Preparación ante ataques que buscan la destrucción total

El panorama de amenazas ha cambiado drásticamente. ¿Está preparado para los nuevos ataques destructivos?

Autores: Brian Hymer, arquitecto de sistemas estratégicos en Quest® Software, y Randy Franklin Smith, experto en seguridad de Windows y Active Directory

INTRODUCCIÓN

Los profesionales en TI y seguridad han estado mucho tiempo luchando contra graves amenazas. Por un lado, están los riesgos como cortes eléctricos, fallos de hardware y desastres naturales. Por otro lado, están el personal interno malintencionado y los hackers astutos, totalmente equipados con innovadoras herramientas y técnicas para abusar de las vulnerabilidades y crear virus, malware y ransomware cada vez más sofisticados.

Defenderse de estas amenazas nunca ha sido pan comido, pero, en líneas generales, se conseguía limitar los riesgos de forma significativa. Por lo general, las amenazas naturales se encuentran en un alcance geográfico, de modo que disponer de un centro de datos de reserva en otra ubicación era un método de defensa eficaz. Los atacantes humanos solían centrarse en un objetivo específico: obtener acceso a los datos para robarlos y venderlo con ánimo de lucro o para cifrarlos, secuestrarlos y pedir un rescate, de forma que los profesionales de TI sabían priorizar las estrategias de protección de datos.

Pero, sin duda, las cosas han dado un vuelco desagradable: cada vez son más los ataques que buscan la destrucción total de su infraestructura. Por desgracia, son muchas las organizaciones que están bien preparadas. En esta documentación técnica, se repasan algunos de los ataques recientes más destructivos, se analiza su velocidad, alcance y metodología, y se indaga en las mejores estrategias para defender su organización de ellos.

LA VELOCIDAD Y LA POTENCIA DE LOS ATAQUES DESTRUCTIVOS

Seguro que habrá oído nombres que parecen salidos de la ciencia ficción, como NotPetya, Shamoon, Stuxnet, Olympic Destroyer, BlackEnergy, Destover, Wiper o Triton. Pero ¿qué ocurrió realmente en estos ataques destructivos? Para hacerse una idea de su velocidad y escala, y la urgencia de dar con una estrategia de defensa, vale la pena parar a revisar unos pocos incidentes recientes.

Stuxnet

A finales de los años 2000, Israel y Estados Unidos estaban cada vez más preocupados por el programa nuclear de Irán. Antes de 2009, el país producía tanto uranio enriquecido que podría crear dos armas nucleares en el plazo de un año. Como respuesta, según la creencia general, Israel y Estados Unidos empezaron a desarrollar un sofisticado gusano informático, Stuxnet, diseñado no para piratear ordenadores ni para robarles datos, sino para destruir equipos físicos. En concreto, cuando Stuxnet infecta un ordenador conectado a controladores lógicos programables (PLC) específicos que controlan maquinaria industrial

Cada vez son más los ataques que buscan tan solo la aniquilación total de su infraestructura. Muy pocas organizaciones están bien preparadas.

(como centrifugadoras de uranio), lo que hace es alterar la programación de los PLC para obligar a las centrifugadoras a girar demasiado rápido y durante mucho tiempo, a la par que garantizar que los PLC siguen informando de que todo funciona correctamente para que los supervisores del equipo no adviertan dicho comportamiento anómalo. Con el tiempo, las máquinas infectadas acaban destrozadas debido a ese sobreesfuerzo. En 2010, más de quince instalaciones iraníes se vieron infectadas por Stuxnet, y se echó a perder casi una quinta parte de las centrifugadoras nucleares del país.

El objetivo al crear Stuxnet nunca fue que se extendiera más allá de las instalaciones nucleares iraníes, con protección Air Gap y sin conexión a Internet. Sin embargo, de alguna forma, el malware acabó en Internet y empezó a expandirse. Con el tiempo, otros grupos han modificado el virus para atacar otro tipo de organizaciones, como plantas de tratamiento de aguas, centrales eléctricas, organismos públicos y empresas de los sectores farmacéutico, de la aviación y defensa. Entre estos virus modificados (a veces llamados "los hijos de Stuxnet"), se incluyen Duqu, Flame, Havex, Industroyer y Triton.

