pandasecurity.com/business/

Threat Insights Report 2020

panda

Panda Security Threat Insights Report 2020

Nota legal

Índice:

panda

|Resumen ejecutivo

Las ciberamenazas no paran de evolucionar y proliferar. Por esto, los profesionales de seguridad de todo tipo, desde CISOs hasta MSP y otros proveedores deben mirar más allá de los enfoques de ciberseguridad reactivos y adoptar una estrategia más evolucionada. La protección más tradicional pensada para el endpoint, con una sola capa de tecnología entre el usuario y el resto del mundo, ya no es viable en sí misma.

El coste de formar a los profesionales de ciberseguridad es cada vez más alto. Es más, las amenazas que se detectan hoy en día son muy variadas y avanzadas, y se multiplican rápidamente. Por esto, los proveedores de TI y sus clientes no tienen suficiente tiempo para reaccionar y no es viable tener que depender de la gestión manual de las herramientas de ciberseguridad.

En 2020, proteger los endpoints contra las amenazas conocidas ya no es suficiente. Los entornos informáticos también deben estar protegidos contra lo desconocido. Al final, cuando se descubre una nueva ciberamenaza, siempre hay nuevos riesgos por descubrir que no han salido a la luz. . Con ese fin, es vital que los proveedores de TI cambien su estrategia de ciberseguridad. Las últimas amenazas requieren una evolución desde una ciberseguridad basada en una sola tecnología hacia las soluciones de ciberseguridad multicapa que emplean la monitorización basada en los comportamientos (entre otras funcionalidades) para eliminar las amenazas persistentes, los ataques sin fichero y otras actividades maliciosas.

Además, los endpoints interconectados de todo tipo, desde estaciones de trabajo hasta portátiles y servidores, requieren de un enfoque que incorpora las capacidades de la protección avanzada del endpoint (EPP) y la detección y respuesta en el endpoint (EDR), con una postura de seguridad de confianza cero, respaldada por la inteligencia artificial. Este es un gran cambio, pero en cambio necesario, en la forma en la que la industria de la ciberseguridad aborda el problema de las ciberamenazas enfatizando la idea del goodware — procesos conocidos, registrados y clasificados que pueden ejecutarse en el endpoint — evitando que los procesos desconocidos y maliciosos tengan la oportunidad de lanzarse. Estas tecnologías en capas proporcionan un nivel inigualable de control, visibilidad y flexibilidad; necesario en la guerra dinámica contra los atacantes desconocidos.

Los datos compilados por PandaLabs, el laboratorio de ciberseguridad de Panda Security, han arrojado luz sobre varias tendencias emergentes de ciberamenazas que requieren de una ciberseguridad sofisticada de próxima generación para combatirlas.

Hemos desarrollado nuestro 2020 Threat Insights Report sobre esta base, para guiarte y ayudarte a estar protegido contra lo que está por venir. Porque, de cara al futuro, la combinación correcta de protecciones no es la diferencia entre una solución de ciberseguridad u otra; es la diferencia entre estar protegido contra las amenazas del mañana, o convertirse en su víctima.

|Principales conculsiones

El ransomware sigue siendo persistente; un clic todavía basta para paralizar toda una red.

Los ataques sin fichero conforman una preocupación cada vez mayor: ya que son más difíciles de detectar y facilitan las actividades sigilosas de los cibercriminales.

Ahora el Threat Hunting proactivo es una solución esencial para poder reconocer los comportamientos anómalos y maliciosos que se aprovechan de aplicaciones confiables.

Las defensas de la ciberseguridad ya no se pueden basar en una única tecnología; un enfoque de seguridad en capas, combinado con una postura de seguridad de confianza cero, asegura que no haya brechas en una fuerte postura de seguridad.

Introducción

Las ciberamenazas aumentan y evolucionan. Mientras lees este informe, se están desarrollando nuevos ataques que utilizan vulnerabilidades conocidas en todos los ecosistemas, desde sistemas operativos, aplicaciones e incluso el comportamiento humano.

Los ciberdelincuentes buscan, básicamente, tres cosas:

Beneficios económicos, utilizando el ransomware para extorsionar a sus víctimas y conseguir dinero a cambio de recuperar la información secuestrada;

Datos, que se pueden vender en la Dark Web;

El **control de las infraestructuras**, las redes u otros sistemas importantes. Estos accesos se venden a entidades influyentes como naciones, grupos políticos, facciones paramilitares y demás.

El peligro de las ciberamenazas jamás ha sido tan real para las pequeñas y medianas empresas (pymes), los gobiernos locales y organizaciones. En pocos años, la mentalidad ha cambiado. Antes, estas organizaciones solían pensar"no me va a pasar a mí"; en cambioahora su actitud ha pasado a ser "es solo cuestión de tiempo". Hoy en día es innegable que existe un riesgo inherente al operar una red de equipos y hemos visto hasta dónde un incidente de seguridad puede llegar a dañar a unaorganización , llegando a causar un mal irreparable.

Por suerte, a medida que evolucionan las ciberamenazas, también lo hacen las tecnologías de ciberseguridad. Atrás quedaron los días de las aplicaciones de antivirus simples, lentas y reactivas. Las soluciones de ciberseguridad de hoy en día emplean una gama de capacidades diseñadas para mantener las redes libres de infiltraciones, detener los comportamientos maliciosos y frenar las intrusiones futuras. Pero no todas las soluciones de ciberseguridad sonson iguales. Algunas se basan en una arquitectura más antigua y no pueden adaptarse a las nuevas amenazas de manera tan ágil. Otras son reactivas, confiando en poder detectar y reaccionar a una brecha ya activa antes de que pueda actuar. Otras, simplemente no son factibles, permitiendo que sean demasiadas las amenazas que pasen desapercibidas.

