Boletín de Ciberseguridad

Fecha de Publicación
26/09/2022- N.º 43

Mes de Septiembre
12/09/2022 -26/09/2022

Datasec

Índice

Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta segunda quincena del mes de Septiembre se destacan 8 noticias de relevancia: 1 sobre vulnerabilidades tecnológicas, 6 de fraude informático y 1 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Brecha de seguridad en Uber a manos del grupo de hackers LAPS$

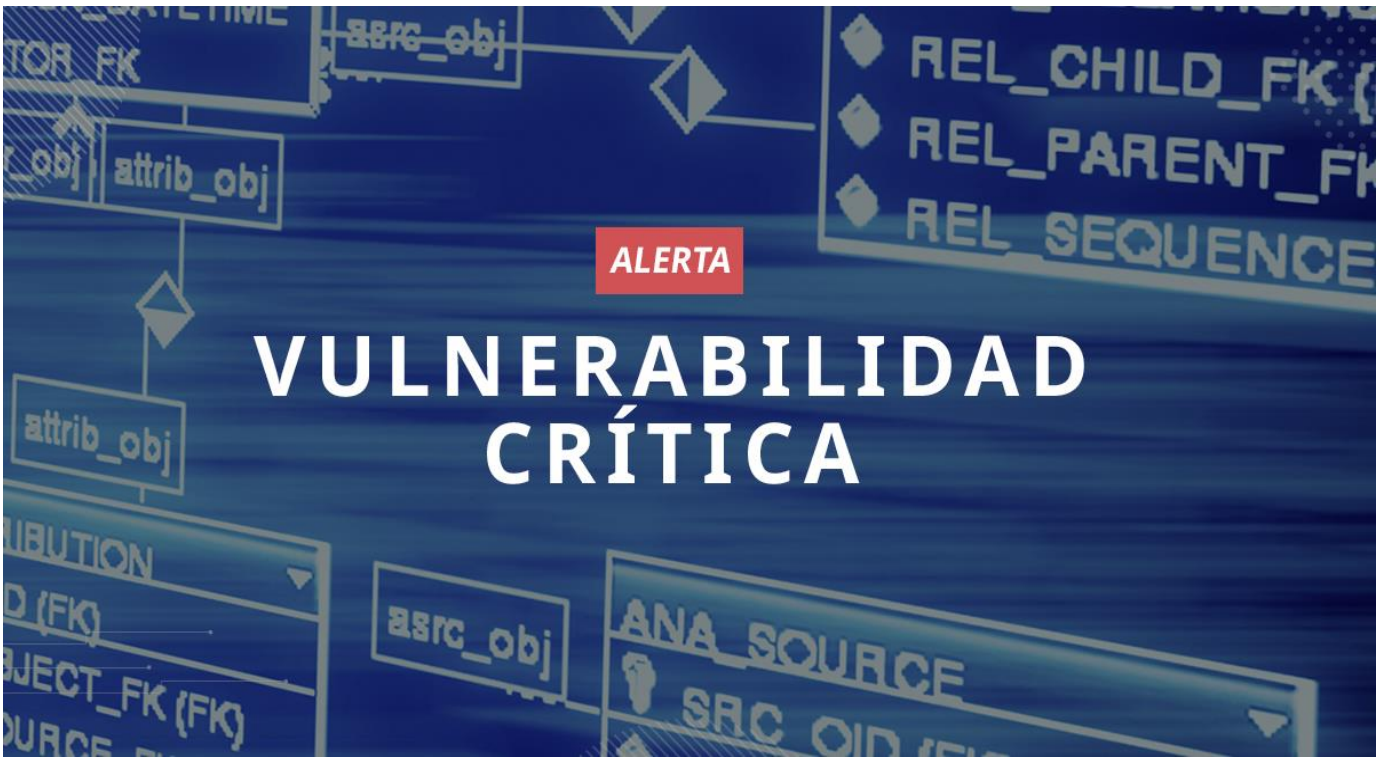
Uber informa sobre el incidente de seguridad que se hizo presente en todos sus servicios incluyendo Ubereats, Uber Freight y Uber Driver.

