Uso de IBM Security QRadar EDR para monitorizar una cadena de suministro ataque altamente sofisticada contra un servicio administración de agua

Proteger infraestructura crucial

actor de amenaza apunta a un servicio administración de agua en Europa responsable de distribuir agua a cerca de un millón de personas.

El servicio inicialmente asume que la nuevo actividad es legítima.

Los atacantes administrar para comprometer servidores y desplegar medidas anti-forense basadas en ransomware.

La seguridad solicitar

Vulnerable posición como infraestructura crucial en cargo de distribución regional de agua

prestaciones de no detección y caza para amenazas sin archivo y movimientos lateral

Falta de protección ransomware

Recursos limitados asignado a seguridad de punto final

Los sitios infraestructura crítica deben adaptar continuamente al manejador de la creciente complejidad del riesgo cibernético y la creciente exposición a los actores amenaza sofisticados.

El tipo de recursos bajo administración fabricante infraestructura crucial un destino ideal para ataques de alto impacto y la exfiltración de datos confidenciales .

Aparte de las tradicionales herramientas análisis red , el servicio administración de agua no tenía punto final supervisión en colocar y sin respuesta prestaciones en mayúsculas y minúsculas de un ataque .

Sus herramientas no permitir el rastreo de operaciones cross-endpoint, como movimientos lateral .

Además, la carencia general de los recursos de TI significó que el operador contratara proveedores externo para administrar servicios esenciales como e\-mail , DNS, VPN y firewalls, lo que creó más complejidad en torno a la coordinación de los esfuerzos de varios proveedores dispares.

A

Limpié el segmento de red infectado en

evitando daños que podrían haber bloqueado servicio esencial a los ciudadanos

segundos

cerrado exitosamente la incidencia dentro de

sin pérdida de datos, interrupción de servicios esenciales o daños a terminales

7 días

El ataque involucró una docena de dispositivos antes de la etapa de despliegue ransomware y varios miles después de eso.

descripción general de la solución

IBM® Security QRadar EDR utiliza NanoOS, que está diseñado para ser indetectable y proporcionar un nivel excepcional de visibilidad a través de puntos finales e infraestructura

Rastrea de forma nativa los movimientos lateral y los intentos anómalos inicio de sesión

Proporciona protección nativo contra ataques ransomware

Ofrece una poderosa interfaz de caza amenaza para permitir el rastreo y reconstrucción de incidentes altamente complejo

El servicio administración de agua ejecutó software IBM Security QRadar EDR en todos los servidores, equipos de escritorio y portátiles del servicio para supervisar continuamente cada activo y monitorizar e investigar de inmediato posibles violaciones seguridad .

Empleando los motores dual de inteligencia artificial incorporado la solución y comportamiento detallado al análisis , el cliente obtuvo visibilidad completo sobre la infraestructura , lo que permitió consultas en tiempo real a los puntos finales y búsquedas extendidas para ambos indicadores de comprometer (IOC) e indicadores de comportamiento (IOB), juntos con data mining avanzado para descubrir amenazas latentes.

Seis meses después de despliegue , el agente QRadar EDR detectó actividad anómala inicial y rastreó a los atacantes en su trayecto para acceso a una información específico definido .

El software antivirus y sistema de detección de intrusiones (IDS) existente en el cliente no detectar ninguna actividad hasta el último estadio del ataque .

Si el cliente no desplegado QRadar EDR, los atacantes habrían logrado adquirir y exfiltrar los datos.

cadena de suministro ataque

El día de la infracción inicial , QRadar EDR marcó un inicio de sesión sospechoso desde un servidor VPN hacia un punto final en el segmento de red sin privilegios.

El equipo de seguridad asumió que el inicio de sesión se debió al trabajo mantenimiento de un proveedor de seguridad externo y, por lo tanto, asignado una prioridad baja a la incidencia .

Los atacantes desplegado programa malicioso inicial , utilizado principalmente para mapa el segmento de red buscando caminos directos a la red privilegiada.

Tras no hallazgo dichas vías disponible , los atacantes desplegado un segundo programa malicioso en memoria para recoger credenciales para su reutilización en posteriores movimientos lateral .

Con las credenciales obtenidas, los atacantes se dirigieron al controlador de dominio y poco después a un servidor de archivos que contenía documentos internos.

Raíz análisis de causas

El inicio de sesión anómalo inicial se produjo fuera del horario cambio , desde un punto final que suele interactuar con servidores pero no con estaciones de trabajo.

El canal VPN estaba gestionado por un proveedor externo que también se cargo de mantener el servidor de correo y los cortafuegos adición de la propia VPN.

