Verne
TECHNOLOGY GROUP

Boletín de alertas

Newsletter Seguridad Verne

Vol. 28/24

ÍNDICE

GootLoader: La Amenaza Persistente del Malware en la Web 3

El ataque a Polyfill[.]io afecta a más de 380.000 hosts, incluidas importantes empresas. 5

¿Te ha llegado este SMS de la DGT? Cuidado, se trata de una multa falsa que roba tu dinero 7

Vulnerabilidad de exposición de información en el plugin MRW 9

Todos los posibles ciberriesgos de la app para ver porno en España: desde robo de datos hasta brechas de seguridad 11

GOOTLOADER: LA AMENAZA PERSISTENTE DEL MALWARE EN LA WEB

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Malware	Usuarios	Alta

GootLoader, un peligroso malware que sigue evolucionando, ha lanzado nuevas versiones que incrementan su capacidad de ataque, según un reciente análisis de la firma de ciberseguridad Cybereason. Este malware, parte del troyano bancario Gootkit, es operado por el grupo conocido como Hive0127 o UNC2565. Utiliza tácticas de optimización en motores de búsqueda (SEO) para engañar a los usuarios y hacer que descarguen cargas maliciosas a través de archivos disfrazados de documentos legales.

GootLoader compromete sitios web legítimos para alojar su carga maliciosa, utilizando archivos JavaScript que simulan ser plantillas de contratos o documentos legales. Una vez que los usuarios desprevenidos descargan estos archivos, el malware se instala y ejecuta scripts de PowerShell que recopilan información del sistema y permiten la persistencia en el dispositivo infectado.

Para evitar la detección, GootLoader ha adoptado técnicas sofisticadas como la ofuscación del flujo de control, el aumento del tamaño de la carga útil y la codificación del código fuente. Además, el malware se inserta en bibliotecas JavaScript legítimas como jQuery y Lodash, dificultando aún más su identificación y análisis.

Recientemente, los atacantes han implementado una herramienta de comando y control llamada GootBot, que facilita movimientos laterales dentro de redes comprometidas, ampliando su alcance y potencial de daño. Esto subraya la continua evolución y adaptación de GootLoader para maximizar sus beneficios financieros a través de ataques cibernéticos.

Los métodos de SEO utilizados por GootLoader son particularmente efectivos para atraer a víctimas que buscan archivos relacionados con negocios, lo que aumenta significativamente el riesgo para empresas y profesionales. Es crucial que las organizaciones refuercen sus medidas de ciberseguridad y capaciten a sus empleados sobre los riesgos de descargar archivos de fuentes no verificadas.

Para una protección efectiva, se recomienda mantener actualizadas las soluciones de seguridad, implementar políticas de filtrado web y educar a los usuarios sobre las técnicas comunes de ingeniería social empleadas por los atacantes. Además, la monitorización constante y el análisis de tráfico pueden ayudar a detectar y neutralizar amenazas antes de que causen daños significativos.

GootLoader representa una amenaza persistente y adaptable en el panorama actual de ciberseguridad. Su capacidad para evolucionar y el uso de técnicas avanzadas de evasión subrayan la necesidad de una vigilancia constante y medidas de protección robustas para mitigar los riesgos asociados con este tipo de malware.

EL ATAQUE A POLYFILL[.]IO AFECTA A MÁS DE 380.000 HOSTS, INCLUIDAS IMPORTANTES EMPRESAS

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Ciberataque	JavaScript Polyfill[.]io	Media

El ataque a la cadena de suministro dirigido a la biblioteca de JavaScript Polyfill[.]io, ampliamente utilizada, tiene un alcance más amplio de lo que se creía anteriormente.

Nuevos hallazgos de Censys muestran que más de 380 000 hosts están incorporando un script polyfill que se vincula al dominio malicioso a partir del 2 de julio de 2024.

"Aproximadamente 237.700 están ubicados dentro de la red Hetzner (AS24940), principalmente en Alemania", señaló. "Esto no es sorprendente: Hetzner es un servicio de alojamiento web popular y muchos desarrolladores de sitios web lo aprovechan".

Un análisis más detallado de los hosts afectados reveló dominios vinculados a empresas importantes como WarnerBros, Hulu, Mercedes-Benz y Pearson que hacen referencia al punto final malicioso en cuestión.

