Boletín de Ciberseguridad N°77

Fecha de publicación: 25/03/2024

Mes de Marzo

11/03/2024 – 25/03/2024

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

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 marzo se destacan 6 noticias de relevancia, siendo estas sobre vulnerabilidades tecnológicas.

Aquellas noticias a tener especial recaudo son las siguientes:

Phishing a través de sitios de publicación de documentos

Hackers explotan sitios populares de publicación de documentos para ataques de phishing.

El malware AndroxGh0st apunta a robar credenciales en la nube

El malware AndroxGh0st apunta a aplicaciones de Laravel para robar credenciales de la nube.

Nuevo ataque 'Loop DoS' afecta a cientos de miles de sistemas

Se ha descubierto que un novedoso vector de ataque de denegación de servicio (DoS) se dirige a protocolos de capa de aplicación basados en el Protocolo de datagramas de usuario (UDP), poniendo en riesgo a cientos de miles de hosts.

Vulnerabilidad Crítica

Npm: 800 paquetes npm con discrepancias explotables

CRÍTICO

Descripción

Una nueva investigación ha descubierto más de 800 paquetes en el registro npm que tienen discrepancias con sus entradas de registro, de los cuales 18 explotan una técnica llamada confusión manifiesta.

Estado

Los hallazgos provienen de investigadores de seguridad independientes, quienes informaron que el problema podría ser aprovechado por actores de amenazas para engañar a los desarrolladores para que ejecuten código malicioso.

"Es una amenaza real, ya que los desarrolladores pueden ser engañados para que descarguen paquetes que parecen inocentes, pero cuyas dependencias ocultas son en realidad maliciosas", informaron.

La confusión manifiesta se documentó por primera vez en julio de 2023, cuando el investigador de seguridad Darcy Clarke descubrió que las discrepancias en los metadatos del manifiesto y del paquete podrían utilizarse como arma para organizar ataques a la cadena de suministro de software.

El problema surge del hecho de que el registro npm no valida si el archivo de manifiesto contenido en el tarball (paquete.json) coincide con los datos del manifiesto proporcionados al servidor npm durante el proceso de publicación a través de una solicitud HTTP PUT al punto final del URI del paquete.

Como resultado, un actor de amenazas podría aprovechar esta falta de verificación cruzada para proporcionar un manifiesto diferente que contenga dependencias ocultas que se procese durante la instalación del paquete para instalar sigilosamente dependencias maliciosas en el sistema del desarrollador.

El manifiesto visible o 'falso' puede engañar a los desarrolladores e incluso auditar herramientas que dependen de los datos disponibles en la base de datos de registro npm. En realidad, el instalador toma el archivo package.json del tarball, que puede ser diferente del visible proporcionado en la solicitud HTTP PUT.

NPM dijo que identificó más de 800 paquetes en los que había una discrepancia entre el manifiesto en el registro npm y el archivo package.json dentro del tarball.

Si bien muchas de estas discrepancias son el resultado de diferencias en las especificaciones del protocolo o variaciones en la sección de scripts del archivo del paquete, se dice que 18 de ellas fueron diseñadas para explotar una confusión manifiesta.

Un paquete notable en cuestión es yatai-web-ui, que está diseñado para enviar una solicitud HTTP a un servidor con información sobre la dirección IP de la máquina en la que se instaló el paquete.

Los hallazgos muestran que los actores de amenazas nunca han utilizado el vector de ataque para realizar ataques de envenenamiento. Dicho esto, es fundamental que los desarrolladores tomen medidas para garantizar que los paquetes estén libres de comportamientos sospechosos.

"Dado que npm no resolvió este problema, confiar en los paquetes sólo por su apariencia en el sitio web de npm puede ser arriesgado", comentaron los investigadores.

