***SEGURIDAD INFORMÁTICA***

***MALWARE:*** La palabra “MALWARE” es una contracción de “MALICIOUS SOFTWARE” es decir Software maliciosos. En otras palabras los malware son software intruso que está diseñados deliberadamente para provocar daños en equipos y sistemas informáticos. Estos pueden acceder a una red mediante Phishing, archivos adjuntos maliciosos, descargas maliciosas, ingeniería social o unidad flash.

La diferencia entre un virus y el malware es que el malware es un término genérico para una variedad de amenazas on line, incluidos virus, spyware, adware, rasonware y otros tipos de software maliciosos, entonces un virus informático es solo un tipo de malware.



E aquí que aparece el Virus informático “I LOVE YOU”, ya que un virus es un tipo de software malicioso, que se propaga entre computadoras daña los datos y al software. Se inserta o se adjunta a un programa o documento legítimo que admite macros (acción o conjunto de acciones que se puede ejecutar todas las veces que desee) esperando por medio de phishing que el usuario lo ejecute a fin de ejecutar su código.

***I LOVE YOU 2000***

El malware ILOVEYOU apareció por primera vez el 4 de mayo del año 2000 en Filipinas.

Los presuntos creadores son Onel de Guzmán y Rionel Ramones dos programadores de Filipinas. Guzmán el principal sospechoso fue descubierto por su proyecto académico de fin de curso que incluía código similar al utilizado en el virus.

 No se presentaron cargos en su contra debido a falta de leyes específicas contra el cibercrimen en Filipinas.

¿Cómo se propagó?

Se propagó a través del correo electrónico que llegaba a la bandeja de entrada con el asunto “I LOVE YOU”. El correo contenía un archivo adjunto llamado “LOVE- LETTER-FOR-YOU. txt. vbs” la extensión.”vbs” indicaba que era un script Visual Basic al hacer doble clip el script se ejecutaba. Esto activaba el malware que comenzaba a sobrescribir y renombrar archivos en el sistema del usuario causando pérdidas de datos.

 Activado el malware accedía a la lista de contactos del usuario en Microsoft Outlook y enviaba copias a todos los contactos con el mismo asunto y así se propagó rápidamente a través de redes corporativas y personales.

Métodos utilizados para infectar sistemas.

 Ingeniería social: el asunto del correo resultaba atractivo y engañoso. El archivo adjunto tenía nombre sugerente, el script un lenguaje que Windows podía ejecutar. Creaba o modificaba archivos del sistema para garantizar su persistencia en el sistema infectado. Robo de contraseñas.

¿Qué tipo de daño causó?

Causó un daño masivo a nivel global tanto en términos de impacto financiero con la pérdida de datos.

Aceptó a 45 millones de computadoras aproximadamente en todo el mundo fue uno de los más dañinos de la historia.

Impacto económico

Se estima entre 5 y 10 millones de dólares en daños por la pérdida de datos, la interrupción de operaciones y los costos de reparación y recuperación.

 Impacto social

Generó conciencia sobre la seguridad informática y la importancia de la protección contra amenazas cibernéticas. Resaltó la vulnerabilidad de los sistemas de correo electrónico y la necesidad de educar a los usuarios sobre los riesgos asociados con los archivos adjuntos y los enlaces en el correo.

Cómo operaba el malware?

El malware operaba atravez de

* Recepción del correo electrónico.
* El archivo adjunto malicioso
* Apertura del archivo
* Acceso a contactos de Outlook
* Envío de copias del correo original
* Sobre escritura de archivos
* Alteración de archivos del sistema
* Extracción de contraseñas
* Modificación de configuración del sistema
* Envío de información recopilada a los atacantes
* Rápida expansión.

¿Que lo hacía efectivo?

Lo hacía efectivo el mensaje y un asunto atractivo (te amo) que incentiva al usuario abrirlo. Las medidas tomadas para detener la propagación del malware fueron: desactivación de cuentas de correo, se bloqueaban y filtraban mensajes en el asunto y el archivo adjunto para evitar que se propague.

Las compañías de seguridad actualizaron sus bases de datos, distribuyeron herramientas de eliminación de malware, se intensificó la educación y concienciación sobre seguridad, implementaron parches y actualizaciones para para corregir vulnerabilidad en sistemas operativos y aplicaciones, se desarrollaron y mejoraron filtros de seguridad en los servidores de correo para detectar y bloquear mensajes maliciosos.

 Lecciones aprendidas

La importancia de educar al usuario, implementar las medidas de seguridad en los correos electrónicos, crear las copias de seguridad de datos, actualizar y mantener sistemas operativos y aplicaciones con los últimos parches, tener un plan de respuestas a incidentes y una estrategia para manejar ataques de malware.

