Panda Adaptive Defense

Guía de administración de Panda Adaptive Defense

Autor: Panda Security

Versión: 4.30.00

Fecha: 5/25/2023

TOC

Panda Adaptive Defense

Guía de administración de Panda Adaptive Defense

Autor: Panda Security

Versión: 4.30.00

Fecha: 5/25/2023

Aviso legal.

Marcas registradas.

Información de contacto.

Oficinas centrales:

Panda Security

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 España.

https://www.pandasecurity.com/spain/about/contact/

Acerca de la Guía de administración de Panda Adaptive Defense

Para obtener la versión más reciente de la documentación en formato PDF consulta la dirección web:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/latest/ADAPTIVEDEFENSEoAP-guia-ES.pdf

Para consultar un tema específico, accede a la ayuda web del producto disponible en:

https://www.pandasecurity.com/enterprise/downloads/docs/product/help/adaptivedefense/latest/es/index.htm

Información sobre las novedades de la versión

Para conocer las novedades de la ultima versión de Panda Adaptive Defense consulta la siguiente URL:

https://info.pandasecurity.com/aether/?product=AD&lang=es

Documentación técnica no incluida en esta Guía de administración para módulos y servicios compatibles con Panda Adaptive Defense

Para acceder a la Guía del usuario para Panda Advanced Reporting Tool consulta la siguiente URL:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/ADVANCEDREPORTINGTOOL-AETHER-Guia-ES.pdf

Para acceder a la Guía para el usuario de Panda Data Control consulta la siguiente URL:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/DATACONTROL-AETHER-Guia-ES.pdff

Para acceder a las guías de Panda SIEMFeeder consulta las siguientes URLs:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeeder-Manual-ES.PDF

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeederAD-ManualDescripcionEventos-ES.pdf

Soporte técnico

Panda Security ofrece un soporte técnico global cuyo objetivo principal es responder a cuestiones especificas sobre el funcionamiento de sus productos. El equipo de soporte técnico también genera documentación sobre detalles técnicos del producto, que ofrece a través de su portal eKnowledge Base.

Para acceder a información específica del producto consulta la siguiente URL:

https://www.pandasecurity.com/spain/support/adaptive-defense-aether.htm

Para acceder al portal eKnowledge Base consulta la siguiente URL:

https://www.pandasecurity.com/spain/support/#enterprise

Encuesta sobre la Guía de administración de Panda Adaptive Defense

Evalúa esta Guía de administración y envíanos sugerencias y peticiones para próximas versiones de la documentación en:

https://es.surveymonkey.com/r/feedbackADGuideES

Glossary

1

100% Attestation Service

Servicio de Panda Adaptive Defense incluido en la licencia básica que clasifica el 100% de los procesos ejecutados en los equipos de usuario y servidores para emitir una valoración sin ambigüedades (goodware o malware, sin sospechosos).

A

Adaptador de red

Hardware que permite la comunicación entre diferentes equipos conectados a través de una red de datos. Un equipo puede tener más de un adaptador de red instalado y es identificado en el sistema mediante un número de identificación único.

Adware

Programa que una vez instalado o mientras se está instalando, ejecuta, muestra o descarga automáticamente publicidad en el equipo.

Agente Panda Security

Uno de los dos módulos del software de cliente Panda Adaptive Defense . Se encarga de las comunicaciones entre los equipos de la red y los servidores en la nube de Panda, además de gestionar los procesos locales.

Alerta

Ver Incidencia.

Análisis forense

Conjunto de técnicas y procesos ejecutados por el administrador de la red con herramientas especializadas para seguir la ejecución de un programa malicioso y determinar las consecuencias de la infección.

Análisis heurístico

Análisis estático formado por un conjunto de técnicas que inspeccionan de forma estática los ficheros potencialmente peligrosos. Este tipo de análisis se realiza en base a cientos de características que ayudan a determinar la

probabilidad de que el fichero pueda llevar a cabo acciones maliciosas o dañinas cuando se ejecute en el equipo del usuario.

Anti-tamper

Conjunto de tecnologías que evitan la manipulación de los procesos de Panda Adaptive Defense por parte de amenazas avanzadas y APT que buscan sortear las capacidades de protección de la herramienta de seguridad instalada.