Shamoon

En 2012, le tocó el turno a una empresa petrolífera de sufrir uno de estos ciberataques destructivos. El 15 de agosto, un virus más tarde conocido como Shamoon infectó tres cuartas partes de las 40 000 estaciones de trabajo de Saudi Aramco: se borraron los discos duros y apareció la imagen de la bandera estadounidense en llamas. A pesar de que la empresa declaró que sus actividades de exploración y producción petrolíferas no se vieron afectadas por el ataque y que su red interna principal estuvo off-line solo diez años, un consultor al que se contrató para ayudar en la operación de recuperación señaló que Saudi Aramco tuvo que recompilar su centro de operaciones de seguridad desde cero. Eso fue cinco meses antes de que su sistema finalmente volviera a conectarse. También observó que el ataque habría provocado con facilidad la bancarrota de una empresa más pequeña.

Shamoon desapareció de los titulares durante cuatro años pero, en 2016, se utilizó una versión del malware ligeramente modificada contra varias organizaciones civiles y administrativas en Arabia Saudí y otros estados del golfo Pérsico. El destructivo malware volvió a asomar la cabeza a finales de 2018, cuando sacudió a varias víctimas en Oriente Medio. Esta nueva variante de Shamoon es aún más destructiva que las anteriores, ya que elimina todos los archivos de los ordenadores infectados antes de borrar el registro de arranque maestro. Tras esto, la recuperación de los archivos no es difícil, sino imposible.

BlackEnergy

2015 fue el año del éxito del primer ciberataque en una red eléctrica. En diciembre, los hackers que usaban el malware BlackEnergy pudieron infiltrarse en varios centros de distribución de energía en Ucrania y desconectar sistemas eléctricos. Aunque este ataque afectó únicamente a unos 225 000 clientes y duró solo unas horas, demuestra el poder del malware para destruir una infraestructura crítica. Los futuros ataques a proveedores de energía demostraron que sus consecuencias eran aún más devastadoras.

NotPetya

El que puede ser el ataque más costoso y de mayor alcance hasta la fecha llegó en 2017. Un ejecutivo financiero de la oficina ucraniana del gigante de envíos internacionales Maersk había hecho recientemente una petición común: que el equipo de TI instalara la solución de software de contabilidad M.E.Doc en un único ordenador. El equipo de TI accedió porque M.E.Doc no era una aplicación cualquiera, sino la solución de contabilidad fiscal de facto que utilizaba todo el mundo que hacía negocios en Ucrania. Luego, el 27 de junio, las pantallas de los ordenadores de la sede de Maersk se volvieron negras. Según los investigadores, hackers patrocinados por el Estado habían pirateado los servidores de actualizaciones de M.E.Doc y utilizaron una puerta trasera para liberar el malware en todas las empresas que usaban el software.

En cuestión de horas, Maersk quedó efectivamente paralizada. Cayeron sus 150 controladores de dominios en todo el mundo, excepto uno en Ghana que, por suerte, resultó estar off-line durante el ataque del malware. Durante días, sus terminales de envío en todo el planeta estuvieron congelados, decenas de miles de camiones tuvieron que dar la vuelta y los contenedores de productos perecederos se quedaron sin refrigeración. La limpieza supuso la recompilación de 4000 servidores y 45 000 estaciones de trabajo. Un ejecutivo de Maersk señaló que NotPetya acarreó a la empresa unos costes entre los 250 y 300 millones de dólares, a pesar

de que otros trabajadores internos sospechan que el daño fue mayor.

Sin embargo, las consecuencias no se limitaron a Maersk: NotPetya infectó a empresas de todo el mundo, desde Alemania y Estados Unidos hasta Tasmania, a una velocidad de vértigo. A NotPetya solo le hicieron falta 45 segundos para hacer caer la red de un gran banco ucraniano. Una parte de uno de los principales centros de tránsito de Ucrania se infectó por completo en 16 segundos. Se estancaron prácticamente todas las agencias federales de Ucrania. Se estimó que el daño total fue de más de 10 000 millones de dólares.

