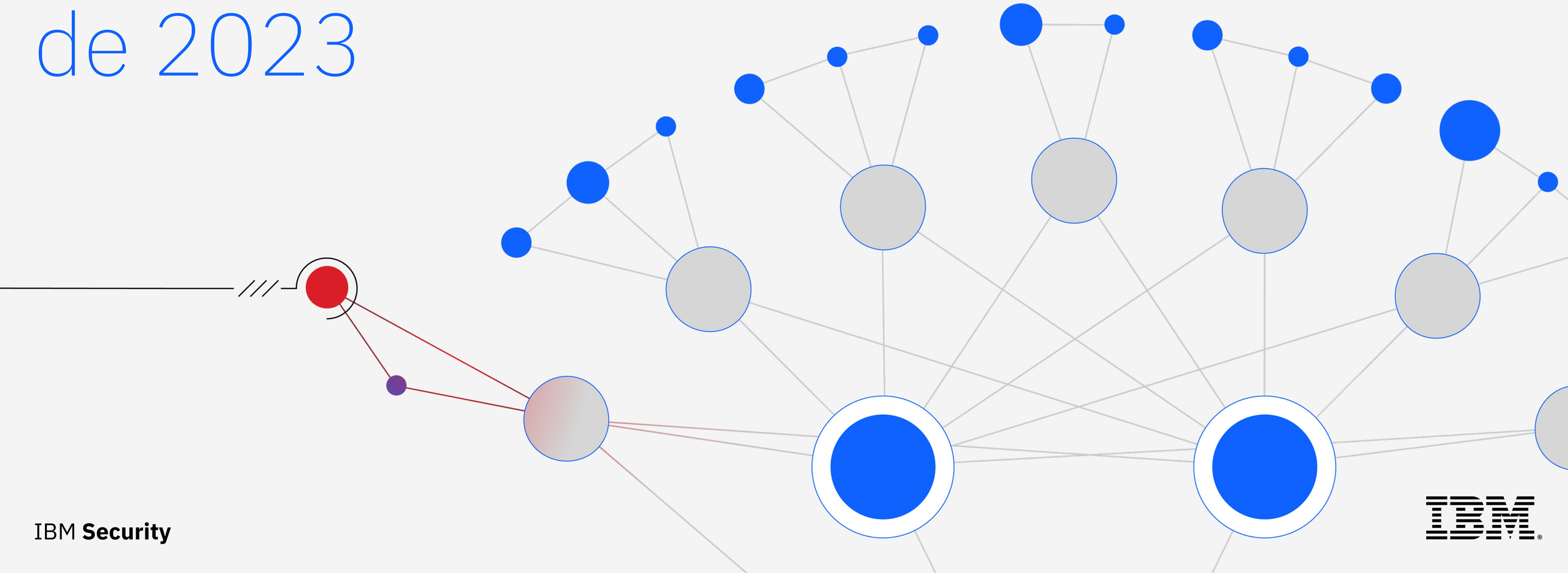
Índice de inteligencia de amenazas de X-Force de 2023

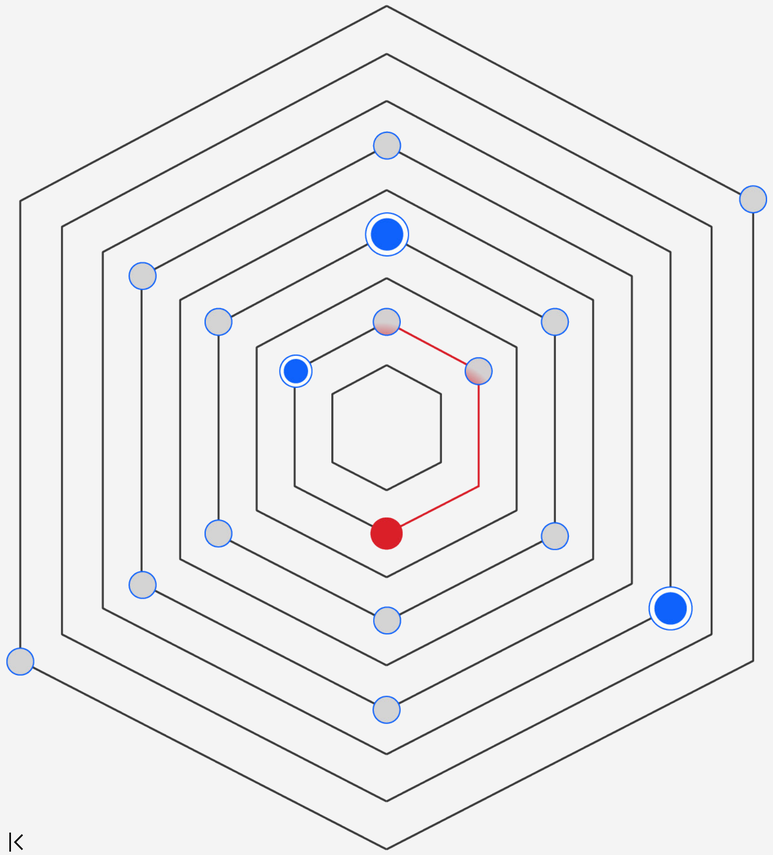


IBM **Security**

Índice

01

Resumen ejecutivo



2022 fue otro año complicado para la ciberseguridad- debido a varios acontecimientos. Entre los más significativos, se destacan los efectos persistentes de la pandemia y el estallido del conflicto militar en Ucrania. Todo eso hizo de 2022 un año de inestabilidad y crisis económicas, geopolíticas y humanitarias, lo que creó el tipo de caos que suele beneficiar a los cibercriminales.

