TRUST IN GERMAN SICHERHEIT

BEAST

Superando los límites de la detección tradicional de malware.

G DATA CyberDefense AG | September 2019

Detectar malware sofisticado en el mundo real se ha convertido en una tarea desafiante cuando se depende únicamente de detecciones basadas en firmas tradicionales.

Límite número 1: detección retrospectiva

En primer lugar, la detección basada en firmas es, por definición, un método reactivo. Independientemente del nivel de automatización involucrado: solo después de que un archivo sea categorizado como malicioso, se puede escribir una firma para ese archivo o un grupo de archivos relacionados (normalmente, una familia de malware).

Hoy en día, los autores de malware rompen este enfoque reactivo al aumentar en gran medida la frecuencia con la que lanzan malware que es percibido como nuevo.

Límite número 2: singularidad del malware.

El cibercrimen se ha convertido en una industria multimillonaria. Al igual que las empresas tradicionales, los cibercriminales aumentan su eficiencia utilizando herramientas de automatización. Algunos autores de malware utilizan servicios de automatización para monitorear activamente si las soluciones anti-malware detectan su malware. Una vez que se registra una detección, eliminan inmediatamente el patrón identificado de sus muestras o modifican automáticamente sus programas para evitar la detección.

Aplican ampliamente la encriptación y los empacadores en sus muestras para ocultar su núcleo malicioso. Algunos autores de malware lanzan una nueva muestra de malware cada pocos minutos. Otros incluso generan una muestra individual para cada víctima ("polimorfismo en el lado del servidor").

Efectivamente, cuando los archivos maliciosos son tan únicos, resulta difícil encontrar patrones maliciosos que puedan ser utilizados para generar una firma tradicional que pueda identificar toda una familia de malware. Incluso si existen patrones que se puedan utilizar para crear una firma, este esfuerzo puede resultar prácticamente inútil.

Límite número 3: evasión del análisis en el backend.

Otro problema es que la identificación de archivos maliciosos a menudo depende del análisis en el backend de los proveedores de seguridad. Cada muestra potencialmente maliciosa que los proveedores obtienen es analizada exhaustivamente, por ejemplo, en sistemas de pruebas aisladas (sandbox) que ejecutan las muestras y tratan de identificar cualquier acción maliciosa. Solo si las muestras son identificadas como maliciosas, se inicia un proceso para encontrar patrones maliciosos. Desafortunadamente, las muestras de malware a menudo están diseñadas para ser conscientes de su entorno y detectar si están siendo analizadas. Pueden exponer su comportamiento malicioso solo si se encuentran en un ambiente que consideran seguro.

comportamiento en un momento específico, en una ubicación específica, después de ejecutarse durante cierta cantidad de tiempo o después de reconocer interacción del usuario que normalmente no está presente en un sistema de pruebas aisladas (sandbox). Debido a estos problemas, además de los métodos de detección tradicionales, también necesitamos poder detectar el comportamiento malicioso donde ocurre: en el sistema afectado.

La solución: análisis de comportamiento.

Por lo tanto, los proveedores de seguridad han implementado tecnologías de detección que analizan el comportamiento de los procesos en un sistema para determinar si es malicioso o benigno. Con el fin de ser eficientes con el hardware, dicho análisis se enfoca especialmente en partes sospechosas del sistema, como el sistema de archivos, el registro o la carpeta de inicio automático. Esto permite a los proveedores de seguridad detectar familias de malware completamente desconocidas.

La mayoría de estas soluciones intentan traducir el comportamiento amenazante en valores para determinar un grado de "maldad". Matemáticamente, no es posible evitar una pérdida de precisión cuando muchos de estos valores se agregan en un puntaje total. Incluso con el aprendizaje automático, aún existe un nivel de incertidumbre en este método que conduce a un cierto nivel de error en la clasificación de un proceso como malicioso o benigno.

La mayoría de los consumidores no se verán afectados por esto. Sin embargo, las empresas a menudo utilizan herramientas de software altamente especializadas y utilizan procesos de manera intencionada e inofensiva, lo cual es inusual en la mayoría de los otros entornos. Si el umbral de una herramienta de análisis de comportamiento se establece demasiado alto, bloqueará esos procesos; si es demasiado bajo, el malware podría no ser detectado. En el mundo real, los proveedores de seguridad tienden a evitar errores de detección al solicitar a los usuarios que autoricen los procesos que ocurren. Cuando esto ocurre con demasiada frecuencia, los usuarios suelen desactivar la tecnología o ignorar las advertencias. De cualquier manera, el riesgo de infecciones aumentará.