En un momento en el que el mercado de la ciberseguridad está altamente competido d por la necesidad deproporcionar a los CISO, los MSP, los proveedores de servicios TI y las pymes la mejor solución para todos ellos, ¿cómo se puede encontrar la opción correcta?

Lo primero es hacer las preguntas adecuadas.

¿Por qué reaccionar ante las ciberamenazas?

¿Qué más hay que no pueda ver la solución? ¿Esta amenaza tendrá como consecuencia un futuro ataque?

¿Por qué debe ser el caso que una solución de ciberseguridad solo detecte las amenazas que han tenido éxito (es decir, las que han conseguido infiltrarse en una red)?

Está claro que las modalidades de seguridad reactivas ya no son las adecuadas, dado el contexto en el que estamos inmersos . Hay demasiadas amenazas y demasiados vectores de ataque en cualquier entorno IT, los cuales pueden causar una brecha de cualquier tipo. A día de hoy, las soluciones de ciberseguridad deben contar con capacidades predictivas, ser proactivas y estar preparadas para cualquier situación comprometida que pueda surgir. Son tanto la espada como el escudo.

Esto ha dado lugar a un modelo de tecnología estructurado en capas combinado con una postura de seguridad de confianza cero que no permite que ningún proceso desconocido se ejecute en los endpoints de la red.

Los datos en este informe demostrarán por qué las soluciones de protección en el endpoint utilizan esta metodología con éxito y por qué usarla no solo es lógico, sino que es obligatorio para estar libre de amenazas.

panda

|Metodología

Este informe se basa en los datos de telemetría y los datos de detecciones recopilados durante 2019 desde los agentes de Panda en los endpoints donde está instalada la tecnología Panda Adaptive Defense. Fueron compilados y analizados por el laboratorio de seguridad de Panda Security. PandaLabs constituye el centro neurálgico para todo lo relacionado con las ciberamenazas, y ayuda a desarrollar la tecnología de Panda.

PandaLabs mantiene un estado constante de vigilancia, siguiendo de cerca diversas tendencias y novedades en los ciberataques para formular pronósticos, tácticas y estrategias para futuras amenazas y para alertar al público sobre peligros inminentes.

Los profesionales de ciberseguridad de PandaLabs proporcionan contramedidas de manera ininterrumpida en tiempo real para proteger a los clientes de Panda Security contra todo tipo de amenazas a escala global. También llevan a cabo investigaciones forenses de las amenazas, realizando análisis detallados de todo tipo de amenazas para mejorar nuestras soluciones de seguridad y para mantener informado a la sociedad.

Datos únicos de telemetría

La tecnología de Adaptive Defense monitoriza de manera constante todas las acciones que resultan de los procesos en ejecución en los endpoints protegidos. Cada evento se cataloga en función de más de 2.000 características únicas. Estos eventos de telemetría no se consideran incidentes, objetos maliciosos ni anomalías; en su lugar, representan información relacionada con un objeto en particular, por ejemplo:

Procesos: creación de procesos, ejecución de procesos, inyección de procesos, etc.

Fichero: Cuando un proceso/evento crea un nuevo fichero, la edición de un fichero, la eliminación de un fichero, la apertura de un fichero y otras operaciones.

Comunicaciones: la apertura de una toma de comunicación, el uso de un protocolo de comunicación, la dirección y origen de ésta , etc.

Registro: La creación, edición y eliminación de claves de registro.

Administración: el uso de las credenciales de administrador , eventos de inicio/cierre de sesión, la instalación de procesos, la actividad del servicio entre muchos otros.

Estas acciones se envían a la plataforma cloud de Panda Security, donde se analizan con técnicas de Machine Learning para extraer de manera automática la inteligencia de amenaza avanzada. Esta información permite a Panda Security clasificar cada proceso que se ejecuta, con falsos positivos y falsos negativos cerca de cero.

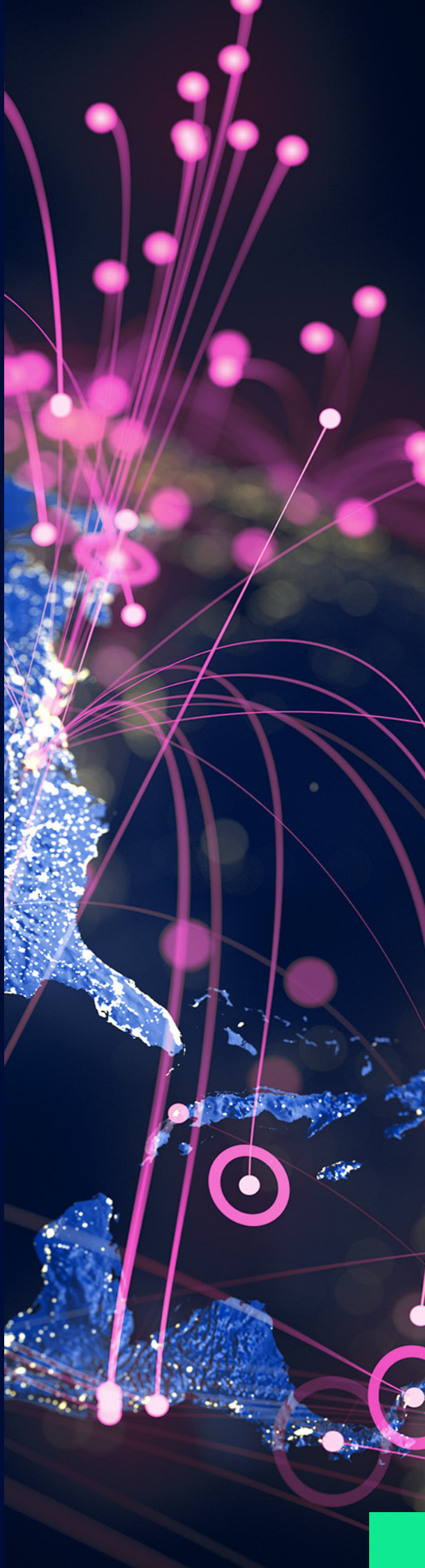
Panda está comprometido con una postura de seguridad de confianza cero y por eso, Adaptive Defense detiene prácticamente todas las amenazas basadas en malware; las que logren entrar en un endpoint, ya sea con medidas engañosas o debido a un error del usuario, no pueden ejecutarse. Esto se debe al Servicio de Clasificación del 100% de todos los procesos, que evita que se ejecuten aquellos que son desconocidos y no están clasificados.

