Adaptive Defense 360

&

Adaptive Defense

Novedades de la versión 2.4

Índice

1. Resumen de las novedades de la versión

La versión 2.4 de la familia de productos y servicios de Adaptive Defense cubre los siguientes objetivos:

1. **Detección/Mitigación en fase de explotación en el ciclo de vida de los ciber ataques. – Tecnología Anti-exploit dinámica**
   Adaptive Defense y Adaptive Defense 360 incorporan en esta versión una nueva tecnología anti-exploit dinámica que evita los intentos de explotación mediante la monitorización de la actividad en los dispositivos y la identificación de tales intentos de explotación, tanto conocidos como desconocidos o zero-day.

2. **Detección de ataques sin ficheros (malwareless o fileless attacks) y monitorización en consola de administración.**
   Panda Adaptive Defense y Panda Adaptive Defense 360, incorpora técnicas que detectan estos tipos de ataques gracias a la monitorización de los procesos, correlación de acciones y a la capacidad de la protección de identificar comportamientos y usos maliciosos de aplicaciones legítimas.

   En la versión 2.4 se robustecen estas técnicas. Estos casos se gestionarán a partir de esta versión como cualquier otro tipo de detección, es decir, se presentarán en consola como detecciones de malware y podremos monitorizar su ciclo de vida, se enviarán alertas por email y formará parte de los dashboards e informes.

3. **Identificación de los equipos que están siendo utilizados para expandir un ataque en la red**
   A partir de la versión 2.4 cuando la detección de un malware o PUP o el bloqueo de un elemento se produzcan desde un equipo de la red, la información de este, IP origen y el usuario, será parte de la información disponible en el ciclo de vida de ese malware, PUP o elemento bloqueado.

4. **Exportación detalle de estado de los equipos y servidores para su integración en aplicaciones operacionales**
   En la versión 2.4 se incluye un nuevo informe en formato csv, que puede ser exportado y programado periódicamente, con el detalle del estado de los equipos y servidores protegidos.

5. **Mayor flexibilidad en la integración con SIEM on-premise**
   A partir de la versión 2.4 los logs podrán ser enviados vía protocolo Syslog y opcionalmente cifrados mediante SSL/TLS. Además, en esta versión, se despliega un servicio de VPN para ofrecer una mayor seguridad al envío de logs vía FTP/sFTP.

6. **Facilidades en la fase de análisis forense: Exportación del detalle del ciclo de vida de una o varias detecciones e información de líneas de comandos y parámetros (Versión 2.4.1)**
   En la versión 2.4.1 se incluye la funcionalidad de exportación a csv del detalle del ciclo de vida de una detección o bloqueo o de varias detecciones o bloqueos.

   Además, se presentará en consola, el detalle de la línea de comandos y sus parámetros en caso de que el atacante haga uso de técnicas como por ejemplo el uso de PowerShell.

2. Detección y Mitigación en fase de explotación en el ciclo de vida de los ciber ataques. – Tecnología Anti-exploit dinámica

Un exploit es una secuencia de comandos que se aprovecha de un error o una vulnerabilidad en una aplicación software legítima. Los atacantes usan tanto ejecutables como fichero no ejecutables o ataques fileless basados en scripting como medio para acceder y usar los sistemas de los puestos de trabajo y servidores para llevar acabo los ataques.

En un escenario típico, el atacante manipula un programa legítimo para ejecutar código mientras evita su detección. Este código se descargará un malware, un ejecutable malicioso (PE: fichero ejecutable), o usará herramientas legítimas del sistema para realizar acciones maliciosas sin ejecutables o sin ficheros (ataques malwareless o ataques Fileless).

Para llegar a controlar totalmente el equipo, el atacante debe pasar por una cadena de etapas donde la explotación de las vulnerabilidades es el desencadenante y parte vital para ellos.
El bloqueo del intento de explotación de una vulnerabilidad en la cadena parará completamente el ataque.

Adaptive Defense y Adaptive Defense 360 incorporan en esta versión una nueva tecnología anti-exploit dinámica que evita tales intentos de explotación mediante la monitorización de la actividad en los dispositivos y la identificación de tales intentos de explotación, tanto conocidos como desconocidos.

2.1.¿Por qué es importante detener un ataque en fase de explotación?

Un ataque, se compone de una cadena de acciones o movimiento para los cuales se utilizan diferentes técnicas para penetrar en el sistema y evadir los mecanismos de detección implementados.

Los ataques maliciosos se desencadenan a través de la explotación de una vulnerabilidad en una aplicación confiable que, en principio, se realiza normalmente sin ni siquiera levantar sospechas. Los atacantes aprovechan la vulnerabilidad en el software para explotar la aplicación y comprometer tanto a ella como al sistema. El atacante puede llegar a tener control total de la máquina atacada y desde esta continuar atacando otras.

El objetivo de un sistema de protección avanzada como lo es Panda Adaptive Defense, es el de identificar y detener esta cadena de acciones para evitar la ejecución de código malicioso que comprometa tanto las aplicaciones como el sistema y el propio puesto de trabajo o servidor.

Las acciones o fase de la cadena de un ataque, lo que se conoce como el modelo de ciclo de vida "Cyber Kill Chain" (CKC) y su extensión desde el perímetro hasta los puesto de trabajo y servidores conocida como la "Cyber Kill Chain" extendida[1].

[1] Se quieres saber más sobre la Cyber-Kill Chain, te recomienda la lectura de este documento "Entendiendo los ciber-ataques. Parte I. "The Cyber-Kill Chain", la secuencia de acciones en un ataque"

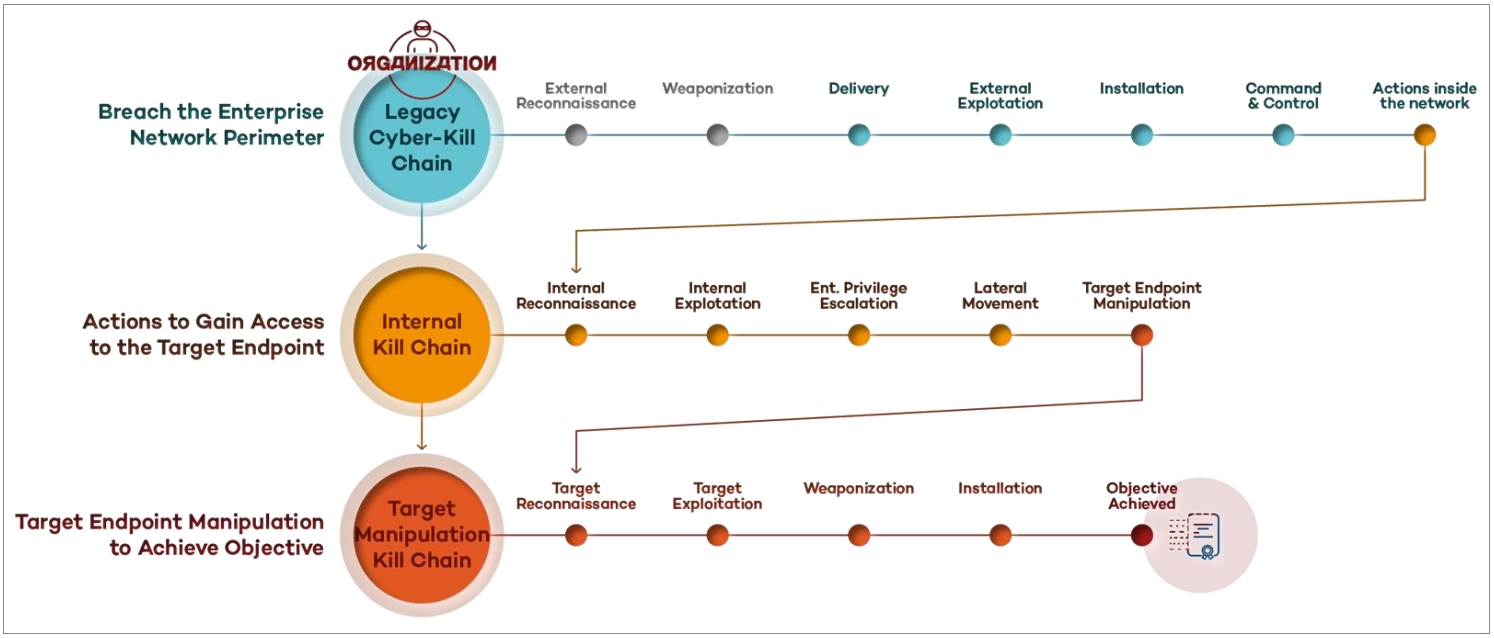


Figura 1. La Cyber-Kill Chain Extendida. Acciones para obtener acceso a los dispositivos y servidores objetivo del ataque y su manipulación por el atacante

