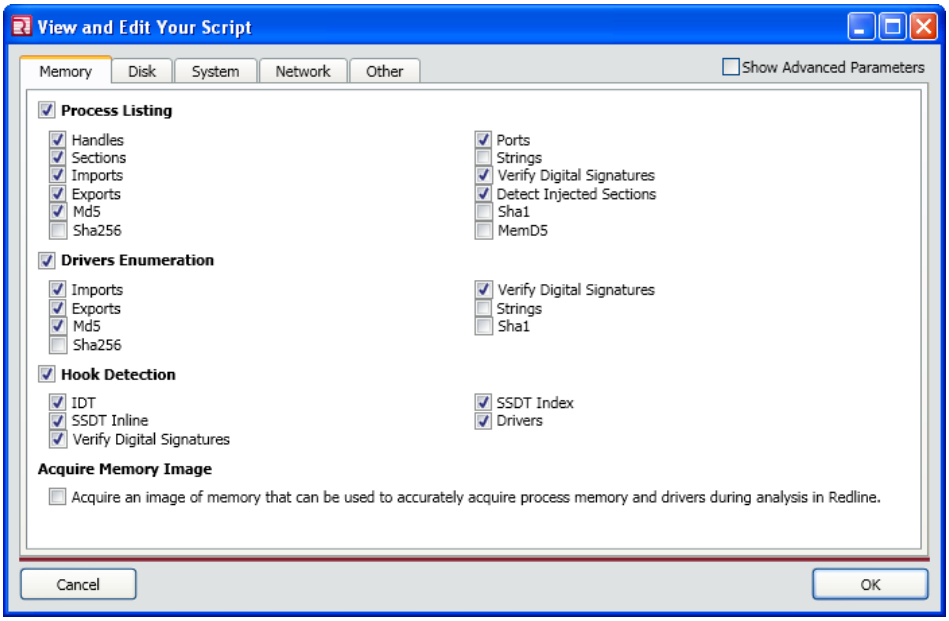


Figura 33. Edición del script del agente de recolección completo

145. La casilla "Show Advanced Parameters" permitirá definir incluso más detalles.
146. Una vez terminada la revisión o el ajuste de los datos a recopilar, pulse "OK".

147. En caso de querer que el agente obtenga una imagen de la memoria, para un posterior análisis más concienzudo, se deberá marcar la casilla bajo "Acquire Memory Image". Hay que tener en cuenta que esto generará un fichero tan grande como la memoria en uso del sistema a analizar, por lo que la unidad de almacenamiento de las evidencias tendrá que tener espacio libre suficiente.

148. Por otro lado hay que seleccionar en qué directorio vacío se va a guardar el agente, pulsando el botón "Browse". Se recomienda, al igual que en el caso del *IOC Finder*, que se almacene en una memoria USB, que será la que luego se conecte al equipo posiblemente comprometido.

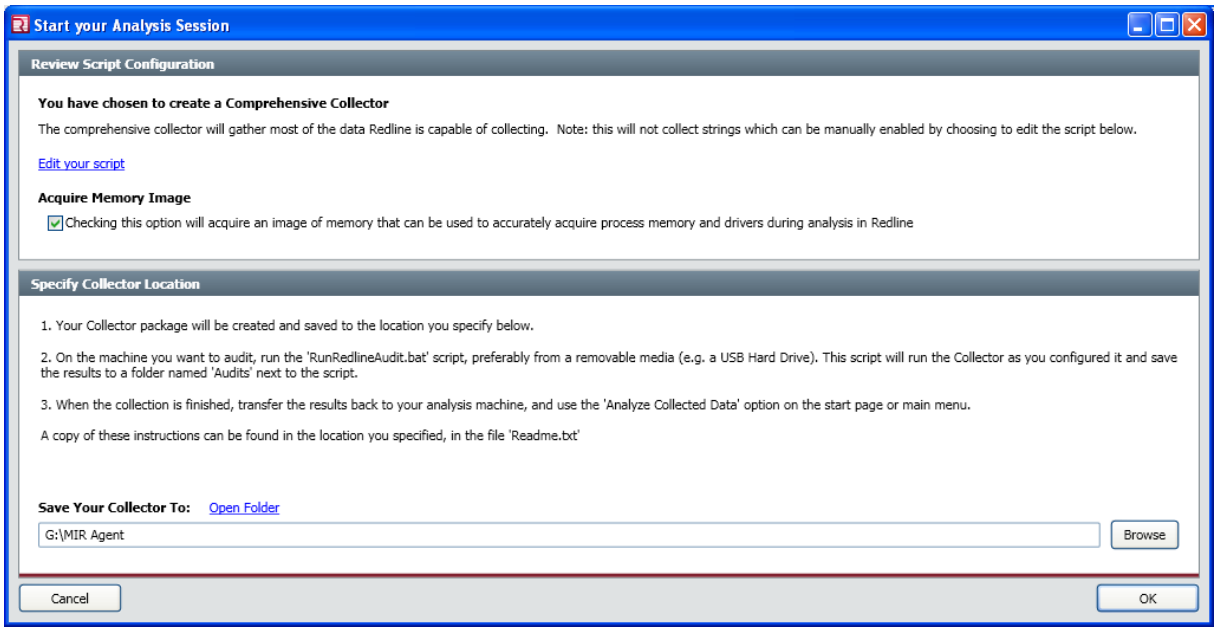


Figura 34. Terminando de configurar el agente de recolección completo

149. Hecho todo esto bastará pulsar el "OK" para que se generen los scripts y se copien los ejecutables al directorio indicado.

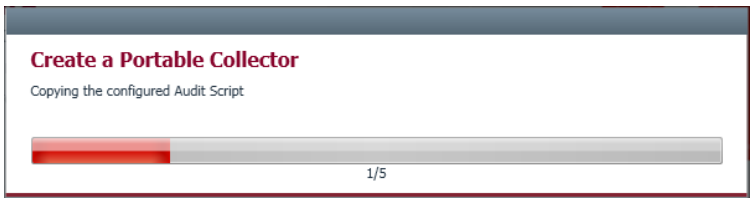


Figura 35. Copiado del agente de recolección completo a la memoria USB

150. Una vez que se hayan terminado de copiar los datos a la memoria USB, aparecerá una ventana con unas instrucciones de uso.

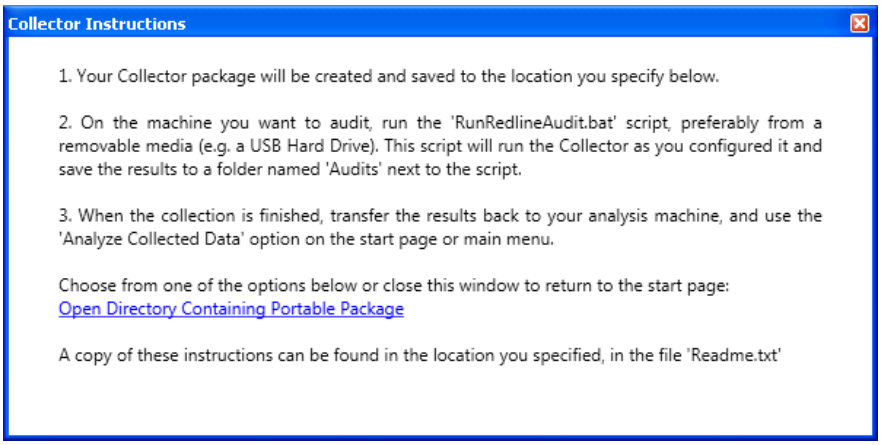


Figura 36. Instrucciones sobre de uso del agente de recolección completo

151. Ahora que se dispone de de una memoria USB con el agente de recolección completo preparado, para ejecutarlo bastará conectar la memoria USB en el equipo posiblemente comprometido, ir al directorio donde está el agente y ejecutar "RunRedlineAudit.bat". Se abrirá una consola del sistema que recolectará toda la información pertinente y la almacenará en la ruta desde la que se ha ejecutado el agente, dentro de la carpeta "Audits". Al estar usando una memoria USB significa que se guardará en dicha memoria, de forma similar a cuando se usa el *IOC Finder*. Una vez que haya terminado de recolectar la información, se cerrará la consola.

9.2.3. CREACIÓN DE UN RECOLECTOR DE DATOS PARA DETERMINADOS FICHEROS IOC

152. Una vez conocidos los indicadores de compromiso a buscar, plasmados en un fichero .IOC, se puede generar un agente (*MIR Agent*) que recolecte específicamente esos datos. De ese modo el tiempo de recolección será más breve y las acciones serán más concisas.

153. Para generar este agente, existe la opción *Collect Data → Create an IOC Search Collector*.

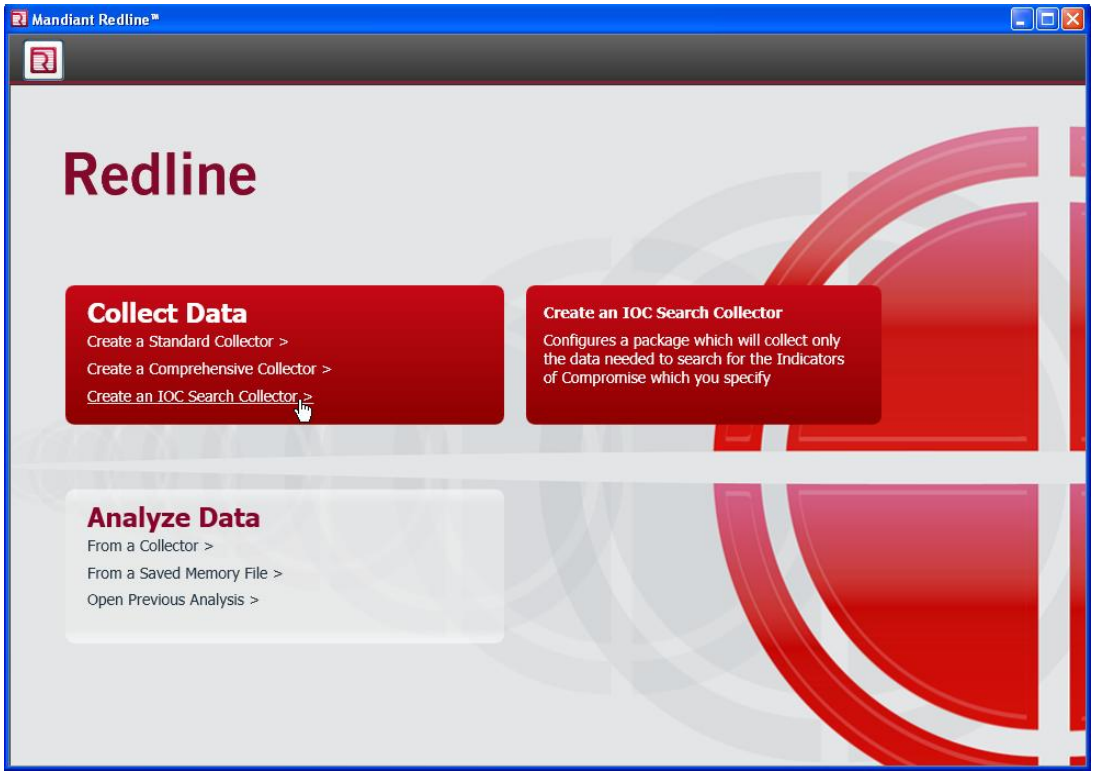


Figura 37. Opción para crear un agente de recolección específico

154. A continuación se selecciona con el botón "Browse" el directorio donde se encuentren los ficheros IOC que definen los datos necesarios para identificar un compromiso en un sistema.

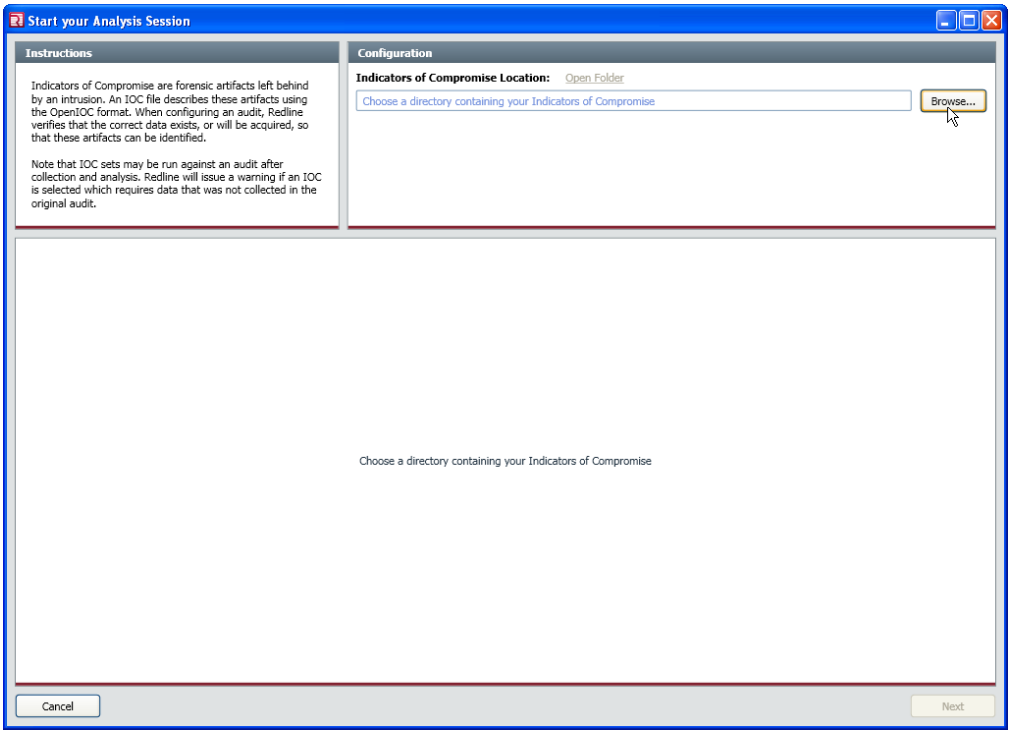


Figura 38. Carga de IOCs para crear el agente de recolección específico

155. Si hay varios IOC en el directorio y sólo se va a generar el agente para uno de ellos, basta con desmarcar el checkbox a su izquierda para que se ignoren.

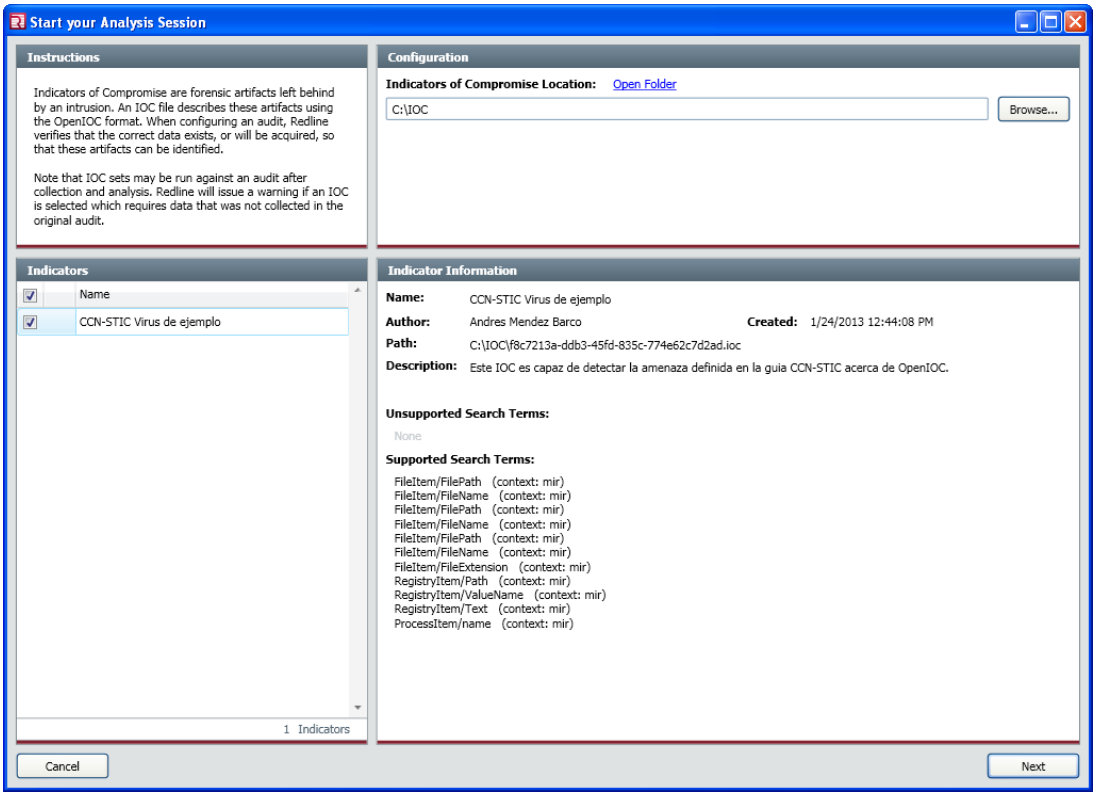


Figura 39. Selección de IOC para crear el agente de recolección específico

156. Pulsando en "Next" aparece la siguiente pantalla, que ofrece distintas opciones.

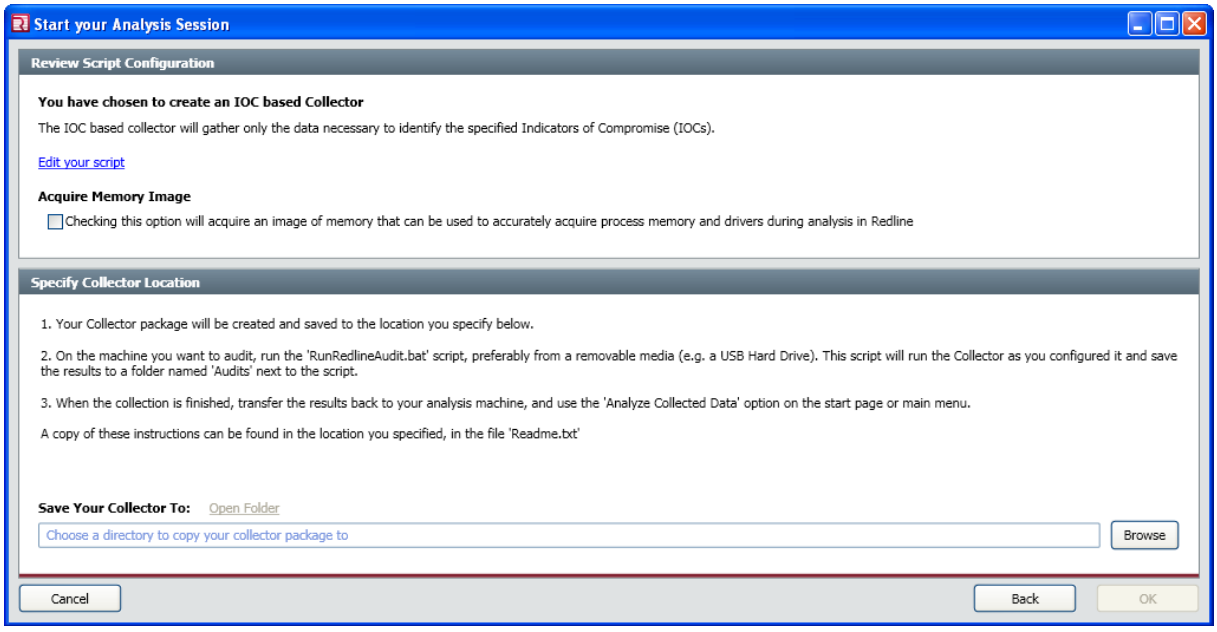


Figura 40. Ajustes del agente de recolección específico

157. Por un lado se puede ajustar más todavía los elementos que interesa recopilar (aunque no debería ser necesario). Para ello, pulse en "Edit your script". En la nueva ventana,

aparecerá marcada la información que el IOC necesita que se recopile del sistema cuando se analice por el agente. A través de las distintas pestañas y casillas se marca o desmarca lo que se considere relevante para un posterior análisis.