Los detalles del ataque surgieron a fines de junio de 2024, cuando Sansec alertó que el código alojado en el dominio Polyfill había sido modificado para redirigir a los usuarios a sitios web con temática de juegos de azar y para adultos.

Los cambios en el código se realizaron de tal manera que las redirecciones solo se producían en ciertos momentos del día y solo contra los visitantes que cumplían ciertos criterios.

Se dice que el comportamiento nefasto se introdujo después de que el dominio y su repositorio GitHub asociado se vendieran a una empresa china llamada Funnull en febrero de 2024.

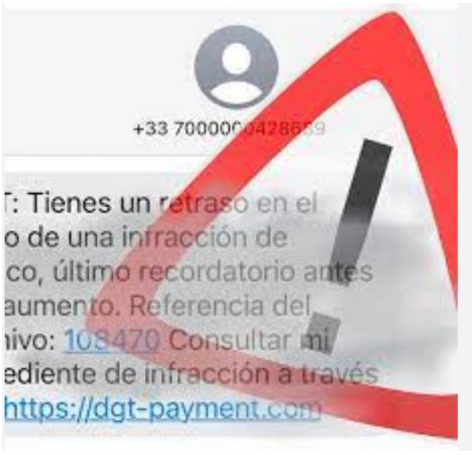
Desde entonces, el desarrollo ha llevado al registrador de dominios Namecheap a suspender el dominio, a las redes de distribución de contenido como Cloudflare a reemplazar automáticamente los enlaces de Polyfill con dominios que conducen a sitios espejo alternativos seguros, y a Google a bloquear los anuncios de los sitios que incorporan el dominio.

Si bien los operadores intentaron relanzar el servicio bajo un dominio diferente llamado polyfill[.]com, Namecheap también lo eliminó a partir del 28 de junio de 2024. De los otros dos dominios registrados por ellos desde principios de julio (polyfill[.]site y polyfillcache[.]com), el último sigue en funcionamiento.

Además de eso, se ha descubierto una red más extensa de dominios potencialmente relacionados, incluidos bootcdn[.]net, bootcss[.]com, staticfile[.]net, staticfile[.]org, unionadjs[.]com, xhsbpza[.]com, union.macoms[.]la, newcrbpc[.]com, que están vinculados a los mantenedores de Polyfill, lo que indica que el incidente podría ser parte de una campaña maliciosa más amplia.

¿TE HA LLEGADO ESTE SMS DE LA DGT? CUIDADO, SE TRATA DE UNA MULTA FALSA QUE ROBA TU DINERO

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Correo Malicioso	Usuarios	Alta



La Dirección General de Tráfico (DGT) ha advertido sobre una nueva campaña de phishing, conocida como 'smishing', que utiliza mensajes de texto para engañar a las víctimas y obtener sus datos privados y bancarios. Esta estafa se presenta como un aviso de multas de tráfico pendientes de pago, instando a los destinatarios a efectuar el pago en un plazo de 24 horas para evitar recargos del 50% y posibles demandas. Los mensajes, que generan una sensación de urgencia, incluyen un enlace que, al ser clicado, solicita información sensible como accesos bancarios y datos de tarjetas de crédito.

Lo que distingue a esta campaña de estafas anteriores es la evolución en su técnica. Antes, los mensajes procedían de números aleatorios, lo que podía despertar sospechas. Sin embargo, la nueva modalidad utiliza una técnica llamada 'SMS spoofing', que permite falsificar el ID del remitente para que el mensaje parezca provenir directamente de la

DGT. Esta manipulación del remitente aumenta significativamente la credibilidad del fraude, haciendo que las víctimas potenciales sean más propensas a caer en la trampa.

La DGT ha vuelto a emitir una alerta sobre esta evolución de la estafa, subrayando la importancia de no responder a estos mensajes ni proporcionar datos personales a través de enlaces sospechosos. La técnica de 'SMS spoofing' consiste en modificar la información del remitente en los mensajes de texto para que estos parezcan enviados por una fuente confiable, en este caso, la propia DGT. Esto refuerza la percepción de autenticidad del mensaje, aumentando las probabilidades de que las víctimas proporcionen la información solicitada.

