LIBRO ELECTRÓNICO

5 razones por las que no se puede prevenir el ransomware

NetApp

Contenido

Dado el número de ataques de alto nivel a lo largo de los años y las graves consecuencias de las infecciones, cabría pensar que los métodos de prevención han madurado hasta el punto en que el ransomware pronto será visto como algo del pasado.

Piensa en la antes ubicua amenaza de los exploit kits, como el infausto Angler, que en su época supuso un tremendo dolor de cabeza para los equipos de seguridad. Estos kits prácticamente han desaparecido gracias al implacable esfuerzo de los investigadores.

Pero el ransomware sigue por todas partes y la prevención total es, en la práctica, imposible. Hagamos una cuenta atrás con los motivos para ello.

5

Vale la pena

Los atacantes están más motivados que nunca porque los ataques con éxito ofrecen enormes dividendos. El rescate medio que pagaron las organizaciones en Estados Unidos, Canadá y Europa aumentó de 115 123 USD en 2019 a 312 493 USD en 2020: un aumento del 171 % de un año para el otro. La media en el primer trimestre de 2021 fue de 850 000 USD. Desde 2019, los incidentes relacionados con el ransomware han aumentado un 65 %. La frecuencia de los ataques no deja de crecer: se estima que de un ataque cada 11 segundos pasaremos a uno cada 2 segundos en 2031. Los asaltos serán cada vez más habituales. Con estos números, no extraña que el ransomware siga estando entre las actividades predilectas de los delincuentes.

Y aunque las fuerzas del orden desaconsejen hacerlo, las organizaciones siguen pagando los rescates. Es natural que las empresas quieran proteger sus datos, pero el coste de la interrupción del negocio a menudo supera el del propio rescate, lo que significa que pagar suele ser la opción más rentable.

4

Es barato

Además, la inversión necesaria para realizar una campaña de ransomware es baja. Hoy en día, un atacante puede comprar un kit prefabricado por una cantidad relativamente pequeña. El kit contiene todo lo necesario para poner en marcha y monetizar el ataque, incluidos servicios de cifrado, el agente con la carga útil y herramientas de ofuscación. Una suscripción típica de ransomware como servicio (RaaS) cuesta solo 100 USD al mes. Las variantes más complejas y potentes pueden costar miles de dólares, aunque los dividendos potenciales también aumentan. Por si fuera poco, los kits incluyen planes de asistencia para que los atacantes puedan obtener el máximo valor del servicio.

3

Ha demostrado su eficacia

El ransomware es un negocio rentable. Olvídate del estereotipo de un delincuente con capucha en una sala oscura: esto es una red bastante sofisticada, comparable a cualquier programa para partners corporativo. Uno de los últimos ejemplos de RaaS es DarkSide, detectado por primera vez en agosto de 2020 y convertido al modelo de distribución RaaS en noviembre. Basándonos en los incidentes denunciados, la reclamación típica a cambio de las claves para desbloquear los datos está entre los 200 000 y los 2 millones de USD. Los operadores de DarkSide no solo obtienen grandes sumas, sino que también se presentan como “Robin Hoods”: toman dinero de grandes empresas rentables y llegan a hacer donativos a la caridad con las ganancias. Los informes procedentes de sitios de filtraciones indican que este ransomware ha afectado al menos a 90 víctimas hasta la fecha. Ahora mismo, más de 2 TB de datos robados se almacenan en sitios de DarkSide, lo que supone un incentivo más para pagar.

2

¡El retorno de la inversión es muy rápido!

Otra razón por la que el ransomware resulta tan atractivo es que, después de colarse en una organización, normalmente mediante adjuntos de correo electrónico, URL maliciosas, protocolos de escritorio remoto poco seguros o publicidad infectada (el denominado “malvertising”), actúa con rapidez. Analiza la red para localizar archivos, cifra el contenido y exige un rescate. Por desgracia, una vez que el proceso de cifrado comienza, poco se puede hacer por anularlo. Y está surgiendo una nueva y alarmante tendencia, una metodología por la que los atacantes roban los datos antes de cifrarlos. En mayo de 2021, Colonial Pipeline, que suministra el 45 % del combustible de toda la Costa Este de EE. UU., se vio afectado por un ataque de ransomware. Dicho ataque se realizó con DarkSide o un sistema afiliado. Aparte de bloquear los sistemas informáticos de Colonial Pipeline, DarkSide robó más de 100 GB de datos de la empresa. Este robo demuestra que el grupo extorsiona a sus víctimas por partida doble. No solo piden dinero por desbloquear los ordenadores afectados, sino que también exigen un pago por los datos capturados, que amenazan con filtrar al público si la víctima no paga.

1

Las personas no son fiables

Hasta ahora, hemos visto por qué el ransomware está por todas partes, pero no hemos hablado de cómo detenerlo. Aunque es cierto que un gran número de ataques podría evitarse con una mayor higiene en las actualizaciones, hay un motivo principal por el que la prevención total es imposible: las personas.