El atacante, debe ejecutar con éxito todas las fases de la "Cyber Kill Chain" extendida para alcanzar sus objetivos, nosotros deben detener el ataque el cualquiera de las fases previas al acceso por parte del atacante de los activos que son objetivo de sus acciones. Por consiguiente, debemos de desplegar tecnologías en cada una de las fases en la búsqueda de detener el ataque cuanto antes mejor.

La tecnología dinámica de anti-exploit, que se incorpora en esta versión 2.4, se orientan precisamente a detectar y abortar un ataque en cuanto se detecta un intento de explotación de una aplicación confiable.

El objetivo es detener el ataque completo incluso antes de que esa aplicación u otras creadas a raíz de esta explotación sea bloqueada por la protección avanzada a ser clasificadas como maliciosas como consecuencia de la monitorización de sus acciones maliciosas.

2.2. Que aporta la tecnología anti-exploit incluida en Adaptive Defense

Adaptive Defense incorpora nuevas tecnologías anti-exploit desarrolladas en los laboratorios de Panda Security por **Expertos en ciber-seguridad**. Las tecnologías de Adaptive Defense, se basan en **el conocimiento de Panda Security que evoluciona continuamente** siendo alimentado con información en tiempo real que proviene de sensores en millones de dispositivos y la **monitorización continua de los procesos y su actividad en los puestos de trabajo y servidores**.

Los **principales beneficios** de esta tecnología son:

- Proporciona una capa de **protección adicional que detecta y bloquea, opcionalmente, los exploits en tiempo real**. Cuando se produce el exploit, la tecnología evita la ejecución de código malicioso, la infección del equipo y que se propague a otros dispositivos en la organización.
- **Monitoriza** el comportamiento interno del proceso comprometido en busca de **anomalías** indicativas de una explotación de una vulnerabilidad conocida o zero-day.
- **Detecta independientemente del exploit** utilizado en cada ataque, dotando a Adaptive Defense de una protección eficaz contra **todo tipo de exploits y especialmente contra exploits 0-Day** que se aprovechan de:
    - Vulnerabilidades en Navegadores: Internet Explorer, Firefox, Chrome, Opera y otros.

    - Familias de aplicaciones especialmente atacadas: Java, Adobe Reader, Adobe Flash, Microsoft Office, reproductores de media…
    - Vulnerabilidades de sistemas operativos que ya no tienen soporte como Microsoft XP y otros.
- Es Imperceptible para el usuario, no ralentiza el sistema.

La gran **diferencia** con otros productos del mercado, radica es su carácter **generalista** evitando la explotación de vulnerabilidades conocidas, así como las más peligrosas: las no conocidas o de tipo 0-Day.

Su carácter generalista, es el resultado de la inversión de Panda Security en investigación para el desarrollo de tecnologías proactivas cuya naturaleza es siempre generalista. Estas tecnologías están muy orientadas a detectar anomalías y comportamientos atípicos en su contexto de ejecución.

Estas tecnologías únicas dotan a **Adaptive Defense** de los mecanismos necesarios para detectar y bloquear ataques que en algún punto de la cadena hacen uso de técnicas de explotación de **vulnerabilidades.**

La detección se basa en la **monitorización continua** de todas las acciones que se producen en los sistemas, tanto de los procesos en ejecución desde fichero como en memoria.

Estas detecciones bloquean y evitan, en estados prematuros del ataque, que **aplicaciones confiables se vean comprometidas** por estos exploits, pero de forma totalmente **imperceptible** para el usuario del equipo protegido.

4.3. Factores diferenciales de la tecnología anti-exploit en Adaptive Defense

Las actuales soluciones de anti-exploit del mercado se basan en su gran mayoría, en un análisis **morfológico** de ficheros y/o de **contexto** en su ejecución o bien implementan varias **características** de protección **ausentes** en **Windows** (protección ASR, DEP, EAF, así como detecciones específicas de vulnerabilidades ya conocidas, las Common Vulnerabilities and Exposures -CVE-).

Estas técnicas, como cabe esperar, no son suficientes ante ataques a la seguridad que buscan una o varias vías de entrada en los sistemas haciendo uso de diferentes tipos de vulnerabilidades incluyendo las de 0-Day.

Adaptive Defense es la única solución del mercado que, mediante la **monitorización continua de los procesos**, en este caso, los procesos comprometidos por los atacantes u otros procesos que se encuentran en el sistema, es capaz de **detener estos ataques antes o durante** la explotación de la vulnerabilidad.

Teniendo en cuenta todo esto, los **factores diferenciales de la tecnología anti-exploit** que a partir de ahora se incluye en nuestras soluciones de la familia de **Adaptive Defense**, son:

- **Es generalista**. Detecta técnicas de explotación de vulnerabilidades conocidas y no conocidas (vulnerabilidades 0-days).

- A diferencia de otras soluciones del mercado, la nueva tecnología anti-exploit no se centra en complementar allí donde el sistema operativo Windows tiene vulnerabilidades de seguridad, sino que **se basa en la monitorización continua de los procesos** que corren en los dispositivos y la correlación de la información recogida en la nube mediante algoritmos de machine learning.

- **La eficiencia** de la nueva tecnología anti-exploit de Adaptive Defense se debe a la **minuciosa sincronización** de:

- **La protección anti-exploit en el puesto de trabajo y servidores**, totalmente integrada con la protección avanzada, por lo que no se requieren actualizaciones, ni procesamiento extra, ya que el modelo sigue siendo en base a la monitorización de todas las acciones de las aplicaciones y procesos en ejecución.
- **Los algoritmos de machine learning especializados y gestionados en la nube**, que al ser parte del servicio gestionado se mantienen continuamente adaptados a nuevos sistemas, aplicaciones y técnicas avanzadas de explotación y evasión.
- **El Servicio gestionado de nuestro equipo experto de threat hunters** trabajando con precisión la detección de ciertas técnicas avanzadas de explotación.

2.5. Aplicación de la nueva tecnología anti-exploit en Panda Adaptive Defense

A partir de la versión 2.4 de Panda Adaptive Defense, que incluye una nueva versión de protección puestos de trabajo y servidores, versión 7.70, estaréis protegidos con nuestra nueva tecnología anti-exploit basada en la monitorización continua y expuesta con anterioridad (siempre y cuando la protección anti-exploit este activada en los perfiles de seguridad).

1. Configuración de la tecnología anti-exploit. Modos de comportamiento

A partir de la versión 2.4, la consola web de gestión permite la configuración de esta tecnología a nivel de perfil de seguridad. La tecnología anti-exploit se **activa o desactiva** independientemente del resto de protecciones en Adaptive Defense, incluso de la Protección Avanzada.

Por defecto en esta versión, la tecnología, tras la actualización o en una instalación nueva, esta desactivada, aunque desde Panda Security os invitamos vivamente a activar esta protección paulatinamente en los perfiles de seguridad de su parque.

En el momento en el que la protección anti-exploit se activa, su modo de funcionamiento es por defecto, solo **notificar en consola** y opcionalmente vía email. En este modo, los exploits detectados, no se bloquean por lo que es una configuración poco recomendable en situaciones normales.

