BOLETÍN DE CIBERSEGURIDAD
DICIEMBRE 2023

ADV
Integradores y Consultores S.A. de C.V.
AN Advisor Company

ÍNDICE

NOTICIAS INTERNACIONALES

ENCUENTRAN NKABUSE, UN SOFTWARE MALICIOSO COMPATIBLE CON DIVERSAS PLATAFORMAS QUE APROVECHA LA TECNOLOGÍA BLOCKCHAIN.

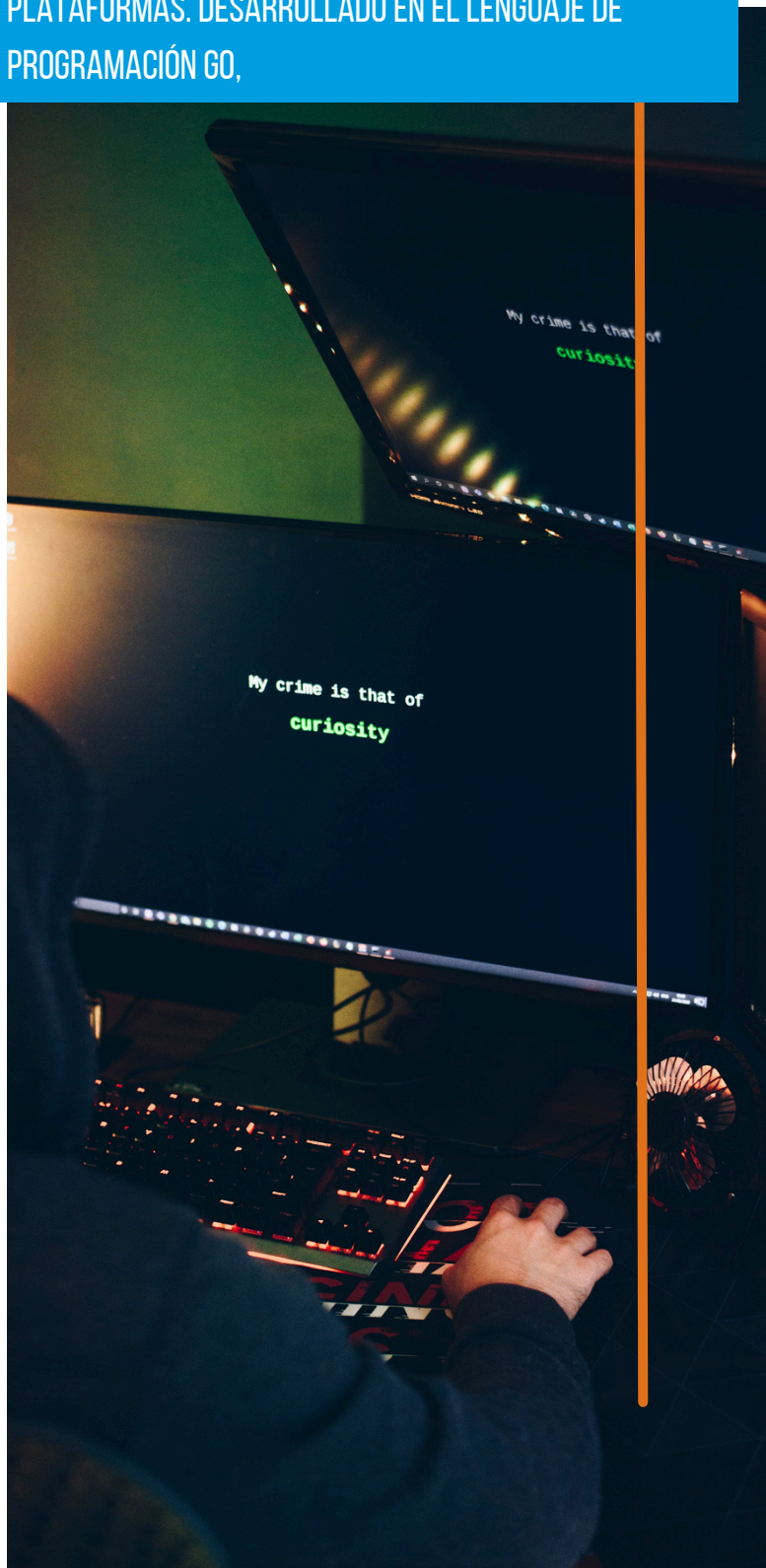
SE HA IDENTIFICADO UN NUEVO MALWARE VERSÁTIL LLAMADO NKABUSE QUE OPERA EN MÚLTIPLES PLATAFORMAS. DESARROLLADO EN EL LENGUAJE DE PROGRAMACIÓN GO,

Desarrollado en el lenguaje de programación Go, este malware avanzado utiliza la tecnología NKN, un protocolo de red peer-to-peer orientado a blockchain. Funciona como un flooder, inundando canales de red con mensajes sin sentido, y también actúa como una puerta trasera que concede a los delincuentes el control sobre el equipo infectado.

Durante la investigación de un incidente reciente, los expertos de Kaspersky descubrieron este malware, que explota el protocolo NKN conocido por su descentralización y privacidad. Se han detectado posibles víctimas en Colombia, México y Vietnam.

NKAbuse funciona como una amenaza híbrida, operando tanto como puerta trasera/RAT (herramienta de acceso remoto) como flooder, lo que lo convierte en una doble amenaza versátil. En su función de puerta trasera/RAT, permite a los atacantes acceder de manera no autorizada a los sistemas de las víctimas, lo que posibilita la ejecución encubierta de comandos, el robo de datos y la monitorización de actividades. Esta capacidad es especialmente valiosa para actividades de espionaje y filtración de datos. Además, en su función de flooder, puede lanzar ataques DDoS destructivos, afectando significativamente las operaciones de organizaciones al abrumar y interrumpir servidores o redes específicas.

Las funciones avanzadas de este malware incluyen la captura de pantallas, la administración de archivos, la recuperación de información del sistema y de la red, así como la ejecución de comandos del sistema. Los datos recopilados se envían al atacante a través de la red NKN, utilizando comunicación descentralizada para lograr un ataque eficiente y sigiloso.



ENCUENTRAN NKABUSE, UN SOFTWARE MALICIOSO COMPATIBLE CON DIVERSAS PLATAFORMAS QUE APROVECHA LA TECNOLOGÍA BLOCKCHAIN.

El proceso de infiltración de NKAbuse comienza explotando la antigua vulnerabilidad RCE CVE-2017-5638, lo que permite a los atacantes tomar el control de los sistemas afectados. Posteriormente, el malware descarga un implante en el host de la víctima y se coloca en el directorio temporal para su ejecución. Para garantizar su funcionamiento continuo dentro del sistema, NKAbuse establece la persistencia mediante la creación de una tarea cron y se sitúa en la carpeta de inicio del host.

El uso del protocolo NKN destaca la avanzada estrategia de comunicación de NKAbuse, aprovechando la descentralización y la privacidad de NKN para una comunicación eficiente y sigilosa entre los nodos infectados y los servidores C2. La elección de Go como lenguaje de programación proporciona compatibilidad multiplataforma, permitiendo a NKAbuse dirigirse a varios sistemas operativos y arquitecturas, incluidos los Linux de escritorio y los dispositivos IoT. La capacidad de Go para producir binarios autónomos simplifica la implementación y mejora la robustez, convirtiendo a NKAbuse en una herramienta formidable en el ámbito de las amenazas de ciberseguridad.

Ec. R. (2023, 21 diciembre). Descubren NKAbuse, un malware multiplataforma que aprovecha la tecnología blockchain. El Comercio Perú. https://elcomercio.pe/tecnologia/descubren-nkabuse-un-malware-multiplataforma-que-aprovecha-la-tecnologia-blockchain-noticia/

RANSOMWARE BLACKCAT AUMENTA SU IMPORTANCIA TRAS LA INTERVENCIÓN DEL FBI.

EL BURÓ FEDERAL DE INVESTIGACIÓN DE LOS ESTADOS UNIDOS (FBI) REVELÓ HOY QUE SE INFILTRÓ EN LA SEGUNDA BANDA DE RANSOMWARE MÁS PROLÍFICA DEL MUNDO.