158. La casilla "Show Advanced Parameters" permitirá definir incluso más detalles.

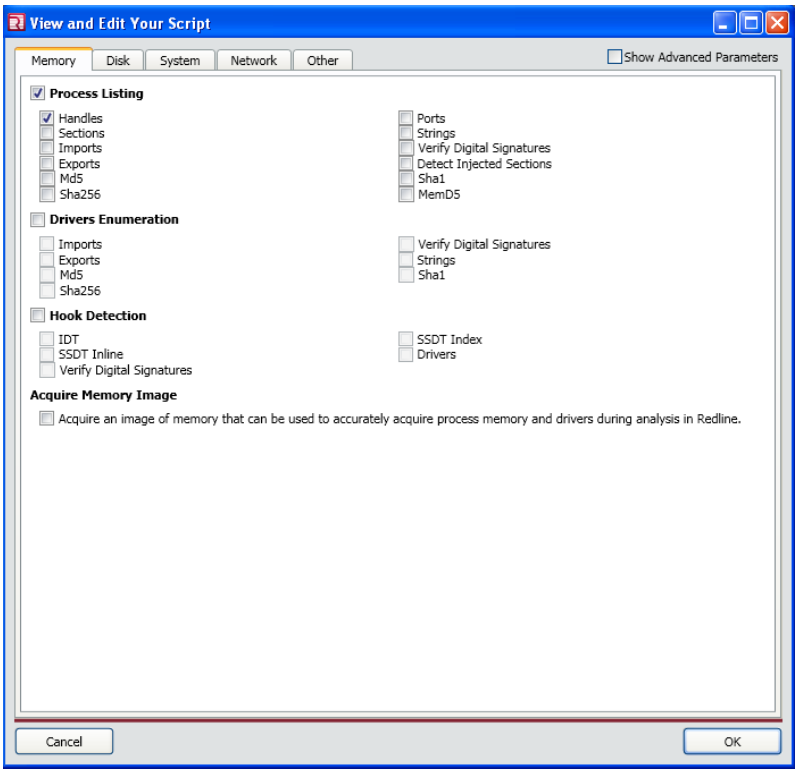


Figura 41. Edición del script del agente de recolección específico

159. Una vez terminada la revisión o el ajuste de los datos a recopilar, pulse "OK".

160. En caso de querer que el agente obtenga una imagen de la memoria, para un posterior análisis más concienzudo, se deberá marcar la casilla bajo "Acquire Memory Image". Hay que tener en cuenta que esto generará un fichero tan grande como la memoria en uso del sistema a analizar, por lo que la unidad de almacenamiento de las evidencias tendrá que tener espacio libre suficiente.

161. Por otro lado, se puede seleccionar en qué directorio vacío se va a guardar el agente, pulsando el botón "Browse". Se recomienda, al igual que en el caso del *IOC Finder*, que se almacene en una memoria USB, que será la que luego se conecte al equipo posiblemente comprometido.

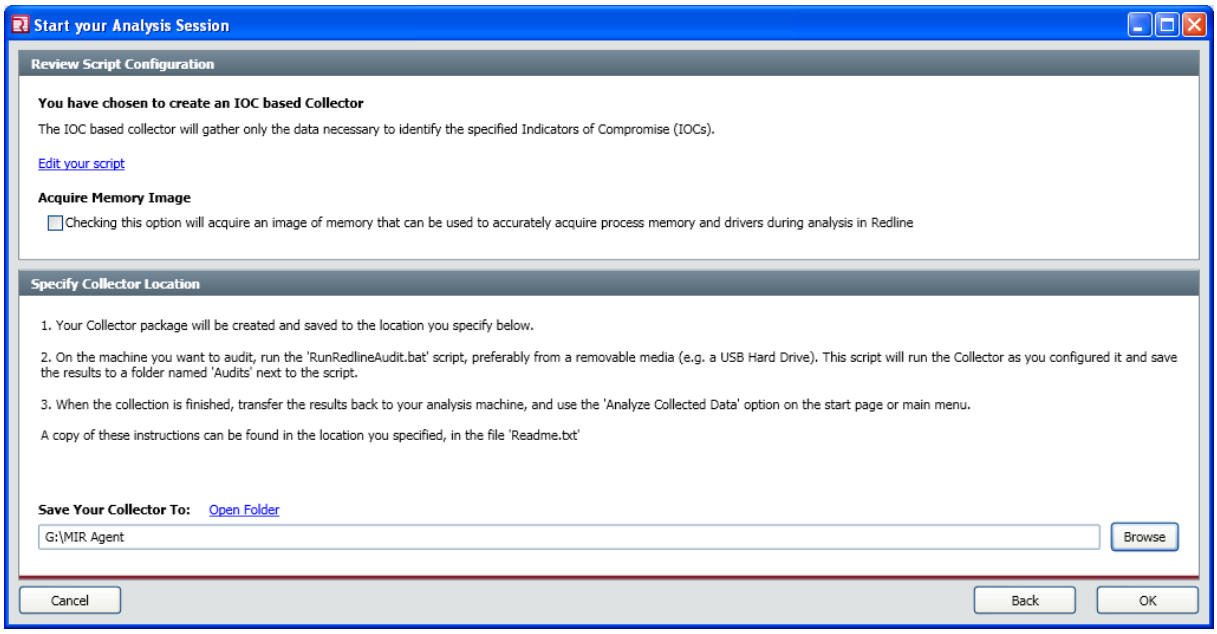


Figura 42. Terminando de configurar el agente de recolección específico

162. Hecho todo esto bastará pulsar el "OK" para que se generen los scripts y se copien los ejecutables al directorio indicado.

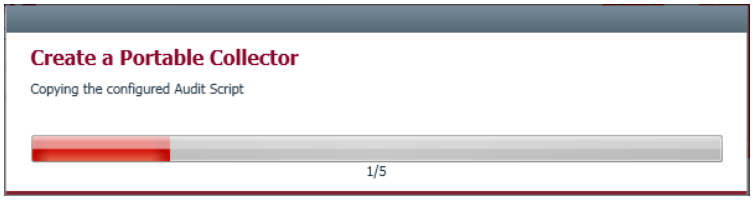


Figura 43. Copiándose el agente de recolección específico a la memoria USB

163. Una vez que se hayan terminado de copiar los datos a la memoria USB, aparecerá una ventana con unas instrucciones de uso.

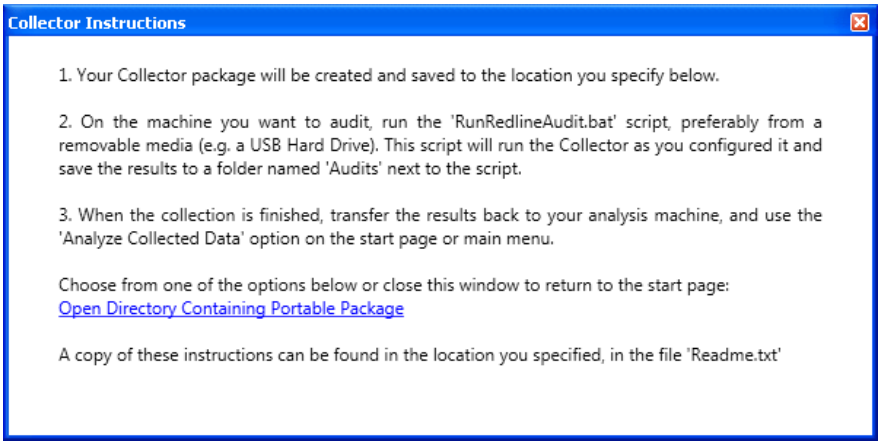


Figura 44. Instrucciones sobre de uso del agente de recolección específico

164. Ahora que se dispone de una memoria USB con el agente de recolección específico preparado, para ejecutarlo bastará conectar la memoria USB en el equipo posiblemente comprometido, ir al directorio donde está el agente y ejecutar "RunRedlineAudit.bat". Se abrirá una consola del sistema que recolectará toda la información pertinente y la almacenará en la ruta desde la que se ha ejecutado el agente, dentro de la carpeta "Audits". Al estar usando una memoria USB significa que se guardará en dicha memoria, de forma similar a cuando se usa el *IOC Finder*. Una vez que haya terminado de recolectar la información, se cerrará la consola.

9.2.4. USO DE UN RECOLECTOR DE DATOS CREADOS CON REDLINE

165. La ejecución del agente de recolección de datos creado con *Redline* es muy sencilla. Bastará con ejecutar con permisos de administrador "RunRedlineAudit.bat" y esperar a que finalice la recolección.

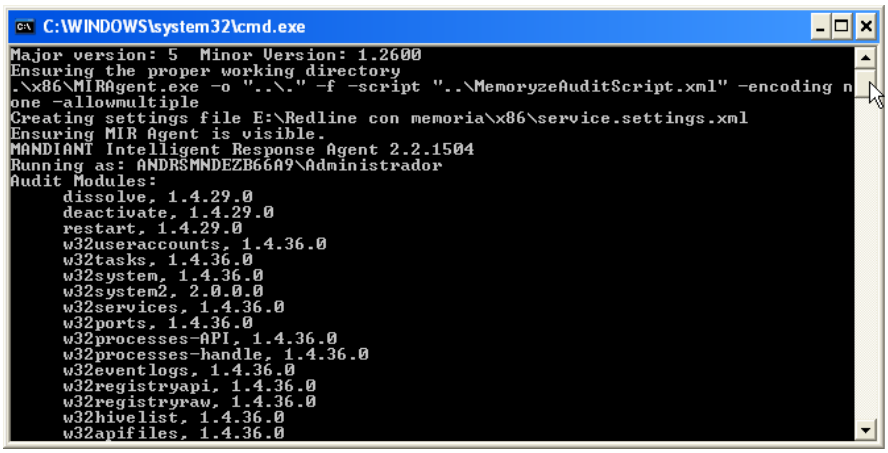


Figura 45. Ejecución del agente de recolección

166. Una vez se tengan las evidencias del sistema, se podrá buscar indicadores de compromiso mediante *IOC Finder* o situaciones anómalas mediante *Redline*.

9.3. ANÁLISIS DE EVIDENCIAS DE COMPROMISO

167. Una vez que el agente de Redline ha extraído las evidencias de un sistema, éstas se analizan para tratar de encontrar en ellas indicadores de compromiso.

168. El equipo donde se analicen las evidencias, aunque estas sean cargadas desde una memoria USB, necesitará, como mínimo, el mismo espacio que dicho análisis ocupa en la memoria USB libre en el disco duro.

9.3.1. ANÁLISIS DE EVIDENCIAS SIN VOLCADO DE MEMORIA

169. Para analizar las evidencias, hay que seleccionar la opción *Analyze Data → From a Collector*.

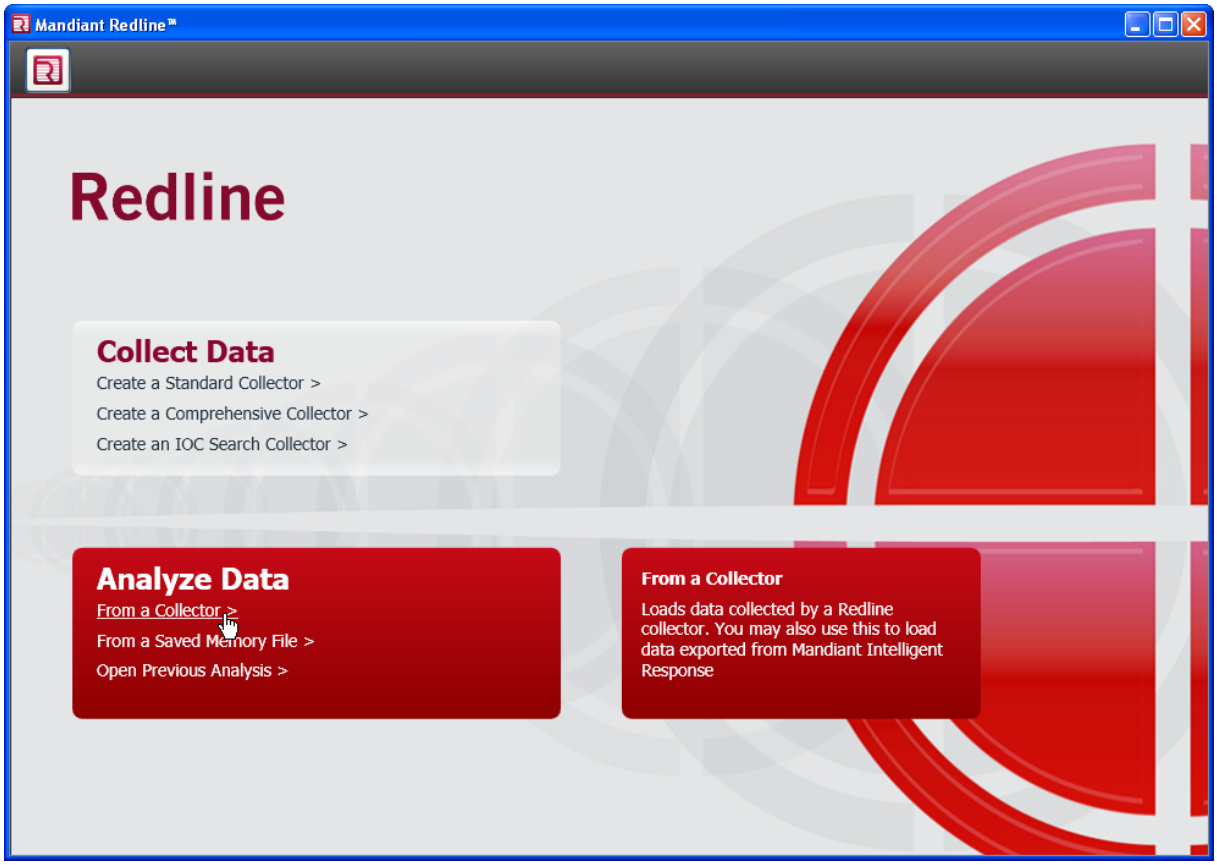


Figura 46. Opción para analizar los datos recolectados por un agente

170. En "Audit Location" hay que seleccionar "Browse" y navegar por los directorios hasta la carpeta de la memoria USB donde esté la auditoría (dentro de Audits > Nombre del sistema > carpeta con la fecha), pulsando a continuación "Aceptar".

171. Si se dispone de ficheros .IOC con amenazas identificadas, se pueden cargar para que *Redline* trate de identificar esas amenazas durante el análisis. Para ello, dentro de "Indicators of Compromise Location" se selecciona el directorio donde se encuentran los .IOC. A continuación aparecerá en la zona inferior de la ventana un listado con los IOC que haya cargado (por defecto estarán todos marcados para ser utilizados durante el análisis). Es posible desmarcar aquellos que no se desee utilizar.

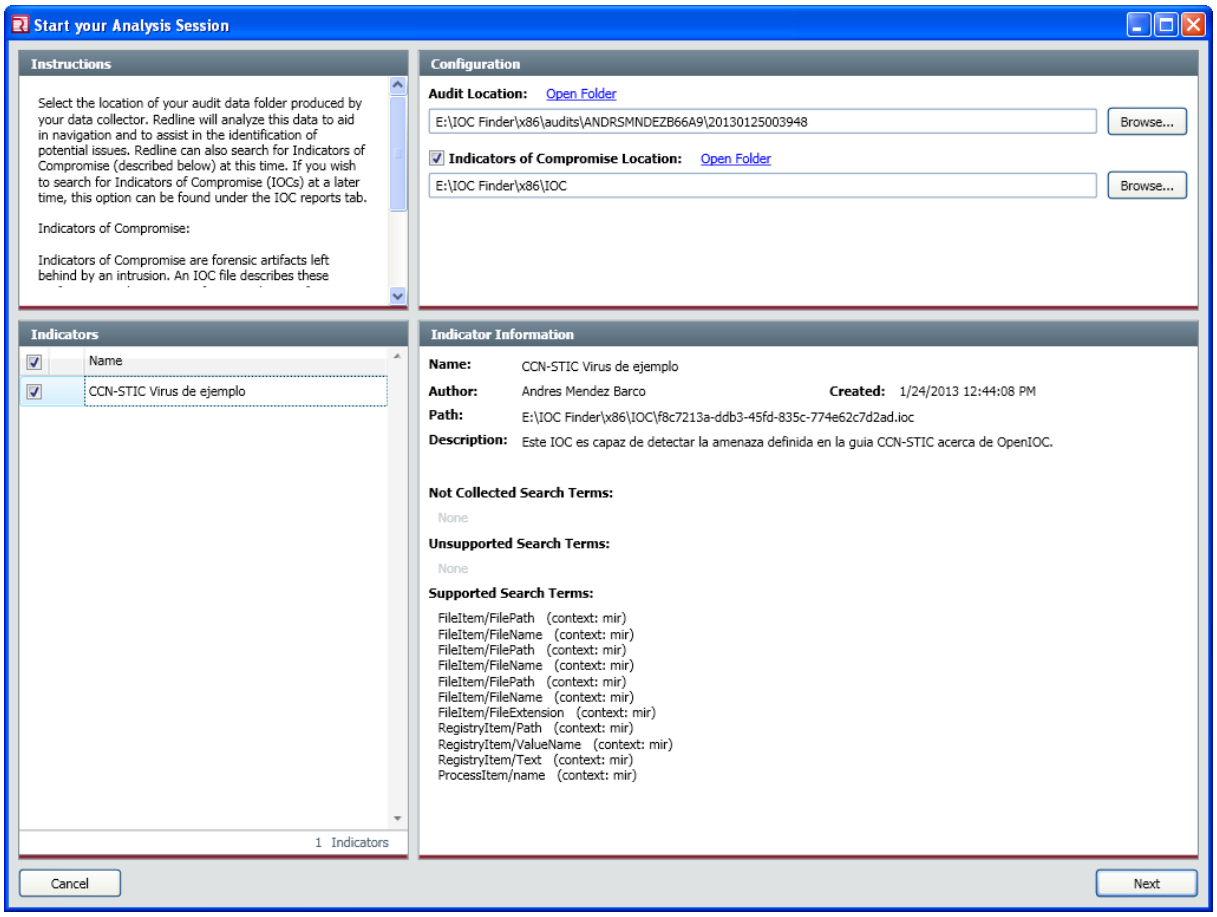


Figura 47. Selección de los datos recolectados para analizar

172. En la siguiente pantalla, pulsando en "Browse", se selecciona el directorio y el nombre del fichero donde se almacenará el análisis resultante. En función de la cantidad de datos a analizar, así ocupará el fichero resultante del análisis, con extensión .mans. Habitualmente los ficheros .mans suelen ocupar de 150Mb en adelante.