Esta configuración puede cambiarse en cualquier momento para permitir a la protección anti-exploit **notificar en consola y actuar** en caso de detectar este tipo de ataques. En la actuación se bloqueará el ataque y se aplicarán medidas de resolución para evitar que el atacante siga comprometiendo la aplicación, el equipo y por consiguiente vuestra red.

Figura 2. Configuración de la tecnología de anti-exploits en el perfil de seguridad

Modo 1: Solo notificar en consola cuando se detecta un exploit

En este modo de comportamiento de la tecnología, cuando se identifique un intento de explotación, no se actuará y simplemente se registrará el hecho presentándose en la consola web de administración y si en la información del módulo Advanced Reporting Tool (ART) y/o en los logs enviados como parte del servicio de SIEMFeeder.

Modo 2: Notificar en consola y actuar ante una la detección Exploits

En este modo de comportamiento de la tecnología, además de notificar en la consola y alertas por email al administrador, la tecnología actuará en el puesto de trabajo o servidor protegido ante la detección de un exploit, bloqueando **el ataque, sin requerir ninguna intervención** por parte del usuario final.

Sin embargo, dado que la gran mayoría de exploits residen en la memoria de la aplicación que está siendo comprometida, en muchas ocasiones es necesario limpiar esa memoria y se requerirá **finalizar el proceso comprometido.**

Si el proceso comprometido es un **proceso crítico del sistema**, detener el ataque puede requerir incluso un **reinicio del equipo**.

Notificación al usuario del equipo comprometido cuando se requiere actuación
Dado el inconveniente que la finalización de una aplicación confiable o el reinicio del sistema, de forma inadvertida, puede ocasionar al usuario final del equipo, el administrador cuenta en la consola con opciones para permitir al usuario finalizar voluntariamente el proceso comprometido, para salvar el trabajo en curso por ejemplo, o reiniciar voluntariamente su equipo.

Figura 3. Exploit detectado y bloqueado

Figura 4. Exploit detectado que requiere finalizar el proceso comprometido

Figura 5. Exploit eliminado tras finalizar el proceso comprometido

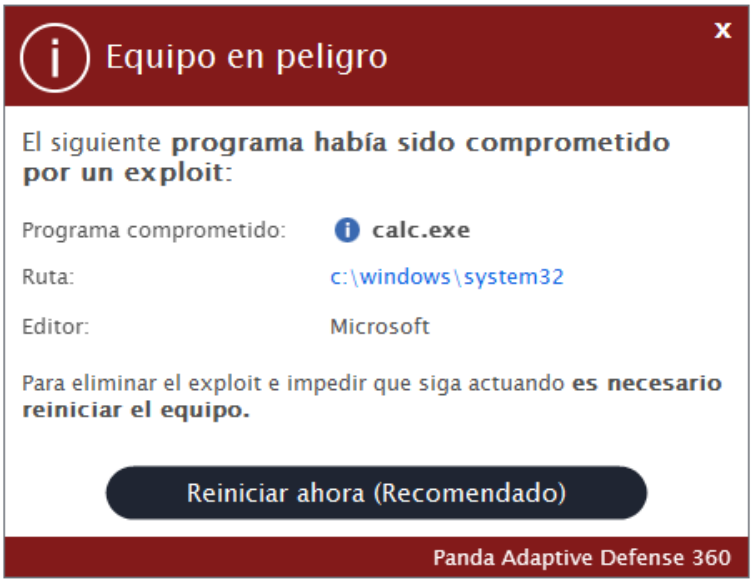


Figura 6. Exploit detectado que requiere reiniciar el equipo. Esta tostada se visualizará periódicamente en el puesto de trabajo o servidor, hasta que se reinicie el equipo

Sin embargo, es **importante** señalar que **desde que se detecta hasta que se finalizar el proceso comprometido o se reinicia la máquina, el intento de explotación sigue cargado en memoria y ejecutando código malicioso**. Con el objetivo de transmitir esta criticidad al

usuario final, hasta que este no finalice la aplicación comprometida o llegados al caso, reinicie el equipo, la aplicación en local mostrará un aviso recordatorio de que debe reiniciar el equipo.

2. Monitorización detecciones anti-exploit

La información de los exploits detectados, tanto en el modo de solo notificación o en el de notificación y actuación, serán visualizados de la siguiente manera en consola:

Visualización en la consola de Adaptive Defense

Dashboard de Actividad. Panel de programas clasificados
Los exploits se contabilizarán en el total de programas clasificados como malware y exploits

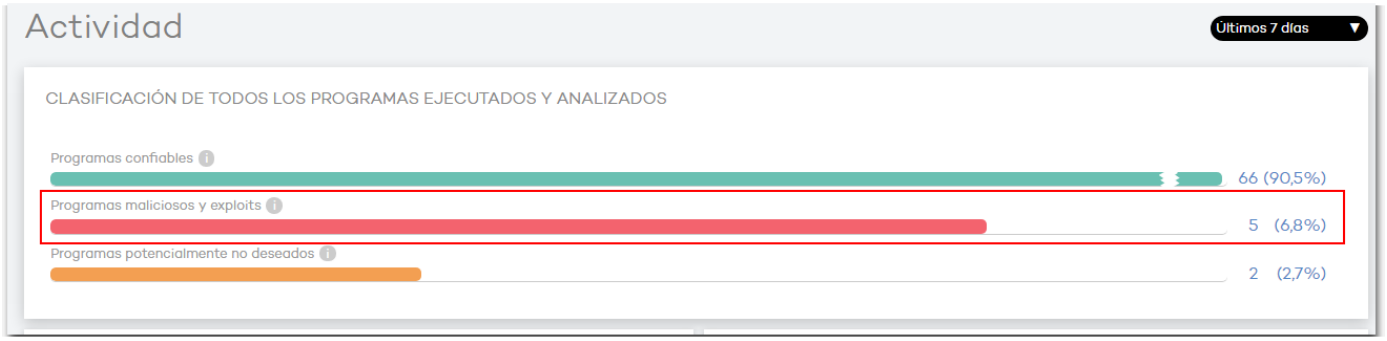


Figura 7. Dashboard de Actividad con Programas maliciosos y exploits

Dashboard de Actividad. Panel de programas maliciosos y exploits
Los exploits detectados serán visualizados en tiempo real en la consola de gestión, en la sección de alertas de Malware y Exploits, en una sección específica creada en esta versión.

Figura 8. Dashboard de programas maliciosos y exploits

Detalle de Exploits detectados
Las alertas de exploit tendrán la siguiente información

- **Nombre del equipo**
- **Ruta del programa comprometido**
- **Acción** llevada a cabo en el dispositivo cuando se detectó el exploit. Con los siguiente valores posibles:

- **Permitido por el administrador**. Cuando el modo es solo notificar.
- **Bloqueo inmediato**. Cuando el modo es notificar y bloquear. El exploit se ha podido bloquear inmediatamente sin requerir intervención del usuario del equipo.
- **Bloqueo no inmediato**. Cuando el modo es notificar y bloquear. Se ha solicitado la finalización de la aplicación comprometido al usuario, el cual lo ha ejecutado posteriormente.
- **Permitido por el usuario**. Cuando el modo es notificar y bloquear. Se ha solicitado la finalización de la aplicación comprometido al usuario, pero este no lo ha realizado
- **Detectado pendiente de reinicio**. Cuando el modo es notificar y bloquear. Esta acción se dará en dos posibles casos:
  - Cuando para bloquear y remediar el exploit sea necesario reiniciar el sistema, porque son sus procesos los que están comprometidos.
  - Cuando se ha requerido la finalización de una aplicación comprometida y el usuario no ha respondido al cabo de un tiempo, se pasa a un estado en el que se requerirá el reinicio del equipo.