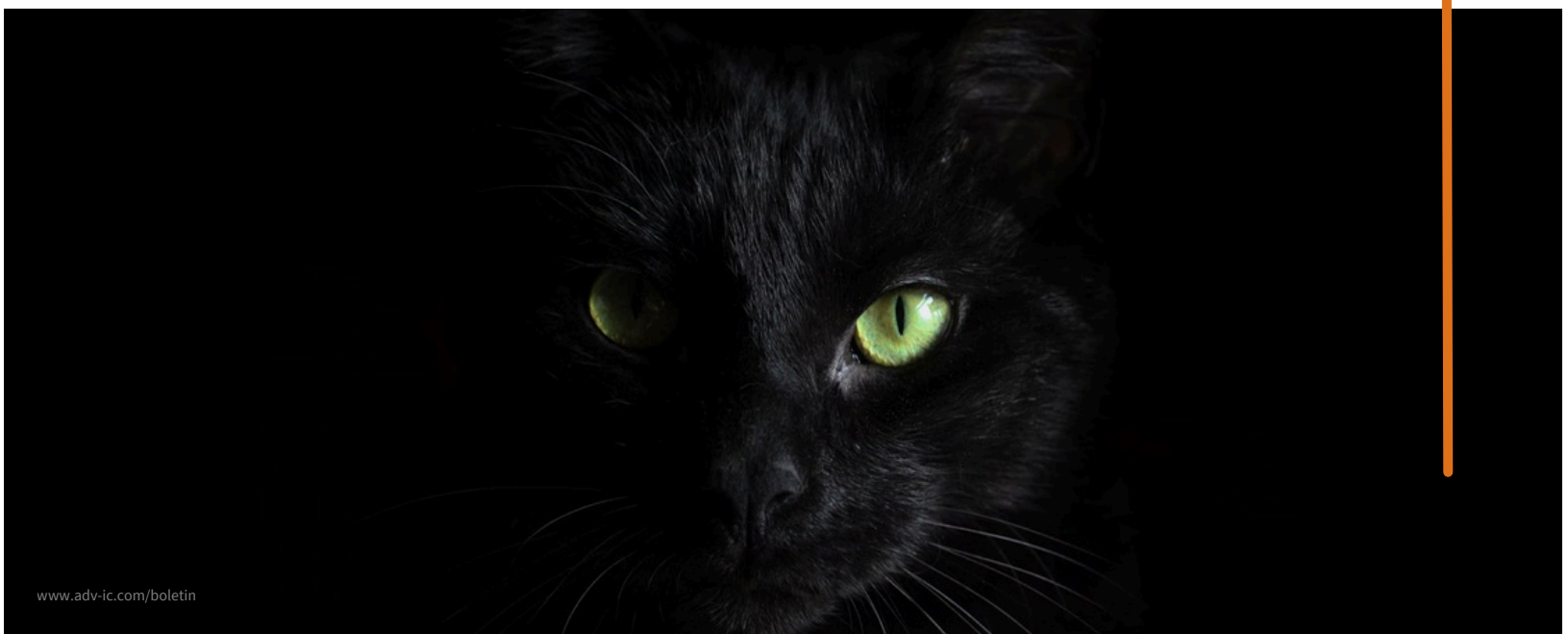
El Buró Federal de Investigación de los Estados Unidos (FBI) reveló hoy que se infiltró en la segunda banda de ransomware más prolífica del mundo, un grupo criminal con sede en Rusia conocido como ALPHV y BlackCat. El FBI afirmó que confiscó el sitio web darknet del grupo y lanzó una herramienta de descifrado que cientos de empresas afectadas pueden utilizar para recuperar sus sistemas. Mientras tanto, BlackCat respondió "desembargando" brevemente su sitio darknet con un mensaje que prometía comisiones del 90 por ciento para los afiliados que continuaran trabajando con el grupo delictivo, y declaró una temporada abierta para atacar desde hospitales hasta plantas nucleares.

Rumores sobre una posible acción de las fuerzas del orden contra BlackCat surgieron en la primera semana de diciembre, después de que el sitio darknet del grupo ransomware quedara fuera de línea y permaneciera inaccesible durante aproximadamente cinco días. BlackCat logró finalmente restablecer su sitio en línea, atribuyendo la interrupción a fallas en el equipo.

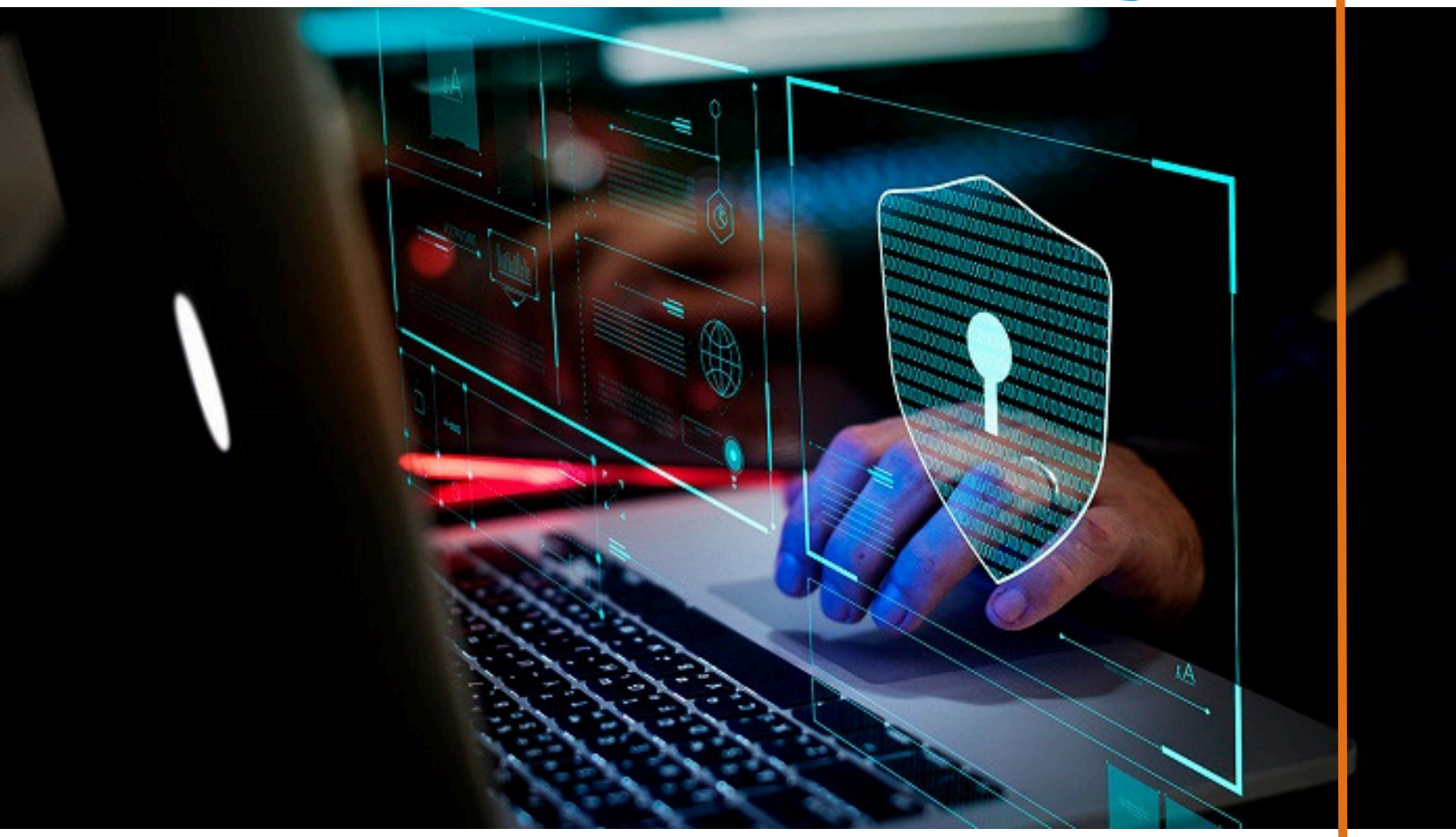
Sin embargo, hoy el sitio web de BlackCat fue reemplazado por un aviso de embargo del FBI, mientras que los fiscales federales en Florida emitieron una orden de registro explicando cómo los agentes del FBI lograron acceder y perturbar las operaciones del grupo.