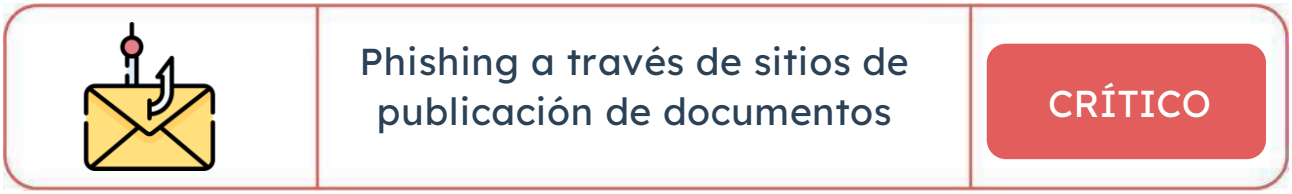
"Las organizaciones deben introducir procedimientos que verifiquen que todos los paquetes que ingresan a la organización o que utilizan sus equipos de desarrollo son seguros y confiables. Específicamente en el caso de confusión manifiesta, se requiere que cada paquete se analice para ver si hay algún paquete oculto."

Remediación / Referencias

Por mayor información acceder a:

https://docs.npmjs.com/cli/v10/configuring-npm/package-json

https://thehackernews.com/2024/03/over-800-npm-packages-found-with.html



Descripción

Hackers explotan sitios populares de publicación de documentos para ataques de phishing

Estado

Los actores de amenazas están aprovechando los sitios de publicación de documentos digitales (DDP) alojados en plataformas como FlipSnack, Issuu, Marq, Publuu, RelayTo y Simplebooklet para llevar a cabo phishing, recolección de credenciales y robo de tokens de sesión, lo que subraya una vez más cómo los actores de amenazas están reutilizando servicios legítimos con fines maliciosos.

Alojar señuelos de phishing en sitios DDP aumenta la probabilidad de un ataque de phishing exitoso, ya que estos sitios a menudo tienen una reputación favorable, es poco probable que aparezcan en las listas de bloqueo de filtros web y pueden infundir una falsa sensación de seguridad en los usuarios que los reconocen como familiares o legítimo.

Si bien se han utilizado servicios populares basados en la nube como Google Drive, OneDrive, Dropbox, SharePoint, DocuSign y Oneflow para alojar documentos de phishing en el pasado, el último desarrollo marca una escalada diseñada para evadir los controles de seguridad del correo electrónico.

Los servicios DDP permiten a los usuarios cargar y compartir archivos PDF en un formato de libro interactivo basado en navegador, agregando animaciones de cambio de página y otros efectos esqueuomórficos a cualquier catálogo, folleto o revista.

Se ha descubierto que los actores de amenazas abusan del nivel gratuito o del período de prueba sin costo que ofrecen estos servicios para crear múltiples cuentas y publicar documentos maliciosos.

Además de explotar la reputación favorable de su dominio, los atacantes aprovechan el hecho de que los sitios DDP facilitan el alojamiento de archivos transitorios, lo que permite que el contenido publicado deje de estar disponible automáticamente después de una fecha y hora de vencimiento predefinidas.

Es más, las funciones de productividad integradas en sitios DDP como Publuu podrían actuar como elemento disuasivo, impidiendo la extracción y detección de enlaces maliciosos en mensajes de phishing.

En los incidentes analizados por investigadores, los sitios DDP se integran en la cadena de ataque en la etapa secundaria o intermedia, generalmente incorporando un enlace a un documento alojado en un sitio DDP legítimo en un correo electrónico de phishing.

El documento alojado en DDP sirve como puerta de entrada a un sitio externo controlado por el adversario, ya sea directamente haciendo clic en un enlace incluido en el archivo señuelo o mediante una serie de redireccionamientos que también requieren resolver CAPTCHA para frustrar los esfuerzos de análisis automatizados.

La página de inicio final es un sitio falso que imita la página de inicio de sesión de Microsoft 365, lo que permite a los atacantes robar credenciales o tokens de sesión.

“Los sitios DDP podrían representar un punto ciego para los defensores, porque no son familiares para los usuarios capacitados y es poco probable que sean marcados por controles de filtrado de contenido web y correo electrónico”, informaron expertos.

"Los sitios DDP crean ventajas para los actores de amenazas que buscan frustrar las protecciones de phishing contemporáneas. Los actores de amenazas pueden abusar de las mismas características y beneficios que atraen a usuarios legítimos a estos sitios para aumentar la eficacia de un ataque de phishing".

