INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 4

19 DE OCTUBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado.

Ejercicio: Hemos visto en la teoría una taxonomía estándar de incidentes de ciberseguridad. Empleamos dicha taxonomía para poder comunicarnos de una forma sencilla con los distintos CSIRT o CERT en caso de un incidente. En este ejercicio el objetivo es buscar noticias que nos sirvan de ejemplo para ilustrar los distintos tipos de incidentes descritos en la taxonomía.

Contenido abusivo

1) SPAM:

Detectan una campaña de 'spam' malicioso dirigido a usuarios de la Caixa.

La compañía desarrolladora de 'software' de seguridad Avast ha detectado una nueva campaña de 'spam' malicioso por correo electrónico que afecta a los clientes de la Caixa en España.

2) Delito de odio:

Condenan a prisión a siete personas por incitar a la violencia contra menores migrantes en Melilla a través de Facebook.

La Audiencia Provincial de Málaga considera un delito de odio los mensajes lanzados en 2017 en un grupo con 14.000 seguidores en los que se hacían llamamientos a agredir a los niños que vivían en las calles de la ciudad.

3) Pornografía infantil, contenido sexual o violento inadecuado:

Detenida una pareja por usar a su bebé para hacer pornografía infantil.

La Policía Nacional ha arrestado en Madrid a los padres de una niña de pocos meses, ya que el progenitor agredía sexualmente a la bebé, mientras que la madre intercambiaba archivos de pornografía infantil.

Contenido dañino

1) Sistema infectado: sistema infectado con malware

WannaCry", que tuvo lugar en mayo de 2017. WannaCry fue un ransomware que se propagó a nivel mundial, afectando a sistemas de computadoras en más de 150 países.

Este malware explotó una vulnerabilidad en el sistema operativo Windows que había sido parcheada previamente por Microsoft, pero muchas organizaciones no habían aplicado la actualización en sus sistemas. Como resultado, WannaCry se extendió rápidamente y cifró los archivos en las computadoras de las víctimas

2) Servidor C&C (Mando y Control)

El caso del botnet "Conficker", que comenzó a propagarse en 2008. Conficker fue un gusano informático que infectó una gran cantidad de computadoras en todo el mundo.

Este malware se comunicaba con servidores de comando y control para recibir instrucciones y actualizaciones de su infraestructura. Los servidores C&C utilizados por Conficker permitían a los atacantes controlar y coordinar las acciones de las computadoras infectadas. Conficker fue particularmente resistente y difícil de desactivar debido a su capacidad para cambiar dinámicamente los dominios de sus servidores C&C, lo que dificultaba su bloqueo.

3) Distribución de malware

El gusano ILOVEYOU se distribuyó principalmente a través del correo electrónico y tenía un asunto atractivo, como "ILOVEYOU" o "Love Letter for You". El correo electrónico contenía un archivo adjunto llamado "LOVE-LETTER-FOR-YOU.TXT.vbs", que en realidad era un archivo de script Visual Basic que ejecutaba el malware cuando se abría.

Una vez que se abría el archivo adjunto, el gusano ILOVEYOU se propagaba a través de la libreta de direcciones del usuario y se enviaba a todos los contactos de correo electrónico.

4) Configuración de malware:

El caso de "Stuxnet", que se descubrió en 2010. Stuxnet es un gusano informático altamente sofisticado que se diseñó específicamente para atacar sistemas de control industrial, como los utilizados en instalaciones nucleares. Lo que hace que Stuxnet sea interesante desde el punto de vista de la configuración de malware es que incluía una serie de características técnicas avanzadas.

5) Malware dominio DGA:

El malware de robo de datos QSnatch infectó más de 62.000 dispositivos NAS QNAP.

Hasta mediados del pasado mes de junio, el malware QSnatch (alias «Derek») había infectado 62.000 dispositivos en todo el mundo, incluyendo 3.900 en el Reino Unido y 7.600 en los EE.UU., según la alerta del Centro Nacional de Ciberseguridad (NCSC) de GCHQ y la Agencia de Ciberseguridad e Infraestructura (CISA) del Departamento de Seguridad Nacional.

Obtención de información

1) Escaneo de redes (scanning):

Pillan a eBay escaneando la conexión de los ordenadores que visitan sus páginas.