- **Riesgo**. Siempre que no sea un bloque inmediato, se indicará que ha existido un riesgo, desde que se detectó hasta que se bloqueó, si llega a hacerse.
- **Fecha de detección.**

Figura 9. Alertas de programas maliciosos y exploits detectados

Figura 10. Detalle de alertas de Exploit

El detalle de la alerta incluye además información relevante para el **análisis forense** del incidente: ciclo de vida y **grafo** con la línea de tiempo del ataque hasta que se detuvo, si esto fue así y **URLs navegadas** antes de que se produjera la detección, ya que es muy probable que alguna de estas esté relacionada con el incidente.

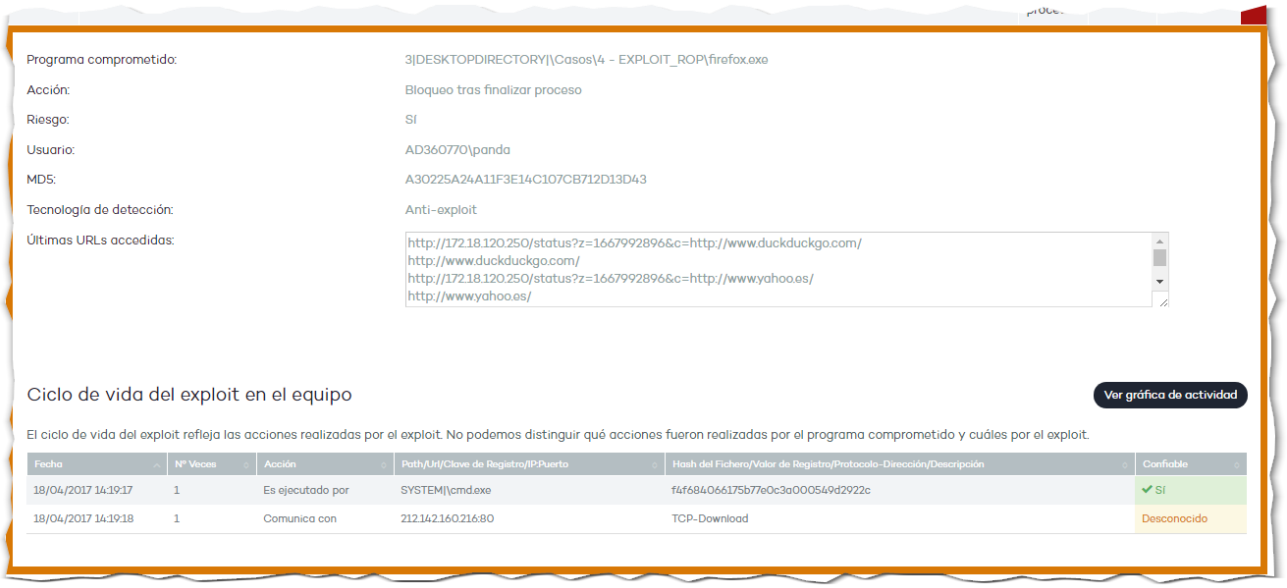


Figura 11. Información detallada del exploit, incluidas las URL navegadas antes de la detección y el ciclo de vida del exploit

Figura 12. Ciclo de vida del exploit en el tiempo

Los filtros predefinidos en la sección de exploits, al igual que en malware, PUPs y elementos bloqueados, permitirán identificar los equipos afectados, las aplicaciones comprometidas, etc.

Informes pre-configurados

Los informes ejecutivos, informes ejecutivos extendidos y el informe de amenazas incluirán información de los exploits detectados.

Alertas por email ante detecciones de exploits

Además, en el caso de tener activado el **envío de email de alertas** de malware, el administrador y/o responsables de seguridad recibirá inmediatamente un correo notificando de dicha detección, con todo detalle para una ágil respuesta.

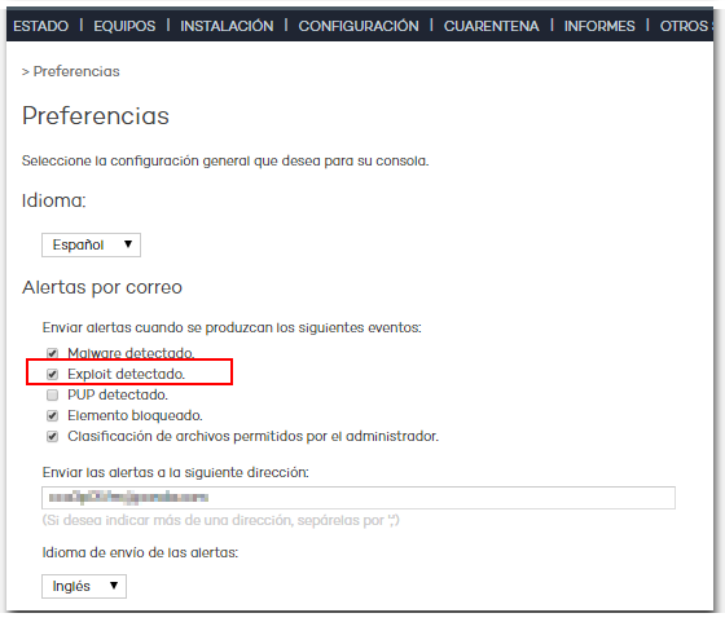


Figura 13. Configuración de alertas por correo electrónico en real time, incluidas las alertas de exploits detectados

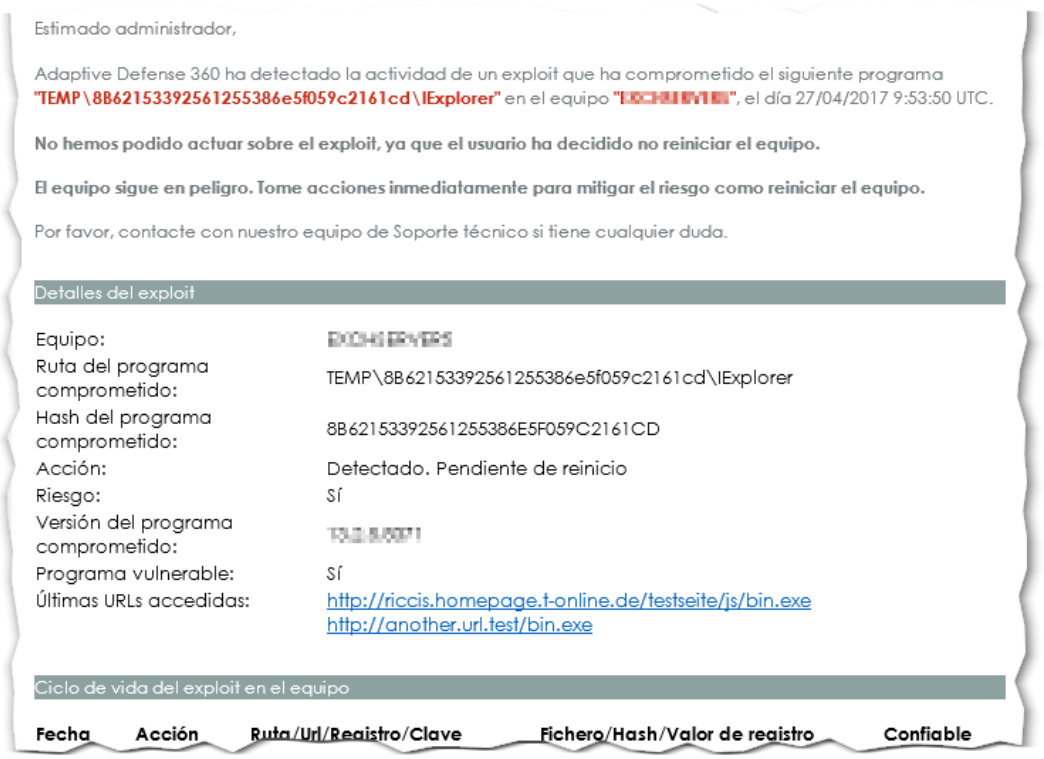
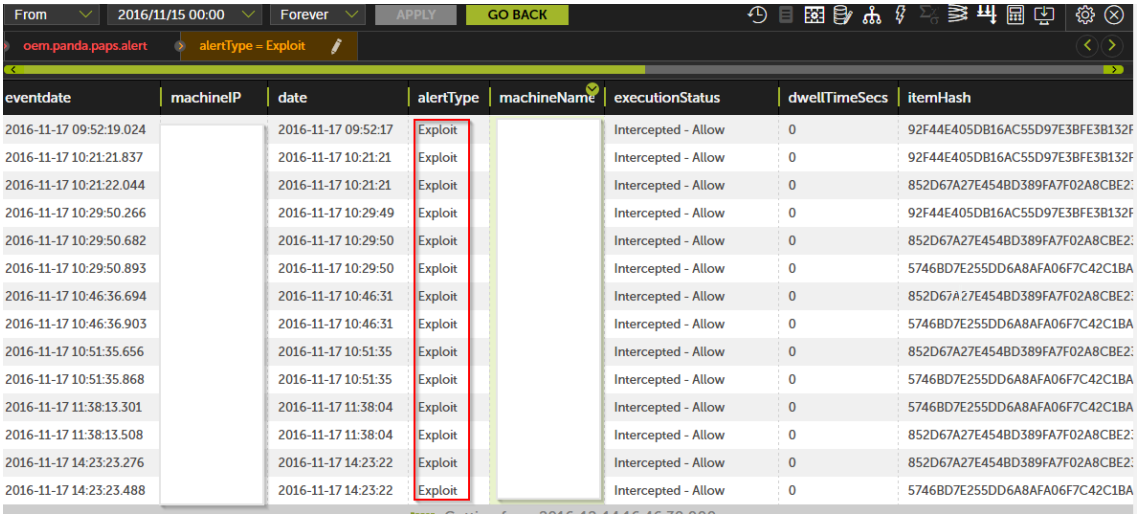