Remediación / Referencias

Por mayor información acceder a:

https://blog.talosintelligence.com/threat-actors-leveraging-document-publishing-sites/

https://thehackernews.com/2024/03/hackers-exploiting-popular-document.html

StrelaStealer	Phishing de StrelaStealer afecta a más de 100 organizaciones en la UE y USA	CRÍTICO

Descripción

Investigadores de ciberseguridad han detectado una nueva ola de ataques de phishing que tienen como objetivo ofrecer un ladrón de información en constante evolución conocido como StrelaStealer.

Estado

Las campañas impactan a más de 100 organizaciones en la UE. y los EE. UU.

Estas campañas vienen en forma de correos electrónicos no deseados con archivos adjuntos que eventualmente lanzan la carga útil DLL de StrelaStealer.

En un intento de evadir la detección, los atacantes cambian el formato del archivo adjunto inicial del correo electrónico de una campaña a la siguiente, para evitar la detección a partir de la firma o los patrones generados previamente.

StrelaStealer, divulgado por primera vez en noviembre de 2022, está equipado para desviar datos de inicio de sesión de correo electrónico de clientes de correo electrónico conocidos y exfiltrarlos a un servidor controlado por un atacante.

Desde entonces, se detectaron dos campañas a gran escala relacionadas con el malware en noviembre de 2023 y enero de 2024 dirigidas a los sectores de alta tecnología, finanzas, profesional y legal, manufactura, gobierno, energía, seguros y construcción en la UE. y los EE.UU.

Estos ataques también apuntan a ofrecer una nueva variante del ladrón que incluye mejores técnicas de ofuscación y anti-análisis, mientras se propaga a través de correos electrónicos con temas de facturas que contienen archivos adjuntos ZIP, lo que marca un cambio respecto de los archivos ISO.

Dentro de los archivos ZIP hay un archivo JavaScript que coloca un archivo por lotes, que, a su vez, inicia la carga útil DLL ladrón usando rundll32.exe, un componente legítimo de Windows responsable de ejecutar bibliotecas de enlaces dinámicos de 32 bits.

El malware ladrón también se basa en una serie de trucos de ofuscación para dificultar el análisis en entornos aislados.

"Con cada nueva ola de campañas de correo electrónico, los actores de amenazas actualizan tanto el archivo adjunto del correo electrónico, que inicia la cadena de infección, como la carga útil de la DLL", dijeron los investigadores.

La divulgación se produce cuando Symantec, propiedad de Broadcom, reveló que instaladores falsos para aplicaciones conocidas o software descifrado alojado en GitHub,

Mega o Dropbox están sirviendo como conducto para un malware ladrón conocido como Stealc.

También se han observado campañas de phishing que entregan Revenge RAT y Remcos RAT (también conocido como Rescoms), y este último se entrega mediante un cifrador como servicio (CaaS) llamado AceCryptor, según ESET.

Durante la segunda mitad de [2023], Rescoms se convirtió en la familia de malware más frecuente empaquetada por AceCryptor. Más de la mitad de estos intentos ocurrieron en Polonia, seguida de Serbia, España, Bulgaria y Eslovaquia.

Otro malware comercial destacado incluido en AceCryptor en el segundo semestre de 2023 incluye SmokeLoader, STOP ransomware, RanumBot, Vidar, RedLine, Tofsee, Fareit, Pitou y Stealc. Vale la pena señalar que muchas de estas cepas de malware también se han difundido a través de PrivateLoader.

Se ha descubierto que otra estafa de ingeniería social observada por Secureworks se dirige a personas que buscan información sobre personas fallecidas recientemente en motores de búsqueda con obituarios falsos alojados en sitios web falsos, lo que dirige el tráfico a los sitios a través del envenenamiento por optimización de motores de búsqueda (SEO) para, en última instancia, impulsar el software publicitario. y otros programas no deseados.