Confías en que tus empleados nunca querrían dañar la organización de forma intencionada, pero las infecciones se siguen produciendo porque las personas no están superatentas en todo momento ante los peligros que suponen los enlaces y correos electrónicos maliciosos y los intentos de phishing.

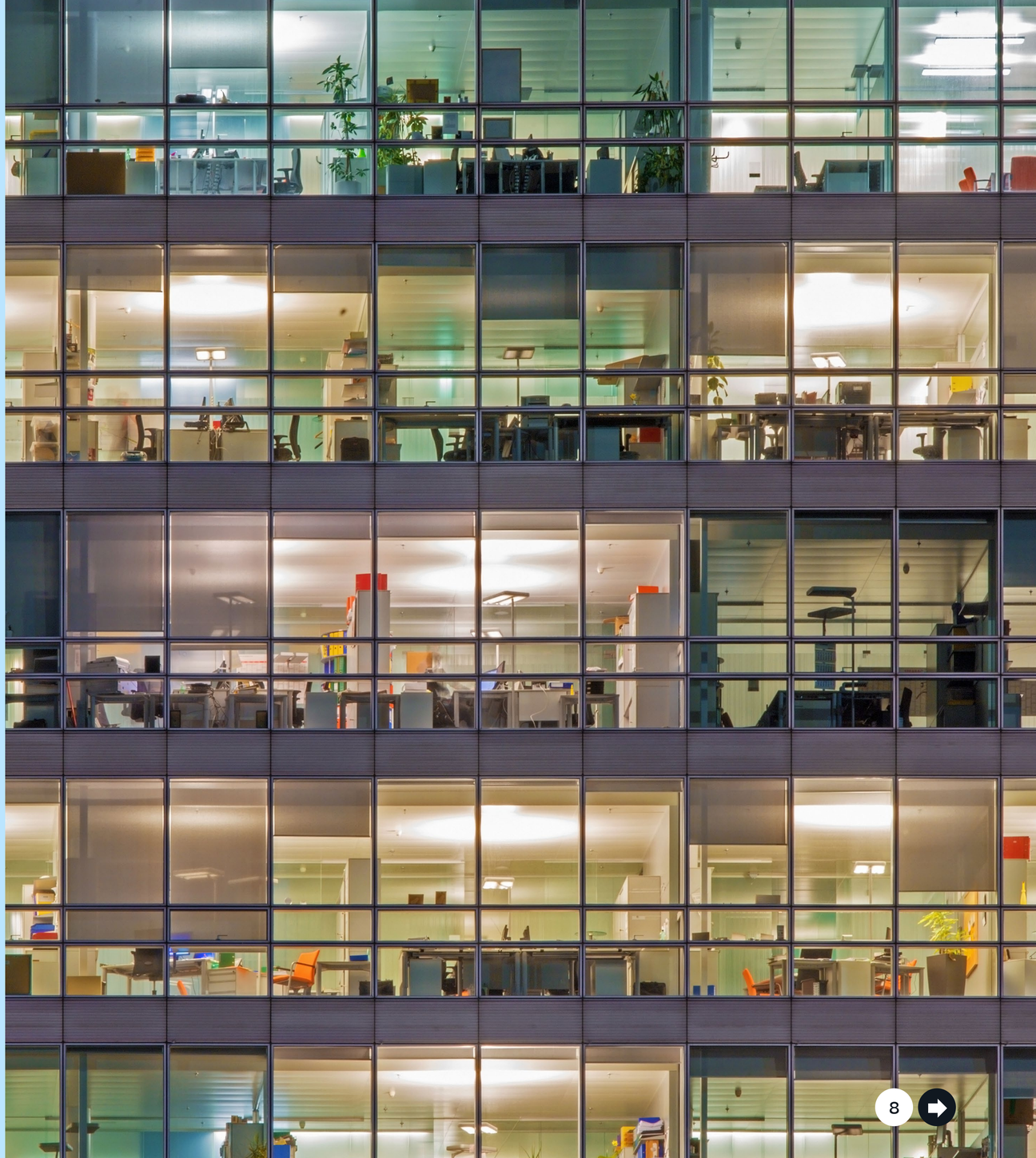
Es probable que muchos lectores estén familiarizados con la formación periódica obligatoria sobre seguridad informática y concienciación. Esta formación está bien, sin duda, pero hasta los empleados más atentos pueden cometer un error de juicio momentáneo al hacer clic en un enlace o abrir un correo electrónico. Y ese error es cuanto se necesita si no hay implementadas políticas de seguridad hiperrestrictivas que acaban afectando a la capacidad de las personas para desarrollar su trabajo. La detección debe realizarse en cuestión de segundos, no de minutos, ni horas, ni días.

Protección contra ransomware de confianza cero

Y si no se puede prevenir el ransomware, ¿qué puedes hacer para protegerte?