|Resultados

No hay bolas de cristal: Los datos alimentan la inteligencia de amenazas global

Esta clasificación sumada al servicio de Threat Hunting, respaldado en lainteligencia artificial y que monitoriza los comportamientos de las aplicaciones para asegurarse de que los ataques sin fichero y otras amenazas avanzadas no puedan llevarse a cabo, son garantía de éxito a la hora de eludir ataques avanzados.

Los datos que se representan en este informe son diferentes a los de otros informes de la industria. Como líderes en el mercado de la ciberseguridad, con más de 30 años de experiencia y habiendo logrado múltiples innovaciones en el sector, Panda Security está comprometido con hacer frente a las amenazas futuras, a la vez que nos enfocamos en evitar que los endpoints sean vulnerados por cualquier amenaza actual.



panda

Percepciones basadas en los datos, no en la intuición

Datos de telemetría de Panda, 2019. Las cifras se normalizan a un millón de endpoints.

Todos los datos de telemetría recopilados en 2019:

1,2
petabytes por millón de endpoints

Detecciones de malware

70.000
alertas de malware

Ejecutables identificadas

426M
de ejecutables identificados

Aplicaciones ejecutadas

79,5M
de procesos hijo ejecutados
(procesos creados o librerías cargadas)

Archivos Dynamic Library (DLL) identificados

336M
archivos identificados

Nota: Las acciones que toman los procesos en general y la evolución de las detecciones de malware en la red, independientemente de si se han ejecutado archivos maliciosos o no, ayudan a los administradores a tomar decisiones a la hora de definir las acciones de mitigación y ajustar las políticas de seguridad.

Detección y remediación

Malware
14,9M
de eventos

Exploits
76.000
alertas

Potentially Unwanted Programs (PUP)
7,9M
de alertas

Comunicaciones

Eventos de red
1,4B
eventos

Cambios de DNS
2MM
eventos
(consultas DNS fallidas)

Descargas
1,6MM
eventos

Nota: monitorizar las conexiones de red establecidas por procesos es clave para identificar los destinos sospechosos o potencialmente peligrosos que se utilizan para lanzar ciberataques o para robar datos.

Comportamiento de entidad (archivo)

Procesos
1,7B
eventos

Operaciones de registro
735M
eventos

Scripts
1,9MM
eventos

Acceso a datos
92MM
eventos

Operaciones de dispositivos
973M
eventos

Eventos de inicio/cierre de sesión
133MM
eventos

Nota: la información detallada sobre los comportamientos de las entidades permite a los administradores a centrar su atención en las actividades sospechosas que realizan los elementos nuevos que todavía no se han identificado, y a compilar datos que pueden ser útiles para llegar a conclusiones sobre su riesgo potencial.