"Los visitantes de estos sitios son redirigidos a sitios web de citas electrónicas o entretenimiento para adultos o se les presentan inmediatamente mensajes CAPTCHA que instalan notificaciones web push o anuncios emergentes cuando se hace clic", dijo la compañía.

"Las notificaciones muestran advertencias falsas de alerta de virus de aplicaciones antivirus conocidas como McAfee y Windows Defender, y persisten en el navegador incluso si la víctima hace clic en uno de los botones".

"Los botones enlazan a páginas de inicio legítimas para programas de software antivirus basados en suscripción, y una identificación de afiliado incrustada en el hipervínculo recompensa a los actores de amenazas por nuevas suscripciones o renovaciones".

Si bien la empresa de falsificación actualmente se limita a llenar las arcas de los estafadores a través de programas afiliados para software antivirus, las cadenas de ataque podrían reutilizarse fácilmente para generar ladrones de información y otros programas maliciosos, convirtiéndolos en una amenaza más potente.

El desarrollo también sigue al descubrimiento de un nuevo grupo de actividades rastreado como Fluffy Wolf que aprovecha los correos electrónicos de phishing que contienen un archivo adjunto ejecutable para entregar un cóctel de amenazas, como MetaStealer, Warzone RAT, XMRig miner y una herramienta legítima de escritorio remoto llamada Remote Utilities.

La campaña es una señal de que incluso los actores de amenazas no capacitados pueden aprovechar los esquemas de malware como servicio (MaaS) para llevar a cabo ataques exitosos a escala y saquear información confidencial, que luego puede monetizarse aún más para obtener ganancias.

"Aunque son mediocres en términos de habilidades técnicas, estos actores de amenazas logran sus objetivos utilizando sólo dos conjuntos de herramientas: servicios legítimos de acceso remoto y malware económico", señalaron expertos.

Remediación / Referencias

Por mayor información acceder a:

https://unit42.paloaltonetworks.com/strelastealer-campaign/

https://thehackernews.com/2024/03/new-strelastealer-phishing-attacks-hit.html

El malware AndroxGh0st apunta a robar credenciales en la nube

CRÍTICO

Descripción

El malware AndroxGh0st apunta a aplicaciones de Laravel para robar credenciales de la nube.

Estado

Los investigadores de ciberseguridad han arrojado luz sobre una herramienta denominada AndroxGh0st que se utiliza para apuntar a aplicaciones Laravel y robar datos confidenciales.

Funciona escaneando y extrayendo información importante de los archivos .env, revelando detalles de inicio de sesión vinculados a AWS y Twilio.

Clasificado como un cracker SMTP, explota SMTP utilizando varias estrategias, como explotación de credenciales, implementación de shell web y escaneo de vulnerabilidades.

AndroxGh0st se ha detectado en estado salvaje desde al menos 2022, y los actores de amenazas lo aprovechan para acceder a archivos del entorno Laravel y robar credenciales para varias aplicaciones basadas en la nube como Amazon Web Services (AWS), SendGrid y Twilio.

Se sabe que las cadenas de ataques que involucran el malware Python explotan fallas de seguridad conocidas en Apache HTTP Server, Laravel Framework y PHPUnit para obtener acceso inicial y escalar privilegios y persistencia.

A principios de enero, las agencias de inteligencia y ciberseguridad de EE. UU. advirtieron sobre atacantes que implementaban el malware AndroxGh0st para crear una botnet para "identificar y explotar víctimas en redes objetivo".

Androxgh0st ingresa por primera vez a través de una debilidad en Apache, lo que le permite acceder a sistemas vulnerables.

Después de esto, explota vulnerabilidades adicionales para ejecutar código y establecer un control persistente, esencialmente asumiendo el control de los sistemas objetivo.

Androxgh0st está diseñado para filtrar datos confidenciales de diversas fuentes, incluidos archivos .env, bases de datos y credenciales de la nube. Esto permite a los actores de amenazas entregar cargas útiles adicionales a los sistemas comprometidos.

Investigadores han observado un aumento en la actividad de explotación por lo que es esencial que los usuarios actúen rápidamente para actualizar sus instancias a la última versión.