Ataques en la nube

Los ataques destructivos para nada se limitan a entornos de TI locales, a pesar de que no todos los incidentes en la nube hasta la fecha tienen que ver con malware con nombres creativos. Por ejemplo, en 2014, el proveedor de IaaS Code Spaces quebró tras sufrir un ataque en varias fases en sus servidores; la mayoría de sus datos, backups, configuraciones de maquinaria y backups externas acabaron eliminados de forma parcial o total.

Más recientemente, en febrero de 2019, los hackers asaltaron al proveedor de correo electrónico VFEmail y formatearon todos los discos de todos los archivos y servidores de backup en su infraestructura de Estados Unidos, de modo que destruyeron todos los datos de correo electrónico de los clientes estadounidenses. Asimismo, los atacantes fueron a por los recursos de sistemas de la empresa en los Países Bajos; sin embargo, como los pillaron con las manos en la masa, la empresa consiguió salvar algunos de sus datos de backup. Aun así, el ataque prácticamente borró toda la infraestructura de la empresa en cuestión de horas. La empresa esperaba echar el cierre, pero se sigue aferrando a la vida.

LOS MOTIVOS DETRÁS DE LOS ATAQUES DESTRUCTIVOS

Los ataques tradicionales suelen estar motivados por razones económicas, por ejemplo, cobrar a cambio de la clave de descifrado en un ataque de ransomware, obtener información personal (PII) o información de estado protegida (PHI) que sirve para identificar robos o venderse en el mercado negro, o recopilar credenciales de usuario que se pueden utilizar en futuros ataques que reportan beneficios económicos. Por lo general, los ataques destructivos tienen una serie completamente distinta de motivaciones, incluidas las siguientes:

- **Motivos políticos:** el hackeo por parte de las naciones es cada vez mayor. Por ejemplo, los expertos creen que Stuxnet lo desarrollaron Estados Unidos e Israel en conjunto para alterar el programa nuclear de Irán, y que NotPetya era un ataque de motivación política contra Ucrania. Algunos creen que Shamoon, el ataque de 2012, era parte de la represalia de Irán contra la participación de Estados Unidos en Stuxnet. Los hackers patrocinados por el Estado suelen estar altamente capacitados y bien financiados para que sus ataques sean especialmente devastadores.
- **Motivos sociales:** algunos ataques se basan en el deseo de un cambio social. A menudo llamados "hacktivistas", estos grupos suelen diseñar ataques por denegación de servicio (DoS) hacia organizaciones que consideran opuestas a sus ideas. Por ejemplo, el grupo hacktivista Anonymous es probablemente el más conocido por su campaña de DoS en 2010 que atacó PayPal.com y los sitios de Visa y MasterCard en represalia a aquellas empresas que cortaron el servicio a Wikileaks por orden del gobierno estadounidense.
- **Venganza:** en el lado opuesto del espectro, se encuentra el trabajador interno disgustado. Por ejemplo, a comienzos de 2002, Roger Duronio, administrador de TI en UBS Paine Webber, diseñó supuestamente una bomba lógica y la utilizó en miles de sistemas que usaban herramientas de administración estándar Unix. A continuación, dejó el trabajo y fue directo a la oficina de su broker para invertir 21 000 dólares en acciones de UBS o PW. Cuando la bomba lógica explotó unas semanas más tarde, hizo caer unos 2000 servidores y eliminó todos los archivos que estos contenían. Los daños fueron tan graves que los empleados se vieron obligados a trabajar con papel y bolígrafo. La empresa se gastó 3 millones de dólares solo en servicios de consultoría para restablecer los sistemas. ¿Qué es lo que motivó a Duronio? Aparentemente, no estaba contento con su prima, que era de 18 000 dólares en lugar de los 50 000 que él esperaba.

