ENCRYPT 4.0

Iniciativa conjunta de desarrollo de la mano de obra cibernética para permitir que la industria europea supere la escasez de profesionales de la ciberseguridad

No. 2020-1-RO01-KA202-079983

O3: Revisión de casos de estudio sobre ciberataques

Cofinanciado por el programa Erasmus+ de la Unión Europea

CONTENIDO

INTRODUCCIÓN

Con la llegada de las tecnologías de la información (TI) y el auge de la cuarta revolución industrial, las empresas se enfrentan a nuevos retos relacionados con la ciberseguridad y la protección de datos. Esto es especialmente relevante para las pymes industriales, que a menudo no disponen de los recursos internos y la capacidad para evaluar eficazmente los riesgos de ciberseguridad asociados a las tecnologías recientemente implementadas basadas en la Industria 4.0. Al mismo tiempo, las pymes se convierten con mayor frecuencia en víctimas de diversos ciberdelitos. Según el último informe Verizon 2021 Data Breach Investigations Report *(Verizon, 2021)*, las pymes son víctimas y mucho más vulnerables a los ciberataques en comparación con las grandes empresas, ya que carecen de recursos, personal, información y capacidad en general para evitar los riesgos de un ciberataque.

Mientras tanto, las ciberamenazas tienen diversas fuentes y son cada vez más complejas, por ejemplo, y si los equipos no han experimentado vulnerabilidades similares y carecen de una orientación clara sobre cómo responder a ellas, pueden tardar días e incluso semanas en reaccionar adecuadamente, lo que puede ser fatal para algunos procesos de fabricación. Según el 2021 SMB IT Security Report, los empleados que no siguen las directrices se consideran el principal obstáculo para la ciberseguridad y esta tendencia se ha agravado con el aumento del trabajo a distancia, debido a la pandemia de COVID-19 (Untangle, 2021). No obstante, cuando se produce un fallo de ciberseguridad, no sólo afecta a las personas, sino que también puede causar pérdidas financieras, de confianza de los clientes y perjudicar a la reputación de la empresa (Acronis, 2021).

Teniendo en cuenta lo anterior, el consorcio del proyecto Encrypt 4.0 ha elaborado este documento para que sirva de herramienta de conocimiento, permitiendo realizar un análisis crítico de ciberataques reales y lecciones aprendidas de los mismos, así como hojas de ruta sobre cómo prevenirlos, identificarlos, abordarlos y recuperarse de ellos.

El presente documento está específicamente adaptado a las necesidades de las pymes industriales de la UE que operan en el contexto de la Industria 4.0, y representa una recopilación de casos de estudio sobre ciberataques que tiene como objetivo apoyar a las pymes para potenciar su ciberseguridad y prevenir los ciberataques.

ESTRUCTURA Y METODOLOGÍA

La revisión de casos de estudio de Encrypt 4.0 contiene un total de **18 casos de estudio**. Cada uno de los socios del proyecto ha preparado 3 estudios de casos reales de ciberataques basados en la investigación documental, la experiencia y las observaciones personales y las entrevistas en profundidad con directores generales, profesionales de la ciberseguridad y especialistas en TI, que abarcan varios tipos de ciberataques y ofrecen un análisis crítico de las razones de las violaciones de seguridad, cómo se abordaron y cuáles fueron las consecuencias.

El consorcio de ENCRYPT 4.0 ha construido un modelo específico "PREVENIR-IDENTIFICAR-RESPONDER-RECUPERAR" (PIRR) basado en el modelo "Identificar, Proteger, Detectar, Responder y Recuperar" del Instituto Nacional de Normas y Tecnología (NIST). La tipología de los ciberataques se basa en el modelo STRIDE[1] así como en el marco MITRE ATT&CK. El análisis del

[1] Para leer más acerca del model STRIDE:

modelo PIRR contiene 4 categorías/secciones principales basadas en los más importantes pasos para combatir un problema de ciberseguridad, así como secciones de lecciones aprendidas (véase la Fig. 1).

Fig. 1. "Prevenir – Identificar – Responder – Recuperar" (PIRR) categorías del modelo

Benjamin, P., 2018. Demystifying STRIDE Threat Models [online]. DEV Community. Available at: https://dev.to/pbnj/demystifying-stride-threat-models-230m;

PREVENIR

Esta sección se centra en la reducción del riesgo de exposición a los ciberataques y en las medidas preventivas, y para cada caso de estudio se incluye lo siguiente:

- Prácticas específicas de seguridad que tuvieron efectos demostrados en ciberataques reales;
- Conceptos erróneos de ciberseguridad: prácticas que las empresas aplicaron y tuvieron un impacto nulo o incluso negativo en incidentes reales.

IDENTIFICAR

El objetivo principal de esta sección es ayudar a las pymes a distinguir entre los diferentes tipos de ataques cibernéticos categorizados utilizando el modelo STRIDE y el marco MITRE ATT&CK. El modelo STRIDE representa un modelo de amenazas de alto nivel centrado en el sistema y en identificar categorías generales de ataques. Tiene las siguientes 6 categorías:

+Spoofing (suplantación de identidad)

+Tampering (alteración)

+Repudiation (repudio)

+Information disclosure (revelación de la información)

+Denial of service (denegación de servicio)

+Elevation of privilege (elevación de privilegios)

En los casos prácticos de ENCRYPT 4.0, se utilizó STRIDE para identificar las amenazas en un nivel superior, mientras que se aplicó el marco MITRE ATT&CK para especificar los ataques con más detalle. El marco ATT&CK toma el punto de vista de un atacante para ayudar a las organizaciones a comprender cómo abordan, se preparan y ejecutan con éxito los ataques.

RESPONDER

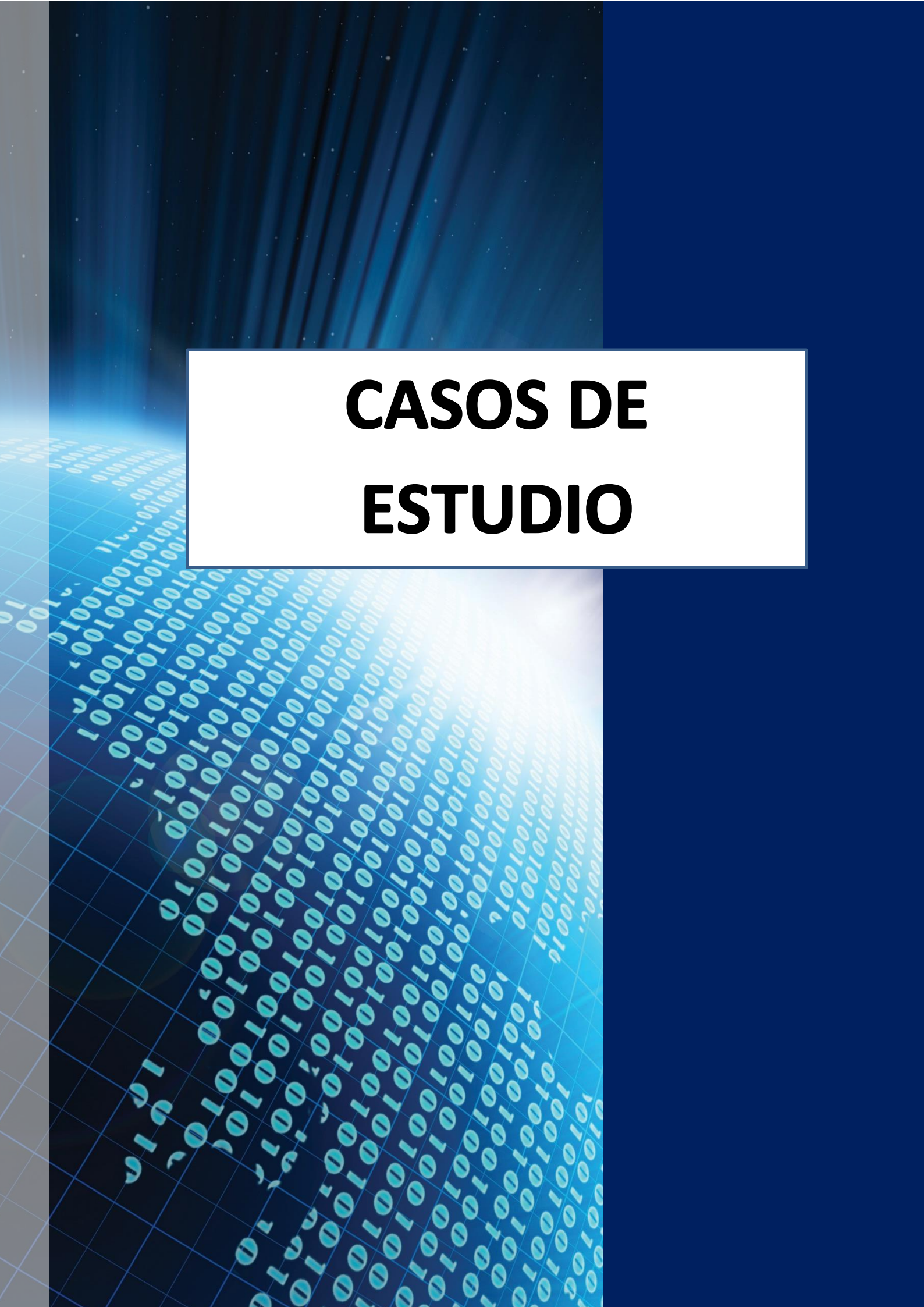
Esta sección describe las situaciones en las que la amenaza ya está presente, brindando análisis de ciberataques reales y consejos sobre cómo reaccionar en casos similares después de identificarlos.

Los ciberataques dentro de los casos prácticos se describen en el siguiente formato:

- QUIÉN: el atacante
- A QUIÉN: la organización objetivo
- POR QUÉ: los motivos detrás del ataque (fue aleatorio o dirigido)
- QUÉ: la propiedad objetivo
- CÓMO: descripción del ataque y cuáles fueron las técnicas utilizadas.
- ESTRATEGIA: cómo se abordó la amenaza y las medidas que tuvieron un efecto nulo o negativo.

RECUPERAR

La sección proporciona información sobre cuáles fueron las consecuencias del ataque, así como un análisis sobre cómo realizar una recuperación del sistema después de que algunos procesos se hayan dañado y recuperar el acceso a los datos que se perdieron, en base a los casos reales de ataque descritos en la sección RESPONDER. La sección sigue los modelos STRIDE MITRE ATT&CK que describen las prácticas de recuperación basadas en cada grupo específico de ciberamenazas presentado en la sección IDENTIFICAR.


CASOS DE
ESTUDIO

CASO DE ESTUDIO 1: LA SHELL INVERSA

LA ORGANIZACIÓN OBJETIVO

Asociación Innovalia es un centro tecnológico privado e independiente que fue creado por el Grupo Innovalia con el fin de articular una masa crítica capaz de alcanzar con éxito sus ambiciones de investigación a largo plazo y sus objetivos estratégicos. Innovalia es una alianza de pymes de base tecnológica con sede en España. Tiene presencia internacional con oficinas en País Vasco, Madrid, Cataluña, Canarias, Europa, Asia, Oriente Medio, Centro y Sudamérica. Desde su fundación, la Asociación Innovalia ha desarrollado una especial sensibilidad y conocimiento de las características particulares de las pymes de base tecnológica. Hoy se ha convertido en un referente en el área de I+D por y para las pymes en España. También ofrece soluciones para facilitar los procesos internacionales de innovación dirigidos a las pymes. Como agente tecnológico de la Red Tecnológica del País Vasco (Innobasque), Innovalia reúne las capacidades, laboratorios y recursos de las empresas que fundaron la asociación.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

La información para este caso de estudio fue recopilada a través de una entrevista en profundidad con el técnico de TI de la empresa. Durante la interacción el entrevistador planteó preguntas iniciales, de modo que el entrevistado se animara a responder. La información restante se completó a posteriori con los datos proporcionados por la persona entrevistada.

PREVENIR

The practice that Innovalia applied before the incident was the installation of a **firewall software**. La práctica que aplicaba Innovalia antes del incidente era la instalación de un **software de firewall**.

Prácticas específicas de seguridad:

- ☑ **la concienciación de los empleados sobre los correos no fiables.** En este caso, un hacker envió un correo electrónico aparentemente legítimo en el que pedía a nuestros empleados que hicieran clic en un enlace del correo para restablecer la contraseña de acceso, con el pretexto de que se habían registrado varios intentos fallidos de inicio de sesión.
- ☑ **la instalación de firewalls internos** para reforzar su firewall externo estándar. Cuando el personal trabajó desde casa durante la pandemia de COVID-19, se les pidió que instalaran un firewall en su red doméstica.

"La inyección de comandos es un ciberataque en el que un atacante toma el control del sistema operativo del host, inyectando código en una aplicación vulnerable a través de un comando. Este código se ejecuta con independencia de cualquier mecanismo de seguridad y puede utilizarse para robar datos, colapsar sistemas, dañar bases de datos e incluso instalar malware que pueda utilizarse posteriormente". (StackHawn, 2022)

IDENTIFICAR

El tipo y naturaleza del ciberataque fue: **Inyecciones de código en una vulnerabilidad en el servidor web apache de la empresa a través de la ejecución remota de comandos**. Este tipo de ataque se puede describir en detalle según el marco MITRE ATT&CK, como se muestra a continuación.

- ☑ Reconocimiento: escaneo activo: escaneo de bloques de IP y escaneo de vulnerabilidades
- ☑ Acceso inicial: servicios remotos externos
- ☑ Ejecución: Intérprete de comandos y secuencias de comandos: Power Shell
- ☑ Escalada de privilegios:
  - Process Injection: Dynamic-link Library Injection; Portable Executable Injection; Thread Execution Hijacking; Asynchronous Procedure Call; Thread Local Storage; Ptrace System Calls; Proc Memory; Extra Window Memory Injection; Inyección de proceso: inyección de biblioteca de enlace dinámico; inyección ejecutable portátil; secuestro de ejecución de subprocesos; llamada de procedimiento asíncrono; almacenamiento local de subprocesos; llamadas al sistema Ptrace; memoria de proceso; inyección de memoria de ventana adicional;
  - Ejecución desencadenada por eventos: modificación de la configuración de la shell de Unix,

- ☑ Evasión de defensa: Inyección de Procesos y Plantillas
- ☑ Exfiltración: transferir datos a la cuenta de la nube.
- ☑ Impacto:
  - Manipulación de datos: manipulación de datos almacenados, transmitidos y en tiempo de ejecución
  - Parada de servicio
  - Apagado/reinicio del sistema

RESPONDER

- ☑ **QUIÉN:** El atacante no pudo ser identificado con precisión. Solo se conocía el lugar de origen, China.
- ☑ **A QUIÉN:** Asociación Innovalia
- ☑ **POR QUÉ:** Fue al azar
- ☑ **QUÉ:** Sistema de la Asociación Innovalia
- ☑ **CÓMO:** Inyección de procesos con ejecución remota de comandos.
- ☑ **ESTRATEGIA:** La amenaza se atajó con el firewall que tenía el servidor en ese momento. Siga los pasos descritos en la siguiente sección, sobre cómo bloquear IPs.

RECUPERAR

Las principales consecuencias del ataque fueron:

- ☑ Sistema comprometido
- ☑ Investigación y Análisis
- ☑ Actualización de la versión del servidor
- ☑ Cambiar credenciales

La **estrategia de recuperación** se centró en bloquear la IP a través del firewall:

En primer lugar, inicie sesión en el servidor en el que necesita bloquear la dirección IP. Luego, haga clic en Inicio, escriba Firewall de Windows con seguridad avanzada y presione Entrar. En el panel izquierdo, haga clic en Reglas de entrada para mostrar las reglas configuradas actualmente en el panel central.

En el panel de la derecha, haga clic en Acciones > Nueva regla: para Tipo de regla, seleccione Personalizada y haga clic en Siguiente; para Programa, seleccione Todos los programas y haga clic en Siguiente; para Protocolo y Puertos, seleccione cualquiera del menú desplegable Tipo de Protocolo y haga clic en Siguiente; y para Ámbito: en ¿A qué direcciones IP remotas se aplica esta regla?, seleccione el botón de opción: Estas direcciones IP: haga clic en Agregar.

Luego, ingrese la dirección IP que desea bloquear del servidor y haga clic en Aceptar. También puede optar por bloquear un rango de direcciones IP seleccionando la opción Este rango de direcciones IP: botón de opción. Después de terminar de agregar las direcciones IP, haga clic en Siguiente. Para Acción, seleccione Bloquear la conexión y haga clic en Siguiente. Para Perfil, deje todas las opciones marcadas y haga clic en Siguiente. Para Nombre, asigne a la regla un nombre descriptivo, como Lista negra de IPs. También puede ingresar una descripción opcional de la regla. Haga clic en Finalizar. La regla recién creada con el nombre dado, ahora se muestra en el panel de reglas de entrada del medio. Para ordenar las reglas alfabéticamente por nombre, puede hacer clic en el encabezado de la columna Nombre. Si necesita deshabilitar la regla, haga clic derecho en la regla en la lista y haga clic en Deshabilitar regla. Si necesita modificar el alcance de las direcciones IP para la regla, haga clic con el botón derecho en la regla de la lista y haga clic en Propiedades. Luego haga clic en la pestaña Ámbito, realice los cambios necesarios y haga clic en Aplicar.

LECCIONES APRENDIDAS

Hemos aprendido que es mejor tener ciertas medidas preventivas y defensivas, útiles para este tipo de ataques, como:

- ☑ Para mantener el servidor actualizado
- ☑ Para agregar monitoreo a la máquina servidor
- ☑ Para segmentar la red en VLANS, y
- ☑ Para aislar máquinas que estén expuestas al exterior.

CASO DE ESTUDIO 2: LA IMPRUDENCIA DE UN EMPLEADO

La organización aplicó el Sistema de detección de intrusos (IDS), que monitorea la red de CARSA en busca de actividades maliciosas o violaciones de políticas. CARSA aplica un software de firewall para proteger su red y sistema del acceso no autorizado.

