



TRUST IN
GERMAN
SICHERHEIT



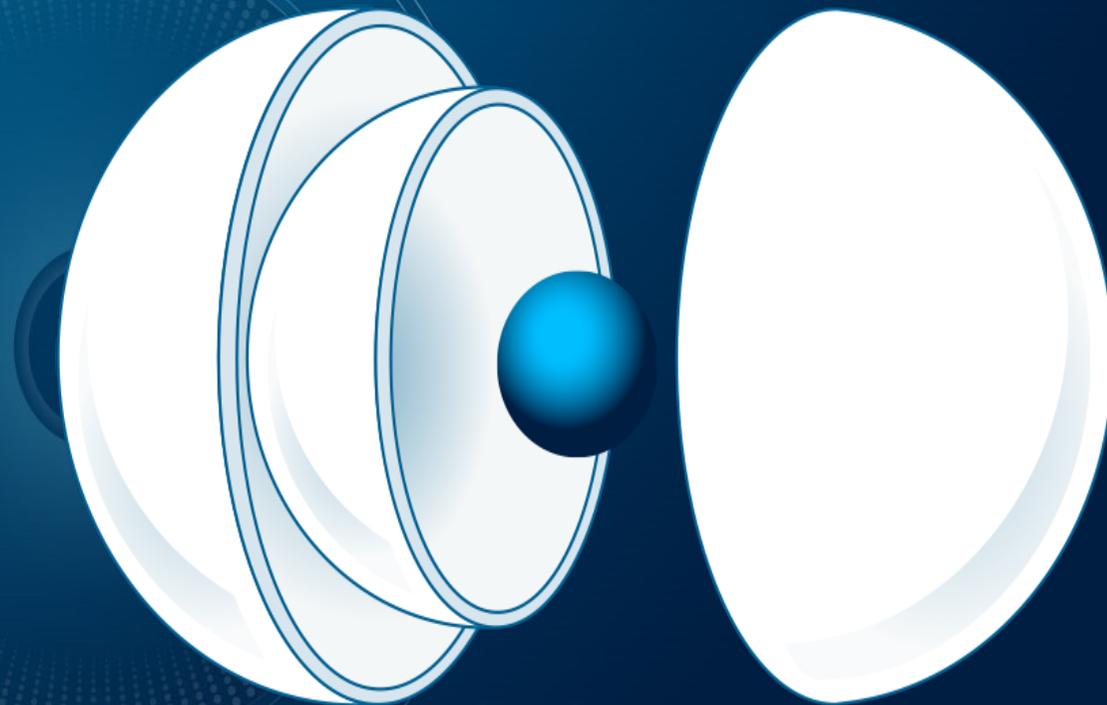
G DATA - DeepRay®

Cambiamos las reglas del juego.

Nuestra innovadora tecnología G DATA DeepRay utiliza la Inteligencia Artificial y el Machine Learning para protegerle de las tácticas más sofisticadas del cibercrimen.

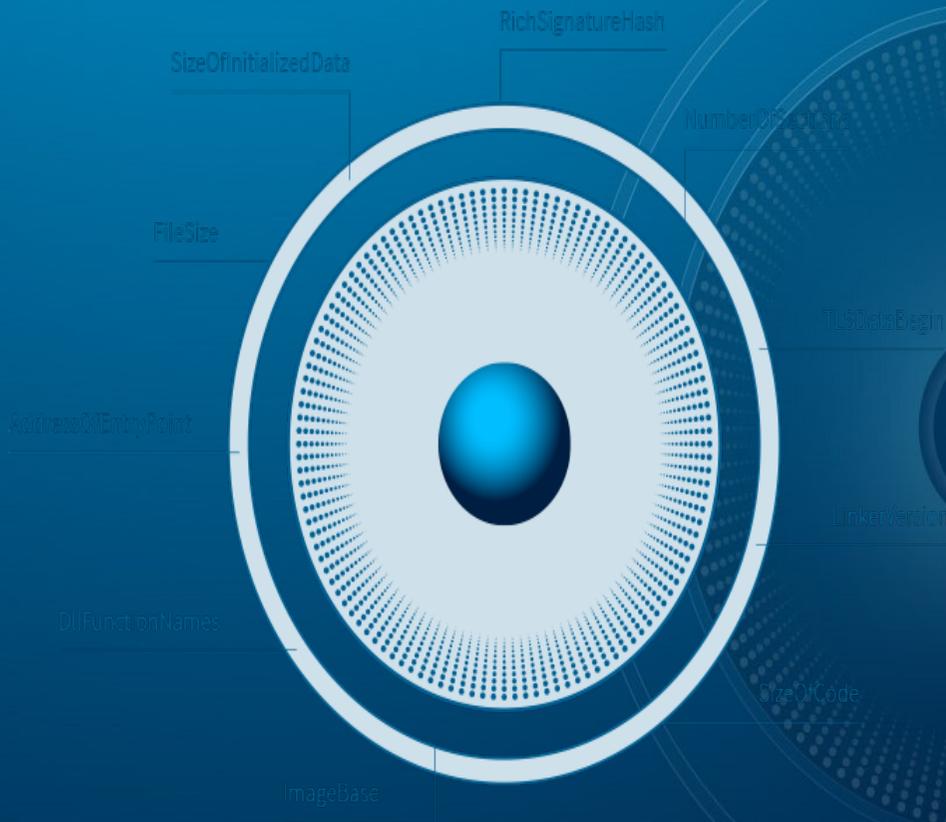
La ofuscación del malware, clave de su éxito.

