CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

INTECO (cert)

EL PUESTO DEL OPERADOR

Guía básica de protección de Infraestructuras Críticas

INTECO Instituto Nacional de Tecnologías de la Comunicación
www.inteco.es
@intecocert

Noviembre 2013

INDICE

Autores

Jesús Díaz Vico

Daniel Fírvida Pereira

Marco Antonio Lozano Merino

Coordinación

Deepak Daswani Daswani

Elena García Díez

1 OBJETIVO DE LA GUÍA

Esta guía básica de protección de Infraestructuras Críticas relativa al Puesto del Operador pretende recoger una referencia de los aspectos esenciales de seguridad relativos al puesto del usuario o del operador SCADA.

Para ello, se hace referencia a las amenazas que pueden tener mayor impacto en una infraestructura tecnológica de este tipo, ofreciendo en la mayoría de los casos soluciones y alternativas aplicables de alto nivel.

Características, necesidades y tecnologías sectoriales específicas presentes en determinados puestos de operador pueden limitar la aplicación directa de algunas medidas contempladas en esta guía. La aplicabilidad a entornos concretos ha de valorarse de forma proporcional a factores tecnológicos, propiedades técnicas de los sistemas a proteger o el modelo de negocio de la compañía interesada. En este aspecto, por lo tanto, la guía debe contemplarse como una serie de medidas deseables, pero no siempre estrictamente necesarias, para mejorar la seguridad del puesto de los operadores de infraestructuras críticas. Adicionalmente, estando la guía destinada a la protección del Puesto del Operador de Infraestructuras Críticas, siendo inherente a éste la necesidad de unos elevados requisitos de seguridad, se asumirá que estos equipos están adheridos a las políticas de seguridad corporativas, por lo que medidas de seguridad básicas, como el uso de contraseñas robustas, se dan por supuestas.

Nótese que algunos fragmentos de este documento se apoyan en el contenido del informe "Detección de APTs" elaborado por INTECO y CSIRT-CV, disponible en el portal de INTECO-CERT[1] o el portal de CSIRT-CV[2]. Dicho informe puede ayudar a una correcta interpretación del contenido.

Esta publicación técnica se enmarca en las acciones específicas del CERT de Seguridad e Industria en su línea de trabajo de protección de Infraestructuras Críticas definida en el convenio suscrito en octubre de 2012 por la Secretaria de Estado de Seguridad (SES), dependiente del Ministerio del Interior, y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), dependiente del Ministerio de Industria, Energía y Turismo, para la cooperación efectiva en materia de ciberseguridad entre CNPIC, FCSE e INTECO.

[1] http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf
[2] http://www.csirtcv.gva.es/sites/all/files/downloads/Detecci%C3%B3n_APT.pdf

2 EL USUARIO

Gran parte de los incidentes que se producen en los sistemas de Tecnologías de la Información son provocados por sus propios usuarios. En el caso de entornos SCADA o de carácter industrial, a pesar de tratarse de sistemas con una criticidad elevada y que cuentan con controles adicionales, podría ocurrir lo mismo. Por esta razón, uno de los elementos clave que se tratarán en esta guía comprenderá las acciones destinadas a los aspectos técnicos y buenas prácticas a la hora de interactuar con elementos que forman parte de este entorno, como es el caso de las *Human Machine Interfaces* (HMI).

Ofrecer a los usuarios información relativa a los distintos tipos de amenazas existentes, así como el modo de mitigarlas, es uno de los aspectos clave a la hora de hacer frente a los peligros que acechan los sistemas informáticos.

TIPOS DE AMENAZAS

Los entornos SCADA, a pesar de contar con dispositivos desarrollados específicamente para realizar tareas especializadas, por lo general adolecen de los mismos problemas de seguridad que otras arquitecturas tecnológicas, principalmente porque comparten tecnologías como sistemas operativos o dispositivos de red. Si a la característica anterior se le añade que estas están gestionadas y manejadas por humanos, se puede hablar de una infraestructura sujeta a multitud de problemas de seguridad, sin mencionar las vulnerabilidades propias de dispositivos específicos, como PLCs.

En los puntos siguientes se explican las amenazas que pueden tener mayor impacto dentro de una arquitectura SCADA.

APTS (ADVANCED PERSISTENT THREAT)

En la actualidad, **los ciberataques y los fallos en los sistemas de las infraestructuras críticas se encuentran en el Top 5 de riesgos globales** según el reciente informe 'Global Risks 2012'[3] que publica cada año el World Economic Forum (WEF)[4], en el que refleja la interconexión actual entre riesgos geopolíticos, ambientales, sociales, económicos y tecnológicos.

Dentro de los riesgos tecnológicos, los ciberataques ocupan un lugar preeminente como principal preocupación, ya que poseen un elevado impacto y grado de probabilidad de ocurrencia.

En los últimos 4 años el número de amenazas cibernéticas se ha multiplicado de manera exponencial produciéndose además un cambio en la naturaleza de las mismas: se ha pasado de amenazas conocidas, puntuales y dispersas, a amenazas de gran sofisticación, persistentes, y con objetivos muy concretos, surgiendo una nueva categoría de amenazas en el mundo del cibercrimen, las *Advanced Persistent Threats* (Amenazas Persistentes y Avanzadas), en adelante **APT o APTs**.

Las APT se caracterizan por ser amenazas reales sofisticadas que, aunque no siempre tienen una alta complejidad técnica, suponen acciones muy premeditadas y persistentes, siendo altamente eficaces ante las contramedidas establecidas en el/los sistema/s objetivo.

[3] http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf
[4] http://www.weforum.org/

Con un marcado carácter silencioso, sus pretensiones son elevadas: los afectados raramente son conscientes de que son objetivo de un ataque y desconocen su origen, alcance o autoría. Una vez definido un único objetivo, los cibercriminales iniciarán una campaña ofensiva en la que no importa el tiempo que se invierta.

Los atacantes no esperan conseguir un beneficio a corto plazo (como pudieran buscar otros tipos de ataques masivos), sino que prefieren pasar desapercibidos, mientras actúan constantemente hasta alcanzar su objetivo. Entre estos objetivos se encuentran: **económicos** (espionaje), **militares** (búsqueda de debilidades, revelación de información), **técnicos** (credenciales, código fuente) o **políticos** (desestabilizar, desorganizar o debilitar misiones diplomáticas), afectando a sectores tan diversos y críticos como el gubernamental, financiero, tecnológico, centros de investigación, etc.

INGENIERÍA SOCIAL

Al inicio de este punto se comentaba que el factor humano (el usuario) es uno de los elementos más críticos a la hora de llevar a cabo un plan de seguridad. Consecuentemente, la ingeniería social es, sin duda, el punto más vulnerable del usuario.

Se denominan técnicas de ingeniería social a todas aquellas prácticas por las cuales el atacante intenta conseguir su objetivo a través del engaño y/o la manipulación de las personas, ya sea para obtener información privilegiada, conseguir que el usuario visite un determinado enlace, abra un documento que se le envía por correo o deje pasar a un desconocido en las instalaciones de la organización, por ejemplo. En definitiva, **que la víctima haga despreocupadamente acciones que puedan perjudicarle bien a él o a la organización para la que trabaja**.

Mediante este tipo de técnicas se derivan otras muchas que, haciendo uso de diferentes tecnologías como el correo electrónico, la navegación, etc., pueden dar lugar distintas vías de infección.