Y así sucedió.

IBM® Security X-Force ha sido testigo de la existencia de agentes de amenazas oportunistas que aprovechan el desorden y lo usan a su favor para infiltrarse en gobiernos y empresas de todo el mundo.

El Índice de inteligencia de amenazas de IBM Security X-Force de 2023, analiza tendencias y patrones de ataque, nuevos y existentes, e incluye miles de millones de puntos de referencia que van desde dispositivos de red y terminales, planes de respuesta a incidentes (IR), bases de datos de vulnerabilidades y brechas (vulnerabilidades de seguridad) y mucho más. Este informe es una recopilación exhaustiva de los datos de investigación compilados entre enero y diciembre de 2022.

Ofrecemos estos resultados como recurso para los clientes de IBM, los investigadores en ciberseguridad, los legisladores, los medios de comunicación y la comunidad más amplia de profesionales y directivos del sector de la seguridad. Con un panorama actual inestable, en el que las amenazas son cada vez más sofisticadas y maliciosas, se requiere un esfuerzo por parte de todos si queremos proteger a las empresas y a los ciudadanos. Hoy, más que nunca, usted necesita contar con información sobre amenazas y seguridad para proteger sus activos críticos y adelantarse a los atacantes.

De esta forma, usted también podrá prosperar.

Cómo cambió nuestro análisis de datos para 2022

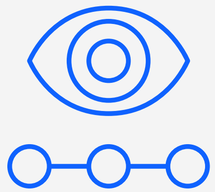
En 2022, modificamos la forma de analizar parte de nuestros datos. Estos cambios nos han permitido ofrecer análisis más exhaustivos y alinearnos más con los marcos estándar del sector. Esto, a su vez, le permite tomar decisiones de seguridad informadas y proteger mejor a su empresa frente a las amenazas.

Cambios en nuestro análisis en 2022:

- **Vectores de acceso inicial:** La adopción del marco MITRE ATT&CK para seguir más de cerca los vectores de acceso inicial permite alinear los resultados de nuestra investigación con el sector de la ciberseguridad en general e identificar tendencias importantes a nivel técnico.
- **Brechas y ataques de día cero:** La extrapolación de nuestra sólida base de datos de vulnerabilidades, la cual incluye casi 30 años de recopilación de datos, ayuda a contextualizar el análisis e identificar la amenaza real que plantean dichas vulnerabilidades. Este proceso también sirve para contextualizar la proporción cada vez menor de brechas que pueden convertirse en armas y de días con cero impacto.
- **Métodos de los agentes de amenazas y su impacto:** Identificar los pasos que siguen los agentes durante un ataque del impacto real de un incidente nos permitió identificar las fases críticas que lo componen. En este proceso también se identificaron las áreas que deben dominar los equipos de respuesta y saber cómo gestionarlas tras un incidente.

02

Aspectos destacados del informe



Principales acciones sobre los objetivos observadas: En casi una cuarta parte de todos los incidentes corregidos en 2022, la implementación de puertas traseras, con un 21 %, fue la principal acción en cuanto a objetivos. En particular, un repunte de Emotet, un malware polivalente, a principios de año contribuyó significativamente al aumento de la actividad de puerta traseras, en comparación con años anteriores.
A pesar de este incremento, el ransomware, que ocupaba el primer puesto desde al menos 2020, constituyó una gran parte de los incidentes, con un 17 %, lo que reforzaba aún más la persistencia de la amenaza que supone este malware.

La extorsión fue el impacto de ataque más común en las organizaciones: Con un 27 %, la extorsión fue el método preferido por los agentes de amenazas. Las víctimas en la manufactura representaron el 30 % de los incidentes que acabaron en extorsión, es decir, los ciberdelincuentes siguieron con la tendencia de aprovecharse de un sector en crisis.

El phishing fue el principal vector de acceso inicial: El phishing, identificado en el 41 % de los incidentes, sigue siendo el vector de infección principal, seguido por la explotación de aplicaciones de cara al público en un 26 % de los casos. Las infecciones por macros maliciosas han perdido popularidad, probablemente debido a la decisión de Microsoft de bloquear las macros de forma predeterminada. Por otro lado, aumentó el uso de archivos ISO y LNK maliciosos como táctica principal para distribuir malware mediante correo no deseado en 2022.