El mismo contenido, pero con un envoltorio diferente. Una estrategia sencilla que ha facilitado el crecimiento exponencial del cibercrimen en los últimos años. Los hackers camuflan sus amenazas con los llamados 'packers' y ofuscadores de software. Una vez que el malware se convierte en una amenaza conocida, sus creadores solo tienen que 'reempaquetarlo' y liberarlo en una nueva oleada de ciberataques (malware ofuscado). Y repetir el proceso tantas veces como quieran. Es una forma rápida, sencilla y muy rentable de seguir difundiendo código malicioso.



Jugando al escondite: Game Over

Gracias a la nueva tecnología DeepRay, basada en el Machine Learning y la Inteligencia Artificial, estamos destruyendo uno de los cimientos que sostienen el lucrativo negocio del cibercrimen: el malware ofuscado. Ya no basta con transformar un malware conocido en un ciberataque nuevo usando técnicas de ofuscación de software al alcance de cualquiera. Los cibercriminales tendrán ahora que reescribir el código malicioso por completo, multiplicando los esfuerzos, los recursos y los tiempos empleados para ello.



G DATA DeepRay, Inteligencia Artificial al servicio de la ciberseguridad.

G DATA utiliza una red neuronal compuesta por varios perceptrones capaces de identificar y analizar procesos sospechosos. Esta red trabaja con un algoritmo en continuo proceso de mejora gracias al aprendizaje adaptativo y la propia experiencia de nuestros analistas. Así por ejemplo, los archivos ejecutables se categorizan usando una variedad de indicadores, entre ellos la relación entre el tamaño del archivo y el código ejecutable, la versión del compilador y el número de funciones del sistema importadas.

Si DeepRay marca un archivo como sospechoso, se realiza un análisis profundo en la memoria del proceso correspondiente. Esto implica la identificación de patrones asociados con familias de malware conocidas o con un amplio abanico de comportamientos maliciosos. Gracias a DeepRay, nuestras soluciones de seguridad detectan con eficacia los archivos maliciosos ocultos y, tan importante como esto, a una velocidad muy superior a la que ofrecen las soluciones habituales. Así evitamos los daños causados por el malware desconocido incluso en las fases más tempranas de la infección.