SPEAR PHISING ATTACKS

Esta técnica consiste en utilizar la ingeniería social para engañar al usuario por medio del correo electrónico, teniendo como objetivo usuarios o compañías específicas. Quizás el ejemplo más representativo es el envío de un correo con una URL o adjunto malicioso y con un mensaje sugerente que incite a la víctima a abrir el mismo. En dichos correos suelen adjuntarse ficheros PDF, DOC, XLS, etc. que tratarán de explotar alguna vulnerabilidad para ejecutar código dañino en el equipo. En el peor de los casos contarán con *0-days*, los cuales ofrecerán más garantías de éxito para conseguir acceso a la máquina, incluso aunque la víctima cuente con software correctamente actualizado. Los *Spear Phising Attacks* se encuentran entre los métodos más utilizados como vía de infección.

INFECCIONES A TRAVÉS DE SITIOS WEB

Mediante esta técnica, un atacante hace que el usuario se infecte sólo con visitar un determinado sitio web previamente comprometido. En líneas generales, el funcionamiento es el siguiente: los atacantes buscan un sitio web vulnerable e inyectan un *script* malicioso entre su código HTML. La víctima visita la página comprometida y el sitio web devuelve la página consultada junto con el código malicioso, el cual generalmente obligará al navegador de la víctima a hacer nuevas peticiones a otros servidores web controlados también por el atacante. Desde estos servidores web maliciosos, el atacante intentará explotar alguna vulnerabilidad del navegador del usuario, descargando malware e infectando al equipo del usuario en caso de un ataque exitoso.

Lo habitual es encontrar código malicioso inyectado a través de un *iframe* en la web vulnerada que es visitada por el usuario. Este *iframe* abre en paralelo, de manera prácticamente trasparente al usuario, de un segundo sitio web, que será el que invoque la descarga y ejecución del malware que infecte al usuario. Otra opción es que la web

[5] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

vulnerada haga una redirección al sitio malicioso.

DISPOSITIVOS FÍSICOS

Otro de los métodos que se podría utilizar para introducir malware en una empresa u organización es a través de dispositivos físicos. Basta con la conexión a la red de USBs, CDs, DVDs, tarjetas de memoria o equipamiento IT infectados para introducir el malware en la organización objetivo.

Como ejemplo, en el caso de los ataques dirigidos con Stuxnet[6], la infección inicial del mismo se realizó a través de un USB infectado (algunas fuentes indican que fue introducido por un doble agente que **trabajaba para** Israel utilizando un USB para infectar las máquinas de las instalaciones nucleares de Natanz).

En un hipotético escenario, el atacante podría, a través de técnicas de ingeniería social y otro tipo de artimañas, burlar la seguridad física de las instalaciones de la organización objetivo y acceder con un USB infectado a un equipo conectado a la red corporativa. Otro escenario de ataque posible podría ser que el atacante suplante la identidad de un cliente, colaborador, o se haga pasar por alguien interesado en el organismo objetivo en cuestión y regale, dentro de una supuesta campaña de marketing, dispositivos USB, tarjetas de memoria, CDs o DVDs, *smartphones*, *tablets*, portátiles o cualquier tipo de dispositivo infectado a los empleados, incluso software. Es posible que el atacante haga llegar a las víctimas software pirata malicioso empaquetado de forma que imita el empaquetado del fabricante original y que los usuarios objetivos no se den cuenta del engaño. O el "típico" ejemplo de dejar "olvidado" un USB infectado con una etiqueta que indique "Información privada". Es muy probable que la curiosidad del usuario que encuentre ese USB "perdido" le haga conectarlo a su equipo, infectándolo. Hay que recordar que el ser humano es curioso por naturaleza y muchas técnicas de ingeniería social funcionan bajo esa premisa.

VULNERABILIDADES EN LOS DISPOSITIVOS Y 0-DAYS

Aunque se han mencionado brevemente en los puntos previos, existen otras amenazas que son difíciles de mitigar. Se trata de aquellos fallos que se encuentran "embebidos" en los dispositivos específicos, como PLC's por ejemplo, que forman parte de la arquitectura de un sistema SCADA o componen los elementos que controlan alguna infraestructura crítica. Estas vulnerabilidades inicialmente quizás no supusieran un problema ya que los sistemas se encontraban desconectados de Internet, pero una vez que las infraestructuras se han conectado, los problemas han quedado al descubierto y muchos investigadores han destapado multitud de fallos de seguridad relacionados con estos dispositivos.

Por fortuna, cuando alguno de estos fallos es reportado a los fabricantes, muchos de ellos liberan parches de seguridad que corrigen los fallos y en algunas ocasiones, incluso envían nuevos dispositivos con los problemas subsanados. Es muy importante tomar conciencia de este problema ya que en la mayoría de las ocasiones es muy difícil, si no imposible, determinar si los dispositivos que forman parte de una arquitectura cuentan con vulnerabilidades o no. En caso afirmativo, lo más recomendable es actuar y tratar de mitigar la amenaza que supone el fallo de seguridad cuanto antes.

[6] http://es.wikipedia.org/wiki/Stuxnet

3 EL PUESTO DEL OPERADOR

Uno de los elementos clave en entornos industriales es el control de los procesos. Este control se realiza a través de interfaces que permiten disponer en tiempo real de información acerca de la evolución del proceso al operador que lo supervisa. Esta información se concreta en paneles de control diseñados de manera específica (denominados "paneles del operador") o a través de pantallas de ordenador. Para el primer caso es relativamente complejo establecer medidas de seguridad, ya que al ser fabricado para una necesidad específica habría que analizar el dispositivo concreto con el fin de establecer los controles. En el segundo caso, al tratarse de un ordenador (PC o servidor), será más sencillo especificar determinadas medidas de seguridad que garanticen la misma.

A lo largo de este punto se describirán los elementos esenciales para establecer una serie de controles mínimos que garanticen la seguridad relativa a los puestos del operador soportados por PCs o servidores, así como las diferentes herramientas y técnicas que permitan identificar y/o mitigar los posibles ataques.

CONTROLES ESPECÍFICOS DEL PUESTO

Las necesidades de seguridad de organizaciones y empresas no tienen un carácter homogéneo, debiéndose adaptar en función de la estrategia de negocio. No obstante, siempre debe existir una serie de controles que se pueden aplicar para garantizar unos niveles aceptables de seguridad.

CONFIGURACIÓN SEGURA DEL HARDWARE Y DEL SOFTWARE

Aunque en muchas empresas existen entornos muy heterogéneos en cuando a software y hardware, es aconsejable realizar instalaciones seguras de las aplicaciones y sistemas operativos, atendiendo a las siguientes recomendaciones:

- Eliminar cuentas innecesarias.
- Desactivar servicios que no se vayan a utilizar, así como los puestos asociados.
- Limitar la ejecución manual y automática de programas.
- Implementar políticas de actualización de software (sistemas operativos, aplicaciones y firmwares) con los parches de seguridad que no sobrepasen las 48h tras la publicación de los mismos por parte del fabricante.
- Crear imágenes de los sistemas (snapshots) con las configuraciones de seguridad para una rápida restauración de los mismos en caso de incidente. Estas imágenes se deben almacenar en un dispositivo fuera de la red para evitar que sean comprometidas.
- Realizar las tareas de administración remota mediante VNC, Telnet, etc. sobre canales seguros (SSL, IPSEC, etc.).
- Emplear aplicaciones que verifiquen la integridad de los archivos de los sistemas para evitar alteraciones.
- Utilizar herramientas de gestión que faciliten la administración de los sistemas como el Directorio Activo en Windows o Puppet en sistemas Unix/Linux.