Aumento del accionar de hackers y del malware destructivo: La guerra de Rusia en Ucrania abrió la puerta a lo que muchos en la comunidad de la ciberseguridad esperaban que fuera una muestra de cómo la cibernética facilita la guerra moderna. Aunque es cierto que las peores predicciones sobre el ciberespacio no se han cumplido hasta la fecha de publicación de este informe, sí ha habido un notable resurgimiento de la acción de hackers y del malware destructivo. X-Force también observó cambios sin precedentes en el mundo de la ciberdelincuencia, con un aumento de la cooperación entre grupos de ciberdelincuentes y bandas de Trickbot dirigidas a organizaciones ucranianas.

03

Estadísticas

27 %

Porcentaje de ataques con extorsión

Los agentes de amenazas trataron de extorsionar a las víctimas en más de una cuarta parte de todos los incidentes a los que respondió X-Force en 2022. Las tácticas que utilizan fueron evolucionando en la última década y se espera que sigan haciéndolo aún más y de manera más agresiva.

21 %

Porcentaje de incidentes en los que se implementaron puertas traseras

La implementación de puertas traseras fue el principal objetivo el año pasado; se produjo en más de uno de cada cinco incidentes notificados en todo el mundo. Gracias a la intervención exitosa de los defensores, se logró impedir que los agentes de amenazas lograran otros objetivos que podrían haber incluido el ransomware.

17 %

Ataques de ransomware

Incluso en medio de un año caótico para algunos de los sindicatos de ransomware más prolíficos, el ransomware fue el segundo objetivo más común; el primero fue la instalación de puertas traseras, seguido de las interrupciones en las operaciones de las empresas. La proporción de incidentes de ransomware disminuyó del 21 % en 2021 al 17 % en 2022.

41 %

Porcentaje de incidentes que implican phishing para el acceso inicial
Las operaciones de phishing continuaron siendo la principal vía de infección en 2022, con un 41 % de los incidentes corregidos por X-Force mediante el uso de esta técnica para obtener el acceso inicial.

100 %

Aumento del número de intentos de thread hijacking (apropiación de datos informáticos) al mes
En 2022 hubo el doble de intentos de apropiación de datos informáticos al mes en comparación con los datos de 2021. Los correos electrónicos no deseados que conducen a Emotet, Qakbot e IcedID hacen un uso intensivo de la apropiación de datos informáticos.

52 %

Descenso de las denuncias de kits de phishing que tratan de obtener información de las tarjetas de crédito
Casi todos los kits de phishing analizados en los datos buscaban obtener nombres (98 %) y direcciones de correo electrónico (73 %), seguidos de direcciones particulares (66 %) y contraseñas (58 %). Los agentes de amenazas perdieron interés en obtener información de las tarjetas de crédito, su objetivo en el 61 % de los casos en 2021; los datos muestran que solo fue el objetivo en el 29 % de los kits de phishing en 2022, lo que supone un descenso del 52 %.

62 %

Porcentaje de ataques de phishing que utilizan archivos adjuntos de spear phishing
Los atacantes preferían archivos adjuntos contaminados, implementados por ellos mismos o junto con enlaces o spear phishing vía servicio.

26 %

Proporción de vulnerabilidades de 2022 con brechas conocidas
El 26 % de las vulnerabilidades de 2022 se correspondían con brechas conocidas. Según los datos que X-Force ha rastreado desde principios de la década de 1990, esa proporción fue disminuyendo en los últimos años, lo que demuestra las ventajas de un proceso de gestión de parches bien mantenido.

31 %

Porcentaje de ataques mundiales dirigidos a la región Asia Pacífico
Dicha región conservó el primer puesto como la más atacada en 2022, con el 31 % de todos los incidentes. Esta estadística representa un aumento de cinco puntos porcentuales con respecto a la cuota total de ataques a los que respondió X-Force en la región en 2021.

04

Principales vectores de acceso inicial

En 2022, X-Force pasó de rastrear los vectores de acceso inicial como categorías más amplias, como por ejemplo phishing y credenciales robadas, a las técnicas de acceso inicial enumeradas en el marco MITRE ATT&CK Matrix para Enterprise. Este cambio le permite a X-Force hacer un seguimiento más detallado de las tendencias importantes a nivel técnico. También proporciona datos que pueden usarse y compararse con mayor facilidad, mientras se alinea con los trabajos de estandarización del sector en general.