  En un entorno con Windows, un usuario privilegiado descontento lo tiene indiscutiblemente más fácil para desatar el caos: lo único que tiene que hacer es desmantelar Active Directory. Si cae Active Directory, también cae toda la red, aunque todo esté bien en los servidores o aplicaciones.
- **Cortina de humo:** con cada vez más frecuencia, los hackers emparejan los ataques diseñados para robar información con los ataques destructivos para eliminar cualquier rastro. El ataque destructivo puede obstaculizar las investigaciones forenses, lo que dificulta la identificación de los atacantes y, por consiguiente, evita su acusación y protege su modus operandi, lo que les permite seguir usando las mismas técnicas en el futuro. Por ejemplo, el malware del llamado Olympic Destroyer paralizó los sistemas de TI antes de las

NotPetya hizo caer la red de un gran banco ucraniano en solo 45 segundos. Se estima que el daño total causado por el ataque en 2017 a nivel mundial fue de más de 10 000 millones de dólares.

ceremonias oficiales de inauguración de los Juegos Olímpicos de Invierno de 2018, celebrados en Corea del Sur. Sin embargo, Olympic Destroyer borró su rastro de una forma tan eficaz que, cuando reapareció más tarde ese mismo año (con organizaciones financieras y laboratorios de prevención de amenazas biológicas y químicas como sus objetivos), los investigadores no estaban seguros de si se trataba del mismo grupo o de otros grupos con distintos intereses.

- **Daños colaterales:** no todas las víctimas de ataques destructivos son un blanco concreto: algunos son meros daños colaterales. Por ejemplo, los arquitectos del ataque NotPetya iban claramente detrás de Ucrania: los cálculos indican que el 80 % de las infecciones se produjo en dicho país, pero las empresas de todo el mundo, entre las que se incluía Maersk, sufrieron asombrosos daños.

Cualquier organización puede ser el objetivo de un ataque destructivo, o simplemente un daño colateral de un ataque dirigido a otra persona o empresa.

METODOLOGÍA

Como hemos visto, los ataques destructivos toman numerosas formas diferentes. Algunos utilizan malware o virus, mientras que otros confían en la fuerza bruta. Unos tratan de borrar datos, mientras que otros buscan provocar daños físicos. Veamos con profundidad cómo se desarrollan.

Acceso inicial

Normalmente, el primer paso en un ataque es obtener acceso a la red. Puede que le suenen muchas de las técnicas que utilizan para ello, como las que se enumeran a continuación. Es importante enfatizar que los ataques destructivos no solo tienen como objetivo ordenadores, como estaciones de trabajo y servidores; en la superficie expuesta al ataque también se incluyen dispositivos IoT, routers y mucho más.

- **Phishing:** Shamoon se introdujo en la red de Saudi Aramco cuando un empleado del equipo de tecnología informática abrió un correo electrónico de phishing malicioso.
- **Puerta trasera:** la puerta trasera de un software de actualizaciones en una solución de software empresarial de terceros permitió a los atacantes liberar NotPetya en Maersk y otras organizaciones de todo el planeta.
- **Dispositivo USB infectado:** dado que las instalaciones nucleares iraníes no tienen conexión a Internet, Stuxnet tuvo que introducirse mediante un dispositivo USB físico, ya fuera de forma deliberada o accidental.
- **Vulnerabilidades de software:** una técnica usada en el ataque de NotPetya, así como en el ataque de ransomware de WannaCry en 2017, fue una herramienta de penetración conocida como EternalBlue y creada por la Agencia de Seguridad Nacional de Estados Unidos, pero se filtró en una infracción desastrosa. EternalBlue aprovecha una vulnerabilidad de un protocolo de Windows en particular, lo que da total libertad a los hackers para ejecutar de forma remota su propio código en cualquier máquina sin revisar.
- **Pirateo por wifi o transmisor:** en 2015, los creadores de Jeep Cherokee se vieron obligados a retirar del mercado 1,4 millones de vehículos después de que unos investigadores demostraran que se podía piratear de forma remota el sistema de los coches a través de Internet; los atacantes podían tomar el control de las puertas, los frenos, el motor o las funciones de conducción autónoma del vehículo. De forma similar, la Administración de Alimentos y Medicamentos de Estados Unidos confirmó que determinados dispositivos cardiacos implantables tienen vulnerabilidades que podrían permitir a un hacker agotar la batería o administrar choques o ritmos incorrectos.
- **Vulnerabilidades en dispositivos IoT:** en octubre de 2016, el mayor ataque de DDoS de la historia desmontó grandes sitios de Internet (como Twitter, Netflix, Reddit y CNN) asaltando a un proveedor de servicios llamado Dyn. La botnet empleada en el ataque constaba de un gran número de dispositivos conectados a Internet, como impresoras, cámaras digitales, monitores de bebés y routers de consumidores, infectados por un malware llamado Mirai.
- **Vulnerabilidades en otros dispositivos:** ¿qué pasaría si alguien restableciera los ajustes de fábrica de todos los routers, firewalls y puntos de acceso inalámbricos u otros ajustes? ¿O si los pirateara para determinados propósitos? En 2018, el FBI animó a los consumidores a reiniciar sus routers para ayudar a interrumpir la difusión de un malware llamado VPNFilter, que los investigadores creen que utiliza un grupo vinculado a la inteligencia militar rusa para iniciar ciberataques coordinados contra Ucrania. Desde entonces, se ha ido actualizando el malware para poder sobrevivir a estos reinicios; ya se ha avisado a todo aquel que use cualquiera de los más de 70 dispositivos vulnerables para actualizar el firmware enseguida.[1]

