NioGuard Security Lab

Soluciones de copia de seguridad empresariales

Prueba de autodefensa

MARZO DE 2018

01

Introducción

Ante el aumento del número de ataques en los que los cryptolockers cierran los procesos de bases de datos para cifrar los archivos que contienen (Cerber, GlobeImposter, Rapid, Serpent) y pueden cifrar copias de seguridad locales y en la red para solicitar un rescate (Rapid, Spora), hemos decidido probar las funciones de autodefensa de las principales soluciones de copia de seguridad utilizadas en entornos empresariales disponibles para evaluación.

Esta prueba tiene como objetivo comprobar la resistencia de los procesos del producto cuando se enfrentan a ataques típicos dirigidos a software de seguridad como los que se describen a continuación, así como verificar la capacidad de autodefensa de la copia de seguridad local y los archivos del producto. El ransomware puede cifrar los archivos de copia de seguridad y los archivos de configuración que forman parte del programa de copia de seguridad, impidiendo así su recuperación. Además, una vez que el agresor consigue acceso a los procesos del agente o del servidor, puede eliminar las copias de seguridad de los archivos no solo locales, sino también en la nube, haciéndose pasar por una solución de copia de seguridad.

Este documento es un resumen del informe de prueba para soluciones de copia de seguridad empresariales, e incluye la descripción del entorno de prueba, la lista de soluciones comprobadas y sus versiones, una descripción de los casos de prueba, así como los resultados y las conclusiones derivadas de los mismos. No otorgamos una calificación a las soluciones que se han probado ni tampoco ningún premio, sino que ofrecemos los resultados "tal cual" únicamente con fines informativos.

02

Entorno de prueba

Las pruebas se han realizado en las siguientes máquinas virtuales:

- Windows 8.1 SP1, de 32 bits, compilación 9600
- Windows 10 Enterprise, 64 bits, compilación 16299
- Windows Server 2012 R2 Standard, 64 bits, v. 6.3.9600, compilación 9600

Hemos probado las soluciones de copia de seguridad en plataformas de 32 y de 64 bits porque las técnicas de inyección de procesos empleadas en los casos de prueba varían en dichas plataformas. Además, las compilaciones de productos de 32 y 64 bits pueden contener otro grupo de funciones, incluidas las de autodefensa, y es posible que su implementación dependa de la arquitectura del sistema operativo.

03

Productos comprobados

Se comprobaron las últimas versiones disponibles de los siguientes productos en el momento de las pruebas:

Nombre del producto	Componentes	Versión
Acronis Backup	Management Server	12.5 9010
	Agent	12.5 9010
Arcserve	Unified Data Protection Server	6.5.4175 Update 2 Build 667
	Unified Data Protection Client	6.5.4175.791 v.r6.5
Veeam	Backup & Replication	9.5 Update 3
	Agent for Microsoft Windows	2.1.0.423
Veritas Backup Exec	Server	16.0 Rev. 1142
	Agent Utility for Windows	16.0 ver. 1142.1632

Todos los productos se instalaron con la configuración predeterminada y se actualizaron antes de realizar las pruebas.

04 Casos de prueba

La suite consta de 31 pruebas que simulan ataques a archivos de copia de seguridad locales, archivos, procesos y servicios de los productos, y almacenamiento en la nube, que tienen el objetivo de interrumpir el servicio de copia de seguridad y recuperación. La categoría "Protección de los archivos del producto" contiene pruebas sencillas que intentan destruir archivos de copia de seguridad y de la aplicación, para que sea imposible recuperar los datos cifrados por el ransomware.

El segundo grupo de pruebas "Protección de los procesos y servicios del producto" es crucial para la autodefensa, ya que el malware puede inyectar su código malicioso en un agente de copia de seguridad y actuar fingiendo ser una solución de copia de seguridad a fin de obtener los privilegios necesarios para controlar los archivos de copia de seguridad. Un ciberdelincuente puede conseguir que un proceso malicioso termine procesos y servicios, lo que puede provocar un fallo general de la aplicación de copia de seguridad y recuperación, o la eliminación de los archivos de copia de seguridad. El último grupo de pruebas es "Protección de la copia de seguridad en la nube y recuperación" y su objetivo son las interfaces de comunicación con el almacenamiento en la nube. Los ataques de envenenamiento de DNS o uso inadecuado de la CLI pueden interrumpir el servicio de copia de seguridad en la nube.