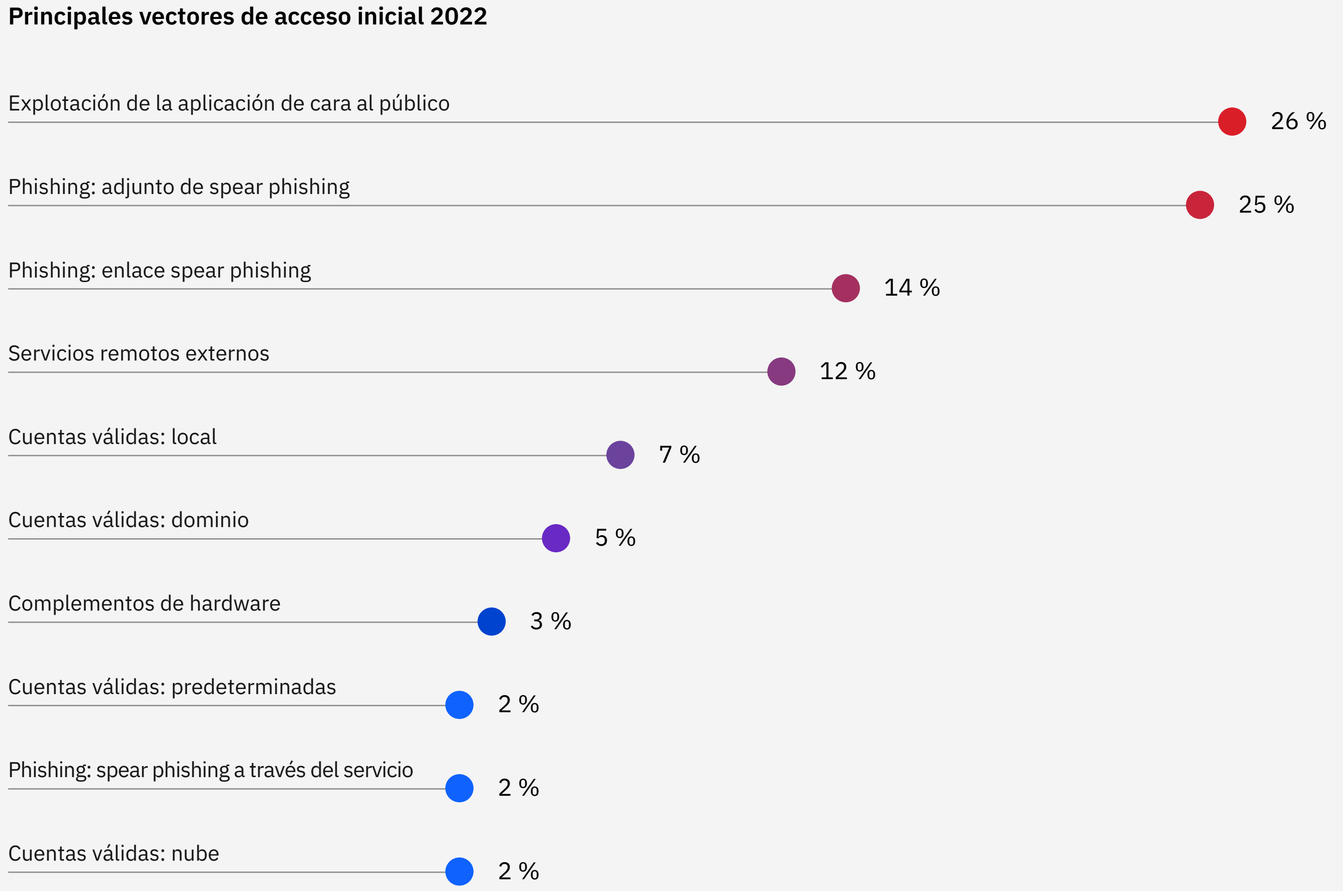


Figura 1: Principales vectores de acceso inicial observados por X-Force en 2022. Fuente: X-Force

Figura 2: Tipos de subtécnicas de phishing como porcentaje del total de casos de phishing observados por X-Force en 2022. Fuente: X-Force

Phishing

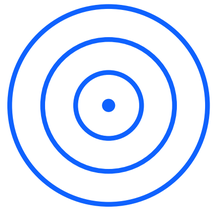
Phishing (T1566), ya sea mediante archivos adjuntos, enlaces o como un servicio, sigue siendo el principal vector de infección, el cual representó el 41 % de todos los incidentes corregidos por X-Force en 2022. Este porcentaje se mantiene estable a partir de 2021, después de haber tenido un aumento del 33 % en 2020. Considerando todos los incidentes de phishing, se utilizaron documentos adjuntos de spear phishing (T1566.001) en el 62 % de los ataques, enlaces de spear phishing (T1566.002) en el 33 % y spear phishing como un servicio (T1566.003) en el 5 %. X-Force también ha observado que, en algunos casos, los agentes de amenazas emplearon archivos adjuntos con phishing como servicio o enlaces.

Los datos de IBM X-Force Red de 2022 enfatizan aún más el valor del phishing y de las credenciales mal gestionadas para los agentes de amenazas. A través de las pruebas de penetración de 2022 para clientes, X-Force Red descubrió que aproximadamente el 54 % de las pruebas revelaron autenticación o manejo inadecuados de las credenciales. El equipo de X-Force Red Adversary Simulation realizaba regularmente spear phishing con códigos QR dirigidos a tokens de autenticación multifactor (MFA). Muchas empresas carecían de visibilidad de las aplicaciones y terminales expuestos a través de portales de gestión de acceso a identidades e inicio de sesión único (SSO), como Okta.

En segundo lugar, la explotación de aplicaciones de cara al público (T1190), definida como atacantes que se aprovechan de una debilidad en un equipo o programa de cara a Internet, se identificó en el 26 % de los incidentes a los que respondió X-Force. Esta cifra se corresponde con lo que los informes anteriores del Índice de inteligencia de amenazas denominaban “explotación de vulnerabilidades” y supone un descenso con respecto al 34 % registrado en 2021.