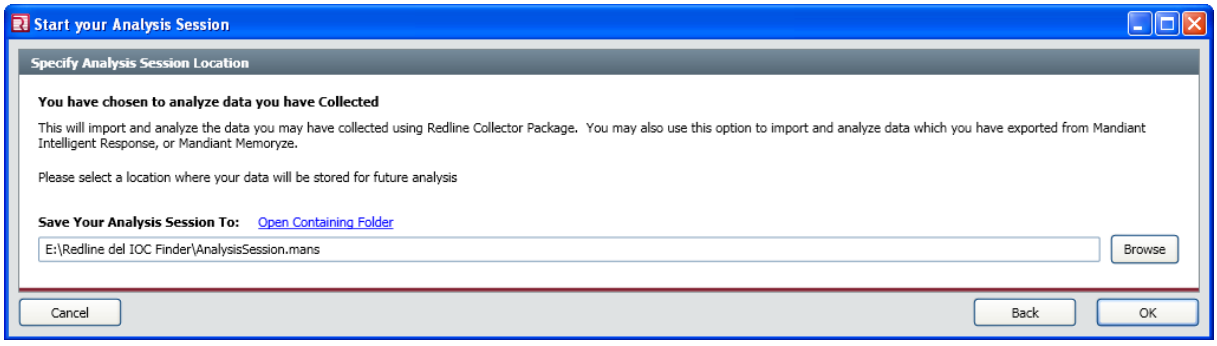


Figura 48. Selección del fichero donde guardar el análisis

173. Una vez terminado el análisis se mostrará una ventana nueva con los resultados, cuya explicación se tratará en el apartado 9.4 (INFORME DE EVIDENCIAS DE COMPROMISO) de la presente guía.

9.3.2. ANÁLISIS DE EVIDENCIAS DESDE UN VOLCADO DE MEMORIA

174. El análisis de las evidencias existentes en un volcado de memoria se realiza mediante la opción *Analyze Data → From a Saved Memory File*.

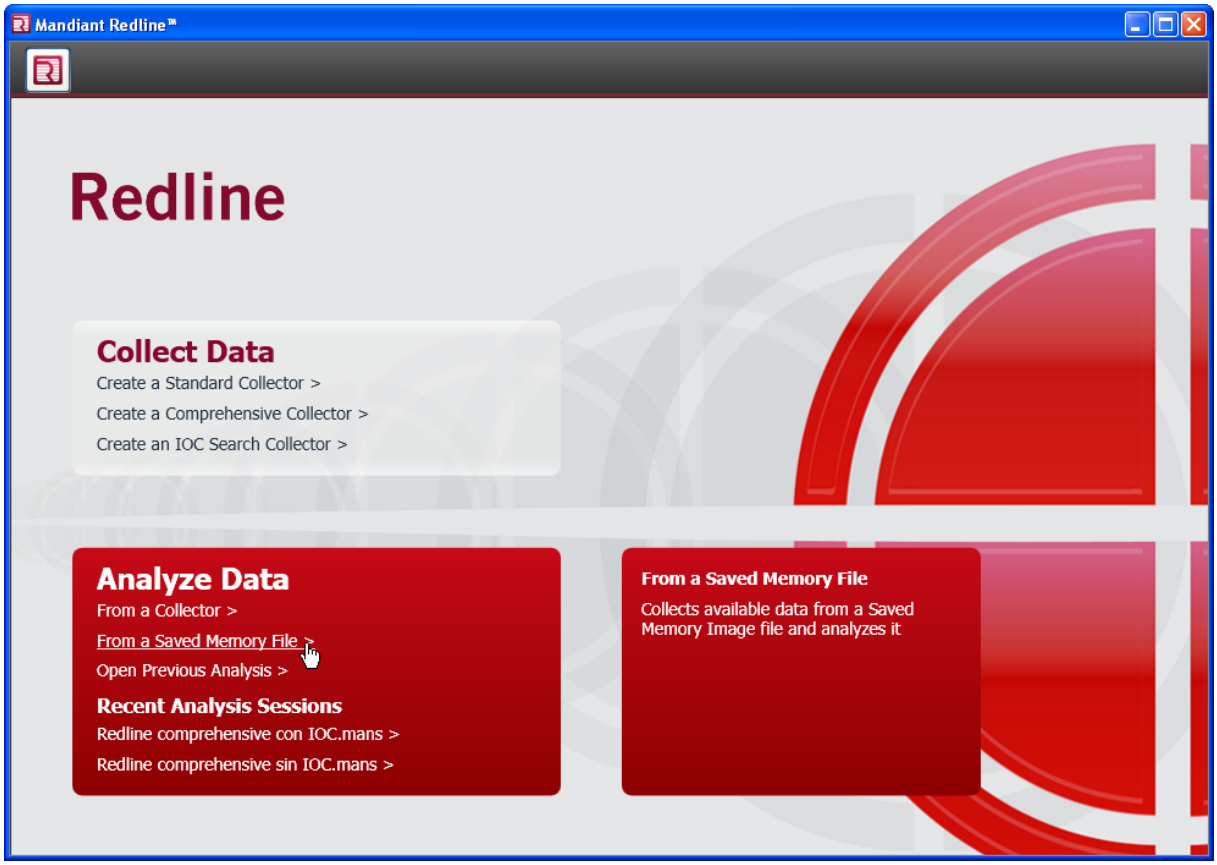


Figura 49. Opción para analizar el contenido de la memoria obtenida por un agente

175. Se puede observar que después de haber realizado el análisis de unas evidencias aparece una nueva sección inferior "Recent Analysis Sessions", que muestra los ficheros .mans donde se han almacenado los resultados. Se deberán conservar estos ficheros pues son el resultado del análisis, con los comentarios y ajustes realizados.

176. En "Location of Saved Memory Image", se selecciona "Browse" para navegar por los directorios hasta la carpeta de la memoria USB donde esté la auditoría (dentro de *Audits → Nombre del sistema*, seleccionando la carpeta con la fecha) y seleccionar el fichero .img, pulsando a continuación en "Aceptar".

177. Si se dispone de ficheros .IOC con amenazas identificadas, éstos se pueden cargar para tratar de identificar esas amenazas concretas durante el análisis. Para ello dentro de "Indicators of Compromise Location" se debe seleccionar "Browse" y navegar por los directorios hasta aquél en el que se encuentran los ficheros .IOC. A continuación aparecerá en la zona inferior de la ventana un listado con los IOC que se hayan cargado(por defecto estarán todos marcados para ser utilizados durante el análisis). Es posible desmarcar aquellos que no se desee utilizar.

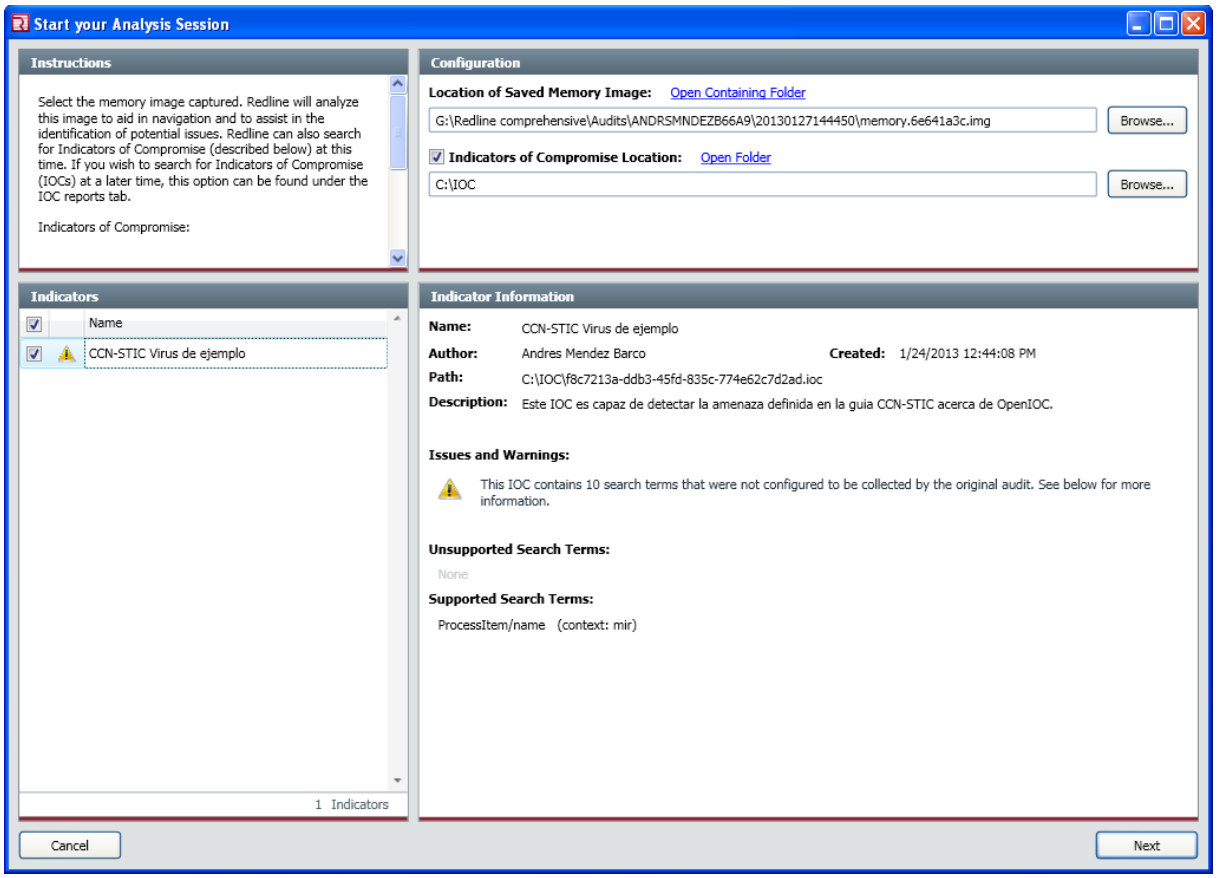


Figura 50. Selección de los datos recolectados para analizar

178. Es importante destacar que si la recolección de datos realizada previamente no contiene el tipo de datos que necesita analizar el .IOC, aparecerá un mensaje de aviso como el que puede ver en la captura de pantalla anterior. Como los datos recopilados en este ejemplo no tienen esa información, habría que desmarcar la opción "Indicators of Compromise Location" y pulsar a continuación el botón "Next".

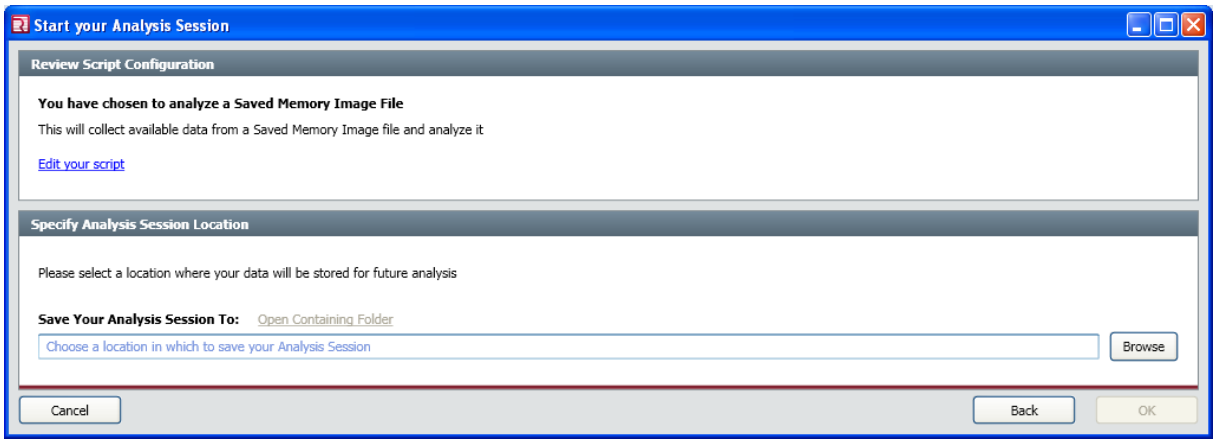


Figura 51. Ajustes del análisis y del lugar de almacenamiento del mismo

179. En la siguiente pantalla se pueden ajustar los componentes de la memoria a analizar pulsando "Edit your script".

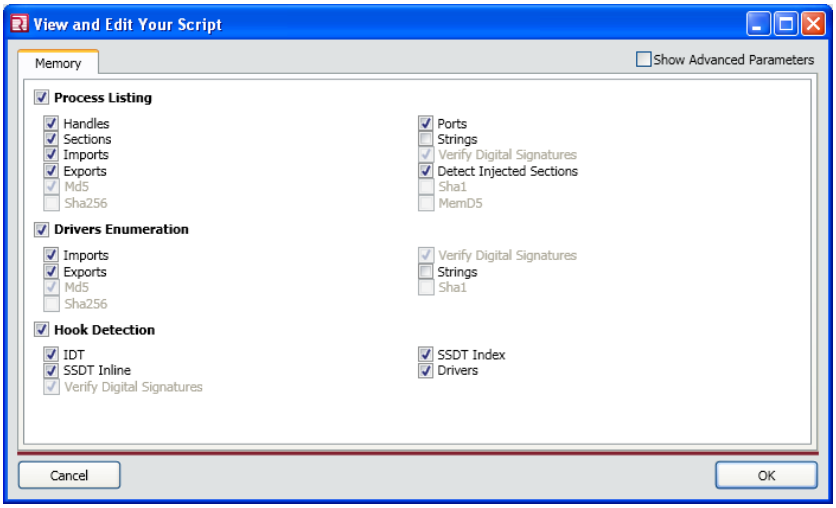


Figura 52. Selección de los datos de memoria recolectados para analizar

180. Una vez seleccionados los datos a analizar, hay que pulsar "OK" para volver a la pantalla previa.

181. De vuelta a la pantalla anterior, pulsando en "Browse" se selecciona el directorio y el nombre del fichero donde se almacenará análisis resultante. En función de la cantidad de datos a analizar, así ocupará el fichero resultante del análisis, con extensión .mans. Habitualmente los ficheros .mans suelen ocupar de 150Mb en adelante.

182. Es posible que se soliciten permisos elevados de sistema para realizar el análisis. En ese caso, se deberá utilizar un usuario con permisos de administrador y desmarcar la opción "Proteger mi equipo y mis datos contra la actividad de programas sin autorización".

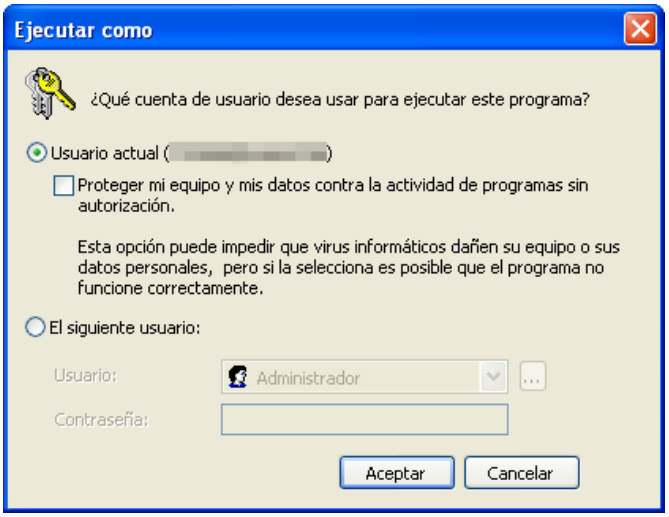


Figura 53. Selección del usuario y permisos necesarios en Windows XP

183. Una vez terminado el análisis se mostrará una ventana nueva con los resultados, cuya explicación se tratará en el apartado "9.4 INFORME DE EVIDENCIAS DE COMPROMISO" de la presente guía.

9.3.3. CARGA DE UN ANÁLISIS ANTERIOR

184. Una vez realizado el análisis de unas evidencias, se puede cargar el resultado mediante la opción *Analyze Data* → *Open Previous Analysis* cargando el fichero .mans.

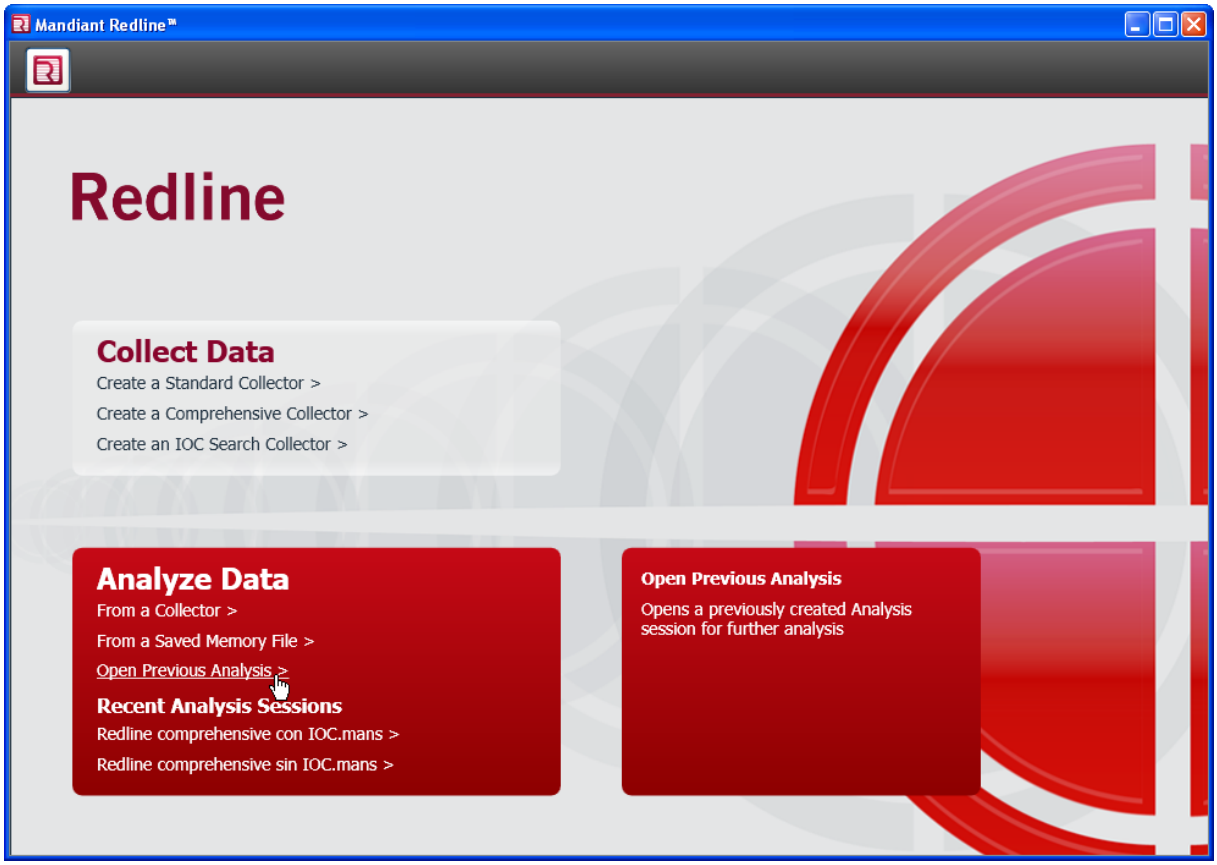


Figura 54. Cargar un proyecto de análisis anterior

185. De esta forma se obtiene el mismo resultado que si se carga un análisis reciente de los que aparecen en "Recent Analysis Sessions".