Las prácticas de seguridad específicas que tuvieron efectos demostrados en otros ciberataques son:

Validar y sanear las entradas: buscar caracteres de escape y otros símbolos especiales para el idioma de la aplicación y el sistema operativo, como marcas de comentarios, caracteres de terminación de línea y delimitadores de comandos. Si la aplicación solo espera un conjunto limitado de valores, aceptar solo esos valores, por ejemplo, incluyéndolos en la lista blanca o activándolos condicionalmente.

"En 2021, el 83% de las organizaciones declararon haber sufrido ataques de phishing. En 2022, se espera que se produzcan otros seis mil millones de ataques".(CyberTalk, 2022)

Evite construcciones de evaluación vulnerables: evitamos el uso de "eval ()" y funciones equivalentes en entradas de usuario sin procesar. CARSA usó funciones dedicadas específicamente del idioma para procesar de forma segura los datos proporcionados por los usuarios.

Bloquear el intérprete: si tiene control sobre la configuración del servidor, es mejor limitar la funcionalidad del intérprete al mínimo requerido para la aplicación, para evitar la escalada a la inyección de comandos del sistema. Por ejemplo, si su aplicación PHP no usa la función system( ), puede deshabilitar esa función en su archivo php.ini, especificándola en la directiva disabled_functions. Las funciones comúnmente deshabilitadas para PHP incluyen: exec() , passthru ( ), shell_exec (), system(), proc_open (), popen (), curl_exec (), curl_multi_exec (), parse_ini_file () y show_source ().

Verificar nuestro código: CARSA usó herramientas de verificación de código estático para buscar vulnerabilidades relacionadas con la validación de entrada y la evaluación insegura.

Escanear las aplicaciones: la organización utilizó un escáner para garantizar que las aplicaciones estén a salvo de varios tipos de ataques. Por ejemplo, CARSA cuenta con un Sistema de Detección de Intrusos.

El ciberataque se produjo dentro de CARSA, y el tipo de ciberataque fue **'ataque de phishing**'. El ataque de phishing es un tipo de ataque de ingeniería social que a menudo se usa para robar datos de usuarios, incluidas las credenciales de inicio de sesión.

Según el modelo STRIDE, este tipo de ataque tiene como "Amenaza" la elevación de privilegios, porque la propiedad violada es la "autorización". En este tipo de ciberataque, el usuario permite que alguien haga algo para lo que no está autorizado.

Según el marco MITRE ATT&CK, este ataque es:

- ☑ Reconocimiento: Phishing para obtener información: servicio de spearphishing, archivo adjunto de spearphishing y enlace de spearphishing.
- ☑ Acceso Inicial: Phishing: archivo adjunto de spearphishing, enlace o a través del servicio.
- ☑ Ejecución: los atacantes pueden enviar mensajes de phishing para obtener acceso a los sistemas de las víctimas. Todas las formas de phishing son ingeniería social enviada electrónicamente. El phishing puede ser dirigido, conocido como spearphishing. En el spearphishing, el atacante apuntará a una persona, empresa o industria específica. De manera más general, los adversarios pueden realizar phishing no dirigido, como en campañas masivas de spam de malware.
- ☑ Descubrimiento: la detección se puede realizar a través de: Registro de la aplicación (contenido), el archivo (creación del archivo) o el tráfico de red (contenido o flujo).
- ☑ Movimiento lateral: phishing interno.
- ☑ Exfiltración: ingeniería social y ataques de phishing; correo saliente, descargas a dispositivos inseguros, cargas a servicios externos y comportamiento inseguro de la nube.
- ☑ Impacto: pérdida de datos confidenciales, daño a la reputación, pérdida de clientes, costo del tiempo de inactividad, etc.

RESPONDER

QUIÉN: El atacante fue una persona/organización externa desconocida, a través de un empleado de CARSA .
A QUIÉN: Las credenciales para acceder a un software de pago (no público ni de código abierto).
POR QUÉ: El robo de credenciales así como información sensible de la entidad.
QUÉ: datos y contraseñas.
CÓMO: Un empleado instaló un software que no estaba permitido por la empresa, según se define en la política de la empresa. Este tipo de software no estaba permitido debido a su dudosa confiabilidad y seguridad. (Por lo general, todo software que se instala en las computadoras de los empleados debe ser supervisado por el personal técnico informático de la entidad). Este software tenía un “troyano” de red. Hay varias formas en que un troyano ataca un sistema, en este caso particular, era un "troyano infostealer", como suena, este troyano busca datos en su computadora infectada.
ESTRATEGIA: La estrategia seguida fue rastrear la dirección mac para identificar la máquina infectada y el empleado responsable. Posteriormente, se eliminó el software y el virus.

RECUPERAR

IMPACTO: robo de credenciales de usuario a nivel local

ESTRATEGIA DE RECUPERACIÓN:

- ☑ A través de la dirección MAC sabíamos qué empleado estaba siendo atacado, sin que él se diera cuenta.
- ☑ Se desinstaló un software que no debería haber sido instalado.
- ☑ Programas antivirus y antimalware en la máquina específica.
- ☑ Credenciales de usuario comprometidas modificadas.

MEJOR ESTRATEGIA: se podría haber formateado todo el ordenador porque nunca se puede estar seguro de su eliminación completa.

LECCIONES APRENDIDAS

Para aumentar la responsabilidad de los empleados a través de:

- ☑ capacitación con charlas breves sobre la importancia de no instalar software sin previo aviso y confirmación de seguridad por parte del equipo de soporte técnico y,
- ☑ recordando las políticas de seguridad de la empresa y las normas comunes de seguridad en ciberseguridad.
- ☑ actualizar el software de las máquinas de la empresa (software: windows y programas antivirus). Para recordar a los empleados que ejecuten el análisis antivirus varias veces.

CASO DE ESTUDIO 3: LA TARJETA DE CRÉDITO EN UNA PYME VÍA RED WIFI

LA ORGANIZACIÓN OBJETIVO

Bodegas **Monje** está situada en un enclave excepcional de la isla de Tenerife, en el paraje conocido como "La Hollera" del municipio de El Sauzal con vistas al Teide. Una larga tradición de productores de vino acompaña a la familia Monje desde 1750. Las barricas de roble y los modernos sistemas de maceración conviven para dotar a los vinos tintos, blancos y rosados de un carácter y sabores especiales, que se adaptan perfectamente a la mejor gastronomía canaria. Esta bodega también acoge iniciativas culturales, gastronómicas y de ocio que amplían los límites del vino y lo devuelven al entorno social del que históricamente procede, una auténtica apuesta por el enoturismo. Wine&Tours.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

El método aplicado para recolectar la información para este caso de estudio fue una entrevista en profundidad.

PREVENIR

La organización no aplicó ninguna práctica de ciberseguridad antes de este evento. Solo tienen un firewall en el proveedor de servicios de internet (Router Movistar).

Las prácticas específicas de seguridad establecidas en Bodegas Monje, que han tenido efectos probados en la prevención de este tipo de sucesos, se programaron después del evento. En particular, las acciones emprendidas tuvieron éxito en la prevención de nuevos ataques de naturaleza similar.

IDENTIFICAR

Un cliente del establecimiento accedió a la empresa para consumir los productos fabricados, y se conectó a internet a través de la red WIFI. El ciberataque fue identificado por el propio cliente afectado. Esta persona detectó movimientos en sus cuentas bancarias con pagos en línea realizados con su tarjeta de crédito, pero no por él. Todos estos movimientos los realizó justo después de su visita a la empresa "Bodegas Monje".

El cliente alertó al banco para que intentara cancelar esos pagos y bloquear la tarjeta para evitar que el ciberdelincuente siguiera usándola.
Posteriormente, notificó a la empresa "Bodegas Monje" ya que fue el último lugar donde efectivamente lo usó.

RESPONDER

QUIÉN: el propio cliente de una empresa que accedió a la red local con fines ilegales.
A QUIÉN: a otro cliente, a través de la empresa.
POR QUÉ: por robar dinero.
QUÉ: apropiarse indebidamente de datos bancarios y realizar cargos, beneficiándose del dinero de otra persona.
CÓMO: infiltración a través de la red Wifi de los clientes.
ESTRATEGIA: rediseñar la red para separar la conexión de los clientes que visitan el negocio del sistema de pago y la red interna de la empresa.

RECUPERAR

IMPACTO:

- ☑ La tarjeta de crédito de un cliente del establecimiento comprometida
- ☑ La confianza de los clientes en la seguridad de la empresa podría verse comprometida y no podrían confiar en realizar pagos por este método tan fácilmente.
- ☑ Si más clientes se vieran afectados por este ciberataque, impactaría directamente en la reputación de la empresa.

ESTRATEGIA DE RECUPERACIÓN:

La estrategia llevada a cabo por el propietario de la empresa, desde el momento en que tuvo conocimiento del incidente, fue apagar el wifi y/o desconectar la red de invitados. Luego, contactó a una empresa de ciberseguridad para solucionarlo.

La nueva estrategia de recuperación realizada por el equipo de ciberseguridad fue rediseñar la red para separar la red del cliente de la red interna de la empresa donde se almacenan los datos más sensibles (datos propios de empleados y clientes, como los datos del sistema de pago).

No se pudo recuperar el dinero robado después de que se rediseñó la red. El cliente tuvo que cambiar la antigua tarjeta de crédito "robada" por otra nueva. No se pudo identificar a la persona que llevó a cabo el ciberataque. No se pudieron emprender acciones legales.

Hay una estrategia mejor que emprender en esta situación. En lugar de desconectar la red wifi de la empresa, se podría haber hecho, además:

- ☑ Hacer una lista de toda la información comprometida, con todos los datos de contacto de los posibles clientes que podrían verse afectados (cronología, de quiénes estaban en la empresa al mismo tiempo que el cliente afectado).
- ☑ Informar a otros clientes para que estén al tanto de cualquier movimiento extraño en sus cuentas bancarias realizado con pagos en línea realizados con su tarjeta de crédito.
- ☑ Recopilar la mayor cantidad de información posible no solo para poder identificar al culpable del ciberataque, sino también para advertir mejor a los clientes que también podrían verse afectados.

Cambiar las contraseñas de inmediato para evitar un cierre repentino de la empresa, porque en ese momento la red no estaba separada, funcionaba para los clientes y para los empleados al mismo tiempo.

LECCIONES APRENDIDAS

Entre las lecciones aprendidas, se destacan las siguientes:

- ☑ es mejor tener la red segmentada
- ☑ se deben implementar políticas de confianza cero
- ☑ no hace falta ser una gran empresa para sufrir un ciberataque

es necesario contar con equipos actualizados y sistemas de ciberseguridad activos (con firewall profesional, IPS, antivirus, etc.).

CASO DE ESTUDIO 4: DIVULGACIÓN DE LA INFORMACIÓN DE HANESBRANDS

LA ORGANIZACIÓN OBJETIVO

Hanesbrands Inc. (HBI) es una empresa de ropa multinacional fundada en 1901 y con sede en Winston-Salem, EE. UU. Tienen más de 250 puntos de venta en 47 países. Entre las marcas más famosas de la

empresa se encuentran Hanes, Champion, Playtex, Bali, L'eggs, Just My Size, Barely There, Wonderbra, Duofold , Celebrity, Maidenform, Zorba, etc. Una de las ventajas competitivas de Hanesbrands es que el 70% de la ropa que venden se fabrica en sus propias instalaciones, así como en las de los contratistas asociados. De esta forma, la empresa logra controlar la mayor parte de la cadena de suministro, lo que también permite establecer fuertes prácticas de sustentabilidad y contribuye a su éxito mundial. En 2021, HBI fue nombrada una de las empresas más éticas del mundo por Ethisphere y pasó a formar parte de las 100 empresas más sostenibles de Barron durante tres años consecutivos. Para garantizar que la empresa siga una política de sostenibilidad a largo plazo, ha establecido objetivos globales de sostenibilidad para 2030 (en línea con los Objetivos de Desarrollo Sostenible de las Naciones Unidas bajo tres pilares: Personas, Planeta y Producto) y ha iniciado un sitio web de sostenibilidad.

"Según un nuevo informe de Blumira e IBM, el ciclo de vida medio de las filtraciones dura 287 días, y las organizaciones tardan 212 días en detectar inicialmente una filtración y 75 días en contenerla." (VentureBeat, 2022)

En 2019, la empresa tuvo unos ingresos de 7.000 millones de dólares y unos 61.000 empleados. Se ha informado de que HBI gasta más de 100 000 dólares en ciberseguridad, utilizando principalmente productos de Akamai, como los servicios en la nube.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

El método aplicado para recopilar la información para este estudio de caso fue la investigación documental, las fuentes de información específicas se pueden encontrar en la sección de Bibliografía de este documento.

PREVENIR

☑ **Prácticas que no surtieron efecto:** Autenticación en el sitio web - Para realizar el seguimiento de su pedido de ropa, el usuario recibía un enlace para iniciar sesión como invitado en el sitio web. El usuario invitado tenía amplios derechos para obtener información de los pedidos realizados por todos los demás usuarios simplemente modificando la URL de invitado. Por lo tanto, la base de datos se vio comprometida a través del sitio web, ya que no solicitó autenticación y consideró al usuario invitado como un usuario válido. Los datos visibles para otros clientes consistían en nombres, últimos dígitos de sus tarjetas de crédito, dirección, número de teléfono, etc.

☑ **Prácticas que han tenido efectos demostrados en ciberataques reales de este tipo:**

1. Descubrimiento de exposición de datos (usando sistemas de escaneo externos).
2. Autenticación sólida (inicio de sesión único que permite a un usuario iniciar sesión en varios sistemas diferentes o diferentes nombres de usuario/contraseñas para cada sistema).

3. Priorización del acceso a los datos (p. ej., RR. HH. solo puede necesitar acceso a la información de los empleados y el departamento de contabilidad solo puede necesitar acceso a los datos de presupuesto e impuestos. Los usuarios invitados deben tener un acceso mínimo a los datos en principio).
4. Implementación de infraestructuras de monitoreo y soluciones automatizadas que pueden identificar rápidamente problemas potenciales antes de que se conviertan en emergencias, aislar bases de datos infectadas y señalar a los equipos de soporte y TI para los próximos pasos.

IDENTIFICAR

El ataque contra Hanesbrands Inc. fue de **tipo divulgación de información.**

En la última semana de junio y la primera de julio de 2015 Hanesbrands Inc. fue víctima de un ciberataque. Después de que se robaron los datos, los atacantes informaron a la empresa sobre la violación sin dar un motivo para su acción. Es muy probable que la debilidad de la empresa se descubriera mediante el escaneo [1]. Los piratas informáticos crearon una orden de pago de "invitado" en el sitio web de Hanesbrands [2] (sin siquiera registrarse en el sitio web). Con el enlace del pedido recibido, los piratas informáticos lograron drenar la base de datos de la empresa que era responsable de almacenar los datos de todos los pedidos de los clientes (pedidos que se realizaron en su sitio web o por teléfono); resultó que con el enlace de salida del "invitado" se podía acceder a cualquier otro pedido sin autenticarse. En una semana, los atacantes lograron obtener información de más de 900.000 clientes. Para no ser detectados, lo más probable es que los piratas informáticos hayan utilizado Port Knocking [3] para ocultar su actividad. Según Hanesbrands, los atacantes usaron capturas de pantalla [4] para extraer los datos, sin embargo, es muy probable que usaran una forma más automatizada, como un script que analizara los datos directamente [5].

El ataque descrito por el marco MITRE ATT&CK:
[1]Escaneo activo: Escaneo de vulnerabilidades (T1592.002).
[2] Acceso inicial: aprovechar la aplicación pública (T1190).
[3] Persistencia: Señalización de tráfico: Port Knocking (T1205.001).
[4] Captura de pantalla (T1113).
[5] Recopilación automatizada (T1119).

El ataque fue identificado por la empresa luego de ser notificado por los adversarios. Hanesbrands no sabía que esto estaba sucediendo hasta que los piratas informáticos se lo hicieron saber.

RESPONDER

En junio de 2015, los atacantes informaron a Hanesbrands Inc. sobre la infracción. A través de una cuenta de invitado en su sitio web, los atacantes lograron extraer información general de los usuarios de 900.000 clientes. Después de recibir una notificación sobre la filtración, Hanesbrands agregó autenticación a su base de datos de "pedidos de clientes" y eliminó la opción de "salida de invitado" (aunque ya la habían arreglado).

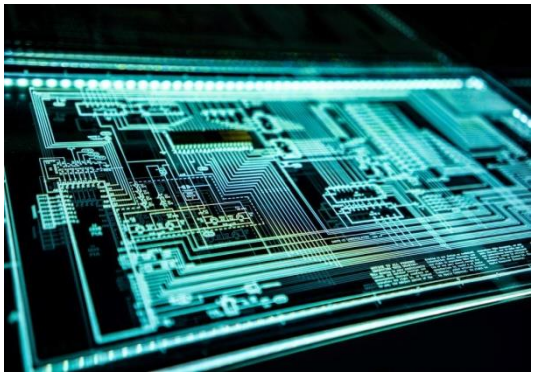
QUIÉN: Desconocido.

A QUIÉN: Hanesbrands Inc.

POR QUÉ: Fue un ataque dirigido para obtener información sobre base de datos de clientes y listas de clientes, pero los atacantes no pidieron rescate después de todo. Simplemente informaron a Hanesbrands que obtuvieron los datos.

QUÉ: Información general de 900.000 clientes: nombres, direcciones, información sobre el estado de los pedidos de los clientes, números de teléfono y los 4 últimos dígitos de su tarjeta de crédito. Pero no se revelaron los nombres de usuario ni las contraseñas de los clientes. Los hackers no comprometieron los sistemas corporativos de Hanesbrands.

CÓMO: Haciéndose pasar por un "invitado" que estaba revisando un pedido (los atacantes no estaban registrados en el sitio web), lograron encontrar una brecha en la base de datos de Hanesbrands al explotar el enlace del pedido. Los piratas informáticos pudieron acceder a los detalles y el estado de los pedidos de los clientes, y extraer los datos durante aproximadamente una semana utilizando la opción "explotar con pago" en el sitio web.