Figura 14. Ejemplo de una alerta por correo ante la detección de un exploit que comprometió al navegador Internet Explorer. El usuario no termino la aplicación y por lo tanto el nivel de riesgo es alto

Detalle de la información disponible en Advanced Reporting Tool (solo para clientes con el módulo Advanced Reporting tool)

Las detecciones de los intentos de explotación de vulnerabilidades, sea cual sea la técnica utilizada, se recibirán en ART como una alerta similar a las de malware y PUP pero con AlertType=Exploit



eventdate	machineIP	date	alertType	machineName	executionStatus	dwellTimeSecs	itemHash
2016-11-17 09:52:19.024		2016-11-17 09:52:17	Exploit		Intercepted - Allow	0	92F44E405DB16AC55D97E3BFE3B132F
2016-11-17 10:21:21.837		2016-11-17 10:21:21	Exploit		Intercepted - Allow	0	92F44E405DB16AC55D97E3BFE3B132F
2016-11-17 10:21:22.044		2016-11-17 10:21:21	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 10:29:50.266		2016-11-17 10:29:49	Exploit		Intercepted - Allow	0	92F44E405DB16AC55D97E3BFE3B132F
2016-11-17 10:29:50.682		2016-11-17 10:29:50	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 10:29:50.893		2016-11-17 10:29:50	Exploit		Intercepted - Allow	0	5746BD7E255DD6A8AFA06F7C42C1BA
2016-11-17 10:46:36.694		2016-11-17 10:46:31	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 10:46:36.903		2016-11-17 10:46:31	Exploit		Intercepted - Allow	0	5746BD7E255DD6A8AFA06F7C42C1BA
2016-11-17 10:51:35.656		2016-11-17 10:51:35	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 10:51:35.868		2016-11-17 10:51:35	Exploit		Intercepted - Allow	0	5746BD7E255DD6A8AFA06F7C42C1BA
2016-11-17 11:38:13.301		2016-11-17 11:38:04	Exploit		Intercepted - Allow	0	5746BD7E255DD6A8AFA06F7C42C1BA
2016-11-17 11:38:13.508		2016-11-17 11:38:04	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 14:23:23.276		2016-11-17 14:23:22	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 14:23:23.488		2016-11-17 14:23:22	Exploit		Intercepted - Allow	0	5746BD7E255DD6A8AFA06F7C42C1BA

Figura 15. Ejemplos de detecciones de tipo Exploit en la tabla *alerts* en Advanced Reporting Tool

En consecuencia, en el caso de verificarse detecciones de este tipo en el parque, la Aplicación Vertical de Incidentes de Seguridad reflejaran estas detecciones.

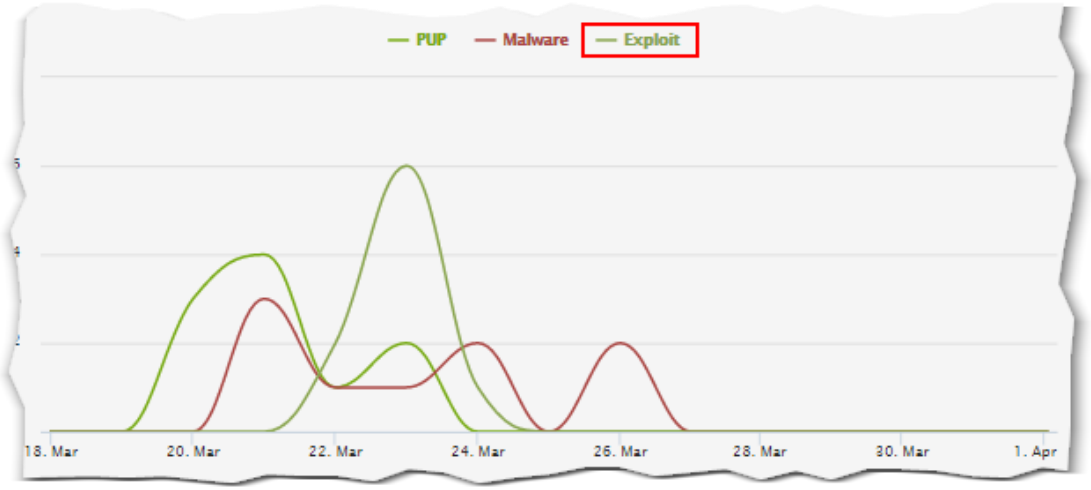


Figura 16. Exploits en la aplicación Vertical de *Security Incidents*

Ver también **Mejoras en el servicio Advanced Reporting Tool**

Esta funcionalidad solo está disponible para clientes suscritos a Advanced Reporting Tool (ART)

Detalle de la información disponible en el SIEM (solo para clientes con el módulo SIEMFeeder)

Las detecciones de los intentos de explotación de vulnerabilidades, sea cual sea la técnica utilizada, se recibirán en el SIEM como una alerta similar a las de malware y PUP. En concreto como un evento de tipo “exploits”.

Ver también **Mejoras en el servicio SIEMFeeder**

3. Detección de ataques malwareless (script-based) y fileless

Los ataques malwareless, o script-based attacks, utilizan archivos no ejecutables, explotan vulnerabilidades en aplicaciones legítimas y comunes como Chrome, Firefox, Internet Explorer, Microsoft Office (Word, Excel, etc), Java VM o productos Adobe y comprometen los puestos de trabajo o servidores mediante el despliegue y ejecución de código en memoria, cuando el usuario abre esos ficheros que contienen por ejemplo macros.
Los ataques con ficheros no ejecutables manipulan la pila de memoria de la aplicación legítima y consiguen sus intenciones maliciosas sin descargar ningún fichero ejecutable malicioso.

Los ataques fileless son los basados en secuencias de comandos con código interpretado, como Java y PowerShell. Estas secuencias de comandos maliciosas se ejecutan sin necesidad de escribir en el disco, son los denominados ataques sin ficheros (fileless).

Por último, muchos ataques utilizan una combinación de macros y línea de comandos con PowerShell. Por ejemplo, apertura de un documento Word con una macro que podría usar técnicas de evasión para ocultarse y desplegar un ataque a través de PowerShell desde un servidor Command&Control remoto.