Un comunicado del Departamento de Justicia de EE. UU. afirma que el FBI desarrolló una herramienta de descifrado que permitió a las oficinas de campo y socios de la agencia en todo el mundo ofrecer a más de 500 víctimas afectadas la capacidad de restaurar sus sistemas.

"Con una herramienta de descifrado proporcionada por el FBI a cientos de víctimas de ransomware en todo el mundo, las empresas y las escuelas pudieron reabrirse, y los servicios de atención médica y de emergencia pudieron volver a estar en línea", dijo la fiscal general adjunta Lisa O. Monaco. "Continuaremos priorizando las interrupciones y colocaremos a las víctimas en el centro de nuestra estrategia para desmantelar el ecosistema que alimenta el cibercrimen".



RANSOMWARE BLACKCAT AUMENTA SU IMPORTANCIA TRAS LA INTERVENCIÓN DEL FBI.



El DOJ informa que desde la formación de BlackCat hace aproximadamente 18 meses, el grupo delictivo ha dirigido sus ataques a las redes informáticas de más de 1,000 organizaciones víctimas. Los ataques de BlackCat suelen implicar el cifrado y robo de datos; si las víctimas se niegan a pagar un rescate, los atacantes suelen publicar los datos robados en un sitio darknet vinculado a BlackCat.

BlackCat se formó reclutando operadores de varias organizaciones de ransomware competidoras o disueltas, incluidas REvil, BlackMatter y DarkSide. Este último grupo fue responsable del ataque al Colonial Pipeline en mayo de 2021, que causó escasez de combustible y aumentos de precios en todo el país.

Al igual que muchas otras operaciones de ransomware, BlackCat opera bajo el modelo "ransomware como servicio", donde equipos de desarrolladores mantienen y actualizan el código ransomware, así como toda su infraestructura de soporte. Los afiliados son incentivados a atacar objetivos de alto valor porque generalmente obtienen el 60-80 por ciento de cualquier pago, y el resto va a los criminales que dirigen la operación de ransomware.

BlackCat logró recuperar brevemente el control sobre su servidor darknet hoy. Poco después de que se publicara el aviso de embargo del FBI, la página de inicio fue "desembargada" y adaptada con una declaración sobre el incidente desde la perspectiva del grupo de ransomware.

BlackCat afirmó que la operación del FBI solo afectó una parte de sus operaciones, y que como resultado de las acciones del FBI, 3,000 víctimas adicionales ya no tendrán la opción de recibir claves de descifrado. El grupo también anunció que eliminaba formalmente cualquier restricción o desaliento contra atacar hospitales u otra infraestructura crítica.

RANSOMWARE BLACKCAT AUMENTA SU IMPORTANCIA TRAS LA INTERVENCIÓN DEL FBI.

BlackCat ransomware raises ante after FBI disruption. (2023, 19 diciembre) https://krebsonsecurity.com/2023/12/blackcat-ransomware-raises-ante-after-fbi-disruption/.

"Debido a sus acciones, estamos introduciendo nuevas reglas, o mejor dicho, estamos eliminando TODAS las reglas excepto una, no pueden tocar a la CIS [una restricción común contra atacar organizaciones en Rusia o la Comunidad de Estados Independientes]. Ahora pueden bloquear hospitales, plantas nucleares, cualquier cosa, en cualquier lugar".

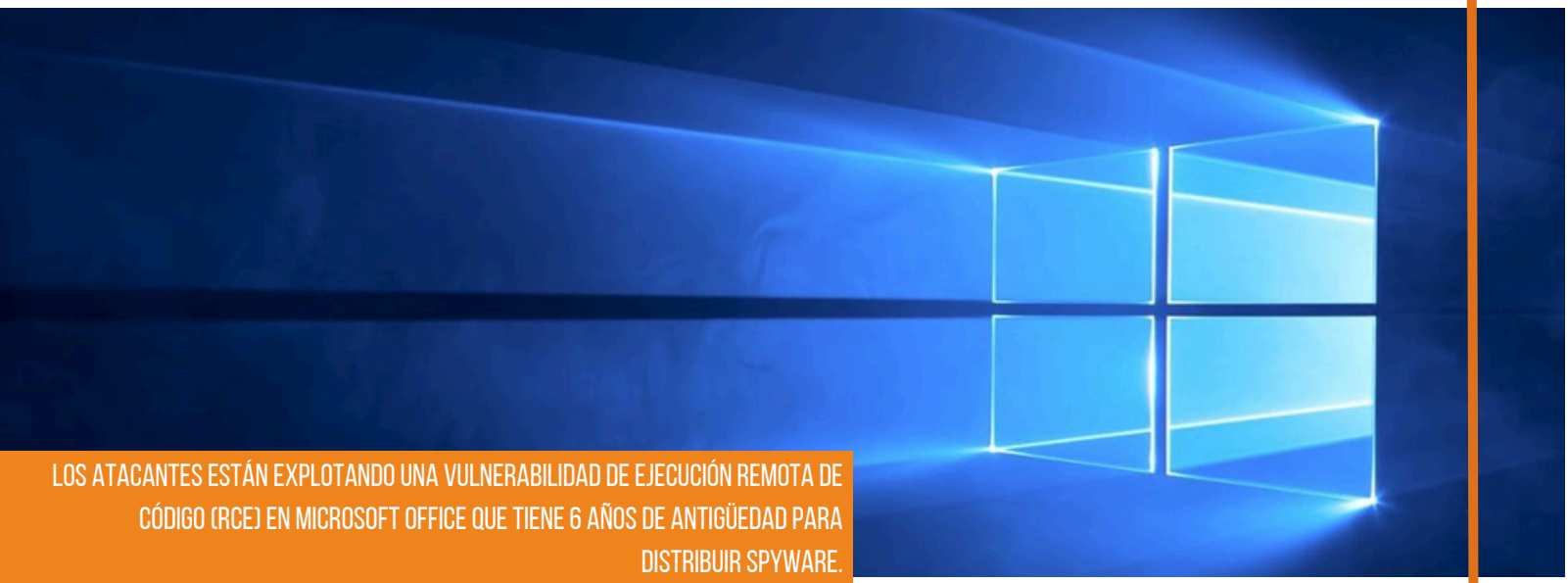
El grupo delictivo también dijo que establecería comisiones para afiliados en un 90 por ciento, presumiblemente para atraer el interés de posibles afiliados que de otro modo podrían estar asustados por la reciente infiltración del FBI. BlackCat también prometió que todos los "anunciantes" bajo este nuevo esquema gestionarían sus cuentas de afiliados desde centros de datos completamente aislados entre sí.

El sitio darknet de BlackCat actualmente muestra el aviso de embargo del FBI. Pero, como explicó el fundador de BleepingComputer, Lawrence Abrams, en Mastodon, tanto el FBI como BlackCat tienen las claves privadas asociadas con la URL del servicio oculto de Tor para el sitio de filtración de datos de BlackCat.

"Cualquiera que sea el último en publicar el servicio oculto en Tor (en este caso, el sitio de filtración de datos de BlackCat), recuperará el control sobre la URL", dijo Abrams. "Esperen ver este tipo de ida y vuelta en los próximos días".

El DOJ dice que cualquier persona con información sobre los afiliados de BlackCat o sus actividades puede ser elegible para una recompensa de hasta $10 millones a través del programa "Recompensas por Justicia" del Departamento de Estado, que acepta presentaciones a través de una línea de información basada en Tor (visitar el sitio solo es posible mediante el navegador Tor).

LOS ATACANTES ESTÁN APROVECHANDO UN FALLO DE SEGURIDAD DE MICROSOFT OFFICE DE 6 AÑOS DE ANTIGÜEDAD PARA PROPAGAR SPYWARE.



LOS ATACANTES ESTÁN EXPLOTANDO UNA VULNERABILIDAD DE EJECUCIÓN REMOTA DE CÓDIGO (RCE) EN MICROSOFT OFFICE QUE TIENE 6 AÑOS DE ANTIGÜEDAD PARA DISTRIBUIR SPYWARE.

Esta campaña de correo electrónico utiliza archivos maliciosos de Excel como señuelo y se caracteriza por tácticas de evasión sofisticadas.