Investigadores han descubierto que las páginas web de eBay realizan escáneres de puertos en los ordenadores de los usuarios que las visitan, incluso sin cuenta.

2) Análisis de paquetes (sniffing):

En 2007, se descubrió un ataque de sniffing en la red inalámbrica de TJX Companies, una cadena minorista que incluye tiendas como TJ Maxx y Marshalls. Los atacantes lograron acceder a la red inalámbrica de la empresa y llevar a cabo un ataque de análisis de paquetes para interceptar transacciones de tarjetas de crédito y obtener información confidencial de los clientes.

Este ataque de análisis de paquetes en la red inalámbrica resultó en uno de los mayores casos de robo de datos de tarjetas de crédito en la historia.

3) Ingeniería social

Uber cae ante ataques de la ingeniería social.

Uber afirmó que el ataque comenzó cuando las credenciales de un contratista de la red interna de Uber fueron compradas por Lapsus$ a un IAB. Los atacantes procedieron entonces a intentar utilizar las credenciales repetidamente, activando múltiples notificaciones push multifactor de Duo Security en el teléfono del contratista hasta que éste finalmente sucumbió al diluvio y aceptó una de ellas, otorgando a los intrusos un punto de acceso.

Intento de intrusos

1) Explotación de vulnerabilidades conocidas:

Blaster se aprovechó de una vulnerabilidad en el sistema operativo Windows conocida como "RPC DCOM" (Remote Procedure Call Distributed Component Object Model), que había sido parcheada por Microsoft antes del lanzamiento del gusano.

Este gusano se propagó rápidamente a través de Internet y afectó a un gran número de sistemas, causando estragos en redes empresariales y domésticas.

2) Intento de acceso con vulneración de credenciales:

Heartland Payment Systems es una empresa de procesamiento de pagos que sufrió un importante ataque de ciberseguridad que involucró la violación de credenciales.

En este incidente, los atacantes lograron infiltrarse en la red de Heartland Payment Systems y acceder a los sistemas que procesaban transacciones de tarjetas de crédito. Utilizaron técnicas de escaneo y explotación para ganar acceso no autorizado a la red de la empresa.

Una vez dentro, los atacantes instalaron malware en los sistemas de procesamiento de pagos que les permitió interceptar información de tarjetas de crédito durante las transacciones. Esta información robada se utilizó para llevar a cabo fraudes con tarjetas de crédito.

3) Ataque desconocido:

El ataque a la infraestructura de Internet de Estonia en 2007. Este ataque se centró en una serie de sitios web gubernamentales y empresas estonias y causó interrupciones significativas en los servicios en línea del país. Lo que hizo que este ataque fuera interesante es que, en ese momento, no se entendía completamente su origen y naturaleza.

Intrusión

1) Compromiso de cuenta con privilegios:

El caso de "Target" en 2013. Target Corporation, una cadena de tiendas minoristas en los Estados Unidos, fue víctima de un ataque cibernético en el que se comprometieron las cuentas de acceso con privilegios.

En este caso, los atacantes obtuvieron acceso a las credenciales de una empresa proveedora de servicios de calefacción, ventilación y aire acondicionado (HVAC) que tenía conexiones con la red de Target. Los atacantes aprovecharon estas credenciales para acceder a la red de Target y, una vez dentro, se movieron lateralmente para acceder a sistemas más sensibles.

Una vez en la red de Target, los atacantes pudieron instalar malware en los sistemas de punto de venta de la tienda, lo que les permitió robar información de tarjetas de crédito de millones de clientes que realizaron compras en las tiendas de Target durante la temporada de compras navideñas.

2) Compromiso de cuenta sin privilegios:

El caso de "Sony Pictures" en 2014. En este incidente, los atacantes comprometieron cuentas de empleados de Sony Pictures sin necesidad de privilegios adicionales.

Los atacantes utilizaron técnicas de ingeniería social y phishing para obtener acceso a las credenciales de inicio de sesión de empleados, incluyendo nombres de usuario y contraseñas. Una vez dentro de la red de Sony Pictures, los atacantes tuvieron acceso a sistemas y bases de datos críticos.

3) Compromiso de aplicaciones:

La Generalitat sufre un fallo de seguridad online: 5.000 usuarios expuestos.