Difusión en la red y daños

Una vez que el malware se infiltra, se expande desde la máquina infectada hasta otros ordenadores de la red. Una técnica tiene que ver con una vulnerabilidad llamada Mimikatz, que permite a los hackers recopilar las

1 Para obtener más información, puede leer el informe inicial de Cisco Talos sobre VPNFilter y la entrada del blog en la que se actualiza la lista de dispositivos afectados. Sin embargo, asegúrese de buscar la información más actualizada con su motor de búsqueda favorito u otras opciones de investigación.

credenciales de la memoria de un ordenador y usarlas para acceder a otros equipos. En ocasiones, los hackers triunfan recopilando credenciales de administrador con privilegios y credenciales de usuarios corrientes. En organizaciones que carecen de la adecuada segmentación de la red y otros perímetros de seguridad, el malware puede extenderse rápidamente, y los atacantes más activos pueden realizar movimientos laterales con mucha más facilidad. Gracias a las tácticas sigilosas y a la falta de supervisión continua y alertas, pueden pasar a menudo desapercibidos.

Luego, se desarrolla la parte principal del ataque. A menudo, el objetivo es borrar datos específicos o todo el sistema de archivos. Para borrar los datos, algunos ataques sobrescriben archivos enteros pero, como eso lleva mucho tiempo, otros ataques toman atajos que pueden resultar igual de efectivos. Por ejemplo, un ataque puede sobrescribir un bloque de 500 bytes por cada par de megabytes, o simplemente sobrescribir los primeros X bytes de un archivo, lo que borra la información del encabezado. En cualquier caso, la técnica inutiliza el archivo aunque no lo borre por completo. Asimismo, hay malware destructivo que ataca el subsistema de arranque (BIOS), así como malware diseñado para deshabilitar servicios.

A menudo, un ataque se activa cuando el malware llega a un punto de saturación para limitar la capacidad de la víctima para detectar el ataque a tiempo y defenderse. Para evitar dejar una firma de E/S que pueda detectarse más fácilmente, el malware deja la parte más difícil para el cargador de arranque. Además, a menudo se programan los ataques de forma que causen el mayor daño posible. Tanto NotPetya como Shamoon se desencadenaron mientras muchos empleados estaban fuera para preparar fiestas nacionales o religiosas, lo que limitó las posibilidades de detectar el ataque de inmediato y la capacidad de respuesta de las víctimas.