Los actores de amenazas utilizan reclamos relacionados con la actividad empresarial en correos no deseados que entregan archivos que contienen CVE-2017-11882, una vulnerabilidad RCE que se remonta a 2014 y que puede permitir la toma de control del sistema, según revela una publicación de blog de Zscaler del 19 de diciembre. El objetivo final del ataque es cargar Agent Tesla, un troyano de acceso remoto (RAT) y un keylogger avanzado descubierto por primera vez en 2014, y extraer credenciales y otros datos de un sistema infectado a través de un bot de Telegram administrado por los atacantes.

CVE-2017-11882 es una vulnerabilidad de corrupción de memoria que se encuentra en el Editor de ecuaciones de Microsoft Office. Un atacante que explota con éxito la vulnerabilidad puede ejecutar código arbitrario en el contexto del usuario actual e incluso tomar el control del sistema afectado si un usuario ha iniciado sesión con derechos de administrador. Aunque la vulnerabilidad ha sido parcheada desde hace tiempo, las versiones antiguas de Microsoft Office que aún están en uso pueden ser vulnerables.

A pesar de tener casi una década de antigüedad, Agent Tesla sigue siendo un arma común utilizada por los atacantes y cuenta con funciones como registro de portapapeles, keylogging de pantalla, captura de pantalla y extracción de contraseñas almacenadas de diferentes navegadores web.

El vector de ataque es único en el sentido de que combina una vulnerabilidad de larga data con nuevas tácticas de complejidad y evasión que demuestran la adaptación en los métodos de infección de los atacantes, lo que "hace imperativo que las organizaciones se mantengan actualizadas sobre las amenazas cibernéticas en evolución para proteger su paisaje digital", señaló Kaivalya Khursale, investigador de seguridad senior de Zscaler, en la publicación.

En su vector de infección inicial, la campaña parece ser convencional, con actores de amenazas utilizando correos electrónicos con ingeniería social con señuelos orientados a los negocios en mensajes salpicados de palabras como "pedidos" y "facturas". Los mensajes agregan un sentido de urgencia al solicitar una respuesta inmediata de los destinatarios.

LOS ATACANTES ESTÁN APROVECHANDO UN FALLO DE SEGURIDAD DE MICROSOFT OFFICE DE 6 AÑOS DE ANTIGÜEDAD PARA PROPAGAR SPYWARE.

Writer, E. M. C. (2023, 20 diciembre). Attackers exploit 6-Year-Old Microsoft Office bug to spread spyware. https://www.darkreading.com/cloud-security/attackers-exploit-microsoft-office-bug-spyware

Pero una vez que un usuario cae en la trampa, el método de ataque se desvía hacia lo no convencional, encontraron los investigadores. Abrir el archivo adjunto de Excel malicioso con una versión vulnerable de la aplicación de hojas de cálculo inicia la comunicación con un destino malicioso que empuja archivos adicionales, el primero de los cuales es un archivo VBS fuertemente obfuscado que utiliza nombres de variables de 100 caracteres de longitud. Esto agrega "una capa de complejidad al análisis y desobfuscación", escribió Khursale.

Este archivo inicia la descarga de un archivo JPG malicioso, después de lo cual el archivo VBS ejecuta un ejecutable PowerShell que recupera el DLL codificado en Base64 del archivo de imagen, descodifica el DLL y carga los procedimientos maliciosos desde el DLL decodificado.

Después de que se carga PowerShell, hay otra táctica novedosa: ejecuta el archivo RegAsm.exe, cuya función principal está típicamente asociada con operaciones de lectura y escritura en el registro, señaló Khursale. Sin embargo, en el contexto del ataque, el propósito del archivo es llevar a cabo actividades maliciosas bajo la apariencia de una operación genuina. A partir de aquí, el DLL obtiene la carga útil de Agent Tesla e inyecta un hilo en el proceso RegAsm.

Una vez desplegado, el RAT spyware procede a robar datos de una variedad de navegadores, clientes de correo y aplicaciones FTP, enviándolos a un destino malicioso controlado por los actores de amenazas. También intenta desplegar ganchos de teclado y portapapeles para monitorear todas las pulsaciones de teclas y capturar datos copiados por el usuario.

Específicamente, Agent Tesla utiliza "window hooking", una técnica utilizada para monitorear mensajes de eventos, eventos de ratón y pulsaciones de teclas. Cuando un usuario actúa, la función del actor de amenazas intercepta antes de que ocurra la acción, dijo Khursale. El malware finalmente envía los datos exfiltrados a un bot de Telegram controlado por el actor de amenazas.

Zscaler incluyó una lista completa de indicadores de compromiso (IoCs) en la publicación del blog, incluida una lista de las URL de Telegram utilizadas para la exfiltración; URL maliciosas; varios archivos maliciosos de Excel, VBS, JPG y DLL; y ejecutables maliciosos, para ayudar a identificar si un sistema ha sido comprometido. La publicación también incluye una lista extensa de navegadores y clientes de correo y FTP desde los cuales Agent Tesla intenta robar credenciales para ayudar a las organizaciones a mantenerse alerta.

UN NUEVO ACTOR DE AMENAZAS LLAMADO 'GAMBLEFORCE' ESTÁ DETRÁS DE UNA SERIE DE ATAQUES DE INYECCIÓN SQL.

Investigadores han identificado a un nuevo actor de amenazas que está dirigiéndose a organizaciones en la región de Asia-Pacífico mediante ataques de inyección SQL, utilizando únicamente herramientas de pruebas de penetración de código abierto y públicamente disponibles.

Los cazadores de amenazas de Group-IB identificaron por primera vez al nuevo grupo en septiembre, apuntando a empresas de juegos de azar en la región y denominándolo "GambleForce". En los tres meses transcurridos desde entonces, el grupo ha dirigido sus ataques a organizaciones de varios sectores, incluidos el gubernamental, minorista, de viajes y sitios web de empleo.

Según un informe de Group-IB, GambleForce ha atacado a al menos dos docenas de organizaciones en Australia, Indonesia, Filipinas, India y Corea del Sur. "En algunos casos, los atacantes se detuvieron después de realizar reconocimiento", escribió Nikita Rostovcev, analista de amenazas senior de Group-IB. "En otros casos, extrajeron con éxito bases de datos de usuarios que contenían nombres de usuario y contraseñas con hash, junto con listas de tablas de bases de datos accesibles".

Los ataques de inyección SQL son exploits en los que un actor de amenazas ejecuta acciones no autorizadas, como recuperar, modificar o eliminar datos, en una base de datos de una aplicación web, aprovechando vulnerabilidades que permiten la inserción de declaraciones maliciosas en campos de entrada y parámetros que la base de datos procesa. Las vulnerabilidades de inyección SQL siguen siendo una de las vulnerabilidades más comunes en las aplicaciones web y representaron el 33% de todas las vulnerabilidades descubiertas en aplicaciones web en 2022.

"Los ataques SQL persisten porque son simples por naturaleza", afirmó Group-IB. "Las empresas a menudo pasan por alto la importancia de la seguridad de la entrada y la validación de datos, lo que lleva a prácticas de codificación vulnerables, software desactualizado y configuraciones inadecuadas de la base de datos", comentó Rostovcev.

Lo que destaca en la campaña de GambleForce es la dependencia del actor de amenazas en herramientas de pruebas de penetración de código abierto públicamente disponibles para llevar a cabo estos ataques. Cuando los analistas de Group-IB analizaron recientemente las herramientas alojadas en el servidor de comando y control (C2) del actor de amenazas, no encontraron una sola herramienta personalizada. En cambio, todas las armas de ataque en el servidor eran utilidades de software públicamente disponibles que el actor de amenazas parece haber seleccionado específicamente para ejecutar ataques de inyección SQL.

UN NUEVO ACTOR DE AMENAZAS LLAMADO 'GAMBLEFORCE' ESTÁ DETRÁS DE UNA SERIE DE ATAQUES DE INYECCIÓN SQL.

La lista de herramientas que Group-IB descubrió en el servidor C2 incluyó dirsearch, una herramienta para descubrir archivos y directorios ocultos en un sistema; redis-rogue-getshell, una herramienta que permite la ejecución remota de código en instalaciones de Redis; y sqlmap, para encontrar y explotar vulnerabilidades SQL en un entorno. Group-IB también descubrió que GambleForce utilizaba la popular herramienta de pruebas de penetración de código abierto Cobalt Strike para operaciones posteriores a la compromisión.