Ataque DDoS con 25,3 mil millones de solicitudes

Empresa de ciberseguridad logró mitigar un ataque de denegación de servicio distribuido (DDoS) con un total de más de 25.300 millones de solicitudes.

Ataque GIFShell de Microsoft Teams: qué es y cómo puede protegerse de él

El método de ataque GIFShell que ocurre a través de Microsoft Teams, es un ejemplo perfecto de cómo los actores de amenazas pueden explotar funciones y configuraciones legítimas que no se han configurado correctamente.



Microsoft	Microsoft realiza corrección de 64 errores	CRÍTICO

Descripción

Microsoft lanza correcciones para 64 errores, incluyendo cinco vulnerabilidades críticas y un zero-day explotado activamente.

Estado

La vulnerabilidad zero-day rastreada por Microsoft es de elevación de privilegios en el controlador del sistema de archivos de registro comunes de Windows. Afecta a todas las versiones de Windows y, si se aprovecha con éxito, un atacante podría obtener privilegios a nivel del sistema.

Microsoft compartió que la vulnerabilidad fue informada por cuatro personas y organizaciones diferentes de forma independiente, lo que sugiere que su explotación puede estar generalizada. Sin embargo, solo se clasifica como Importante, con una puntuación CVSS de 7,8, porque requiere la autenticación de un actor de amenazas, pero esto no lo hace menos peligroso.

Se requiere que el atacante tenga acceso y capacidad para ejecutar código en el sistema de destino, pero encadenar múltiples vulnerabilidades en un ataque es una práctica bastante común que debería considerarse una barrera menor para los actores de amenazas.

Este parche también incluye una segunda vulnerabilidad divulgada públicamente pero aparentemente sin explotar en los sistemas Windows 11 basados en ARM que podría permitir la restricción de especulación de caché. Se conoce como Spectre-BHB, una variante de Spectre v2, que se ha reinventado varias veces y ha estado persiguiendo varias arquitecturas de procesador durante cinco años en este momento.

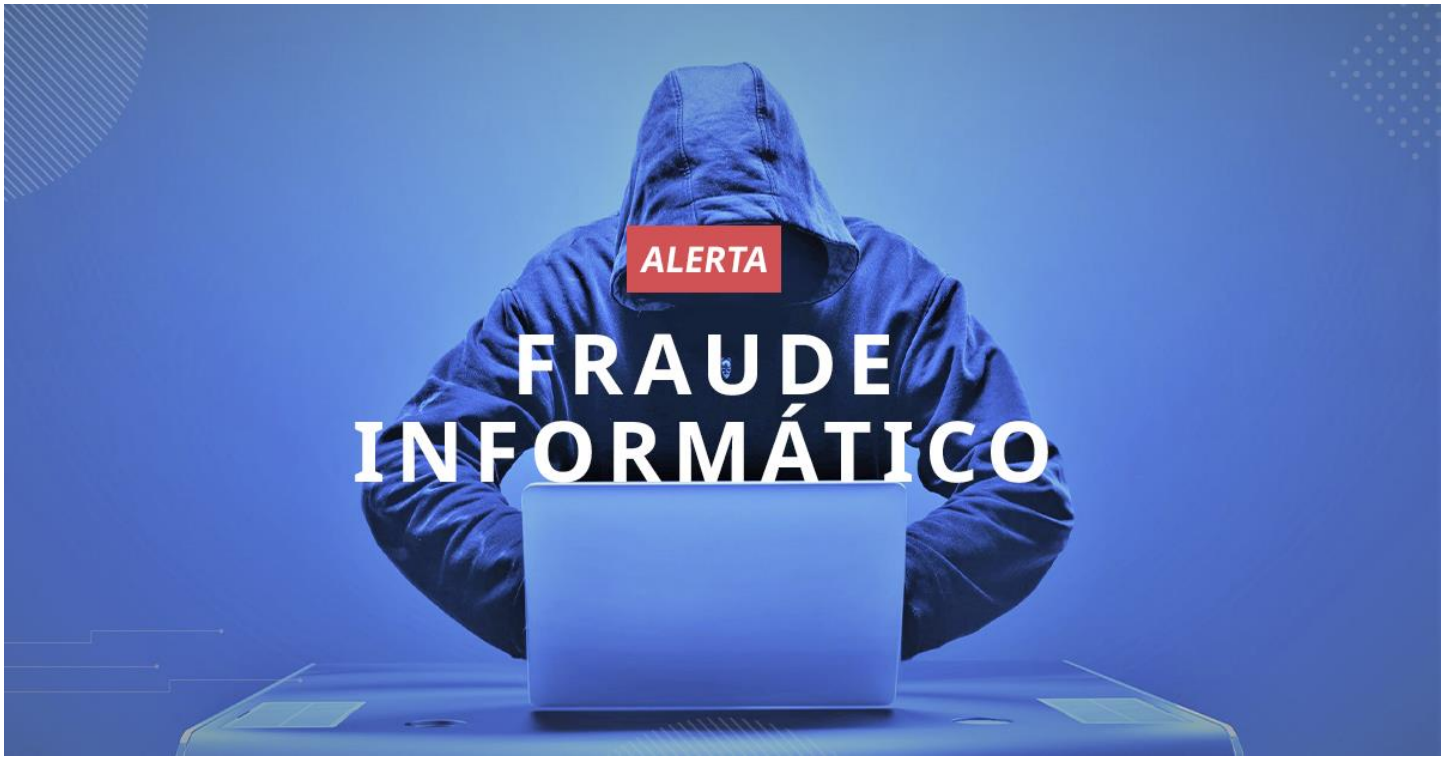
Esta clase de vulnerabilidades plantea un gran dolor de cabeza para las organizaciones que intentan mitigarlas, ya que a menudo requieren actualizaciones de los sistemas operativos, firmware y, en algunos casos, una recopilación de aplicaciones. y endurecimiento. Si un atacante explota con éxito este tipo de vulnerabilidad, podría obtener acceso a información confidencial.