APT (Advanced Persistent Threat)

Conjunto de estrategias emprendidas por hackers orientadas a infectar la red del cliente, utilizando múltiples vectores de infección de forma simultánea para pasar inadvertidos a los antivirus tradicionales durante largos periodos de tiempo. Su objetivo principal es económico (robo de información confidencial de la empresa para chantaje, robo de propiedad intelectual etc.).

Árbol de carpetas

Estructura jerárquica formada por agrupaciones estáticas, utilizada para organizar el parque de equipos y facilitar la asignación de configuraciones.

Árbol de filtros

Colección de filtros agrupados en carpetas que facilitan la organización del parque de equipos y la asignación de configuraciones.

Archivo de identificadores / fichero de firmas

Fichero que contiene los patrones que el antivirus utiliza para detectar las amenazas.

Asignación automática de configuraciones

Ver Herencia.

Asignación indirecta de configuraciones

Ver Herencia.

Asignación manual de configuraciones

Asignación de una configuración a un grupo de forma directa, en contraposición al establecimiento de configuraciones automático o indirecto, que utiliza el recurso de la herencia para fijar configuraciones sin intervención del administrador.

ASLR (Address Space Layout Randomization)

Técnica implementada por el sistema operativo para mitigar los efectos de ataques de tipo exploit basados en desbordamiento de buffer. Mediante ASLR el sistema operativo introduce aleatoriedad a la hora de asignar direcciones de memoria para reservar espacio destinado a la pila, el heap y las librerías cargadas por los procesos. De esta forma, se dificulta la utilización ilegítima de

llamadas a funciones del sistema por desconocer la dirección física de memoria donde residen.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

Conjunto de recursos desarrollados por la empresa Mitre Corp. para describir y categorizar los comportamientos peligrosos de los ciberdelincuentes, basados en observaciones a lo largo de todo el mundo. ATT&CK es una lista ordenada de comportamientos conocidos de los atacantes, separados en tácticas y técnicas, y que se expresan a través de una matriz. Ya que esta lista es una representación completa de los comportamientos que los hackers reproducen cuando se infiltran en las redes de las empresas, es un recurso útil para desarrollar mecanismos tanto defensivos como preventivos y resolutivos por parte de las organizaciones. Consulta Mitre corp..

Audit

Modo de configuración de para visualizar la actividad de los procesos ejecutados en los equipos protegidos de la red sin desencadenar ninguna acción de protección (desinfección o bloqueo).

B

Backup

Área de almacenamiento de ficheros maliciosos no desinfectables, así como de spyware y herramientas de hacking detectadas. Todos los programas eliminados del sistema por ser clasificados como amenazas se copian de forma temporal en el área de backup / cuarentena durante un periodo de entre 7 y 30 días según su tipo.

BitLocker

Software instalado en algunas versiones de los equipos Windows 7 y superiores encargado de gestionar el cifrado y descifrado de los datos almacenados en los volúmenes del equipo y utilizado por Panda Full Encryption.

Bloquear

Acción de que impide la ejecución de los programas instalados en el equipo del usuario debido a uno de los motivos siguientes: Programas clasificados como amenaza. Programas desconocidos para y la política de protección avanzada esta configurada como lock o como hardening y su origen es no confiable. Programas bloqueados por políticas establecidas por el administrador.

C

Caché (rol)

Equipos que descargan y almacenan de forma automática todos los ficheros necesarios para que otros equipos con Panda Adaptive Defense instalado puedan actualizar el archivo de identificadores, el agente y el motor de protección sin necesidad de acceder a Internet. De esta manera se produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Cambio de comportamiento

Al clasificar como malware o goodware un programa que el administrador permitió su ejecución cuando todavía era desconocido, se puede comportar de dos maneras: Eliminarlo de la lista de Programas permitidos: si se ha clasificado como goodware seguirá pudiéndose ejecutar, si se ha clasificado como malware, se impedirá su ejecución. Mantener en la lista de Programas permitidos: se seguirá permitiendo su ejecución independientemente de que se trate de malware o goodware.