La solución real: BEAST

BEAST es una tecnología de detección basada en el comportamiento, desarrollada por G DATA, que monitorea el comportamiento y registra cada acción observada en una base de datos gráfica local y ligera. BEAST no se basa en la identificación del malware en sí, sino en la observación de comportamientos maliciosos genéricos. Esto es especialmente útil contra malware raro y familias de malware.

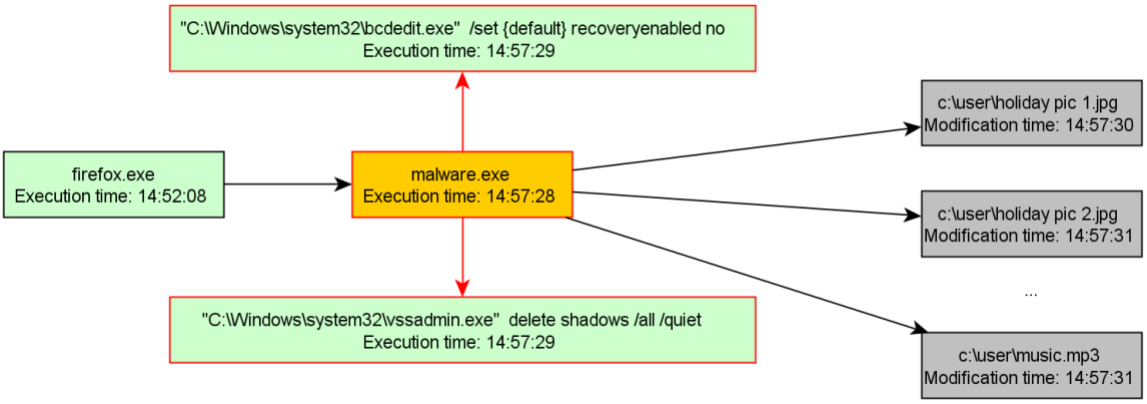
En lugar de depender de patrones específicos de malware, BEAST analiza el comportamiento de los procesos y programas en el sistema para identificar acciones que se asemejen a patrones maliciosos conocidos. Al almacenar y comparar estos comportamientos en su base de datos, BEAST puede detectar nuevas variantes de malware y comportamientos sospechosos que no se ajustan a las firmas tradicionales de malware.

Esta capacidad para detectar comportamientos maliciosos genéricos hace que BEAST sea una herramienta eficaz contra amenazas desconocidas y en constante evolución, lo que mejora significativamente la protección contra malware poco común o variantes que aún no han sido identificadas por otras técnicas de detección.

Cómo funciona BEAST: Coincidencia de reglas basada en gráficos.

En un sistema protegido, BEAST monitorea el comportamiento y registra cada acción. Las acciones incluyen el acceso al sistema de archivos, al registro del sistema, las conexiones de red y la comunicación entre procesos. Cada vez que se agrega algo a la base de datos gráfica, se busca en el gráfico patrones de comportamiento malicioso.

El siguiente gráfico puede ser utilizado para ilustrar este tipo de coincidencia basada en reglas.



Este usuario ejemplar probablemente ha sido engañado por un sitio web para descargar y ejecutar el archivo malicioso "malware.exe" desde Internet en el navegador Firefox. En realidad, en este caso, se trata de una infección de ransomware. El ransomware cifra los archivos del usuario y luego solicita al usuario que pague una cierta cantidad de dinero para obtener la clave de desencriptación de los archivos.

El proceso malicioso aquí comienza inmediatamente una instancia de la herramienta del sistema "bcdedit" para deshabilitar la función de reparación de inicio de Windows. Luego, inicia una instancia de la herramienta del sistema "vssadmin" para eliminar las llamadas "copias de sombra" o "shadow copies", que se pueden utilizar para restaurar archivos que han sido sobrescritos accidentalmente. Después, procede a cifrar varios archivos en el directorio "C:\user".