La versión de Cobalt Strike descubierta en el servidor C2 utilizaba comandos en chino. Sin embargo, eso solo no es evidencia del país de origen del grupo de amenazas, según indicó el proveedor de seguridad. Otra pista sobre la posible ubicación del grupo de amenazas fue que el servidor C2 cargaba un archivo desde una fuente que alojaba un marco en chino para crear y gestionar shells inversos en sistemas comprometidos.

Según Group-IB, la telemetría disponible sugiere que los actores de GambleForce no buscan datos específicos al atacar y extraer datos de bases de datos de aplicaciones web comprometidas. En cambio, el actor de amenazas ha estado intentando extraer cualquier dato disponible, incluidas credenciales de usuario en texto plano y con hash. Sin embargo, no está claro cómo el actor de amenazas podría estar utilizando los datos exfiltrados, según el proveedor de seguridad.

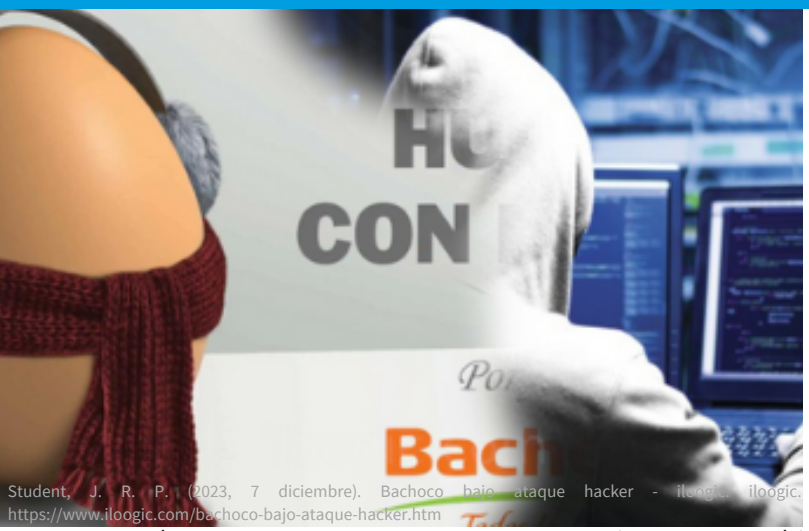
Los investigadores de Group-IB derribaron el servidor C2 del actor de amenazas poco después de descubrirlo. "No obstante, creemos que GambleForce es probable que se reagrupe y reconstruya su infraestructura antes de mucho y lance nuevos ataques", dijo Rostovcev.

Writer, J. V. C. (2023, 14 diciembre). New «GambleForce» threat actor behind string of SQL injectionattacks. https://www.darkreading.com/cloud-security/gambleforce-threat-actor-sql-injectionattacks

NOTICIAS NACIONALES

ATAQUE A BACHOCO CONFIRMADO

UN EMPLEADO DE BACHOCO HA VERIFICADO LA INTRUSIÓN EN EL SISTEMA SAP DE LA EMPRESA.



Student, J. R. P. (2023, 7 diciembre). Bachoco bajo ataque hacker - iloogic. iloogic. https://www.iloogic.com/bachoco-bajo-ataque-hacker.htm

Un empleado de Bachoco ha verificado la intrusión en el sistema SAP de la empresa. En una publicación en Reddit, el usuario u/Informal-Setting-190 compartió lo que parece ser una captura de pantalla de una computadora bloqueada dentro de la red corporativa. En la imagen se observa el fondo de pantalla distintivo de la empresa y el nombre de usuario 'whiteninja'.

"El ciberataque a Bachoco resultó en la interrupción de operaciones vitales, incluido el sistema SAP, un patrón característico de los ataques perpetrados por el ransomware Cactus. Estos ataques tienen como objetivo deshabilitar sistemas clave para presionar a las organizaciones y forzarlas a cumplir con las demandas de los atacantes".

El ransomware Cactus ha estado activo desde marzo de 2023 y se dirige a grandes entidades comerciales. Se sospecha que Cactus obtiene acceso inicial a la red de la víctima al explotar vulnerabilidades conocidas en los dispositivos VPN de Fortinet.

Se ha observado que el ransomware Cactus utiliza varias extensiones para los archivos a los que apunta, dependiendo de su estado de procesamiento. Cuando se prepara un archivo para el cifrado, el malware cambia su extensión a .CTSo. Después de completar el proceso de cifrado, la extensión se convierte en .CTS1. Además, este ransomware cuenta con un "modo rápido", el cual se asemeja a un cifrado ligero. Al ejecutar el malware en los modos rápido y normal de forma consecutiva, el mismo archivo se cifra dos veces, añadiendo una nueva extensión después de cada proceso (por ejemplo, .CTS1.CTS7).

En relación con estos eventos de ransomware, se adjuntan los siguientes indicadores de compromiso.

Indicador de compromiso principal:

- MD5: 1add9766eb649496bc2fa516902a5965
- SHA-256: 0933f23c466188e0a7c6fab661bdb8487cf7028c5cec557efb75fde9879a6af8
- MD5: 5737cb3a9a6d22e957cf747986eeb1b3
- SHA-256: 9ec6d3bc07743d96b723174379620dd56c167c58a1e04dbfb7a392319647441a

Indicadores de compromiso adicionales:

- d7429c7ecea552403d8e9b420578f954f5bf5407996afaa36db723a0c070c4de
- 78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17
- 9ec6d3bc07743d96b723174379620dd56c167c58a1e04dbfb7a392319647441a
- 298855bf350b823ae6d30bf0ff43f3621d01fd696b73f4fa440ce275071dfd42
- 69b6b447ce63c98acc9569fdcc3780ced1e22ebd50c5cad9ee1ea7a4d42e62cc

CLOUDFLARE AMPLÍA SUS OPERACIONES EN MÉXICO, CON UN EQUIPO LOCAL

Cloudflare, líder en conectividad en la nube que brinda servicios de red de entrega de contenido y ciberseguridad, anunció su expansión en el mercado mexicano en octubre de 2023 como parte de sus compromisos con América Latina.

En una entrevista con Business Insider México, Michelle Zatlyn, cofundadora, presidenta y COO de Cloudflare, compartió los objetivos de la expansión en uno de sus mercados clave en América Latina. Más del 38% de los ataques en México se dirigieron a empresas de criptomonedas, seguidas de las telecomunicaciones, la hospitalidad y, finalmente, la educación.

Zatlyn mencionó que Carlos Torales, VP de Cloudflare América Latina, destacó la importancia de invertir localmente para atender las necesidades empresariales en la región. La decisión de expandirse en México surgió como la opción número uno después de evaluar dónde invertir, considerando el talento disponible y la facilidad para hacer negocios en el país.

En el tercer trimestre de 2023, Cloudflare bloqueó en promedio 115 millones de ciberamenazas en México, desde phishing hasta ataques DDoS. La expansión se realiza en un momento de madurez para Cloudflare, y Zatlyn destaca la importancia de tener al líder adecuado, como Carlos, liderando el equipo.

La empresa planea contratar a más de 100 personas en los próximos 12 a 18 meses para respaldar la expansión y establecer un "negocio que funcione". La decisión de expandirse en México se basa en la madurez del mercado y en contar con el liderazgo adecuado.

Pintle, F. (2023, 19 diciembre). Cloudflare amplía sus operaciones en México, con un equipo local. Business Insider México | Noticias pensadas para ti. https://businessinsider.mx/cloudflare-mexico-expansion-michelle-zatlyn/

MICHELLE ZATLYN COOFUNDADORA, PRESIDENTA Y COO DE CLOUDFLARE

Según Cloudflare, México, junto con Brasil, se encuentra entre los diez principales países del mundo en términos de personas conectadas a Internet, lo que destaca la importancia de la ciberseguridad para las próximas generaciones. La expansión en México continuará, con inversiones en puntos de presencia, centros de datos y un enfoque en ayudar a las empresas a adoptar soluciones modernas para mantener su competitividad a nivel local y global.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: DICIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-7100	12/24/2023	vulnerability, which was classified as critical, was found in PHPGurukul Restaurant Table Booking System 1.0. Affected is an unknown function of the file /admin/bwdates-report-details.php.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-37924

Descripción: The manipulation of the argument fdate leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-248952.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-7058	12/22/2023	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-7058

Descripción: The manipulation of the argument page leads to path traversal: '../filedir'. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-248749 was assigned to this vulnerability.