Todo por un fallo de seguridad informática en forma de vulnerabilidad. Una vulnerabilidad que ha dejado expuestos hasta 5.000 correos electrónicos y contraseñas de usuarios que se habían dado de alta en aplicaciones del Govern.

4) Robo:

Un grupo de piratas informáticos logró explotar una vulnerabilidad en una aplicación web de Equifax para acceder a los sistemas de la empresa. Esta vulnerabilidad ya tenía un parche disponible, pero no se había aplicado a tiempo en los sistemas de Equifax.

El ataque resultó en el robo de información personal sensible de aproximadamente 143 millones de personas en los Estados Unidos, incluyendo nombres, números de Seguro Social, fechas de nacimiento, direcciones y números de tarjetas de crédito.

Disponibilidad

1) DoS:

Arbor Networks, que se especializa en la mitigación de ataques DDoS, fue víctima de uno de estos ataques.

En ese momento, los ataques DDoS eran menos conocidos y entendidos, y este incidente ayudó a arrojar luz sobre la gravedad de los mismos. El ataque consistió en inundar el sitio web

de Arbor Networks con una gran cantidad de tráfico malicioso, lo que resultó en la caída del sitio y la interrupción de sus servicios.

2) DDoS:

Estonia experimentó una serie de ataques DDoS a gran escala contra sitios web gubernamentales, redes de medios y empresas, lo que resultó en interrupciones significativas en los servicios en línea del país. Los ataques fueron una respuesta a una disputa política con Rusia y se cree que algunos actores respaldados por Rusia estuvieron involucrados.

El ataque DDoS no solo afectó a sitios gubernamentales, sino que también impactó en empresas privadas, bancos y medios de comunicación. Los atacantes utilizaron botnets (redes de dispositivos comprometidos) para inundar los servidores con tráfico malicioso, lo que provocó la caída de varios sitios web.

3) Sabotaje:

Imputan a un hombre por sabotaje informático a una empresa de Cantabria, que estuvo dos días sin conexión.

La Guardia Civil ha imputado a un hombre como presunto autor de un delito de sabotaje informático contra una empresa de Cantabria, la cual, a consecuencia del ataque, permaneció durante dos días sin tener conexión tanto interna como a internet. El perjuicio económico casado por el ataque se cuantificó en 3.000 euros.

4) Interrupciones:

El incendio del principal data center de OVH pone de relieve la importancia de tener un plan de recuperación ante desastre.

El proveedor cloud europeo OVH está teniendo que hacer frente a un incendio en su centro de datos de Estrasburgo, lo que está afectando a todas las empresas que tenían allí alojadas algunos de sus servicios, como páginas web.

Compromiso de la información

1) Acceso no autorizado a información:

WikiLeaks, un sitio web conocido por publicar documentos confidenciales y clasificados, obtuvo acceso a miles de cables diplomáticos del Departamento de Estado de los Estados Unidos. La filtración fue realizada por Chelsea Manning, quien era analista de inteligencia en el ejército de EE. UU. y había descargado los documentos clasificados.

El acceso no autorizado a esta información confidencial se realizó a través de la interceptación de tráfico y la filtración de documentos físicos. Manning utilizó un dispositivo USB para descargar los cables diplomáticos y luego los entregó a WikiLeaks. La filtración reveló comunicaciones diplomáticas delicadas y secretas entre Estados Unidos y sus embajadas en todo el mundo, lo que generó controversia y preocupación a nivel internacional.

2) Modificación no autorizada de información:

WannaCry es un ejemplo de ransomware, que es un tipo de malware que cifra los datos en el sistema de la víctima y exige un rescate para descifrarlos. El ataque se realizó empleando credenciales sustraídas o a través de vulnerabilidades en sistemas Windows no parcheados.

Una vez que el malware infectaba un sistema, cifraba los datos y mostraba un mensaje de rescate en el que se exigía un pago en Bitcoin a cambio de la clave de descifrado.

3) Pérdida de datos:

el buscador de Internet Cuil anunció su lanzamiento. Cuil, considerado en ese momento como un competidor potencial de Google, sufrió una pérdida significativa de datos en sus primeros días de funcionamiento.

La compañía promocionó su capacidad para indexar una gran cantidad de páginas web, pero poco después de su lanzamiento, experimentó un fallo importante en uno de sus discos duros. Como resultado de este fallo, gran parte de los datos de indexación se perdió, y la calidad de los resultados de búsqueda de Cuil se vio afectada negativamente. Esto llevó a una recepción negativa por parte de los usuarios y expertos en tecnología.