Dado que el inicio de las dos herramientas del sistema mencionadas anteriormente es una preparación típica del ransomware antes de cifrar los archivos, con la intención de evitar que el usuario restaure su sistema, el comportamiento (destacado en rojo) puede considerarse claramente malicioso. Por lo tanto, el proceso "malware.exe" sería detenido y el archivo binario sería movido a cuarentena. Sin embargo, las binarios "vssadmin.exe" y "bcdedit.exe" son herramientas del sistema benignas que solo son abusadas por el ransomware, por lo que se mantendrían en el sistema.

Nuevas oportunidades: Eliminación Retrospectiva.

G DATA, ya sea con sistemas automatizados en el backend o mediante procesos de análisis manuales, identifica muchas Indicadores de Compromiso (IOC) todos los días. Un IOC podría ser un servidor de comando y control (C&C) utilizado para operar una botnet, o un archivo en particular que se ha identificado como malicioso.

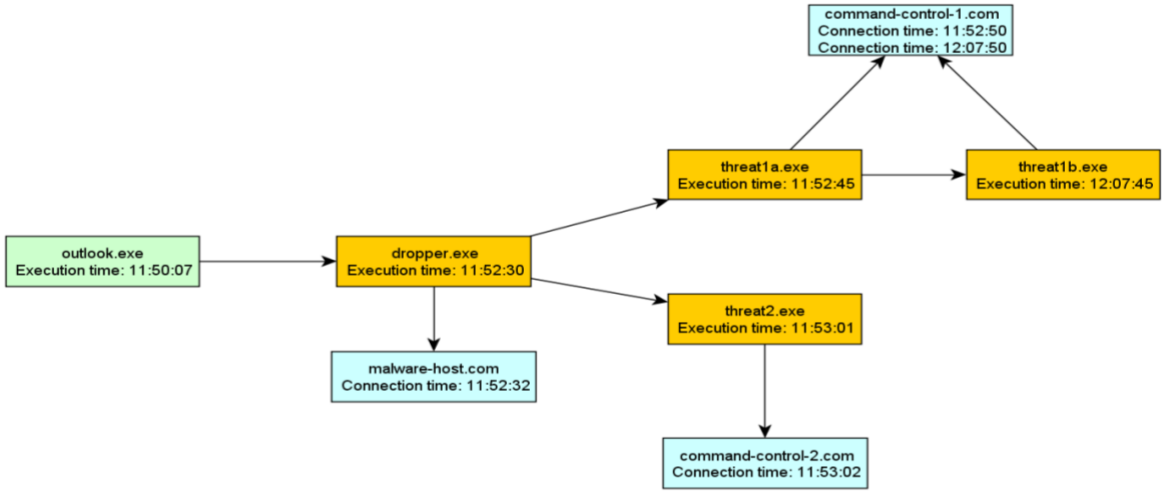
En el software de seguridad tradicional para puntos finales, las acciones solo se comparan con listas de IOC en el momento exacto en que se lleva a cabo la acción. Por ejemplo, antes de ejecutar un archivo, se compara con una lista de archivos maliciosos conocidos. O si un proceso se conecta a un host, el host se verifica en una lista de C&C conocidos. Si el host es identificado como malicioso, todo el proceso se detecta como malicioso.

El problema principal es que los procesos de identificación de IOC de los proveedores de seguridad son, nuevamente, reactivos, ya que comienzan después de que los proveedores comienzan a analizar la amenaza, lo que obviamente solo puede ocurrir después de que una amenaza haya surgido. Incluso si esto se realiza de forma automatizada y en un período de tiempo muy corto, el intervalo de tiempo sigue siendo significativo en el contexto de la detección de malware. En pocas palabras: los proveedores de seguridad a menudo llegan tarde y solo pueden llegar tarde si se basan en métodos tradicionales.

En BEAST, las acciones (comportamiento) se almacenan en una base de datos gráfica local. Por lo tanto, todo lo que está en esta base de datos puede compararse con los IOC identificados por G DATA incluso después de que hayan ocurrido. Y como la base de datos gráfica también contiene todas las acciones relacionadas con el IOC, todas estas acciones pueden deshacerse, permitiendo efectivamente una eliminación retrospectiva de malware.