TABLA DE VULNERABILIDADES RELEVANTES: DICIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-48690	12/21/2023	Railway Reservation System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-48690

Descripción: The 'bynum' parameter of the train.php resource does not validate the characters received and they are sent unfiltered to the database.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-48434	12/20/2023	Online Voting System Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-5913

Descripción: The 'username' parameter of the reg_action.php resource does not validate the characters received and they are sent unfiltered to the database.

TABLA DE VULNERABILIDADES RELEVANTES: DICIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-6768	12/20/2023	Authentication bypass vulnerability in Amazing Little Poll affecting versions 1.3 and 1.4.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-6768

Descripción: This vulnerability could allow an unauthenticated user to access the admin panel without providing any credentials by simply accessing the "lp_admin.php?adminstep=" parameter.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-47702	12/19/2023	IBM Security Guardium Key Lifecycle Manager 4.3 could allow a remote attacker to traverse directories on the system.	CVSS v3.1:9.1[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-46817

Descripción: An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view modify files on the system. IBM X-Force ID: 271196.

TABLA DE VULNERABILIDADES RELEVANTES: DICIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2019-25158	12/19/2023	A vulnerability has been found in pedroetb tts-api up to 2.1.4 and classified as critical. This vulnerability affects the function onSpeechDone of the file app.js.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2019-25158

Descripción: The manipulation leads to os command injection. Upgrading to version 2.2.0 is able to address this issue. The patch is identified as 29d9c25415911ea2f8b6de247cb5c4607d13d434. It is recommended to upgrade the affected component. VDB-248278 is the identifier assigned to this vulnerability.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-6483	12/18/2023	The vulnerability exists in ADiTaaS (Allied Digital Integrated Tool-as-a-Service) version 5.1 due to an improper authentication vulnerability in the ADiTaaS backend API.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-6483

Descripción: An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable platform. Successful exploitation of this vulnerability could allow the attacker to gain full access to the customers' data and completely compromise the targeted platform.

TABLA DE VULNERABILIDADES RELEVANTES: DICIEMBRE 2023

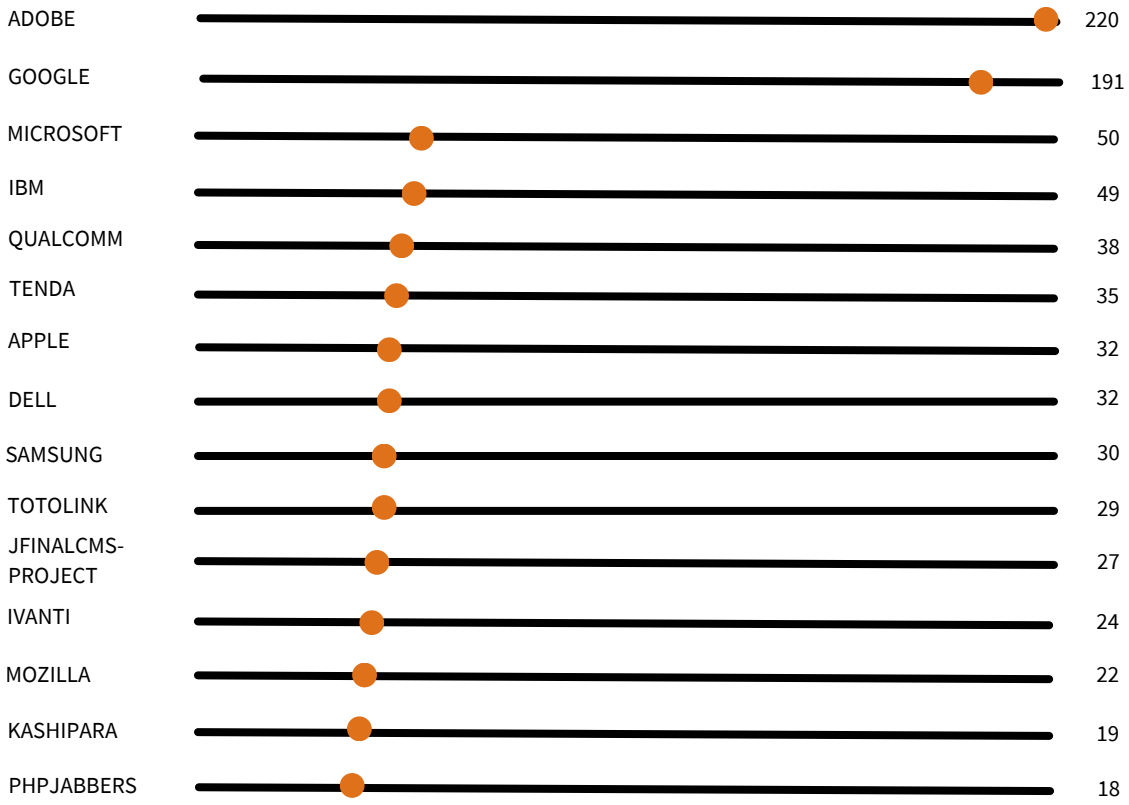
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-6553	12/15/2023	The Backup Migration plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.3.7 via the /includes/backup-heart.php file.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-6553

Descripción: This is due to an attacker being able to control the values passed to an include, and subsequently leverage that to achieve remote code execution. This makes it possible for unauthenticated attackers to easily execute code on the server.

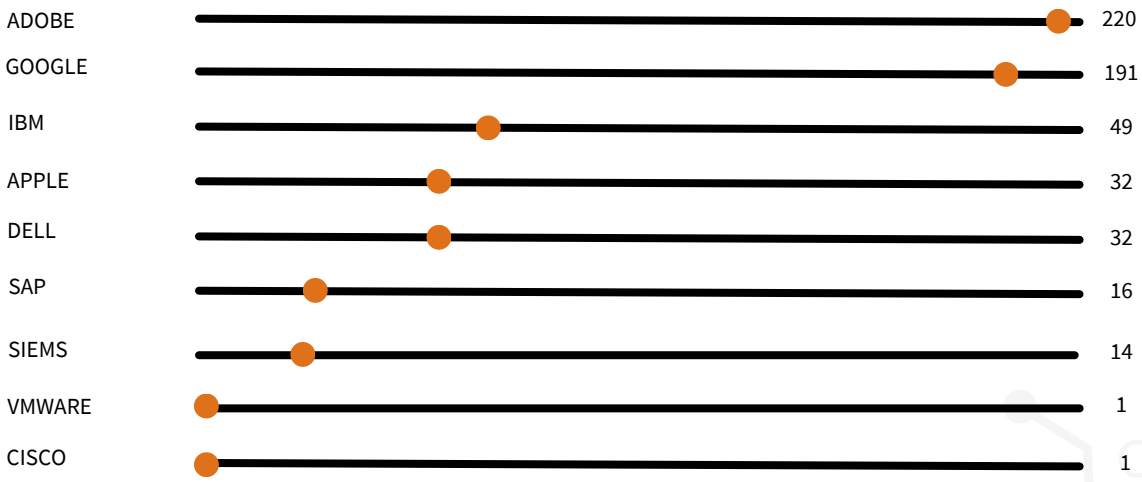
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-6756	12/13/2023	A vulnerability was found in Thecosy IceCMS 2.0.1. It has been classified as problematic. Affected is an unknown function of the file /login of the component Captcha Handler.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-6756

Descripción: The manipulation leads to improper restriction of excessive authentication attempts. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-247884.

FABRICANTES CON VULNERABILIDADES RELEVANTES: DICIEMBRE DE 2023



EMPRESAS MULTINACIONALES CON VULNERABILIDADES: DICIEMBRE DE 2023



CULTURA DE CIBERSEGURIDAD

INCIDENT RESPONSE.

DEFINICIÓN.

La "Incident Response" (Respuesta a Incidentes) es esencial en ciberseguridad, abordando la detección, gestión y recuperación de eventos no deseados en el ámbito digital. Frente a amenazas cibernéticas constantes, como ataques y malware, la respuesta a incidentes actúa como marco estratégico para mitigar riesgos y proteger la integridad de sistemas y datos.