ESTABLECIMIENTO DE MEDIDAS ANTIMALWARE

Como en cualquier arquitectura tecnológica compuesta por PCs y servidores, esta debe estar protegida por algún tipo de solución antimalware, tanto en la parte cliente como en la parte de red. Hay que mencionar que, aunque estas medidas son útiles y necesarias, se debe considerar que se trata únicamente de un elemento de seguridad más a implantar y en ningún caso se puede hablar de una solución definitiva. Principalmente porque la mayor parte de soluciones antimalware se basan en firmas o heurísticas que nada tienen que hacer contra determinados ataques o vulnerabilidades, como las *0-day*, pero si contra amenazas ya conocidas que puedan llegar a los sistemas.

Este inconveniente se agrava cuando, además, no es posible aplicar soluciones antimalware a determinados dispositivos como PLCs. En este caso se deberán aplicar soluciones intermedias que se implementen a nivel de red (segmentación de la red, utilización de WAF, etc.).

Las medidas esenciales a tomar pasarían por:

- Desplegar soluciones antimalware en todos los dispositivos de la empresa que lo admitan, como PCs, servidores, dispositivos móviles, *proxies*, etc. y realizar análisis programados y ante eventos (por ejemplo la inserción de un dispositivo externo de almacenamiento).
- Actualizar las soluciones con los últimos archivos de firmas, versiones, etc. También se debería verificar que todos los dispositivos han recibido la actualización.

CAPACIDAD PARA LA RECUPERACIÓN DE DATOS

Recuperar los sistemas y la operativa normal del negocio en el menor tiempo posible debe ser un punto clave dentro de la estrategia de seguridad de cualquier organización. En este aspecto, la capacidad para la recuperación de los datos es algo esencial que se puede conseguir con las siguientes recomendaciones:

- Establecer una política de copias de seguridad en base a la criticidad de los sistemas sobre los que se realizan las mismas. En cualquier caso, debería realizarse una copia semanal como mínimo y los datos deben de estar cifrados.
- En la medida de lo posible, establecer tres tipos de copia de seguridad: una para el sistema operativo, otra para aplicaciones y una última para datos. De ese modo se pueden restaurar de manera independiente sobre otro sistema o hardware.
- Realizar simulacros de restauración y verificación de las copias para asegurar que es posible la restauración de los sistemas en caso de desastre.

USO CONTROLADO DE PRIVILEGIOS DE ADMINISTRACIÓN

Los privilegios de "administrador" deben otorgarse exclusivamente a los usuarios autorizados que realizarán las tareas de gestión y mantenimiento de los sistemas operativos que soportan la arquitectura SCADA. De ese modo se evitará que los usuarios convencionales puedan instalar aplicaciones o realizar tareas exclusivas de los administradores.

ACCESO BASADO EN EL "NEED TO KNOW"

"*Si no puedo tocarlo, no puedo romperlo*" debería ser la premisa a seguir, respetando los criterios de usabilidad que permitan realizar el trabajo del operador de manera efectiva y eficiente. De esta manera, los usuarios/operadores únicamente deben tener acceso a las aplicaciones y funciones del sistema operativo necesarias para la actividad que desarrollan en su puesto de trabajo.

En este sentido también se pueden establecer controles de carácter físico como la restricción de uso de soportes de almacenamiento como USBs o DVDs.

OTROS TIPOS DE CONTROL

Hasta ahora se han visto medidas de control basadas principalmente en una correcta configuración de los componentes hardware y software del sistema, así como elementos esenciales como antivirus o la preparación para acciones fundamentales como procesos de *backup* correctos. A continuación, se verán otros tipos de control como el despliegue de sistemas de detección de intrusos, *HoneyTokens* o la utilización de herramientas de detección de exploits.

UTILIZACIÓN DE HIDS

Es importante disponer de mecanismos de detección en cada una de las máquinas de la empresa/organización, con el objetivo de detectar anomalías en el propio sistema operativo. Estas defensas no se refieren únicamente a antivirus (aunque sean imprescindibles), sino también a otras herramientas que permitan proteger, alertar y generar eventos cuando se detecta algo "inesperado". Aquí es donde entran en juego los HIDS (*Host-based Intrusion Detection System*).

Los HIDS no son más que agentes que se instalan de forma individual en cada equipo y cuya función es la de monitorizar el estado del sistema. Para ello utilizan una base de datos de los objetos que deben monitorizar. Para cada uno de estos objetos, el HIDS almacena sus atributos (permisos, fechas, resumen MD5, etc.) en una base de datos. Cuando se produce algún cambio en alguno de estos atributos, generará un evento informando del mismo. Para gestionar de forma centralizada cada uno de los agentes se utiliza un *manager*, cuya función será la de correlar los eventos de cada uno de los agentes así como los logs de los diversos dispositivos de red (*switches*, *routers*, *firewalls*, etc.). De esta forma, podrá tener un punto de control desde el que monitorizar el estado de cada agente, configurar alertas en función de los eventos y *logs* recibidos, buscar indicadores de compromiso (IOC), etc.

La Imagen 1 muestra de forma gráfica una arquitectura de este tipo, en concreto de la plataforma Open-Source OSSEC, la cual Integra todos los aspectos de un HIDS, control de registro y SIM/SEM (*Security Incident Management/Security Events Management*) en una solución de código simple, potente y abierta.

Imagen 1. Arquitectura OSSEC.

Cada uno de los agentes se instalará en las diversas máquinas (independientemente del S.O.), enviando cada uno de los eventos al OSSEC Server, el central manager. Cuando se detecte algún tipo de anomalía, el administrador será notificado para llevar a cabo las acciones paliativas oportunas.
Es interesante considerar una arquitectura de este tipo para añadir una capa más de protección a los sistemas. Además debe valorarse también la implementación de sistemas NAC (*Network Access Control*) para garantizar el cumplimiento de ciertas políticas de seguridad en cada uno de los equipos. El uso de estas medidas de seguridad junto con la correlación de la información será realmente eficiente para detectar una posible intrusión en nuestros sistemas.

Aparte de arquitecturas como OSSEC, se recomienda el uso de servicios como Splunk[7], sistema de *cloud logging* para enviar y sincronizar logs desde múltiples dispositivos y aplicaciones. Este tipo de soluciones permitirán investigar todo tipo de incidentes de seguridad a partir de los *logs* reportados. Para ver el potencial de este tipo de servicios se puede consultar la serie de posts "APTish Attack via Metasploit[8]" de Sysforensics, donde se investiga en profundidad una intrusión mediante el script *persistence* (*persistence.rb*) de Metasploit.

HONEYTOKENS

El concepto de HoneyTokens no es para nada nuevo[9]. Desde hace más de una década, estos sistemas se han implementado a nivel de red y *host* para identificar intrusiones. Sin embargo, este tipo de contramedidas parece que están siendo cada vez más adoptadas en organizaciones y empresas debido al "miedo" de las mismas sobre una posible intrusión en sus sistemas.

El objetivo de un HoneyToken es muy similar al de un IDS (*Intrusion Detection System*), es decir, detectar intrusiones en los sistemas. Sin embargo, utilizan un procedimiento diferente. Mientras que un IDS generalmente se basa en firmas para detectar patrones anómalos, un HoneyToken utiliza un enfoque más astuto. Al igual que cualquier otro tipo de HoneyPot, la idea de un HoneyToken es crear un "cepo" y esperar a que el atacante caiga en el mismo para alertar de la intrusión. Quizás el concepto más simple de HoneyToken sería el de la creación de una cuenta de correo falsa dentro de nuestro dominio para identificar posibles campañas de APT en forma de *Spear Phishing Attack* hacia nuestra organización.