La urgencia generada por estos mensajes y la amenaza de recargos y demandas judiciales hacen que muchas personas no se detengan a analizar la veracidad del mensaje, lo que incrementa el éxito de la estafa. Al hacer clic en el enlace proporcionado, los usuarios son redirigidos a sitios web fraudulentos diseñados para parecer legítimos, donde se les solicita información crítica que los estafadores utilizan para robar identidades y dinero.

Este tipo de estafas, aunque no son nuevas, han adquirido un mayor grado de sofisticación con la incorporación del 'SMS spoofing'. La DGT aconseja a los ciudadanos mantenerse alerta y verificar siempre la autenticidad de los mensajes recibidos antes de tomar cualquier acción. Recomienda, además, no hacer clic en enlaces de dudosa procedencia y contactar directamente con las autoridades en caso de dudas sobre la autenticidad de una multa o cualquier otra comunicación recibida.

En resumen, la evolución de las estafas de smishing que suplantan a la DGT representa un riesgo considerable para los ciudadanos, que deben estar informados y precavidos para no caer en estas trampas. La manipulación del ID del remitente, que hace que los mensajes parezcan más reales, es una táctica poderosa que requiere una mayor conciencia y medidas de seguridad por parte de los usuarios para proteger sus datos personales y financieros.

VULNERABILIDAD DE EXPOSICIÓN DE INFORMACIÓN EN EL PLUGIN MRW

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Vulnerabilidad	CVE-2024-6506	MRW	Alta

La seguridad de la información es una preocupación crítica en el mundo digital actual. Uno de los componentes esenciales para mantener la seguridad es garantizar que los plugins utilizados en aplicaciones y sitios web no presenten vulnerabilidades. Recientemente, se ha identificado una vulnerabilidad de exposición de información en el plugin MRW, que es una herramienta utilizada para la gestión de envíos y logística. Esta vulnerabilidad plantea serias preocupaciones para los desarrolladores y usuarios de este plugin.

La vulnerabilidad de exposición de información en el plugin MRW se refiere a la capacidad de un atacante para acceder a datos sensibles que no deberían estar disponibles públicamente. Esta vulnerabilidad puede surgir debido a varios factores, como configuraciones incorrectas, errores en el código, o falta de cifrado adecuado. En el caso del plugin MRW, la vulnerabilidad se ha asociado a la exposición de datos de clientes y detalles de envíos, lo que puede incluir nombres, direcciones, números de teléfono y estados de entrega.

El impacto de esta vulnerabilidad puede ser significativo. La exposición de información sensible puede llevar a varios problemas, tales como:

- Robo de Identidad: Los datos expuestos pueden ser utilizados por delincuentes para suplantar la identidad de los clientes, lo que puede resultar en fraudes financieros y otras actividades delictivas.
- Daño a la Reputación: Las empresas que utilizan el plugin MRW pueden sufrir daños a su reputación si se descubre que no han protegido adecuadamente la información de sus clientes. Esto puede llevar a una pérdida de confianza por parte de los clientes y, en última instancia, a la pérdida de negocio.
- Problemas Legales: Dependiendo de la jurisdicción, las empresas pueden enfrentar sanciones legales y multas por no proteger adecuadamente la información de los clientes, especialmente en regiones con regulaciones estrictas de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa.

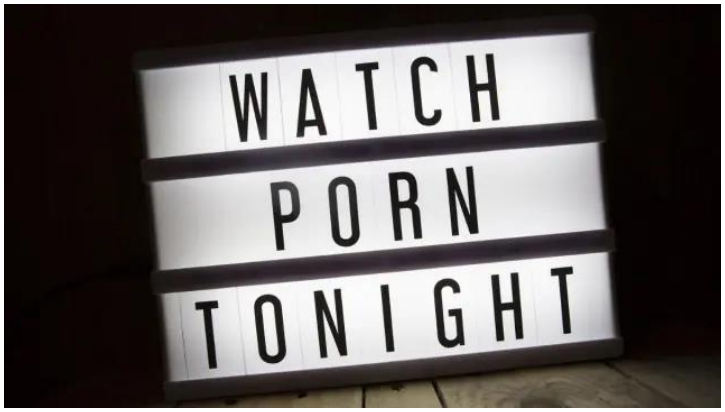
Para mitigar esta vulnerabilidad, se recomienda a los desarrolladores y administradores de sistemas tomar varias acciones:

- Actualizar el Plugin: Verificar si hay una actualización disponible para el plugin MRW que solucione la vulnerabilidad. Los desarrolladores del plugin suelen lanzar parches para corregir problemas de seguridad.
- Revisar Configuraciones: Asegurarse de que las configuraciones del plugin sean las correctas, limitando el acceso a la información sensible solo a usuarios autorizados.
- Implementar Cifrado: Asegurar que los datos sensibles estén cifrados tanto en tránsito como en reposo para protegerlos de accesos no autorizados.
- Realizar Pruebas de Seguridad: Llevar a cabo auditorías de seguridad regulares y pruebas de penetración para identificar y corregir vulnerabilidades potenciales.

La vulnerabilidad de exposición de información en el plugin MRW es un recordatorio crucial de la importancia de mantener una seguridad robusta en todas las capas de las aplicaciones web. Las empresas deben estar siempre alerta y proactivas en la gestión de la seguridad de sus sistemas, adoptando las mejores prácticas y respondiendo rápidamente a las amenazas. La implementación de medidas de seguridad adecuadas no solo protege la información sensible de los clientes, sino que también salvaguarda la reputación y la continuidad del negocio en un entorno digital cada vez más desafiante

TODOS LOS POSIBLES CIBERRIESGOS DE LA APP PARA VER PORNO EN ESPAÑA: DESDE ROBO DE DATOS HASTA BRECHAS DE SEGURIDAD

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Correo malicioso	Usuarios	Media



Las aplicaciones de contenido para adultos en España están en el centro de una creciente preocupación por los riesgos de ciberseguridad, especialmente el robo de datos personales y la sextorsión. Las autoridades y expertos en ciberseguridad advierten que el uso de estas aplicaciones puede exponer a los usuarios a múltiples amenazas, debido a las vulnerabilidades en la protección de datos y la privacidad.

Una de las principales preocupaciones es el almacenamiento y procesamiento seguro de los datos personales de los usuarios, incluyendo nombres, direcciones y números de identificación. Estas aplicaciones, si no se gestionan correctamente, pueden ser susceptibles a ciberataques que resulten en la filtración de información sensible. Esta información puede ser utilizada para marketing no autorizado, venta de datos a terceros, o peor aún, para extorsionar a los usuarios mediante la amenaza de divulgar su consumo de contenido pornográfico.

La sextorsión se ha identificado como una de las amenazas más graves en este contexto. Los ciberdelincuentes pueden acceder a la información personal y utilizarla para chantajear a los usuarios, exigiendo dinero a cambio de no publicar detalles comprometidos sobre su actividad en estas plataformas. Esta práctica se ha vuelto alarmantemente común, afectando a un número significativo de personas, quienes muchas veces se ven obligadas a ceder ante las demandas por temor al escándalo y la vergüenza pública.