ESTRATEGIA: Una vez que los atacantes notificaron a Hanesbrands sobre la infracción, la empresa puso autenticación a su base de datos para detener el fallo de divulgación de información. Además, repararon el enlace “usuario invitado” a través de la cual se gestionaba la fuga. Hanesbrands notificó a sus clientes sobre la infracción por correo electrónico y correo postal. Desde ese accidente, Hanesbrands está invirtiendo cada vez más en ciberseguridad cada año.

RECUPERAR

- ☑ **IMPACTO:** Las consecuencias fueron la filtración de información general de los clientes. No se revela ninguna demanda u otro daño directo.
- ☑ **ESTRATEGIA DE RECUPERACIÓN:** Hanesbrands informó a sus clientes sobre la infracción. Se reparó el enlace de "usuario invitado" [1] para no tener acceso directo a la base de datos y deshabilitarlo en general como una opción [2]. Servicio de atención al cliente ofrecido para responder si los usuarios tienen inquietudes. Además, se realizó una auditoría de seguridad [3] y un análisis de vulnerabilidades [4] de sus sistemas existentes y se invirtió en capacitación en ciberseguridad [5].

Las soluciones descritas por el marco MITRE ATT&CK:

[1] Configuración del software (M1054).
[2] Desactivar o eliminar una función o un programa (M1042).
[3] Auditoría (M1047).
[4] Análisis de vulnerabilidades (M1016).
[5] Guía para desarrolladores de aplicaciones (M1013).

☑ **MEJOR ESTRATEGIA:** Después de reparar el enlace de "usuario invitado" a través del cual un cliente puede revisar su compra, Hanesbrands lo deshabilitó como una opción. En su lugar, podrían haber agregado un monitoreo de actividad sospechosa y/o políticas para revisar solo cierta cantidad de compras.

LECCIONES APRENDIDAS

Los ataques de divulgación de información son poco frecuentes, ya que muchas herramientas modernas brindan ciberseguridad automática y asesoran a las empresas sobre lo que podría ser una posible brecha. El ataque a Hanesbrands muestra que el rastro de auditoría de base de datos es débil y la falta de experiencia en seguridad pueden aprovecharse con bastante facilidad. En muchos casos, las bases de datos se violan debido a un nivel insuficiente de experiencia en ciberseguridad y la falta de capacitación/formación relevante de los empleados no técnicos que, como resultado, pueden violar las reglas básicas de seguridad de la base de datos. El personal de TI también podría carecer de la experiencia necesaria para hacer cumplir las políticas de seguridad, llevar a cabo procesos y acciones de informes de incidentes adecuados.

Otro punto es que la base de datos en Hanesbrand era vulnerable debido a una configuración incorrecta; las bases de datos generalmente quedan totalmente desprotegidas debido a eso. A menudo se olvida que, por lo general, los atacantes son especialistas en TI altamente profesionales, que seguramente saben cómo explotar dichas vulnerabilidades. Esto se puede contrarrestar desactivando las cuentas de la base de datos predeterminadas, junto con un personal de TI capacitado y con experiencia.

Hanesbrands tuvo la suerte de que solo se filtró información general, además de que los atacantes informaron a la empresa después de extraer todos los datos que pudieron. Además de eso, Hanesbrands informó a sus clientes de inmediato sobre la infracción, lo que demuestra que la empresa quiere ser sincera con sus clientes y que el problema se tomó en serio.

CASO DE ESTUDIO 5: SPOOFING (SUPLANTACIÓN DE INDENTIDAD) EN HUMANA

TARGETED ORGANISATION

Humana es una compañía de seguros de salud con sede en Louisville, Kentucky . Fundada en 1961 como operador de una residencia de ancianos, la compañía pasó a ser propietaria y administradora de hospitales, y luego a planes de seguro de salud en la década de 1980. A partir de mayo de 2015, Forbes estimó que la empresa tenía un valor de 26.7 mil millones de dólares. En 2020, Humana tuvo ingresos de 77.155 mil millones de dólares y alrededor de 48.000 empleados. Mensualmente, Humana gasta más de 100.000 dólares en ciberseguridad. Humana está utilizando productos de ciberseguridad como "Akamai" (plataforma de entrega en la nube) y " Prolexic (soluciones de seguridad para proteger sitios web, centros de datos y aplicaciones IP empresariales de ataques de denegación de servicio distribuido (DDoS))", "Proofpoint" (solución para proteger a su gente y los datos críticos de amenazas de correo electrónico avanzadas), "Alert Logic" (detección y respuesta gestionadas con guante blanco) y otros programas.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

El método aplicado para recopilar la información para este caso de estudio fue la investigación documental, las fuentes de información específicas se pueden encontrar en la sección de Bibliografía de este documento.

PREVENIR

☑ **Prácticas que no surtieron efecto:** alertas por intentos fallidos de inicio de sesión: Humana aplicó esta práctica antes del incidente. No fue efectivo ya que la organización tardó aproximadamente un día en tomar medidas en respuesta a los numerosos intentos fallidos de inicio de sesión recibidos.

☑ **Prácticas que han tenido efectos probados en ciberataques reales:**

1. Bloqueo de cuenta después de un intento fallido de inicio de sesión.
2. Bloqueo del tráfico de internet de países extranjeros con los que la organización no hace negocios.
3. Forzar un restablecimiento de contraseña.

IDENTIFICAR

El ataque contra Humana fue del **tipo Spoofing.**

El 3 de junio de 2018, Humana fue el objetivo de un sofisticado ciberataque de suplantación de identidad que ocurrió en Humana.com. El mismo día, Humana se dio cuenta de un aumento significativo de intentos de error de inicio de sesión desde direcciones IP de países extranjeros [1]. Para no revelar su ubicación real, los atacantes utilizaron Proxies Multi-Hop [2]. El volumen de los intentos de inicio de sesión en Humana.com sugirió que se lanzó un ataque grande y de base amplia. La naturaleza del ataque y los comportamientos observados indicaron que el atacante tenía una gran base de datos de identidades de usuarios y contraseñas que se ingresaban con la intención de identificar cuáles podrían ser válidas en Humana.com por "fuerza bruta"[3]. La cantidad excesiva de errores de inicio de sesión sugirió que la información de las credenciales no se originó en Humana [4] (y muy probablemente se compraron en la web "oscura"). El 4 de junio Humana bloqueó las IPs. En base a estos hechos, esto puede describirse como un ataque de suplantación de identidad. Los atacantes recopilaron datos [5] de unos 65.000 usuarios que incluyen:

☑ Reclamaciones médicas, odontológicas y oftalmológicas, incluidos los servicios prestados, el nombre del proveedor, las fechas del servicio, los cargos y los importes pagados, etc.

☑ Información de la cuenta de gastos, como los gastos de la cuenta de ahorros para la salud y la información del saldo.

"El spoofing es una técnica de ataque que se basa en la falsificación de datos en una red de forma que permite que un sitio o comunicación maliciosa se haga pasar por uno de confianza". (The Cyberwire Glossary, n.d.)

Después del incidente, Humana tomó medidas adicionales como el bloqueo de la cuenta después de un intento fallido de inicio de sesión, bloqueando el tráfico de Internet de países extranjeros con los que la organización no hace negocios y forzando un restablecimiento de contraseña.

El ataque descrito por el marco MITRE ATT&CK:

[1] Intérprete de scripts y comandos: CLI de dispositivos de red: (T1059.008).
[2] Proxy: Multi-hop Proxy (T1090.003).
[3] Fuerza bruta: relleno de credenciales (T1110.004).
[4] Recopilar información de identidad de la víctima: Credenciales (T1589.001).
[5] Recopilación automatizada (T1119).
El ataque fue identificado por alertas de errores de múltiples intentos de inicio de sesión.

RESPONDER

- ☑ **QUIÉN:** desconocido
- ☑ **A QUIÉN:** Humana
- ☑ **POR QUÉ:** Robo de identidad (probablemente vendido a terceros)
- ☑ **QUÉ:** Información confidencial de los usuarios (reclamaciones médicas, dentales y oftalmológicas, incluidos los servicios prestados, el nombre del proveedor, las fechas del servicio, los cargos y los montos pagados, etc.; información de la cuenta de gastos, como los gastos de la cuenta de ahorro para la salud y la información del saldo).
- ☑ **CÓMO:** Los atacantes recogieron grandes cantidades de cuentas y credenciales. Luego, usando multi-hop proxies, inicio de sesión forzado con las cuentas que tenían. Después de un inicio de sesión exitoso, los atacantes recopilaron datos de usuario a través de transferencias de datos de pequeño tamaño.
- ☑ **ESTRATEGIA:** Una vez que Humana notó el aumento significativo en la cantidad de errores de intentos de inicio de sesión, sus operadores de ciberseguridad bloquearon las direcciones IPs extranjeras desde las que se realizaron los múltiples intentos de inicio de sesión. Después de eso, Humana forzó el restablecimiento de la contraseña en todas las cuentas que se sabe que fueron violadas e incluso lanzó un producto que ofrece a los miembros una protección contra el robo de identidad durante un año.

RECUPERAR

- ☑ **IMPACTO:** The consequence was the leaking of confidential information of users (medical, dental, and vision claims including services performed, provider name, dates of service, charge and paid amounts etc; spending account information such as health saving account spending and balance information). Many negligence lawsuits were filed towards Humana after that. There is no information if the lawsuits were won by the company which suggests that the results were probably negative. La consecuencia fue la filtración de información confidencial de los usuarios (reclamaciones médicas, dentales y oftalmológicas, incluidos los servicios prestados, el nombre del proveedor, las fechas del servicio, los cargos y los montos pagados, etc.; información de la cuenta de gastos, como los gastos de la cuenta de ahorro para la salud y la información del saldo). Después de eso, se presentaron muchas demandas

por negligencia contra Humana. No hay información sobre si las demandas fueron ganadas por la empresa, lo que sugiere que los resultados probablemente fueron negativos.

☑ **ESTRATEGIA DE RECUPERACIÓN:** Humana notificó a varios miembros para informarles sobre la violación de datos después de que había pasado un mes. También tomaron una serie de medidas para aumentar su ciberseguridad, entre ellas: 1) forzar un restablecimiento de contraseña [1]; 2) implementar nuevas alertas para inicios de sesión exitosos y fallidos [2] y 3) cuentas bloqueadas que estaban conectadas a actividades sospechosas [3]. Además, implementaron una serie de controles técnicos para mejorar la seguridad del portal web (bloqueo de ataque de fuerza bruta, defensa de inyección SQL [4], instalación de un certificado de seguridad SSL [5], etc.). La empresa también bloqueó todas las direcciones IPs extranjeras que no eran relevantes para sus operaciones [6].

Las soluciones tomadas por Humana descritas por el marco MITRE ATT&CK:

[1] Políticas de contraseñas (M1027).
[2] Prevención de intrusiones en la red (M1031).
[3] Políticas de uso de la cuenta (M1036).
[4] Configuración del software (M1054).
[5] Inspección SSL/TLS (M1020).
[6] Filtrar tráfico de red (M1037).

☑ **MEJOR ESTRATEGIA:**

Humana podría haber notificado a los usuarios antes. También podrían haber agregado medidas de seguridad adicionales como:

- Usar la autenticación basada en el intercambio de claves entre las máquinas en la red de una organización o la autenticación de múltiples factores para el acceso remoto;
- Usar una lista de control de acceso para denegar direcciones IPs privadas en interfaces descendentes;
- Implementar el filtrado del tráfico entrante y saliente;
- Configurar routers y switches, si es posible, para rechazar paquetes que se originen desde fuera de la red local de una organización, que afirman originarse desde adentro;
- Habilitación de sesiones de cifrado en el router de una organización, para que los hosts de confianza fuera de su red puedan comunicarse de forma segura con sus hosts locales.

LECCIONES APRENDIDAS

Las lecciones aprendidas podrían identificarse como la necesidad de centrarse más en proteger los datos personales de los usuarios, organizar formaciones del personal para crear conciencia sobre las ciberamenazas, notificar a los usuarios sobre fugas de datos debido a las numerosas demandas por negligencia contra Humana. Después del incidente (Humana no reveló ninguna información de que tal ataque hubiera ocurrido hasta un mes después).

Los efectos del ataque no solo estuvieron relacionados con los gastos para hacer frente al mismo y las demandas, sino con el gran daño a la reputación de Humana y su confiabilidad. Dado que la empresa opera en el sector de los seguros de salud, es crucial para ella contar con las más altas medidas de seguridad y confianza de sus clientes, ya que los datos almacenados en sus sistemas

son muy sensibles y confidenciales. Es por eso que Humana fue y sigue siendo uno de los principales objetivos de los ciberataques, mucho antes del especificado en este caso y también después. Teniendo en cuenta esto, el error de apreciación de la gravedad de este ataque podría considerarse sorprendente.

CASO DE ESTUDIO 6: DENEGACIÓN DE SERVICIO EN WILLIAM HILL

ORGANIZACIÓN OBJETIVO

William Hill es una empresa de apuestas en línea con sede en Londres, Inglaterra, fundada en 1934 por William Hill. La empresa cambió de manos muchas veces: fue comprada por primera vez en 1971 por Sears Holdings. Después de venderse varias veces en abril de 2021, fue adquirida por Ceasars Entertainment. En 2020, la empresa tuvo ingresos de 1324,3 millones de libras esterlinas y 12000 empleados (8000 en el Reino Unido) en 2021. La empresa solía tener más de 1400 tiendas de apuestas, pero en 2019 comenzó a cerrar más de 800 tiendas debido a las bajas ganancias, pero afirmando que mantendrán su personal intacto.

Mensualmente, William Hill gasta más de $100.000 en ciberseguridad. La empresa está utilizando productos de ciberseguridad como “Prolexic” (soluciones de seguridad para proteger sitios web, centros de datos y aplicaciones IP empresariales de ataques de denegación de servicio distribuido (DDoS))”, “Proofpoint” (solución para proteger a su gente y datos críticos de amenazas de correo electrónico avanzadas), “F5 BIG-IP Application Security Manager” (cortafuegos de aplicaciones web flexible que protege las aplicaciones web en entornos de tradicionales, virtuales y de nubes privadas), “Check Point” (protege a sus clientes de los ciberataques de quinta generación con una tasa de captura líder en la industria de malware, ransomware y amenazas dirigidas avanzadas), etc.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

El método aplicado para recopilar la información para este estudio de caso fue la investigación documental, las fuentes de información específicas se pueden encontrar en la sección de Bibliografía de este documento.

PREVENIR

☑ **Prácticas que no surtieron efecto:**

1. Difusión de red anycast: William Hill tiene este tipo de defensa, que es útil para retener grandes cantidades de clientes que visitan su sitio web o puede disolver grandes cantidades de tráfico de red no deseado (como el ataque DDoS). Esta estrategia suele funcionar para la mayoría de los casos de ataques DDoS.
2. El simple aumento del ancho de banda de la red (cuánto tráfico puede contener) no demostró ser efectivo en este ataque.

☑ **Prácticas que han tenido efectos demostrados en ciberataques reales de este tipo:**

1. Implementación de protección DDoS a nivel de servidor: reglas adicionales que ayudan a identificar y bloquear el tráfico de red malicioso.
2. Añadir difusión de red Anycast de terceros: esto puede ayudar a las empresas a aumentar enormemente su capacidad de asumir mucho más tráfico de red o manejar ataques DDoS.

IDENTIFICAR

El ataque contra William Hill fue del **tipo Denegación de Servicio.**

El 1 de noviembre de 2016, William Hill fue objeto de un ataque de denegación de servicio distribuido de alto rendimiento [1]. Antes del ataque, los adversarios recopilaron información sobre los detalles de la red del sitio web de William Hill [2]. Después, los adversarios inundaron el sitio web de William Hill con tráfico para que no pudiera funcionar correctamente. El ataque impidió a los clientes realizar apuestas en los partidos de la Liga de Campeones del martes por la noche. El ataque a William Hill se realizó con la ayuda de un malware llamado "Mirai"[4], que crea una red de numerosos sistemas informáticos que se conoce como "botnet"[3] para iniciar el ataque DDoS a través de ellos.

El ataque descrito por el marco MITRE ATT&CK:

[1] Denegación de servicio de red: Direct Network Flood (T1498.001).

[2] Recopilar información de la red de la víctima: dirección IP (T1590.005).

[3] Adquirir infraestructura: Botnet (T1583.005).

[4] Gusano informático que usa una base de datos de credenciales predeterminadas. Los dispositivos IoT (dispositivos fitness, asistentes de voz, accesorios smarthome, etc.) son escaneados e infectados.

El ataque se identificó justo después de que el sitio web de William Hill dejara de responder y dejara de ser accesible.

RESPONDER

QUIÉN: Desconocido.

A QUIÉN: William Hill.

POR QUÉ: Disputas comerciales: es muy probable que la empresa rival realice tales acciones, especialmente en el momento de eventos deportivos populares como la UEFA Champions League/Extorsión. Si William Hill no logra manejar la situación, es probable que se solicite un rescate.

QUÉ: El sitio web de William Hill estuvo inactivo durante 24 horas, lo que provocó pérdidas por 4,4 millones de libras esterlinas. William Hill tardó días en restaurar completamente su sitio web y sus sistemas.

"Según Cloudflare, en el cuarto trimestre de 2021 laindustria manufacturera fue la que más ataques DDoS en la capa de aplicaciones recibió, registrando un aumento del 641% trimestre a trimestre en el número de ataques..." (Cook, 2022)

CÓMO: En el sitio web de William Hill se llevó a cabo un ataque de denegación de servicio distribuido de alto rendimiento con una red "botnet" (múltiples computadoras que fueron infectadas por un virus de malware y se usaron para realizar dicho ataque sin su conocimiento o consentimiento) creada por un malware llamado "Mirai".

ESTRATEGIA: Después de notar que su sitio web no funciona, los especialistas en TI comenzaron a filtrar el tráfico entrante. William Hill usó la difusión de la red Anycast: envió el tráfico de red y lo dispersó por la red de los servidores de la empresa. Esa solución distribuye el tráfico de red hasta el punto en que la red de la empresa absorbe el tráfico. La utilidad de esta estrategia depende del tamaño de la red de la empresa y del tamaño del ataque DDoS. En el caso de William Hill, incluso con su infraestructura y seguridad de primer nivel, no fueron suficientes para manejar tal ataque.