№	Categoría de prueba	Caso de prueba
	Protección de los archivos del producto	
1	Protección de los archivos de copia de seguridad locales	Cambiar el nombre, eliminar o cifrar archivos de copia de seguridad locales
2	Protección de los propios archivos del producto de copia de seguridad	Eliminar archivos del programa
3		Modificación del registro de arranque maestro y cifrado de MFT
	Protección de los procesos y servicios del producto	
4	Terminación de los procesos y servicios	Finalizar tarea en el Administrador de tareas
5		Detención de los servicios y terminación de procesos con PowerShell
6		Uso de TerminateProcess()
7		Uso de TerminateThread()
8		Uso de TerminateJobObject()
9		Uso de DebugActiveProcess()
10		Uso de WinStationTerminateProcess()
11		Envío del evento WM_CLOSE
12		Envío del evento WM_QUIT
13		Envío del evento WM_SYSCOMMAND (SC_CLOSE)
14		Envío de todos los eventos de Windows posibles
15	Inyección de código	Uso de CreateRemoteThread()
16		Uso de NtCreateThreadEx()
17		Uso de QueueUserAPC()

№	Categoría de prueba	Caso de prueba
	Protección de los procesos y servicios del producto	
18	Inyección de código	Uso de SetWindowsHookEx()
19		Uso de RtlCreateUserThread()
20		Uso de SetThreadContext()
21		Inyección reflexiva de DLL
22	Modificación de la memoria de procesos	Bloqueo del acceso a las páginas de memoria de procesos mediante el atributo PAGE_NOACCESS
23		Intento de liberar memoria de procesos mediante NtFreeVirtualMemory()
24		Anulación de asignación de todos los objetos asignados mediante NtUnmapViewOfSection()
25		Asignación de toda la memoria disponible mediante NtAllocateVirtualMemory()
26		Asignación de toda la memoria disponible mediante NtMapViewOfSection()
27		Escritura en la memoria de procesos mediante NtWriteVirtualMemory()
28	Modificación de objetos de procesos	Duplicación de objetos de procesos para consumir recursos disponibles
29		Duplicación de objetos de procesos con cierre de objetos originales
	Protección de la copia de seguridad en la nube y recuperación	
30	Modificación de datos de la copia de seguridad en la nube	Uso de la CLI del producto para eliminar, modificar o cifrar datos en la nube
31	Envenenamiento de DNS	Modificación de archivo de hosts

05

Resultados

Nombre del producto	Plataforma de 32 bits/64 bits	Número de pruebas superadas	Número de pruebas no superadas	No aplicable (N/A)	Porcentaje de aciertos
Acronis Backup	32	26	4	1	87 %
	64	25	6	0	81 %
Arcserve	32	5	24	2	17 %
	64	4	26	1	13 %
Veeam	32	4	26	1	13 %
	64	4	27	0	13 %
Veritas Backup Exec	32	5	22	4	19 %
	64	4	27	0	13 %