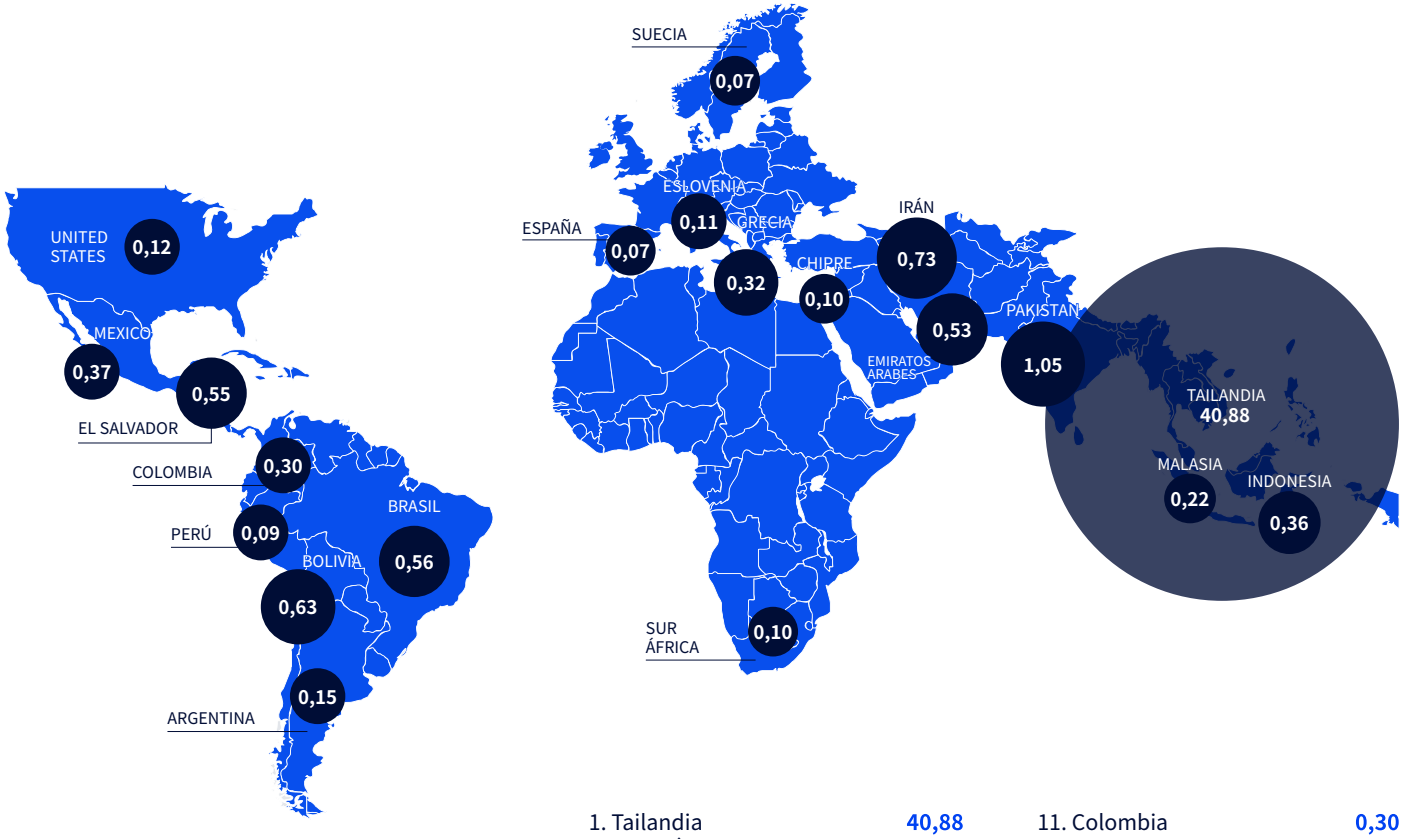
Hotspots globales: ¿Los atacantes o los atacados?

Los datos muestran que hay una clara concentración de objetivos en Oriente Medio y Sudamérica. Sin embargo, Tailandia es sin duda el líder de la tabla. Aunque este resultado puede ser de esperar, podemos decir que es un arma de doble filo. Estos países son objetivos atractivos para los ciberatacantes porque hay muchos sistemas expuestos y poco protegidos. Por este motivo, en estos países, los hackers han tenido mayor éxito.

Por otro lado, estos son ataques que fueron parados por la tecnología de Panda, lo cual nos da una idea de la frecuencia de los ataques que se llevan a cabo en una región. Podemos suponer que estos no son los objetivos finales ya que es probable que estos sistemas comprometidos sean la fuente de otros ataques, incluso más sofisticados, contra objetivos en todo el mundo.

Los principales países para ataques de malware

A ranking of countries with at least 1,000 reporting machines, based on the ratio of malware alerts (not infections) to reporting machines.



1. Tailandia	40,88	11. Colombia	0,30
2. Pakistán	1,05	12. Malasia	0,22
3. Irán	0,73	13. Argentina	0,15
4. Bolivia	0,63	14. Estados Unidos	0,12
5. Brasil	0,56	15. Eslovenia	0,11
6. El Salvador	0,55	16. Chipre	0,10
7. Emiratos Árabes Unidos	0,53	17. Sudáfrica	0,10
8. México	0,37	18. Perú	0,09
9. Indonesia	0,36	19. Suecia	0,07
10. Grecia	0,32	20. España	0,07

Los datos que se representan en este informe

Estos datos, recopilados desde los endpoints donde está instalado Panda Adaptive Defense, revelan la perseverancia de ciertas extensiones de archivo, muchas de las cuales los usuarios las ven todos los días. Y detrás de cada una de estas extensiones hay una vulnerabilidad en el diseño del archivo que puede ser explotada por los cibercriminales para llevar a cabo ataques.

El PDF, un formato de archivo muy común que se utiliza todos los días, encabeza la lista, y con mucha razón: son notorios desde hace décadas por su capacidad para llevar a cabo ataques maliciosos e inyectar código en los procesos de las aplicaciones. También se utilizan muy a menudo en las campañas de phishing en las que, si el usuario hace clic, puede desencadenar un ataque.

Eventos de acceso a datos

Ranking de las extensiones de archivo a las que se consiguió acceder en 2019 y el número de eventos de acceso únicos registrados

#	Eventos únicos	Extensión	Descripción
1	220.124.750	.pdf	Archivo Formato de Documento Portátil
2	178.096.618	.odf	OpenDocument formula (Asociado con aplicaciones de MS Office)
3	60.203.323	.job	Objeto de tarea del Programador de Tareas de Windows
4	51.313.631	.pem	Privacy Enhanced Mail Certificate (relacionado con la autenticación segura de sitios web)
5	48.607.743	.mdb	Microsoft Access Database
6	28.006.668	.xls	Hoja de cálculo de Microsoft Excel (97–2003 formato legacy)
7	25.388.869	.doc	Documento de Microsoft Word (formato legacy 97–2003)
8	17.199.902	.cer	Internet Security Certificate (relacionado con la validación de la autenticidad de los sitios web)
9	16.896.788	.pst	Archivo Personal Information Store de MS Outlook (archivo de buzón)
10	10.927.605	.p12	Archivo Personal Information Exchange (archivo que contiene un certificado digital)
11	10.576.428	.dwg	Archivo AutoCAD Drawing Database
12	9.234.914	.odt	Formato OpenDocument Text Document
13	8.403.811	.ods	Formato OpenDocument Spreadsheet
14	6.175.198	.ini	Windows Initialization File (generalmente se utilizan para cargar las configuraciones de las aplicaciones)
15	5.375.405	.ppt	Presentación de MS PowerPoint
16	5.100.168	.dat	Formato de archivo de datos genérico (generado por aplicaciones específicas)
17	4.418.416	.txt	Archivo de texto plano