IMPACTO: El ataque DDoS contra William Hill provocó que su sitio permaneciera inactivo durante más de 24 horas en las que los clientes no podían apostar en los partidos de la Liga de Campeones de la UEFA. Eso resultó en pérdidas por más de £ 4.4 millones en un solo día. Afortunadamente para William Hill, solo se apuntó a su sitio web, lo que mantuvo intactos los datos confidenciales de sus usuarios (lo cual es una pista de que los adversarios querían impedir que los usuarios visitaran el sitio web y no robar datos). Los especialistas en TI de William Hill tardaron más de 4 días trabajando día y noche en reactivar su sitio web y los sistemas afectados.

ESTRATEGIA DE RECUPERACIÓN: Para hacer frente al ataque, William Hill filtró el tráfico de red entrante [1]. Filtrando el tráfico de la red - bloqueando el tráfico de ataque solamente y permitiendo el legítimo. También comenzó a utilizar proveedores de difusión de red Anycast de terceros (empresas que ofrecen este tipo de servicio - que disuelve el ataque DDoS al dispersar todo el tráfico entrante a través de su red).

- ☑ Control de estado del host, que alertará a los especialistas de TI de la empresa cuando se detecte un uso anormal de la red [2]. Si se detecta a tiempo, se pueden tomar medidas para ayudar a mantener disponible el servicio del sitio web.
- ☑ Se puede utilizar el "enrutamiento de agujero negro". Es una técnica que canaliza tanto el tráfico legítimo como el malicioso a una ruta nula y se retira de la red. No es una buena solución ya que hace que el sitio web sea inaccesible.
- ☑ Limitación de velocidad. Limita la cantidad de solicitudes que puede recibir el servidor; por sí solo, no puede detener el ataque DDoS, pero es una herramienta útil en la estrategia de defensa general.

La estrategia de recuperación descrita por el marco MITRE ATT&CK:

a. [1] Filtrar tráfico de red (M1037).
b. [2] Estado del sensor: estado del host (DS0013).

LECCIONES APRENDIDAS

El ataque contra William Hill puede mostrarnos que incluso una empresa con una ciberseguridad excepcional y que esté preparada para manejar este tipo de ataques puede sufrirlos.

A pesar de que su sitio web fue eliminado por el ataque DDoS (por lo general, estos ataques son solo una cortina de humo para el ataque real), la seguridad de alto nivel de la empresa estaba intacta y funcional, manteniendo segura la información confidencial del cliente. Eso demostró a sus clientes que están seguros y mantuvo la credibilidad de la empresa. Dado que los adversarios no intentaron explotar más la vulnerabilidad de William Hill, señala que lo más probable es que el ataque se haya producido por rivalidad empresarial (empresa competidora que quiere aprovechar el mercado de apuestas) o un intento de extorsión (la empresa depende de su sitio web, y mantenerlo inactivo por parte de los competidores genera pérdidas).

Con la entrada en la era de los dispositivos inteligentes (IoT) cuando todo se puede operar de forma remota (luces inteligentes para el hogar, aspiradoras, neveras, relojes inteligentes, etc.), también debemos pensar en la seguridad que se debe aplicar. Todos estos dispositivos inteligentes tienen una dirección IP y pueden ser pirateados a través de la red, para obtener información o "zombificados" (su dispositivo está siendo controlado sin que usted lo sepa y comienza a funcionar de una manera extraña) y utilizados en ataques DDoS para inundar un sitio web.

CASO DE ESTUDIO 7: COBALT STRIKE: EL USO DE HERRAMIENTAS DE RED TEAMING POR CIBERDELINCUENTES

LA ORGANIZACIÓN OBJETIVO

Cobalt Strike es una herramienta de red teaming desarrollada en 2012. Su principal objetivo es ayudar a los equipos rojos a probar y simular ciberataques. Como la herramienta tiene buenas capacidades para eludir los límites de seguridad mediante evasiones, los atacantes han secuestrado algunas de sus versiones para utilizar como herramienta de entrega de cargas maliciosas como el ransomware. Este caso de estudio no se centra en una sola organización, ya que Cobalt Strike se utiliza para realizar ataques en masa dirigidos a varios tipos de organizaciones, como fábricas, instituciones financieras, empresas de telecomunicaciones, etc.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

El método aplicado para recopilar la información para este caso de estudio fue la investigación documental, las fuentes de información específicas se pueden encontrar en la sección de Bibliografía de este documento.

PREVENIR

La detección y prevención de un ataque que hace uso de la herramienta de red teaming Cobalt Strike implica una cadena de seguridad en toda la infraestructura. Esto comienza con el software de protección y supervisión en el cliente de punto final y llega hasta el nivel de la red. Además, la inteligencia activa sobre amenazas también es necesaria para mantener actualizadas las herramientas de detección basadas en firmas.

Esto usualmente involucra:

- ☑ Seguridad de punto final (como antivirus, monitoreo basado en host)
- ☑ Seguridad de red (como cortafuegos, proxy, detección de firmas/patrones en el tráfico)
- ☑ Seguridad del correo electrónico
- ☑ Corrección de las políticas de host/seguridades configuradas

IDENTIFICAR

Cobalt Strike es una herramienta comercial multifuncional que cumple con diferentes técnicas de ataques. Teniendo en cuenta la herramienta y sus capacidades en sí, se puede categorizar como Divulgación de información y Elevación de privilegios. Sin embargo, dado que también se puede usar para descartar más cargas maliciosas, especialmente porque se observaron ataques de ransomware en combinación con Cobalt Strike, la lista se puede ampliar con Tampering y Denegación de servicio.

Teniendo en cuenta todas las características de la herramienta, es una herramienta de acceso remoto con capacidades de movimiento lateral. Esto conduce a una enorme lista de técnicas de ataque utilizadas por Cobalt Strike y, por lo tanto, solo comentaremos algunas de ellas aquí.

- ☑ Mecanismo de control de elevación de abuso (T1548)
  Una vez que Cobalt Strike se ejecutó en un sistema, tiene la capacidad de realizar varias técnicas utilizadas para obtener permisos más altos.
- ☑ BITS Jobs (T1197)
  BITS es una herramienta de Windows que Cobalt Strike puede usar para descargar cargas de pago
- ☑ Intérprete y secuencias de comandos (T1059)
  Cobalt Strike puede usar varias herramientas para ejecutar comandos, códigos y secuencias de comandos. Esto incluye PowerShell, Windows Command Shell, Visual Basic, Python y JavaScript.
- ☑ Explotación para la escalada de privilegios (T1068)
  Para obtener mayores privilegios, Cobalt Strike puede explotar vulnerabilidades dentro del sistema operativo.

☑ Captura de entrada (T1056)/Captura de pantalla (T1113)
Cobalt Strike también puede actuar como registrador de teclas y recopilar capturas de pantalla del sistema infectado.

RESPONDER

☑ **QUIÉN:** Desconocido
☑ **A QUIÉN:** Múltiples organizaciones en todo el mundo
☑ **POR QUÉ:** Cobalt Strike se utilizó en varias campañas centradas en diferentes objetivos. El motivo del ataque es obtener acceso a la red de organización interna para el movimiento lateral. Otra razón podría ser causar daños a las empresas al atacar la red comprometida con por ejemplo un ransomware.
☑ **QUÉ:** Principalmente para acceso remoto, red comprometida y movimiento lateral.
☑ **CÓMO:** Cobalt Strike es una herramienta comercial de formación de equipos rojos que se utiliza para simular ataques. La herramienta se utiliza para obtener el acceso inicial a la red de una empresa, así como para acciones posteriores con la red comprometida.
☑ **ESTRATEGIA:** Dependiendo de la empresa atacada, se desconoce la información sobre cómo se identificaron y reaccionaron ante el ataque.

RECUPERAR

☑ **IMPACTO:** El atacante puede obtener acceso completo a la red dentro de la empresa. Esto puede conducir a la divulgación de información, así como a más ataques, los cuales son ejecutados dependiendo del operador del ataque.
☑ **ESTRATEGIA DE RECUPERACIÓN:** Dependiendo de la empresa atacada, se desconoce la información sobre cómo fue su estrategia de recuperación.
☑ **MEJOR ESTRATEGIA:**
- Mantener actualizados los sistemas antivirus.
- Utilizar sistemas de detección y prevención de intrusiones
- Supervisar adecuadamente los sistemas en busca de actividades sospechosas
- Configurar adecuadamente los sistemas y deshabilitar los servicios no requeridos
- Concienciar a los empleados.
- Utilice la segmentación a nivel de red y limite la comunicación permitida al mínimo requerido

LECCIONES APRENDIDAS

Aunque es necesario crear herramientas de red teaming que puedan ser utilizadas para la simulación de ataques en una red y encontrar posibles puntos vulnerables, hay que tener en cuenta que dicha herramienta también puede ser comprometida y utilizada por un atacante.

CASE STUDY 8: ATAQUE ZERO-DAY - GRUPO DE HACKERS HAFNIUM ATACA SERVIDORES DE INTERCAMBIO

LA ORGANIZACIÓN OBJETIVO

A principios de 2021, los investigadores encontraron múltiples vulnerabilidades críticas en Microsoft Exchange Server que llevaron a una exposición masiva en todo el mundo. Las vulnerabilidades fueron utilizadas por múltiples organizaciones criminales, sobre todo el grupo HAFNIUM, antes de que Microsoft proporcionara los parches. Esto hizo que los ataques fueran especialmente difíciles de responder y recuperarse.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

El método aplicado para recopilar la información para este caso de estudio fue la investigación documental, las fuentes de información específicas se pueden encontrar en la sección de Referencias de este documento.

PREVENIR

Decenas de miles de empresas se vieron afectadas por este ataque. Debido a la exposición general de los servidores Microsoft Exchange a Internet y al potencial de eludir la autenticación del ataque, fue muy difícil de prevenir en primer lugar. Esto lleva a suponer que las diferentes prácticas de seguridad que se aplican a esas empresas no tuvieron ningún impacto.

IDENTIFICAR

Hay cuatro vulnerabilidades que llevaron a los ataques descritos. Las vulnerabilidades son **CVE-2021-26855, conocido como" ProxyLogon", CVE-2021-27065, CVE-2021-26857, y CVE-2021-26858**. La técnica para explotar estas vulnerabilidades se describe como **"Explotación para la ejecución de clientes" (T1203)** en el marco MITRE ATT&CK.

CVE-2021-26855 es un bypass de autenticación utilizando el proxy interno del servidor de Exchange. Con esto un atacante puede obtener acceso privilegiado al propio Servidor. Si se combina con otra vulnerabilidad como CVE-2021-27065, que permite escribir archivos arbitrarios en el sistema, o CVE-2021-26857, para obtener acceso al sistema (T1078) a través de una deserialización insegura, se crea una cadena de explotación sin restricciones.

Los ataques se produjeron antes de que Microsoft pudiera publicar un parche para las vulnerabilidades. Según numerosos recursos, este lapso de tiempo fue de unos 58 días de ataques Zero-day. El primer grupo al que se asoció a estas vulnerabilidades fue HAFNIUM. Más tarde, otros múltiples grupos comenzaron a aprovecharse de estas vulnerabilidades. Las capacidades del ataque permitían múltiples escenarios, desde la exfiltración de datos (T1567) hasta el despliegue de ransomware (T1486).

La siguiente es una lista de acciones tomadas por el grupo HAFNIUM utilizando este tipo de ataque:

- ☑ T1589 – recopilación de direcciones de correo electrónico de los usuarios a los que pretendían dirigirse

- ☑ T1071 – marco C2 de código abierto (por ejemplo, convenio)
- ☑ T1560 – 7-Zip, WinRAR para comprimir archivos robados para su extracción
- ☑ T1059 – exportar datos de buzones a través de PowerShell
- ☑ T1567 – extraiga datos a través de sitios compartidos, incluido MEGA
- ☑ T1105 – descarga de malware y herramientas en hosts comprometidos (por ejemplo, Nishang, PowerCat)
- ☑ T1003 – volcado de credenciales con LSASS, y las bases de datos de directorios activos (NTDS.DIT)
- ☑ T1505 – Despliegue de WebShells en hosts comprometidos (SIMPLESEESHARP, SPORTSBALL, etc.)

La identificación de los ataques puede tener lugar debido a la inspección de registros en posibles máquinas comprometidas. Microsoft publicó una guía sobre la detección de cada vulnerabilidad de acuerdo con su Indicador de Compromiso .

RESPONDER

QUIÉN: HAFNIUM (probable grupo patrocinado por estados con vínculos con China)
A QUIÉN: Diferentes empresas en todo el mundo, principalmente la industria de EE. UU.
POR QUÉ: Exfiltración de datos y probablemente ganancia de dinero a través de ransomware
QUÉ: Conocimiento de la empresa, como datos, direcciones de correo electrónico, buzones de correo
CÓMO: Aprovechamiento de múltiples vulnerabilidades en Microsoft Exchange Server para permitir la ejecución remota de código no autenticado
ESTRATEGIA: Escanear el rango de IPs de internet para recopilar las listas de IPs de los servidores Microsoft Exchange. Aprovechando las vulnerabilidades mencionadas para desplegar web shells, o beacons C2. Utilizando este acceso permitido para comprimir y exfiltrar datos a través de sitios web de intercambio en línea como MEGA. Desplegar ocasionalmente el ransomware "DearCry". Esto fue posible debido a la tardía disponibilidad del parche y a la mala gestión de parches de las empresas.

RECUPERAR

IMPACTO: Las consecuencias de este ataque pueden considerarse como pérdida de información, ya que tanto la exfiltración como el ransomware entran en esta categoría. Además, si las organizaciones intentaron pagar el rescate para recuperar sus datos, también terminaron con un daño financiero.

ESTRATEGIA DE RECUPERACIÓN: Dependiendo del ataque específico, la recuperación puede diferir. El proceso de recuperación de un ransomware puede llevar mucho tiempo. Todos los sistemas infectados deben reinstalarse o se debe restaurar una copia de seguridad.
Si las copias de seguridad se han almacenado en un sistema infectado, obviamente no se pueden usar para el proceso de recuperación.

La recuperación de la exfiltración de datos es diferente. Al principio, se deben aplicar los parches disponibles y se deben eliminar los rastros de web shells o beacons C2. Es importante evaluar qué y cuántos datos se robaron para medir el impacto.

MEJOR ESTRATEGIA

- ☑ Mantener actualizados los sistemas antivirus
- ☑ Utilizar sistemas de detección y prevención de intrusiones
- ☑ Supervisar adecuadamente los sistemas en busca de actividades sospechosas
- ☑ Configurar adecuadamente los sistemas y deshabilitar los servicios no requeridos
- ☑ Gestión rápida de parches para corregir vulnerabilidades lo antes posible
- ☑ Utilice la segmentación a nivel de red y limite la comunicación permitida al mínimo requerido

LECCIONES APRENDIDAS

El ataque Zero-day con cadenas de ataque parece muy intimidante. La clave para enfrentar estos desafíos es una adecuada segmentación de la red y monitoreo del sistema para identificar posibles ataques de manera oportuna. Los sistemas de prevención e intrusión en la red también pueden ayudar a detectar este tipo de ataques.
Lo que también es importante es que los parches para vulnerabilidades críticas deben aplicarse lo antes posible para remediar aún más los ataques.
Como otra lección aprendida, quiero mencionar a los investigadores de seguridad de DevCore que primero detectaron las vulnerabilidades y ayudaron con Microsoft en el proceso de parche. Esto refuerza la importancia de la investigación de seguridad independiente por una buena causa.

CASO DE ESTUDIO 9: WannaCry: CUANDO UN RANSOMWARE PARALIZA EL SISTEMA SANITARIO

LA ORGANIZACIÓN OBJETIVO

En 2017, un nuevo ransomware denominado **WannaCry (WannaCrypt)** dirigido al sistema operativo Windows, infectó a miles y miles de clientes en todo el mundo. En lugar de dirigirse a una organización específica, el ataque fue generalizado y afectó a muchas empresas de diferentes ámbitos.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

El método aplicado para recopilar la información para este estudio de caso fue la investigación documental, las fuentes de información específicas se pueden encontrar en la sección de Bibliografía de este documento.

PREVENIR

Varias empresas se vieron afectadas por este ataque, lo que hace suponer que las diferentes prácticas de seguridad que se aplican a esas empresas no tuvieron ningún impacto.

IDENTIFICAR

WannaCry es una aplicación maliciosa que se clasifica como **ransomware** ya que cifra los archivos específicos del usuario en un sistema objetivo. Esto conduce a la manipulación de los datos y su destrucción, ya que el propietario del sistema infectado no es capaz de descifrar los archivos. Esto posteriormente termina en un ataque de denegación de servicio debido a los archivos y datos perdidos.

Una de las principales características de WannaCry es su técnica de búsqueda automática de posibles sistemas objetivo que el ransomware intenta infectar también. Como este malware puede infectar otros sistemas a partir de uno ya infectado, también se le denomina gusano informático. Para lograr este objetivo, se utiliza un exploit de vulnerabilidad de software en el protocolo SMB de Microsoft Windows llamado Eternal Blue, que se corresponde con el MITRE ATT&CK ID T1210.

Antes de que el malware pueda propagarse e infectar otros sistemas, primero necesita buscarlos y encontrarlos. Esto se hace a través de varias técnicas como el escaneo de sistemas remotos (T1018), la enumeración de sesiones de escritorio remotas activas (T1563), el escaneo de nuevas unidades conectadas en el sistema infectado (T1120). Una vez que se encuentra un posible dispositivo o unidad remota, WannaCry intenta copiarse en el sistema objetivo y ejecuta su comportamiento malicioso.

Antes de que el ransomware comience su cifrado, realiza cambios en el sistema infectado para desactivar las opciones de recuperación, lo que se denomina T1490. Después busca archivos específicos del usuario en varios directorios (T1083) y comienza a cifrar cada archivo encontrado (T1486). Para la comunicación con el servidor de comando y control se utiliza la red Tor (T1573/T1090).

