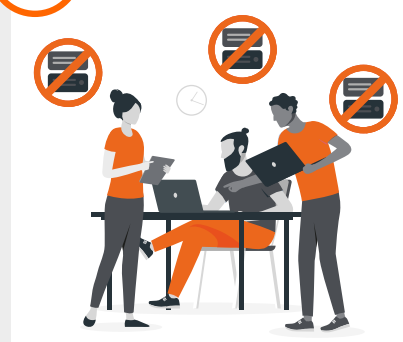
Eventos de *software* vulnerable

Muchas pérdidas pueden evitarse parcheando el *software* vulnerable antes de que los ciberdelincuentes tengan la oportunidad de explotarlo. Los ejemplos de pérdidas que figuran a continuación ponen de manifiesto la importancia de mantener actualizado el *software*, y detallan el proceso de investigación para evaluar cómo se aprovechan las vulnerabilidades conocidas y se ajustan las pérdidas resultantes.

- Alerta sobre la vulnerabilidad de los servidores

1



1. El evento

El 16 de julio, el equipo de IT de la Empresa 'Ejemplo' recibió una llamada de ventas externas para informarles de que no podían utilizar ningún sistema. Las estadísticas del servidor monitorizado mostraban que muchos sistemas se habían caído. Durante una investigación inicial, el equipo de IT descubrió un mensaje que indicaba que los servidores estaban cifrados. Llegaron a la conclusión de que la empresa había sido víctima de un ataque de *ransomware*. El equipo de IT de la Empresa 'Ejemplo' se puso en contacto con el Centro de Respuesta a Incidentes Cibernéticos de Chubb y se contrató a un gestor de incidentes y a expertos en informática forense para respaldar la investigación.

La inspección inicial de los sistemas reveló que el autor del ataque había comprometido varias partes de la red y la infraestructura.

2

2. El problema

En respuesta, la Empresa 'Ejemplo' contuvo rápidamente el ataque desactivando los servidores. Pero, para entonces, el autor del ataque ya había cifrado los servidores virtualizados y los hipervisores de los centros de datos de la empresa. Al evaluar las opciones de recuperación, descubrieron que era posible restaurar completamente el entorno informático utilizando las copias de seguridad, ya que el autor del ataque no pudo cifrarlas ni dañarlas. La estrategia de las copias de seguridad de la Empresa 'Ejemplo' se había actualizado, en los 12 meses anteriores para proteger mejor su IT de los ataques de *ransomware*, manteniendo copias de seguridad de almacenamiento *offline* y conservando la autenticación en servidores de las copias de seguridad independientes al Active Directory.

A partir del día siguiente, investigadores informáticos y expertos forenses ayudaron a la Empresa 'Ejemplo', evaluando la situación y comunicándose con el autor del ataque, al tiempo que daban prioridad a la recuperación de los activos. En paralelo, investigaron desde el punto de vista forense la causa principal y el impacto del incidente para apoyar una recuperación segura. Además, se investigó si el autor del ataque había filtrado datos para la extorsión posterior y se comprobó la naturaleza y la cantidad de datos, según se afirmaba en la nota de rescate.

Al revisar los datos de registro dentro de las copias de seguridad, estos mostraron que, el 19 de junio, casi un mes antes, el autor del ataque inició sesión desde 6X.XXX.XX.232 en un servidor SSL-VPN alojado en Europa con credenciales pertenecientes a la cuenta «Fred.Bloggs». El servidor VPN se gestionaba localmente y ejecutaba la versión 6.2.0-vr, que no estaba actualizada. Este inicio de sesión se originó desde una IP conocida por ser un nodo de salida de TOR, lo cual era sospechoso, ya que normalmente un usuario no iniciaría sesión utilizando la red TOR. El autor del ataque volvió a autenticarse unos 25 minutos después, esta vez utilizando una IP geolocalizada en un país en el que la Empresa 'Ejemplo' no operaba.

El autor del ataque aumentó sus privilegios de acceso menos de una hora después al obtener acceso a una cuenta de administrador de dominio. Pudo hacerlo porque las credenciales de esta cuenta estaban almacenadas en un archivo de configuración en cada dispositivo Windows conectado al dominio. Esto permitió al autor moverse lateralmente entre los servidores e hipervisores ubicados en el Reino Unido y Alemania que soportaban las operaciones europeas de Empresa Ejemplo.

En julio, el autor del ataque creó persistencia instalando *software* de acceso remoto y una herramienta de distribución de *software*. Esto le permitió desplegar y propagar el *ransomware* a todos los servidores del dominio. Afortunadamente, los puntos finales —es decir, los portátiles y las estaciones de trabajo— consiguieron bloquear el *ransomware* a través de un agente antivirus avanzado que no se ejecutaba en los servidores.

Al no haber registros que mostraran intentos fallidos de inicio de sesión desde la cuenta «Fred.Bloggs», se determinó que el autor del ataque tenía credenciales válidas y que no había realizado un ataque de fuerza bruta. Los registros también muestran actividad de código del autor del ataque explotando una vulnerabilidad conocida (CVE-2022-123XXX) dentro del *software* VPN, versión 6.2.0-vr. La vulnerabilidad, cuando se explota, permite a un usuario obtener credenciales válidas utilizadas recientemente. El autor del ataque confirmó este método de entrada en la nota de rescate y durante las negociaciones.

3

3. La solución

Tras confirmar que las copias de seguridad no estaban afectadas por el *malware*, los esfuerzos de recuperación de datos y sistemas, así como el trabajo de configuración actualizada continuaron durante los cinco días siguientes. Estos esfuerzos lograron su objetivo, por lo que no hubo necesidad de negociar más con el autor del ataque y no se abonó rescate alguno.