Sin embargo este concepto puede ser utilizado dentro de muchos ámbitos:

- La creación de un recurso web falso: por ejemplo, añadir al robots.txt una entrada *admin* como "Disallowed".
- La creación de un registro falso en la base de datos: por ejemplo, añadir números de tarjetas de créditos falsas de forma que cualquier acceso a las mismas genere el evento oportuno.
- Monitorizar un puerto que no debería ser accedido.
- La creación de ejecutables "cepo", de forma que si estos son extraídos y ejecutados por un atacante envíen información sobre el entorno de dicho intruso.

Como puede verse, al igual que la ingeniería social, la creación de este tipo de contramedidas depende de la astucia y creatividad del responsable de seguridad.

Como ejemplo, el siguiente script, desarrollado por Antonio Villalón, muestra un ejemplo sencillo de HoneyToken. La idea es crear un fichero denominado "Despidos.doc" en un recurso compartido por Samba, y utilizar la API *inotify* para monitorizar el acceso al mismo mediante la siguiente instrucción:

```
inotifywait -m -e access DESPIDOS.DOC
| while read FILE ACTION; do ACCION
done
```

De forma más elaborada:

```
#!/bin/sh
MARGEN=60
LASTU=0
LASTT=0
# Accion a realizar ante un acceso
function action(){
    echo "ACCESO de $USER a $FILE en modo $ACTION"
}
```

[7] http://www.splunk.com/
[8] http://sysforensics.org/2012/11/aptish-attack-via-metasploit-part-one-of-four.html
[9] http://www.symantec.com/connect/articles/honeytokens-other-honeypot
[10] http://software-security.sans.org/blog/2009/06/04/my-top-6-honeytokens/
[11] http://www.securityartwork.es/2009/05/15/honeytokens/
[12] http://linux.die.net/man/2/inotify_add_watch

```
function buffer(){
    if [ $USER -eq $LASTU ]; then
        DIFF=`expr $TIME \- $LASTT`
        if [ $DIFF -gt $MARGEN ]; then
            action
        fi
    else action
    fi
    LASTU=$USER
    LASTT=$TIME
}
```

```
if [ $# -ne 1 ]; then
    echo "Deteccion de acceso a ficheros"
    echo "USO: $0 fichero"
    exit -1
fi

inotifywait -m -e access $1|while read FILE ACTION; do
    USER=`ps -ef|grep $FILE|head -1|awk '{print $1}'`
    TIME=`date +%s`
    buffer
done
```

Mediante la sustitución de la función *action()* por algo más elaborado (por ejemplo, el envío de un evento por correo, un SMS, SNMP, etc.) se conseguiría un sistema de detección de intrusos para detectar accesos ilegítimos en un sistema (siempre y cuando se acceda al fichero en cuestión).

Tal y como comenta Villalón, el uso de este tipo de ganchos es particularmente interesante, porque a cambio de una inversión mínima —existen HoneyTokens muy sencillos y su mantenimiento una vez implantados es casi inexistente— se obtiene una información de alto valor. Téngase en cuenta que uno de los principales problemas de los IDS basados en red es la tasa de falsos positivos que pueden llegar a generar y el coste asociado a procesar toda la información que producen día a día. Asimismo, sistemas más complejos como HoneyNets no suelen implantarse con frecuencia, salvo en entornos grandes y/o especialmente concienciados en temas de seguridad ya que, generalmente, los beneficios obtenidos del sistema no suelen cubrir el coste asociado a la implantación y mantenimiento del mismo.

INDICADORES IOC

En los puntos anteriores se ha hecho mención a los IOC o indicadores de compromiso. Dicha tecnología, la cual está teniendo gran auge en los últimos años, consiste en utilizar *XML Schemas* para describir las características técnicas de una amenaza por medio de las evidencias de compromiso que la misma deja en el equipo comprometido. Por ejemplo en función de los procesos, entradas de registro, servicios, ficheros descargados, etc. tras la infección.

Por medio de OpenIOC[13], framework *open-source* desarrollado por Mandiant, se podrá describir de forma semántica el comportamiento de APTs o malware por medio de ficheros XML y utilizar los mismos para buscar signos de infección en una máquina, sin necesidad de llegar a realizar un análisis exhaustivo de la misma para identifica el tipo de amenaza. La Imagen 2 muestra un extracto de plantilla IOC, desarrollada por AlientVault[14], correspondiente al APT Red October[15].

```
<definition>
  <Indicator operator="OR" id="542d9551-0768-4f18-96fe-9c53303277e7">
    <IndicatorItem id="6ee5a771-8da3-4d80-b772-7f4169283c56" condition="is">
      <Context document="FileItem" search="FileItem/FileName" type="mir" />
      <Content type="string">fsmgmtio32.msc</Content>
    </IndicatorItem>
    <IndicatorItem id="39539fc2-42a3-4a38-a5fc-4dc1940356bc" condition="is">
      <Context document="FileItem" search="FileItem/FileName" type="mir" />
      <Content type="string">cfsyn.pcs</Content>
    </IndicatorItem>
    <IndicatorItem id="ec996bcd-b8e4-4d31-91ae-d6b8089f2c33" condition="is">
      <Context document="FileItem" search="FileItem/FileName" type="mir" />
      <Content type="string">frpdhry.hry</Content>
    </IndicatorItem>
```

Imagen 2. Fichero IOC.

[13] http://blog.zeltser.com/post/44795789779/indicators-of-compromise-entering-the-mainstream
[14] https://github.com/jaimeblasco/AlienvaultLabs/blob/master/malware_analysis/RedOctober/48290d24-834c-4097-abc5-4f22d3bd8f3c.ioc
[15] http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies

Con esta plantilla y con ayuda de IOC Finder (una de las aplicaciones de OpenIOC) se podrían localizar indicios del Red October en algún ordenador comprometido con este malware.

Supóngase, por ejemplo, que una organización ha resultado comprometida por dicha APT. Tras acotar la infección e identificar el tipo de amenaza, se analizarían otros equipos dentro de la misma VLAN para averiguar si los mismos han podido resultar también infectados. Para ello, habría de ejecutarse IOC Finder, como se muestra en la Imagen 3, en cada una de las máquinas sospechosas.

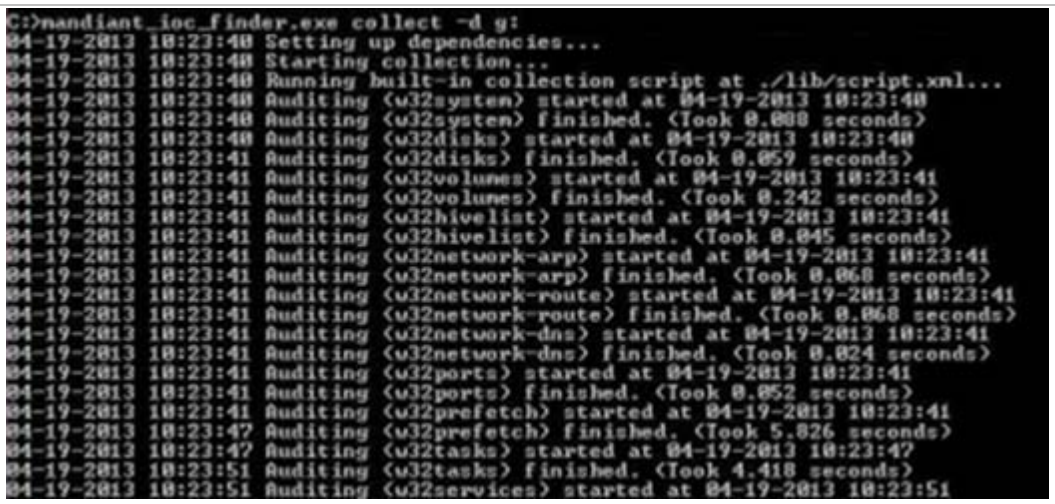

Imagen 3. Mandiant IOC Finder (Collect).