ESTRATEGIAS DE PREVENCIÓN Y DETECCIÓN

Dado que cualquier organización puede ser objetivo de un ataque destructivo o simplemente un daño colateral de un ataque dirigido a otra persona, todas las empresas deben seguir los pasos para mitigar los riesgos. El primer paso es implementar las prácticas recomendadas de seguridad estándar para evitar que los atacantes obtengan acceso a la red, limitar su alcance y su capacidad de realizar movimientos laterales si obtienen acceso, y detectar su actividad maliciosa. Estas son algunas de las mejores estrategias:

- Asignar permisos basados estrictamente en el principio de privilegios mínimos.
- Usar un modelo de seguridad por niveles para separar a los usuarios privilegiados de los usuarios empresariales normales, como el Enhanced Security Administrative Environment (ESAE) de Microsoft, a veces conocido como el modelo "Red Forest".
- No ejecutar código de no confianza.
- No ejecutar software sin actualizar y estar al tanto de las revisiones.
- Aplicar cambios en el entorno y utilizar herramientas que permitan evitar cambios en los objetos más importantes, como los grupos más privilegiados.
- Supervisar de cerca los cambios de configuración y otros cambios en el sistema, y vigilar operaciones poco comunes, como comandos que puedan alterar particiones de arranque o hacer caer un sistema.
- Supervisar la actividad de los usuarios, sobre todo, la actividad de las cuentas privilegiadas. Lo ideal es utilizar una herramienta que cree una referencia de actividad normal y que busque anomalías y las analice en contexto para minimizar el aluvión de alertas mientras detecta rápidamente las amenazas reales.
- Automatizar las respuestas. Los ataques modernos se desarrollan en cuestión de segundos, de modo que no se puede permitir estar satisfecho con un panel en su centro de operaciones de seguridad; en el momento en que un ser humano detecta un problema, lo investiga y toma alguna medida, ya está hecho el daño. Por ello, la automatización y la organización de la seguridad resultan esenciales.

ESTRATEGIAS DE RECUPERACIÓN ANTE DESASTRES

Aunar potentes estrategias de protección y detección resulta crucial, pero no suficiente en absoluto. En muchos de los ataques que se han descrito con anterioridad, las víctimas fueron criticadas con motivo por no haber implementado elementos básicos para la seguridad; por ejemplo, en el momento del ataque de NotPetya en 2017, algunos de los servidores de Maersk seguían disponiendo de Windows 2000, para el que Microsoft dejó de ofrecer soporte en 2010. Además, el insuficiente trabajo de segmentación de la red de Maersk permitió al malware expandirse fácilmente desde el punto inicial por toda la red.

Las potentes técnicas de protección y detección son cruciales, pero no suficientes; también se necesita una estrategia completa de recuperación ante desastres.

Si sufre algún ataque catastrófico y tiene solo herramientas nativas disponibles, prepárese para un proceso de restauración de bosques largo, complicado y propenso a errores.

Sin embargo, recuerde que Maersk no hizo nada mal como para infectarse. El malware se liberó mediante un paquete de software de contabilidad fiscal estándar que utilizaban casi todas las empresas de Ucrania. Varias organizaciones sufrieron devastadores daños en el ataque y, al igual que Maersk, la mayoría de ellas no eran los objetivos previstos del ataque, sino meros daños colaterales.

La lección está clara: aunque su organización piense que no tiene enemigos e implementa todas las prácticas recomendadas de seguridad que recomiendan los expertos, no puede garantizar que no será víctima de un ataque destructivo. Por ello, es fundamental disponer de una estrategia evaluada y demostrada de recuperación ante desastres.

Maersk no tenía ninguna y se salvó de pura casualidad. Cuando NotPetya desmontó los 150 controladores de dominios, nadie pudo encontrar un backup. Si la empresa no podía restablecerlos, estaba condenada al fracaso. Sin embargo, gracias a un corte eléctrico local, un solo controlador de dominio en Ghana resultó estar desactivado en el momento del ataque, lo que acabó salvando a la empresa. Por desgracia, el ancho de banda en la oficina de Ghana era tan lento que se habría tardado días en cargar los datos desde el controlador de dominio, y nadie allí disponía de un visado británico, de modo que el equipo de recuperación tuvo que hacer lo imposible por trasladar el preciado equipo a la sede de la empresa en Reino Unido en un tiempo récord. Finalmente, fueron capaces de usar la máquina para recompilar los otros controladores de dominios.