9.4. INFORME DE EVIDENCIAS DE COMPROMISO

186. Una vez que *Redline* ha analizado las evidencias de un sistema, mostrará un informe de lo que ha identificado como situaciones anómalas. Si se seleccionó que analizara las evidencias contra ficheros .IOC, también mostrará los indicadores de compromiso que se hayan detectado.

187. La pantalla está dividida en varias secciones:

- **Investigative Steps**: En la esquina superior izquierda, hay un menú con las distintas secciones que componen el informe, ordenadas por los pasos a seguir a la hora de analizar las situaciones anómalas para determinar si constituyen un indicador de que el sistema ha sido comprometido. Eso mismo es lo que se muestra inicialmente en la zona principal.

- **Processes**: Justo debajo, hay unas pestañas que permiten ir a los detalles de los distintos elementos analizados: *Processes* (Procesos), Host (Sistema) y *IOC Reports* (Informes sobre IOC).
- **Barra de navegación**: Permite moverse por el informe como si fuera una página web. Se puede ir al comienzo del informe pulsando "Home".
- **Start Your Investigation**: Es la zona principal, donde se muestra lo que se haya seleccionado. Muestra "Start Your Investigation", con los pasos a seguir para analizar los resultados, en el mismo orden en el que se ve el menú "Investigative Steps".

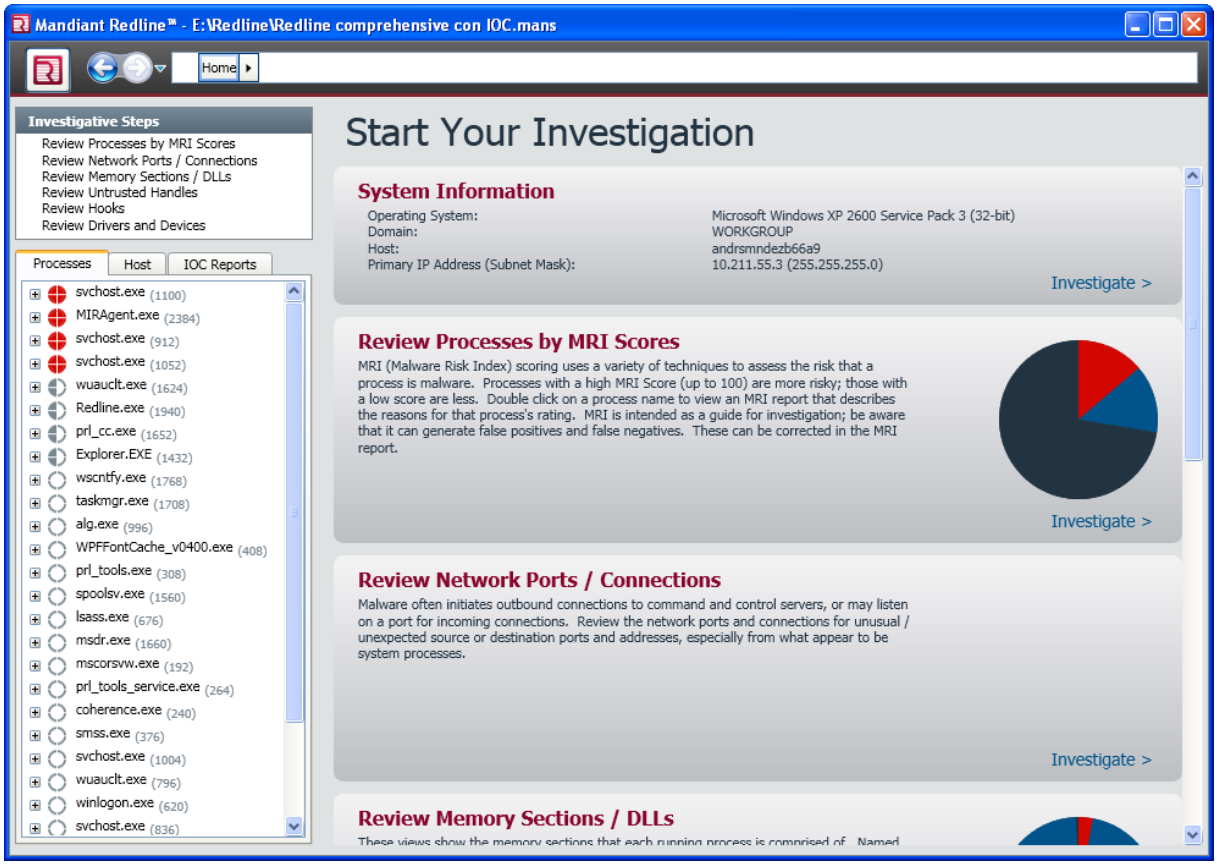


Figura 55. Home del informe del Redline

188. Se describirá a continuación la información que se puede obtener en cada sección.

9.4.1. REVISIÓN DE LOS PROCESOS SEGÚN SU PUNTUACIÓN MRI (*REVIEW PROCESSES BY MRI SCORES*)

189. *Redline* asigna un *Código dañino Risk Index Scoring* (MRI) a cada proceso. Asigna el siguiente símbolo de mayor a menor riesgo de que se trate de una amenaza o código dañino:

- Diana roja: alta probabilidad de que se trate de un código dañino.
- Diana gris con zonas vacías: cierta probabilidad de que se trate de código dañino.
- Diana gris totalmente vacía: muy poca probabilidad de que se trate de código dañino.

190. En esta pantalla, por defecto, sólo se muestran los procesos que tienen la diana roja. Si se quieren ver todos los procesos, hay que pulsar en la zona derecha (bajo "Review Processes by MRI Scores") en "All Processes". Para volver a ver sólo los procesos con mayor riesgo, se debe pulsar también a la derecha en "Redline Processes".

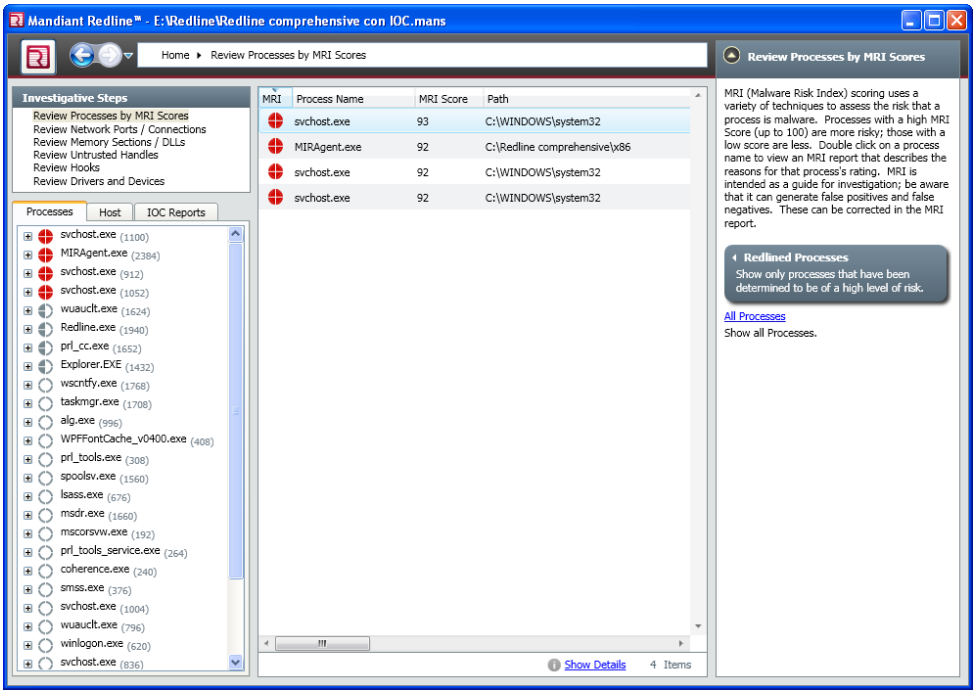


Figura 56. Procesos con mayor riesgo según Redline

191. Seleccionando uno de ellos, aparecerá abajo la opción "Show Details". Pulsándola aparecerá otra sección con los detalles del proceso (son los mismos que pueden verse moviendo el scroll del listado de procesos, aunque en esta vista se muestra toda la información en un solo pantallazo).

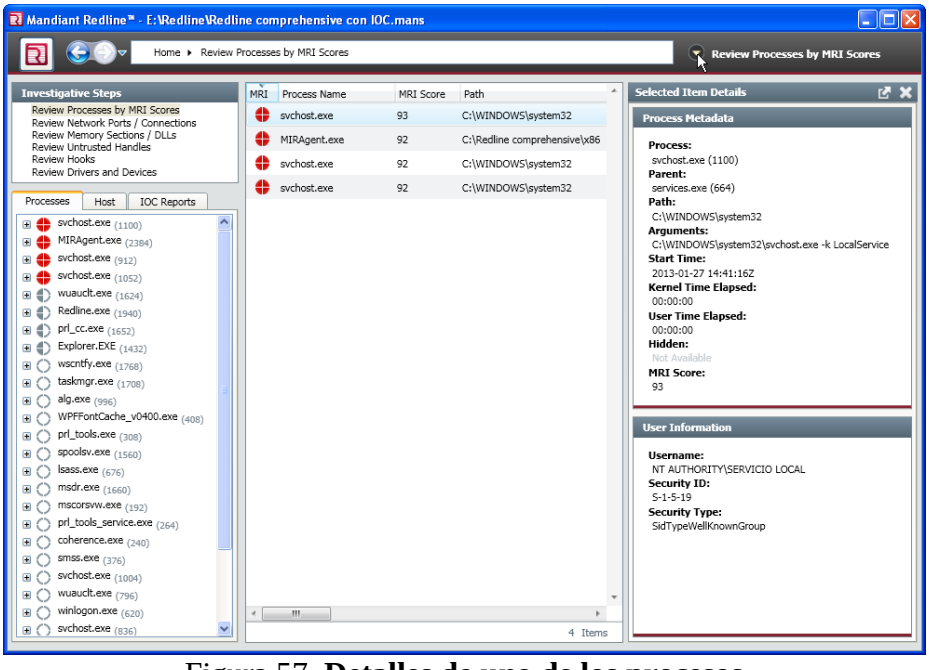


Figura 57. **Detalles de uno de los procesos**

9.4.2. REVISIÓN DE LOS PUERTOS Y LAS CONEXIONES DE RED (*REVIEW NETWORK PORTS / CONNECTIONS*)

192. En esta pantalla, por defecto, se muestran los procesos que están usando la red de comunicaciones. Para ver sólo los procesos que tienen un puerto a la escucha (esperando recibir una conexión), se debe pulsar en la zona derecha (bajo "Review Network Ports / Connections") en "Listening Ports". Para ver sólo los procesos que ya tienen establecida una conexión se debe seleccionar, también a la derecha, "Established Ports".

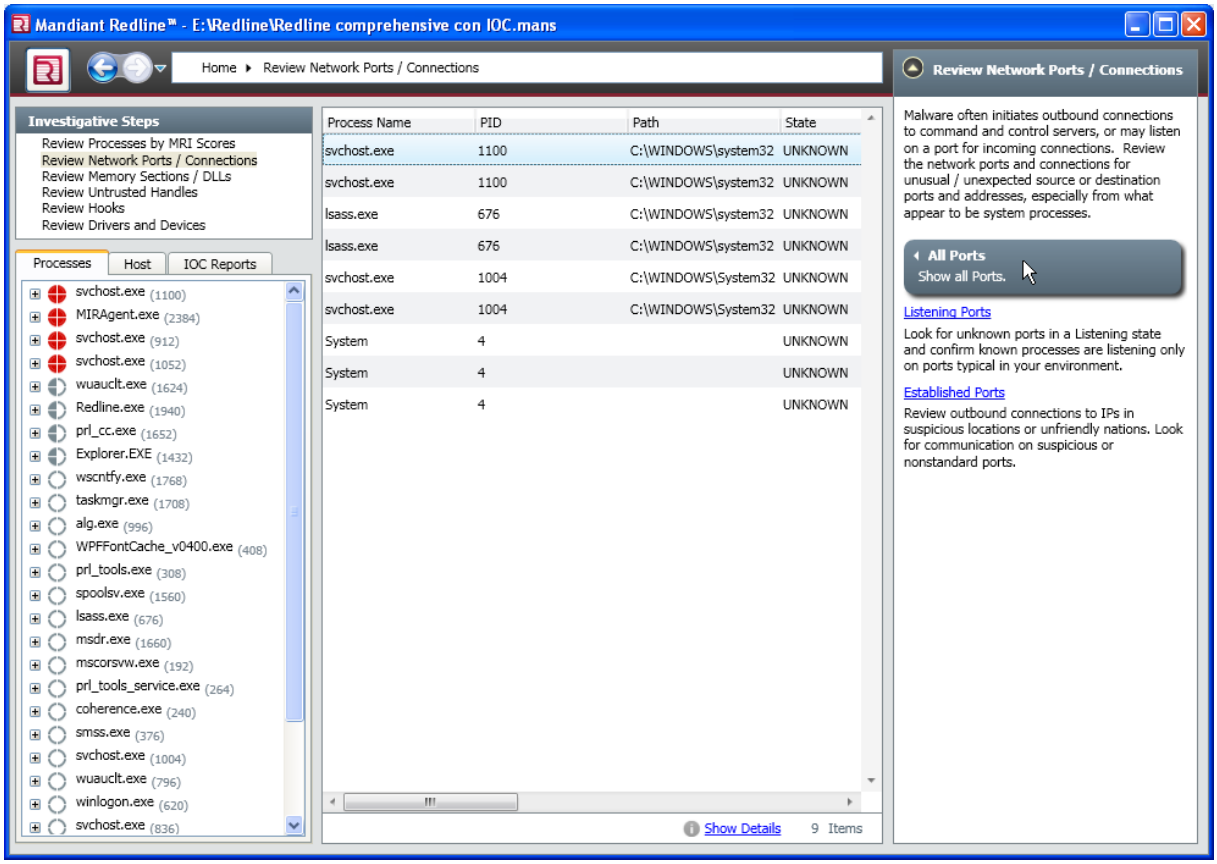


Figura 58. Procesos con uso de la red

193. Seleccionando uno de ellos, aparecerá abajo la opción "Show Details". Pulsándola aparecerá otra sección con los detalles del proceso (son los mismos que pueden verse moviendo el scroll del listado de procesos, aunque en esta vista se muestra toda la información en un solo pantallazo).

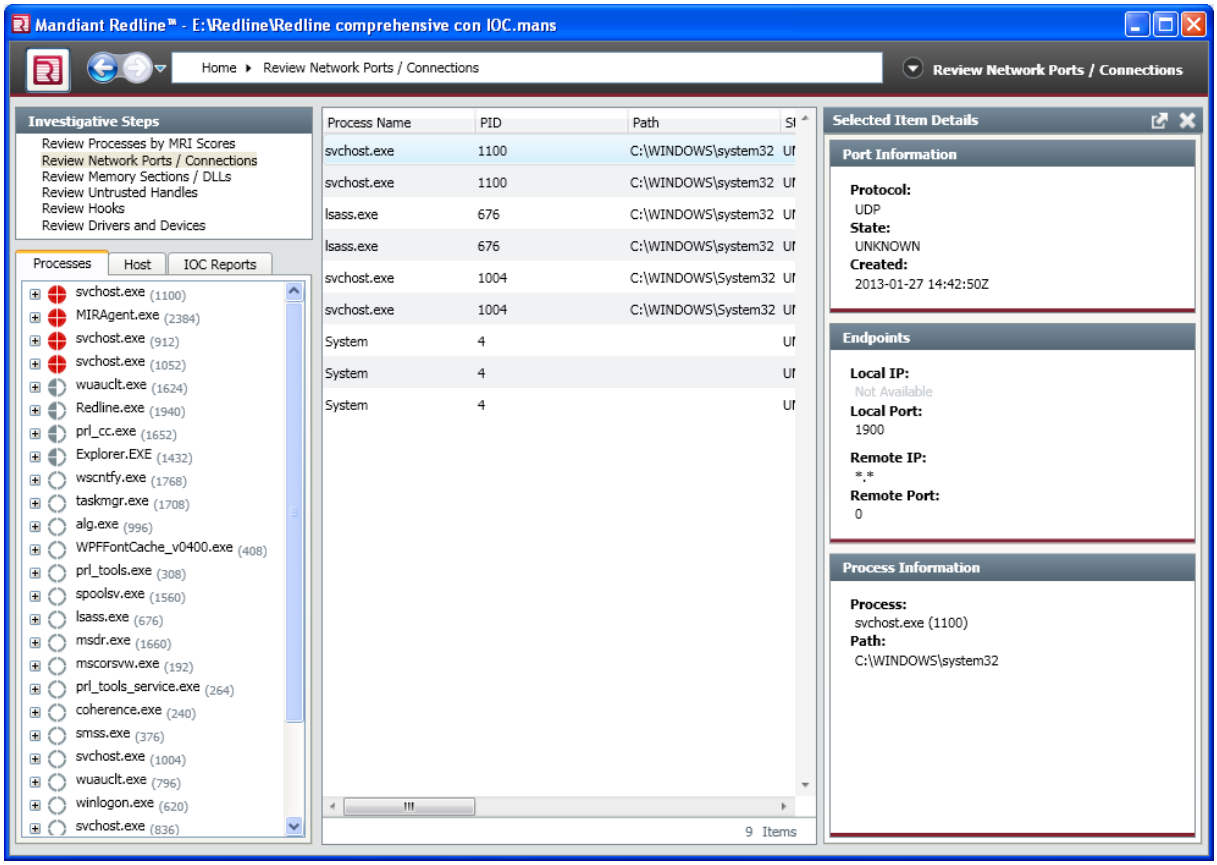


Figura 59. Detalle del uso de la red de un proceso

9.4.3. REVISIÓN DE LAS SECCIONES DE MEMORIA Y DLL (*REVIEW MEMORY SECTIONS / DLLS*)

194. En esta pantalla, por defecto, se muestran las librerías en uso que están siendo usadas por menos de 4 procesos (*Least Frequency of Occurrence –Untrusted Only*) y que, además, no están firmadas digitalmente y/o no han sido verificadas. La opción "Hide Whitelisted Items" oculta los procesos que están en la lista blanca (*whitelist*). El listado resultante son aquellas librerías, ordenadas de menor a mayor número de ocurrencias (hasta 3).