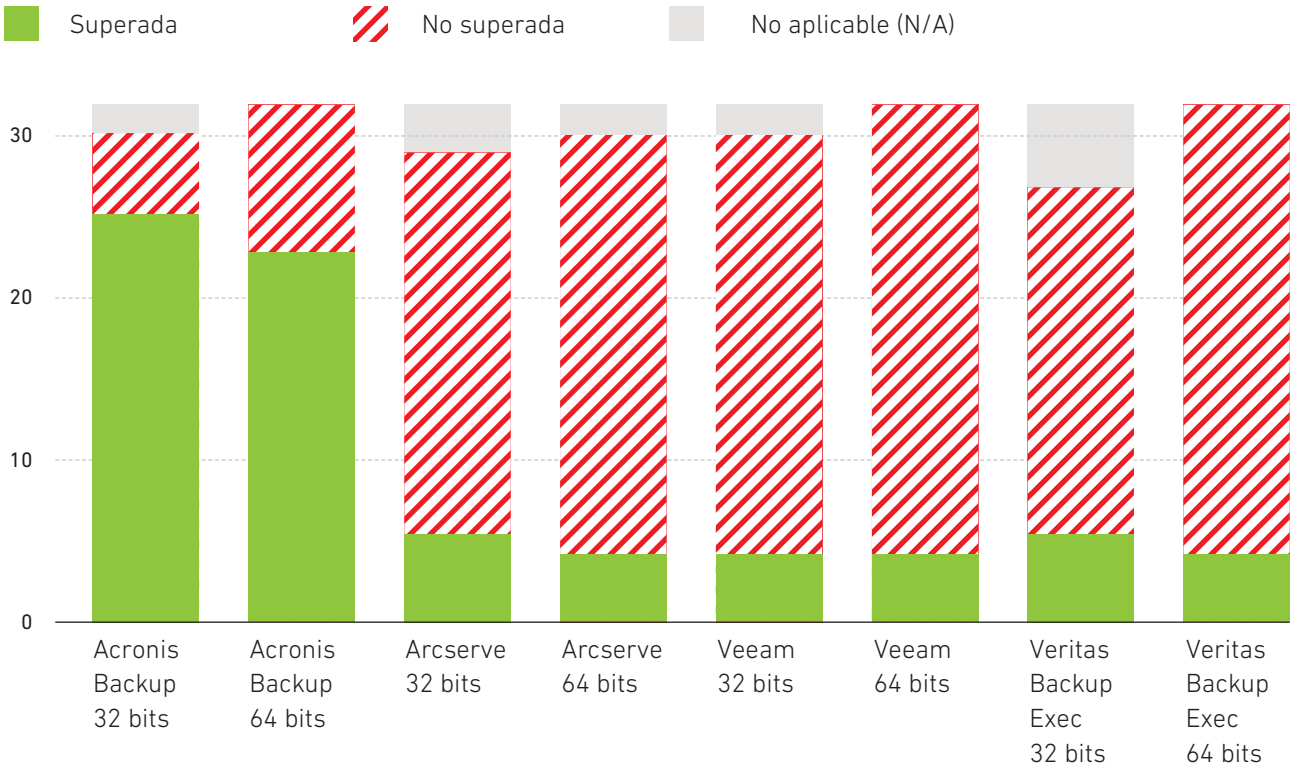
Número de pruebas superadas: el producto resistió el ataque y mantuvo el servicio de recuperación operativo.

Número de pruebas no superadas: el producto sufrió un fallo general tras el ataque, por lo que el servicio de recuperación dejó de funcionar.

No aplicable: la prueba utiliza una función de la API de Windows que no admite la versión actual de Windows o bien la característica comprobada no está disponible en el producto. Por ejemplo, una solución no tiene herramienta de CLI para administrar las copias de seguridad o no ofrece almacenamiento en la nube entre las ubicaciones disponibles para guardar las copias de seguridad.

Porcentaje de aciertos: se calcula como el número de pruebas superadas/(número total de pruebas - N/A).

Nota: *el resultado solamente muestra el número total de pruebas no superadas, sin especificar concretamente en qué pruebas se ha fallado. Esto es intencionado y se hace con el fin de evitar que los ciberdelincuentes puedan averiguar cuáles son los puntos flacos de los productos comprobados.*



06

Conclusión

El objetivo de la prueba era verificar la capacidad de autodefensa del software de copia de seguridad para proteger sus archivos, procesos, servicios y almacenamiento en la nube frente a situaciones que podrían surgir como consecuencia del ransomware.

Los resultados mostraron que la mayoría de los productos probados en la mayoría de los casos no están listos para responder a ataques como los del ransomware, lo que abre la puerta a un ciberdelincuente potencial para bloquear las copias de seguridad del usuario y desactivar los servicios de copia de seguridad y recuperación. Solo Acronis Backup mostró buenos resultados con un 87 % y un 81 % de aciertos para productos de 32 y 64 bits, lo que demuestra que ofrece autodefensa integral, así como continuidad del servicio.

07 Copyright y descargo de responsabilidad

Solo se permite el uso de los resultados que ofrece este informe con la autorización explícita y por escrito de NioGuard Security Lab antes de cualquier publicación.

Declinamos toda responsabilidad por daños y pérdidas que puedan producirse en relación con el uso de la información proporcionada en el presente documento, incluida la de la prueba. No garantizamos la precisión ni la integridad del contenido de este informe.

Para obtener más información sobre NioGuard Security Lab y la metodología de la prueba, visite nuestro sitio web www.nioguard.com o diríjase a nosotros por correo electrónico: ada@nioguard.com.