FICHA TÉCNICA

Recuperación tras un ataque de ransomware con SafeMode de FlashArray

Utilice las copias instantáneas SafeMode™ de FlashArray™ de Pure Storage® para proteger sus datos.

El ransomware (cuando un intruso de manera furtiva encripta sus archivos y exige un pago para desencriptarlos o desbloquearlos) puede ser catastrófico para las organizaciones. La pérdida de sus datos y el impacto monetario no son las únicas preocupaciones; en muchos casos, el ataque provoca la suspensión completa de la actividad de la empresa durante días y hace que esta se convierta en el centro de la atención pública por motivos negativos. Además, la reputación de su empresa y el valor de su marca también pueden verse perjudicados. En 2020, Garmin sufrió un ataque de ransomware en el que el periodo de inactividad duró casi cinco días; aunque no se conoce el importe exacto del rescate pagado, se calcula que fue de unos 10 millones de dólares.

¿Qué es el ransomware?

En la primera mitad de 2020, el número total de ataques de ransomware notificados aumentó un 715% en términos interanuales, según el último Informe sobre el panorama de amenazas de 2020 publicado por Bitdefender. El hecho de que haya más personas teletrabajando y de que el entorno empresarial haya cambiado debido a la pandemia global ha supuesto una oportunidad, que ha sido aprovechada por los ciberdelincuentes.

Los efectos del ransomware afectan a todos los sectores, desde la tecnología hasta los seguros, el petróleo y el gas o la educación superior. En 2019, más de 500 escuelas se vieron afectadas por el ransomware. El software de ransomware es un gran negocio y las víctimas son cada vez más y tienen que pagar cifras exorbitantes para volver a operar con normalidad.

Lo que mucha gente desconoce es que el software para realizar ataques de ransomware es tan fácil de conseguir como el software comercial. Puede descargarse y comprarse fácilmente y con frecuencia una parte de las ganancias generadas por cualquier ataque va a parar al desarrollador. Los atacantes no tienen por qué tener unos conocimientos o una cualificación especiales. Pueden ser empleados descontentos con unos conocimientos mínimos y acceso a una infraestructura crítica. Con una rápida descarga desde la red oscura, pueden lanzar un ataque de ransomware antes de que se bloqueen sus cuentas de empleado.

Defensa

Proteja sus datos de los ataques maliciosos de ransomware, los daños a su reputación y las costosas exigencias de rescate.

Protección

Independientemente de quién le ataque, los datos solo pueden eliminarse contactando con el Soporte de Pure.

Sencillez

SafeMode solo necesita tres sencillos pasos para configurarse y puede activarse gratuitamente.

Cómo protege SafeMode los datos críticos

Echemos un vistazo a dos ejemplos de ataques posibles, que parten de la idea de que un atacante ha conseguido los derechos de administración de un FlashArray.

1. **El atacante encripta volúmenes y elimina los originales:** en este escenario, se destruyen los volúmenes originales. Cuando un volumen es "destruido" pasa a estar en un área especial de FlashArray y a eliminarse del inventario de volúmenes, aunque sigue existiendo en la papelera de eliminación. La papelera de eliminación tiene un temporizador ajustado por defecto en 24 horas, que permite que los objetos se recuperen o se eliminen de manera permanente. Si el atacante también ha borrado los volúmenes, todos los datos de estos se han perdido y ahora usted depende totalmente de lo que le exija. En cambio, con SafeMode activado, el atacante no puede eliminar los datos de los volúmenes que están en la papelera de eliminación, ni siquiera con privilegios de administrador. En nuestro ejemplo concreto, el atacante puede eliminar los volúmenes porque no se ha activado SafeMode.
2. **El atacante encripta volúmenes y elimina todas las copias instantáneas, así como los volúmenes:** en este caso, existen unos puntos de recuperación a los que se puede volver en forma de copias instantáneas. Sin embargo, el atacante las ha destruido y eliminado, así que no hay nada desde lo que poder restaurar. Esto ha sido posible porque, como en el Ejemplo 1, el atacante ha eliminado las copias instantáneas debido a que no se había activado SafeMode.