En tercer lugar, el abuso de cuentas válidas (T1078) se identificó en el 16 % de los incidentes observados. Se trata de casos en los que los atacantes obtuvieron y abusaron de las credenciales de cuentas existentes para conseguir el acceso. Estos incidentes fueron cuentas en la nube (T1078.004) y cuentas predeterminadas (T1078.001) con un 2 % cada una, cuentas de dominio (T1078.002) con un 5 % y, también, cuentas locales (T1078.003) con un 7 %.

La información en las tarjetas de crédito se redujo de forma significativa, pasando de ser el objetivo en el 61 % de los casos en 2021 al 29 % de los kits de phishing en 2022.



Los kits de phishing duran más y se centran en la IPI más que en los datos de las tarjetas de crédito

IBM Security analizó miles de kits de phishing de todo el mundo por segundo año consecutivo e identificó que su desarrollo está operativo durante más tiempo y llega a más usuarios. Los datos indican que la vida útil de los kits de phishing observados se ha más que duplicado año tras año, mientras que la mediana de la implementación del grupo de datos se mantuvo relativamente baja en 3,7 días.

En total, la implementación más corta duró minutos y la más larga, descubierta en 2022, más de tres años. Nuestra investigación descubrió lo siguiente:

- Un tercio de los kits implementados duraron aproximadamente 2,3 días el año pasado, más del doble que el año anterior, cuando la misma proporción no duraba más de un día.
- Aproximadamente la mitad de todos los kits denunciados afectaron a 93 usuarios, mientras que en 2021, cada implementación no superó el promedio de 75 víctimas potenciales.
- El máximo total de víctimas de un ataque de phishing denunciado fue de algo más de 4 000, aunque se trató de un caso atípico.
- Casi todos los kits de phishing analizados que fueron reportados buscaban obtener nombres en un 98 %. Le siguieron las direcciones de correo electrónico con un 73 %, las direcciones particulares con un 66 % y las contraseñas con un 58 %.
- La información en las tarjetas de crédito se redujo de forma significativa, pasando de ser el objetivo en el 61 % de los casos en 2021 al 29 % de los kits de phishing en 2022.
- El menor número de kits de phishing que buscan los datos de las tarjetas de crédito indica que los phishers están dando prioridad a la información personal identificable (IPI), lo que les proporciona opciones más amplias y maliciosas. La IPI puede recopilarse y venderse en la dark web u otros foros o utilizarse para ejecutar nuevas operaciones contra diversos objetivos.

Marcas más suplantadas

Las principales marcas que fueron víctimas de suplantación de la identidad son, en su mayoría, grandes empresas de tecnología. X-Force cree que este cambio con respecto a la lista de 2021, algo más diversa, se debe a la mejora de la capacidad para identificar las marcas elegidas a la hora de configurar un kit para suplantar la identidad, no solo la que tiene como objetivo predeterminado. Muchos kits de phishing son polivalentes y la marca suplantada puede cambiarse alterando un simple parámetro. Por ejemplo, un kit puede suplantar a Gmail de forma predeterminada, pero una actualización de una línea lo convierte en un ataque que suplanta a Microsoft.

Las credenciales robadas para dichos servicios son muy valiosas. Obtener el acceso a las cuentas que usan las víctimas para gestionar la totalidad de su presencia en línea puede dar acceso a otras cuentas. El enfoque de los atacantes en esta forma de acceso inicial se destaca en el 2022 Cloud Threat Landscape Report, el cual descubrió un aumento de más del triple en el 200 % de las cuentas en la nube que se anuncian para la venta en la dark web con respecto a lo observado en 2021.

Marcas más suplantadas año tras año

	2022	2021
1	Microsoft	Microsoft
2	Google	Apple
3	Yahoo	Google
4	Facebook	BMO Harris Bank
5	Outlook	Chase
6	Apple	Amazon
7	Adobe	Dropbox
8	AOL	DHL
9	PayPal	CNN
10	Office365	Hotmail

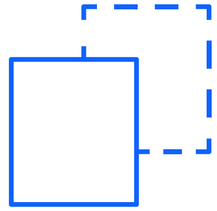
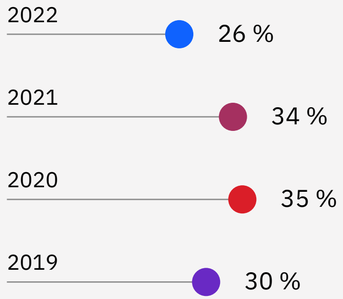


Figura 3: Esta tabla identifica las principales marcas suplantadas en 2021 y 2022, lo que demuestra que los criminales se centran cada vez más en las grandes marcas tecnológicas. Fuente: Datos del kit de phishing de IBM

Porcentaje de incidentes provocados por la explotación de vulnerabilidades en los últimos cuatro años



Vulnerabilidades

La explotación de vulnerabilidades, reflejada para 2022 como explotación de aplicaciones de cara al público (T1190), ocupó el segundo lugar entre los principales vectores de infección y fue uno de los métodos preferidos por los atacantes desde 2019. Las vulnerabilidades se explotaron en el 26 % de los ataques que X-Force corrigió en 2022, el 34 % en 2021, el 35 % en 2020 y el 30 % en 2019.