Finalmente, Microsoft llamó la atención sobre otros dos errores importantes: Hay una vulnerabilidad de Elevación de privilegios en la cola de impresión, la cual se logra resolver con el parche. Se han causado desafíos adicionales para ciertos proveedores y modelos de impresoras. Si ha experimentado desafíos, sería bueno probar esta actualización con un cuidado adicional para asegurarse de que ningún problema afecte su entorno.

Remediación / Referencias

En primer lugar, debe corregir las vulnerabilidades ya parcheadas. Además, recomendamos proteger todas las computadoras y servidores conectados a Internet con soluciones de seguridad equipadas con tecnologías para la detección de vulnerabilidades y la prevención de exploits. Esto ayudará a defender a su empresa contra vulnerabilidades conocidas y desconocidas.

Para obtener más información ingrese a:
https://www.kaspersky.com/blog/microsoft-patch-tuesday-september-2022/45501/



WINTERMUTE	**Wintermute pierde USD 160 millones en incidente de piratería**	IMPORTANTE

Descripción

Activos digitales por un valor de USD 160 millones, fueron robados de la firma de comercio de criptomonedas Wintermute.

Estado

El hack involucró una serie de transacciones no autorizadas que transfirieron USD Coin, Binance USD, Tether USD, Wrapped ETH y otras 66 criptomonedas a la billetera del atacante.

La compañía dijo que sus operaciones de finanzas centralizadas (CeFi) y extrabursátiles (OTC) no se han visto afectadas por el incidente de seguridad.

El creador de mercado de activos digitales, que proporciona liquidez a más intercambios y plataformas criptográficas, advirtió sobre la interrupción de sus servicios en los próximos días, pero enfatizó que es solvente con el doble de esa cantidad en capital restante.

Los detalles que rodean el método de explotación exacto utilizado para perpetuar el ataque son desconocidos en este momento, aunque expertos declaran que el ataque fué causado por una vulneración de tipo Blasfemia en su billetera comercial.

Wintermute reconoció además que usó Profanity, un software de generación de direcciones personalizadas de Ethereum, junto con una herramienta interna para generar direcciones con muchos ceros al frente.

El proyecto de código abierto está actualmente abandonado por su mantenedor anónimo, que se hace llamar johguse, citando problemas de seguridad fundamentales en la generación de claves privadas.