Ciclo de protección adaptativa

Nuevo enfoque de seguridad basado en la integración de un conjunto de servicios de protección, detección, monitorización, análisis forense y resolución, todos ellos centralizados en una única consola de administración accesible desde cualquier lugar y en cualquier momento.

Ciclo de vida del malware

Detalle de todas las acciones desencadenadas por un programa malicioso, desde que fue visto por primera vez en un equipo del cliente hasta su clasificación como malware y posterior desinfección.

CKC (Cyber Kill Chain)

La empresa Lockheed-Martin describió en 2011 un marco o modelo para defender las redes informáticas, en el que se afirmaba que los ciberataques ocurren en fases y cada una de ellas puede ser interrumpida a través de controles establecidos. Desde entonces, la Cyber Kill Chain ha sido adoptada por organizaciones de seguridad de datos para definir las fases de los ciberataques. Estas fases abarcan desde el reconocimiento remoto de los activos del objetivo hasta la exfiltración de datos.

Clave de recuperación

Cuando se detecta una situación anómala en un equipo protegido con Panda Full Encryption o en el caso de que hayamos olvidado la contraseña de desbloqueo, el sistema pedirá una clave de recuperación de 48 dígitos. Esta clave

se gestiona desde la consola de administración y debe ser introducida para completar el inicio del equipo. Cada volumen cifrado tendrá su propia clave de recuperación independiente.

Configuración

Ver Perfil de configuración.

Consola Web

Herramienta de gestión del servicio de seguridad avanzada Panda Adaptive Defense, accesible desde cualquier lugar y en cualquier momento mediante un navegador web compatible. Con la consola web el administrador puede desplegar el software de protección, establecer las configuraciones de seguridad y visualizar el estado de la protección. También permite utilizar herramientas de análisis forense que establecen el alcance de los problemas de seguridad.

Cuarentena

Ver Backup.

Cuenta de usuario

Ver Usuario (consola).

CVE (Common Vulnerabilities and Exposures)

Lista de información definida y mantenida por The MITRE Corporation sobre vulnerabilidades conocidas de seguridad. Cada referencia tiene un número de identificación único, ofreciendo una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

D

DEP

Característica de los sistemas operativos que impide la ejecución de páginas de memoria destinadas a datos y marcadas como no ejecutables. Esta característica se diseñó para prevenir la explotación de fallos por desbordamiento de buffer.

Desbloqueado (programa)

Programas inicialmente bloqueados por no haber obtenido todavía una clasificación, pero que el administrador de la red permite su ejecución de forma selectiva y temporal para minimizar las molestias a los usuarios de la red.

Desbordamiento de buffer

Fallo en la gestión de los buffers de entrada de un proceso. En estos casos, si el volumen de datos recibido es mayor que el tamaño del buffer reservado, los

datos sobrantes no se descartan, sino que se escriben en zonas de memoria adyacentes al buffer. Estas zonas de memoria pueden ser interpretadas como código ejecutable en sistemas anteriores a la aparición de la tecnología DEP.

Descubridor (rol)

Equipos capaces descubrir puestos de usuario y servidores no administrados para iniciar una instalación remota del agente Panda Adaptive Defense.

Desinfectable

Fichero infectado por malware del cual se conoce el algoritmo necesario para poder revertirlo a su estado original.

DHCP

Servicio que asigna direcciones IP a los nuevos equipos conectados a la red.

Dialer

Programa que marca un número de tarificación adicional (NTA), utilizando para ello el módem. Los NTA son números cuyo coste es superior al de una llamada nacional.

Dirección IP

Número que identifica de manera lógica y jerárquica la interfaz de red de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

Dirección MAC

Identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta o interfaz de red.

Directorio Activo

Implementación propietaria de servicios LDAP (Lightweight Directory Access Protocol, Protocolo Ligero/Simplificado de Acceso a Directorios) para máquinas Microsoft Windows. Permite el acceso a un servicio de directorio para buscar información diversa en entornos de red.

Distribución Linux

Conjunto de paquetes de software y bibliotecas que conforman un sistema operativo basado en el núcleo Linux.

DNS (Domain Name System)

Servicio que traduce nombres de dominio con información de diversos tipos, generalmente direcciones IP.