No todas las vulnerabilidades explotadas por los atacantes terminan convirtiéndose en un ciberincidente. El número de incidentes derivados de la explotación de vulnerabilidades en 2022 disminuyó un 19 % con respecto a 2021, tras experimentar un incremento del 34 % con respecto a 2020. X-Force declaró que esta oscilación fue impulsada por la vulnerabilidad Log4J que se difundió a fines de 2021.

La explotación del acceso es un área clave de investigación que persigue el equipo de X-Force Red Adversary Simulation Services para continuar simulando amenazas avanzadas. El equipo aumentó su atención a la investigación de vulnerabilidades para la explotación de sistemas operativos (SO) y aplicaciones con el fin de ampliar el acceso y llevar a cabo una escalada de privilegios. Este enfoque se debió, en gran medida, a ejercicios anteriores con clientes habituales que han reforzado las vías de ataque tradicionales de Active Directory, así como a la necesidad de buscar nuevas vías de ataque.

Aunque las vulnerabilidades son un vector de acceso inicial habitual, y el sector responde a varias de las principales cada año, no todas las vulnerabilidades son iguales. Es importante que los responsables de la toma de decisiones tengan una visión completa del panorama de las vulnerabilidades y se aseguren de disponer del contexto necesario para comprender la amenaza real que representa para sus redes una vulnerabilidad determinada.

Hace casi 30 años, y antes de la aparición del sistema Common Vulnerabilities and Exposures (CVE), X-Force comenzó a crear una sólida base de datos de vulnerabilidades. Esta base de datos es actualmente una de las más completas del sector de la ciberseguridad. Aunque las vulnerabilidades son un riesgo importante para la seguridad, hay muchas más vulnerabilidades notificadas que brechas conocidas. Además, a pesar de la atención pública sobre los ataques de día cero, el número real de este tipo de ataques conocidos se ve empequeñecido por el número total de vulnerabilidades detectadas.

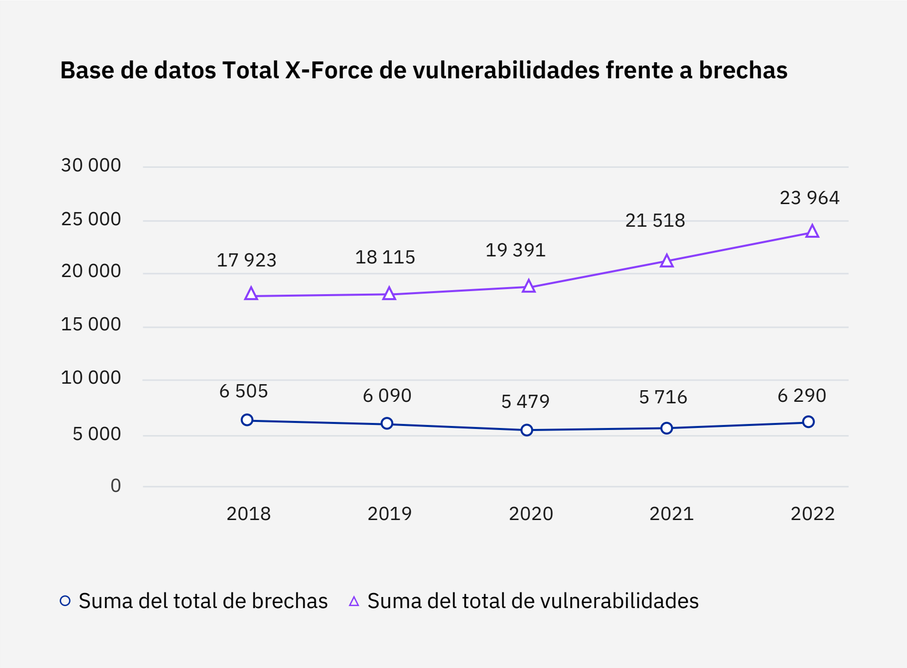


Figura 4: Vista de la base de datos de vulnerabilidades de X-Force que muestra las vulnerabilidades y los ataques de los últimos cinco años. Fuente: X-Force

Cada año se alcanza un nuevo récord de vulnerabilidades. El número total de vulnerabilidades rastreadas en 2022 fue de 23 964, frente a las 21 518 de 2021. La tendencia al aumento interanual de la vulnerabilidad ha persistido durante la última década. Cabe añadir, no obstante, que el análisis de nuestra base de datos de vulnerabilidades mostró que la proporción de brechas conocidas y viables con respecto a las vulnerabilidades reportadas disminuyó en los últimos años: 36 % en 2018, 34 % en 2019, 28 % en 2020, 27 % en 2021 y 26 % en 2022.