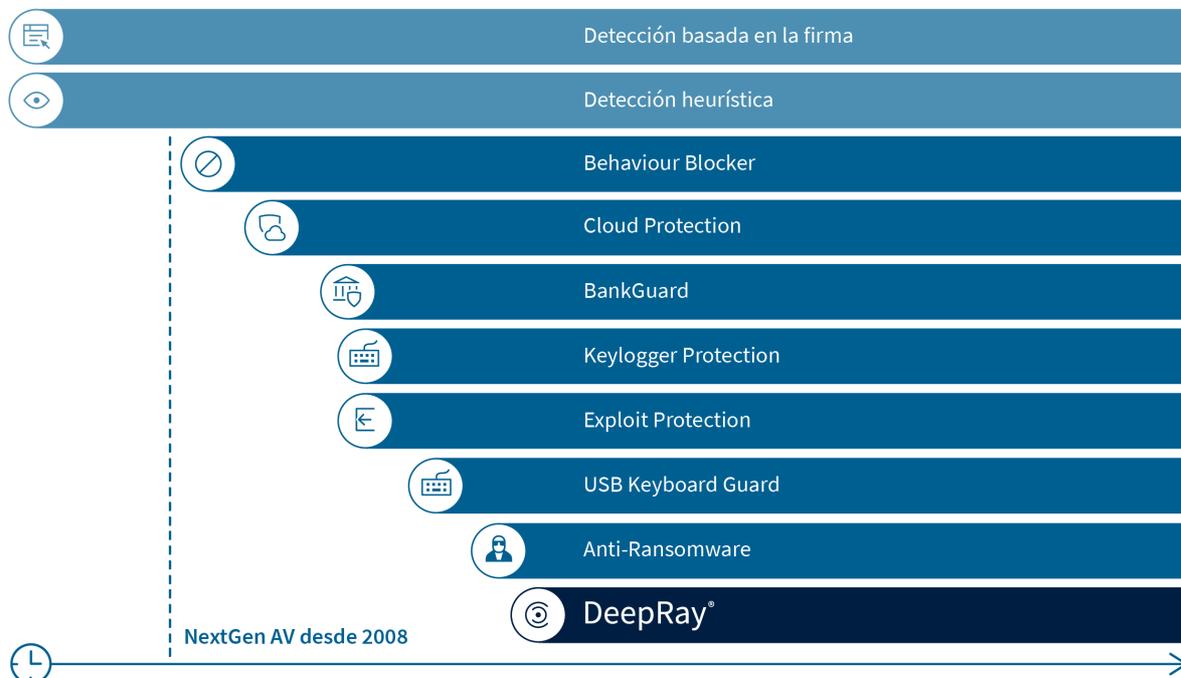
Contents

La seguridad informática utiliza inteligencia artificial y aprendizaje automático.....	3
¿Cómo se distribuye el malware a los endpoints?.....	3
El malware utiliza la táctica de la ofuscación.....	4
DeepRay® cambia las reglas del juego.....	4
¿Cómo funciona DeepRay®?.....	5
Defensa rápida contra todo tipo de amenaza	5
Nivel de protección óptimo desde el primer momento	6

La seguridad informática utiliza inteligencia artificial y aprendizaje automático

Los ciberdelincuentes y los proveedores de soluciones de seguridad informática siempre se han enfrentado a una carrera contra el tiempo. Los ataques con las tácticas conocidas se pueden frustrar más rápido y fácilmente que los ataques con nuevo malware. Por eso los ciberdelincuentes no dejan de idear nuevos métodos para sortear la protección de las soluciones de seguridad. Los enfoques tradicionales como las tecnologías de detección basada en la firma solo pueden reaccionar a los ataques.

Desde 2008, nuestra oferta también incluye tecnologías de última generación capaces de bloquear inmediatamente amenazas nuevas o modificadas. DeepRay® protege a los usuarios de las sofisticadas tácticas de los ciberdelincuentes. Las innovaciones tecnológicas con inteligencia artificial, aprendizaje automático y redes neuronales nos ayudan a hacer frente a la situación de amenaza.



¿Cómo se distribuye el malware a los endpoints?

Los desarrolladores de malware operan en un mercado que se rige por una lógica de negocio tradicional. Crear malware es muy costoso, por lo que la inversión tiene que amortizarse con un beneficio proporcional. Para lograr este beneficio, es necesario que el malware infecte la mayor cantidad posible de endpoints. Pero una vez que se identifica el malware, los programas antivirus son capaces de detectarlo y ya no puede provocar más daños. Por lo tanto, el malware deja de ser rentable.

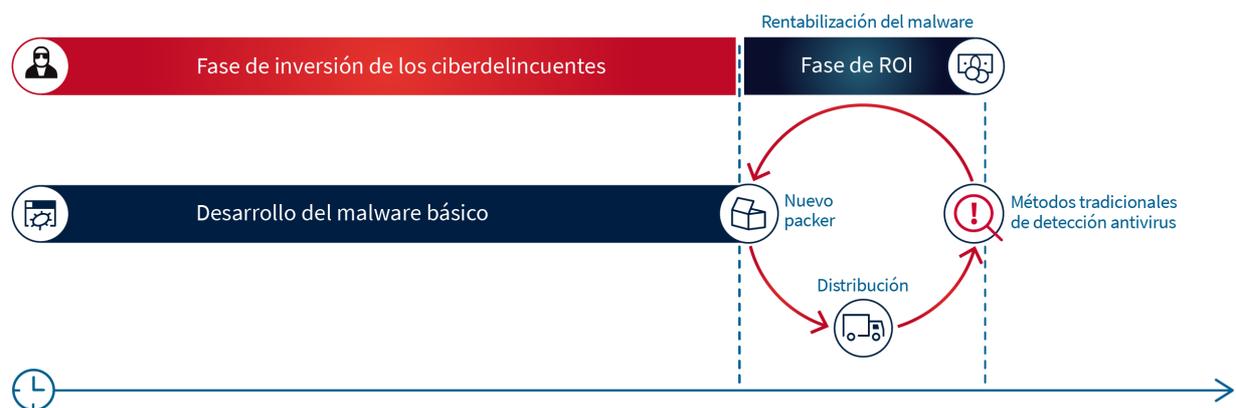
Para evitar tener que crear un nuevo malware una y otra vez, con los costes que ello supone, los desarrolladores optan por camuflar el malware en su lugar. Camuflarlo es mucho más sencillo y barato, por lo que también resulta más eficiente que programar un nuevo malware. Los