Dominio

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios está centralizada en un servidor llamado Controlador Principal de Dominio (PDC) o Directorio Activo (AD).

E

Entidad

Predicado o complemento incluido en las tablas de acciones del módulo análisis forense.

Entidad (Data Control)

Conjunto de datos que tomados como una unidad adquieren un significado propio.

EoL (End Of Life)

Término utilizado para indicar el final del ciclo de vida de un producto. A partir de la fecha indicada el producto ya no recibirá actualizaciones ni parches que corrijan sus defectos, convirtiéndose en un objetivo claro para los hackers.

Equipos sin licencia

Equipos cuya licencia ha caducado o no ha sido posible asignar una licencia válida por haberse superado el número máximo permitido de instalaciones de la protección. Estos equipos no están protegidos, pero son visibles en la consola web de administración.

Evento

Acción relevante ejecutada por un proceso en el equipo del usuario y monitorizada por. Los eventos se envían a la nube de en tiempo real como parte del flujo de telemetría. Allí, los analistas, threat hunters y los procesos automáticos de Machine Learning los analizan en su contexto para determinar si son susceptibles de pertenecer a la cadena CKC de un ataque informático. Consulta “CKC (Cyber Kill Chain)”.

Excluido (programa)

Son programas inicialmente bloqueados por haber sido clasificados como malware o PUP, pero que el administrador de la red permite su ejecución de forma selectiva y temporal excluyéndolos del análisis.

Exploit

De forma general un exploit es una secuencia de datos especialmente diseñada para provocar un fallo controlado en la ejecución de un programa vulnerable. Después de provocar el fallo, el proceso comprometido interpretará por error parte de la secuencia de datos como código ejecutable, desencadenando acciones peligrosas para la seguridad del equipo.

F

Filtro

Contenedor de equipos de tipo dinámico que agrupa de forma automática aquellos elementos que cumplen con todas las condiciones definidas por el administrador. Los filtros simplifican la asignación de configuraciones de seguridad y facilitan la administración de los equipos del parque informático.

FQDN (Fully Qualified Domain Name)

Es un nombre de dominio que especifica la localización de forma precisa y sin ambiguedades dentro del árbol de jerarquía del sistema de nombres DNS. El FQDN especifica todos los niveles del dominio incluyendo el nivel superior y la zona raiz (root).

G

GDPR (General Data Protection Regulation)

Normativa que regula la protección de los datos de los ciudadanos que viven en la Unión Europea. Consulta el enlace http://www.privacy-regulation.eu/es/index.htm para acceder al reglamento completo.

Goodware

Fichero clasificado como legítimo y seguro tras su estudio.

Grafo de actividad / grafo de ejecución

Representación visual de las acciones ejecutadas por las amenazas, poniendo énfasis en el enfoque temporal.

Grupo

Contenedor de tipo estático que agrupa a uno o más equipos de la red. La pertenencia de un equipo a un grupo se establece de forma manual. Los grupos se utilizan para simplificar la asignación de configuraciones de seguridad y para facilitar la administración de los equipos del parque informático.

Grupo de trabajo

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios residen en cada uno de los equipos de forma independiente.

H

Hardening

Modo de configuración de que bloquea los programas clasificados como malware y los ficheros desconocidos cuyo origen es una fuente no fiable: Internet.

Unidades externas de almacenamiento Otros equipos de la red del cliente.

Heap Spraying

Head Spray es una técnica utilizada para facilitar la explotación de vulnerabilidades por parte de un proceso malicioso independiente. Debido a la constante mejora de los sistemas operativos, la explotación de vulnerabilidades se ha convertido es un proceso muy aleatorio. Debido a que el comienzo de la región de memoria heap de un proceso es predecible, y las posteriores reservas de espacio son secuenciales, Head Spray aporta predictibilidad a los ataques, sobrescribiendo porciones de la región de memoria heap del proceso objetivo. Estas porciones de memoria serán referenciadas más adelante por un proceso malicioso para ejecutar el ataque. Esta técnica es muy empleada para explotar vulnerabilidades de navegadores y sus plugins correspondientes.