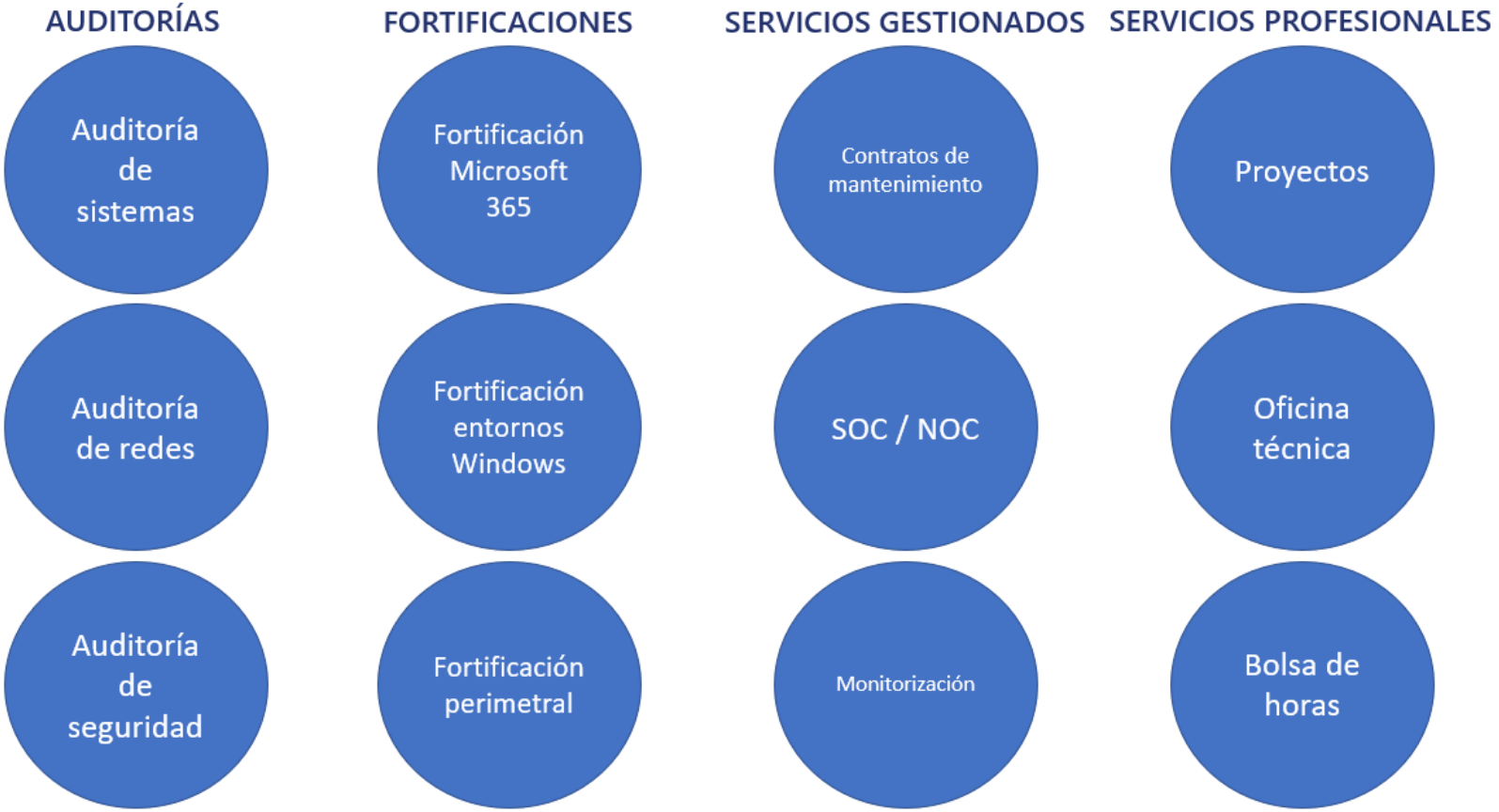
Además, los riesgos no se limitan a los adultos. Existe una creciente preocupación por el acceso de menores a estos sitios. Los delincuentes pueden utilizar identidades robadas de adultos para permitir que los menores accedan a contenido inapropiado. Este acceso no autorizado puede derivar en un mercado negro de credenciales, agravando aún más el problema y exponiendo a los menores a peligros significativos.

La seguridad de estas aplicaciones requiere una gestión rigurosa que incluya pruebas de penetración y auditorías periódicas para identificar y corregir vulnerabilidades. Sin embargo, el mero hecho de que los datos personales puedan ser manejados por personal autorizado ya representa un riesgo inherente, pues una brecha de seguridad podría tener consecuencias devastadoras para la privacidad de los usuarios.

Para mitigar estos riesgos, es crucial que los usuarios sean conscientes de las medidas de seguridad básicas. Esto incluye utilizar contraseñas fuertes y únicas, habilitar la autenticación de dos factores, y estar atentos a cualquier actividad sospechosa en sus cuentas. Además, es fundamental que las plataformas implementen tecnologías avanzadas de encriptación y políticas estrictas de manejo de datos para proteger a sus usuarios de posibles amenazas .

En resumen, mientras las aplicaciones de contenido para adultos pueden ofrecer un espacio para la exploración de la sexualidad, también presentan riesgos significativos para la privacidad y la seguridad de los usuarios. Es vital que tanto los desarrolladores como los usuarios tomen medidas proactivas para protegerse de las crecientes amenazas en el ciberespacio.

> SERVICIOS VERNE PARA PYMES



¿TE GUSTARÍA AMPLIAR INFORMACIÓN O RECIBIR ASESORAMIENTO DE UN ESPECIALISTA?

www.vernegroup.com

CONTACTA