Confiar en una "estrategia" improvisada de recuperación ante desastres es algo muy común, pero también muy arriesgado. Como hemos visto, el ataque a VFEmail casi destruye la empresa, que sigue aferrada a la vida solo porque se consiguió salvar algunos de sus servidores de backup. Este caso es especialmente irónico, dado que el servicio que estableció como respuesta al virus ILoveYou que se expandió por correo electrónico en 2001 y uno de los puntos de venta clave era su capacidad para detectar spam y malware. Asimismo, resulta especialmente triste, dado que VFEmail había sufrido varios ataques potentes de DDoS con los años, pero parece que no se los tomaron lo suficientemente en serio.

Herramientas nativas

Si sufre algún ataque catastrófico y tiene solo herramientas nativas disponibles, prepárese para un proceso de restauración de bosques largo, complicado y propenso a errores.

Dado que los bosques de Active Directory son complejos y tienen numerosas interconexiones entre los controladores de dominios, la recuperación de un bosque de Active Directory resulta todo un desafío. Entre otras cosas, se debe:

- Reconstruir servicios de Active Directory
- Limpiar metadatos
- Restablecer confianzas
- Restablecer cuentas
- Reiniciar la replicación

Todas estas tareas incluyen complejos procedimientos que se deben realizar correctamente; omitir un paso o alterar el orden puede hacer que falle todo el proceso. Intentar llevar a cabo la recuperación de un bosque de forma manual solo con herramientas nativas con el estrés de un fallo catastrófico y la dirección vigilando de cerca es una tarea poco envidiable.

Si quiere ver con sus propios ojos lo duro que es, consulte la guía de recuperación de bosques de Active Directory de Microsoft, que ofrece una plantilla para la recuperación de un bosque de Active Directory si un fallo en todo el bosque hace que todos los controladores de dominios del bosque dejen de funcionar con normalidad.[2] Este es un resumen de los pasos de alto nivel que se deben seguir tras determinar que es necesario llevar a cabo una recuperación de bosques:

1. **Determinar cómo recuperar el bosque:** para prepararse para la recuperación, Microsoft recomienda determinar primero la estructura actual del bosque, identificar las funciones que realiza cada controlador de dominio, decidir qué controlador restaurar para cada dominio y garantizar que todos los controladores grabables están off-line.

   Tenga en cuenta que Microsoft ha calculado unos 12 minutos para la lectura rápida de este paso de preparación; la descripción de cada paso secundario tiene una extensión de, como mínimo, una página.

2 La guía de recuperación de bosques de Active Directory de Microsoft se encuentra disponible en https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/manage/ad-forest-recovery-guide.

2. **Llevar a cabo la recuperación inicial (un controlador en cada dominio):** a un alto nivel, estos pasos son para restaurar el primer controlador de dominios grabable en cada dominio; vuelva a conectar a la red cada controlador grabable restaurado y añada el catálogo global a un controlador de dominios en el dominio raíz del bosque.

   Completar solo el primer paso (restaurar el primer controlador de dominio) requiere 13 pasos secundarios independientes, algunos de los cuales incluyen procedimientos de varios pasos que Microsoft documenta por separado. Por ejemplo, debe crear una red aislada, captar roles principales de operaciones, aumentar el valor del grupo RID disponible y eliminar los datos de Active Directory de cualquier controlador de dominios no restaurado a partir de la backup.

3. **Volver a implementar otros controladores de dominios en el bosque:** Una vez que tenga un bosque estable con un controlador de dominio por cada dominio y un catálogo global en el bosque, ya podrá empezar a implementar de nuevo otros controladores en el bosque instalando DS de Active Directory.

4. **Realizar una limpieza:** una vez recuperado todo el bosque, debe volver a poner en marcha a los usuarios y aplicaciones de línea de negocio. Entre otras cosas, debe volver a configurar la resolución de nombres (DNS) y determinar qué cambios pueden haberse producido entre la hora de la backup y la hora del desastre, así como volver a aplicarlos.