Los malware “RANSOMWARE” son aquellos códigos maliciosos que le exigen al usuario el pago de un rescate por el secuestro de un archivo, donde puede tener archivos importantes o afectar el buen funcionamiento del equipo. Accediendo por medio de archivos adjuntos en correos electrónicos. El “WANANACRY” es un ejemplo.

 ***WANNACRY 2017***

El malware wannaCry apareció por primera vez en mayo de 2017.

Los presuntos creadores un grupo de hackers conocido como Lazarus Group o APT38 o Hindden Cobra de Corea del Norte.

Su propagación Ethernal Blue es una vulnerabilidad de Windows se propagó de una máquina a otra dentro de una red, sin necesidad de interacción del usuario.

El ran software escaneaba redes en busca de sistemas vulnerables, una vez identificado lo infectaba y cifraba sus archivos.

El sistema comprometido mostraba una nota de rescate y exigía pagos en Bitcoin criptomoneda para descifrar los datos.

 Método utilizado

Escaneo de redes en busca de sistemas vulnerables.

Utilizan correos electrónicos de phishing con archivo adjunto malicioso o enlaces a sitios web comprometidos para infectar sistemas.

 De esta manera se expanden rápidamente y comprometen un gran número de sistemas en poco tiempo.

Daños causados

El principal fue el cifrado de archivo y la clave de descifrado era proporcionada solo después de pagar el rescate.

Organizaciones como hospitales y empresas sufrieron grandes interrupciones en sus operaciones al no poder acceder a archivos críticos y sistemas.

Los usuarios que decidieron no pagar el rescate sufrieron pérdida permanente de datos importantes.

Este ataque afectó la confianza en la seguridad informática y en la práctica de protección de datos.

wannaCry afectó aproximadamente 230,000 sistemas en más de 150 países, hospitales, empresas, universidades sistemas de transportes.

El caso más notable fue el Servicio Nacional de Salud del Reino Unido, esto provocó la cancelación de citas, retraso en tratamientos, etc.

Impacto económico

 Pérdida económica global oscilaron entre 4000 y 8,000 millones de dólares.

 Gasto en seguridad y prevención: mejorar el sistema de seguridad, actualizar software y educar a los empleados sobre ciberseguridad.

 Impacto social

Interrupción de servicios esenciales como el servicio nacional de salud que puso en riesgo la vida de pacientes.

El aumento de conciencia sobre ciberseguridad tanto al público como las organizaciones.

Cómo operaba

El mal se infiltraba en sistemas que no habían instalado un parche de seguridad publicado por Microsoft en marzo de 2017.

También se distribuía a través de correo electrónico de phishing o archivos adjuntos que al abrir activa la infección. Dentro del sistema ejecutaba un cifrado utilizando un algoritmo AES-128 para encriptar archivos en la computadora de la víctima como documentos, imágenes, base de datos, etc.

 Eran renombrados con la extensión” WNCRY” y la clave de cifrado se almacenaba en el servidor de control de los atacantes. Tras el cifrado se mostraba una nota de rescate y el precio a pagar. La nota también contenía un tiempo límite después el rescate aumentaría y al no ser pagada en una semana los archivos serían eliminados.

Tenía capacidad de gusano, se propagaba automáticamente.

Un investigador de seguridad “Malware Techo” descubrió y activó accidentalmente un interruptor de apagado que detuvo la propagación.

¿Qué lo hacía efectivo?

Lo hacía efectivo que no tenía la necesidad de interacción del usuario.

La falta de actualización del sistema, la propagación automática en una misma red al tener la funcionalidad de gusano, el cifrado que hacía imposible para las víctimas recuperar sus archivos sin la clave, que muchas organizaciones no estaban preparados para un ataque de esta magnitud.

Medidas para detener la propagación

Interruptor de apagado (kill switch) el malware intentaba conectarse a este dominio al iniciarse y si la conexión tenía éxito el malware se desactivaba. Así se frenó el ataque.

 Aplicación de parches

Desconexión de sistemas afectados para evitar la propagación aún más.

Avisos globales: organizaciones de ciberseguridad, gobierno, empresas privadas emitieron avisos urgentes, instando a usuarios actualizar sus sistemas operativos, tomar medidas.

Lecciones aprendidas

Las lecciones aprendidas la importancia de mantener los sistemas actualizados el riesgo de seguir usando sistemas operativos obsoletos, la importancia de tener un plan de respaldo y recuperación ante desastres robustos. La capacitación de empleados la importancia de educar a usuarios y empleados para reconocer correos electrónicos de phishing.

 La respuesta al ataque mostró la necesidad de una mayor cooperación internacional entre gobierno, el sector privado, agencias de ciberseguridad para compartir información sobre amenazas y coordinar acciones de mitigación de manera eficiente.