Este tipos de ataques sin ficheros o con ficheros no ejecutables no son nuevos, pero están creciendo en prevalencia y son imperceptibles para las soluciones antimalware tradicionales.

Panda Adaptive Defense y Panda Adaptive Defense 360, incorpora técnicas que detectan estos tipos de ataques gracias a la monitorización de los procesos, correlación de acciones y a la capacidad de la protección de identificar comportamientos y usos maliciosos de aplicaciones legítimas.

En la versión 2.4 se robustecen estas técnicas. Estos casos se gestionarán a partir de esta versión como cualquier otro tipo de detección, es decir, se presentarán en consola como detecciones de malware y podremos monitorizar su ciclo de vida, se enviarán alertas por email y formará parte de los dashboards e informes.

4. Equipos utilizados para expandir un ataque en la red (Origen de infección)

Como es bien conocido, los atacantes penetran en la red de las empresas utilizando los puntos más débiles de esta y de ahí mediante técnicas de escalado de privilegios, técnicas de evasión y movimientos laterales entre equipos y servidores, se van aproximándose a su objetivo hasta alcanzarlos. En muchas ocasiones, los equipos son dispositivos zombis en manos de un C&C del cual recibe órdenes desde el exterior. Estos equipos zombis puedes ser el origen de un ataque a otros dispositivos.

En estos y otros escenarios, es importante la identificación precoz de los puestos de trabajo y servidores que originan una infección en el parque.

A partir de la versión 2.4 cuando la detección de un malware o PUP o el bloque de un elemento se produzca desde un equipo de la red, la información de este IP origen y el usuario, será parte de la información disponible en el ciclo de vida de ese malware, PUP o elemento bloqueado.

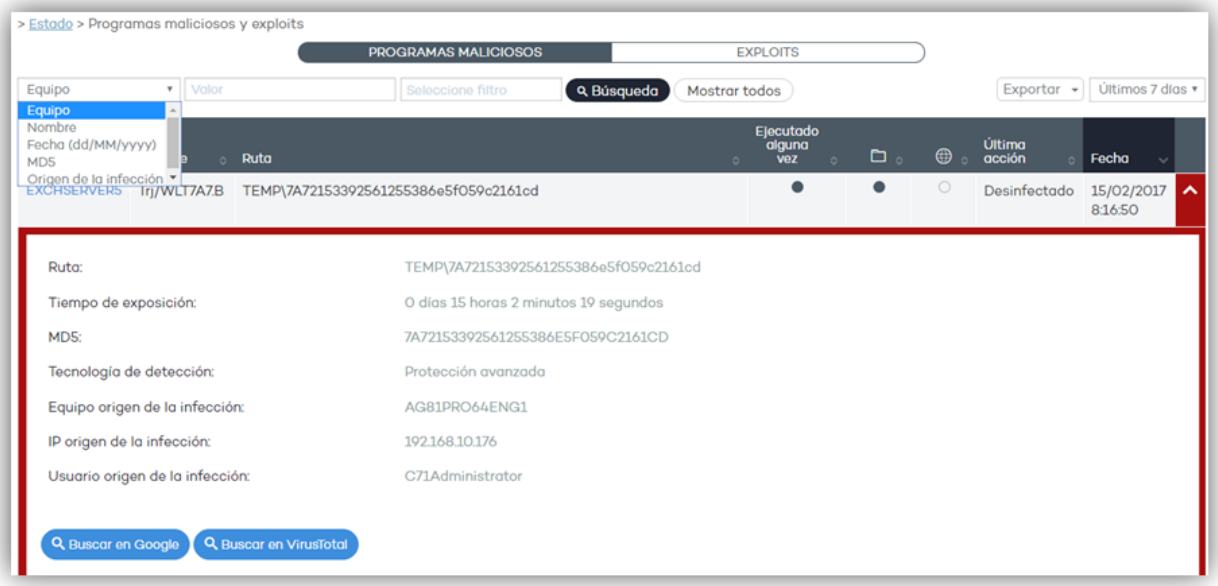


Figura 17. Ejemplo de detección donde conocemos el origen del fichero malicioso

5. Informe de detalle de estado de los equipos

En numerosas ocasiones, sobre todo en medianas y grandes empresas, donde la seguridad de los puestos es gestionada, junto con otros sistemas y aplicaciones, con procesos y herramientas del departamento TIC o por equipos subcontratados, se necesita que la información del estado de seguridad de los equipos y servidores se integre en estos procesos y herramientas. Ejemplo de este caso, son las herramientas corporativas de ticketing.

Por este motivo, en la versión 2.4 se incluye un informe en csv, que puede ser exportado y programado periódicamente, con el detalle del estado de los equipos y servidores protegidos.

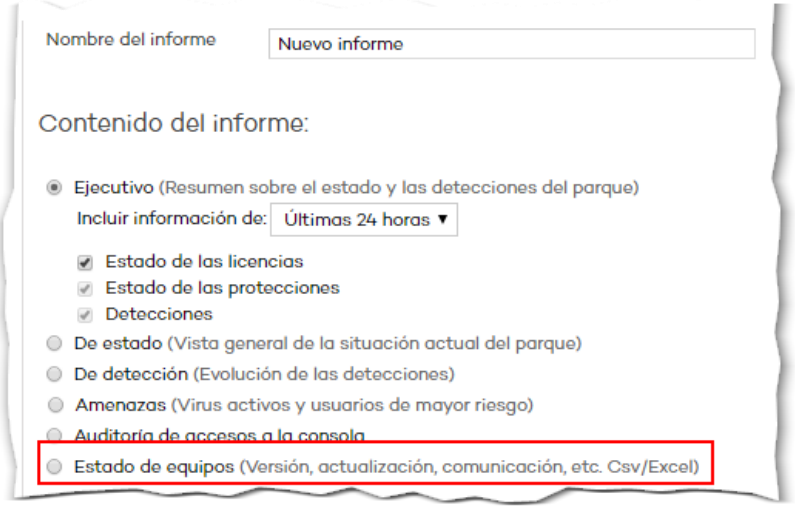


Figure 18. Informe de estado de equipos que permite la integración de esta información en software operacional de la organización como por ejemplo ticketing

6. Mejoras en el servicio Advanced Reporting Tool

Esta funcionalidad solo está disponible para clientes suscritos a Advanced Reporting Tool (ART)

6.1. Datos incorporados a las tablas ya existentes

- En la tabla **OPS**, se incluye la línea de comandos con la que se lanzó la aplicación, incluyendo sus parámetros.

- En la tabla **ALERTS**:
  - Tendremos eventos tipo Exploit y si está disponible, se incluirán las últimas URLs navegadas, hasta un máximo de 10, separadas por "*" en el campo UrlList.
  - En el caso de detecciones de tipo malware, si la detección se produce cuando se intenta mover o copiar un fichero malware desde un equipo de la red a otro, se incluirá su IP así como el usuario autenticado.

- En la tabla **SOCKETS**, hasta ahora se indicaba solo el protocolo a nivel de red (TCP, UDP, ICMP). En esta versión se incluye información respecto a conexiones a nivel de aplicación para RDP (Remote Desktop Protocol), permitiendo identificar los casos de ataques por RDP, ya que aparecerá el valor TCP-RDP para la clave Protocol.

6.2. Nuevo Widget en la aplicación vertical Security Incidents

Se presentan dos nuevos widget asociados a la información del equipo origen de una copia o movimiento de un malware a otro equipo. Uno de los widget es un grafo de nodos, donde se representa la relación entre los equipos en evolución en el periodo de tiempo seleccionado.