El plan de respuesta incluye fases clave: identificación precisa del incidente, movilización de equipos de respuesta para investigación y recolección de evidencia, y la fase de contención y erradicación para limitar la amenaza y eliminarla. La comunicación efectiva con partes interesadas es vital, manteniendo transparencia y confianza.

Recopilar lecciones aprendidas contribuye a mejorar el plan de respuesta y evolucionar estrategias de seguridad. La implementación de medidas correctivas abarca la revisión de políticas, actualizaciones de software y capacitación del personal para prevenir futuros incidentes. La comunicación durante la respuesta implica informar a partes internas y externas, asegurando transparencia y gestión de reputación.

En resumen, la respuesta a incidentes no solo reacciona ante amenazas, sino que es parte integral de la estrategia de ciberseguridad, fortaleciendo la capacidad de una organización para enfrentar y recuperarse de eventos adversos en el entorno digital.

COMO FUNCIONA.

La función de Incident Response (respuesta a incidentes) se desarrolla mediante un conjunto estructurado de pasos diseñados para identificar, contener, erradicar y recuperarse de eventos cibernéticos no deseados. A continuación, se describen los principales pasos y se proporcionan ejemplos para ilustrar cómo funciona la respuesta a incidentes:

- Detección e Identificación:

Ejemplo: El sistema de monitoreo de seguridad de una empresa detecta patrones de tráfico inusuales en la red, lo que podría indicar un intento de ataque.

- Reporte y Evaluación:

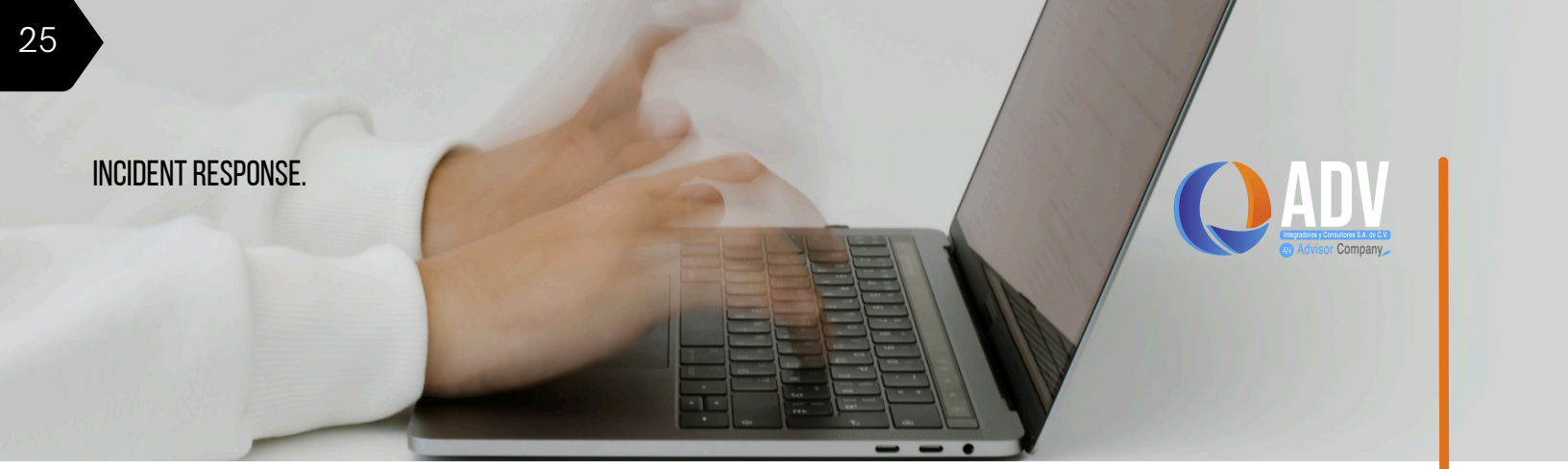
Ejemplo: Un usuario informa a los equipos de seguridad que ha recibido un correo electrónico sospechoso con un enlace que parece malicioso. El equipo evalúa la amenaza potencial.

- Movilización del Equipo de Respuesta:

Ejemplo: Un equipo de respuesta a incidentes se reúne para investigar el incidente, compuesto por expertos en seguridad, forenses digitales y representantes de TI.

- Análisis Forense:

Ejemplo: Se realiza un análisis forense del sistema afectado para determinar el alcance del incidente, recopilando datos relevantes como registros de actividad, archivos de registro y otros indicadores.



- Contención:

Se aislan los sistemas afectados para prevenir la propagación del malware o la actividad maliciosa a otras partes de la red.

- Erradicación:

Ejemplo: Se eliminan completamente las amenazas y se aplican parches de seguridad para cerrar las vulnerabilidades explotadas.

- Recuperación:

Ejemplo: Se restauran los sistemas afectados desde copias de seguridad confiables para asegurar la continuidad del negocio.

- Comunicación:

Ejemplo: Se informa a los empleados, clientes y otras partes interesadas sobre la naturaleza del incidente, las acciones tomadas y las medidas preventivas recomendadas.

- Lecciones Aprendidas y Mejora Continua:

Ejemplo: Se lleva a cabo una revisión post-incidente para identificar áreas de mejora en políticas, procedimientos y controles de seguridad.

Este proceso iterativo y estructurado permite a las organizaciones enfrentar y aprender de los incidentes cibernéticos de manera efectiva, fortaleciendo su postura de seguridad a lo largo del tiempo. La rapidez y eficacia en la respuesta a incidentes son cruciales para minimizar el impacto y mitigar las amenazas en evolución.

RIESGOS

Aunque la respuesta a incidentes es esencial para mitigar y gestionar eventos cibernéticos no deseados, también conlleva ciertos riesgos que deben abordarse para garantizar su efectividad. Algunos de los riesgos asociados con la respuesta a incidentes incluyen:

- Falsos Positivos:

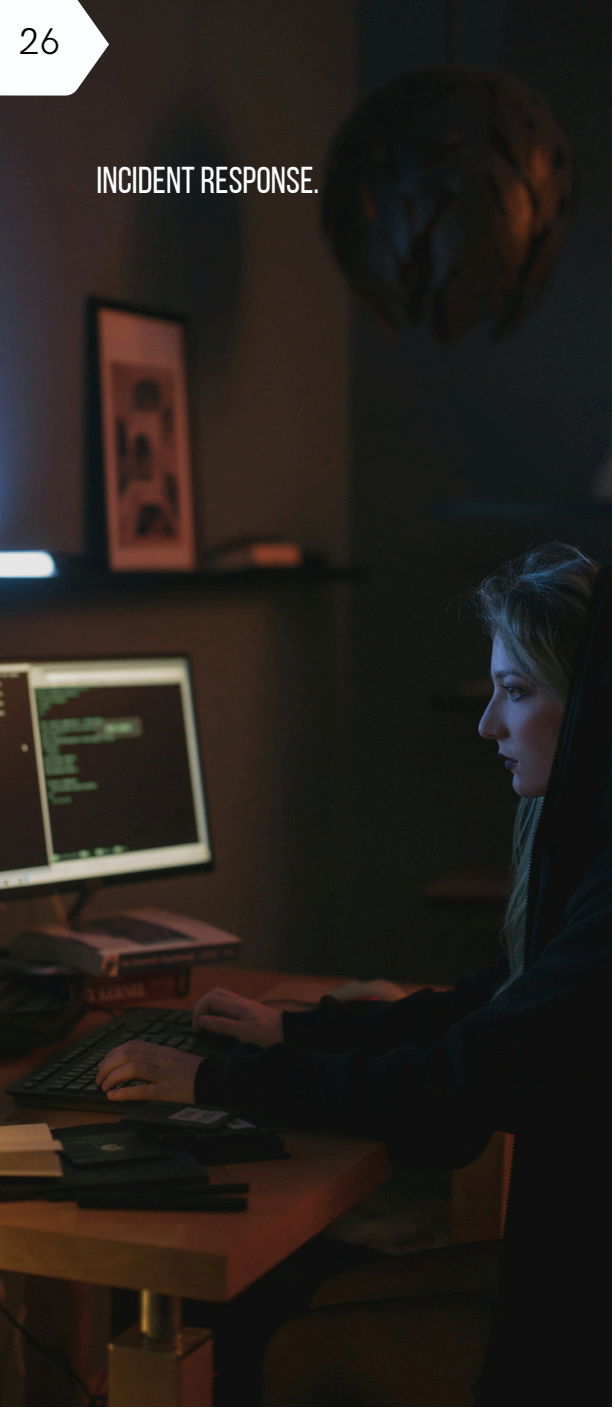
Descripción: La detección de eventos que parecen ser incidentes, pero que resultan ser benignos o normales.
Riesgo: Malgasto de recursos y tiempo en la respuesta a eventos que no representan una amenaza real.