Mediante este proceso (obsérvese el parámetro *collect)*, IOC Finder recopilará un conjunto de datos del equipo sospechoso (en este caso, de su unidad "*g:*") y los irá almacenando dentro de determinado directorio en forma de ficheros XML. Estos ficheros representarán multitud de atributos correspondientes a procesos, entradas de registros, ficheros, etc. que posteriormente servirán como fuente de inspección para localizar cualquier indicio de infección, en este caso del APT Red October.

Una vez finalizado el proceso de recolección (proceso que puede llevar horas) bastará con ejecutar IOC Finder con el parámetro *report.* Para ello será necesario especificar, por un lado, la fuente de datos previamente generada y, por otro, el/los fichero(s) *.ioc* que define los patrones de infección que se quiere localizar, como se muestra en la Imagen 4.

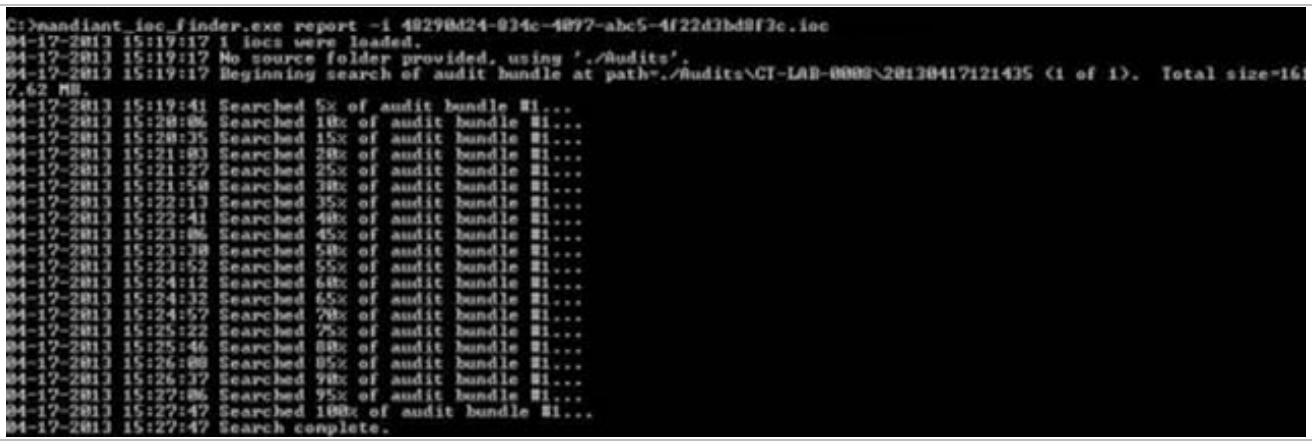

Imagen 4. Mandiant IOC Finder (Report).

Como se puede ver, los indicadores de compromiso representan una manera eficiente y rápida para identificar y definir amenazas avanzadas que de otra forma resultarían muy complejas de evidenciar y que, en algunos casos, pasarían inadvertidas por sistemas AV o HIDS. Por tanto, es aconsejable considerar su uso para analizar equipos que muestren comportamientos extraños, por ejemplo, aquellos que presenten patrones de tráfico poco comunes.

Para más información sobre IOC puede consultar la presentación titulada Identifying & Sharing Threat Information[16] de Mandiant o el *whitepaper* Using IOC (Indicators of Compromise) in Malware[17] de SANS Institute.

EMET Y CRYSTALAEP

En puntos previos se ha hablado de los modos que tienen los atacantes de irrumpir en los sistemas a través de diversas técnicas (ingeniería social, *spear phishing*, etc.). Si además se añade el uso de *encoders*, *packers* u otros elementos de ofuscación, se complica la detección de este tipo de amenazas para que puedan ser detectadas, por ejemplo, por los antivirus. Por ello es altamente recomendable contar con herramientas especializadas en la detección de exploits que permitan detectar intentos de explotación de procesos (por ejemplo el navegador) que en otro caso no serían detectados por el antivirus.

EMET

Una de las herramientas más conocidas para frenar este tipo de ataques es EMET (Enhanced Mitigation Experience Toolkit)[18], herramienta desarrollada por Microsoft que intenta reducir las probabilidades de que un atacante ejecute código malicioso a través en un determinado programa. La utilización de ficheros PDF maliciosos para comprometer equipos mediante ataques de phishing es un claro ejemplo de este hecho. Lo mismo sucede con aplicaciones como Flash, Java, Firefox, documentos de Office, etc. El uso de EMET puede ayudar enormemente a prevenir un gran número de ataques que tratan de aprovecharse de software inseguro y de configuraciones de seguridad débiles en los S.O. Algunos de los beneficios que nos ofrece EMET se describen a continuación:

- **Implementación de múltiples medidas de seguridad** como DEP, ASLR, SEHOP, EAF, HSA, NPA, BUR sin necesidad de recompilar software.
- **Altamente configurable**: las medidas de mitigación son muy flexibles, permitiendo aplicar las mismas en los procesos que se elijan. Esto implica que no hace falta implementar ciertas medidas de seguridad a todo un producto o conjunto de aplicaciones (lo que podría generar problemas si un determinado proceso no soporta ciertas medidas de mitigación, como aquellas que no soportan DEP).
- **Facilidad de uso y de despliegue**: EMET dispone de una interfaz gráfica desde la que configurar todos los parámetros deseados, eliminando la necesidad de modificar claves de registro a mano o cualquier otro tipo de configuración delicada. Además, es fácilmente desplegable por medio de políticas de grupo y del System Center Configuration Manager.

Recientemente, EMET ha publicado la versión 4[19], donde aparte de las funcionalidades comentadas anteriormente, incorpora las siguientes características de seguridad:

- **Certificate Pinning**: quizás una de las funcionalidades más significativas de esta nueva versión de EMET es el "Certificate Trust" (certificados de confianza). Mediante esta característica EMET

[16] http://scap.nist.gov/events/2011/itsac/presentations/day2/Wilson%20-%20OpenIOC.pdf
[17] http://www.sans.org/reading-room/whitepapers/incident/ioc-indicators-compromise-malware-forensics-34200
[18] http://support.microsoft.com/kb/2458544
[19] http://blogs.technet.com/b/srd/archive/2013/06/17/emet-4-0-now-available-for-download.aspx

permitirá especificar reglas mediante las cuales se podrán indicar las CA (Certification Authorities) asociadas a un sitio SSL/TSL. Hechos bien conocidos como los de Comodo o Diginotar demostraron que la infraestructura PKI no presenta una arquitectura de seguridad lo suficientemente fiable al depositar la confianza en un elevado número de entidades cuyas políticas de seguridad no son lo robustas que debieran ser. EMET trata de reducir dicha confianza permitiendo elegir al usuario la asociación de un certificado X.509 con la autoridad certificadora de su elección. La Imagen 5 muestra una "pin rule" (regla) en la cual se asocia el dominio login.live.com con la CA VeriSign. Cualquier certificado utilizado por Internet Explorer para login.live.com que se origine a partir de una CA raíz diferente de la configurada en dicha regla será detectada por EMET reportada como sospechosa.