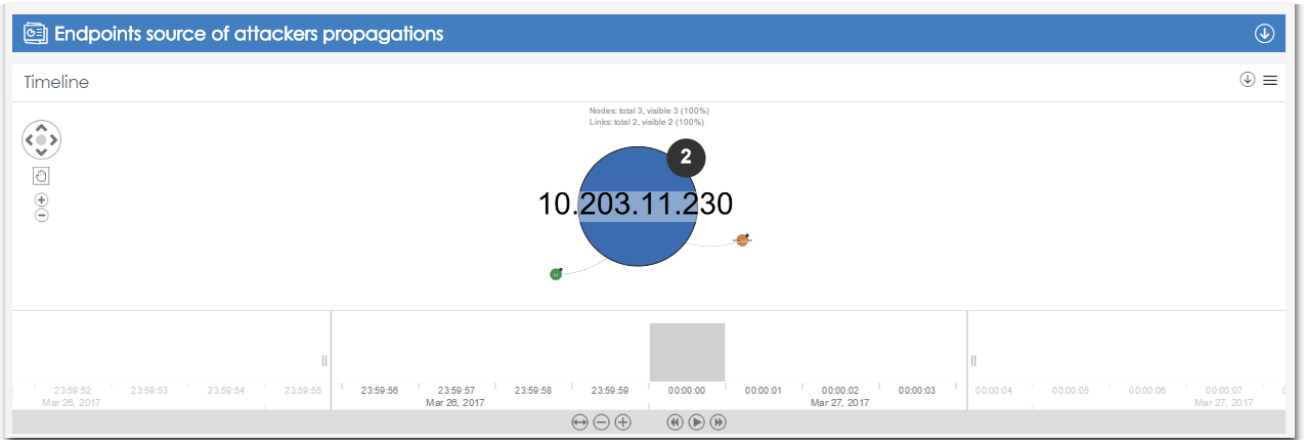


Figura 19. Nuevo widget en ART con el ciclo de vida de equipos origen de infecciones y los equipos afectados

El segundo es un grafo de afinidad, donde se relacionan los equipos origen y los equipos destino.

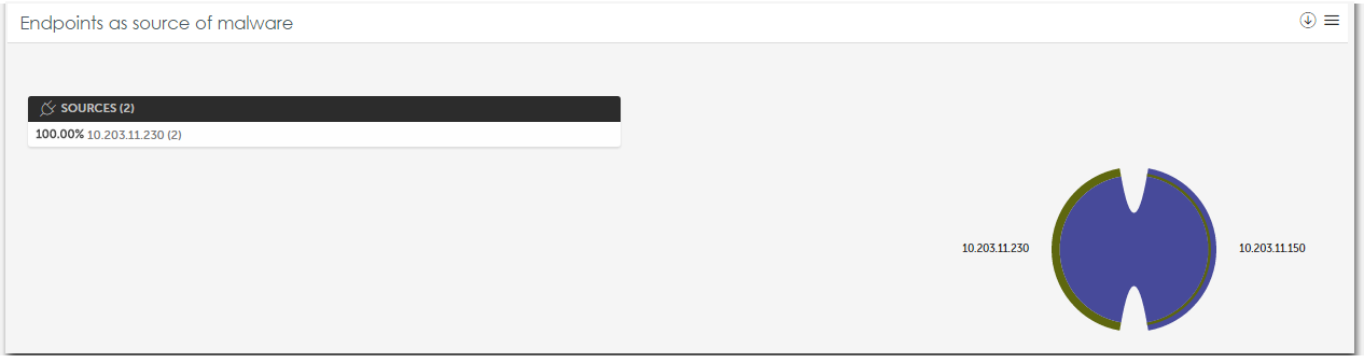


Figura 20. Nuevo Widget en ART con la relación de máquina infectante y máquinas infectadas

6.3. Actualización de la categoría de los hashes involucrados en los eventos

En todas las tablas donde se incluye la categoría asociada al hash del proceso padre o proceso hijo, por cada hash padre e hijo, si existe, se visualizará la categoría en el momento del evento pero además ahora se presentará la categoría actualizada (con una cadencia máxima de 4 horas)

7. Mejoras en el servicio SIEMFeeder

Esta funcionalidad solo está disponible para clientes suscritos a SIEMFeeder.

7.1. Más información en los eventos

- En eventos de **OPS**, se incluye la línea de comandos con la que se lanzó la aplicación, incluyendo sus parámetros.

- En los eventos **ALERTS**:
    - Tendremos eventos tipo Exploit y si está disponible, se incluirán las últimas URLs navegadas, hasta un máximo de 10, separadas por "*" en el campo UrlList. En el caso de exploit con origen documento se rellenará el campo Doclist

Figura 21. Formato eventos de tipo Alert en SIEMFeeder

    - En el caso de detecciones de tipo malware, si la detección se produce cuando se intenta mover o copiar un fichero malware desde un equipo de la red a otro, se incluirá su IP así como el usuario autenticado.

- En los eventos **SOCKETS**, hasta ahora se indicaba solo el protocolo a nivel de red (TCP, UDP, ICMP). En esta versión se incluye información respecto a conexiones a nivel de aplicación para RDP (Remote Desktop Protocol), permitiendo identificar los casos de ataques por RDP, ya que aparecerá el valor TCP-RDP para la clave Protocol.

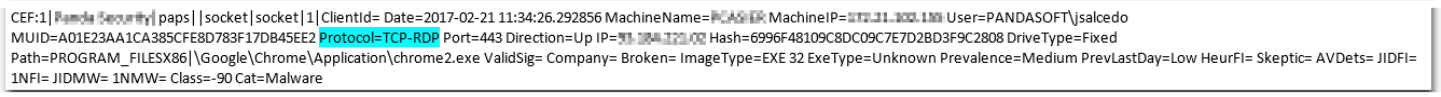


Figura 22. Eventos de tipo Sockets en SIEMFeeder

7.2. Mayor flexibilidad en la integración con tu SIEM on-premise

Además de la entrega de logs de la actividad de los equipos y servidores protegidos vía sFTP o FTP, a partir de la versión 2.4 los logs podrán ser enviados vía protocolo Syslog. Opcionalmente, los datos pueden ser enviados cifrados mediante SSL/TLS. Para hacer uso del protocolo Syslog se requiere un servidor Syslog en el lado cliente que, en ocasiones, ya existe en el SIEM.

Es importante tener en cuenta que se requerirá información previa de configuración y un tiempo de ajuste de los parámetro del servicio (número de conexiones simultaneas, reintentos – por defecto 3-, etc.).

Por último, en esta versión, con el objetivo de fortalecer el nivel de seguridad e integridad de la información, se despliega un servicio de VPN para el envío de logs vía FTP/sFTP.

Nota: El formulario de recogida de información para la puesta en marcha del servicio, estará disponible en la extranet con los datos necesario actualizados.

8. Otras mejoras de la versión 2.4

A partir de la versión 2.4 de Adaptive Defense y Adaptive Defense 360 con protección 7.70 y agente 7.71, el comportamiento de algunas características funcionales se ven mejoraras de la siguiente forma:

1. **Gestión de Exclusiones:**
   - Las exclusiones que se realizan a nivel de perfil, también afectarán a la protección avanzada
   - Consistencia en el envío de alertas de detecciones y las exclusiones: Si un elemento es excluido de la protección avanzada, no se enviarán más alertas por email sobre ese elemento hasta que deje de ser un elemento excluido.

2. **Modo Lock y usuarios avanzados**: Si el usuario decide ejecutar una aplicación no clasificada como confiable previamente, se permitirá su ejecución y además la carga de todas las librerías que esta aplicación necesitara, incluso si estas no están todavía clasificadas como confiables. Es decir, el usuario no se verá interrumpido, dando prioridad a su decisión a nivel de aplicación.

3. Corrección de los casos de **detecciones en Servidores Exchange en elementos en tránsito**, para los cuales no existe ruta que mostrar en consola.

4. Cuando la protección en un puesto de trabajo o servidor está funcionando con la **protección antimalware desactiva** y la **protección avanzada**, se corregirá la información mostrada en la traybar del equipo protegido, indicándose que la protección avanzada esta activa.