***NOTPETYA-2016***

Fue el ciberataque más violento de la historia, es de tipo de ransonware-gusano apareció por primera vez en una empresa de navíos en Ucrania, en junio del 2017. Su objetivo fue generar destrucción sin obtener beneficios ya que borraba los archivos por completo, sin posibilidades de recuperar por lo menos parte de estos. Pensado para causar gran daño a Ucrania.

Encriptaba todo el disco duro en lugar de la MFT (Tabla de Archivos Maestros). Utilizaba la misma vulnerabilidad ethernet blue (CVE-2017-0144) que el ataque wannacry había utilizado en todo el mundo a principios del 2017. Se propaga a través de archivos adjuntos de correo electrónico. Los atacantes enviaban correos electrónicos a los departamentos de recursos humanos con solicitudes de empleo falsas adjuntas. Los PDF adjuntos contienen un enlace de DROPBOX infectado o son en realidad archivos ejecutables ocultos. Por esta razón su propagación por las redes fue muy rápido sin necesidad de que el usuario intervenga. Microsoft ya publicó un parche para la vulnerabilidad Eterhelblue pero muchas organizaciones no lo habían instalado todavía. Los afectados fueron sitios web de instituciones,empresas ucranianas, bancos, ministerios, diarios, empresas de electricidad, bancos entre otros. Otros países que sufrieron este ataque también fueron Francia, Alemania, Polonia, Reino Unido, Estados Unidos, Australia, Italia, etc. Según declaraciones de autoridades ucranianas, los investigadores de seguridad, Google y varios gobiernos han atribuido los ataques de Notpeteya al gobierno ruso, específicamente al grupo de piratas informático Sandworm dentro de la organización de inteligencia militar rusa GRU. La solución fue la actualización constante del software.

***EMOTET 2014-2021***

¿Qué es EMOTET?

Emotet es un troyano que se propaga principalmente a través de correos electrónicos no deseados (malspam). La infección puede llegar a través de un script (secuencia de comandos o guion que indica al ordenador las instrucciones que debe realizar) malicioso, archivos de documentos con macros o enlaces maliciosos.

Emotet es una familia de malware operada por un grupo de ciberdelincuencia conocido como “MEALYBUG” o “TA542. Aunque comenzó como un troyano bancario, más tarde se convirtió en una botnet (conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática) que paso a ser una de las amenazas más frecuentes de todo el mundo

***HISTORIA***

Identificado por primera vez en 2014, Emotet sigue infectando sistemas y perjudicando a los usuarios a día de hoy.

La primera versión estaba diseñada para robar datos bancarios interceptando el tráfico de internet. Poco después se detectó una nueva versión, denominada Emotet dos, venia empaquetada con varios módulos, entre ellos un sistema de transferencia de dinero, un módulo de malspam y un módulo bancario dirigido a bancos alemanes y austriacos.

En enero de 2015, una nueva versión de Emotet apareció. La versión tres, contenía modificaciones sigilosas diseñadas para mantener el malware volando bajo el radar y añadía nuevos objetivos bancarios suizos.

En el 2018 la nueva versión del troyano Emotet incluyen la capacidad de instalar otro malware en las maquinas infectadas. Este malware puede incluir otros troyanos y ransomware. En julio del 2019 un ataque de Emotet, en Lake City, Florida, le costó a la ciudad 460.000 dólares en pagos de ransomware. Una vez infectado Emotet descargó otro troyano bancario conocido como “TrickBot” y el ransomware “Ryuk”.

En 2019 se observa una campaña de spam impulsada por botnets dirigidas a victimas alemans, polacas, italianas e inglesas con línea de asunto astutamente redactada como “Aviso de remesa de pago” y “Factura Vencida”. Al abrir el documento de Microsoft Word infectado se inicia una macro, que a su vez descarga Emotet desde Sitios WordPress comprometidos.

Además de ser un troyano, Emotet también puede cargar un módulo gusano a través del cual se propaga en la red de las empresas. De esta forma, pues instalarse en otros equipos sin que los usuarios tengan que hacer click y activar un archivo adjunto, en este contexto Emotet también realiza ataques de fuerza bruta con el objetivo de descifrar contraseñas. Por tal motivo es considerado el malware más peligroso del mundo.

Tiene el súper poder de la invisibilidad, trabaja de la mano de la ingeniería social. Y se camufla en correos electrónicos con contenidos maliciosos, con un solo click en un enlace. Sin saberlo el cibernauta descarga el software malicioso y le da acceso a datos confidenciales, contraseñas, historia de búsqueda, etc., cualquier tipo de información atractiva para los hacker.