Para una identificación basada en el comportamiento de este ataque, se pueden utilizar las siguientes técnicas de MITRE ATT&CK:

- ☑ T1210: Explotación de servicios remotos
- ☑ T1018: Descubrimiento de sistema remoto
- ☑ T1563: Secuestro de sesión de servicio remoto (secuestro de RDP .002)
- ☑ T1120: Detección de dispositivos periféricos
- ☑ T1490: Inhibir la recuperación del sistema
- ☑ T1083: Descubrimiento de archivos y directorios
- ☑ T1486: Datos cifrados para impacto
- ☑ T1573: Canal cifrado (criptografía asimétrica .002)
- ☑ T1090: Proxy (.003 Multi-hop Proxy)

RESPONDER

En 2017 un nuevo ransomware denominado WannaCry (WannaCrypt) dirigido al sistema operativo Windows infectó a miles y miles de clientes en todo el mundo. En lugar de dirigirse a una organización específica, el ataque fue generalizado. Grandes empresas, algunas de las cuales dirigen sus negocios en todo el mundo, como los fabricantes de automóviles, se vieron afectadas por el ransomware. Sin embargo, también se vieron afectados otros grupos de organizaciones como el transporte público, los servicios sanitarios o los servicios de telecomunicaciones.

- ☑ **QUIÉN:** Desconocido
- ☑ **A QUIÉN:** Diferentes empresas en todo el mundo
- ☑ **POR QUÉ:** Gran daño debido a la pérdida de datos y probablemente ganancia de dinero de los atacantes
- ☑ **QUÉ:** Conocimiento de la empresa, como datos
- ☑ **CÓMO:** Infección de ransomware que se distribuyó a través de una vulnerabilidad encontrada en Microsoft Windows
- ☑ **ESTRATEGIA:** La nota de rescate utilizada por WannaCry apareció en la pantalla de los sistemas infectados. Los sistemas antivirus y los firewalls detectaron la infección y la propagación del ransomware y, por tanto, no evitaron que los sistemas sufrieran más infecciones y daños.

RECUPERAR

IMPACTO: Las consecuencias de este ataque pueden considerarse como una pérdida de información, ya que todos los archivos que fueron encriptados por el ransomware ya no son legibles. Además, si las organizaciones han intentado pagar el rescate para recuperar sus datos, también han terminado con un daño financiero.

ESTRATEGIA DE RECUPERACIÓN: El proceso de recuperación de un ransomware puede llevar mucho tiempo. Todos los sistemas infectados deben ser reinstalados o es necesario restaurar una copia de seguridad. Si se han almacenado copias de seguridad en un sistema infectado, obviamente no se pueden utilizar para el proceso de recuperación.

MEJOR ESTRATEGIA

- ☑ Mantener actualizados los sistemas antivirus
- ☑ Utilizar sistemas de detección y prevención de intrusiones
- ☑ Supervisar adecuadamente los sistemas en busca de actividades sospechosas
- ☑ Configurar adecuadamente los sistemas y deshabilitar los servicios no requeridos
- ☑ Gestión rápida de parches para corregir vulnerabilidades lo antes posible
- ☑ Concienciar de los empleados.
- ☑ Utilizar la segmentación a nivel de red y limitar la comunicación permitida al mínimo requerido

LECCIONES APRENDIDAS

Los ataques de ransomware son hoy en día comunes y pueden afectar a todas las empresas. Se recomienda encarecidamente seguir las prácticas de seguridad conocidas para que la

infraestructura informática sea lo más segura posible y así limitar los daños de un ataque al mínimo.

CASO DE ESTUDIO 10: ESPIAR DATOS PRIVADOS SENSIBLES

LA ORGANIZACIÓN OBJETIVO

En otoño de 2020, a nivel nacional se anunció una nueva alerta de seguridad. Muchas entidades públicas y privadas se vieron gravemente afectadas, al igual que en otras oleadas sucesivas anteriores, por **ataques de malware del tipo EMOTET**, lo que ha derivado en numerosos problemas. EMOTET es un **malware** que infecta ordenadores que ejecutan el sistema operativo Microsoft Windows a través de enlaces o archivos adjuntos maliciosos infectados (por ejemplo, PDF, DOC, ZIP, etc.).

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

La información necesaria para describir este ciberataque se recopiló a través de una entrevista con el técnico de TI de la empresa. La interacción se realizó con la condición de mantener la información sensible en el anonimato. Incluso si el entrevistado estaba dispuesto a describir el incidente, no se pudo obtener cierta información porque el problema se delegó a una empresa especializada y tuvo que investigarse por separado.

PREVENIR

Si bien se han realizado campañas de concientización por parte de entidades y organizaciones especializadas sobre las medidas a tomar, muchas organizaciones públicas y privadas se han visto afectadas, según informes existentes.

En el caso de la empresa analizada, desde la perspectiva de la ciberseguridad, se operaron procedimientos y mecanismos específicos, pero estos no fueron suficientes debido a la poca experiencia en el campo del dominio digital de algunos trabajadores.

IDENTIFICAR

Emotet es un troyano inicialmente asociado con el fraude bancario que, desde 2017, se ha limitado a la distribución de spam y payload secundario. Actualmente se pueden identificar numerosas variantes de Emotet y, lamentablemente, este malware continúa evolucionando hacia nuevas variantes con capacidades y técnicas de evasión más complejas.

Según las descripciones proporcionadas y el suplemento de los informes de los medios, los siguientes detalles estuvieron involucrados en la incidencia:

- ☑ Se recibió un correo electrónico de phishing con un archivo comprimido adjunto y con la contraseña incluida en el mensaje
- ☑ El malware fue encriptado y protegido con contraseña en un archivo de almacenamiento
- ☑ Evadió soluciones antimalware mediante el uso de archivos protegidos con contraseña como archivos adjuntos

- ☑ El cargador de troyanos contenía un código benigno de una DLL de Microsoft para evadir las soluciones antivirus.
- ☑ Secuestro de subprocesos para distribuir código malicioso utilizando archivos protegidos con contraseña como archivos adjuntos
- ☑ Se aprovecharon los sistemas comprometidos para enviar correos electrónicos maliciosos a otros contactos
- ☑ Los sistemas de correo electrónico se cierran temporalmente para detener una mayor propagación del troyano
- ☑ Redes internas afectadas

"EMOTET era mucho más que un simple malware. Lo que hacía que EMOTET fuera tan peligroso es que el malware se ofrecía en alquiler a otros ciberdelincuentes para instalar otros tipos de malware, como troyanos bancarios o ransomwares, en el ordenador de la víctima." (EUROPOL, 2022)

De acuerdo con el marco MITRE ATT&CK, esta incidencia se puede describir de la siguiente manera:

1. T1566.001 – archivo adjunto de Spearphishing
2. T1204.002 - Ejecución de usuario: archivo malicioso
3. T1027 - Archivos o información oculta
4. T1036 – Masquerading
5. T1586.002 – Cuentas comprometidas: cuentas de correo electrónico
6. T1586.002 – Cuentas comprometidas: cuentas de correo electrónico
7. T1499 - Denegación de servicio de punto final
8. T1498 - Denegación de servicio de red

RESPONDER

QUIÉN: El atacante no pudo ser identificado con precisión. Solo se conocía el lugar de origen, Vietnam.

A QUIÉN: objetivo no específico.
POR QUÉ: Recopilación de datos confidenciales y pagos de ransomware.
QUÉ: Datos de empresa/usuarios.
CÓMO: archivo adjunto de Spearphishing, ejecución de scripts, inyección de procesos.
ESTRATEGIA: La amenaza comenzó en un ordenador sin antivirus y se ha extendido lateralmente. Se realizó un proceso de limpieza por una empresa especializada en IT&C.

RECUPERAR

IMPACTO: Las principales consecuencias del ataque fueron las siguientes:

- ☑ Pérdida de datos
- ☑ Interrupción regular de la actividad

- ☑ Sistema comprometido
- ☑ Costos financieros

ESTRATEGIA DE RECUPERACIÓN: La estrategia de recuperación se centró en limpiar y reinstalar los equipos comprometidos, limpiar y/o reinicializar los buzones de correo comprometidos.

MEJOR ESTRATEGIA

- ☑ Instalar y mantener actualizado un Antivirus/Antimalware
- ☑ Adoptar una prevención de intrusiones en la red
- ☑ Restringir contenido basado en la web
- ☑ Asegurar la conciencia del usuario ante la ciberseguridad
- ☑ Mejores políticas de contraseña
- ☑ Gestión de cuentas privilegiadas
- ☑ Deshabilitar o quitar función o programa
- ☑ Prevención de ejecución
- ☑ Auditoría
- ☑ Gestión de cuentas de usuario
- ☑ Prevención de comportamientos en el punto final
- ☑ Políticas de uso de la cuenta

LECCIONES APRENDIDAS

Incluso si Emotet fue eliminado a través de una actividad concertada internacional, queda por ver si esto tendrá un impacto duradero.

Se debe tener en cuenta que los programas maliciosos utilizan casi las mismas técnicas para penetrar y propagarse en la naturaleza, por lo que es obligatorio ser consciente y cuidadoso, ya que los ciberataques seguirán existiendo en el futuro. Medidas tales como considerar comunicarse con el mundo usando un ordenador aislado de la red que aloja la infraestructura crítica, usar soluciones de seguridad capaces y actualizadas, considerar tener las últimas actualizaciones, son algunas de las que deben preverse.

CASO DE ESTUDIO 11: ACCESO ILÍCITO A LAS CREDENCIALES

LA ORGANIZACIÓN OBJETIVO

As any modern company, in the case of described situation, electronic communications via the Internet with their customers and suppliers is the most preferred way. Within this type of communication one of the most used is the electronic e-mail. It allows asynchronously keeping contact with stakeholders managed in an efficient way by more than one person. The company found over half a century on the market has been strongly developed on digitalisation in every department, and in this context is included also the customers relation department. For related employees has been created an e-mail group for managing the online requests from dedicated computers protected by antivirus and spam filtering functionality on the email server.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

The information needed to describe this cyber-attack was collected through an interview with one of the IT technicians of the company. The interaction was performed with the condition of keeping sensitive information anonymously. Even if the interviewee was willing to describe the incident, some information could not be obtained because the problem was managed by a different team. La información necesaria para describir este ciberataque se recopiló a través de una entrevista a uno de los técnicos informáticos de la empresa. La interacción se realizó con la condición de mantener la información sensible en el anonimato. Incluso si el entrevistado estuviera dispuesto a describir el incidente, no se pudo obtener cierta información porque el problema fue manejado por un equipo diferente.

PREVENIR

Aunque la Dirección Nacional de Ciberseguridad ha llevado a cabo campañas de concienciación sobre las medidas a tomar, muchos públicos, organizaciones privadas y particulares se han visto afectados, según los informes existentes.

La empresa hizo cumplir el uso de herramientas de seguridad y regulación personalizada en el trabajo en línea, pero esto no fue suficiente debido a la básica experiencia en el campo del dominio digital de algunos empleados.

IDENTIFICAR

Phishing es un término global para un **ataque de ingeniería social** que se lleva a cabo actualmente a través de correos electrónicos o aplicaciones de redes sociales. Normalmente, los ciberdelincuentes envían mensajes masivos no solicitados. Quieren dirigirse al mayor número posible de personas para atrapar a algunas de ellas con su truco.

Los ciberdelincuentes intentan explotar la tendencia de algún tipo de 'gran oferta' o con algunas instrucciones administrativas. Muchos de estos tipos de mensajes parecen ser legítimos, ya que utilizan la misma identidad visual que las empresas conocidas, los servicios en línea o las aplicaciones. Algunos ejemplos incluyen empresas como Google, Amazon, Microsoft, Yahoo, LinkedIn, etc. o servicios y aplicaciones bancarias populares, como la gestión de correo electrónico basado en la web.

Se pretende lograr la credibilidad copiando el esquema de color, el estilo, el logotipo y los lemas de la identidad copiada. Se utilizan las típicas líneas de asunto atractivas.

Phishing es un término que engloba los ataques de tipo ingeniería social que se llevan a cabo actualmente a través de correos electrónicos o aplicaciones de redes sociales.

Según la descripción proporcionada y los informes de los medios complementarios, los siguientes detalles estuvieron involucrados en la incidencia:

- ☑ Se ha recibido un correo electrónico de phishing diseñado con ingeniería social que reclamaba la necesidad de cambiar urgentemente la contraseña de acceso para evitar la finalización del servicio;
- ☑ El suministro de credenciales a los atacantes condujo al acceso en la cuenta de correo electrónico y la interrupción del acceso legítimo mediante el cambio de contraseña;
- ☑ La cuenta comprometida se usó para mensajes de phishing no solicitados enviados a los contactos existentes y otras direcciones propiedad del atacante;
- ☑ Debido a los mensajes masivos de spam enviados a través de internet, el servicio de correo electrónico se incluyó en la lista negra, de modo que se interrumpió el funcionamiento normal;
- ☑ El sistema de correo electrónico se suspendió temporalmente para detener más spam;
- ☑ Las operaciones en línea se vieron afectadas.

De acuerdo con el marco MITRE ATT&CK, esta incidencia se puede describir de la siguiente manera:

1. T1598.001 - Spearphishing de servicio
2. T1598.002 - Spearphishing de archivo adjunto
3. T1598.003 - Spearphishing de link

RESPONDER

- ☑ **QUIÉN:** No se ha podido identificar con precisión al atacante, ya que se han registrado los orígenes de varios países. Es posible que se haya utilizado una VPN.
- ☑ **A QUIÉN:** objetivo no específico
- ☑ **POR QUÉ:** Recopilación de datos confidenciales y extorsión con dinero
- ☑ **QUÉ:** Datos de empresa/usuarios
- ☑ **CÓMO:** Phishing, robo de credenciales.
- ☑ **ESTRATEGIA:** La amenaza comenzó abriendo un correo electrónico suplantado, accediendo a enlaces falsificados y enviando datos confidenciales. El equipo de TI llevó a cabo el restablecimiento de credenciales y la exclusión de los servicios de listas negras.

RECUPERAR

IMPACTO: Las principales consecuencias del ataque fueron las siguientes:

- ☑ Pérdida de credenciales
- ☑ Interrupción regular de la actividad
- ☑ Sistema comprometido

ESTRATEGIA DE RECUPERACIÓN: La estrategia de recuperación se centró en restablecer las credenciales y limpiar los correos electrónicos comprometidos de clientes.

MEJOR ESTRATEGIA

- ☑ Instalar y mantener actualizado un sistema de filtrado de correo electrónico/antivirus/antimalware
- ☑ Adoptar una prevención de intrusiones en la red
- ☑ Restringir contenido basado en la web
- ☑ Asegurar la conciencia del usuario
- ☑ Mejores políticas de contraseña
- ☑ Gestión de cuentas privilegiadas
- ☑ Auditoría
- ☑ Gestión de cuentas de usuario
- ☑ Prevención de conductas en el punto final
- ☑ Políticas de uso de la cuenta

LECCIONES APRENDIDAS

Aunque el phishing no es una técnica nueva, sigue siendo una de las principales formas de muchos ataques de ciberseguridad.

Hay que tener en cuenta que los malwares utilizan prácticamente esta técnica para penetrar y propagarse, por lo que es obligatorio estar atento y tener cuidado ya que los ciberataques de este tipo seguirán existiendo. Medidas como considerar el uso de servicios de correo electrónico protegidos y mejor actualizados, más conciencia sobre el acceso a los correos electrónicos y analizar adecuadamente la legitimidad del remitente.

CASO DE ESTUDIO 12: APLICACIONES OBSOLETAS EXPUESTAS EN LÍNEA

LA ORGANIZACIÓN OBJETIVO

En la actualidad, muchas empresas han cambiado la forma de prestar sus servicios al pasar a ofrecerlos de manera online. Este es el caso del ejemplo en desuso, en el que en un mostrador se prestaban servicios de tipo financiero iniciados en 1998 y que han migrado a internet desde hace más de una década. El nuevo enfoque mejoró la actividad general de la empresa y la satisfacción de los clientes. Sin embargo, estos logros sólo fueron posibles después de un importante esfuerzo en el desarrollo del software necesario. Esta aplicación en línea permitía a los clientes y a los empleados realizar las operaciones. La plataforma desarrollada en ese momento se mantuvo hasta la liberación de la nueva actualización. Con el tiempo, el número de empleados se redujo debido a la automatización de los procesos existentes y a los cambios del mercado. La actualización a la nueva versión se retrasó, ya que se necesitaba un hardware y un software considerable.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

La información necesaria para describir este ciberataque se recopiló a través de una entrevista con el director general de la empresa. La interacción se realizó con la condición de mantener la información sensible en el anonimato.

PREVENIR

Si bien se han realizado campañas de concientización por parte de la Dirección Nacional de Seguridad Cibernética sobre las medidas a tomar, muchas organizaciones públicas o privadas ignoran o demoran la decisión y acciones necesarias para actualizar sus sistemas de información.

La empresa hizo cumplir el uso de soluciones de seguridad conocidas, cortafuegos, segmentación de red, etc., pero esto no fue suficiente ya que quedó expuesta la vulnerabilidad en uno de los módulos de software operados.

IDENTIFICAR

Ataques de inyección de flujo abusar de la capacidad de una aplicación web en línea para aceptar contenido cargado, como diferentes tipos de documentos o archivos de imágenes. Usando el enfoque de inclusión de archivos remotos, un atacante puede explotar la vulnerabilidad en el código del lado del servidor para aceptar una URL en otro sitio como una entrada válida. Esta acción luego se usa para ejecutar el código malicioso del atacante. Además, la inclusión de archivos locales se puede utilizar para obtener una aplicación web que devuelva el contenido deseado del sistema de archivos local.

Un ejemplo popular se encuentra en el caso del marco PHP utilizado por WordPress que permite al hacker acceder a su archivo de configuración. Este ataque también puede permitir el acceso para descargar cualquier archivo de código fuente PHP que ejecute el sitio web, lo que ofrece nuevas posibilidades para otras vulnerabilidades de seguridad. Las versiones recientes de PHP están protegidas contra la inclusión de archivos remotos de forma predeterminada, pero si por error se expone la inclusión de archivos locales, este tipo de ataque aún es posible.