programadores de malware a menudo no se encargan ellos mismos de ocultarlo o distribuirlo, sino que se lo venden a diferentes hackers. Estos hackers se encargan de empaquetar y distribuir los nuevos paquetes a usuarios desprevenidos utilizando distintos métodos. En ese caso, el programador recibe una parte del dinero del rescate que se exige con el ransomware. Este modelo de negocio “Ransomware as a service” es el que utiliza, por ejemplo, el software malicioso “Gandcrab” tan extendido actualmente. Sabemos por los foros especializados que el programador y sus clientes se reparten un porcentaje del 60 y el 40 por ciento de las ganancias.

El malware utiliza la táctica de la ofuscación

El número de packers ya es incalculable y, sin embargo, sigue creciendo constantemente. Cada uno de estos packers se puede modificar de manera rápida y sencilla. Con ello se pretende burlar y sortear a los antivirus. Este es el principal obstáculo para la detección tradicional de malware.

En algunos casos, los packers también se utilizan en varias capas. Pero el software malicioso como núcleo del archivo ejecutable no cambia. Esta es la forma más rentable de alargar la vida del malware y sacar el máximo beneficio posible.

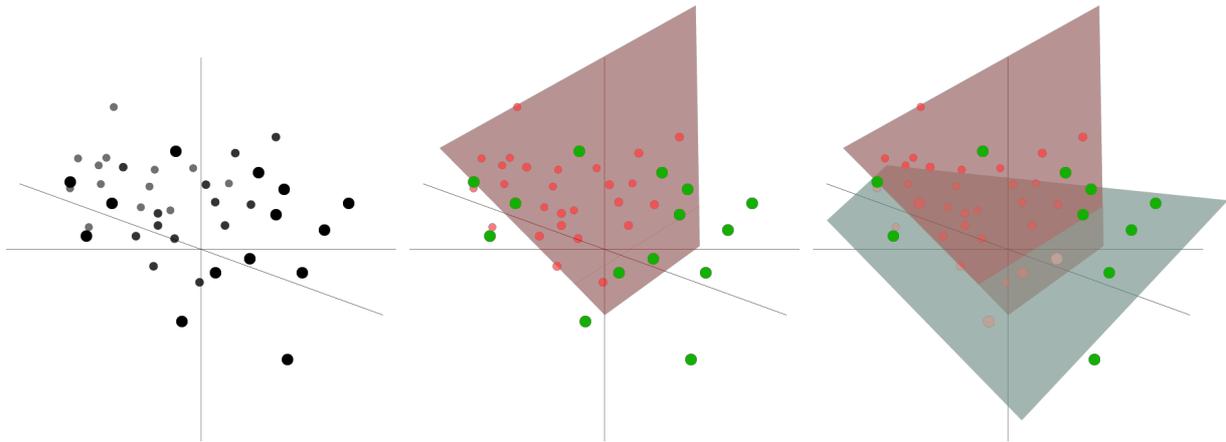


DeepRay® cambia las reglas del juego

Con DeepRay® hemos desarrollado una tecnología de aprendizaje automático cuyas capacidades proporcionan a G DATA una ventaja competitiva decisiva frente a los ciberdelincuentes. Una vez que se ejecuta el malware ofuscado con un packer, el contenido original se desempaqueta de nuevo en la memoria. Dada la dificultad de analizar y evaluar constantemente el contenido de todos los procesos, hemos adoptado un enfoque diferente. La tecnología de autoaprendizaje que hemos desarrollado es capaz de detectar si un archivo está camuflado o no. Gracias a ella, no importa qué método de ofuscación o qué packer se utiliza, ni si el método es conocido. Ya no basta con cambiar la técnica de ofuscación para burlar a DeepRay®. Ahora, los ciberdelincuentes se verán obligados a reescribir el código malicioso por completo.

¿Cómo funciona DeepRay®?