5. Cuando se produce una detección y se comunica este hecho al usuario del puesto de trabajo o servidor, **la notificación es visible unos minutos**, ocultándose automáticamente, si el usuario no ha tenido ocasión de ver la notificación, pierde información importante para su seguridad. A partir de ahora, se incluyen **notificaciones periódicas hasta que el usuario confirma su visualización.**

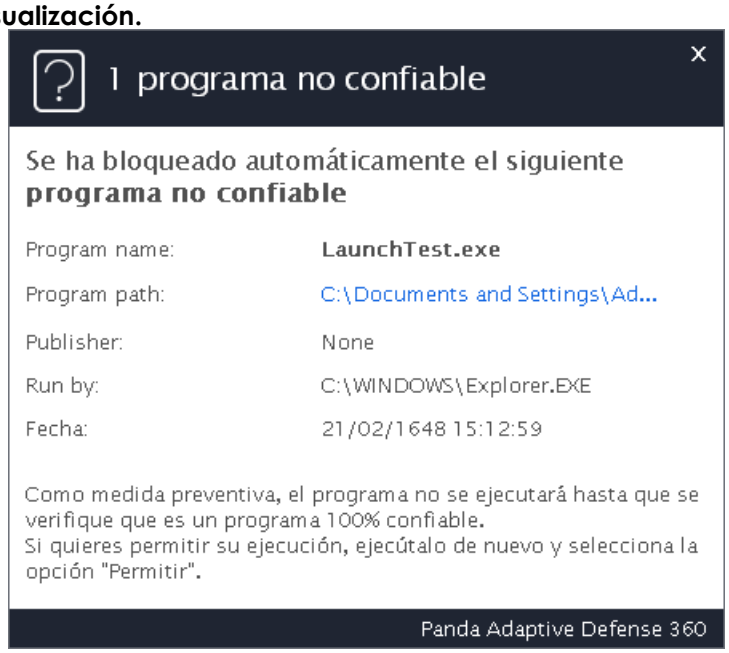


Figura 23. Tostada que recuerda al usuario que un elemento fue bloqueado

Además a partir de esta versión:

- Será posible activar el módulo de **Remote Control 100% Panda** e **integrado** en la protección y agente de Adaptive Defense/Adaptive Defense 360 de los puesto de trabajo y servidor ya protegidos.
- Se incluye un acceso directo a **guía de servicio SIEMFeeder** desde la consola web

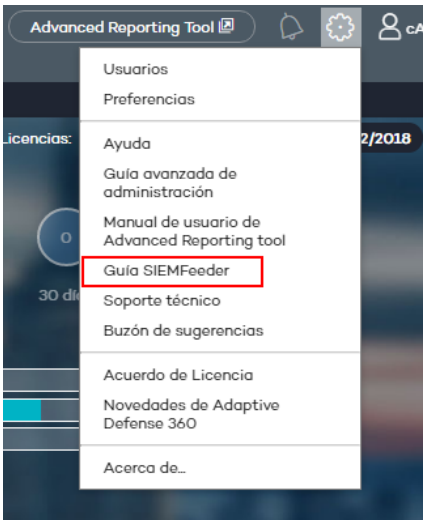


Figura 24. Acceso directo a la Guía de SIEMFeeder

Por último, hemos hecho cambios en el acuerdo de licencia:

- Ajustes la cláusula de licenciamiento de Terminal Server,
- Nueva clausula sobre el uso del servicio, destinado exclusivamente a ofrecer el máximo nivel de protección a nuestros clientes y partners
- Por último, se informa que podríamos contactar con los administradores de la consola web para realizar encuestas del producto con el objetivo de mejorar este, existe lógicamente un mecanismo para dejar de recibir esta tipo de comunicaciones.

Por este motivo, la primera vez que se accede a la consola de gestión después de la actualización a la versión 2.4, se solicitará **volver a confirmar el acuerdo de licencia**.

9. Nuevos sistemas compatibles

A partir de la versión 2.4 de Adaptive Defense y Adaptive Defense 360 con protección 7.70 y agente 7.71, se soportan los siguientes sistemas:

- **Server Core 2008 (32 y 64 bits), 2008R2 (64 bits), 2012 y 2012 R2, sin GUI instalada**. Debido a la ausencia de GUI en el servidor, se recomiendas las siguientes prácticas:
  - Realizar el proceso de instalación y actualización de una forma programada, ya que no se avisará de la necesidad de reinicio en el servidor y se ejecutará cuando se requiere en dichos procesos o se notificará de su necesidad en consola (según configuración en el perfil). Se recomienda asegurarse de que el servidor se ha reiniciado correctamente monitorizando en la consola.
  - Es importante mantener actualizado en el perfil cualquier cambio que afecte al proxy, ya que, en caso de no replicarse correctamente la configuración, el servidor no muestra ninguna ventana solicitando conexión.
- **Windows MultiPoint Server 2012**
- Nueva versión de protección para **MAC** basado en **Virus Barrier X9**

10. Exportación del ciclo de vida y detalle de la línea de comandos (Versión 2.4.1)

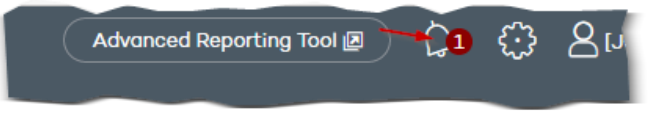
En la versión 2.4.1 se incluye la funcionalidad de exportación a csv del detalle del ciclo de vida de una detección o bloqueo o de varias detecciones o bloqueos. Esta información puede ser fácilmente importada y/o gestionada con aplicaciones como Excel, permitiendo el análisis forense desde un punto de vista global de la red, con el máximo nivel de granularidad y correlacionando cualquier elemento o entidad.

Por ejemplo, podremos exportar todas las detecciones que se han producido en las últimas 24 horas e identificar cuantos equipos se han visto afectados por un determinado malware como parte de un ataque.
Podremos también identificar todos los accesos a ficheros que se han producido en ese ataque y determinar con detalle el impacto en la organización.
Podremos también correlacionar las detecciones en el tiempo e identificar la secuencia en los movimientos laterales de un atacante y su forma de entrada a la red corporativa.

Además, en esta versión se presentará en consola, y por lo tanto será también exportable, el detalle de la línea de comandos y sus parámetros en caso de que el atacante haga uso de técnicas filessless o script-based, por ejemplo el uso de PowerShell.

11. ¿Cuándo y cómo puedes actualizar a la v2.4?

La nueva versión 2.4, estará disponibles desde el 8 de mayo de 2017 accediendo a la información que se publicará en la consola de gestión en el área de notificaciones.



Ten, por favor, en cuenta que la versión de la consola será la 2.4, la de la protección es la 7.70, y la del agente la 7.71.

- Para actualizar la versión de la consola a la versión 2.4, tienes que, activamente, pulsar el botón que encontrarás en la notificación.

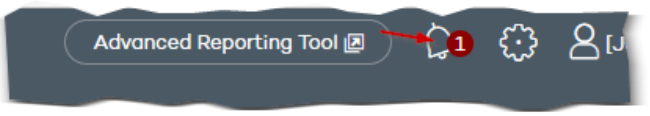
  Ten por favor en cuenta, que a lo largo de las próximas semanas actualizaremos la versión de consola automáticamente. Este es el calendario de actualización automática.
  - Clientes de menos de 101 licencias: Miércoles 17/05
  - Clientes de entre 101 y 501 licencias: Miércoles 29/05
  - Clientes de más de 501 licencias: Lunes 12/06

- La versión del agente a la 7.71 se actualia automáticamente en los puestos, una vez hayas actualizado la versión de la consola a la 2.4.

- La versión de la protección se actualizará a la 7.70 de forma automática si así está configurado en las políticas de seguridad que aplican ese equipo. Esto lo ves en los perfiles de configuración.

12. ¿Cuándo y cómo puedes actualizar a la v2.4.1?

La nueva versión 2.4.1, estará disponibles en Junio y te lo notificaremos en la consola de gestión en el área de notificaciones.



A diferencia de la versión 2.4, la versión 2.4.1. solo conlleva una actualización de consola y no es necesario ningún tipo de actualiación en los equipos protegidos.