Herencia

Método de asignación automática de configuraciones sobre todos los grupos descendientes de un grupo padre, ahorrando tiempo de gestión. También llamado Asignación automática de configuraciones o Asignación indirecta de configuraciones.

Herramienta de hacking

Programa utilizado por hackers para causar perjuicios a los usuarios de un ordenador, pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.

Hoaxes

Falsos mensajes de alarma sobre amenazas que no existen y que llegan normalmente a través del correo electrónico.

I

Identificador

Palabra clave utilizada en las búsquedas de que permite seleccionar un tipo de entidad.

IDP (Identity Provider)

Servicio centralizado responsable de gestionar las identidades de los usuarios.

IFilter

Librería del sistema operativo que permite el acceso al contenido de ficheros ofimáticos.

Incidencia

Mensaje relativo a la protección avanzada de Panda Adaptive Defense, susceptible de requerir la intervención del administrador. Las incidencias se

reciben mediante la consola de administración y el correo electrónico (alertas), y el usuario del equipo protegido mediante mensajes generados por el agente que se visualizan en el escritorio de su dispositivo.

Indexar

Proceso que analiza el contenido de los ficheros y lo almacena en una base de datos de rápido acceso para acelerar su búsqueda.

Indicador de ataque (IOA)

Es un indicio con alta probabilidad de pertenecer a un ataque informático. Por lo general, se trata de ataques en fase temprana o en fase de explotación. Estos ataques no suelen utilizan malware, ya que los atacantes suelen utilizar las propias herramientas del sistema operativo para ejecutarlos y así ocultar su actividad.

Indicio

Detección de una cadena de acciones anómala de los procesos que se ejecutan en los equipos del cliente. Son secuencias de acciones poco frecuentes que se analizan en detalle para determinar si pertenecen o no a la secuencia de un ataque informático. Consulta “CKC (Cyber Kill Chain)”.

Informes avanzados

Ver Adware.

Inventario

Base de datos mantenida por con los ficheros clasificados como PII encontrados en el parque informático.

IP (Internet Protocol)

Principal protocolo de comunicación en Internet para el envío y recepción de los datagramas generados en el nivel de enlace subyacente.

J

Joke

Broma con el objetivo de hacer pensar a los usuarios que han sido afectados por un virus.

L

Llave USB

Dispositivo utilizado en equipos con volúmenes cifrados que permite almacenar la clave en una memoria portátil. De esta forma, no se requiere introducir ninguna contraseña en el proceso de inicio del equipo, aunque es necesario que el dispositivo USB que almacena la contraseña esté conectado en el equipo.

Lock

Modo de configuración de que bloquea los programas desconocidos y los ya clasificados como amenazas.

M

Machine learning

Es una rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas para capaces de generalizar comportamientos a partir de una información no estructurada suministrada en forma de ejemplos.

Malware

Término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecta a la seguridad e integridad de los sistemas informáticos. El malware se infiltra y daña un ordenador sin el conocimiento de su dueño, con finalidades muy diversas.

Malware freezer

Comportamiento del backup / cuarentena cuyo objetivo es evitar la pérdida de datos por falsos positivos. Todos los ficheros clasificados como malware o sospechosos son enviados a la zona de backup / cuarentena, evitando su borrado completo en previsión de un fallo en la clasificación que derive en pérdida de datos.

MD5 (Message-Digest Algorithm 5)

Algoritmo de reducción criptográfico que obtiene una firma (hash o digest) de 128 bits que representa de forma única una serie o cadena de entrada. El hash MD5 calculado sobre un fichero sirve para su identificación unívoca o para comprobar que no fue manipulado / cambiado.

Microsoft Filter Pack

Paquete de librerías IFilter que abarca todos los formatos de fichero generados por la suite de ofimática Microsoft Office.

Mitre corp.

Empresa sin ánimo de lucro que opera en múltiples centros de investigación y desarrollo financiados con fondos federales dedicados a abordar problemas relativos a la seguridad. Ofrecen soluciones prácticas en los ámbitos de defensa e inteligencia, aviación, sistemas civiles, seguridad nacional, judicatura, salud y ciberseguridad. Son los creadores del framework ATT&CK. Consulta >ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

MyTerm

N

Normalización

En Data Control, es una tarea que forma parte del proceso de indexación de textos, y que consiste en eliminar todos los caracteres innecesarios (generalmente caracteres separadores o delimitadores) antes de almacenarlos en la base de datos.