195. Es conveniente indicar que las librerías de código dañino habitualmente son utilizadas por un único proceso y que no suelen estar firmadas o, si lo están, su firma no está verificada. Por lo tanto, como posibles indicadores de la presencia de código dañino, se deben analizar las librerías que cumplan dichas condiciones para ver si deben estar o no en uso.

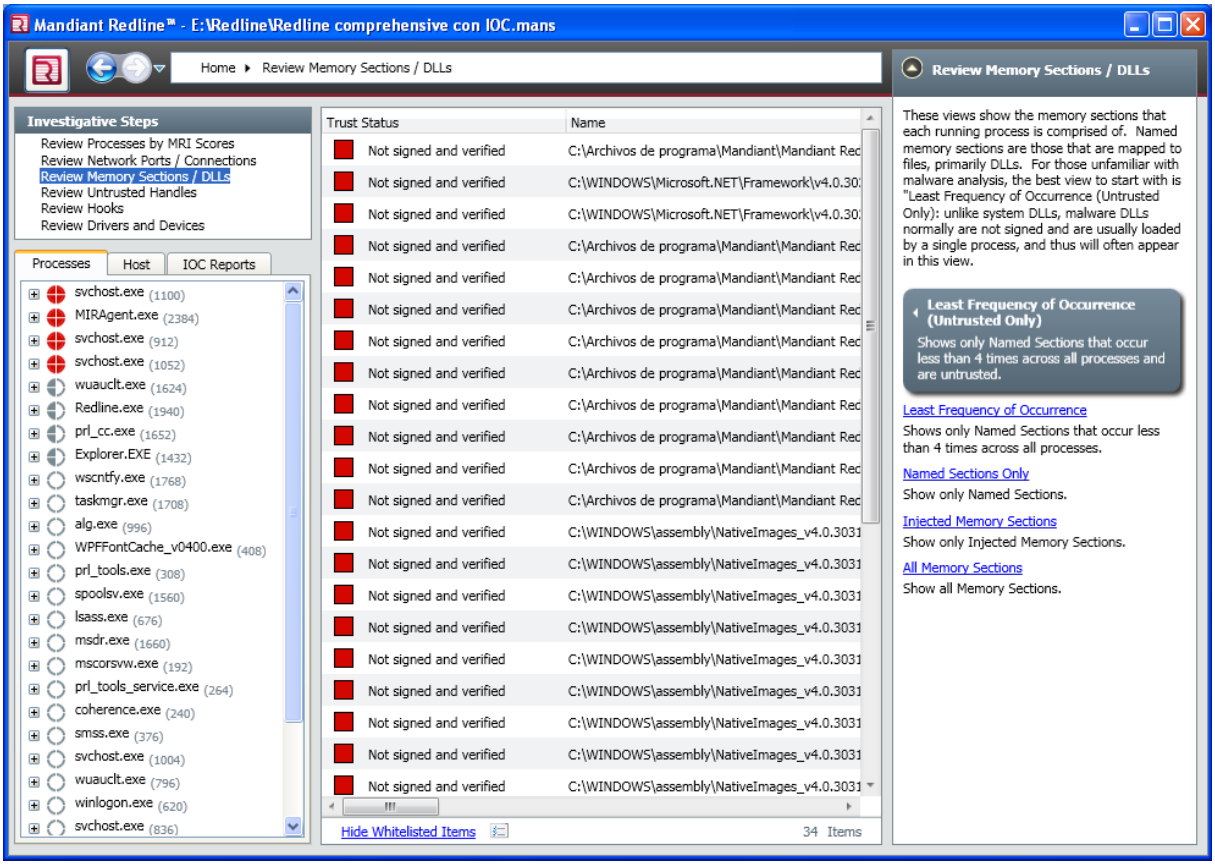


Figura 60. Listado de librerías no verificadas y de poca ocurrencia

196. Otras opciones de revisión disponibles en la sección derecha de esta pantalla, bajo "Review Memory Sections / DLLs", son las indicadas a continuación. En todas ellas se pueden ocultar los procesos que están en la lista blanca (whitelist), y que por lo tanto son confiables, seleccionando "Hide Whitelisted Items":

- ***Least Frequency of Occurrence:*** muestra los procesos tanto firmados y verificados como los que no lo están, y que además se usan menos de 4 veces. En la columna "Trust Status" aparecerán ahora indicadas librerías firmadas y verificadas ("Digitally signed and verified").
- ***Named Sections Only:*** muestra todos los procesos, estén o no firmados y verificados, se usen las veces que se usen.
- ***Injected Memory Sections:*** muestra las secciones de memoria que han sido inyectadas. Es conveniente indicar que una de las técnicas utilizadas por el código dañino consiste en introducir (inyectar) código en zonas de memoria de aplicaciones legítimas o confiables.
- ***All Memory Sections:*** muestra todos los procesos. Si se ordena este listado por "Trust Status", se pueden ver aquellos procesos que no están firmados o verificados (*Not signed and verified*), que han sido inyectados (*Injected*), que se encuentran en la mayoría de los procesos (*Found in 75% of all Processes*), ignorados por la configuración (*Ingnored per configuration*), firmados y verificados (*Digitally signed and verified*), o indeterminados (*Undetermined*).

9.4.4. REVISIÓN DE REFERENCIAS NO CONFIABLES (*REVIEW MEMORY UNTRUSTED HANDLES*)

197. En esta pantalla, por defecto, se muestran las referencias no confiables que no aparecen ni tan siquiera en 3 procesos que resultan tener el menor riesgo en base a su valor MRI.

198. Es conveniente indicar que las referencias abstractas o punteros inteligentes (*handles*) son utilizados por el sistema operativo para hacer referencia a ficheros, claves del registro, tuberías y otros recursos. Pueden indicar la presencia de código dañino cuando se utilizan por procesos que no son confiables o cuando son utilizados por muy pocos procesos.

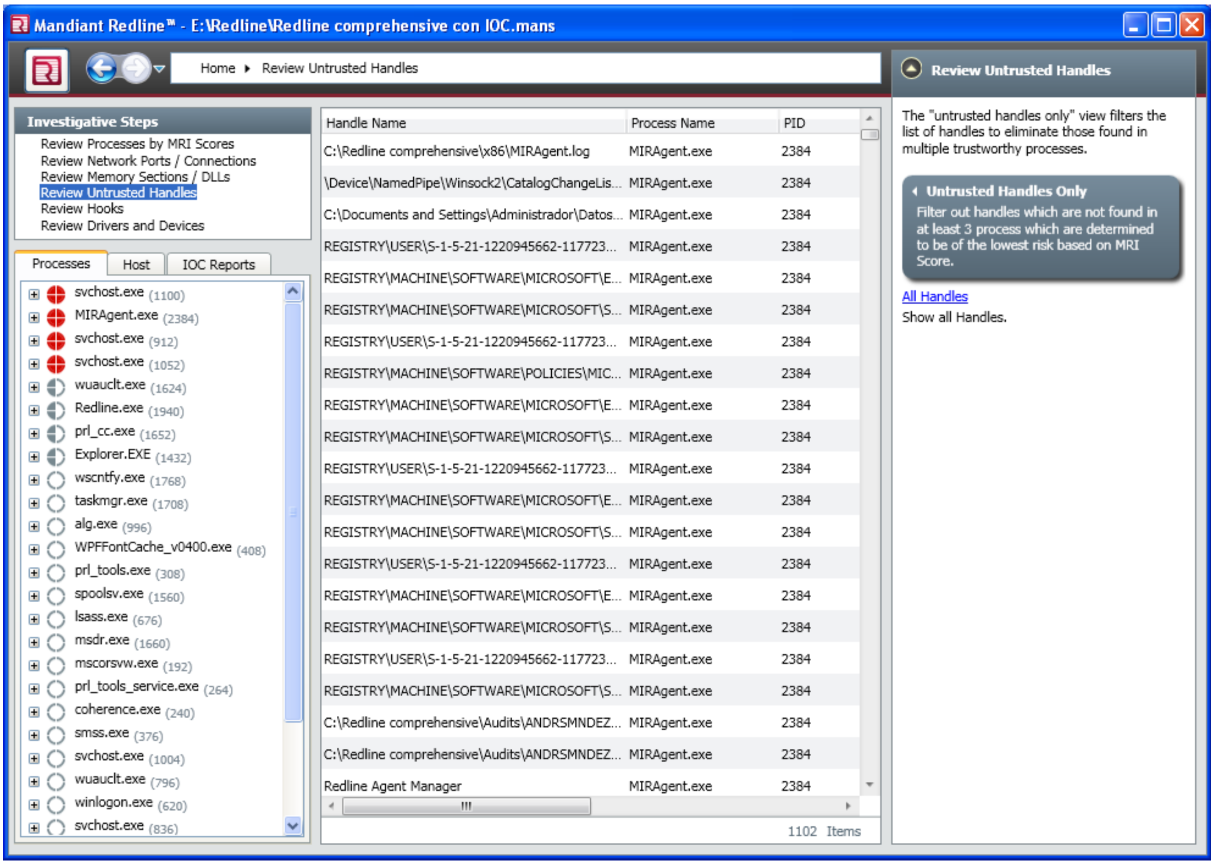


Figura 61. Listado de referencias no confiables y de poca ocurrencia

199. La opción "All Handles" (zona derecha, bajo "Review Untrusted Handles") permite ver todas las referencias, tanto confiables como no.

9.4.5. REVISIÓN DE CADENAS NO CONFIABLES (*REVIEW MEMORY HOOKS*)

200. En esta pantalla, por defecto, se muestran los *hooks* que *Redline* considera como no confiables (*Untrusted Hooks*). Como su análisis puede no ser del todo acertado, se recomienda revisar los *hooks* que aparecen en el resto de vistas.

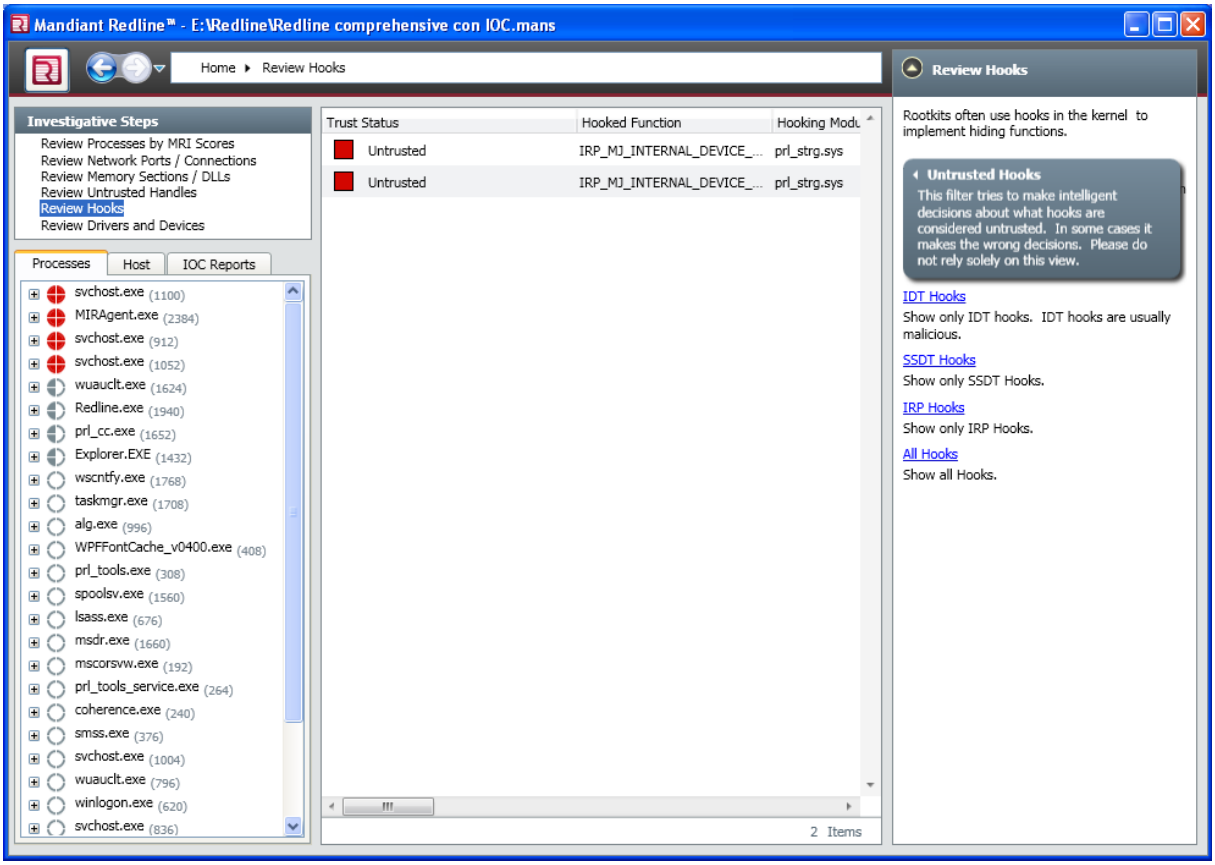


Figura 62. Listado de *hooks* que *Redline* considera no confiables

201. Es conveniente indicar que las cadenas (*hooks*) son subrutinas que se inyectan en los mecanismos habituales del sistema, permitiendo a una tercera parte el monitorizar y modificar los datos (mensajes, eventos o llamadas de función) que pasan de un origen a un destino (por ejemplo, las pulsaciones de teclado). Pueden presentarse en código dañino para obtener información o alterar ésta en tránsito (como es el caso de los *rootkits*).

202. Otras opciones de revisión disponibles en la sección derecha de esta pantalla, bajo "Review Hooks" son las siguientes:

- ***IDT Hooks:*** muestra los *hooks* de tipo IDT (*Interrupt Descriptor Table*). Afectan al kernel para capturar, por ejemplo, pulsaciones de teclado. Este tipo de *hooks* suele ser malicioso.
- ***SSDT Hooks:*** muestra los *hooks* de tipo SSDT (*System Service Descriptor Table*). Son los empelados por los antivirus o firewalls personales.
- ***IRP Hooks:*** muestra los *hooks* de tipo IRP, que suelen atacar a los drivers NTFS, DISK, FAT, TCPIP, NDIS, KBDCLASS…(ver Anexo A Glosario)
- ***All Hooks:*** muestra todos los *hooks*.

9.4.6. REVISIÓN DE LOS CONTROLADORES Y DISPOSITIVOS (*REVIEW DRIVERS AND DEVICES*)

203. En esta pantalla se muestran los controladores y dispositivos del sistema. El código dañino suele utilizar controladores en capas para interceptar paquetes, pulsaciones y

consultas al sistema de ficheros. Se pueden ocultar los controladores que están en la lista blanca (whitelist), y que por lo tanto son confiables, pulsando en "Hide Whitelisted Items".

204. Para ver bien esta información, se recomienda minimizar la zona derecha pulsando en el desplegable de "Review Drivers and Devices".

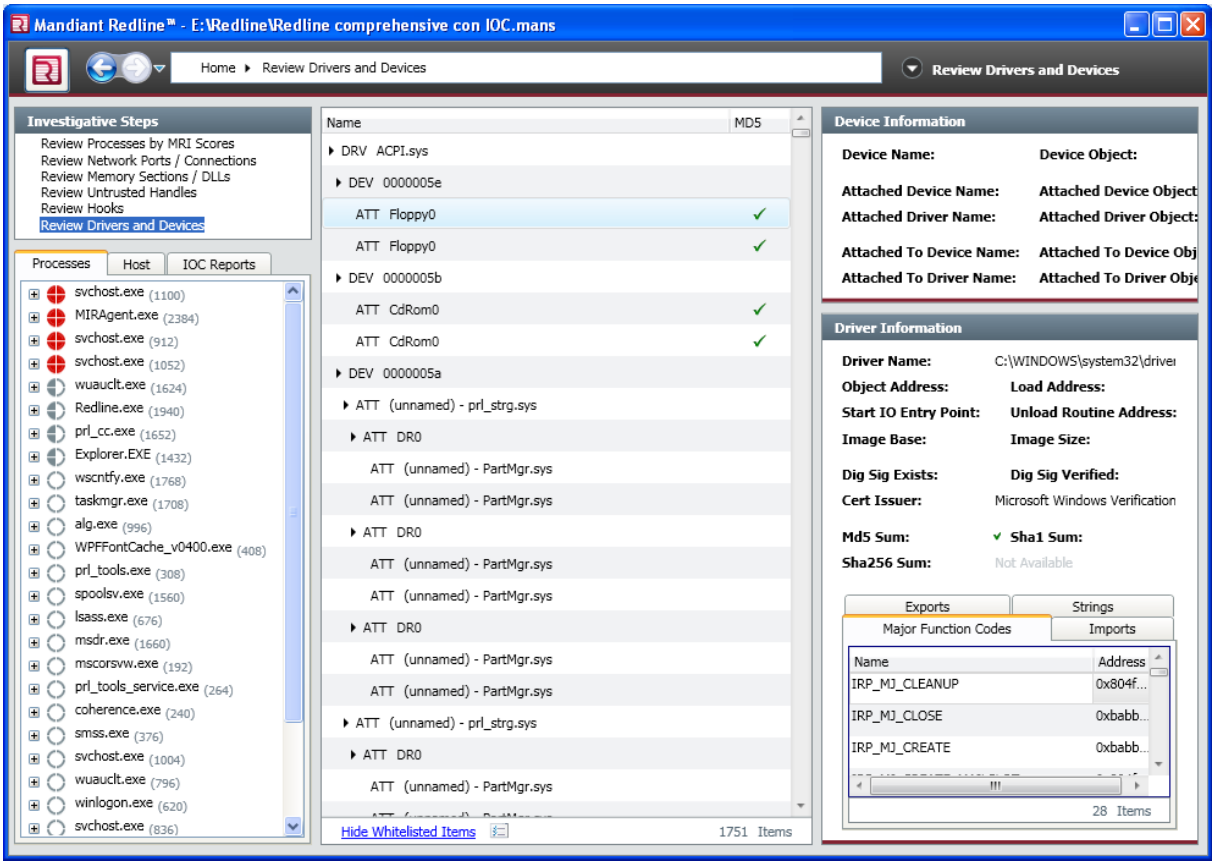


Figura 63. Listado de controladores y dispositivos

9.4.7. PROCESOS (*PROCESSES*)

205. Esta pestaña muestra el listado de procesos, con su indicador de nivel de riesgo a su izquierda.

206. *Redline* asigna un *Código dañino Risk Index Scoring* (MRI Scoring) a cada proceso. Asigna el siguiente símbolo de mayor a menor riesgo de que se trate de una amenaza o código dañino:

- Diana roja: alta probabilidad de que se trate de un código dañino;
- Diana gris con zonas vacías: cierta probabilidad de que se trate de código dañino;
- Diana gris totalmente vacía: muy poca probabilidad de que se trate de código dañino.