Estas cifras pueden cambiar con la exposición de los días cero y los ataques a vulnerabilidades más antiguas, a veces años después de que fueran identificadas, y hay varias razones que podrían explicar este descenso. En primer lugar, el establecimiento de programas formales de recompensas por errores ha incentivado el descubrimiento proactivo de vulnerabilidades en las aplicaciones. Además, existen varias vulnerabilidades conocidas y bien establecidas que ya sirven como medio de explotación del sistema para los atacantes, lo que reduce la necesidad de que configuren nuevas brechas. El descenso se debe, probablemente, a una combinación de múltiples factores, pero no sugiere que la explotación de vulnerabilidades se esté convirtiendo en una amenaza menor.

Mientras que la proporción de ataques de las vulnerabilidades disminuye, en los últimos cinco años ha aumentado la gravedad de aquellos rastreados por X-Force. En 2018, el 58 % de las vulnerabilidades tenían una puntuación media según el sistema CVSS (sistema común de puntuación de vulnerabilidades),

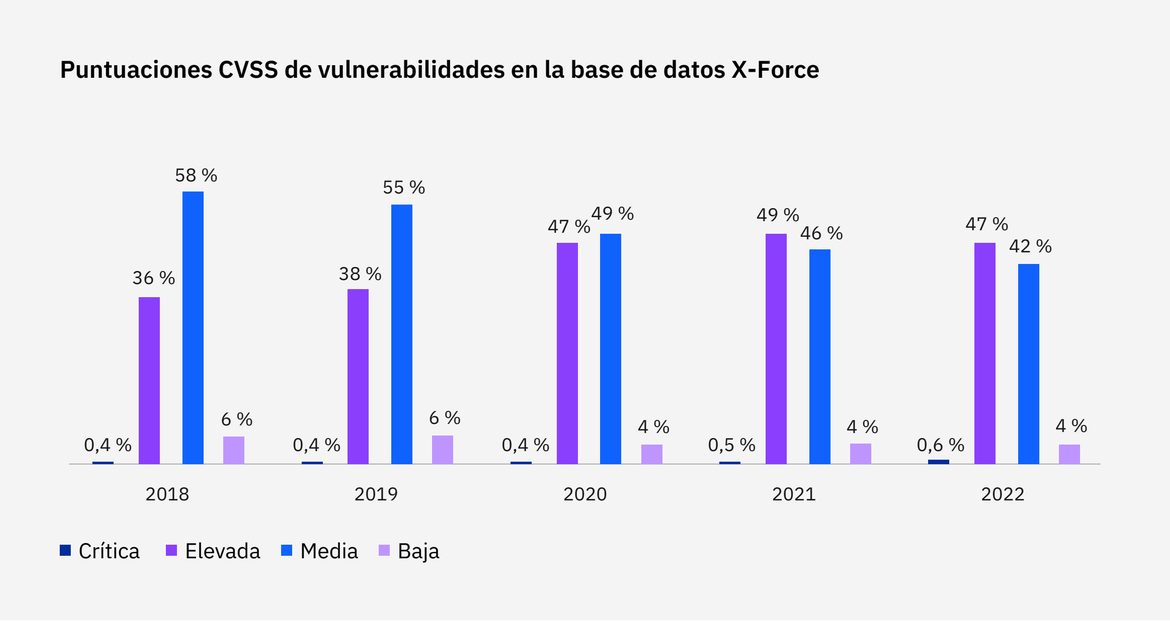


Figura 5: Base de datos de vulnerabilidades X-Force que muestra la gravedad de las vulnerabilidades rastreadas en nuestro sistema. Fuente: X-Force

4,0-6,9 sobre 10, frente a algo menos del 36 % de gravedad elevada, 7,0-9,9. El diferencial entre ambas se invirtió en 2021 y las vulnerabilidades de gravedad elevada representan ahora cinco puntos porcentuales más que las de gravedad media.

Aún así, de todas las vulnerabilidades que X-Force ha rastreado desde 1988, el 38 % de ellas tienen una puntuación elevada, mientras que solo el 1 % alcanza la puntuación crítica de 10. La mitad de las vulnerabilidades rastreadas tienen una clasificación media, mientras que el 11 % restante tiene una clasificación baja, de 3,9 o inferior. Estas puntuaciones por sí solas no guardan correlación con la gravedad real de una CVE, ya que no tienen en cuenta cómo se lleva a cabo el ataque o si realmente ocurrió. Sin embargo, las puntuaciones ayudan a los defensores a comparar vulnerabilidades y a dar prioridad a la rapidez con la que deben abordarlas. El gráfico de la Figura 6 de la página siguiente ayuda a poner en perspectiva la verdadera naturaleza del problema de vulnerabilidad al que se enfrenta el sector de la ciberseguridad.

Vulnerabilidades de la tecnología operativa (OT)

Las vulnerabilidades de los sistemas de control industrial (ICS) descubiertas en 2022 disminuyeron por primera vez en dos años: 457 en 2022 frente a 715 en 2021 y 472 en 2020. La explicación puede encontrarse en los ciclos de vida de los ICS y en cómo se suelen gestionar y parchar. Los atacantes saben que con la demanda de un tiempo de inactividad mínimo, largos ciclos de vida de los equipos y software más antiguo y menos compatible, muchos componentes ICS y redes OT siguen en riesgo de ser víctimas de vulnerabilidades antiguas. La infraestructura suele durar muchos años más que los puestos de trabajo de oficina estándar, lo que prolonga la vida útil de las vulnerabilidades específicas de los ICS más allá de las que pueden explotar las TI.