La mayoría de los intentos de ataque dirigidos a su infraestructura de honeypot se originaron en EE. UU., Reino Unido, China, Países Bajos, Alemania, Bulgaria, Kuwait, Rusia, Estonia e India.

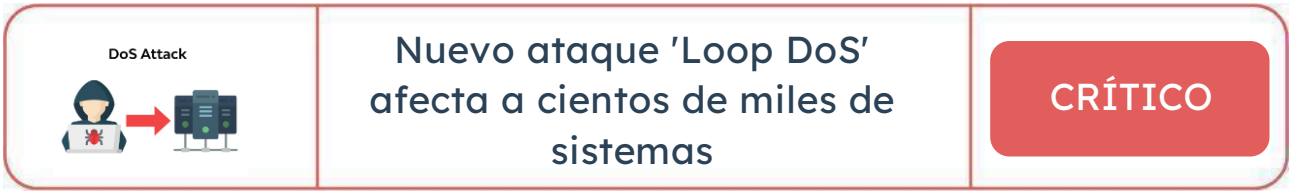
Remediación / Referencias

Por mayor información acceder a:

https://www.cisa.gov/news-events/alerts/2024/01/16/cisa-and-fbi-release-known-iocs-associated-androxgh0st-malware

https://blogs.juniper.net/en-us/security/shielding-networks-against-androxgh0st

https://thehackernews.com/2024/03/androxgh0st-malware-targets-laravel.html



Descripción

Se ha descubierto que un novedoso vector de ataque de denegación de servicio (DoS) se dirige a protocolos de capa de aplicación basados en el Protocolo de datagramas de usuario (UDP), poniendo en riesgo a cientos de miles de hosts.

Estado

Llamados ataques Loop DoS, el enfoque empareja "servidores de estos protocolos de tal manera que se comunican entre sí indefinidamente", dijeron investigadores.

UDP, por diseño, es un protocolo sin conexión que no valida las direcciones IP de origen, lo que lo hace susceptible a la suplantación de IP.

Por lo tanto, cuando los atacantes falsifican varios paquetes UDP para incluir la dirección IP de la víctima, el servidor de destino responde a la víctima (a diferencia del actor de la amenaza), creando un ataque de denegación de servicio (DoS) reflejado.

El último estudio encontró que ciertas implementaciones del protocolo UDP, como DNS, NTP, TFTP, Active Users, Daytime, Echo, Chargen, QOTD y Time, pueden usarse como armas para crear un bucle de ataque que se perpetúa a sí mismo.

"Empareja dos servicios de red de tal manera que siguen respondiendo indefinidamente a los mensajes del otro", dijeron los investigadores. "Al hacerlo, crean grandes volúmenes de tráfico que resultan en una denegación de servicio para los sistemas o redes involucradas. Una vez que se inyecta un disparador y el bucle se pone en movimiento, ni siquiera los atacantes pueden detener el ataque".

En pocas palabras, dados dos servidores de aplicaciones que ejecutan una versión vulnerable del protocolo, un actor de amenazas puede iniciar la comunicación con el primer servidor falsificando la dirección del segundo servidor, lo que hace que el primer servidor responda a la víctima (es decir, el segundo servidor). con un mensaje de error.

La víctima, a su vez, también mostrará un comportamiento similar, enviando otro mensaje de error al primer servidor, agotando efectivamente los recursos de cada uno y haciendo que cualquiera de los servicios no responda.

"Si un error como entrada crea un error como salida, y un segundo sistema se comporta igual, estos dos sistemas seguirán enviando mensajes de error de un lado a otro indefinidamente", explicaron los expertos.

Asimismo, estimaron que se puede abusar de 300.000 hosts y sus redes para llevar a cabo ataques Loop DoS.

Si bien actualmente no hay evidencia de que el ataque haya sido utilizado como arma en la naturaleza, los investigadores advirtieron que la explotación es trivial y que múltiples productos de Broadcom, Cisco, Honeywell, Microsoft, MikroTik y Zyxel se ven afectados.