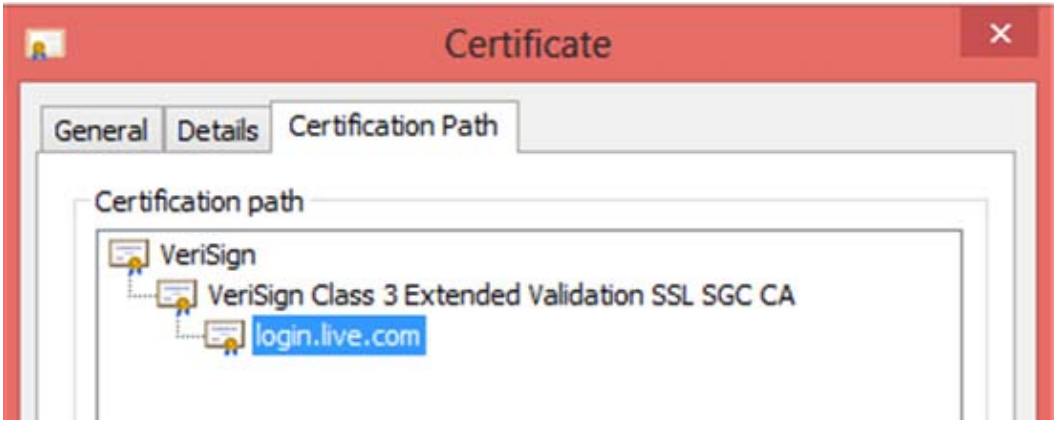

Imagen 5. Pin rules en EMET.

- **Mitigaciones ROP:** una de las técnicas de exploiting más utilizadas para evadir DEP (Data Execution Prevention) y ASLR (Address Space Layout Randomization) son los ROP (Return Oriented Programming) gadgets. La idea de esta técnica es buscar determinados sets de instrucciones en memoria (por ejemplo, DLLs) que puedan ser utilizadas para llamar a ciertas APIs de Windows con las que eludir DEP. Este set de instrucciones debe acabar en una instrucción de tipo RETN para poder enlazar cada uno de los gadgets que se vayan construyendo. Puesto que DEP impide ejecutar código desde la pila, únicamente se almacenarían en ella las direcciones de cada uno de estos gadgets. De esta forma, jugando con las instrucciones RETN y las direcciones alojadas de la pila, se podría ejecutar código fuera de la misma. Por ejemplo, si fuera posible encontrar ciertos gadgets para llamar a la función *VirtualProtect()*, quizás podría cambiarse el tipo de acceso a cierta página en memoria, marcándola como ejecutable, y posteriormente alojar determinado shellcode en dicha página. Si en lugar de *VirtualProtect()*, se pudiera construir gadgets para llamar a la función *SetProcessDEPPolicy()*, sería posible desactivar DEP para el proceso actual y ejecutar código desde la pila. La Imagen 6 muestra un ejemplo de ROP-chain generado por el script Mona.py a partir de MSVCR71.dll para llamar a *VirtualAlloc()*.
- **Modo auditoría**: si se detecta una vulnerabilidad, EMET no matará el proceso afectado si no que reportará dicho ataque y dejará que continúe. Este modo sólo es aplicable a determinadas medidas de mitigación, como por ejemplo los relacionados con los ataques que empleen ROP gadgets como los vistos anteriormente. Con esta funcionalidad se evitarían falsos positivos que generarían cierres inesperados de las aplicaciones, interfiriendo con la experiencia del usuario.

Imagen 6. Ejemplo de *ROP-chain* generado por el script *Mona.py*.

- Para utilizar EMET únicamente se lanza su interfaz gráfica y se seleccionan los procesos, así como las medidas de mitigación que se quieren implementar. Como se observa en la Imagen 7, EMET dispone de dos grupos de configuración. Por un lado aquellos parámetros que afectan al propio sistema y por otro, los que se quieren aplicar al software elegido. Es importante señalar que EMET es dependiente totalmente del sistema operativo en el que se instale, lo que implica que sobre una máquina Windows XP algunas de las medidas de seguridad como SEHOP (Structured Exception Handler Overwrite Protection) o ASLR (las mostradas en el System Status) no estarán disponibles.

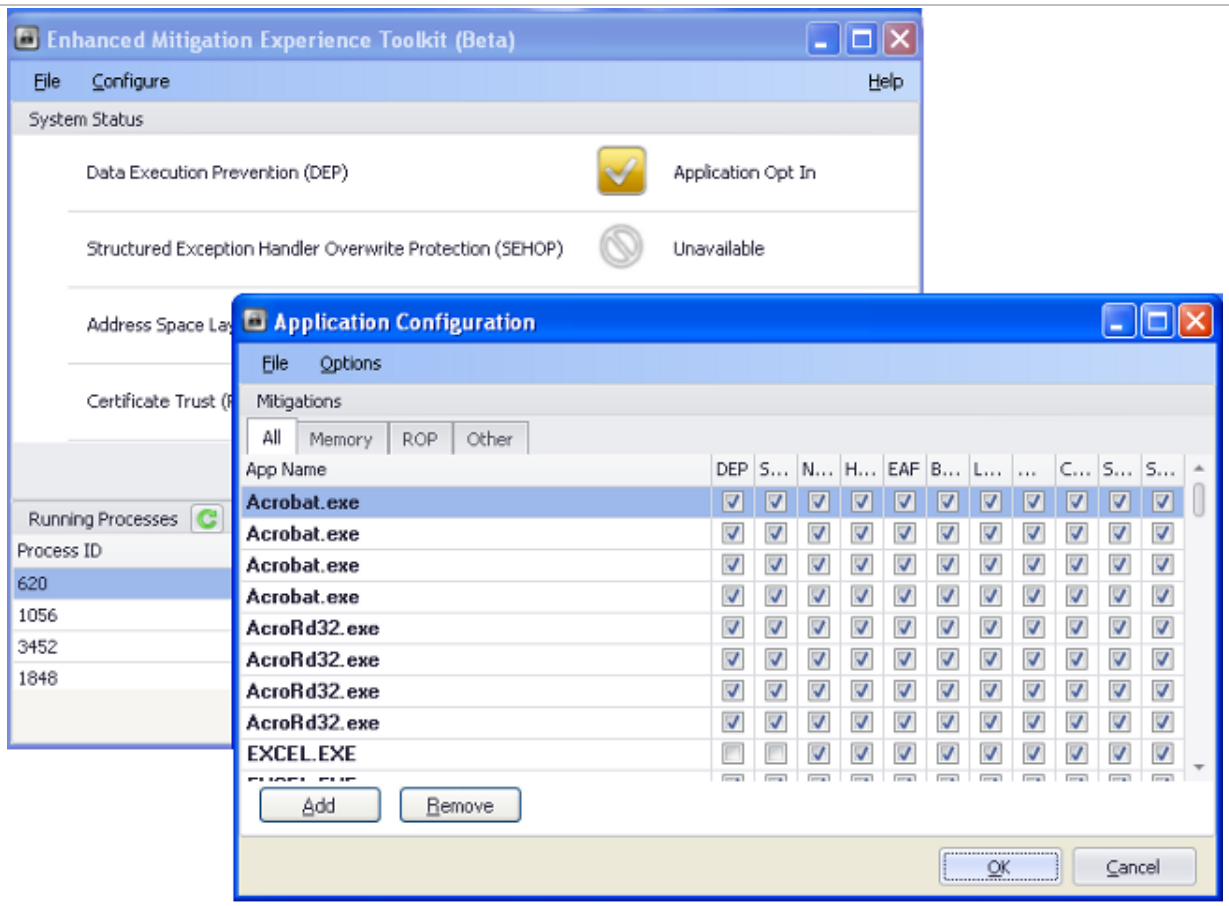

Imagen 7. Grupos de configuración de EMET.