Debido a la naturaleza del acceso , la alerta se mantuvo activo para monitorizar cada funcionamiento , pero en ese apuntar , el equipo de seguridad interno asignado una prioridad baja al suceso , asumiendo que el proveedor estaba ejecutando mantenimiento de la infraestructura .

Al día siguiente , QRadar EDR emitió una segundo alerta , mostrando la actividad de un programa malicioso utilizado para prueba de diagnóstico por la imagen del red interno, seguido de otra alerta señalización la presencia de un vector en memoria con registro de teclas y recopilación credencial . prestaciones

En ese apuntar , el equipo de seguridad se concentró en estos hechos, iniciando una sesión de caza amenaza mientras los atacantes finalmente lograban, a través de una serie de movimientos lateral , acceso a uno de los controladores dominio .

El equipo decidió aprovechar la invisibilidad de la tecnología NanoOS para seguir rastreo a los atacantes el largo posible para comprender el modus operandi y sus objetivos.

Como los atacantes intentaron alcanzar el servidor de archivos que contenía información confidencial , el equipo decidió detener e iniciar el plan erradicación .

Mientras se remediaban los varios dispositivos, los atacantes se dieron cuenta de que, a pesar del alto nivel de acceso , no podían acceso a la información que buscaban.

Al darse cuenta de que estaban cubierta , desplegado un ransomware en toda la infraestructura para cobertura sus huellas.

Ataque y reconstrucción

Una vez borrar las motivaciones del ataque , el operador necesitaba entender todo el ataque para reforzar los puntos débiles de la infraestructura .

El ataque involucró una docena de dispositivos antes de la etapa de despliegue ransomware y varios miles después de eso.

Los atacantes consiguieron acceso a la VPN y servidor de correo proveedor y los utilizaron como entrada inicial apuntar a la red interna.

Los atacantes reutilizaron las credenciales del proveedor para movimiento a otras máquinas, y finalmente se establecieron en una estación de trabajo específico .

En ese apuntar , utilizaron una cadena de herramientas para prueba de diagnóstico por la imagen el red interno e identificar objetivos para movimientos lateral .

En el estadio final, usaron el propio controlador de dominio para dispersar ransomware en todos dispositivo .

el proceso

El cliente automatizó el proceso limpieza utilizando módulo remediación de QRadar EDR, y utilizó la protección anti-ransomware de la solución para impedir pérdida de datos y disrupción operativo .

Desastre evitado: respuesta y remediación

El servicio administración de agua asegurado acceso VPN y realizó una sesión de caza amenaza que identificó cada máquina a la que los atacantes lograron acceso .

El módulo remediación QRadar EDR automatizó el proceso limpieza , y el segmento se limpió en asunto de segundos.

El servicio obtuvo todas herramientas utilizadas durante el reconocimiento y movimiento lateral estadio e inmediatamente propagó una política que incluía IOC y comportamientos en toda la infraestructura .

No se identificaron hosts comprometido adicionales después del despliegue de política .

Las credenciales se restablecido de inmediato para todos los usuarios, y el ataque de cibersecuestro no requirió mayor intervención porque el cliente habilitado protección anti- ransomware QRadar EDR para todos los dispositivos, evitando la pérdida de información importante y interrupción de las actividades normal .

El servicio cerrado con éxito la incidencia en el segundo día, sin pérdida de datos, interrupción de servicios esenciales o daños a los terminales.

Si el servicio no hubiera empleado QRadar EDR, los ataque seguramente habrían exfiltrado información confidencial y podrían haber permanecido activo durante un período prolongado, con toda la infraestructura eventualmente inhabilitado por el último ataque de cibersecuestro .

Tal ataque habría tenido una enorme repercusión en la capacidad de la instalación para seguir entregando servicios esenciales a los ciudadanos de la región , potencialmente agrupamiento en bloques por completo.

Dada la dificultad para identificar los ataques cadena de suministro , el servicio podría haber sido infracción nuevamente a través del mismo canal si no se hubiera disponible información forense para precisar la causa raíz de la vulneración .

© Copyright IBM Corporation 2023.

IBM Corporation, IBM Security , New Orchard Road, Armonk, Nueva York 10504

Producido en los Estados Unidos de América, junio de 2023.

IBM , el logotipo de IBM , IBM Security y QRadar son marcas comerciales o marcas comerciales registrado de International Business Machines Corporation , en los Estados Unidos y/o en otros países.

Otros nombres producto y servicio pueden ser marcas comerciales de IBM o de otras empresas.

Una lista actual de IBM marca registrada está disponible en ibm.com/marca marca comercial .

Este documento es actual a la fecha inicial de publicación y puede ser modificado por IBM en cualquier tiempo .