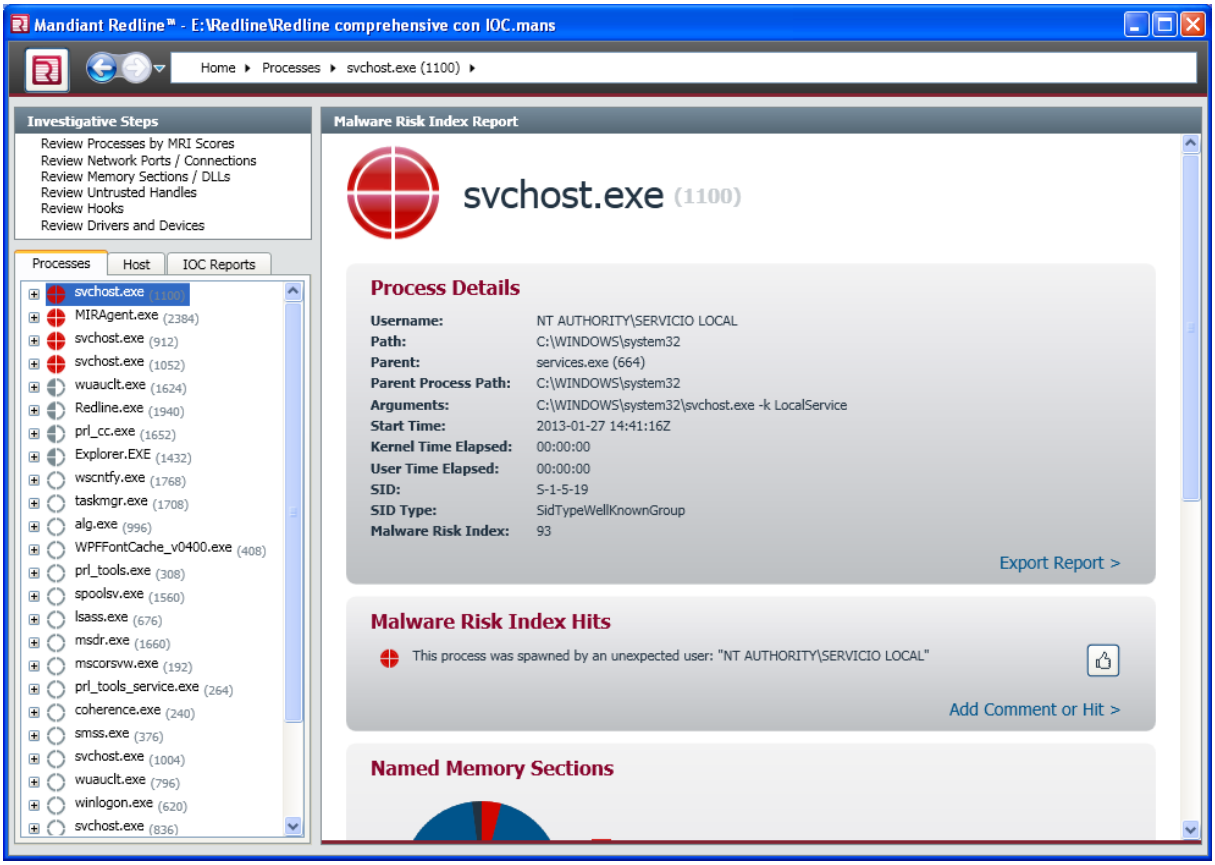


Figura 64. Resumen de los detalles de un proceso

207. Pulsando en el símbolo "+" a la izquierda de cada proceso, se despliegan las siguientes opciones:

- ***Handles:*** muestra en la zona principal las referencias de los procesos, bien sea a un fichero, a una clave del registro de Windows, etc. Desplegando esta opción se pueden ver referencias concretas:
  - *File Handles*: muestra las referencias a ficheros.
  - *Directory Handles*: muestra las referencias a directorios.
  - *Process Handles*: muestra las referencias a otros procesos.
  - *Registry Key Handles*: muestra las referencias a claves del registro.
  - *Semaphore Handles*: muestra las referencias a semáforos.
  - *Mutant Handles*: muestra las referencias del proceso a *mutant* (o *mutex*). Los *mutex* son empleados por el código dañino para identificar si un sistema ya ha sido infectado, puesto que evita que dos hilos escriban al mismo tiempo en la misma zona de memoria.
  - *Event Handles*: muestra las referencias a eventos.
  - *Section Handles*: muestra las referencias a secciones.
- ***Memory Sections:*** muestra las zonas de memoria (con sus ejecutables, drivers y demás información que se haya obtenido). Desplegando esta opción se pueden ver referencias concretas:

- *Named Memory Sections:* muestra drivers e información sobre los mismos.
- *Detailed Sections:* muestra secciones en concreto. Seleccionando una de ellas aparecerá a la derecha toda la información acerca de la misma.

- ***Strings:*** muestra los strings que pueda haber.
- ***Ports:*** muestra el uso de la red que esté haciendo el proceso.

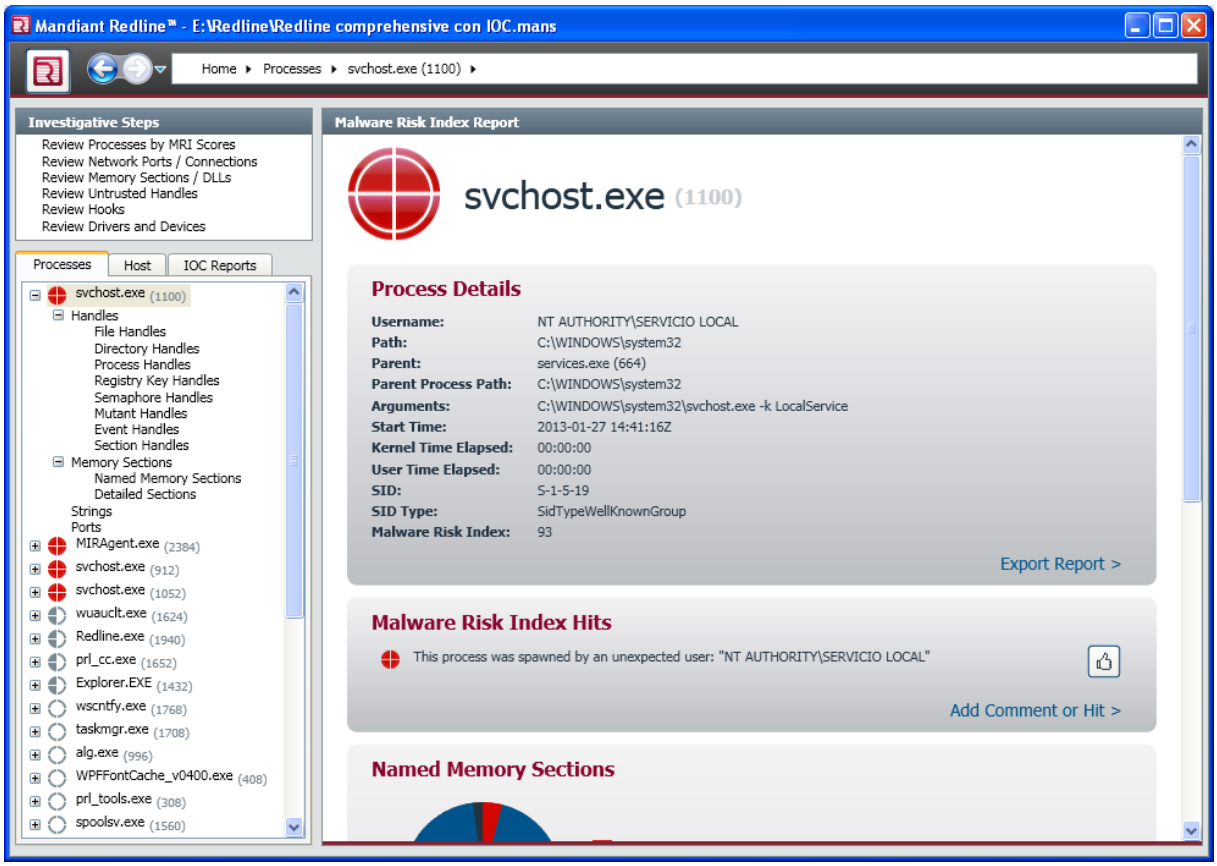


Figura 65. A la izquierda, elementos para ver los detalles de un proceso

208. En la zona central se puede ver la siguiente información del proceso seleccionado:

- ***Process detail***: información general sobre el proceso. La opción "Export Report >" almacena toda la información de la zona central a un fichero en formato Microsoft Word .docx.
- ***Código dañino Risk Index Hits***: muestra los motivos que provocan el nivel de MRI asignado al proceso. La opción "Add Comment or Hit >" abrirá una nueva ventana que permitirá marcar:
  - *Hit (Acierto):* indicar que se considere el proceso como malicioso de forma manual. El texto que se introduzca se mostrará luego en esta sección con una diana roja delante y el texto "[User Flagged]" (para recordar que se ha establecido manualmente). En la columna izquierda, donde aparecen listados los procesos, si antes el proceso no estaba marcado con una diana roja, ahora sí lo estará. Con esta información *Redline* recalculará el MRI de todos los procesos. Es posible borrar posteriormente el hit, pulsando en el botón X a su derecha.

- *Comment* (Comentario): introducir un comentario. El texto que se introduzca se mostrará luego en esta sección con una diana gris totalmente vacía delante y el texto "[Comment]" (para recordar que ese texto no es una descripción de un motivo de ser código dañino). Es posible borrar posteriormente el comentario, pulsando en el botón X a su derecha.

Pulsando en el icono se establece el motivo como un falso positivo, pasando el proceso a tener la diana gris con zonas vacías o totalmente (dependerá de que existan o no más motivos por los que se haya considerado como código dañino) y el texto "[False Positive]" (para recordar que se ha establecido manualmente). Con esta información *Redline* recalculará el MRI de todos los procesos. Es posible modificar posteriormente esta condición de falso positivo pulsando en el botón a su derecha.

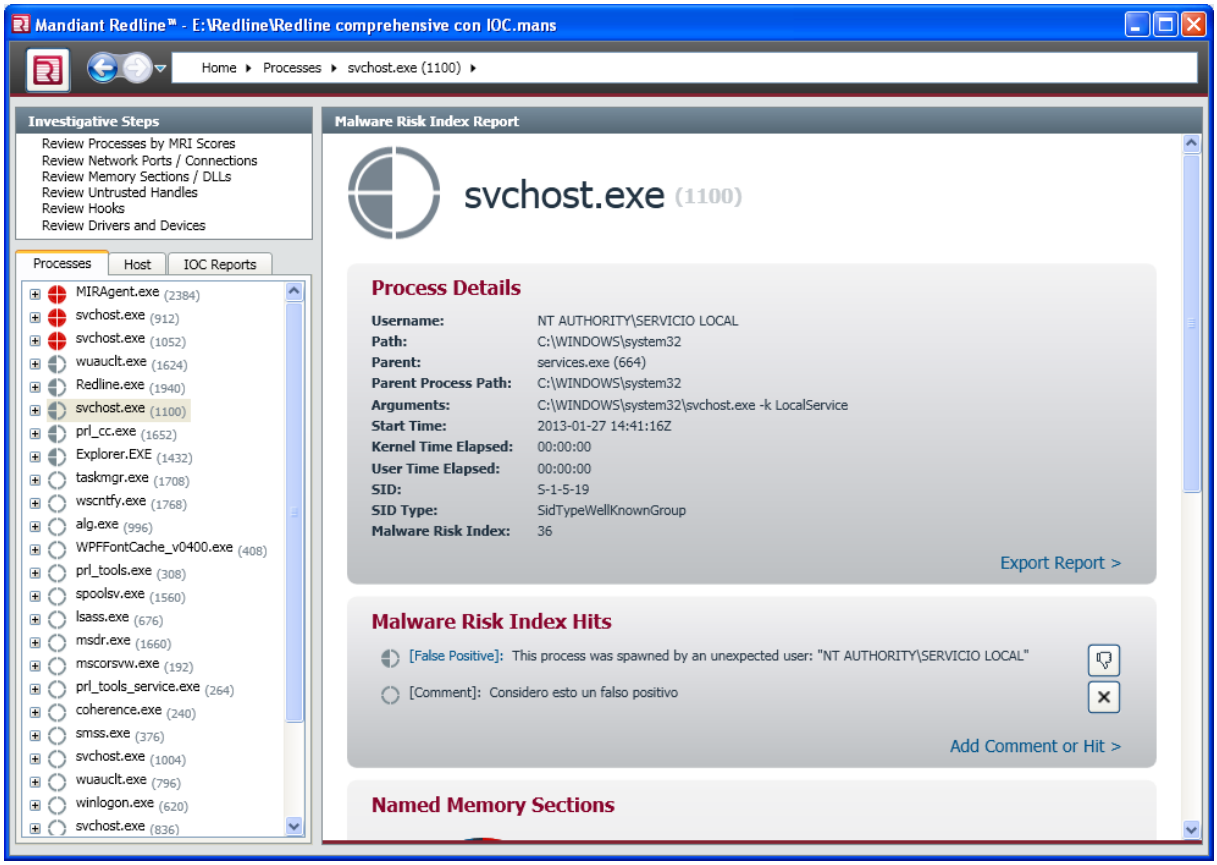


Figura 66. Establecimiento de un proceso malicioso como un falso positivo

- ***Named Memory Sections***: muestra un diagrama en forma de tarta donde se indica:
  - *Negative Factors* (Factores Negativos): porcentaje de motivos por los que se considera el proceso como código dañino. Pueden verse dichos motivos en la zona inferior en la pestaña "Negative Factors". Si se considera que uno de esos motivos es un falso positivo, es posible corregirlo como en la sección "Código dañino Risk Index Hits" pulsando en , pasando de ese modo el motivo a la pestaña "Positive Factors", pudiendo identificarlos ahí porque estarán acompañados del botón X por si cambia de opinión.

- *Positive Factors* (Factores Positivos): porcentaje de motivos por los que se considera el proceso como inocuo. Pueden verse dichos motivos en la zona inferior en la pestaña "Positive Factors". Si se considera que uno de esos motivos es un falso negativo, es posible corregirlo como en la sección "Código dañino Risk Index Hits" pulsando en , pasando de ese modo el motivo a la pestaña "Negative Factors".
- *Ignored Factors* (Factores Ignorados): porcentaje de motivos que no han sido considerados. Pueden verse dichos motivos en la zona inferior en la pestaña "Ignored Factors".

Pulsando en "Aquire Process Address Space >" se obtiene un análisis más profundo del proceso. Para ello se debe haber obtenido previamente una imagen de la memoria habiendo marcado en el agente la opción de "Acquire Memory Image".

Pulsando en "Trust Process Address Space >" se marca el espacio de memoria como inocuo, haciendo que todos los "Negative Factors" pasen a ser "Positive Factors", actualizándose así el MRI.

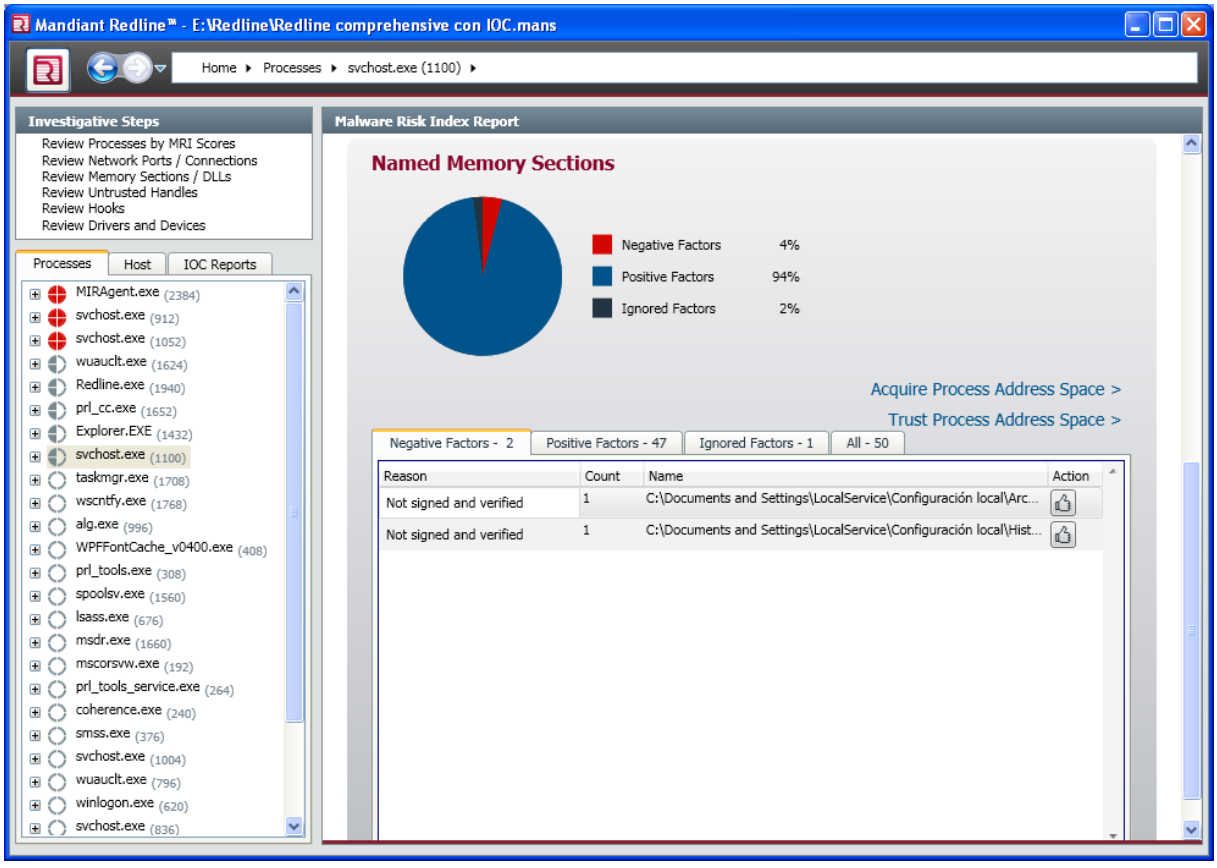


Figura 67. Revisión de las secciones de memoria

9.4.8. SISTEMA (*HOST*)

209. Esta pestaña muestra el listado de evidencias que se han obtenido del sistema, organizadas a la izquierda en forma de árbol. Puede ver toda la información que se ha ido describiendo en las pantallas, a excepción de dos nuevos elementos:

- ***Acquisition History***: muestra las adquisiciones de datos realizados. Es posible cambiar el directorio donde se encuentran las evidencias recogidas por el agente, pulsando en el botón con el icono del lápiz. Para adquirir datos de un proceso o driver, debe pulsarse pulse con el botón derecho sobre uno de esos elementos y seleccionar "Acquire this Process Address Space", pudiendo así extraer de la imagen de memoria que se hubiera realizado (habiendo marcado en el agente la opción de "Acquire Memory Image"), los procesos y drivers para analizarlos con otras herramientas.
- ***Timeline:*** muestra evidencias del sistema (cualquiera que pueda ser asociada a un momento determinado) de forma cronológica. Puede mostrarlas de diversos modos en función de la pestaña seleccionada en la zona inferior:
  - *Fields:* muestra las evidencias que contienen alguna fecha, pudiendo seleccionar cuáles se desea que se muestren. En la zona principal se mostrarán dichos elementos ordenados cronológicamente. De este modo puede ver lo que sucedió en el sistema en algún momento, fuere lo que fuere.