La violación de Wintermute es el último ataque a los protocolos DeFi, incluido el de Axie Infinity, Harmony Horizon Bridge, Nomad y Curve.Finance en los últimos meses. Algunos de estos robos se han atribuido al Grupo Lazarus, respaldado por Corea del Norte.

Según el trabajo de investigación de expertos en la materia, los incidentes de seguridad que golpearon las plataformas DeFi resultaron en pérdidas por una suma de miles de millones de dólares sólo en 2021, y los servicios experimentaron un promedio de cinco ataques por mes.

Remediación / Referencias

La compañía aún investiga el ataque y se encuentra abierta a tratarlo como un white hat, por lo cual, a través de sus redes sociales y medios de comunicación, han incentivado a/los atacantes a comunicarse.

Para más información acceder a:
https://thehackernews.com/2022/09/crypto-trading-firm-wintermute-loses.html

	**Ataque DDoS con 25,3 mil millones de solicitudes**	IMPORTANTE

Descripción

Empresa de ciberseguridad logró mitigar un ataque de denegación de servicio distribuido (DDoS) con un total de más de 25.300 millones de solicitudes.

Estado

Se dice que el fuerte ataque, que tuvo como objetivo a una empresa de telecomunicaciones china no identificada, duró cuatro horas y alcanzó un máximo de 3,9 millones de solicitudes por segundo (RPS).

Los atacantes utilizaron la multiplexación HTTP/2, o la combinación de varios paquetes en uno, para enviar varias solicitudes a la vez a través de conexiones individuales.

El ataque se lanzó desde una botnet que comprendía casi 170.000 direcciones IP diferentes que abarcaban routers, cámaras de seguridad y servidores comprometidos ubicados en más de 180 países, principalmente EE. UU., Indonesia y Brasil.

La misma víctima fue atacada previamente el 21 de julio de 2022, de manera similar en la que el volumen del ataque aumentó a 853,7 gigabits por segundo (Gbps) y 659,6 millones de pps durante un período de 14 horas.

La compañía ha sido bombardeada implacablemente con sofisticados ataques distribuidos de denegación de servicio (DDoS), lo que indica que las ofensivas podrían tener motivaciones políticas frente a la guerra en curso de Rusia contra Ucrania.

Ambos intentos disruptivos fueron ataques de inundación UDP en los que el atacante apunta y abruma puertos arbitrarios en el host de destino con paquetes de Protocolo de datagramas de usuario (UDP).

UDP, al ser tanto sin conexión como sin sesión, lo convierte en un protocolo de red ideal para manejar el tráfico de VoIP. Pero estos mismos rasgos también pueden hacerlo más susceptible a la explotación.

Remediación / Referencias

No existen protecciones internas que puedan limitar la tasa de una inundación UDP. Como resultado, los ataques DoS de inundación UDP son excepcionalmente peligrosos porque pueden ejecutarse con una cantidad limitada de recursos.

Para más información acceder a:
https://thehackernews.com/2022/09/record-ddos-attack-with-253-billion.html

	**Emotet Botnet comenzó a distribuir Quantum y BlackCat Ransomware**	IMPORTANTE

Descripción

El malware Emotet ahora está siendo aprovechado por grupos de ransomware como servicio (RaaS), incluidos Quantum y BlackCat, después del retiro oficial de Conti del panorama de amenazas este año.

Estado

Emotet comenzó como un troyano bancario en 2014, pero las actualizaciones que se le agregaron con el tiempo transformaron el malware en una amenaza muy potente que es capaz de descargar otras cargas útiles en la máquina de la víctima, lo que le permitiría al atacante controlar de forma remota.

Aunque la infraestructura asociada con el cargador de malware invasivo se eliminó como parte de un esfuerzo de aplicación de la ley en enero de 2021, se dice que el cártel de ransomware Conti desempeñó un papel fundamental en su regreso a finales del año pasado.

Desde noviembre de 2021 hasta la disolución de Conti en junio de 2022, Emotet fue una herramienta exclusiva de ransomware de Conti; sin embargo, la cadena de infección de Emotet actualmente se atribuye a Quantum y BlackCat.

Las secuencias de ataque típicas implican el uso de Emotet (también conocido como SpmTools) como un vector de acceso inicial para soltar Cobalt Strike, que luego se usa como una herramienta posterior a la explotación para operaciones de ransomware.