Desde la versión 3 de EMET, se puede aplicar esta configuración mediante la importación de perfiles de protección (protection profiles). Éstos no son más que ficheros XML donde se define la ruta de los ejecutables que se desean proteger; opción bastante útil para portar configuraciones de un equipo a otro. En la Imagen 8 se muestra cómo proteger la suite de Microsoft Office mediante el fichero de configuración Office *Software.xml*.

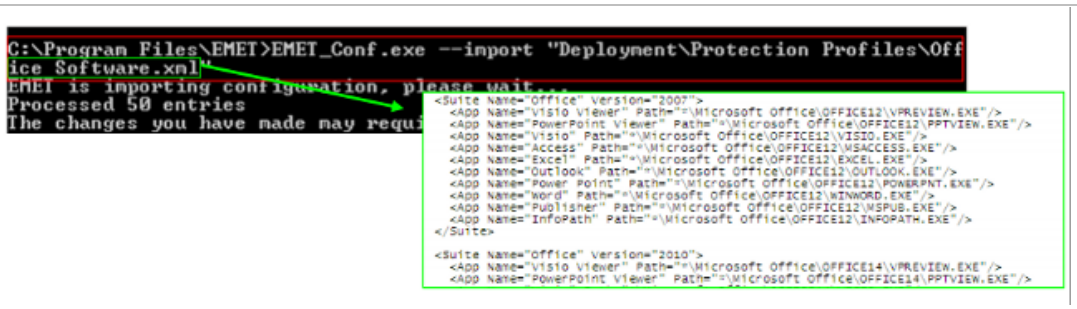

Imagen 8. Fichero de configuración Office *Software.xml*.

CRYSTALAEP[20]

Se trata de otra herramienta utilizada en equipos Windows para prevenir la ejecución de exploits en navegadores y ciertas aplicaciones de uso común, y en donde el antivirus tiene poco que hacer. De

[20] Fuente: http://www.shelliscoming.com/2013/06/crystalaep-una-alternativa-emet.html

modo similar a EMET, CrystalAEP presenta multitud de opciones de protección que pueden aplicarse de forma selectiva a las aplicaciones que se desee, para evitar intentos de explotación.

La interfaz de la aplicación presenta dos paneles de configuración: Basic Options, desde donde podrán elegirse las aplicaciones que se quieran añadir a la lista de protección; y Expert Options, desde donde se podrá definir en detalle qué características de seguridad aplicar, de forma genérica o por cada proceso. Son estas últimas características las que hacen realmente atractiva a la aplicación debido a la multitud de contramedidas existentes para evitar ataques de corrupción de memoria. Dada la naturaleza de muchos exploits, este tipo de medidas podrían protegernos incluso contra cierto tipo de 0-days. Como se muestra en la Imagen 9, desde la pestaña de Memory Monitor se pueden ver algunas de estas opciones:

- Enable Process DEP.
- Use-After-Free Protection.
- Disable RWX Heap.
- Vary Allocation Sizes.
- Windows Validate Allocations.

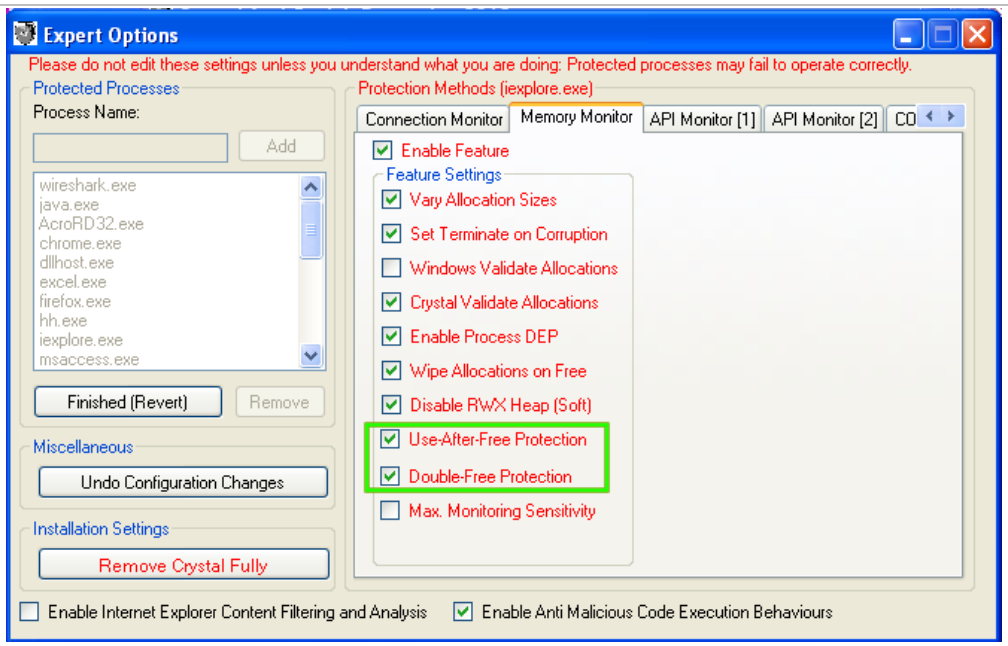

Imagen 9. Uno de los menús de configuración de CrystalAEP.

Asimismo, dentro de la pestaña API Monitor se pueden encontrar más mecanismos de protección relacionados con la API de Windows, como **Anti-ROP Stack** y **Additional Anti-ROP Methods**, para prevenir intentos de explotación que intenten aprovecharse de **ROP gadgets** con los que evadir **DEP** y **ASLR**.

CrystalAEP también proporciona funcionalidades de filtrado de contenido para IExplorer (Anti-Cross-Site Scripting, validación de ficheros PNG, JPEG Y GIF, etc.). Para ver en detalle cada una de estas características, se puede consultar la guía de usuario[21] de la herramienta. CrystalAEP es gratuita y está disponible[22] para Windows XP, Vista y 7 (arquitecturas 32 y 64 bits).

REPUTACIÓN DE SEGURIDAD DEL PROVEEDOR DE SW Y/O HW

Uno de los aspectos que hasta ahora no había tenido especial importancia era comprobar la reputación del proveedor de software o hardware en cuanto a términos de seguridad en su fabricación. Afortunadamente, las últimas noticias relativas a la aparición de puertas traseras o

[21] http://www.crystalaep.com/CrystalUsersGuide.pdf
[22] http://www.crystalaep.com/download.html

cuentas de administración por defecto, la imposibilidad de actualizar el firmware, etc. en dispositivos utilizados en arquitecturas SCADA, han provocado que este aspecto sea considerado a la hora de adquirir tanto aplicaciones como dispositivos **físicos.** Por esta razón, antes de lanzarse a la adquisición se deberían valorar cuestiones como:

- ¿Los dispositivos o aplicaciones cuentan con las capacidades adecuadas para gestionar su seguridad?
- ¿El fabricante ofrece actualizaciones de seguridad?