Nube (Cloud Computing)

Tecnología que permite ofrecer servicios a través de Internet. En este sentido, la nube es un término que se suele utilizar como una metáfora de Internet en ámbitos informáticos.

O

OU (Organizational Unit)

Forma jerárquica de clasificar y agrupar objetos almacenados en directorios.

P

Parche

Pequeños programas publicados por los proveedores de software que modifican sus programas corrigiendo fallos y añadiendo nuevas funcionalidades.

Partición de sistema

Zona del disco duro que permanece sin cifrar y que es necesaria para que el equipo complete correctamente el proceso de inicio en los equipos con activado.

Partner

Empresa que ofrece productos y servicios de Panda.

Passphrase

También llamado Enhanced PIN (PIN mejorado) o PIN extendido, es una contraseña equivalente al PIN pero que permite añadir caracteres alfanuméricos. Se aceptan letras en mayúscula y minúscula, números, espacios en blanco y símbolos.

Payload

En informática y telecomunicaciones es el conjunto de datos transmitidos útiles, que se obtienen de excluir cabeceras, información de control y otros datos que son enviados para facilitar la entrega del mensaje. En seguridad informática referida a amenazas de tipo exploit, payload es la parte del código del malware que realiza la acción maliciosa en el sistema, como borrar los

ficheros o enviar datos al exterior, frente a la parte del encargado de aprovechar una vulnerabilidad (el exploit) que permite ejecutar el payload.

PDC (Primary Domain Controller)

Es un rol adoptado por servidores en redes Microsoft de tipo Dominio, que gestiona de forma centralizada la asignación y validación de las credenciales de los usuarios para el acceso a los recursos de red. En la actualidad el Directorio Activo cumple esta función.

Perfil de configuración

Un perfil es una configuración específica de la protección o de otro aspecto del equipo administrado. Este perfil es posteriormente asignado a un grupo o grupos y aplicado a todos los equipos que lo forman.

Phishing

Intento de conseguir de forma fraudulenta información confidencial de un usuario mediante el engaño. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.

PII (Personally Identifiable Information)

Ficheros que contienen datos que pueden ser utilizados para identificar o localizar a personas concretas.

PIN (Personal Identification Number, número de identificación personal)

Secuencia de números que actúa como contraseña simple y es requerida en el inicio de un equipo que tenga un volumen cifrado. Sin el PIN la secuencia de arranque no se completa y el acceso al equipo no es posible.

Proceso comprometido

Son aquellos procesos vulnerables que han sido afectados por un exploit y pueden comprometer la seguridad del equipo de usuario.

Proceso vulnerable

Son programas que, debido a fallos de programación, no son capaces de interpretar correctamente los datos recibidos de otros procesos. Al recibir una secuencia de datos especialmente diseñada (exploit), los hackers pueden provocar un mal funcionamiento del proceso, induciendo la ejecución de código que compromete la seguridad del equipo del usuario.

Programas potencialmente no deseados (PUP)

Son programas que se introducen de forma invisible o poco clara en el equipo aprovechando la instalación de otro programa que es el que realmente el usuario desea instalar.

Protección (módulo)

Una de las dos partes que componen el software que se instala en los equipos. Contiene las tecnologías encargadas de proteger el parque informático y las herramientas de resolución para desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

Protección avanzada

Tecnología de monitorización continua y recogida de información de los procesos ejecutados en los equipos de la red para su posterior envío de a la nube de . Allí, se analiza mediante técnicas de Machine Learning en entornos Big Data para emitir una clasificación (goodware o malware) precisa.

Protocolo

Conjunto de normas y especificaciones utilizadas para el intercambio de datos entre ordenadores. Uno de los más habituales es el protocolo TCP- IP.

Proxy

Software que hace de intermediario de las comunicaciones establecidas entre dos equipos, un cliente situado en una red interna (por ejemplo, una intranet) y un servidor en una extranet o en internet.

Proxy (rol)

Equipo que hace la funciona de pasarela, conectando a otros puestos de usuario y servidores sin salida directa a Internet con la nube de Panda Adaptive Defense.