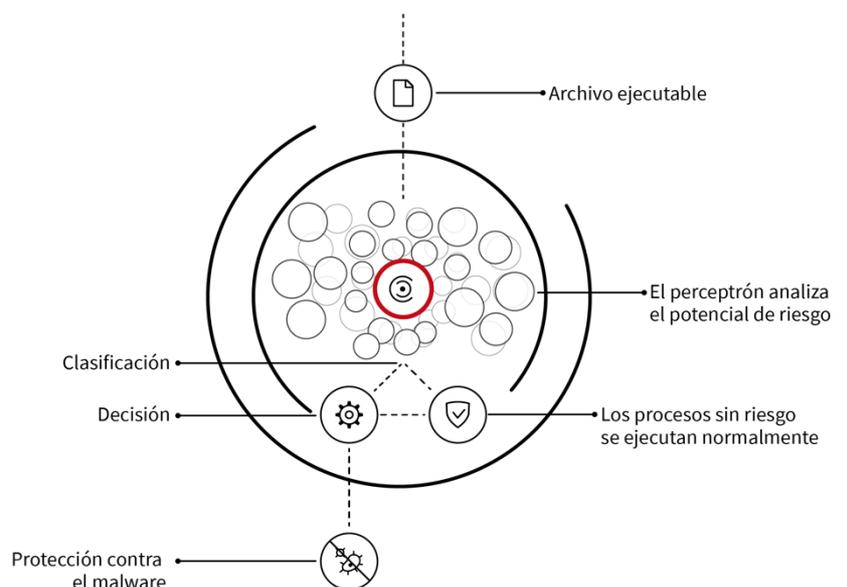
Para la detección inicial, G DATA utiliza una red neuronal compuesta por varios perceptrones. Basándose en varios cientos de criterios, esta red determina si un archivo se ha ocultado de forma sospechosa incluso antes de que se desempaquete el malware y revele su código original. Algunos de estos criterios son el tamaño del archivo general y de su código ejecutable, la versión del entorno de programación utilizado y el número de funciones del sistema importadas.



Como se muestra en el gráfico, los perceptrones dividen un espacio de características –en el caso de DeepRay® en empaquetado o no empaquetado, esto es, en peligroso o seguro. En realidad, para ello se utilizan muchos más planos que los dos planos mostrados en tres dimensiones. Cada uno de los cientos de criterios corresponde a un plano, de modo que la línea divisoria de cada perceptrón pasa por cientos de planos. Este gran número de planos también es necesario para trazar una línea divisoria fiable. El perceptrón aprende el recorrido óptimo por medio de un conjunto de entrenamiento previamente clasificado. Los conjuntos se actualizan continuamente para obtener el mejor resultado de entrenamiento. En DeepRay® se conectan varios perceptrones a una red neuronal para que el proceso sea lo más preciso posible.

Defensa rápida contra todo tipo de amenaza

Si la red neuronal de DeepRay® decide que un archivo es sospechoso, se realiza un análisis profundo en la memoria del proceso correspondiente y se buscan otros procesos cuya seguridad pueda verse afectada. La identificación de estos procesos es importante, ya que el malware a menudo intenta reubicar el comportamiento malicioso en procesos del sistema aparentemente no peligrosos.



Este método de detección se denomina “Taint Tracking”. Para descubrir los posibles riesgos de seguridad, se monitorean las funciones del sistema que permiten el acceso de un proceso a otro. En el caso de que se registre un acceso, el proceso en cuestión también se considerará en peligro o marcado (“tainted” en inglés). Esta marca o “taint” se puede propagar a otros procesos de cualquier nivel, que también se someten a análisis. De este manera es posible detectar incluso “fileless malware” (malware sin archivo) que no está almacenado en el sistema de archivos.

Este análisis profundo implica la identificación de patrones asociados con familias de malware conocidas o con un amplio abanico de comportamientos maliciosos.

Nivel de protección óptimo desde el primer momento

Con el fin de alcanzar un nivel de protección óptimo de forma inmediata, hemos entrenado la red neuronal con información recopilada a lo largo de más de 30 años de experiencia en la detección de malware. Mediante el análisis de nuevas amenazas y la información del G DATA SecurityLabs, el rendimiento aumenta continuamente y DeepRay® se mantiene siempre actualizado.

Además, cada detección exitosa del componente total se utiliza para mejorar la red neuronal, lo que a su vez resulta en un proceso de aprendizaje adaptativo del sistema de IA.

Los archivos seguros se ejecutan con normalidad para que los usuarios disfruten del máximo rendimiento en su dispositivo.

DeepRay® es la novedad más reciente de las soluciones de seguridad de G DATA que detecta de forma proactiva las amenazas y evita daños para el usuario.