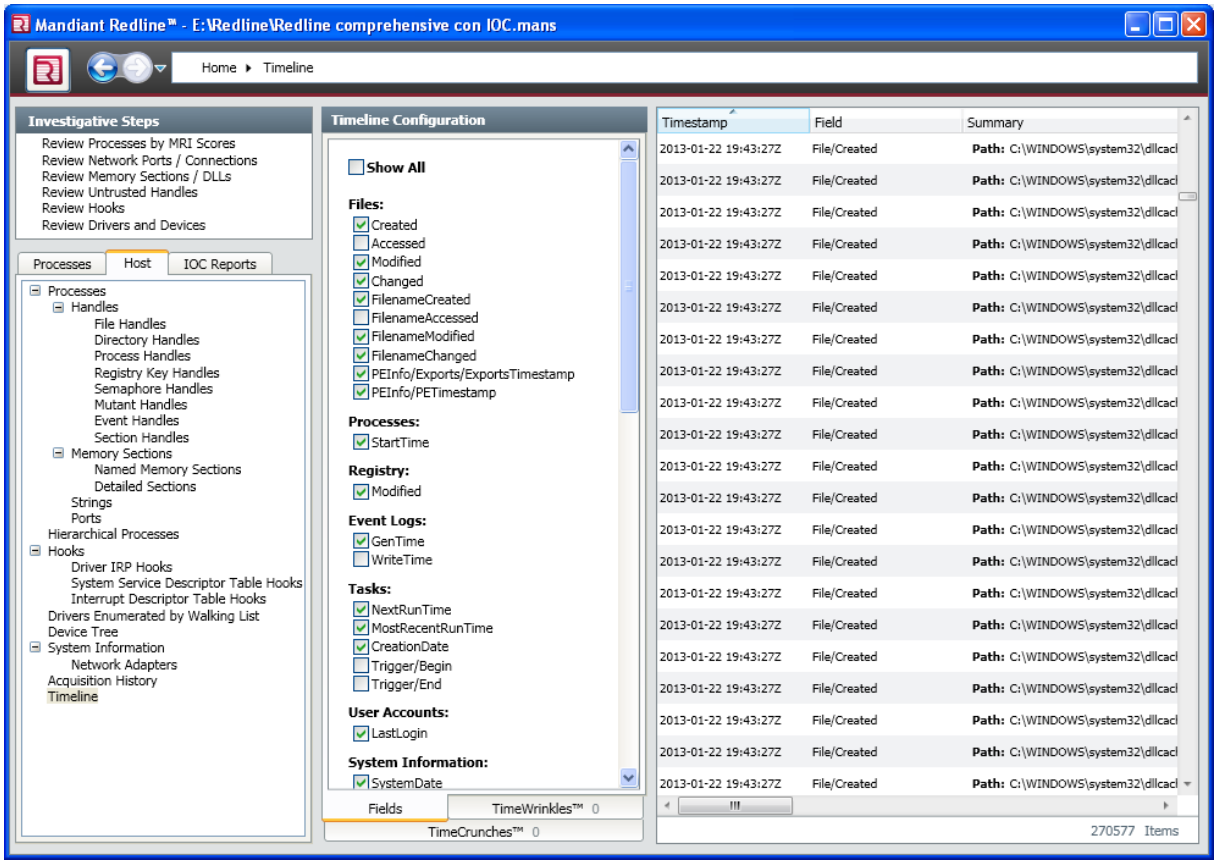


Figura 68. Evidencias del sistema de forma cronológica

  - *TimeWrinkles:* permite establecer, alrededor de una fecha, una ventana de tiempo, para ver qué eventos ocurrieron en dicha ventana. Se puede definir dicha ventana de forma manual, pulsando el botón "New Custom TimeWrinkle" y definiendo la fecha y hora alrededor de la que se desee definir la ventana de tiempo (en el campo "Show" pueden definirse los minutos a mostrar antes y después de esa fecha), o en base a un evento que

se haya visto en la anterior ventana "Fields" (pulsando con el botón derecho del ratón sobre él y seleccionando "Add New TimeWrinkle" en el menú desplegable que aparece).

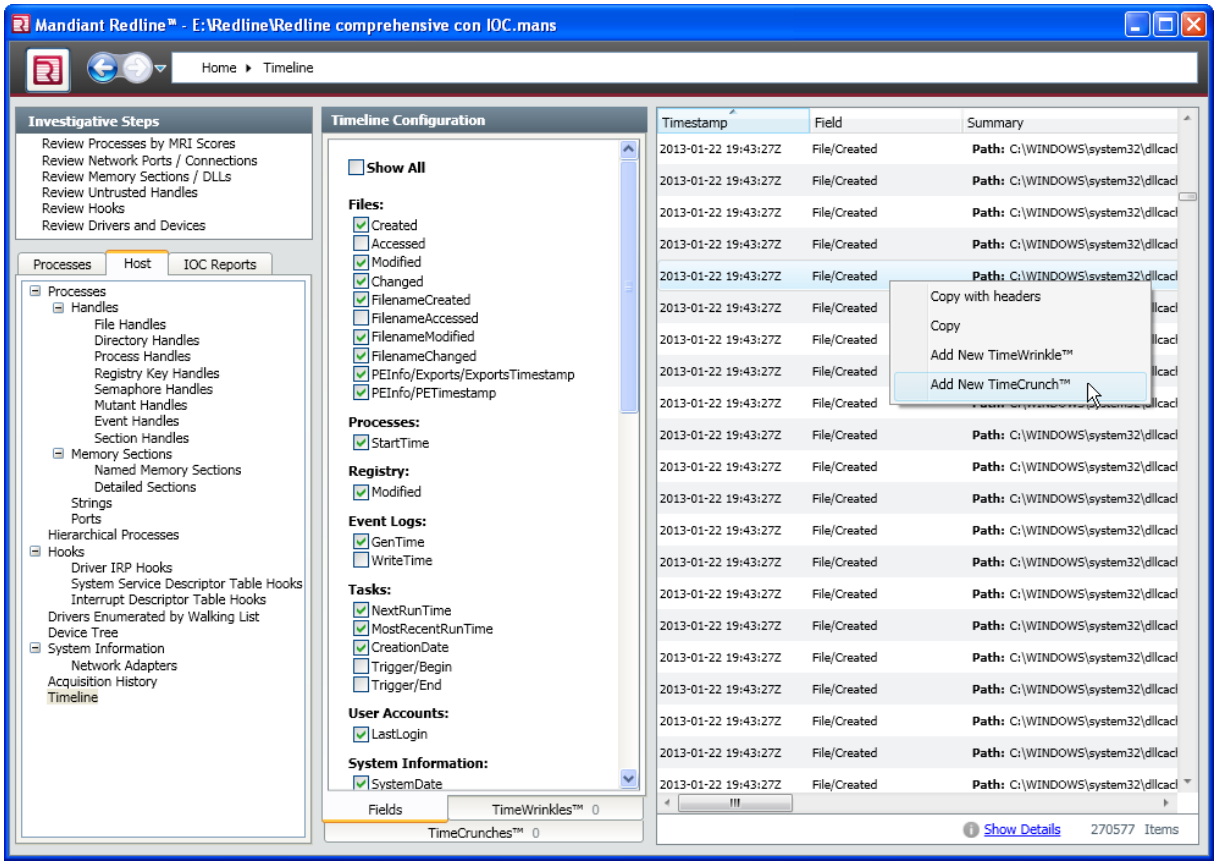


Figura 69. Adición de un evento alrededor del cual se analizará lo sucedido

- *TimeCrunches:* permite ocultar eventos del mismo tipo que ocurrieron durante el mismo minuto. Esto permite quitar elementos que no aportan nada y que sólo generan ruido, dificultando el análisis. Se puede definir dicha ventana de forma manual, pulsando el botón "New Custom TimeCrunch". Se puede definir el tipo de evidencia así como la fecha y hora alrededor de la que eliminar las evidencias, o en base a un evento que se haya visto en la anterior ventana "Fields" (pulsando sobre él con el botón derecho del ratón y seleccionando "Add New TimeCrunch" en el menú desplegable que aparece). Pueden establecerse tantos TimeCrunch como se quiera.

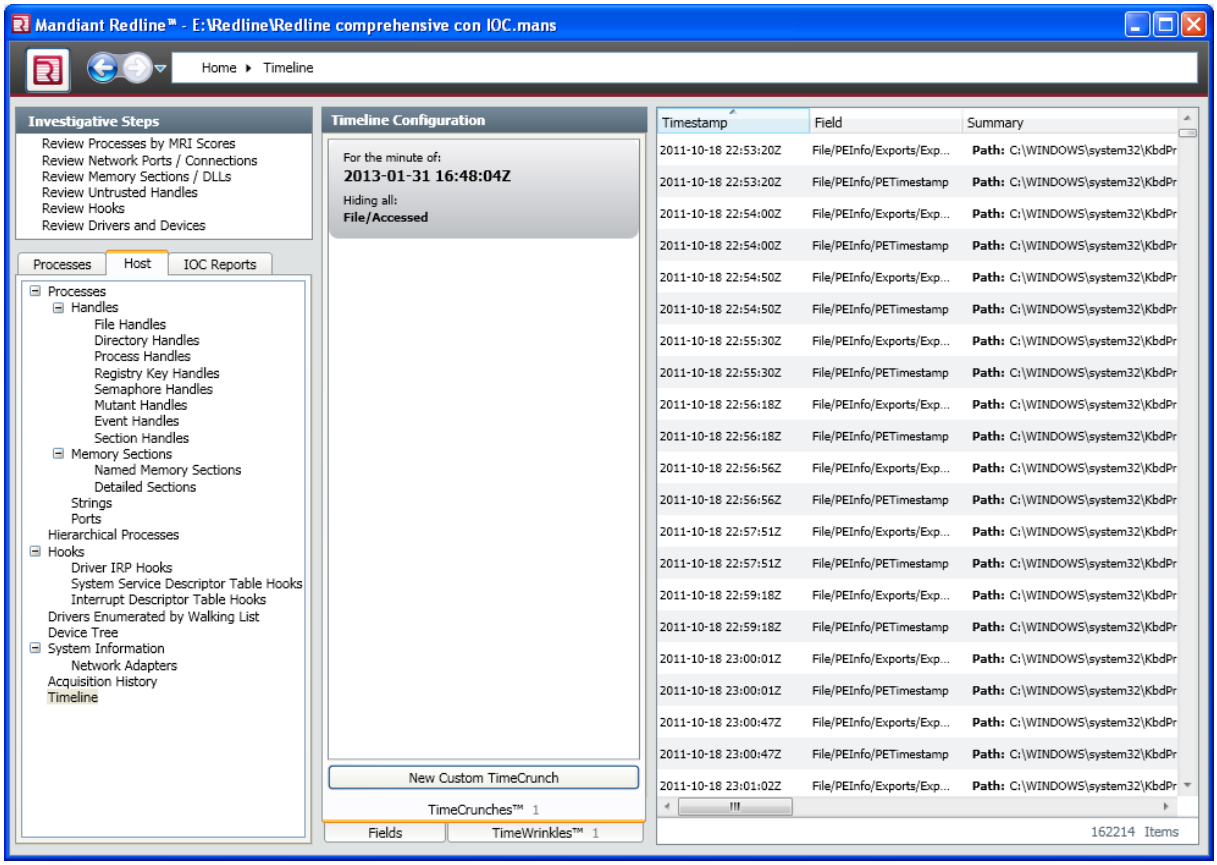


Figura 70. Ocultar eventos de cierto tipo alrededor de cierto momento

9.4.9. INFORMES DE IOC (*IOC REPORTS*)

210. Esta pestaña permite generar informes sobre las evidencias según los indicadores de compromiso que se detecten. Para ello, habrá que indicar la carpeta donde se encuentren los ficheros .IOC (pulsando el botón "Browse").

211. Una vez hecho esto y tras pulsar "OK", se realizará el análisis, dando como resultado el informe en formato Microsoft Word.

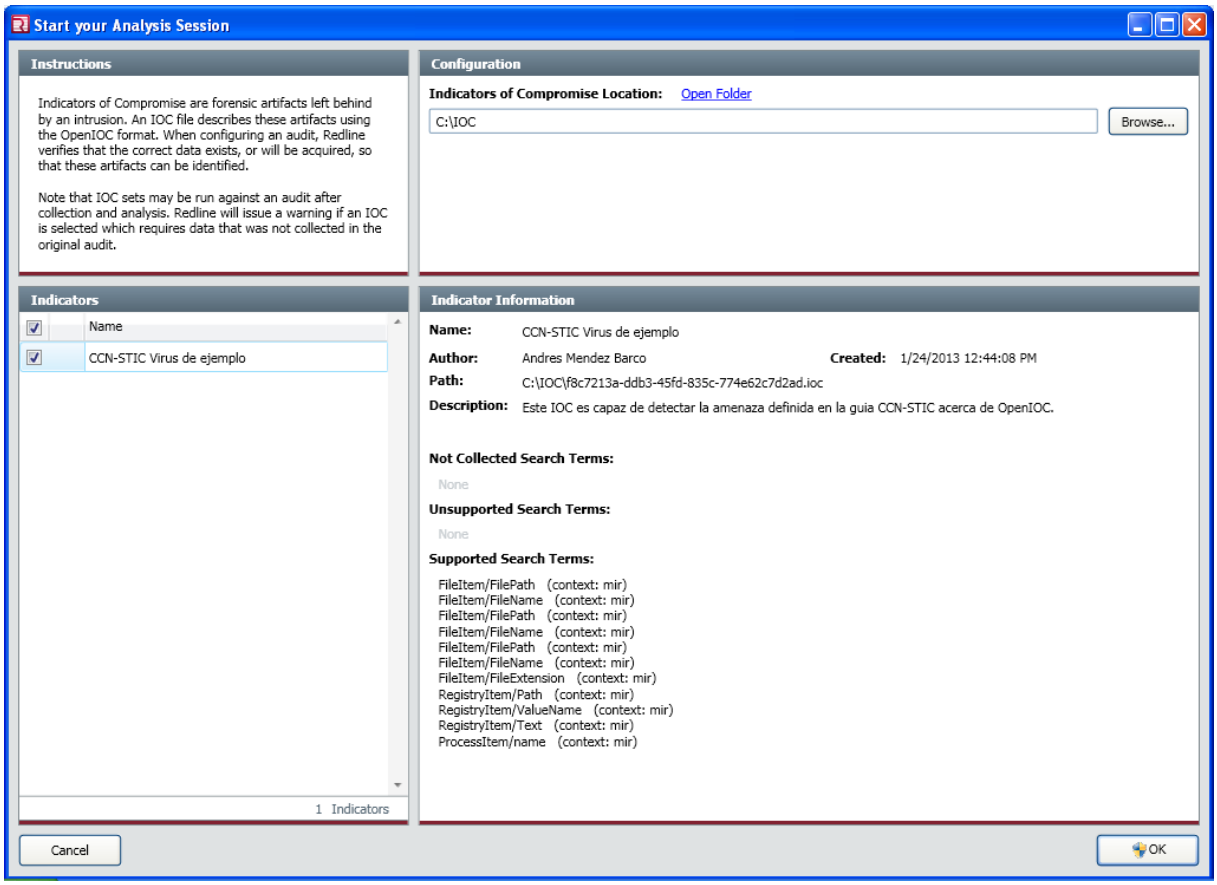


Figura 71. Selección de IOCs con los que analizar las evidencias recopiladas

10. REPOSITORIO DE IOC

212. Puede encontrar algunos ejemplos de ficheros IOC en http://www.openioc.org/iocs/

213. El Centro Criptológico Nacional (CCN) genera también sus propios IOC, que distribuye a las distintas Organizaciones según sus necesidades.

214. El portal REYES (Repositorio común y estructurado de amenazas y código dañino) se encuentra diseñado para ser un repositorio de IOC en sí mismo, por lo que también, a través de esta vía, podrá encontrar múltiples ficheros IOC para su descarga y distribución.

11. COMPARTICIÓN DE INTELIGENCIA CON REYES

215. Cuando se enfrenta un caso de respuesta ante un incidente concreto, se puede presentar la casuística de tener que compartir información de tipo no clasificada con otras organizaciones con el fin de dar celeridad a la investigación, conseguir una mejor y rápida respuesta, y ayudar a mejorar el conocimiento de una ciberamenaza concreta.

216. La plataforma REYES (Repositorio común y estructurado de amenazas y código dañino) está conceptualizada y diseñada bajo la premisa de tener un repositorio organizado de información relativa a inteligencia. Como plataforma de intercambio, el sistema está diseñado para ofrecer distintas capacidades de interrelación entre las distintas entidades que colaborarían en una instancia REYES y también entre distintas instancias REYES.

11.1. CREACIÓN DE EVENTO

217. Para poder importar un fichero de tipo IOC, es necesario generar un evento en la plataforma REYES. Para hacerlo, tan solo es necesario pulsar en el botón Add Event, tal y como se muestra en la siguiente figura:

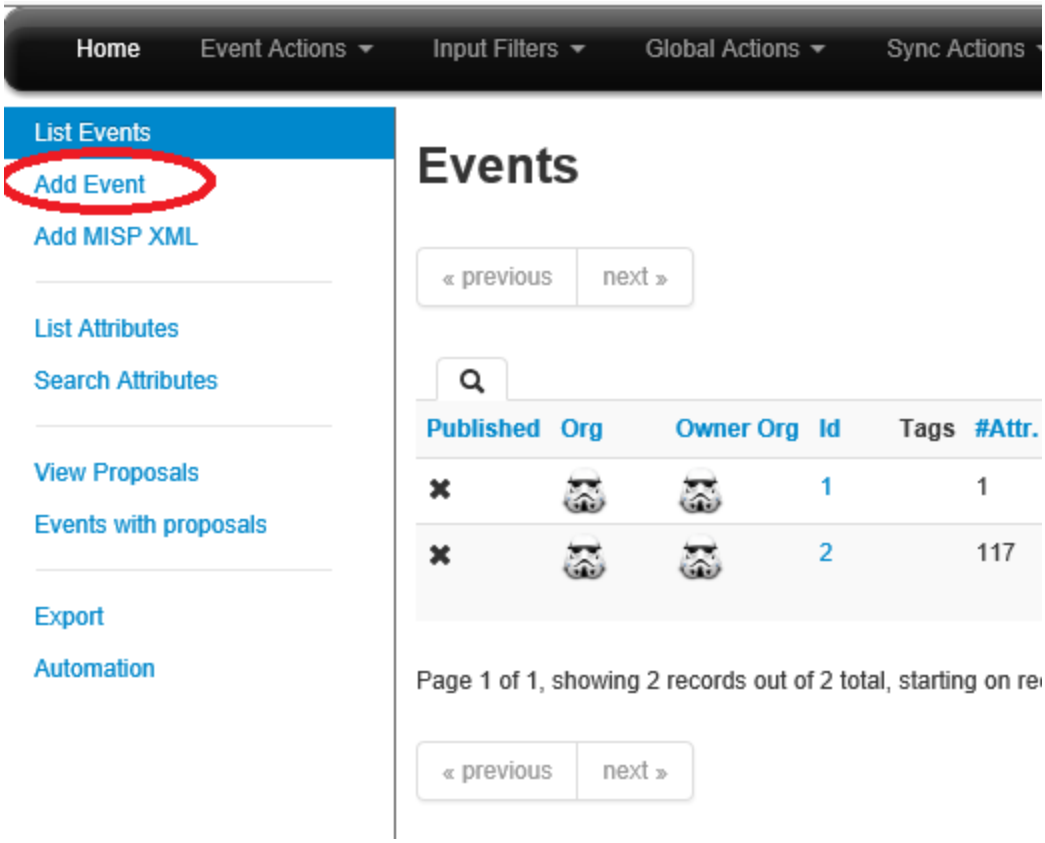


Figura 72. Creación de evento en REYES

218. A la hora de crear un evento, se solicitarán datos sencillos, como un nombre descriptivo, la fecha de entrada del evento, o el tipo de distribución de la evidencia.