Fraude

1) Uso no autorizado de recursos:

El caso de "Mydoom", que fue un notorio gusano de computadora que se propagó en enero de 2004. Mydoom se difundió principalmente a través del correo electrónico y se convirtió en uno de los gusanos más rápidamente extendidos de la historia de Internet.

Este gusano se propagó mediante mensajes de correo electrónico que incluían archivos adjuntos maliciosos. Cuando los destinatarios abrían estos archivos adjuntos, sus computadoras quedaban infectadas y el gusano se apoderaba del sistema. Una vez dentro de las computadoras infectadas, Mydoom podía realizar una serie de acciones maliciosas, como el envío masivo de correos no deseados (spam), el robo de direcciones de correo electrónico y la instalación de "backdoors" que permitían a los atacantes tomar el control remoto de las máquinas afectadas.

2) Derechos de autor:

El caso de "The Pirate Bay". The Pirate Bay es un sitio web de intercambio de archivos que ha estado en el centro de numerosas controversias y casos legales debido a su facilitación de la descarga de contenido protegido por derechos de autor, como películas, música y software sin la debida autorización.

Uno de los casos más notorios relacionados con The Pirate Bay ocurrió en 2009, cuando los fundadores del sitio fueron condenados en un tribunal de Suecia por violaciones de derechos de autor y sentenciados a prisión, además de enfrentar multas significativas. A pesar de las medidas legales y los esfuerzos por cerrar el sitio, The Pirate Bay ha continuado operando, a menudo cambiando de dominio para evadir la persecución legal.

3) Suplantación:

el "Phishing de PayPal en 2003". En 2003, los atacantes llevaron a cabo una campaña de phishing dirigida a los usuarios de PayPal, uno de los servicios de pago en línea más grandes y populares en ese momento.

En esta campaña de phishing, los atacantes enviaron correos electrónicos falsos que parecían ser de PayPal. Estos correos electrónicos instaban a los destinatarios a hacer clic en un enlace y proporcionar información personal, como números de tarjetas de crédito y contraseñas, bajo la falsa premisa de que era necesario para verificar o actualizar su cuenta de PayPal. Los correos

electrónicos y los sitios web a los que dirigían los enlaces eran muy convincentes y se asemejaban mucho a las comunicaciones legítimas de PayPal.

4) Phishing:

La empresa Equifax, una de las principales agencias de informes de crédito en los Estados Unidos, sufrió un importante ataque de phishing que llevó a una violación de datos masiva. En este caso, los atacantes aprovecharon una vulnerabilidad en una aplicación web de Equifax y engañaron a los empleados para que proporcionaran credenciales de acceso. La brecha de seguridad resultante expuso la información personal y financiera de millones de personas.

Vulnerabilidad

1) Criptografía débil:

El ataque "POODLE" (Padding Oracle On Downgraded Legacy Encryption) que se dio a conocer en 2014. POODLE era un ataque contra protocolos de seguridad SSL/TLS utilizados en servidores web y navegadores.

El ataque POODLE se centraba en la debilidad de la implementación de SSL 3.0, un protocolo de seguridad obsoleto, pero aún utilizado en algunas conexiones web. Los atacantes podían aprovechar esta debilidad para descifrar comunicaciones seguras y acceder a información confidencial transmitida entre un navegador y un servidor web.

2) Amplificador DDoS

El caso de "Amplificación NTP" que se informó en 2013.

En este caso, los atacantes aprovecharon servidores NTP (Network Time Protocol) mal configurados que tenían habilitada la función "monlist". El monlist es una función que permite a un servidor NTP proporcionar una lista de las últimas máquinas que se han sincronizado con él, lo que potencialmente permitía a los atacantes enviar pequeñas solicitudes a un servidor NTP mal configurado y recibir respuestas mucho más grandes. Esto se convirtió en una técnica de amplificación para llevar a cabo ataques DDoS.

3) Servicios con acceso potencial no deseado:

El "gusano Morris" (también conocido como el "Worm Morris"), que se propagó en noviembre de 1988 y tuvo un impacto significativo en Internet de la época.

