Machine Learning
Informe técnico

Resumen

En el panorama actual de la seguridad informática, los autores de las amenazas investigan y cambian constantemente de tácticas, lo que hace que las empresas sean más susceptibles de sufrir incidentes y brotes de malware, trastornos en sus negocios y vulneraciones de datos. La plataforma Bitdefender GravityZone Endpoint Security protege sus endpoints ante todo tipo de ataques informáticos sofisticados con gran eficacia, escaso impacto en el usuario final y baja carga administrativa. Consiste en una serie de capas de protección que levantan obstáculos ante los malhechores para que tropiecen con ellos. Cada una de estas capas está diseñada para frenar tipos concretos de amenazas, herramientas o técnicas y cubren diversas etapas de los ataques.

Bitdefender aprovecha el aprendizaje automático en toda su cartera. Los motores de análisis, HyperDetect, Sandbox Analyzer, el Control de contenido o la red de protección global son solo algunos ejemplos de las tecnologías de Bitdefender que hacen uso del Machine Learning. Este documento se centra principalmente en la detección de amenazas basada en el Machine Learning (motor de análisis). La detección de amenazas basada en el Machine Learning de Bitdefender forma parte de la plataforma GravityZone Endpoint Security. Proporciona protección contra amenazas de día cero en la etapa previa a su ejecución.

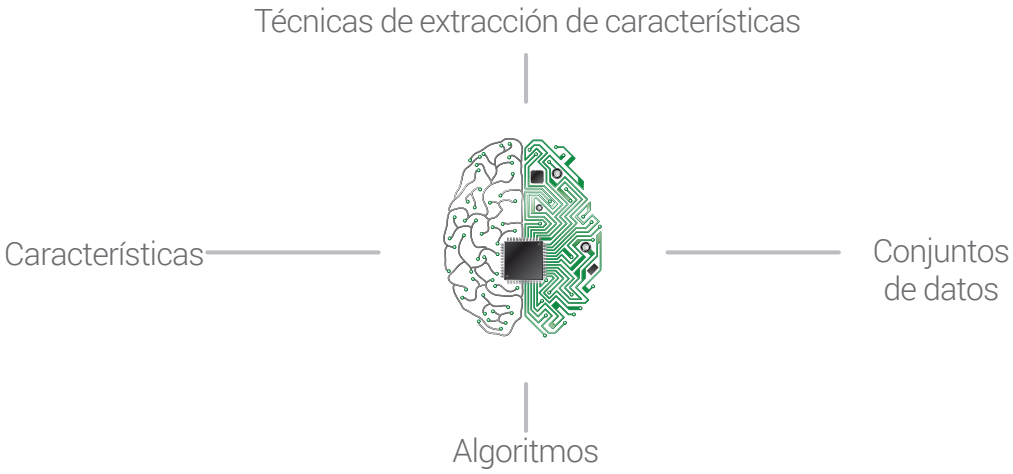
Etapa de detección	Tipo de tecnología	Cobertura de amenazas
Preejecución	Machine Learning	Malware basado en archivos, troyanos, ladrones de contraseñas, exploits, malware ofuscado, ataques selectivos, ataques basados en scripts, malware mutado y polimórfico, ransomware

Comprender la importancia de la tecnología de Machine Learning

El Machine Learning es la capacidad de los programas informáticos para analizar grandes volúmenes de datos, extraer información automáticamente y aprender de ella. En seguridad informática, puede desempeñar un papel importante porque es capaz de predecir las intenciones maliciosas de un objeto (por ejemplo, un archivo o una URL) sin ningún conocimiento previo del objeto. La tecnología de Machine Learning patentada de Bitdefender utiliza algoritmos bien entrenados, algunos de ellos especializados en formas específicas de ataques y otros más genéricos, para predecir, detectar y bloquear amenazas de día cero.