Es posible que la notoria banda de ransomware Conti se haya disuelto, pero varios de sus miembros siguen tan activos como siempre, ya sea como parte de otras bandas de ransomware como BlackCat y Hive o como grupos independientes centrados en la extorsión de datos y otras actividades delictivas.

Quantum también es un grupo derivado de Conti que, en los meses intermedios, ha recurrido a la técnica de phishing de devolución de llamada, denominada BazaCall o BazarCall, como un medio para violar las redes específicas.

Los afiliados de Conti usan una variedad de vectores de acceso inicial que incluyen phishing, credenciales comprometidas, distribución de malware y vulnerabilidades de explotación.

Se han observado más de 1.267.000 infecciones de Emotet en todo el mundo desde principios de año, con picos de actividad registrados en febrero y marzo coincidiendo con la invasión rusa de Ucrania.

Un segundo aumento de infecciones ocurrió entre junio y julio, debido al uso por parte de grupos de ransomware como Quantum y BlackCat. Los datos capturados hasta la fecha muestran que el país objetivo de Emotet es EE. UU., seguido de Finlandia, Brasil, Países Bajos y Francia.

ESET informó anteriormente que las detecciones de Emotet se multiplicaron por 100 durante los primeros cuatro meses de 2022 en comparación con los cuatro meses anteriores, de septiembre a diciembre de 2021.

Remediación / Referencias

Especialistas de seguridad informan que las detecciones de Emotet se multiplicaron por 100 durante los primeros cuatro meses de 2022.

Por mayor información:
https://thehackernews.com/2022/09/emotet-botnet-started-distributing.html

LastPass	Ciberdelincuentes acceden a los sistemas de desarrollo de LastPass	IMPORTANTE

Descripción

La solución de administración de contraseñas LastPass compartió que los atacantes tuvieron acceso a sus sistemas durante un período de cuatro días.

Estado

LastPass reveló que una infracción dirigida a su entorno de desarrollo resultó en el robo de parte de su código fuente e información técnica

La compañía completó la investigación del hackeo en asociación con la firma de respuesta a incidentes Mandiant, y señaló que el acceso se logró utilizando el punto final comprometido de un desarrollador. Si bien el método de entrada inicial sigue siendo "no concluyente", LastPass informó que el criminal abusó del acceso persistente para suplantar al desarrollador, después de que la víctima se autenticara mediante la autenticación de múltiples factores.

A pesar del acceso no autorizado, el atacante no logró obtener ningún dato confidencial de clientes, debido al diseño del sistema y los controles zero-trust implementados para evitar este tipo de incidentes.

Esto incluye la separación completa de los entornos de desarrollo y producción y su propia incapacidad para acceder a las bóvedas de contraseñas de los clientes sin la contraseña maestra establecida por los usuarios.

Además, también se realizaron verificaciones de integridad del código fuente para buscar signos de envenenamiento y que los desarrolladores no poseen los permisos necesarios para enviar el código fuente directamente desde el entorno de desarrollo a la producción.

Remediación / Referencias

LastPass señaló que contrató los servicios de una empresa de seguridad líder en el mundo, para mejorar sus prácticas de seguridad en el código fuente y que implementó barandillas de seguridad de punto final adicionales, para detectar y prevenir los ataques dirigidos a sus sistemas.

Puedes acceder a toda la información en el siguiente enlace:
https://thehackernews.com/2022/09/hackers-had-access-to-lastpasss.html

Uber	Brecha de seguridad en Uber a manos del grupo de hackers LAPSUS$	IMPORTANTE

Descripción

Uber informa sobre el incidente de seguridad que se hizo presente en todos sus servicios incluyendo Ubereats, Uber Freight y Uber Driver.

Estado

Esta no es la primera violación de seguridad a la que Uber debe de hacer frente. Fue objeto de escrutinio por no revelar adecuadamente una violación de datos de 2016 que afectó a 57 millones de pasajeros y conductores y, en última instancia, pagar a los piratas informáticos USD$100,000 para ocultar la violación. Se hizo de conocimiento público recién a finales de 2017.