"Los atacantes necesitan un único host con capacidad de suplantación de identidad para activar los bucles", señalaron los investigadores. "Como tal, es importante mantener iniciativas para filtrar el tráfico falsificado, como BCP38".

Remediación / Referencias

Por mayor información acceder a:

https://cispa.de/en/loop-dos

https://thehackernews.com/2024/03/new-loop-dos-attack-impacts-hundreds-of.html

Campaña masiva infecta más de 39.000 sitios de WordPress

CRÍTICO

Descripción

Una campaña masiva de malware denominada Sign1 ha comprometido más de 39.000 sitios de WordPress en los últimos seis meses, utilizando inyecciones maliciosas de JavaScript para redirigir a los usuarios a sitios fraudulentos.

Estado

Se estima que la variante más reciente del malware ha infectado no menos de 2.500 sitios sólo en los últimos dos meses.

Los ataques implican inyectar JavaScript fraudulento en widgets y complementos HTML legítimos que permiten insertar JavaScript arbitrario y otros códigos, brindando a los atacantes la oportunidad de agregar su código malicioso.

El código JavaScript codificado con XOR se decodifica posteriormente y se utiliza para ejecutar un archivo JavaScript alojado en un servidor remoto, lo que en última instancia facilita las redirecciones a un sistema de distribución de tráfico (TDS) operado por VexTrio, pero solo si se cumplen ciertos criterios.

Es más, el malware utiliza aleatorización basada en el tiempo para recuperar URL dinámicas que cambian cada 10 minutos para sortear las listas de bloqueo. Estos dominios se registran unos días antes de su uso en ataques.

"Una de las cosas más notables de este código es que busca específicamente ver si el visitante proviene de algún sitio web importante como Google, Facebook, Yahoo, Instagram, etc.", dijeron investigadores de seguridad. "Si el referente no coincide con estos sitios principales, entonces el malware no se ejecutará".

Luego, los visitantes del sitio son dirigidos a otros sitios fraudulentos ejecutando otro JavaScript desde el mismo servidor.

La campaña Sign1, detectada por primera vez en la segunda mitad de 2023, ha sido testigo de varias iteraciones, y los atacantes aprovecharon hasta 15 dominios diferentes desde el 31 de julio de 2023.

Se sospecha que los sitios de WordPress han sido tomados mediante un ataque de fuerza bruta, aunque los adversarios también podrían aprovechar las fallas de seguridad en complementos y temas para obtener acceso.

"Muchas de las inyecciones se encuentran dentro de los widgets HTML personalizados de WordPress que los atacantes agregan a los sitios web comprometidos", informaron los

expertos. "Muy a menudo, los atacantes instalan un complemento CSS y JS personalizado simple y legítimo e inyectan el código malicioso utilizando este complemento".

“Este enfoque de no colocar ningún código malicioso en los archivos del servidor permite que el malware permanezca sin ser detectado durante largos períodos de tiempo”

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2024/03/massive-sign1-campaign-infects-39000.html

Conclusiones

Es de suma importancia mantenernos alerta y vigilantes ante la creciente ola de malware que ha caracterizado el inicio del año 2024. La sofisticación de los ataques cibernéticos no tiene precedentes, y es crucial que estemos al tanto de las últimas técnicas empleadas por los ciberdelincuentes, tales como el phishing, vishing, deepfake, entre otros.

La amenaza digital evoluciona constantemente, y nuestra seguridad en línea depende en gran medida de nuestra capacidad para adaptarnos y protegernos contra estas nuevas formas de engaño. Mantenernos informados sobre las últimas tendencias en seguridad cibernética y adoptar medidas proactivas para proteger nuestros datos y nuestra privacidad es fundamental en este entorno digital cada vez más complejo y peligroso.

Recordemos que la seguridad informática es responsabilidad de todos. Mantengamos nuestras defensas actualizadas, practiquemos una navegación segura en línea y estemos atentos a cualquier señal de actividad sospechosa. Juntos, podemos mitigar los riesgos y hacer de Internet un lugar más seguro para todos.

Desde el equipo de Datasec seguimos protegiendo la seguridad de nuestros clientes, socios y colaboradores.

¡Hasta la próxima!