Puerto

Identificador numérico asignado a un canal de datos abierto por un proceso en un dispositivo a través del cual tienen lugar las transferencias de información (entradas / salidas) con el exterior.

Q

QR (Quick Response), código

Representación gráfica en forma de matriz de puntos que almacena de forma compacta información.

R

Reclasificación de elementos

Ver Conceptos clave.

Responsive / Adaptable (RWD, Responsive Web Design)

Conjunto de técnicas que permiten desarrollar páginas Web que se adaptan de forma automática al tamaño y resolución del dispositivo utilizado para

visualizarlas.

Rol

Configuración específica de permisos que se aplica a una o más cuentas de usuario y autoriza a ver o modificar determinados recursos de la consola.

Rootkits

Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los suyos propios). Este tipo de software es utilizado para esconder evidencias y utilidades en sistemas previamente comprometidos.

ROP

ROP es una técnica de ejecución de exploits que permite a un atacante ejecutar código arbitrario en presencia de defensas como DEP o ASLR. Los ataques tradicionales basados en desbordamiento de pila consistían en sobrescribir regiones de memoria enviando bloques de datos a la entrada de programas que no controlaban debidamente el tamaño de los datos recibidos. Estos ataques dejaron de funcionar cuando técnicas como DEP fueron implementadas de forma masiva en los sistemas operativos: en esta nueva situación el sistema operativo impide la ejecución del “código desbordado” ya que reside en regiones de memoria marcadas como de no ejecución (datos). ROP sobrescribe la pila de llamadas (call stack) de un proceso para ejecutar zonas de código del propio proceso, conocidas como “gadgets”. Así, el atacante puede "armar" un flujo de ejecución alternativo al del proceso original, formado por partes de código del proceso atacado.

S

Servicio Advanced Visualization Tool

Servicio avanzado de explotación del conocimiento generado en tiempo real por los productos y . Facilita el descubrimiento de amenazas desconocidas, ataques dirigidos y APTs, representando los datos de actividad de los procesos ejecutados por los usuarios y poniendo el énfasis en los eventos relacionados con la seguridad y la extracción de información.

Servicio Data Control

Modulo compatible con que descubre ficheros PII en la red de la empresa y monitoriza su acceso para cumplir con las regulaciones de almacenamiento de datos vigentes, tales como la GDRP.

Servicio Panda Full Encryption

Módulo compatible con que cifra el contenido de los dispositivos de almacenamiento interno del equipo. Su objetivo es minimizar la exposición de los

datos de la empresa ante la pérdida o robo, o en caso de sustitución y retirada de los dispositivos de almacenamiento sin formatear.

Servicio Panda SIEMFeeder

Modulo compatible con que envía al servidor SIEM de la empresa toda la telemetría generada por los procesos ejecutado en los equipos de usuario y servidores.

Servicio Patch Management

Módulo compatible con Panda Adaptive Defense que parchea y actualizar los programas instalados en los equipos de usuario y servidores para eliminar las vulnerabilidades producidas por fallos de programación, minimizando así su superficie de ataque.

Servidor SMTP

Servidor que utiliza el protocolo SMTP -o protocolo simple de transferencia de correo- para el intercambio de mensajes de correo electrónicos entre los equipos.

Software cliente Panda Adaptive Defense

Programa que se instala en los equipos a proteger. Se compone de dos módulos: el agente Panda y la protección.

Sospechoso

Programa con alta probabilidad de ser considerado malware y clasificado por el análisis heurístico. Este tipo de tecnología solo se utiliza en los análisis programados o bajo demanda lanzados desde el módulo de tareas, y nunca en el análisis en tiempo real. La razón de su uso es la menor capacidad detección de las tareas programadas ya que el código de los programas se analiza de forma estática, sin llegar a ejecutar el programa. Consulta Análisis heurístico.

Spyware

Programa que acompaña a otro y se instala automáticamente en un ordenador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal y utilizarla posteriormente.

SSL (Secure Sockets Layer)

Protocolo criptográfico diseñado para la transmisión segura de datos por red.