Tus empleados necesitan acceso a los datos para hacer su trabajo, igual que el ransomware, por lo que las personas se convierten en el vector de ataque. Es útil establecer políticas y roles que restrinjan el acceso a los datos, pero en exceso pueden llegar a afectar a la productividad.

La respuesta es la detección temprana, el análisis del comportamiento de los usuarios y la acción automatizada una vez que se producen patrones sospechosos. En cuestión de segundos.



NetApp® Cloud Insights ofrece exactamente este tipo de detección con una función denominada Cloud Secure. Cloud Secure permite supervisar la actividad, detectar anomalías y automatizar las respuestas.

- **Supervisar la actividad de los usuarios**
  Para identificar correctamente las vulneraciones, se capturan y analizan las actividades de todos los usuarios en las instalaciones y en los entornos de cloud híbrido. Los datos se recopilan mediante un agente recopilador ligero y sin estado, que está instalado en una máquina virtual del entorno del cliente. Se incluyen también datos de usuario procedentes de los servidores de Active Directory y LDAP, así como su actividad de archivos en el almacenamiento NetApp ONTAP®, tanto en los centros de datos propios como en la cloud.

  Cloud Secure crea un modelo de comportamiento para cada usuario y así detecta anomalías. A partir del modelo de comportamiento, detecta cambios anormales en la actividad del usuario y analiza patrones para determinar si se trata de una amenaza de ransomware o de un usuario malintencionado. Este modelo de comportamiento reduce los casos de falsos positivos.

- **Detectar anomalías e identificar posibles ataques**
  El ransomware y el malware de hoy en día son sofisticados y usan extensiones y nombres de archivo aleatorios, por lo que las soluciones de detección basadas en firma (lista de elementos bloqueados) resultan ineficaces. Cloud Secure usa algoritmos de aprendizaje automático avanzados para descubrir actividades de datos inusuales y detectar un posible ataque. Este enfoque permite una detección dinámica y precisa, y reduce los casos de falsos positivos.

- **Automatizar las políticas de respuesta**
  Cloud Secure te alerta de un posible ataque de ransomware y proporciona múltiples políticas de respuesta automática para proteger tus datos.

  Crea una copia NetApp Snapshot™ cuando detecta un comportamiento inusual. Tus datos quedan protegidos, por lo que puedes recuperarlos rápidamente. Además, se limita la posibilidad de interrupciones por falsos positivos.

Bloquea la capacidad del usuario de acceder a los datos:
- Cuando se detecta un comportamiento anormal (lectura/escritura) de un usuario.
- Cuando se detecta un comportamiento inusual de borrado de archivos.

Cloud Secure proporciona auditoría de acceso detallada, de modo que los administradores pueden identificar rápidamente los datos en peligro y el origen del ataque, lo que permite remediarlo y proceder a la recuperación.

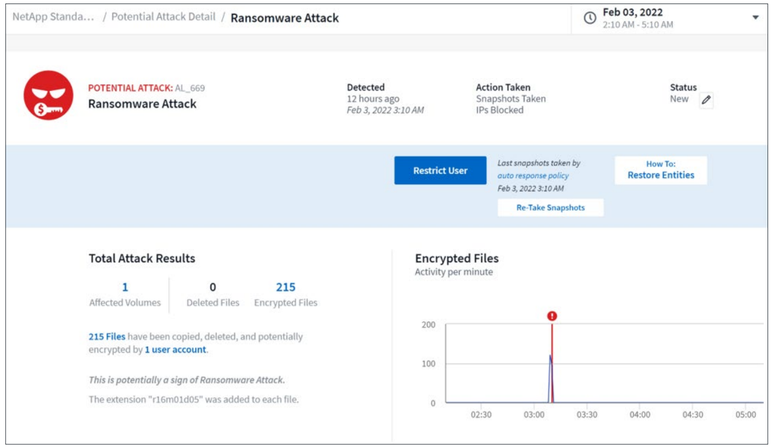


Figura 1) Consola de Cloud Secure donde se muestra un ataque de ransomware.

Si te gustaría obtener más información sobre Cloud Secure, regístrate en nuestra prueba gratuita de 30 días. **Obtén más información y comienza tu prueba gratuita.**

Acerca de NetApp

En un sector lleno de generalistas, NetApp es un especialista. Nos centramos en una cosa: ayudar a tu empresa a aprovechar al máximo sus datos. NetApp incorpora al cloud los servicios de datos de clase empresarial en los que confías y lleva la sencilla flexibilidad del cloud al centro de datos. Nuestras soluciones líderes del sector funcionan en diversos entornos de clientes y en los mayores clouds públicos del mundo.

Como empresa de software centrada en datos y orientada al cloud, solo NetApp puede ayudarte a crear un Data Fabric exclusivo, a simplificar y conectar tu cloud y a proporcionar con seguridad los datos, los servicios y las aplicaciones correctos a las personas adecuadas en cualquier momento y lugar.

NetApp