Además de ser complejos y extremadamente sensibles a los errores humanos, todos estos pasos pueden conllevar muchísimo tiempo. De hecho, Microsoft reconoce que la "velocidad de recuperación no es el objetivo principal" de su guía. En la sección de preguntas frecuentes pertinente se indica que se pueden realizar la mayoría de los pasos de recuperación de bosques mediante herramientas de línea de comandos, de modo que es posible escribir scripts para ayudar a automatizar partes del proceso de recuperación de bosques. Sin embargo, Microsoft advierte que hay que evaluar exhaustivamente los scripts antes de usarlos en una recuperación real, y que se deben actualizar cada vez que se hagan cambios en el entorno de Active Directory, como añadir un nuevo dominio o incluso un nuevo controlador de dominio, o actualizar a una nueva versión de Active Directory.

Recovery Manager for Active Directory – Disaster Recovery Edition

Afortunadamente, existen herramientas que automatizan el proceso de recuperación de bosques, de manera que puede volver a poner en marcha su organización más rápido y con menos esfuerzo y riesgos. Recovery Manager for Active Directory – Disaster Recovery Edition de Quest® le ayudará a implementar una estrategia completa de recuperación y backup para llevar a cabo recuperaciones rápidas a partir de cualquier desastre en un objeto, atributo, directorio y sistema operativo en todo el bosque de Active Directory. De hecho, su funcionalidad de recuperación automatizada puede reducir el tiempo de recuperación a partir de un desastre de Active Directory de nivel de controlador de dominio hasta un 95 %.

On Demand Recovery de Quest amplía la backup y recuperación de Active Directory en un objeto o atributo a la nube para que pueda proteger no solo los entornos locales, sino también las implementaciones híbridas. Con On Demand Recovery puede realizar backups y recuperar Azure AD y Office 365 de forma rápida y segura, ver los objetos solo de la nube y los objetos sincronizados mediante Azure AD Connect, ejecutar informes de diferencias entre la producción y las backups en tiempo real, y realizar restauraciones coordinadas tanto en Active Directory local como en Azure AD.

Implemente una estrategia completa de backup y recuperación en todo su entorno híbrido con Recovery Manager for AD y On Demand Recovery de Quest.

CONCLUSIÓN

Los ataques destructivos están en auge y sus efectos pueden ser devastadores. Todas las organizaciones son vulnerables, independientemente de si son un objetivo directo o un simple daño colateral. Tras el devastador ataque en VFEmail, su director ejecutivo y fundador, Rick Romero, tuiteó: "Nunca pensé que a alguien pudiera importarle tanto mi acto de amor que quiera destruirlo por completo". No cometa el mismo fallo.

Para mitigar el riesgo, implemente prácticas recomendadas de seguridad para bloquear los ataques, limitar su alcance y ayudar a garantizar una detección y respuesta inmediatas. Sin embargo, los expertos en seguridad y ataques del mundo real dejan claro que también se necesita una estrategia completa de recuperación ante desastres. Para obtener más información sobre cómo pueden ayudarle Recovery Manager for AD – Disaster Recovery Edition y On Demand Recovery, visite quest.com/products/recovery-manager-for-active-directory-disaster-recovery-edition y quest.com/products/on-demand-recovery.

ACERCA DE QUEST

Quest ofrece soluciones de software para el mundo de la TI empresarial que cambia rápidamente. Ayudamos a simplificar los retos que plantean la explosión de datos, la expansión de la nube, los centros de datos híbridos, las amenazas de seguridad y los requisitos normativos. Ofrecemos nuestros servicios de forma global a más de 130 000 empresas de 100 países, incluido el 95 % del Fortune 500 y el 90 % del Global 1000. Desde 1987, hemos creado una cartera de soluciones que ahora incluye la gestión de bases de datos, la protección de datos, la gestión de identidades y accesos, la gestión de la plataforma de Microsoft y la gestión unificada de puntos finales. Con Quest, las organizaciones dedicarán menos tiempo a la administración de TI y más a la innovación de sus negocios. Para obtener más información, visite www.quest.com.

Si tiene alguna duda sobre el uso que puede hacer de este material, póngase en contacto con nosotros:
www.quest.com