Según la descripción proporcionada, los informes técnicos complementarios, los boletines de seguridad y vulnerabilidades, los siguientes detalles estuvieron involucrados en el incidente:

- ☑ Mediante un ataque de tipo fuerza bruta, se accede ilegítimamente a una cuenta protegida con una contraseña débil;
- ☑ Las credenciales descubiertas permiten cambiar los datos asociados a la cuenta;
- ☑ La cuenta comprometida permitió que se expusiera la vulnerabilidad de inyección de flujo y se utilizó la ejecución de código no deseado en el servidor para eliminar los registros del historial de acceso;
- ☑ Debido a la ejecución descontrolada del código del lado del servidor, algunos módulos de la aplicación se vuelven inutilizables y conducen al cierre del servicio, por lo que se interrumpió el funcionamiento normal;
- ☑ El sistema se desconectó de internet temporalmente para una mayor investigación relacionada con el mal funcionamiento de la aplicación web;
- ☑ Las operaciones en línea se vieron afectadas.

De acuerdo con el marco MITRE ATT&CK, esta incidencia se puede describir de la siguiente manera:

1. T1110.001 - Adivinar la contraseña
2. T1078 - Acceso a cuentas válidas
3. T1518 - Descubrimiento de software
4. T1082 - Descubrimiento de información del sistema
5. T1007 - Detección de servicios del sistema
6. T0826 - Pérdida de disponibilidad.

RESPONDER

- ☑ **QUIÉN:** El atacante no pudo ser identificado con precisión.
- ☑ **A QUIÉN:** objetivo no específico
- ☑ **POR QUÉ:** Recopilación de datos confidenciales y denegación de servicio
- ☑ **QUÉ:** Datos de empresa/usuarios
- ☑ **CÓMO:** Ataque de fuerza bruta, robo de credenciales y ejecución de código por inyección de flujo.
- ☑ **ESTRATEGIA:** La amenaza comenzó con un ataque de fuerza bruta que condujo a un descubrimiento de credenciales débil, explotando la vulnerabilidad en un módulo de software de acceso no público y luego la ejecución de código no autorizado. La débil estrategia de protección de acceso en línea, el módulo de software obsoleto y el código sin mantenimiento son la causa principal de la incidencia.

RECUPERAR

IMPACTO: Las principales consecuencias del ataque fueron las siguientes:

- ☑ Pérdida de credenciales
- ☑ Sistema comprometido
- ☑ Interrupción regular de la actividad.

ESTRATEGIA DE RECUPERACIÓN: La estrategia de recuperación se centró en la actualización de la plataforma principal, reescribiendo una parte importante del código.

MEJOR ESTRATEGIA

- ☑ Instalar y mantener un software actualizado
- ☑ Hacer cumplir la política de contraseñas seguras
- ☑ Políticas de uso de la cuenta
- ☑ Adoptar un mecanismo de autenticación de dos factores
- ☑ Adopte una prevención de intrusiones en la red
- ☑ Restringir el acceso remoto
- ☑ Asegurar la conciencia del usuario
- ☑ Implementar una auditoría de seguridad periódica
- ☑ Gestión de cuentas de usuario
- ☑ Prevención de conductas en el punto final.

LECCIONES APRENDIDAS

Incluso si se sabe que el software en ejecución obsoleto es propenso a las vulnerabilidades de seguridad, sigue siendo una de las principales formas en muchos ataques de seguridad cibernética.
Las aplicaciones web accesibles en todo el mundo están expuestas a muchas vulnerabilidades y, como consecuencia, requieren una atención especial desde muchas perspectivas.
Medidas como considerar la actualización constante del software, las mejoras y la adopción de nuevas técnicas y soluciones para los mecanismos de autenticación, la adopción de un proceso de auditoría regular son algunas de las medidas comunes que se pueden considerar.

CASO DE ESTUDIO 13: LOS RIESGOS DE UN ATAQUE REALIZADO POR UN ANTIGUO EMPLEADO

LA ORGANIZACIÓN OBJETIVO

La organización donde ocurrió el ciberataque, se dedica al seguimiento comercial, en la rama automotriz, con aproximadamente 2000 empleados. Ubicada en la provincia de Paraná y Santa Catarina en Brasil.

El ciberataque tuvo como objetivo el área de tecnologías de la información, debido al conocimiento que tenía el hacker al ser un ex-empleado de la organización, dándole el beneficio de conocer el sistema.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

La información de este caso de estudio se basa en los riesgos de un ciberataque liderado por un exempleado. El caso de estudio se realiza desde el punto de vista de la organización que sufrió el ciberataque.

El objetivo general de este caso de estudio es demostrar la importancia que las empresas deben prestar en relación con la ingeniería social dentro de sus entornos, con el fin de evitar invasiones y/o fraudes causados por la imprudencia o la asistencia involuntaria de los empleados.

PREVENIR

Para evitar posibles daños, la empresa ya contaba con un departamento de TI que administraba firewalls, herramientas de fuga de información y encriptación de datos.

IDENTIFICAR

En este caso de estudio, la huella comenzó con varias visitas a la página web de la empresa, con la intención de entender su dinámica, sus negocios y especialmente sus marcas (considerando que el atacante dirigió la búsqueda de datos que el hacker aún no conocía).). Cuando la huella comenzó y la información interna y específica de la organización está del lado del atacante, pasó a hacer conexiones a una de las tiendas de la empresa para descubrir los nombres de los gerentes y personas que podrían tener acceso privilegiado dentro de la organización.

Para ello, el atacante se hizo pasar, vía telefónica, como un cliente que tenía problemas legales con la empresa. Para solucionar este problema, la empresa habría llamado al cliente y le habría pedido que hablara con el gerente de la tienda en cuestión, dado que él sería la persona con mayor autonomía para responder ante tal situación. Debido a esta interacción, se logró fácilmente el nombre del gerente, la ubicación donde trabajaba y el número de teléfono.

Luego de esta llamada telefónica, se intentó contactar al gerente en para verificar la información recopilada. El restablecimiento de contraseña se realizó al contactar con el área de tecnologías de la información, haciéndose pasar por el propio empleado, con el fin de que dicha área le informara de los datos de acceso del usuario.

Con un poco de persuasión y el argumento de que los datos para una reunión dependían de este acceso, finalmente el técnico restableció la contraseña e informó de la nueva contraseña por teléfono. Más que eso, fue posible convencerlo de configurar un acceso VPN (tecnología de acceso remoto al entorno de la empresa) para que el hipotético usuario pudiera trabajar desde fuera de la oficina.

RESPONDER

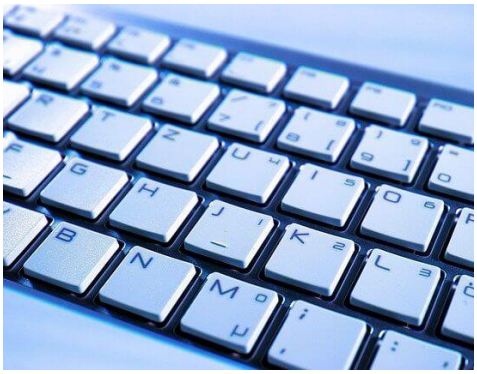
QUIÉN: El atacante era un ex empleado;
A QUIÉN: Una organización que trabaja en el seguimiento comercial, en la rama automotriz;
POR QUÉ: El ataque fue dirigido a la organización con motivos desconocidos;
QUÉ: La propiedad objetivo era el área de tecnología de la información con el fin de recopilar información privilegiada de la organización y datos personales de los empleados actuales;

CÓMO: El ataque comenzó con la obtención del nombre del gerente de una tienda, procedió a contactar al área de tecnología de la información de la empresa y los convenció de restablecer la contraseña. De esa manera, el exempleado se hizo pasar por el gerente y tuvo acceso a todo lo relacionado con información privilegiada, datos personales de empleados y clientes.

RECUPERAR

La empresa comenzó a formar a los colaboradores para que presten atención al tipo de información que suelen pasar a terceros, especialmente si se trata de información crítica. Nunca, bajo ninguna circunstancia, un empleado debe pasar información crítica, como contraseñas, por teléfono. Estos deben ser proporcionados a los interesados a través de medios seguros, tales como cartas certificadas o a través del administrador responsable.

También formar para que los empleados sean conscientes de tener cuidado con la información que comparten en Internet. Formación enfocada en los riesgos que la información compartida puede traer en el trabajo, pero también traer a la vida personal, como secuestros, detalles de vida y seguridad personal.



Esta empresa es consciente de la necesidad de proporcionar las condiciones técnicas y físicas para la aplicación de buenas prácticas de seguridad, pero, sobre todo, de valorar y fomentar la adopción de las mejores prácticas y protocolos de seguridad más estrictos por parte de sus empleados, ya sea en un entorno corporativo o personal para controlar, de la mejor manera posible, el factor más débil de la seguridad de la información: el factor humano.

LECCIONES APRENDIDAS

La organización debe establecer la información en un procedimiento de patrón simple que pueda frustrar al hacker. Este procedimiento tiene 3 etapas:

- ☑ **Público:** Información que puede ser entregada a cualquier persona, por ejemplo, a contactos comerciales y corporaciones específicas, información entre clientes y negocios de la corporación;
- ☑ **Privado:** Información que no puede ser entregada a ninguna persona y que solo concierne al entorno corporativo. Quedan comprendidas en esta categoría las informaciones referentes a procedimientos internos, datos corporativos administrativos y aspectos estratégicos de la empresa;
- ☑ **Confidencial:** Información y datos que no deben ser compartidos dentro y fuera de la empresa, tales como datos de registro de empleados, sueldos, resultados de sectores y acciones estratégicas que atañen únicamente a la dirección o presidencia.

Asimismo, las organizaciones deben contar con procedimientos internos para protegerse de ataques de ingeniería social. Los operadores deben estar bien formados sobre los procesos que deben seguir y las acciones que deben tomar en situaciones donde la empresa se siente atacada, como transferir la llamada a una persona capacitada para manejar este tipo de situaciones. Acciones simples pueden hacer que el ataque falle, inmediatamente se puede hacer una lista de verificación inicial para confirmar los datos del solicitante, ya dificultaría el acceso del hacker. Teniendo en cuenta que los datos personales no son algo muy difícil de obtener, los técnicos

podrían adoptar un proceso de devolución del contacto al número de teléfono registrado del empleado, a fin de confirmar que efectivamente se trata del empleado en cuestión.

CASO DE ESTUDIO 14: LOS CIBERATAQUES COMO UN NUEVO DESAFÍO PARA LA SEGURIDAD NACIONAL

LA ORGANIZACIÓN OBJETIVO

Entidades gubernamentales portuguesas (especialmente el Ministerio de Administración Interior), las Fuerzas de Seguridad y las grandes empresas.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

La información para este estudio de caso fue recabada a través de una investigación documental referente a una tesis de maestría, donde el autor realiza un estudio y varias entrevistas exploratorias a especialistas y responsables de las fuerzas de seguridad nacional, con el fin de concluir si el fenómeno hacktivista plantea una amenaza para las fuerzas de seguridad portuguesas.

PREVENIR

Para prevenir los ataques, uno de los pasos que da el equipo informático responsable de la ciberseguridad en estas organizaciones es vigilar los canales sociales, por ejemplo: IRC's (Internet Relay Chat), todo tipo de chats, Facebook, todo aquello que es posible obtener información en internet, también un seguimiento e intentar ver si hay alguna acción sospechosa.

Según el "modus operandi", definido por los términos del grupo Anonymous (Portugal), inicialmente anuncian en las redes sociales (IRC's y Facebooks), las acciones que realizarán y es entonces cuando comienzan a comunicarse entre ellos. Luego utilizan canales de chat privados para comunicarse entre ellos, lo que motivó la implementación del SOC (Centro de Operaciones de Seguridad) del MIA (Ministerio de Administración Interna), para prepararse para este tipo de ataques.

IDENTIFICAR

Las consecuencias de estos ataques variaron, dependiendo del tipo de ataque. Muchos trataban de un ataque de denegación de servicio, (DOS, DDOS), que provoca un agotamiento de los recursos en términos de sistemas o comunicaciones. También se trató algunos tipos de intentos de ataques de intrusión como inyección SQL y desconfiguración. El phising por correo electrónico, también es uno de los ataques más frecuentes, que a veces da lugar al acceso a información privada.

En noviembre de 2011 se llevó a cabo un ataque a la página web del Sindicato Nacional de la Carrera de Jefes de PSP, con divulgación de datos personales y confidenciales (patentes, teléfonos y direcciones de correo electrónico) de 107 funcionarios de

"Los ataques DDoS han aumentado constantemente su frecuencia en los últimos años. Según un informe de Cloudflare, los ataques DDoS ransom aumentaron casi un tercio entre 2020 y 2021 y se dispararon un 75% en el cuarto trimestre de 2021 en comparación con los tres meses anteriores." (Cook, 2022)

RESPONDER

Un ataque a la Policía de Seguridad Pública fue asumido por el grupo LulzSec Portugal. El grupo portugués Anonymous ha denunciado varios ataques contra sitios web gubernamentales e instituciones relevantes. Generalmente, el perfil del hacker es el de alguien joven, en edad escolar, del nivel secundario. Puede haber una u otra situación en la que ya sean personas más adultas, quizás con menos conocimientos en el área tecnológica pero insatisfechas con la sociedad.

Este tipo de ataque está disponible para cualquier ciudadano. Solo hace falta que la persona busque en internet, herramientas, métodos y grupos y empiece a participar. Estos grupos de Anónimos, en el momento de los ataques, realizaban talleres de cómo hacer un ataque, cursos de "abc" de cómo entender el ataque. Proporcionan herramientas ya desarrolladas y que cualquiera puede acceder al sitio, solo es necesario insertar la dirección de destino y una aplicación desarrollada para el ataque.

La mayoría de los atacantes, es decir, jóvenes aún en la escuela, usan herramientas que son usadas por muchos especialistas, esos especialistas son personas con un grado académico más avanzado, y mayores, que usan herramientas ya desarrolladas con el propósito de ciberatacar. Es decir, en internet es posible buscar y obtener información para realizar el ataque, cómo hacerlo y qué tipo de herramientas se utilizan para ayudar a realizar el ataque.

El ataque realizado por LulzSec Portugal se justificó en Twitter alegando que, como respuesta a la acción de los agentes provocadores, se infiltraron en una manifestación organizada por ellos.

Pero la mayoría de las veces estos ataques ocurren porque estas personas buscan visibilidad o poner en peligro las organizaciones, ya que esto a menudo tiene que ver con el descontento de la gente en cuanto al contexto actual en el que viven los ciudadanos portugueses, y la gente suele demostrar su descontento de esta manera. Otras veces es solo una broma a los agresores, con edades entre 16 o 17 años, que no tienen muchas preocupaciones en términos sociales, muchas veces es porque los amigos lo hacen, y para promocionarse dentro del grupo de amigos, otras veces son experiencias que hacen porque es la era de experimentar cosas nuevas. La mayoría de las veces no se dan cuenta del impacto que pueden tener estos ataques.

Todo comienza con un grupo de hackers que tienen el conocimiento técnico y desarrollan herramientas para ser utilizadas por grupos de personas que no tienen ese mismo conocimiento, lo que hace que el proceso de piratería sea fácil para cualquiera.

Una característica de los grupos portugueses es atacar sitios web desprotegidos y explotar vulnerabilidades. Planean ataques a IRC (Internet Relay Chat) y salas de chat, no asumen su identidad y usan apodos. Los hacktivistas portugueses utilizan las herramientas disponibles online para realizar los ataques, es decir, "no fabrican programas a medida, sino que utilizan los que están disponibles en la red". En cuanto a las personas que asumen la organización y liderazgo de este tipo de iniciativas, muchas veces son personas con poca experiencia técnica, que se dedican a hacer anuncios y difundir las acciones a desarrollar, y muchas veces "aquellas que incluso tienen habilidades técnicas muy especializadas", no tienen idea de que son los más competentes y especializados del grupo, piensan que son personas que saben poco y que solo están ayudando a otros que saben más".

El grupo Anonymous utiliza métodos de hacking convencionales como Havij114 e inyección SQL, siendo su principal innovación la creación de sitios web que realizan ataques DoS.

RECUPERAR

Las posibles consecuencias son el robo de información, la indisponibilidad de los servicios y desfiguraciones del sitio donde se realizan cambios en la información, ya que los piratas informáticos a veces eliminan información, también pueden agregarla.

Estos ataques pueden poner en riesgo la confianza depositada por los ciudadanos en las instituciones que son víctimas de estos grupos, pero también la identificación de vulnerabilidades y la influencia de otras personas con determinados ideales son situaciones que pueden darse.

Estos tipos de ataques evolucionan y las técnicas mejoran con el tiempo, y las organizaciones deben adaptarse y evolucionar para la protección de su red. Se vieron obligados a dejar de acceder a la red hasta que se dieran las condiciones para garantizar que se mantuviera la seguridad de la información interna. Y ya lo han hecho, en total, durante una hora como mucho. En ocasiones, algunos servicios también han estado inaccesibles durante la noche.

CNCseg (Centro Nacional de Ciberseguridad), que tendrá más que ver con el tema de la defensa nacional, existe el Centro de Ciberdefensa, que es competencia del Ministerio de la Defensa Nacional, cuya acción principal es el ataque a los hackers que puedan estar desarrollando ataques, haciendo la detección y contraataque de estos elementos.

MIA participará, al menos en CNCseg, están trabajando en conjunto con el GNS que es la entidad que tiene esta competencia y será uno de los insumos de información para este tipo de ciberseguridad, la idea es que este centro tenga la información sobre lo que está pasando a nivel nacional, el objetivo es recopilar información tanto de los centros tecnológicos de la Administración Pública, la banca, la industria, los distintos ámbitos de la sociedad portuguesa y, con eso, tener una idea del impacto y alcance que puede tener cierto tipo de ataque.

LECCIONES APRENDIDAS

El hacktivismo es visto como un nuevo reto para las instituciones y, especialmente, en el caso de las Fuerzas y Cuerpos de Seguridad, un ataque hacktivista puede tener consecuencias nefastas, que incluso pueden llegar a influir en el desempeño de sus misiones, considerándose por tanto una amenaza real, en el sentido de que se caracteriza por contradecir los objetivos de la organización, produciendo, por regla general, daños materiales y/o morales.