Los límites de las listas blancas

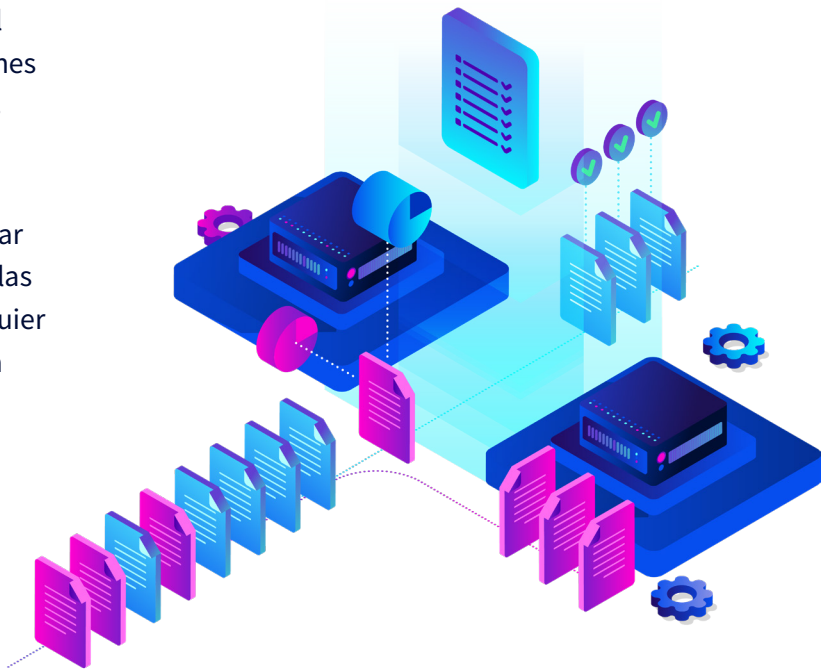
Las listas negras son prácticamente tan antiguas como la tecnología antivirus en sí, y aunque es cierto que son capaces de bloquear ciertas amenazas sencillas, sus límites son conocidos, y son fáciles de sortear. Hoy en día, con el aumento de la seguridad basada en políticas de confianza cero, muchos profesionales de ciberseguridad se consuelan al ver las aplicaciones en una lista blanca, ya que creen que significa que no tienen que preocuparse por estas aplicaciones. Por lo tanto, muchas soluciones de seguridad simplemente obvian las aplicaciones que aparecen en las listas blancas, o basan sus metodologías en estas listas, dando por supuesto que cuando se ejecutan no se utilizarán para llevar a cabo comportamientos anómalos o procesos maliciosos.

Pero esto no debe aliviarnos. De hecho, las listas blancas, al igual que las listas negras, tienen límites; y las nuevas amenazas no solo son capaces de sortear las aplicaciones de seguridad que emplean las listas blancas, sino que pueden explotar las aplicaciones en esas listas en particular. El auge de los ataques sin fichero ha hecho que la monitorización del goodware sea más esencial que nunca, ya que se aprovechan de aplicaciones conocidas y confiables para desplegar ataques y para propagarse a otras máquinas sin ser detectados. Y dado que una aplicación puede generar muchos eventos, es necesario controlar el comportamiento y las ejecuciones de todas las aplicaciones y los procesos, detectando cualquier indicio que pueda parecer ilegítimo durante la búsqueda de ataques ocultos .

Por suerte, hay una solución que va más allá de los límites de las listas blancas: la monitorización activa de todas las aplicaciones y procesos. Cuando la totalidad de la actividad del endpoint se monitoriza, el malware se identificará y jamás podrá ejecutarse, y el goodware no se podrá usar para fines ilegítimos.

Cada vez que una aplicación intenta ejecutarse, o que se carga una librería en los endpoints protegidos con Adaptive Defense, lo primero que hace Events de acceso a datos.

Esto se hace primero en el caché local y luego en el conocimiento basado en la nube (también alimenta el caché local para futuras consultas). El servicio de clasificación (Machine Learning y analistas de PandaLabs) alimenta continuamente el conocimiento basado en la nube con archivos de hash y sus clasificaciones como goodware, malware o aquel potencialmente no deseado.