T

Táctica

En terminología ATT&CK, las tácticas representan el motivo u objetivo final de una técnica. Es el objetivo táctico del adversario: la razón para realizar una

acción. Consulta ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

Tarea

Conjunto de acciones programadas para ejecutarse con una frecuencia y en un intervalo de tiempo configurables.

TCO (Total Cost of Ownership, Coste total de Propiedad)

Estimación financiera que mide los costes directos e indirectos de un producto o sistema

TCP (Transmission Control Protocol)

Principal protocolo del nivel de transporte dentro de la pila de protocolos de Internet, orientado a la conexión para el envío y recepción de paquetes IP.

Técnica

En terminología ATT&CK, las técnicas representan la forma o la estrategia un adversario logra un objetivo táctico. Es decir, el "cómo". Por ejemplo, un adversario, para lograr el objetivo de acceder a algunas credenciales (táctica) realiza un volcado de las mismas (técnica). Consulta ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

Threat hunting

Conjunto de tecnologías y recursos humanos especializados que permiten detectar los movimientos laterales y otros indicadores tempranos de las amenazas, antes de que ejecuten acciones nocivas para la empresa.

Tiempo de exposición (dwell time)

Tiempo que una amenaza ha permanecido sin ser detectada en un equipo de la red.

TLS (Transport Layer Security)

Nueva versión del protocolo SSL 3.0.

Topología de red

Mapa físico o lógico de los nodos que conforman una red para comunicarse.

TPM (Trusted Platform Module, módulo de plataforma segura)

Es un chip que se incluye en algunas placas base de equipos de sobremesa, portátiles y servidores. Su principal objetivo es proteger la información sensible de los usuarios, almacenando claves y otra información utilizada en el proceso de autenticación. Ademas, el TPM es el responsable de detectar los cambios en la cadena de inicio del equipo, impidiendo por ejemplo el acceso a un disco duro desde un equipo distinto al que se utilizó para su cifrado.

Troyanos

Programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad de los datos del usuario.

U

Usuario (consola)

Recurso formado por un conjunto de información que Panda Adaptive Defense utiliza para regular el acceso de los administradores a la consola web y establecer las acciones que éstos podrán realizar sobre los equipos de la red.

Usuario (red)

Personal de la empresa que utiliza equipos informáticos para desarrollar su trabajo.

V

Variable de entorno

Cadena compuesta por información del entorno, como la unidad, la ruta de acceso o el nombre de archivo, asociada a un nombre simbólico que pueda utilizar Windows. La opción Sistema del Panel de control o el comando set del símbolo del sistema permiten definir variables de entorno.

VDI (Virtual Desktop Infrastructure)

Solución de virtualización de escritorio que consiste en alojar máquinas virtuales en un centro de datos al cual los usuarios acceden desde un terminal remoto con el objetivo de centralizar y simplificar la gestión y reducir los costes de mantenimiento. Se distinguen dos grupos de entornos VDI: Persistente: el espacio de almacenamiento asignado a cada usuario se respeta entre reinicios, incluyendo el software instalado, datos y actualizaciones del sistema operativo. No persistente: el espacio de almacenamiento asignado a cada usuario se elimina cuando la instancia VDI se reinicia, restaurándose a su estado inicial y deshaciendo todos los cambios efectuados.

Vector de infección

Puerta de entrada o procedimiento utilizado por el malware para infectar el equipo del usuario. Los vectores de infección más conocidos son la navegación web, el correo electrónico y los pendrives.

Ventana de oportunidad

Tiempo que transcurre desde que el primer equipo fue infectado a nivel mundial por una muestra de malware de reciente aparición hasta su estudio e incorporación a los ficheros de firmas de los antivirus para proteger a los equipos de

su infección. Durante este periodo de tiempo el malware puede infectar equipos sin que los antivirus tradicionales sean conscientes de su existencia.

Virus

Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

VPN (Virtual Private Network)

Tecnología de red que permite interconectar redes privadas (LAN) utilizando un medio público, como puede ser Internet.

W

Widget (Panel)

Panel que contiene un gráfico configurable y que representa un aspecto concreto de la seguridad de la red del cliente. El conjunto de widgets forma el dasboard o panel de control de Panda Adaptive Defense.