La capacidad de los grupos hacktivistas para realizar un ataque suele ser baja, ya que utilizan herramientas disponibles en la red y son poco innovadores en cuanto al hackeo, aprovechando la explotación de vulnerabilidades existentes. En cuanto a la oportunidad, cualquier persona desde un ordenador con acceso a la red y con algún conocimiento o voluntad de aprender de la información disponible en la red es capaz de desarrollar un ciberataque, y este hecho se convierte en preocupante para las fuerzas de seguridad.

En cuanto a la seguridad informática, se suele decir que no existe la seguridad total y que no existen sistemas 100% seguros, por lo que el gobierno y Portugal no son una excepción. Lo que se ha logrado es la creación de un conjunto de infraestructuras que permiten una estructura de seguridad que puede corresponder y dar respuesta a este tipo de fenómenos: el recientemente creado CNCseg, realizado por la PJ con el fin de luchar contra el cibercrimen. Educar a las personas es ciertamente algo que desafiará a todos a darse cuenta de que también usamos nuevas tecnologías, plataformas de Internet y otras redes que tienen el poder de cambiar la seguridad de los ciudadanos.

Consecuencias de un ataque hacktivista a las fuerzas de seguridad nacional:

- ☑ Directas: consecuencias económicas, sociales, políticas y seguridad.
- ☑ Indirectas: el sentimiento de seguridad, la desregulación social y, en definitiva, la soberanía del país, las instituciones y las familias.

"El ransomware costará a las víctimas más de 265.000 millones de dólares anuales en 2031". (Cybersecurity Ventures).

CASO DE ESTUDIO 15: LA "EDAD DEL ORO" DEL "RANSOMWARE". CÓMO PREVENIR Y HACER FRENTE A UN SECUESTRO DE DATOS

LA ORGANIZACIÓN OBJETIVO

La mayoría de las empresas portuguesas están en la "generación 3" de ciberseguridad y los ataques están en la "generación 6". En este caso de estudio conocemos cómo proceder para prevenir ataques de ransomware como el que enfrenta el grupo IMPRESA, cada vez con más frecuencia.

IMPRESA es el grupo de medios portugués más grande y opera en tres áreas de negocios: prensa, digital y televisión.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

La información para este caso de estudio se obtuvo a través de un artículo de noticias sobre la prevención de ransomwares, que incluye la entrevista de Rui Duro, un experto en ciberseguridad.

PREVENIR

Los tiempos de pandemia facilitaron el crecimiento de este tipo de ataques de ransomware. Por un lado, el trabajo en casa, que conduce a la dispersión de los sistemas y aumenta el riesgo. Por otro lado, cada vez más aplicaciones están migrando sistemas a la "nube".

"Esto tiene varios riesgos asociados", dice Rui Duro. Los sistemas ahora están "en otro proveedor de servicios" y es necesario "comprar tecnología también para la nube porque no es segura en sí misma". Para el especialista, "esta evolución a la 'nube' fue muchas veces más rápida que la evolución del conocimiento de los empleados de tecnologías de la información".

Por otro lado, muchas empresas se han visto superadas por la sofisticación de los ataques. “Nosotros (Grupo IMPRESA) estamos en la generación 6 de ataques y la mayoría de las empresas todavía están en la generación 3, en una etapa muy temprana de protección, dada la evolución de los ataques. La mentalidad tiene

que cambiar, tiene que haber presupuesto y recursos para adaptarse a esta nueva realidad”, explica Rui Duro.

IDENTIFICAR

En las páginas de los sitios web del grupo, aparece un mensaje similar al que recibió SIC (canal de televisión portugués): “Los datos internos de los sistemas fueron copiados y eliminados. 50 TB de datos están en nuestras manos. Contacta con nosotros si quieres recuperar los datos”.

Rui Duro explica que “normalmente el ransomware aparece en las empresas a través de lo que llamamos la colocación de una 'carga útil' inicial dentro de la empresa”.

Esto sucede de diferentes maneras, como por ejemplo a través de un ataque de phishing a un elemento de la empresa. Otras veces, alguien de la empresa "descarga" el malware sin darse cuenta. Todavía hay una tercera forma, cuando los actores tienen el propósito de atacar a una empresa específica y están buscando vulnerabilidades: este es un "ataque objetivo".

Una vez que el malware inicial está dentro de la empresa, descarga un segundo malware, que ejecuta el ransomware. Luego comienza a hacer un “escaneo”, buscando servidores y otros sistemas. El objetivo es obtener el mayor beneficio posible. Según el experto, para los delincuentes "no tiene sentido cifrar un ordenador o dos, la idea es cifrar la mayor cantidad de ordenadores posible, y preferiblemente los vitales".

Luego, los piratas informáticos instalan el malware en tantos sistemas como sea posible, pero no cifra los datos de inmediato. Por lo general, "se deja durante varias semanas, a veces más".

Aquellos que atacan saben que una de las formas en que las empresas se recuperan es a través de copias de seguridad, por lo que esperan que haya una copia de seguridad y, tan pronto como se restaura, hay una infección nuevamente.

Cuando se lleva a cabo el cifrado, los ciberdelincuentes presionan a las empresas, generalmente para pedir un rescate en efectivo, generalmente en criptomonedas.

RESPONDER

Dos días después de que el grupo de hackers “Lapsus$ Group” atacara los sitios web del grupo Impresa, los sitios aún no estaban disponibles.

La Policía Judicial portuguesa confirmó que investiga el caso, junto con el Centro Nacional de Ciberseguridad (CNCS), como ya había adelantado el grupo mediático.

Este retraso en el restablecimiento de los sistemas es común en ataques como este. Según Rui Duro, responsable de Check Point Software en Portugal, “el tiempo necesario para hacer frente a estos ataques es muy variable. Depende mucho del tamaño de la empresa, el ataque, la capacidad de la empresa en cuanto a tecnologías de la información (TI) y qué tan preparada estaba la empresa para reemplazar los sistemas. En una empresa pequeña, a veces toma uno o dos días, si

es una empresa grande, incluso puede demorar varias semanas y, a veces, puede implicar rehacer una infraestructura completa".

El ataque de ransomware ya se ha convertido en una amenaza real y próxima para empresas de todo el mundo, y Portugal no es una excepción. Para la Agencia Europea de Ciberseguridad (ENISA), la pandemia ha traído consigo una "edad de oro" para los ciberdelincuentes.

Según la agencia, entre abril de 2020 y julio de 2021 hubo un aumento del 150% en los ataques registrados.

En Portugal aún no hay datos oficiales del último año, pero en el informe anual de seguridad interna, correspondiente a 2020, ya se identifica al ransomware como "la forma más habitual de sabotaje informático, habiendo mantenido elevados índices de casos y afectando especialmente a instituciones del gobierno y las pequeñas y medianas empresas".

Según este informe, los ciberataques se duplicaron en Portugal desde 2019 (754 incidentes) hasta 2020 (1418 incidentes). En el área de Seguridad de la Información, donde predominan los ataques de ransomware, en 2020 hubo cerca de 10 veces más incidentes que en 2019. Rui Duro, responsable de Check Point Software en Portugal, explica que "del 90 al 95% de los casos no son reportados o conocidos. Las empresas terminan recuperándose a través de copias de seguridad y no reportan ataques".

Según datos de un estudio publicado por la empresa que dirige, que crea soluciones tecnológicas de seguridad para las empresas más grandes del mundo, las organizaciones portuguesas sufren una media de 947 ataques de malware a la semana, una cifra superior a la media mundial de 870 ataques. Alrededor del 90% de los archivos maliciosos llegan por correo electrónico.

Los datos de Check Point Software también muestran que, en diciembre de 2021, los ataques de ransomware alcanzaron a más del 2,5 % de las empresas portuguesas.

RECUPERAR

Un ransomware es una forma de malware (combinación de las palabras en inglés "malicious" y "software") diseñado para encriptar servidores y áreas de almacenamiento de computadoras.

Por lo general, los hackers detrás del ataque muestran mensajes que exigen el pago de una suma para descifrar el sistema y devolverlo al propietario. Según el experto en ciberseguridad, los ataques de ransomware son cada vez más sofisticados, y cada vez se ven más piratas intentando "duplicar o triplicar la extorsión".

En doble extorsión, "durante el período en que el malware está esperando una copia de seguridad, copian datos significativos de bases de datos, servidores de correo electrónico, servidores financieros, intentan buscar datos confidenciales y exportan grandes cantidades de datos. Y dicen que no vale la pena intentar recuperar el servicio con copias de seguridad, porque tienen los datos secuestrados".

En el caso de la triple extorsión, con los datos sensibles en su poder, los piratas amenazan con atacar a los clientes y proveedores de la empresa si la empresa no paga el rescate.

LECCIONES APRENDIDAS

Para prevenir un ataque es necesario cambiar de mentalidad y asumir que sucederá. Para el experto en ciberseguridad, esto es lo más importante. “Tengo más de 30 años en el mercado trabajando en esta área, comencé cuando los ataques eran una broma, en comparación con lo que son hoy, pero aún hoy veo a los tomadores de decisiones pensando que todavía no es preocupante, no es relevante y que creen que no les va a pasar a ellos. El primer paso es cambiar esa mentalidad. A todos les puede pasar, hace poco le pasó a EDP. Cuando pase, tengo que estar preparado para ello. ".

Tener en cuenta los tres pilares de la ciberseguridad: personas, procesos y tecnología.

a) Personas

“A menudo, incluso las empresas que se toman en serio la ciberseguridad se centran demasiado en la tecnología como forma de protegerse y olvidan que es necesario formar a las personas para que se comporten de forma segura”, dice el experto.

b) Procesos

“Es importante tener un proceso para recuperarse del desastre, manejar y calificar la información, tener un proceso de respaldo efectivo y repositorios de información. Muchas empresas no están preparadas, y las primeras horas son un completo caos, porque no estaban alerta para preparar el proceso para recuperarse", revela.

c) Tecnología

Es importante tener un proceso para recuperarse del desastre, manejar y calificar la información, tener un proceso de respaldo efectivo, tener repositorios de información. Muchas empresas no están preparadas, y las primeras horas son un completo caos, porque no estaban cuidado de preparar el proceso para recuperarse", revela.

c) Tecnología

"Usar tecnología adecuada a la realidad que tenemos hoy. Muchas empresas compran tecnología y es lo que yo llamo comprar una "falsa sensación de seguridad": compran tecnología, pero ya no es adecuada para la realidad que tenemos hoy. El firewall tradicional, en lugar de comprar un endpoint avanzado que evite el cifrado de los sistemas, se utiliza un endpoint simple, que detecta algún malware, pero no evita estos cifrados".

El especialista recuerda que, en estos casos, “el pánico no ayuda en nada”. En estas situaciones, es necesario informar a las autoridades y nunca pagar el rescate, ya que es lo mismo que perpetuar el crimen, diciéndoles a los ciberdelincuentes que vale la pena. Uno de los procesos que las empresas deben tener con anticipación, para el especialista, es cómo recuperarse de un ataque de este tipo, para que haya esa calma y que todos sepan cuál es su papel en ese proceso.

CASO DE ESTUDIO 16: MALWARE/ KEYLOGGER

LA ORGANIZACIÓN OBJETIVO

Una pequeña empresa manufacturera familiar hizo un uso extensivo de la banca en línea. El empleado de contabilidad inició sesión en el sistema bancario en línea con una empresa y una identificación y contraseña específicas del usuario. Se tuvieron que responder dos preguntas de seguridad para transacciones superiores a 1.000 €.

Se notificó al propietario que una fuente desconocida inició una transferencia de pago de 5.000 €. Se pusieron en contacto con el banco e identificaron que en tan solo una semana los ciberdelincuentes habían realizado diez transferencias desde las cuentas bancarias de la empresa, por un total de 10.000€. ¿Cómo? Uno de sus empleados había abierto un correo electrónico de lo que pensaba que era un proveedor de materiales, pero en cambio era un correo electrónico malicioso mezclado con malware de una cuenta de impostor.

Los atacantes pudieron instalar un malware en los ordenadores de la empresa, utilizando un registrador de teclas para capturar las credenciales bancarias. Un keylogger es un software que monitorea silenciosamente las pulsaciones de teclas del ordenador y envía la información a un ciberdelincuente. Luego pueden acceder a la banca y otros servicios financieros en línea, utilizando números de cuenta y contraseñas válidos.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

La información de este ciberataque se recopiló a través de dos entrevistas, una con el propietario de la empresa y otra con un técnico de la empresa de soporte de TI. Ambos estaban dispuestos a describir y dar detalles del incidente, pero pidieron mantener en el anonimato a ambas empresas porque la información era demasiado sensible para ellos.

Un keylogger es un software que monitoriza silenciosamente las pulsaciones del ordenador y envía la información a un ciberdelincuente.

PREVENIR

En la empresa analizada, los procedimientos y mecanismos de ciberseguridad fueron identificados como no satisfactorios. Aunque los ordenadores de la empresa tenían software antivirus, ninguno estaba actualizado. Además, no se habían llevado a cabo campañas de concientización y algunos empleados parecían tener una comprensión limitada de los riesgos cibernéticos.

IDENTIFICAR

En base a la información proporcionada, se recopilaron los siguientes detalles sobre la incidencia:

- ☑ Se recibió un correo electrónico de phishing diseñado con ingeniería social, con un archivo comprimido adjunto como verificación de un pedido del proveedor.
- ☑ Al abrir el archivo, el malware se instaló en el ordenador.
- ☑ Se instaló un software de registro de teclas que monitorea silenciosamente las pulsaciones de teclas del ordenador y envía la información a un ciberdelincuente.
- ☑ Luego, el ciberdelincuente utiliza las credenciales capturadas para acceder a la cuenta bancaria y realiza la transferencia utilizando números de cuenta y contraseñas válidos.
- ☑ El incidente se identificó solo cuando el ciberdelincuente intenta realizar una transferencia superior a 1000 €.

RESPONDER

Al no contar con un plan de ciberseguridad, la respuesta de la empresa al ataque se retrasó.

QUIÉN: El atacante no pudo ser identificado con precisión. Solo se conocía una dirección de correo electrónico y el posible origen.
A QUIÉN: objetivo no específico.
POR QUÉ: Recopilación de datos confidenciales y uso de estos para robar dinero.
QUÉ: Credenciales de la cuenta bancaria de la empresa.
CÓMO: Keylogger, monitorea silenciosamente las pulsaciones de teclas del ordenador.

ESTRATEGIA: La amenaza comenzó en un ordenador sin antivirus. Un proceso de limpieza fue realizado por un experto en TIC de una empresa. La cuenta bancaria se cerró y las credenciales cambiaron. La empresa de TIC los ayudó a completar una revisión completa de ciberseguridad de sus sistemas e identificar cuál fue el origen del incidente. También se recomiendan actualizaciones del software de seguridad.

RECUPERAR

IMPACTO: La empresa cerró su cuenta bancaria y emprendió acciones legales para recuperar sus pérdidas. La empresa recuperó una pequeña parte de las pérdidas. No se recuperó dinero por tiempo y honorarios legales.

RECUPERACIÓN: La estrategia de recuperación se centró en cerrar la cuenta bancaria para evitar más pérdidas. Otras acciones fueron, limpiar el ordenador y el buzón electrónico comprometido. Revisar todos los ordenadores de la compañía para detectar cualquier otro ataque.

ESTRATEGIA: La empresa debe implementar diversas acciones para prevenir este tipo de incidentes. Su estrategia debe concentrarse en las siguientes acciones/pasos:

- ☑ Implementar políticas de seguridad como la política de cambio de contraseña y la política de administración de usuarios de cuentas.
- ☑ Instale y mantenga un software antivirus/antimalware actualizado.
- ☑ Realizar programas de formación para asegurar la concienciación de los empleados.
- ☑ Restringir el contenido basado en la web.
- ☑ Realizar comprobaciones y auditorías periódicas.
- ☑ Ejecutar prevención e implantación de un sistema de gestión de riesgos.

LECCIONES APRENDIDAS

- ☑ Notificaciones: configurar alertas de transacciones en todas las tarjetas de crédito, débito y cuentas bancarias.
- ☑ Control de acceso. Restringir el acceso a cuentas confidenciales solo a aquellos empleados que necesitan acceso; cambiar las contraseñas a menudo.
- ☑ La empresa debe evaluar su riesgo y las opciones de seguro de responsabilidad cibernética.
- ☑ Elegir bancos que ofrezcan varias capas de autenticación para acceder a cuentas y transacciones.

☑ Crear, mantener y practicar un plan de respuesta a incidentes cibernéticos que se pueda implementar rápidamente.

☑ Los ciberdelincuentes entregan e instalan software malicioso por correo electrónico. Formación a los empleados en la seguridad del correo electrónico.

CASO DE ESTUDIO 17: UN ORDENADOR ROBADO PROVOCA UNA GRAVE VIOLACIÓN DE DATOS

ORGANIZACIÓN OBJETIVO

Una empresa de consultoría de 10 personas envió un pequeño equipo a Hungría para completar un proyecto de un cliente. Durante su estadía, el consultor senior dejó su ordenador portátil de trabajo, que tenía acceso a información confidencial de los clientes y datos bancarios de la empresa, en un automóvil cerrado mientras realizaba un trabajo. Asaltaron el auto y robaron el ordenador portátil. Desafortunadamente, los datos en el ordenador no estaban encriptados porque el empleado no aplicó la política de la compañía para encriptar todos los datos confidenciales en su ordenador. La empresa ahora temía un ciberataque a sus sistemas, cuentas bancarias y fuga de datos de clientes.

Tipo de ataque: Robo físico de un pc no encriptado. El cifrado es el proceso de codificar texto legible para que solo pueda leerlo la persona que tiene la clave de descifrado. Crea una capa adicional de seguridad para la información confidencial.

¿CÓMO SE ADQUIRIÓ LA INFORMACIÓN?