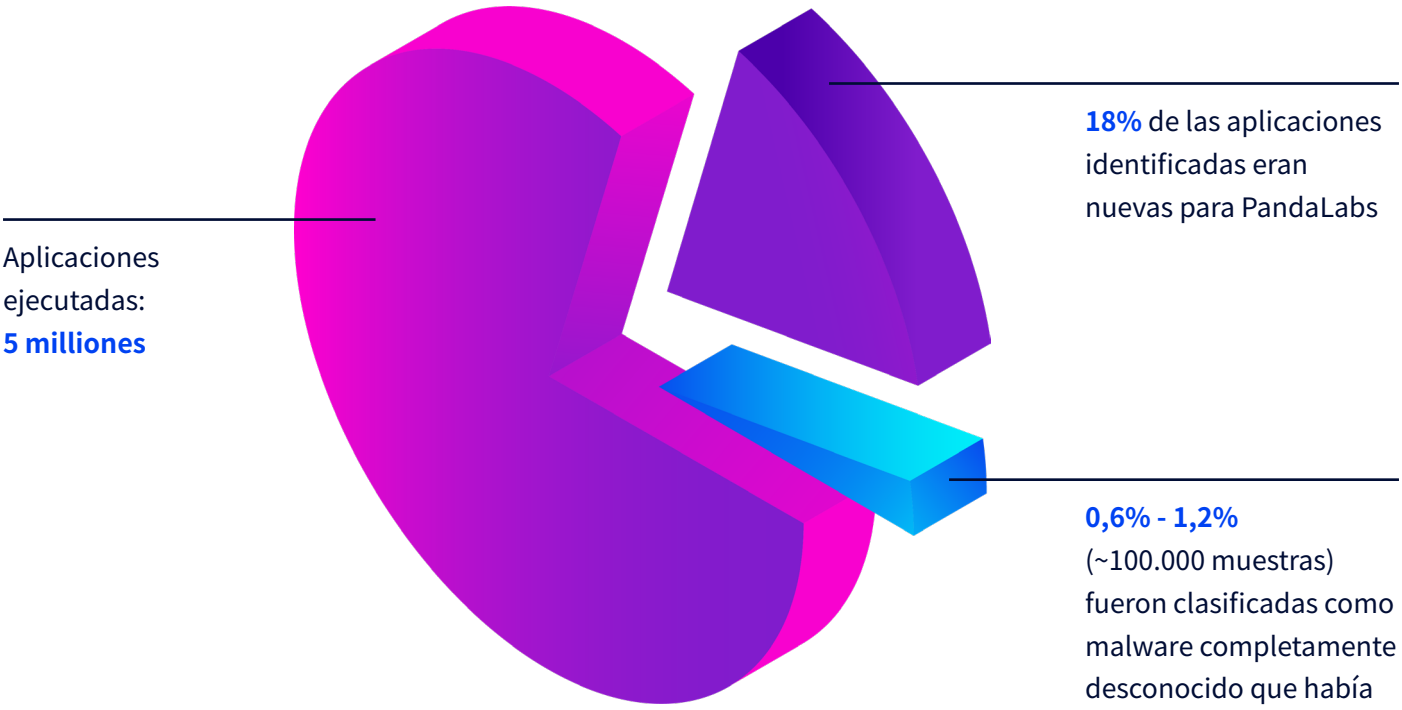


Al mismo tiempo, el Machine Learning procesa continuamente nuevas evidencias que se recopilan desde los procesos que se ejecutan en millones de endpoints protegidos. Sin embargo, como los archivos desconocidos suelen estar bloqueados hasta que se conoce su clasificación, también se ejecutan en una granja de endpoints físicos (no VM) que se almacenan en la nube. Esto permite que el sistema de Machine Learning aprenda observando su comportamiento real a lo largo del tiempo.

Estas nuevas evidencias se evalúan para clasificarlas con la máxima confianza y en el menor tiempo posible. La actividad del endpoint también se monitoriza de manera continua, en tiempo real, para todas las ejecuciones de goodware y su contexto (eventos que ocurren al ejecutarse, los usuarios que ejecutan cada comando o aplicación, el tráfico de red que se genera, los archivos de datos a los que se acceden, eventos antes y después de las operaciones, etc.). Todas estas evidencias ayudan con la identificación de los IoA (Indicadores de Ataque), sin falsos positivos.

Monitorización y ejecución de aplicaciones

Distintas aplicaciones que se ejecutan en la base instalada, mensualmente, por millón de máquinas, 2019 (aprox.)



La nueva amenaza: ataques sin archivos

Estos datos confirman la postura global sobre el hacking en vivo que explota las herramientas de productividad, navegadores y componentes que son ubicuos en la gran mayoría de los endpoints del mundo y que suelen aparecer en las listas blancas. Ninguna aplicación o ejecutable en esta lista blanca se clasificaría como sospechoso, y mucho menos como malware. Esto los convierte en los vectores ideales para desplegar los ataques sin fichero, el hacking en vivo, los ataques Living-off-the-Land (LotL) y demás.

Esta lista demuestra la necesidad apremiante de tener una tecnología anti-exploit. Hay que tener en cuenta que no hay un denominador común para explicar por qué los atacantes eligen estas aplicaciones. Por ejemplo, Microsoft IIS se explota por su habilidad de invocar a innumerables sitios web, mientras las macros de Microsoft Office facilitan la posibilidad de grabar las pantallas y los teclados. Es por esto por lo que un análisis de comportamiento basado en contextos es necesario para poder detectar estos ataques.

Por qué la seguridad en capas es importante.

Una visualización de dónde se detienen las amenazas y por qué es esencial utilizar la ciberseguridad en capas. Los datos se basan en un periodo de 30 días de los endpoints protegidos con Panda Adaptive Defense.

#	Nombre	Ejecutable	Nuevas vulnerabilidades, 2019 (CVE)	Proveedor	Tipo de Aplicación
1	**Firefox**	firefox.exe	**105**	Mozilla	Internet Browser
2	**Microsoft Outlook**	outlook.exe	**7**	Microsoft	Email Client
3	**Internet Explorer**	iexplore.exe	**53**	Microsoft	Internet Browser
4	**Microsoft Word**	winword.exe	**5**	Microsoft	Word Processor
5	**Internet Information Services (IIS) Manager**	w3wp.exe	**N/A**	Microsoft	Web Server
6	**Microsoft Excel**	excel.exe	**7**	Microsoft	Spreadsheet
7	**Adobe Reader**	acroRd32.exe	**N/A**	Adobe Systems	Proprietary File Reader
8	**Winamp**	winamp.exe	**N/A**	Nullsoft	Music Player
9	**Microsoft Access**	msaccess.exe	**N/A**	Microsoft	Database Management
10	**Google Chrome**	chrome.exe	**177**	Google	Internet Browser

Nota: N/A significa que no hay nuevas vulnerabilidades documentadas en 2019. Las vulnerabilidades más antiguas, pero más recientes o desconocidas pueden haber sido explotadas. Fuente: https://www.cvedetails.com

Una solución, múltiples capas

No todas las ciberamenazas son iguales, y cuando una tecnología detiene una amenaza, puede dejar pasar a otras. Se necesita una combinación de tecnologías locales basadas en las firmas, tecnologías basadas en la nube y el análisis de comportamiento basado en contextos para detectar y responder a las ciberamenazas en 2020.