No todas las ofertas están disponible en todos país en los que opera IBM .

Todos los ejemplos cliente citados o descritos se presentan como ilustraciones de la forma en que algunos clientes han utilizado los productos IBM y los resultados que pueden haber logrado.

Los costos ambientales reales y las características rendimiento variar dependiendo de las configuraciones y condiciones persona cliente .

Por lo general, no se pueden proporcionar los resultados esperados, ya que los resultados de cada cliente dependerán completamente de los sistemas y servicios solicitados por el cliente.

LA INFORMACIÓN EN ESTE DOCUMENTO SE PROPORCIONA "TAL CUAL" SIN NINGUNA GARANTÍA, EXPLÍCITA O IMPLÍCITA, INCLUYENDO NINGUNA GARANTÍA DE COMERCIABILIDAD, IDONEIDAD PARA UN FIN DETERMINADO Y CUALQUIER GARANTÍA O CONDICIÓN DE NO VIOLACIÓN.

Los productos IBM están garantizados de acuerdo con los términos y condiciones de los acuerdos bajo los cuales se proporcionan.

Declaración de Buenas Prácticas de Seguridad: Ningún sistema o producto de TI debe considerarse completamente asegurar , y ningún único producto , servicio o medida de seguridad puede ser completamente efectivo para prevenir utilizar o acceso inadecuado .

IBM no garantía que ningún sistema, producto o servicios sea inmune, ni fabricante de su empresa será inmune a la conducta malicioso o no permitido de cualquier parte .

Sobre el servicio administración de agua

Este servicio administración agua en Europa se encarga del manejo y distribución de agua a cerca de un millón de personas.

El servicio se clasificado como infraestructura crucial y servicios esenciales.

componente de la solución

IBM® Security QRadar EDR

Uso de IBM Security QRadar EDR para monitorizar una cadena de suministro ataque altamente sofisticada contra un servicio administración de agua

Uso de IBM Security QRadar EDR para monitorizar una cadena de suministro ataque altamente sofisticada contra un servicio administración de agua

Infraestructura crítica

rspencer@us.ibm.com

Un servicio administración de agua en Europa utiliza IBM Security QRadar EDR para remediar ciberataques que de otro modo podrían haber bloqueado servicio esencial a 1 millón de ciudadanos

La seguridad cibernética

Infraestructura crítica

Gestión de usuarios

Europa

piratas informáticos

programa malicioso

ransomware

remediación

resolución

resistencia

Automatización

IBM

QRadar

punto final detección y respuesta

EDR

© Copyright IBM Corporation 2023.

IBM Corporation, IBM Security , New Orchard Road, Armonk, NY 10504 Producido en los Estados Unidos de América, junio de 2023 IBM , el logotipo de IBM , IBM Security y QRadar son marcas comerciales o marcas comerciales registrado de International Business Machines Corporation , en los Estados Unidos y/u otros países.

Otros nombres producto y servicio pueden ser marcas comerciales de IBM o de otras empresas.

Una lista actual de IBM marca registrada está disponible en ibm.com/marca marca comercial .

Este documento es actual a la fecha inicial de publicación y puede ser modificado por IBM en cualquier tiempo .

No todas las ofertas están disponible en todos país en los que opera IBM .

Todos los ejemplos cliente citados o descritos se presentan como ilustraciones de la forma en que algunos clientes han utilizado los productos IBM y los resultados que pueden haber logrado.

Los costos ambientales reales y las características rendimiento variar dependiendo de las configuraciones y condiciones persona cliente .

Por lo general, no se pueden proporcionar los resultados esperados, ya que los resultados de cada cliente dependerán completamente de los sistemas y servicios solicitados por el cliente.

LA INFORMACIÓN EN ESTE DOCUMENTO SE PROPORCIONA "TAL CUAL" SIN NINGUNA GARANTÍA, EXPLÍCITA O IMPLÍCITA, INCLUYENDO NINGUNA GARANTÍA DE COMERCIABILIDAD, IDONEIDAD PARA UN FIN DETERMINADO Y CUALQUIER GARANTÍA O CONDICIÓN DE NO VIOLACIÓN.

Los productos IBM están garantizados de acuerdo con los términos y condiciones de los acuerdos bajo los cuales se proporcionan.

Declaración de Buenas Prácticas de Seguridad: Ningún sistema o producto de TI debe considerarse completamente asegurar , y ningún único producto , servicio o medida de seguridad puede ser completamente efectivo para prevenir utilizar o acceso inadecuado .

IBM no garantía que ningún sistema, producto o servicios sea inmune, ni fabricante de su empresa será inmune a la conducta malicioso o no permitido de cualquier parte .