La información necesaria para describir el incidente se recopiló a través de una entrevista con el consultor senior de la empresa y el técnico de TI de la empresa TIC que da soporte a la consultora. La interacción se realizó con la condición de mantener la información sensible en el anonimato. Incluso si el entrevistado estaba dispuesto a describir el incidente, no se pudo obtener cierta información de cifrado y esta es la razón por la que se solicitó a la empresa de apoyo de TIC que aclarara el caso.

PREVENIR

Aunque el incidente no es un incidente de ciberataque claro, es un incidente grave y muy común que provoca una serie de ciberataques significativos.

En el caso de la empresa analizada, desde la perspectiva de la ciberseguridad, operaban políticas y mecanismos específicos, pero estos no fueron implementados por algunos empleados debido a su baja experiencia en el campo de la información y los riesgos de la ciberseguridad.

IDENTIFICAR

El empleado denunció inmediatamente el robo a la policía y su empresa. El banco también fue informado para monitorear las transacciones de la cuenta. La empresa informó a la empresa de

soporte de TIC para desactivar el acceso remoto del ordenador portátil y comenzó a monitorear la actividad. El ordenador portátil estaba equipado con herramientas de seguridad y protección con contraseña. Los datos almacenados en el disco duro no estaban encriptados; esto incluía datos confidenciales de los clientes y datos bancarios de la empresa.

Para una identificación basada en el comportamiento de este ataque, se pueden utilizar las siguientes técnicas de MITRE ATT&CK:

- ☑ T1027 – Archivos o información oculta
- ☑ T1036 – Masquerading
- ☑ T1586.002 - Cuentas de compromiso: Cuentas de correo electrónico

RESPONDER

Respuesta: La empresa debe cumplir con las leyes estatales en lo que respecta a una violación de datos. Las leyes estatales y las regulaciones de la UE sobre RGPD son muy estrictas con multas de alto costo.

- ☑ **QUIÉN:** El atacante no pudo ser identificado. Solo se conocía el lugar del incidente.
- ☑ **A QUIÉN:** objetivo no específico
- ☑ **POR QUÉ:** Recopilación de datos confidenciales y obtención de dinero con la venta del equipo robado
- ☑ **QUÉ:** Datos sensibles de los clientes y datos bancarios de la empresa
- ☑ **CÓMO:** pérdida de equipos, fuga de datos confidenciales y ataque a cuentas bancarias
- ☑ **ESTRATEGIA:** La amenaza comenzó en un ordenador sin antivirus y se ha extendido lateralmente. Se realizó un proceso de limpieza por parte de una empresa especializada.

RECUPERAR

IMPACTO: La consultora gastó más de 20.000€ en implementación, seguimiento y mejoras operativas. Una violación de datos tiene un impacto negativo en una marca y se debe reconstruir la confianza.

Las principales consecuencias del ataque fueron las siguientes:

- ☑ Pérdida de datos
- ☑ Pérdida de PC
- ☑ Sistema comprometido
- ☑ Costos financieros

RECUPERAR: La estrategia de recuperación estuvo enfocada en minimizar la reputación de marca y monitorear y controlar los sistemas internos y cuentas bancarias de la empresa. De manera

preventiva, todas las credenciales de las cuentas bancarias cambiaron y los privilegios de los sistemas de los empleados fueron suspendidos y cambiados.

ESTRATEGIA: La empresa debe implementar diversas acciones para prevenir este tipo de incidentes. Su estrategia debe concentrarse en

- ☑ Realizar programas de formación para asegurar la concienciación de los empleados.
- ☑ Realizar comprobaciones y auditorías periódicas.
- ☑ Ejecutar prevención e implantación de un sistema de gestión de riesgos.

LECCIONES APRENDIDAS

- ☑ Las empresas deben establecer y formar a los empleados en el manejo seguro de los dispositivos emitidos por el trabajo.
- ☑ Los dispositivos deben almacenarse de manera segura cuando no estén en presencia del empleado.
- ☑ Las empresas deben tomar medidas para cifrar los datos dondequiera que se almacenen o transmitan.
- ☑ Los empleados deben tener una comprensión clara de la importancia del cifrado y cómo usarlo.
- ☑ Las empresas deben comprender y conocer sus responsabilidades en virtud de las leyes de notificación de violación de datos del país en el que operan.
- ☑ Una revisión periódica de las prácticas de seguridad de la empresa es imprescindible en las organizaciones modernas para prevenir incidentes, descubrir vulnerabilidades y reducir el impacto de los incidentes.

"Hubo un aumento del 57% en las variantes de la botnet Mirai identificadas en 2019. Las variantes de Mirai se utilizan normalmente para ataques de fuerza bruta en dispositivos IoT. Estos ataques aumentaron un 51%, mientras que los exploits web aumentaron un 87% en 2019." (MCCART, 2022).

CASO DE ESTUDIO 18: EL ATAQUE DDOS DETIENE SERVICIOS IMPORTANTES

ORGANIZACIÓN OBJETIVO

La organización objetivo era una empresa proveedora de alojamiento. Los atacantes lanzaron un ataque masivo de denegación de servicio distribuido contra un sitio web específico a mediados de diciembre de 2021, superando un ancho de banda de 1,5 gigabits por segundo y casi 100 millones de paquetes por segundo, el mayor ataque al que se enfrenta una empresa de hosting.

La empresa cree que el atacante se centró en los sitios web con juegos de casino en línea y que el proveedor de alojamiento no era el objetivo real. El ataque DDOS provoca la terminación de la disponibilidad de los servicios del cliente por más de 12 horas.

Un ataque de denegación de servicio distribuido (DDoS) es un intento malicioso de interrumpir el tráfico normal de un servidor, servicio o red objetivo al sobrecargar el objetivo o la infraestructura circundante con una avalancha de tráfico de internet. Los ataques DDoS logran su efectividad al utilizar múltiples sistemas informáticos comprometidos como fuentes de tráfico de ataque. Las máquinas explotadas pueden incluir ordenadores y otros recursos en red, como dispositivos IoT.

¿CÓMO SE HA OBTENIDO LA INFORMACIÓN?

La información necesaria para describir este ciberataque se recopiló a través de dos entrevistas (reuniones presenciales), una con el director general de la empresa y otra con un ingeniero informático de la empresa. Ambos estaban dispuestos a describir y dar detalles del incidente, pero pidieron mantener en el anonimato a ambas empresas y sus nombres porque la información era demasiado sensible para ellos.

PREVENIR

Aunque el proveedor de alojamiento cuenta con varios procedimientos y mecanismos de ciberseguridad, parece que los atacantes encontraron un punto vulnerable para explorar.

El técnico de la empresa notó que el sitio web se volvió lento repentinamente, pero suponen que se trata de un aumento legítimo en el tráfico debido a la temporada navideña. El ataque se identificó justo después de que el sitio web dejó de estar disponible y el cliente se quejó.

IDENTIFICAR

Los atacantes usaron tráfico de fuentes en todo el mundo. Parece que el ataque de denegación de servicio fue creado por un botnet Mirai. Y debido a que la red de bots Mirai tiene la capacidad de enviar alrededor de 600 megabits por segundo, usaron un ataque de segundo nivel con una red de bots Mirai diferente.

Mirai es un malware que infecta dispositivos inteligentes que se ejecutan en procesadores ARC, convirtiéndolos en una red de bots o "zombies" controlados de forma remota. Esta red de bots, llamada botnet, se usa a menudo para lanzar ataques DDoS.

El proveedor de alojamiento utilizó herramientas de análisis de tráfico para identificar el ataque. La característica básica del ataque es el alto volumen proveniente de la misma serie de direcciones IPs. Los ingenieros lograron aislar esas IPs y el sitio web volvió.
Después de eso, intentaron identificar por qué la herramienta de análisis de tráfico no detectó el ataque desde las primeras etapas.

De acuerdo con el marco MITRE ATT&CK, esta incidencia se puede describir de la siguiente manera:

- ☑ T1499 - Denegación de servicio de punto final
- ☑ T1498 - Denegación de servicio de red

RESPONDER

- ☑ **QUIÉN:** El atacante no pudo ser identificado. El ataque vino de todas partes del mundo.
- ☑ **A QUIÉN:** El objetivo era un sitio web específico que albergaba juegos de casino en línea.
- ☑ **POR QUÉ:** Para interrumpir su funcionamiento.
- ☑ **QUÉ:** Página web de la compañía.
- ☑ **CÓMO:** Ataque DDOS utilizando botnets Mirai.
- ☑ **ESTRATEGIA:** El ataque comenzó en un servidor de un proveedor de alojamiento para interrumpir el funcionamiento de un sitio web específico. La herramienta de análisis de tráfico no alertó sobre la posibilidad de un ciberataque. La empresa aumentó la sensibilidad de las alarmas en la herramienta de análisis de tráfico para evitar incidentes similares en el futuro.

RECUPERAR

IMPACTO: El proveedor de alojamiento tuvo algunos costes adicionales significativos para cubrir el ataque y también sufrió un grave daño a la reputación. Tuvieron el coste de mano de obra adicional para recuperar el sitio web y las penalizaciones en el acuerdo de SLA con el cliente. El coste total se estimó en unos 40.000 €.

RECUPERAR: La estrategia de recuperación se centró en aislar las IPs atacantes para detener el ataque y recuperar el funcionamiento del sitio web. Otras acciones fueron aumentar la sensibilidad de las alarmas de la herramienta de análisis de tráfico. Verificar todos los servidores y servicios de alojamiento en busca de otros ataques o actividades sospechosas.

ESTRATEGIA: La empresa debe implementar diversas acciones para prevenir este tipo de incidentes. Su estrategia debe concentrarse en

- ☑ Aumentar la sensibilidad de la herramienta de análisis de tráfico
- ☑ Instalar una segunda herramienta para mayor seguridad
- ☑ Realizar programas de formación para asegurar la concienciación de los empleados
- ☑ Restringir algunos rangos de IP
- ☑ Realizar comprobaciones y auditorías periódicas
- ☑ Ejecucar prevención e implantación de un sistema de gestión de riesgos
- ☑ Certificar su infraestructura y servicios en ISO27001 e ISO22301.

LECCIONES APRENDIDAS

- ☑ La disrupción viene en muchas formas. Las interrupciones o los retrasos pueden presentarse de muchas formas, especialmente para los proveedores de alojamiento. Cuando se identifica un ataque, los equipos de respuesta apropiados deben dedicar recursos para enfrentarlo.
- ☑ Muchos ciberataques se pueden prevenir fácilmente. Los ciberataques sofisticados pueden causar mucho daño, pero muchos de ellos se pueden prevenir fácilmente con la seguridad adecuada. Es importante construir un sistema de administración de seguridad sólido y proactivo para detener los ataques. Tal sistema de gestión requiere mantenimiento continuo, monitoreo todos los sistemas y dispositivos en la red, incluida la actualización de la tecnología y la aplicación de parches de seguridad para vulnerabilidades conocidas.

- ☑ Los ataques DDoS deben tomarse en serio. Los ataques DoS y DDoS de hoy en día son diferentes.
- ☑ Sin límite de tiempo. Los ataques a la capa de red pueden durar más de 48 horas, mientras que los ataques a la capa de aplicación pueden prolongarse durante días. Infiltración de sistemas y redes para espiar—semanas y meses.
- ☑ La ciberseguridad debe ser una prioridad. La ciberseguridad debe ser una de las más altas prioridades para todas las entidades que operan en el panorama actual. Estos ataques se han vuelto sofisticados, dirigidos, capaces y no regulados. Todas las amenazas deben tomarse en serio, incluidos los ataques DDoS, que son cada vez más comunes.

ENCRYPT 4.0

Cofinanciado por el
programa Erasmus+
de la Unión Europea

CONCLUSION

En base al presente documento sobre ciberataques del Proyecto ENCRYPT 4.0, se podrían extraer las siguientes conclusiones:

- ☑ Con el desarrollo de las TIC y en el contexto de la Industria 4.0, la ciberseguridad tiene una importancia creciente y **las empresas que carecen de una ciberdefensa adecuada están poniendo en grave riesgo sus operaciones.**
- ☑ **Los empleados desempeñan un papel clave en la ciberdefensa,** por lo tanto, los empleados tanto de las pymes como de las grandes empresas deben recibir al menos una formación básica sobre cómo proteger los datos de la empresa y trabajar con información confidencial, ya que la mayoría de los ciberataques ocurren debido a la falta de conocimiento sobre estos aspectos, especialmente en el contexto del trabajo a distancia durante la pandemia de COVID-19.
- ☑ **Las pymes, sin tener en cuenta el sector en el que operan, se están convirtiendo en los principales objetivos de los piratas informáticos y los ciberdelincuentes organizados,** pero al mismo tiempo solo un 1/3 de las pymes tienen un plan para contener un posible ciberataque, por lo que las pymes deben prever la ciberseguridad como máxima prioridad para asegurar su competitividad a largo plazo.

BIBLIOGRAFÍA

1. Acronis, 2020. The NHS cyber-attack. [Online] Acronis. Available at:https://www.acronis.com/en-us/blog/posts/nhs-cyber-attack/

2. Barber, B., 2016. William Hill apologise after website attack. [Online] Racing Post. Available at: https://www.racingpost.com/news/william-hill-apologise-after-website-attack/266196 (Case study 6)

3. Blue goose, n.d. Information Security at William Hill. [Online] blue goose. Available at: https://bluegooseis.co.uk/work/william-hill (Case study 6)

4. Braue, D., 2022. Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. [Online] 2022 Cybersecurity Ventures. Available at: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

5. Cook, S., 2022. 20+ DDoS attack statistics and facts for 2018-2022. [Online]. Comparitech. Available at:https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

6. Craver, R., 2015. Hanesbrands database hacked 900K phone, online customers affected. [e-journal] *Winston-Salem Journal.* Available at:

https://journalnow.com/business/hanesbrands-database-hacked/article_543b338e-3664-11e5-b77e-c77df1e08b5c.html (Case study 4)

7. Cyber Startup Observatory. Available at: https://cyberstartupobservatory.com/ (Case study 4)

8. CyberNews, 2021. Thousands of Humana customers have their medical data leaked online by threat actors. [Online] 2022 Cybernews. Available at: https://cybernews.com/news/humana-insurance-customers-medical-data-leaked/ (Case study 5)

9. CyberTalks, 2022. Top 15 phishing attack statistics (and they might scare you) [Online]. CyberTalks. Available at: https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

10. Cyware , 2018. Humana websites hit by sophisticated spoofing attack from 'foreign countries'. [Online] Cyware. Available at: https://cyware.com/news/humana-websites-hit-by-sophisticated-spoofing-attack-from-foreign-countries-5ac77624 (Case study 5)

11. Dissent, 2018. Humana notifies members after credential stuffing attack on Humana.com and Go365.com. [online] 2009 – 2022, DataBreaches.net and DataBreaches LLC. Available at: https://www.databreaches.net/humana-notifies-members-after-credential-stuffing-attack-on-humana-com-and-go365-com/ (Case study 5)

12. EUROPOL, n.d. World's most dangerous malware EMOTET disrupted through global action. [Online] EUROPOL 2022. Available at: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

13. Kolbasuk McGee, M., 2018. Humana Notifying Victims of 'Identity Spoofing' Attack. [online] *Data Breach Today*. Available at: https://www.databreachtoday.asia/humana-notifying-victims-identity-spoofing-attack-a-11153 (Case study 5)

14. McCart, C., 2022. 15+ Shocking botnet statistics. [Online] Comparitech. Available at:https://www.comparitech.com/blog/information-security/botnet-statistics/

15. Mimecast, 2022. Confronting the NEW WAVE OF CYBER ATTACKS: The State of Email security Report 2022. Mimecast. Available at: https://www.mimecast.com/globalassets/documents/ebook/state-of-email-security-2022.pdf

16. Moore, J., 2022. Top 10 List of Cybersecurity Facts for 2022. [Online] Elevity. Available at: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

17. Morran, Ch., 2015. Hanes Website Is The Latest, Oddest Victim Of Data Breach. Consumerist. Available at: https://consumerist.com/2015/07/30/hanes-website-is-the-latest-oddest-victim-of-data-breach/ (Case study 4)

18. StackHawk, 2022. What is Command Injection? [Online]. StackHawk, Available at: https://www.stackhawk.com/blog/what-is-command-injection/

19. The Cyber Wire, n.d. Definition of Spoofing. [Online]. The Cyber Wire. Available at: https://thecyberwire.com/glossary/spoofing

20. VentureBeat, 2022. Report: Average time to detect and contain a breach is 287 days. [Online] VentureBeat. Available at: https://venturebeat.com/2022/05/25/report-average-time-to-detect-and-contain-a-breach-is-287-days/

21. Verizon, 2021. DBIR: 2021 Data Breach Investigation Report. Verizon, 2021. Available at: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf

22. Wallarm, 2021. The Biggest Hacker Attacks on Gambling. 10. [Online] Wallarm. Available at: https://lab.wallarm.com/the-biggest-hacker-attacks-on-gambling/ (Case study 6)

ENCRYPT 4.0

Cofinanciado por el programa Erasmus+ de la Unión Europea

SOCIOS DEL PROYECTO

ENCRYPT 4.0

Joint Cyber Workforce Development Initiative to Enable The European Industry to Overcome the Shortage of Cybersecurity Professionals

El Proyecto ENCRYPT4.0 (2020-1-RO01-KA202-079983) tiene como objetivo permitir que la gerencia de las pymes industriales adopte un enfoque proactivo hacia la ciberseguridad apoyándolas en el proceso de análisis, identificación y abordaje de los riesgos y amenazas cibernéticos aplicables a su organización. Fomentando el aprendizaje interactivo basado en proyectos con respecto al impulso de las habilidades y competencias en ciberseguridad de los empleados de las pymes y/o los profesionales de la ciberseguridad.

"George Emil Palade" University of Medicine, Pharmacy, Sciences and Technology of Târgu Mureș

- Rumanía

Coordinador del proyecto

European Center for Quality Ltd., Consulting company

- Bulgaria

Instituto de Soldadura e Qualidade, Technological institution

- Portugal

Avantalia Soluciones S.L

- España

FH Joanneum, University of Applied Sciencies

- Austria

PCX Management, Computers & Information Systems Ltd.

- Chipre