Según se indica en la Base de Datos Nacional de Vulnerabilidades y en el sitio web de soporte del proveedor del *software* VPN, se descubrió una vulnerabilidad crítica en la versión 6 del *software*. Esto permitía el robo de credenciales y la entrada en el sistema, y se identificó por primera vez en enero de este año. Recibió una calificación de criticidad en el Sistema Común de Puntuación de Vulnerabilidades (CVSS) de 9,8 y se le asignó el identificador CVE-2022-123XXX. El proveedor de *software* creó un parche para estas vulnerabilidades el 2 de febrero (versión 6.2.1-vr), y ese mismo día envió un correo electrónico a sus clientes, entre ellos a la Empresa 'Ejemplo', aconsejando a los usuarios que aplicaran el parche lo antes posible.

4

4. El resultado

La Empresa 'Ejemplo' tuvo 137 días entre la publicación del parche y el momento en que se explotó la vulnerabilidad. Las cláusulas de respuesta al incidente, costes de recuperación de datos y sistemas, extorsión cibernética y las pérdidas por interrupción de negocio se activaron inicialmente en respuesta al incidente cibernético, con sujeción a los límites, franquicia y coaseguro aplicables al suceso de *software* desatendido que se detallan en el suplemento de la Póliza durante 137 días.

A continuación, Chubb ajustó el siniestro según el método estándar, revisando los costes de respuesta al incidente para el Gestor de Respuesta a Incidentes, los expertos forenses informáticos, los abogados y los especialistas en relaciones públicas, las pérdidas por interrupción de la actividad, los costes de recuperación de datos y sistemas, y los gastos de extorsión cibernética.

Eventos de *software* vulnerable

- Vulnerabilidad conocida, no parcheada

1

1. El suceso

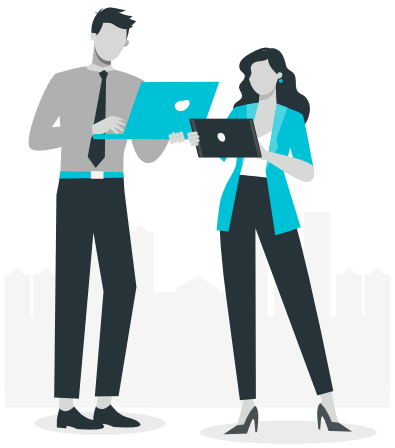
Un fin de semana, la Empresa 'Ejemplo' detectó un acceso no autorizado a sus sistemas informáticos y servidores. El acceso se obtuvo a través de una vulnerabilidad conocida, grave y común, que permitió a los ciberdelincuentes acceder a los sistemas informáticos de la Empresa 'Ejemplo', a sus servidores y a los datos que contenían. Los ciberdelincuentes cifraron los sistemas y filtraron los datos.

2

2. El problema

Con los servidores caídos, la Empresa 'Ejemplo' fue incapaz de procesar o atender los pedidos de sus clientes. Los empleados calcularon que, por cada 24 horas de inactividad de los servidores, la empresa perdería 750 000 euros de beneficios. El ciberdelincuente exigió un rescate de 2 millones de dólares a cambio de facilitar las claves de descifrado y no publicar los datos filtrados, con la amenaza de aumentar el rescate periódicamente si no recibía el pago.

3



3. La solución

La Empresa 'Ejemplo' notificó el incidente en cuanto lo descubrió y contrató rápidamente a un Gestor de Respuesta a Incidentes, que pudo clasificar el incidente basándose en los hechos iniciales. El Gestor de Respuesta a Incidentes recurrió inmediatamente a una empresa especializada en informática forense para que ayudara a la Empresa 'Ejemplo' en la investigación y la contención.

El equipo de respuesta a incidentes ayudó además a la Empresa 'Ejemplo'. Rápidamente contrataron abogados, personal de relaciones públicas y especialistas en extorsión. A continuación, el equipo puso en marcha una estrategia de mitigación que incluía la identificación de servidores que pudieran restaurarse a partir de copias de seguridad.

Finalmente, no se pagó ningún rescate, ya que el equipo de IT y los especialistas en extorsión determinaron que los datos filtrados no eran confidenciales. Descubrieron que los sistemas podían restaurarse en gran medida a partir de copias de seguridad segregadas de forma segura que no se habían visto afectadas por el incidente.

El equipo de respuesta a incidentes ayudó a eliminar el *ransomware* de los servidores afectados y a restaurar los sistemas, incluido el parche que habría evitado la explotación de la vulnerabilidad conocida. El equipo de relaciones públicas colaboró en las comunicaciones a los clientes y los abogados ayudaron a la Empresa 'Ejemplo' a cursar notificación a los organismos legales y reguladores correspondientes.

4

4. El resultado

Finalmente, las operaciones se restablecieron por completo. El equipo forense de IT proporcionó un informe 10 días después del incidente que explicaba el método por el que se obtuvo el acceso, la CVE específica relacionada con la vulnerabilidad y la mitigación recomendada, incluida la fecha en la que los parches estaban disponibles, pero no se implementaron.

Las cláusulas de respuesta al incidente, costes de recuperación de datos y sistemas, extorsión cibernética y las pérdidas por interrupción de negocio se activaron inicialmente, en respuesta al incidente cibernético. Sin embargo, el incidente se debió a una vulnerabilidad conocida que fue explotada. El informe forense de IT confirmó este extremo y constató la disponibilidad de un parche en el momento del incidente, que no se había implementado. El informe detallaba exactamente cuándo accedió el ciberdelincuente al sistema y destacaba el tiempo que los sistemas de la Empresa 'Ejemplo' llevaban sin parchearse. Esto les permitió aplicar el coaseguro y el sublímite correctos con arreglo a los límites de evento de *software* vulnerable.