No obstante, las cifras no cuentan toda la historia. Si bien la tecnología local basada en firmas realiza más detecciones- es porque la mayoría de los ataques son conocidos, y las firmas son económicas, no detiene las mismas amenazas de las que busca el análisis, que generalmente son más sofisticadas y potencialmente más peligrosas. Por lo tanto, aplicar múltiples capas para combatir una variedad de amenazas es el enfoque óptimo para 2020, asegurando así asegurando que todas las amenazas se detengan de la manera más eficiente posible.

Por qué la seguridad en capas es importante

Una visualización de dónde se detienen las amenazas y por qué es esencial utilizar la ciberseguridad en capas. Los datos se basan en un periodo de 30 días de los endpoints protegidos con Panda Adaptive Defense.

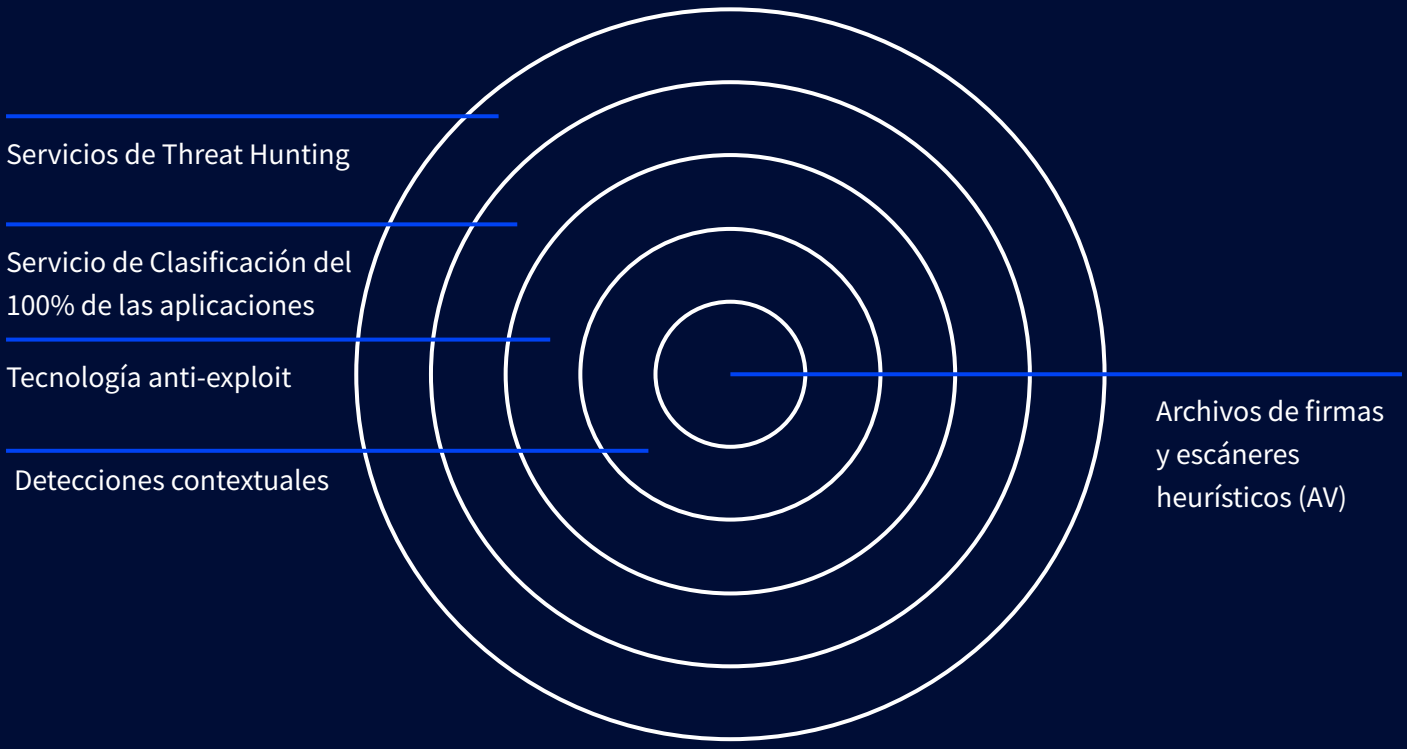
	Tecnología de detección utilizada	Descripción
Endpoints 47,648 Incidentes Detectados 598,952	Firma local	Comprueba los hashes de archivos en un caché de elementos maliciosos que se aloja localmente en el endpoint.
Endpoints 49,228 Incidentes Detectados 500,534	Detección basada en la nube	Comprueba el conocimiento basado en la nube en tiempo real para procesos maliciosos y alimenta el caché local para futuras consultas. El servicio de clasificación al 100% alimenta continuamente el conocimiento basado en la nube.
Endpoints 7,828 Incidentes Detectados 250,733	Análisis de comportamiento basado en contextos	Análisis del contexto de la ejecución para identificar los indicadores de ataque en el endpoint. Deniega la ejecución de procesos hijo y puede bloquear/eliminar procesos padre. Esta tecnología también permite bloquear los ataques que utilizan las herramientas y scripts administrativos y detecta los ataques en memoria, por ejemplo, una ejecución de un Shellcode en la memoria que no ha sido mapeado al archivo que está presente en el disco.

|Conclusión

Las ciberamenazas nunca han sido más variadas de lo que son en 2020. En un día, un endpoint puede ver una estafa de phishing con un enlace a un archivo malicioso, puede descargar un ransomware de un sitio web falsificado, ser víctima de un ataque sin archivo que se mantiene oculto en la memoria durante semanas , meses, o incluso años.