El ataque fue orquestado por un hacker de 18 años, que se hace llamar Tea Pot, quién también se atribuyó la responsabilidad de irrumpir en el fabricante de videojuegos Rockstar Games y quien presuntamente se encuentra afiliado al notorio grupo de pirateria LAPSUS$.

LAPSUS$ utiliza técnicas similares para atacar a las empresas de tecnología, y solo en 2022 ha logrado atacar empresas como Microsoft, Cisco, Samsung, NVIDIA y Okta, entre otros.

La pandilla de extorsionistas con motivación financiera recibió un duro golpe en marzo de 2022 cuando la policía de la ciudad de Londres se movió para arrestar a siete personas de entre 16 y 21 años por sus supuestas conexiones con el grupo. Dos de esos acusados menores enfrentan cargos de fraude.

El ataque se logró engañando a un empleado de Uber para que proporcionara acceso a la cuenta mediante ingeniería social, logrando que éste aceptara un aviso de autenticación multifactor (MFA) que permitía al atacante registrar su propio dispositivo.

Remediación / Referencias

Uber se encuentra trabajando con varias firmas de forenses digitales líderes en el mundo, asimismo adelantó que no se expusieron datos confidenciales y que sus servicios se encuentran operativos.

La compañía agregó que tomó una serie de medidas como parte de sus medidas de respuesta a incidentes, incluida la desactivación de las herramientas afectadas, la rotación de claves de los servicios, el bloqueo de la base de código y también el bloqueo de las cuentas de los empleados comprometidos para que no accedan a los sistemas de Uber o, alternativamente, la emisión de un restablecimiento de contraseña para esas cuentas.

Por mayor información acceder a:
https://thehackernews.com/2022/09/uber-claims-no-sensitive-data-exposed.html

	Ataque GIFShell de Microsoft Teams: qué es y cómo puede protegerse de él	IMPORTANTE

Descripción

El método de ataque GIFShell que ocurre a través de Microsoft Teams, es un ejemplo perfecto de cómo los actores de amenazas pueden explotar funciones y configuraciones legítimas que no se han configurado correctamente.

Estado

Las organizaciones y los equipos de seguridad trabajan para protegerse de cualquier vulnerabilidad y, a menudo, no se dan cuenta de que el riesgo también lo generan las configuraciones en sus aplicaciones SaaS que no se han fortalecido.

La técnica de ataque GIFShell permite a los ciber delincuentes explotar varias funciones de Microsoft Teams para actuar como C&C para el malware y filtrar datos usando GIF sin ser detectados por EDR y otras herramientas de monitoreo de red. Este método de ataque requiere un dispositivo o usuario que ya esté comprometido.

El componente principal de este ataque permite a un atacante crear un shell inverso que entrega comandos maliciosos a través de GIF codificados en base64 en Teams y extrae la salida a través de GIF recuperados por la propia infraestructura de Microsoft.

Microsoft está de acuerdo en que este método de ataque es un problema, sin embargo, no cumple con los requisitos para una solución de seguridad urgente. Informa que pueden tomar medidas en una versión futura para ayudar a mitigar esta técnica, reconoce la investigación, pero afirma que no se han pasado por alto los límites de seguridad.

De acuerdo con las afirmaciones de Microsoft, de hecho, este es el desafío que enfrentan muchas organizaciones: hay configuraciones y características que los actores de amenazas pueden explotar si no se fortalecen.

Remediación / Referencias

Hay configuraciones de seguridad dentro de Microsoft que, si se fortalecen, pueden ayudar a prevenir este tipo de ataque:

- 1- Inhabilitar el acceso externo: Microsoft Teams, de forma predeterminada, permite que todos los remitentes externos envíen mensajes a los usuarios dentro de ese inquilino.
- 2- Inhabilitar conversaciones de inicio de equipos externos no administrados.
- 3- Obtenga información sobre el inventario de dispositivos: puede asegurarse de que todos los dispositivos de su organización cumplan con las normas y sean seguros mediante el uso de su

solución XDR/ EDR/ Gestión de vulnerabilidades, como Crowdstrike o Tenable. Las herramientas de seguridad de punto final son su primera línea de defensa contra actividades sospechosas, como acceder a la carpeta de registro de equipos locales del dispositivo que se utiliza para la filtración de datos en GIFShell.