ENTORNOS "LEGACY"

La obsolescencia programada se define como "*la determinación, la planificación o programación del fin de la vida útil de un producto o servicio de modo que tras un período de tiempo calculado de antemano por el fabricante o por la empresa de servicios durante la fase de diseño de dicho producto o servicio éste se torne obsoleto, no funcional, inútil o inservible.*" Contrario a este término, la "*obsolescencia autorizada*" corresponde a la determinación para hacer permanente un sistema que, por su estructura o larga existencia, ha demostrado ser vulnerable o peligroso para el control de servicios críticos frente a las evolutivas técnicas de ataque a aplicaciones e infraestructuras, pero que debido a su obligatoria operación permanente y sin interrupciones no pueden ser reemplazados por plataformas actuales y más robustas.

A esta categoría pertenecen los sistemas heredados o sistemas "legacy", que a pesar de considerarse anticuados no pueden ser reemplazados o actualizados de forma sencilla debido a que es mayor el impacto en los procesos productivos o industriales que el beneficio de la renovación, pero en muchas ocasiones son otras las excusas para evitar el reemplazo de sistemas caducos. No obstante, un sistema que se considere como heredado, debe cumplir igualmente una serie de condiciones que obligarían al operador a implementar mecanismos de seguridad adicionales que lo protejan de amenazas.

Algunas de las razones que se han argumentado para justificar la negativa a actualizar los equipos y sus correspondientes plataformas son:

- El sector es muy conservador y poco dado a modificar cosas que, en principio, funcionan.
- Miedo a que el software deje de funcionar tras la aplicación de actualizaciones.
- Los responsables de estos equipos son gente de producción y no tienen los medios ni los conocimientos para responsabilizarse de mantener estos sistemas actualizados. Para realizar cambios o modificaciones necesitan ayuda, proporcionada generalmente mediante contratos con terceras partes.
- En muchas ocasiones se desarrolla a medida y tras algunos años ya no es posible contar con el desarrollador/integrador que realizó el proyecto para contratar soluciones derivadas del proyecto inicial.
- Actualizar el sistema operativo puede requerir actualizar el software de supervisión, lo que requiere el trabajo de especialistas externos, que a su vez supone un coste, pero dado que todo funciona, no se ve la necesidad.

El común denominador podría resumirse en la frase "*si funciona, no se toca*", el inconveniente es la definición de funcionamiento que desde antaño tienen estos sistemas, relacionado únicamente con el control y la gestión pero separada totalmente de la seguridad y la auditoria.

Aunque alguna de estas razones pueda parecer más que suficiente para justificar la prevalencia de estos dispositivos, siempre se debe realizar un análisis en profundidad que permita buscar alternativas más seguras a las existentes. En cualquier caso, habrá de darse siempre especial importancia a las recomendaciones del fabricante del sistema o producto afectado.

EQUIPOS MÓVILES

Aunque el acceso remoto a sistemas críticos no es una funcionalidad muy recomendable por la naturaleza de estos sistemas, en ocasiones es necesario disponer de la información que está generando un dispositivo determinado, o simplemente realizar tareas de monitorización para comprobar que el funcionamiento es el correcto. Para realizar este tipo de acciones generalmente se utilizan ordenadores portátiles, tablets y/o similares, por lo que a estos dispositivos, además de las características de seguridad heredadas de la arquitectura (políticas, aplicaciones de seguridad, etc.), se les debe añadir funciones de seguridad adaptadas a su naturaleza física, que los hace propensos a ser robados o perdidos, por ejemplo.

Algunas de las características que deben de tener los dispositivos móviles:

- El dispositivo debe estar protegido con contraseña y los datos que contiene deben estar cifrados.
- Las conexiones que se establecen entre los dispositivos móviles y los equipos en las instalaciones deben estar cifrados para otorgar la máxima confidencialidad en las comunicaciones.

En muchos sistemas, para evitar el acceso a los datos en caso de pérdida o robo, los dispositivos cuentan con aplicaciones que permiten la eliminación de información e incluso el borrado completo de manera remota.

4 CONCLUSIONES

Como en todo sistema de Tecnologías de la Información, en los entornos SCADA o de carácter industrial los usuarios son normalmente el "eslabón más débil" desde el punto de vista de la seguridad, siendo especialmente vulnerables a los conocidos como ataques basados en ingeniería social. Esto se agrava en el caso de las APTs (*Advanced Persistent Threat*), ya que además de su elevada complejidad técnica, son ataques intencionadamente sigilosos, con el fin de alargar su "vida útil" al máximo.

En esta guía recogen las medidas que se pueden tomar, desde el puesto del operador, para protegerse de estas amenazas. Algunas de los mecanismos más efectivos estudiados son:

- Restringir el acceso y los servicios proporcionados a lo que sea estrictamente necesario. Además, todas las comunicaciones deben realizarse por canales seguros.
- Implementar políticas de actualización de software.
- Mantener copias de seguridad de todo lo importante, incluso haciendo "simulacros" para comprobar que las copias son correctas y completas.
- Desplegar medidas antimalware en todos los dispositivos que lo permitan.

También es esencial vigilar que la información importante no sea alterada de forma ilícita. En concreto, entre las medidas más efectivas están los *Host-based IDS*: agentes que monitorizan cada equipo de manera individual; y los *HoneyToken*, que funcionan a modo de cepo para detectar a los atacantes y alertar de una intrusión. También para la detección, son útiles los indicadores IOC, que describiendo las características técnicas de una amenaza, permiten identificarla unívocamente.

Mención especial merecen los mecanismos de protección ante exploits (componentes software utilizados para aprovecharse de fallos de seguridad), ya que estos pueden ser difícilmente detectables mediante herramientas típicas, como antivirus. En este aspecto, los componentes principales de las herramientas EMET Y CrystalAEP, que pueden utilizarse, por ejemplo, para protegerse frente a ejecuciones de código "no autorizadas" o asociación de autoridades de certificación digital a sitios específicos.

Es además destacable que en el sector industrial es relativamente frecuente encontrar sistemas anticuados, conocidos como "legacy systems" debido al impacto que tendría su reemplazo. No obstante, estos sistemas siguen siendo una parte de un todo, y por lo tanto es importante salvaguardar su seguridad, pese a su condición de "sistemas anticuados".

En cualquier caso, y como regla general aplicable a todo lo visto en la guía, debe tenerse en cuenta que siempre habrán de respetarse las recomendaciones del fabricante de los sistemas o productos involucrados.

Por último, recordar que pueden existir características, necesidades y tecnologías sectoriales específicas presentes en determinados puestos de operador que limiten la aplicación directa de algunas medidas contempladas en esta guía. La aplicabilidad a entornos concretos ha de valorarse de forma proporcional a factores tecnológicos, propiedades técnicas de los sistemas a proteger o el modelo de negocio de la compañía interesada. En este aspecto, por lo tanto, la guía debe contemplarse como una serie de medidas deseables, pero no siempre estrictamente necesarias, para mejorar la seguridad del puesto de los operadores de infraestructuras críticas. Adicionalmente, estando la guía destinada a la protección del Puesto del Operador de Infraestructuras Críticas, siendo inherente a éste la necesidad de unos elevados requisitos de seguridad, se asumirá que estos equipos están adheridos a las políticas de seguridad corporativas, por lo que medidas de seguridad básicas, como el uso de contraseñas robustas, se dan por supuestas.