Ingredientes clave de la tecnología de Machine Learning de Bitdefender:

- **Características**: Una característica de Machine Learning es una propiedad medible individual de un fenómeno en observación. Bitdefender extrae tanto características estáticas como dinámicas de archivos y URL. La profunda comprensión de Bitdefender del comportamiento del malware le permite identificar el conjunto correcto de características.
- **Técnicas de extracción de características**: Bitdefender utiliza un emulador especialmente diseñado que desempaqueta y revela técnicas para extraer características estáticas y dinámicas de archivos y URL.
- **Algoritmos de Machine Learning**: Un algoritmo de Machine Learning es un programa que obtiene información a partir de los datos. Bitdefender aprovecha varios algoritmos, los cuales poseen funciones superpuestas que los hacen más resistentes a los ataques avanzados. También incluye algoritmos personalizados de Machine Learning para mejorar la precisión de la detección.
- **Conjuntos de datos**: En el Machine Learning, los conjuntos de datos son muy importantes para el entrenamiento y el ensayo de los modelos de Machine Learning. Bitdefender posee una de las mayores bases de datos del sector con muestras de archivos limpios y maliciosos con los que entrenar y probar los modelos de Machine Learning, lo que mejora drásticamente la eficacia y la precisión de la detección.



Características

- Modelos locales y en la nube de Machine Learning para la detección de archivos maliciosos y URL.
- Diversos algoritmos de Machine Learning con más de 75 000 modelos, que incluyen perceptrones, árboles de decisión binarios, máquinas de Boltzmann restringidas, algoritmos genéticos, máquinas de vectores de soporte, redes neuronales artificiales, algoritmos personalizados para la mitigación de falsos positivos y más de 40 000 características estáticas y dinámicas.

He aquí algunos ejemplos de características que Bitdefender extrae de un archivo:

- El código de desempaquetado contiene cadenas que pueden indicar persistencia en el sistema.
- El archivo está empaquetado con un empaquetador desconocido.
- El archivo está ofuscado (empaquetador desconocido o compilador desconocido).
- Usa anormal de diferentes instrucciones de ensamblaje (cómo por ejemplo call, jump, etc.)
- Varias técnicas de extracción de características: **Emulador**: Emula el código (instrucciones de ensamblaje), mira qué hace y su intención y extrae las características; **Rutina de desempaquetado**: Rutina de desempaquetado diseñada específicamente que puede extraer características dinámicas tales como cadenas, código, scripts HTML inyectados, URL, etc.; **Filtros criptográficos**: Aplica filtros criptográficos para extraer características de datos cifrados.
- Completos conjuntos de datos para entrenar y probar modelos de Machine Learning: muestras nuevas, malware diverso, malware representativo y Machine Learning sin supervisión en la nube.

Beneficios

- Detecta anticipadamente ataques avanzados y evita vulneraciones, además de reducir el coste y el esfuerzo de respuesta ante incidentes.
- Reduce la carga que supone la persecución de amenazas.
- El Machine Learning aumenta en gran medida la tasa de detección de amenazas de día cero en la etapa previa a su ejecución, incluido malware basado en archivos, troyanos, ladrones de contraseñas, exploits, malware ofuscado, ataques selectivos, ataques basados en scripts, malware mutado y polimórfico y ransomware.
- El modelo de Machine Learning local asegura la protección de dispositivos desconectados.
- Forma parte de un único agente de seguridad de endpoint integrado y de una plataforma de administración centralizada, lo que reduce en gran medida la carga administrativa. Los clientes no necesitan implementar una combinación de soluciones de seguridad de endpoints.

Bitdefender

Bitdefender es una empresa global de tecnologías de seguridad que ofrece soluciones completas y de vanguardia para la seguridad informática y protección contra amenazas avanzadas a más de 500 millones de usuarios en más de 150 países. Desde 2001, Bitdefender ha desarrollado sistemáticamente tecnologías galardonadas de seguridad, destinadas a usuarios domésticos y empresariales, proporcionando soluciones de seguridad tanto para las infraestructuras híbridas de datacenter, como de protección para los endpoints. Con el apoyo de su I+D, y su red de alianzas y colaboraciones, Bitdefender disfruta del prestigio de ir en la vanguardia de la seguridad y ofrecer una gama de soluciones sólidas y de total confianza. Para obtener más información visite http://www.bitdefender.es

BD-NGZ-Jan 30 2018-1t-#
Bitdefender-2017-TechnicalBrief-MachineLearning-creat2103-A4-es_ES