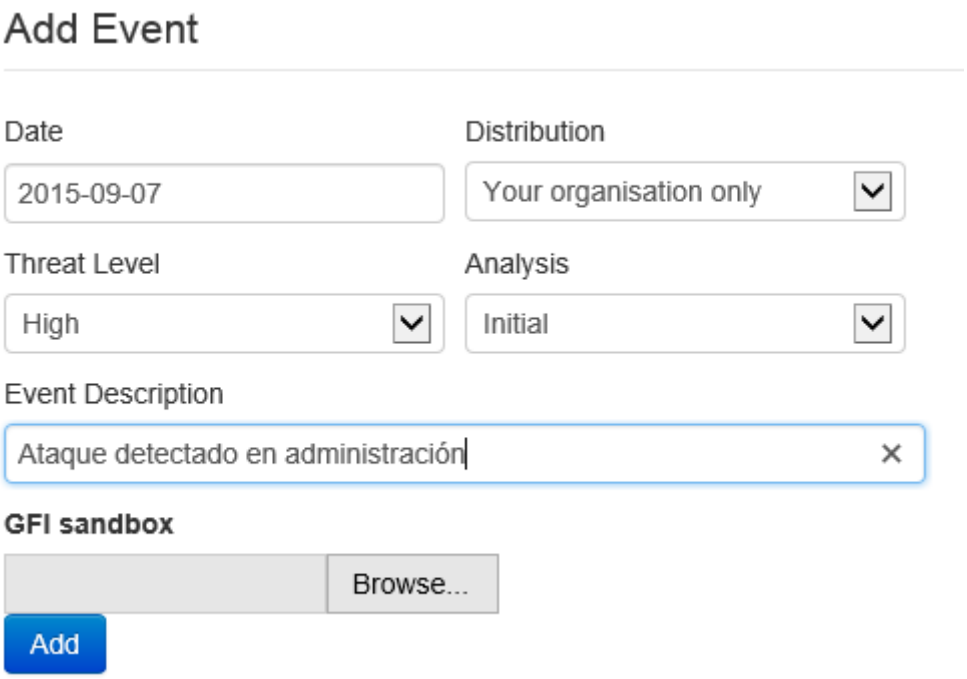


Figura 73. Formulario de creación de evento en REYES

219. Una vez rellenado el formulario, y pulsado el botón Add, se habrá generado el evento de manera satisfactoria.

11.2. IMPORTAR DATOS DESDE FICHEROS IOC

220. Para importar ficheros de tipo IOC, se deberá hacer pulsando en el enlace con leyenda *Populate from OpenIOC*, tal y como se muestra en la siguiente figura:

Figura 74. Importar fichero IOC en REYES

221. El funcionamiento de este formulario es muy sencillo, sólo necesitando subir el fichero de tipo IOC, y pulsando el botón Upload.

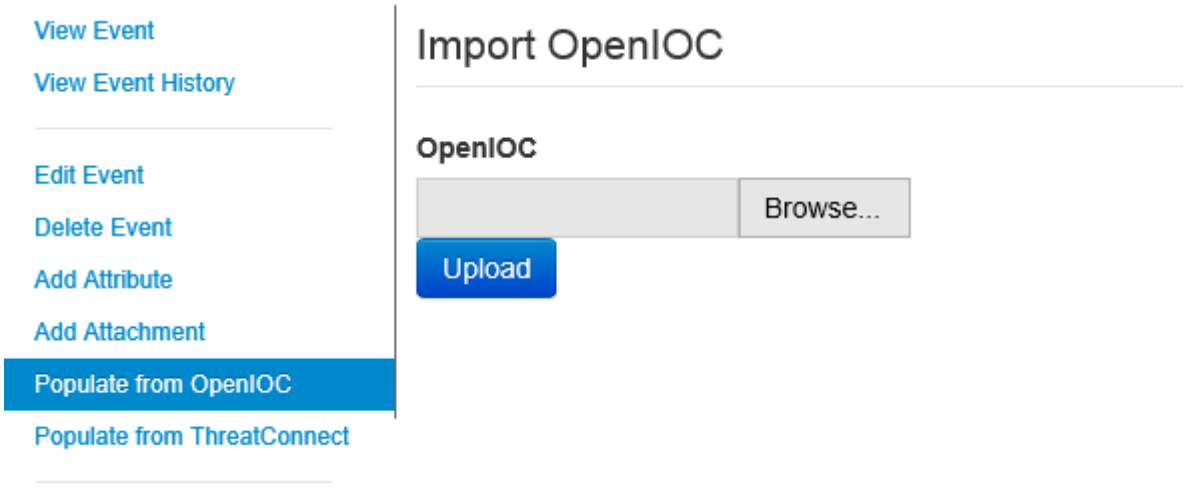


Figura 75. Formulario de subida de ficheros IOC en REYES

222. Una vez subido el fichero de tipo IOC, y si todo ha ido correctamente, se mostrará una pantalla a modo resumen, indicando aquellos indicadores que se han subido correctamente.

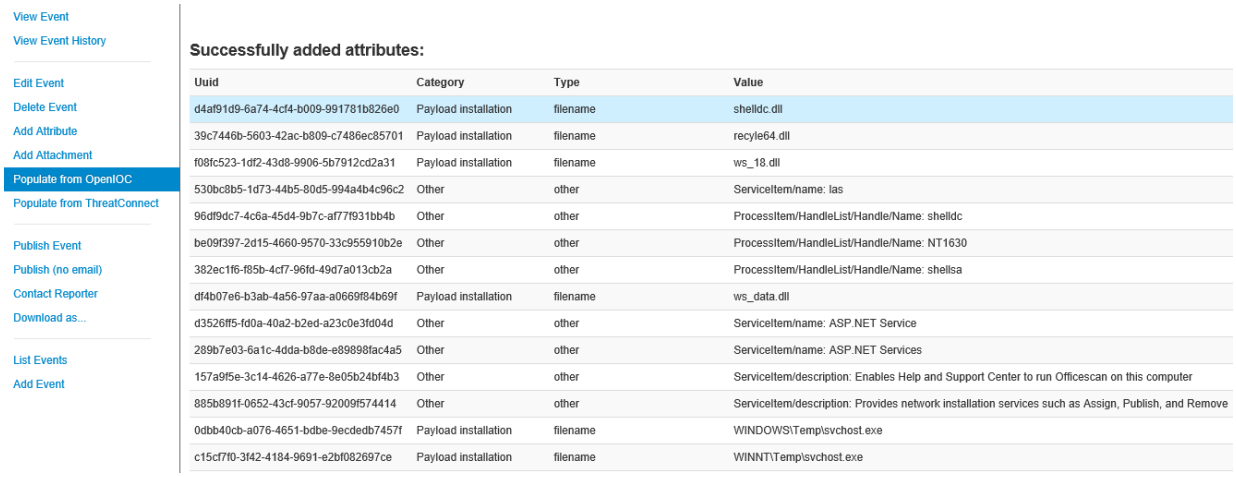


Figura 76. Indicadores subidos correctamente en REYES

11.3. DESCARGA DE FICHEROS IOC

A través del portal de REYES es posible también la descarga de inteligencia en múltiples formatos. Algunos ejemplos son CSV, JSON[19] o formato IOC.

Para la descarga de inteligencia en formato IOC, es posible realizarlo a través de dos vías. La elección de una de ellas dependerá de cómo se hayan subido las evidencias a la plataforma.

[19] Java Script Object Notation.

Si el evento creado en la plataforma REYES se ha alimentado en base a ficheros IOC previamente generados – por ejemplo con la herramienta Redline (Mandiant) -, éstos todavía pueden ser descargados desde la plataforma, ya que en el diseño de la misma se contempla que funcione como un repositorio de IOC. Para realizar este paso, tan sólo debe de buscar el evento deseado, y descargar el fichero IOC correspondiente, tal y como se muestra en la siguiente figura:

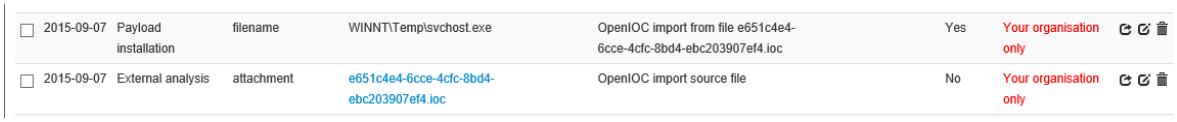


Figura 77. Descarga de ficheros IOC desde REYES

En el caso de que la alimentación de estos eventos se haya producido de manera manual, o sin ayuda de ficheros IOC, es necesario publicar el evento correspondiente para que la plataforma REYES pueda generar, en base a los datos publicados, un fichero IOC.

Para ello, y una vez localizado el evento, se procederá a publicarlo. En función de los cambios realizados en el evento, es posible publicar el mismo y enviar un mensaje de alerta, o publicar el evento sin enviar el mensaje. Una vez decidido este paso se procederá a publicar el evento pulsando el botón "Publish", tal y como aparece en la siguiente figura:

Figura 78. Publicación de evento en REYES

Una vez publicado el evento, en la información general del mismo aparecerá como publicado, tal y como se muestra en la siguiente figura:

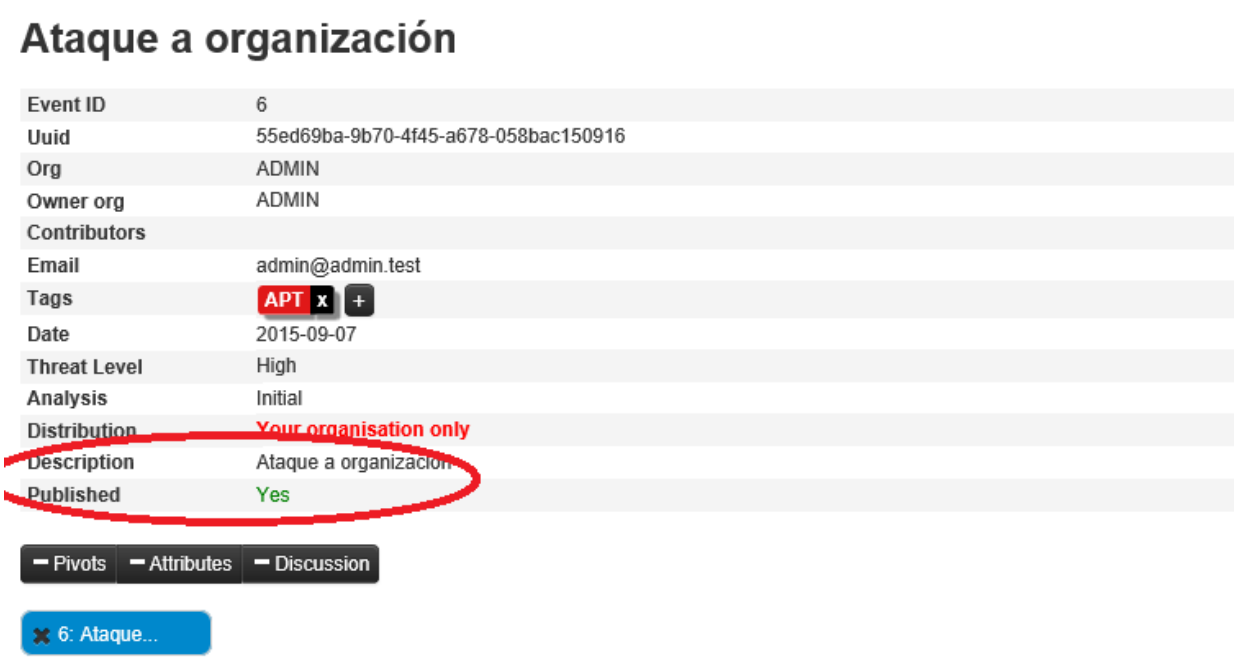


Figura 79. Evento pulicado en REYES

Una vez publicado con éxito un evento, posibilita la descarga de éste en múltiples formatos, incluido el formato IOC.

Para la descarga del evento en formato IOC, sólo tiene que pulsar el botón "Download as" y elegir el formato del mismo, el cual es, en este caso, OpenIOC, tal y como se muestra en la siguiente imagen:

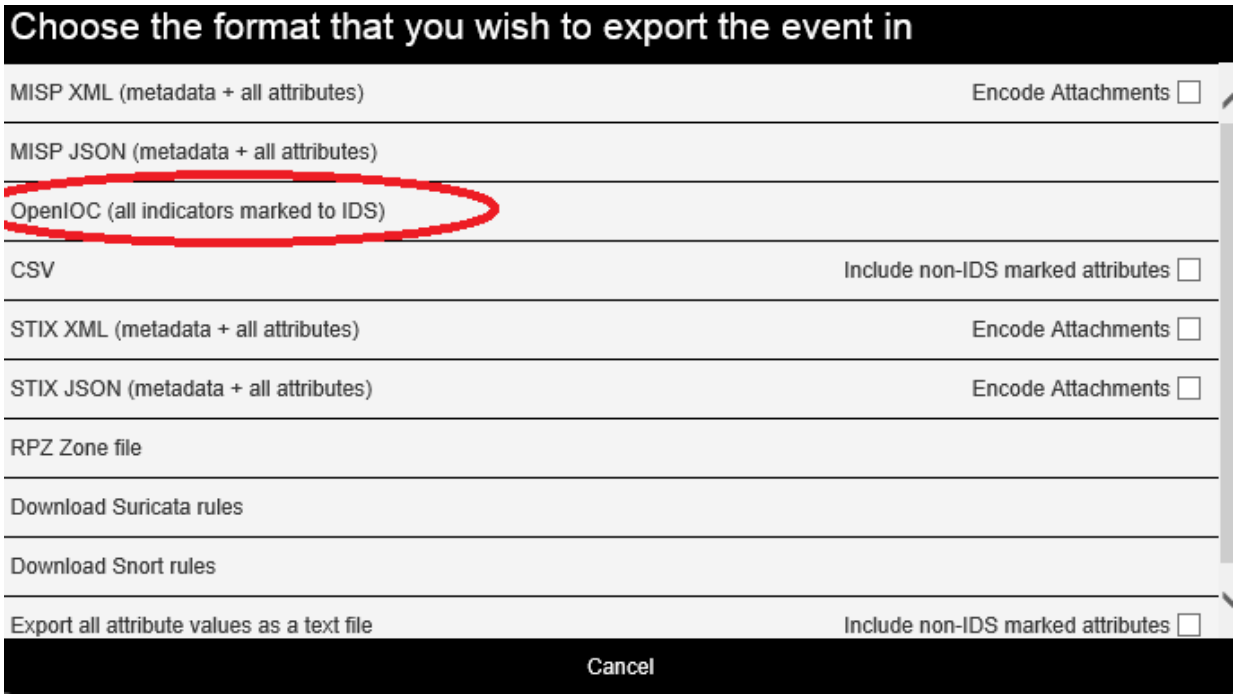


Figura 80. Descarga de fichero OPENIOC en REYES

Una vez pulsado el botón de OpenIOC, REYES generará con los datos del evento un fichero IOC compatible para ser importado.

```
<?xml version="1.0" encoding="utf-8"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <short_description>Event #6</short_description>
  <description>Ataque a organización</description>
  <keywords />
  <authored_by>ADMIN</authored_by>
  <authored_date>2015-09-07T00:00:00</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="55ed69ba-9b70-4f45-a678-058bac150916">
      <IndicatorItem id="d4af91d9-6a74-4cf4-b009-991781b826e0" condition="is">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">shelldc.dll</Content>
      </IndicatorItem>
      <IndicatorItem id="39c7446b-5603-42ac-b809-c7486ec85701" condition="is">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">recyle64.dll</Content>
      </IndicatorItem>
      <IndicatorItem id="f08fc523-1df2-43d8-9906-5b7912cd2a31" condition="is">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">ws_18.dll</Content>
      </IndicatorItem>
      <IndicatorItem id="df4b07e6-b3ab-4a56-97aa-a0669f84b69f" condition="is">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">ws_data.dll</Content>
      </IndicatorItem>
      <IndicatorItem id="0dbb40cb-a076-4651-bdbe-9ecdedb7457f" condition="is">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">WINDOWS\Temp\svchost.exe</Content>
      </IndicatorItem>
      <IndicatorItem id="c15cf7f0-3f42-4184-9691-e2bf082697ce" condition="is">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">WINNT\Temp\svchost.exe</Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
```

Figura 81. Descarga de fichero IOC en REYES

ANEXO A. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Término	Significado
APT	Advanced Persistent Threat (Amenaza Avanzada Persistente)
CERT-EU	Computer Emergency Response Team. European Union
CIRCL	Computer Incident Response Center Luxemburg
CSV	Comma Separated Values
DLL	Dynamic Link Library
FAT	File Allocation Table
HASH	Función resumen
HTML	Hyper Text Markup Language
IDT	Interrupt Description Table
IRP	Input/Output Request Packets
IOC	Indicator of Compromise (Indicador de Compromiso), o fichero que contiene la definición de indicadores de compromiso mediante XML
JSON	Java Script Object Notation
MIR	Mandiant Incident Response
MRI	Malware Risk Index (Indicador de Riesgo de Código dañino)
NCIRC	Nato Computer Incident Response Capability
NDIS	Network Driver Interface Specification
NTFS	New Technology File System
SSDT	System Service Descriptor Table
XML	eXtensible Markup Language
STIX	Structured Threat Information eXpresion
TCPIP	Transmision Control Protocol Internet Protocol
REYES	REpositorio común Y EStructurado de amenazas y código dañino

ANEXO B. REFERENCIAS

CCN-STIC-403 Gestión de Incidentes de Seguridad
CCN-STIC-424 Intercambio de información de ciberamenaza STIX-TAXII. Empleo de REYES
CCN-STIC-425 Ciclo de Inteligencia y Análisis de Intrusiones
CCN-STIC-426 REYES. Manual de usuario (en preparación)
CCN-STIC-431 Herramientas de Análisis de Vulnerabilidades
CCN-STIC-503A Seguridad en Windows 2003 Server (controlador de dominio)
CCN-STIC-817 Gestión de Ciberincidentes