- Falsos Negativos:

Descripción: La falta de detección de eventos reales o la subestimación de su gravedad.
Riesgo: No abordar adecuadamente incidentes genuinos, lo que podría resultar en daños mayores.

- Impacto Operativo:

Descripción: La respuesta a incidentes puede afectar las operaciones normales de la organización.
Riesgo: Interrupciones innecesarias en las operaciones comerciales que podrían tener consecuencias financieras.



INCIDENT RESPONSE.

IMPORTANCIA DE CONOCER

Conocer Incident Response (respuesta a incidentes) es fundamental en el ámbito de la ciberseguridad y para la gestión de riesgos en cualquier organización. Aquí hay varias razones clave por las cuales es esencial comprender y tener un plan de respuesta a incidentes:

- Mitigación de Daños:

La respuesta a incidentes ayuda a minimizar y controlar los daños causados por eventos cibernéticos no deseados. Una acción rápida y efectiva puede reducir el impacto y acelerar la recuperación.

- Preservación de la Continuidad del Negocio:

Un plan de respuesta a incidentes asegura que la organización pueda mantener sus operaciones críticas incluso después de un ataque o incidente. La rápida recuperación contribuye a la continuidad del negocio.

- Protección de la Reputación:

Una respuesta adecuada y transparente demuestra el compromiso de la organización con la seguridad y la protección de los activos de sus clientes. La mala gestión de incidentes puede dañar la reputación y la confianza del público.

- Cumplimiento Normativo:

Muchas regulaciones exigen que las organizaciones implementen planes de respuesta a incidentes. Cumplir con estas normativas es esencial para evitar sanciones y multas.

- Identificación y Gestión de Amenazas:

La respuesta a incidentes contribuye a la identificación de amenazas en curso y permite a la organización adaptar sus estrategias de seguridad para enfrentar los desafíos emergentes.

- Aprendizaje Continuo:

Cada incidente proporciona oportunidades valiosas para aprender y mejorar. La revisión post-incidente permite a la organización identificar áreas de mejora en sus políticas, procedimientos y controles de seguridad.

CASO CONOCIDO

Un caso conocido de Incident Response es el ataque sufrido por Target Corporation en 2013. Este incidente ilustra la importancia de una respuesta efectiva ante amenazas cibernéticas y cómo las organizaciones pueden aprender y mejorar a partir de tales eventos.

Caso Target Corporation (2013):

Descripción del Incidente:
En noviembre de 2013, Target, una cadena minorista líder en los Estados Unidos, sufrió un ataque cibernético significativo. Los atacantes comprometieron el sistema de pago de la tienda, obteniendo acceso no autorizado a datos de tarjetas de crédito y débito de millones de clientes.

INCIDENT RESPONSE.

Detección y Respuesta Inicial:
Target detectó actividad inusual en su red, pero la falta de una respuesta rápida permitió que los atacantes continuaran con sus operaciones durante varias semanas.

Impacto y Magnitud:
Se estima que la información de al menos 40 millones de tarjetas de crédito y débito fue comprometida, junto con datos personales de alrededor de 70 millones de clientes.

Respuesta a Incidentes:
Después de confirmar el incidente, Target movilizó un equipo de respuesta a incidentes para contener y erradicar la amenaza. Colaboraron con expertos en seguridad cibernética y forenses para investigar la brecha y entender su alcance.

Comunicación con Partes Interesadas:
Target informó públicamente sobre el incidente y estableció líneas de comunicación con los clientes afectados. También cooperó con las autoridades regulatorias y agencias de aplicación de la ley.

Lecciones Aprendidas:
El incidente llevó a Target a revisar y mejorar significativamente sus prácticas de seguridad. Se identificaron deficiencias en la detección, respuesta y monitoreo de amenazas.

Impacto a Largo Plazo:
Target experimentó consecuencias significativas, incluyendo pérdida de confianza de los clientes, impacto en las acciones de la empresa y costos asociados con la respuesta al incidente y las acciones legales subsiguientes.

Este caso destaca la importancia de contar con una respuesta a incidentes eficiente y proactiva. Además, resalta la necesidad de aprender de los incidentes para mejorar las prácticas de seguridad y proteger la integridad de los datos y la confianza del cliente.

COMO PUEDE AYUDAR ADV – IC

El Incident Response (respuesta a incidentes) juega un papel crítico en el fortalecimiento y la eficacia de un Security Operations Center (SOC, por sus siglas en inglés). Aquí se describen varias formas en que el Incident Response beneficia a un SOC:

- Detección Temprana de Incidentes:

La implementación de un plan de Incident Response contribuye a la detección temprana de incidentes, proporcionando al SOC la capacidad de identificar amenazas rápidamente.

- Respuesta Rápida y Coordinada:

Facilita una respuesta rápida y coordinada a incidentes detectados, lo que es crucial para minimizar el impacto y reducir el tiempo de respuesta.

Estructura y Proceso Formal:
Establece una estructura y procesos formales para la respuesta a incidentes, proporcionando al SOC una guía clara sobre cómo abordar y manejar diferentes tipos de amenazas.

INCIDENT RESPONSE.

- Colaboración con Equipos de Respuesta:

Facilita la colaboración efectiva entre el SOC y otros equipos de respuesta a incidentes, como equipos de seguridad, forenses digitales y comunicaciones.

• Mejora Continua:
La revisión post-incidente permite al SOC aprender de cada incidente, identificar áreas de mejora y mejorar continuamente sus procedimientos y capacidades.

• Gestión de Recursos Eficiente:
Ayuda a gestionar los recursos del SOC de manera eficiente durante un incidente, asegurando que se asignen adecuadamente para abordar y contener la amenaza.

• Automatización de Procesos:
Permite la automatización de ciertos procesos de respuesta a incidentes, lo que puede acelerar las acciones de contención y mitigación.

• Integración de Herramientas y Tecnologías:
Facilita la integración de herramientas y tecnologías en el entorno del SOC para mejorar la capacidad de detección, análisis y respuesta a incidentes.

• Mejora de la Coordinación Interna:
Mejora la coordinación interna entre analistas del SOC, asegurando una comunicación eficiente y una colaboración efectiva durante la respuesta a incidentes.

• Alineación con Objetivos Empresariales:
Ayuda a alinear las actividades del SOC con los objetivos y las prioridades empresariales, asegurando que la respuesta a incidentes esté alineada con las metas estratégicas de la organización.

• Capacitación y Desarrollo del Personal:
Facilita la capacitación y el desarrollo continuo del personal del SOC, mejorando la capacidad del equipo para abordar y responder a amenazas avanzadas.

En conjunto, la integración efectiva de la respuesta a incidentes en las operaciones diarias del SOC mejor la resiliencia de la organización frente a amenazas cibernéticas y contribuye a la eficacia general del centro de operaciones de seguridad.

REFERENCIAS

REFERENCIAS

- Martinez, C. (2020, 25 noviembre). Respuesta a incidentes de ciberseguridad: guía de NIST. AVSoft. https://www.avsoftware.com.mx/respuesta-a-incidentes-de-ciberseguridad-guia-de-nist/
- ¿Qué es la respuesta a incidentes? | IBM. (s. f.). https://www.ibm.com/mx-es/topics/incident-response
- Plan de respuesta a incidentes de ciberseguridad. (s. f.). Cyberzaintza. https://www.ciberseguridad.eus/empresa-segura/medidas-para-mitigar/plan-de-respuesta-incidentes-de-ciberseguridad

ZERU Cybersecurity Services

Security Operation Center - SOC by

ADV

+52 81 2011 8604

contacto@adv-ic.com

Av. Melchor Ocampo 193, Torre Privanza, Piso 11 Oficina 11D
Colonia Veronica Anzures. Delegación Miguel Hidalgo CP 11300