En un momento en el que el número de amenazas crece y evoluciona constantemente, los profesionales de TI deben utilizar todas las herramientas de las que disponen para mantener la seguridad de sus redes.

Panda Adaptive Defense:
La solución reconocida por el mercado y por el análisis.



Panda Adaptive Defense se compone de múltiples capas de tecnologías de ciberseguridad que trabajan simultáneamente para defender contra los ciberataques y remediarlos. Estas capas pueden agruparse en tecnologías de protección en el endpoint (EPP) y tecnologías de detección y respuesta en el endpoint (EDR).

panda

Capas de tecnología de protección en el endpoint

Archivos de firmas y escáneres heurísticos

Comúnmente conocida como tecnología antivirus tradicional (AV), esta capa ha demostrado su eficacia contra muchas amenazas comunes de bajo nivel. Es una tecnología optimizada para detectar los ataques conocidos, basada en firmas específicas, la detección genérica y heurística y el bloqueo de URL maliciosas.

+ 10.000
Eventos por día

Análisis de comportamientos

Esto se emplea para detectar el uso anormal de los recursos y las aplicaciones; esta capa es esencial para detectar los ataques sin malware y sin fichero. Es eficaz contra los ataques basados en scripts, ataques que utilizan herramientas de goodware (por ejemplo, PowerShell, WMI, etc.), vulnerabilidades en navegadores web y otras aplicaciones que comúnmente son objetivos de ataques, como Java, Adobe Reader, Adobe Flash, Microsoft Office, entre otras. La tecnología de detecciones contextuales de Panda evoluciona de manera continua, adaptándose a las nuevas amenazas gracias a la visibilidad completa proporcionada por Panda Adaptive Defense.

3 Trillions
Eventos en Data Lake

Tecnología anti-exploit

Esta tecnología detecta específicamente los ataques sin fichero que se diseñan para explotar las vulnerabilidades. Complementa la tecnología de detección contextual de Panda al buscar y detectar los comportamientos anómalos, una indicación segura de que un proceso ha sido explotado. Esta tecnología es importante en todos los endpoints, pero es crucial en los endpoints no parcheados y los que están a la espera de estarlo, además de los endpoints que tienen sistemas operativos que ya no son soportados.

2 Millions
Nuevos binarios clasificados cada semana

panda

Protección en el endpoint de próxima generación

100% Servicio de clasificación 100%

TLas soluciones EDR tradicionales identifican el malware, pero nada más. Esto supone un riesgo. Con nuestro servicio de clasificación al 100%, Panda Adaptive Defense monitoriza no solo todas las aplicaciones, sino también todos los procesos en ejecución en el sistema. Con esta tecnología EDR madura (con más de cinco años en funcionamiento), no hay elementos sospechosos que investigar; solo permite la ejecución de aquellos procesos que son conocidos para Panda y que han sido clasificados previamente como confiables. Este servicio gestionado único es un componente central de Adaptive Defense y proporciona la máxima protección sin tener que delegar las decisiones importantes de ciberseguridad a los usuarios finales. Además, este servicio proporciona una protección superior en caso de que una capa anterior falle al detener los ataques en los ordenadores ya infectados y los ataques que emplean los movimientos laterales dentro de una red. Su enfoque basado en la IA garantiza que el 99,98% de las aplicaciones se clasifiquen automáticamente, mientras que los expertos del laboratorio de Panda revisan el 0,02% restante. Es la única tecnología de este tipo disponible hoy en el mercado.

Servicio de Threat Hunting & Investigación

El Servicio de Threat Hunting & Investigación (THIS) es el único de su tipo que se incluye de manera estándar en una solución EDR. Es un servicio avanzado y proactivo que detecta máquinas que han sido comprometidas, ataques en etapas tempranas y actividades sospechosas. Cuando todo lo demás falla para detener los ataques extremadamente sofisticados, que pueden pasar desapercibidos durante meses, el Threat Hunting puede erradicarlos con un conjunto de procedimientos proactivos. Gestionado por los expertos del Equipo de Ciberseguridad Global de Panda, Threat Hunting Investigation Service puede descubrir incluso el más pequeño rastro que dejan los hackers cuando intentan tomar el control de los endpoints a través de técnicas Living-off-the-Land (LotL).

El futuro de ciberseguridad no radica en un único método de protección, sino en una combinación de capas eficaces y probadas de tecnología de seguridad y soluciones avanzadas. Este enfoque es la forma más eficiente y efectiva de proteger los endpoints contra las amenazas conocidas y desconocidas de manera proactiva. Y, a medida que las amenazas se vuelven cada vez más complejas a lo largo de 2020, los distintos proveedores de TI necesitan una solución de ciberseguridad que siempre está un paso por delante de los hackers.

panda

Live demo

Contacta con nosotros

Más información
pandasecurity.com/business

Hablemos
comunication@pandasecurity.com

panda