Para más información acceder a:
https://thehackernews.com/2022/09/microsoft-teams-gifshell-attack-what-is.html

Bitdefender	**Bitdefender lanza descifrador gratuito para el ransomware LockerGoga**	PREVENCIÓN

Descripción

La empresa rumana de ciberseguridad Bitdefender, en colaboración con Europol han puesto a disposición un descifrador para el ransomware LockerGoga.

Estado

Identificado en enero de 2019, LockerGoga acaparó titulares por sus ataques contra el gigante noruego del aluminio Norsk Hydro. Se dice que infectó a más de 1.800 víctimas en 71 países, causando daños estimados en 104 millones de dólares.

La operación de ransomware recibió un golpe significativo en octubre de 2021 cuando 12 personas relacionadas con el grupo, junto con MegaCortex y Dharma, fueron detenidas como parte de un esfuerzo internacional de aplicación de la ley.

Los arrestos, que tuvieron lugar en Ucrania y Suiza, también incluyeron la incautación de dinero en efectivo por un valor de USD $52,000, cinco vehículos de lujo y una serie de dispositivos electrónicos.

La Policía de Zúrich informó que examinó los dispositivos de almacenamiento de datos confiscados a los individuos durante los arrestos de 2021 e identificó numerosas claves privadas que se usaron para bloquear los datos.

También se espera que se publique una utilidad de descifrado para MegaCortex en los próximos meses. También se recomienda a las partes víctimas que presenten una denuncia penal en sus respectivos países de origen, ya que estas claves permiten a las empresas e instituciones agraviadas recuperar los datos que se cifraron previamente con el malware LockerGoga o MegaCortex

Remediación / Referencias

Como un medio para prevenir las infecciones de ransomware, se insta a las organizaciones a manejar de forma segura los correos electrónicos, bloquear los archivos adjuntos de correo electrónico sospechosos, crear copias de seguridad periódicas, hacer cumplir la autenticación de dos factores y mantener los sistemas de TI actualizados.

Para más información acceder a:
https://thehackernews.com/2022/09/europol-and-bitdefender-release-free.html

Conclusiones

La seguridad de la información, analizamos; se está volviendo, en esta era de conflictos y de alta competitividad, en un instrumento cada vez más utilizado para ganar poder frente a otros, utilizado a todo nivel; desde contiendas íntimas o personales, así como motivos de espionaje nacional, comercial e industrial.

Los instrumentos que facilitan los ataques y compromisos siguen teniendo que ver con la interrelación que existe entre el uso de las tecnologías y nosotros con ellas.
Lo que las ciencias de la computación nos muestran a través de la ciberseguridad, es de alguna manera, como la evolución y escalabilidad es tan compleja de hacerla segura ante crecimientos solicitudes antes no consideradas o proyectadas. Este hecho, es uno de los tantos que con más frecuencia veremos en las noticias; ataques de denegación de servicios distribuidos, ataques a sistemas de desarrollo, abuso de credenciales triviales.

Las historias de cuidados se remontan hace mucho tiempo atrás, ahora sucede igual, a través de nuestros boletines, podemos estar atentos y conscientes de las amenazas emergentes que cualquier individuo u organización hoy en día debe cuidar para defenderse de múltiples riesgos que cuestan muy caro.

Una y otra vez la recomendación sigue siendo probar y medir las cuestiones de ciberseguridad con estándares altos. La conciencia en seguridad de la información es parte de una transmisión cultural, que también implica un desarrollo, una pedagogía muchas veces necesaria para reconocer las mejores prácticas de defensa y protección.

Para esto, hoy en día cada vez más naciones generan instrucción específica en ciencias de la computación a temprana edad, incluyendo muchos temas de ciberseguridad.
Desde Datasec aplaudimos estas decisiones y seguiremos apoyando a todos los actores de la sociedad en defender sus activos de valor, del modo más efectivo y óptimo. Cuanto antes aprendamos y realicemos nuestras acciones en conjunto con seguridad, todos saldremos beneficiados.

Ojalá así sea, y a nuestros lectores, los deseos de otro reencuentro fraterno en quince días.

Hasta entonces.