En ambos escenarios, la activación de SafeMode impide que se elimine cualquier volumen o copia instantánea durante el periodo configurado en el temporizador de eliminación. Si este se ajusta en 14 días, los datos de recuperación necesarios para restaurar los servicios críticos estarán totalmente protegidos durante dos semanas. SafeMode no solo impide que incluso las cuentas de usuario con más privilegios eliminen volúmenes y copias instantáneas, sino que también hace que las copias de FlashArray sean inmutables (no modificables). El uso de SafeMode con las copias instantáneas siempre garantizará un punto de recuperación tras un ataque.

Cómo recuperarse de un ataque de ransomware

Si volvemos a nuestros ejemplos, vemos que si SafeMode hubiera estado activado en el Ejemplo #1, usted hubiera podido eliminar los volúmenes encriptados del atacante, para luego restaurar sus volúmenes —al instante— y volver a un estado anterior al de la encriptación.

En el ejemplo #2, el proceso es el mismo. Podría haber eliminado los volúmenes encriptados del atacante y haberlos restaurado a partir de las copias instantáneas. Como el atacante no hubiera podido eliminarlas, estas hubieran estado disponibles para la recuperación. En ambos ejemplos, sería sumamente importante investigar el vector del ataque y adoptar las medidas necesarias para impedir que este volviera a ocurrir.

Figura 1 Los volúmenes atacados/encriptados son sustituidos fácilmente por copias instantáneas de un punto anterior en el tiempo.

Configuración de SafeMode

SafeMode es fácil de configurar. Llame al Soporte de Pure para pedir que se active SafeMode y para proporcionar (hasta cinco) personas de contacto con autorización para solicitar cambios en SafeMode. El Soporte le facilitará un pin de seis cifras para cada usuario autorizado, que deberá usarse para realizar cualquier cambio en el futuro. SafeMode puede estar activado o desactivado, pero el temporizador de eliminación es configurable. La mayoría de nuestros clientes lo ajustan en 14 días, pero el temporizador puede ampliarse hasta 30 días.

Es obligatorio crear una política de copia instantánea para que SafeMode proteja sus datos. Esto se realiza a través de los Grupos de Protección de FlashArray, en los que los anfitriones, los volúmenes, los grupos de volúmenes, los archivos y los directorios pueden copiarse al instante de manera automática periódicamente. La conservación y la frecuencia de las copias instantáneas se pueden personalizar. Incluso se puede añadir un tercer dispositivo, es decir un “destino”, para enviar las copias instantáneas a otro FlashArray, otro servicio de nube u otra FlashBlade®.

Si necesita recuperar espacio de FlashArray, algo que puede ocurrir, por ejemplo, después de una migración de datos a un array, será necesario realizar una llamada telefónica al Soporte de Pure Storage, en la que deberán hablar dos contactos autorizados, que deberán disponer de sus respectivos pines, para poder eliminar de manera permanente cualquier elemento. De todos modos, este proceso no es necesario para la recuperación instantánea de los objetos cuya eliminación aún está pendiente.

Conclusión

SafeMode es una característica sencilla y sin coste adicional, que impide la pérdida permanente de datos debido a errores del administrador o a ataques maliciosos de ransomware. Funciona simplemente impidiendo la eliminación de objetos durante un periodo de tiempo configurado. Si se produce un ataque, en lugar de sufrir una interrupción muy dolorosa y pública, que solo se acabará pagando un rescate, lo único que debe hacer es eliminar los datos encriptados por el atacante y restaurar al instante sus datos desde un punto anterior en el tiempo.

Para ello, solo tiene que llamar al soporte, elegir a sus contactos y configurar el plazo del temporizador. Estos tres pasos le proporcionarán una victoria sencilla y proactiva antes de que le afecte un posible desastre.

PS2024-01 03/2021