Esto es particularmente importante si un sistema ha sido comprometido, pero aún no se han activado acciones maliciosas que podrían haber activado la detección de comportamiento genérico.

Para ilustrar esto, imaginemos el siguiente gráfico de comportamiento simplificado: (Aquí debería ir la ilustración del gráfico, pero como modelo de lenguaje de IA, no tengo capacidad para generar gráficos).



Inicialmente, en el programa de correo Outlook se abre un archivo adjunto infectado. Como resultado, se crea y ejecuta un archivo llamado "dropper.exe" por el proceso "outlook.exe". El nuevo proceso luego se conecta a "malware-host.com" para descargar y ejecutar otros archivos binarios maliciosos ("threat1a.exe", "threat2.exe"). Ambos binarios se conectan a sus respectivos servidores de comando y control ("command-control-1.com", "command-control-2.com"). Después de aproximadamente 15 minutos, "threat1a.exe" recibe una orden para actualizar el archivo binario a "threat1b.exe", que también establece una conexión al mismo servidor de comando y control.

Si, por ejemplo, G DATA identifica el servidor "command-control-2.com" o el archivo binario "dropper.exe" como un IOC, BEAST puede, incluso horas después de la infección, recorrer el gráfico, encontrar y eliminar cada archivo binario relacionado con la infección.

Dos notas adicionales: Primero, cualquier cambio en el registro de Windows y, por lo tanto, en la configuración del sistema, se registra y puede deshacerse (omitiéndolo aquí para mantener el gráfico comprensible). Segundo, el ejecutable outlook.exe, al ser conocido como benigno, no sería eliminado.

¿Cuál es la diferencia con el Bloqueador de Comportamiento existente?

TEl Bloqueador de Comportamiento existente básicamente recibe un flujo de cada acción realizada por un proceso. Asigna un valor numérico de "maldad" particular a cada acción individual. Luego, resume todos los valores de maldad, y cuando se supera un umbral determinado de maldad, se considera que un proceso es malicioso.

En principio, el Bloqueador de Comportamiento tiene una vista centrada en los procesos, mientras que BEAST tiene una visión general de todo el sistema. Además, como el Bloqueador de Comportamiento solo agrega valores numéricos de maldad de acciones, no es posible detectar combinaciones específicas de acciones como maliciosas. Esto dificulta la detección específica de patrones de comportamiento malicioso. Cada vez que se asigna un nuevo o mayor valor de maldad a una acción en el Bloqueador de Comportamiento, esto puede provocar detecciones falsas positivas. Esto hizo que fuera problemático reaccionar rápidamente a nuevas amenazas. E incluso si se consideraba cuidadosamente cada vez que en el pasado se asignaba un nuevo o mayor valor de maldad a una acción para detectar una nueva amenaza, existía un gran riesgo de provocar detecciones falsas positivas. En cambio, en el caso de BEAST, las detecciones se basan en combinaciones muy específicas de acciones maliciosas. Por lo tanto, es más fácil agregar nuevas reglas, al tiempo que es menos propenso a detecciones falsas positivas en general.

Además, la posibilidad de una comparación retrospectiva de IOC (Indicadores de Compromiso) y una eliminación retrospectiva solo es posible con BEAST.

¿Por qué necesitamos BEAST cuando tenemos DeepRay?

La fortaleza de DeepRay radica en su capacidad para analizar empaquetadores, lo que nos permite identificar los núcleos maliciosos de malware. Sin embargo, la identificación inicial de los núcleos maliciosos es un proceso manual. Para las familias de crimeware más prevalentes, esta tarea es manejable. Aún así, incluso para estas familias, BEAST ayudará a cubrir el espacio de tiempo hasta una detección de DeepRay, en caso de que el malware cambie en su núcleo. Pero además de las familias de crimeware más prevalentes, también existe un gran número de familias de malware que no son muy prevalentes como una sola familia, pero que, en conjunto, representan una gran cantidad de infecciones. Y si la razón por la que no son tan prevalentes es porque estas familias se utilizan en ataques dirigidos, son aún más peligrosas. Como BEAST no se basa en la identificación de un núcleo de malware específico, sino en la observación genérica del comportamiento malicioso, BEAST ayudará a mitigar estas amenazas y, por lo tanto, agregará otra capa de seguridad.