El gusano Morris fue uno de los primeros gusanos de Internet y se propagó a través de una variedad de sistemas Unix conectados a la red. Una de las principales formas de infección era aprovechar el servicio Telnet, que permitía a los usuarios iniciar sesión en computadoras remotas. El gusano Morris explotó una vulnerabilidad en el sistema y se infiltró en las computadoras a través de conexiones Telnet no autorizadas.

4) Revelación de información:

El incidente que involucró la base de datos NoSQL Redis en 2013.

Redis es un sistema de almacenamiento en caché y base de datos en memoria utilizado para acelerar la recuperación de datos en aplicaciones web y otros servicios. En 2013, los investigadores de seguridad descubrieron que muchas instalaciones de Redis estaban configuradas incorrectamente y se dejaban abiertas al acceso público sin autenticación. Esto

significaba que cualquier persona con acceso a Internet podía conectarse a estas bases de datos Redis y potencialmente acceder o modificar la información almacenada en ellas.

Este problema de configuración llevó a la exposición de datos confidenciales y la revelación de información sensible en muchas bases de datos Redis. Los investigadores también notaron que algunos ciberdelincuentes aprovecharon esta situación para eliminar o modificar datos y exigir rescates a los propietarios de las bases de datos para restaurar la información.

5) -Sistema vulnerable:

el caso del "Ataque WPAD" que ocurrió en 2016.

El ataque WPAD se basó en la mala configuración de los sistemas de clientes que utilizaban el Protocolo de Descubrimiento de Proxy Web (WPAD). WPAD es un protocolo que permite a los clientes web buscar automáticamente la configuración del servidor proxy en una red local. Los atacantes aprovecharon esta función para llevar a cabo ataques de intermediario (man-in-the-middle) y redirigir el tráfico web a servidores proxy maliciosos controlados por ellos.

El ataque se basó en el supuesto que muchos sistemas estaban configurados para buscar la configuración del servidor proxy en la red local sin verificar adecuadamente la fuente de esa información. Los atacantes podían, por lo tanto, configurar un servidor proxy malicioso en la red local y proporcionar información de configuración falsa a los clientes, lo que les permitía interceptar y manipular el tráfico web de manera efectiva.

Otros

1) Otros:

2) APT

El caso del ataque cibernético conocido como "Stuxnet", que se descubrió en 2010.

Stuxnet fue un malware extremadamente sofisticado y altamente dirigido que se cree que fue desarrollado por agencias gubernamentales de los Estados Unidos e Israel. El objetivo principal de Stuxnet era sabotear el programa nuclear de Irán, específicamente su planta de enriquecimiento de uranio en Natanz.

Este malware utilizó múltiples técnicas avanzadas de ocultación y anonimato para eludir la detección y mantenerse en los sistemas durante un período prolongado. Se distribuyó a través de dispositivos USB y, una vez dentro de los sistemas de las instalaciones nucleares, se propagó y se aprovechó de las vulnerabilidades específicas en los sistemas de control industrial (SCADA) utilizados en las plantas nucleares.

3) Ciberterrorismo:

El ataque cibernético contra Estonia en 2007, que se conoció como el "Ciberataque de Estonia" o el "Ciberataque de Estonia en 2007".

En abril y mayo de 2007, Estonia sufrió una serie de ataques cibernéticos masivos que afectaron a varios de sus sitios web gubernamentales, instituciones financieras y medios de comunicación. Los ataques incluyeron la saturación de sitios web con tráfico, ataques de

denegación de servicio distribuido (DDoS) y otros métodos diseñados para interrumpir las comunicaciones y servicios en línea del país.

4) Daños informáticos PIC:

El caso del "Ataque cibernético en Ucrania en 2015".

En diciembre de 2015, Ucrania experimentó un ataque cibernético que afectó a su infraestructura eléctrica. Los atacantes, que se cree que tenían vínculos con Rusia, llevaron a cabo un ataque coordinado contra empresas eléctricas en Ucrania, lo que resultó en cortes de energía en varias regiones del país.

El ataque involucró el uso de malware y técnicas de ingeniería social para comprometer los sistemas de control industrial utilizados en el sector eléctrico. Esto permitió a los atacantes tomar el control de los interruptores y causar apagones en áreas clave. El ataque dejó a miles de personas sin electricidad durante un período de tiempo significativo, lo que afectó gravemente la prestación de servicios esenciales y la vida cotidiana.