El problema de la vulnerabilidad

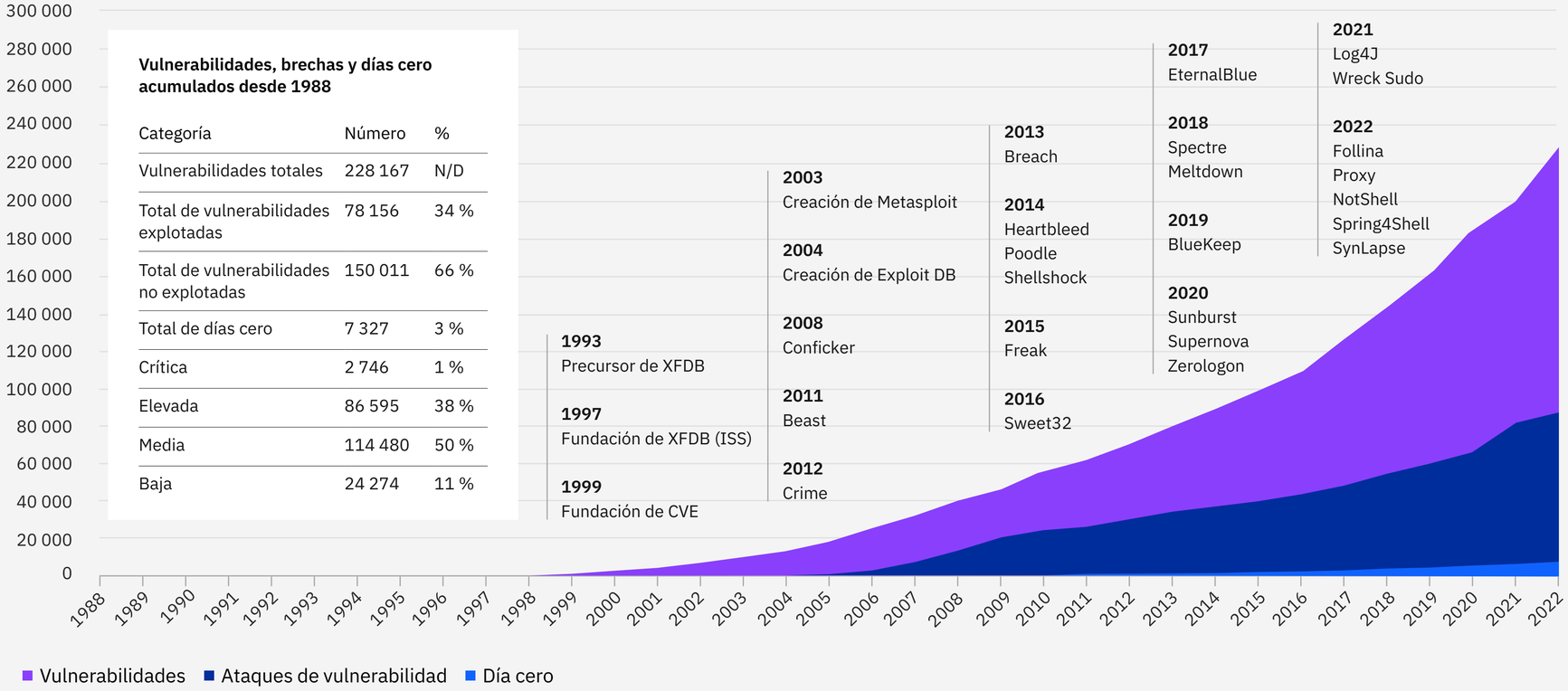


Figura 6: El gráfico muestra el crecimiento de vulnerabilidades, brechas y días cero desde 1988. También se incluye una cronología de los principales acontecimientos relacionados con vulnerabilidades desde 1993. XFDB son las siglas de X-Force Database y Exploit DB son las siglas de Exploit Database. Fuente: X-Force

Principales acciones sobre los objetivos

Anteriormente, el Índice de inteligencia de amenazas de X-Force examinaba la amplia categoría de los principales ataques. Para 2022, X-Force dividió esta clasificación en dos categorías distintas: las acciones específicas que los atacantes llevaron a cabo en las redes de la víctima o sus acciones sobre su objetivo, y el efecto previsto o materializado de esa acción sobre la víctima, o el impacto.

Según los datos de X-Force Incident Response, la implementación de puertas traseras fue la acción más común en sus objetivos, la cual se produjo en el 21 % de todos los incidentes reportados. Le siguieron el ransomware, con un 17 %, y los ataques al correo electrónico empresarial (BEC), con un 6 %. Se descubrieron documentos maliciosos (maldocs), campañas de spam, herramientas de acceso remoto y acceso a servidores en el 5 % de cada uno de dichos casos.

Principales acciones sobre los objetivos en 2022

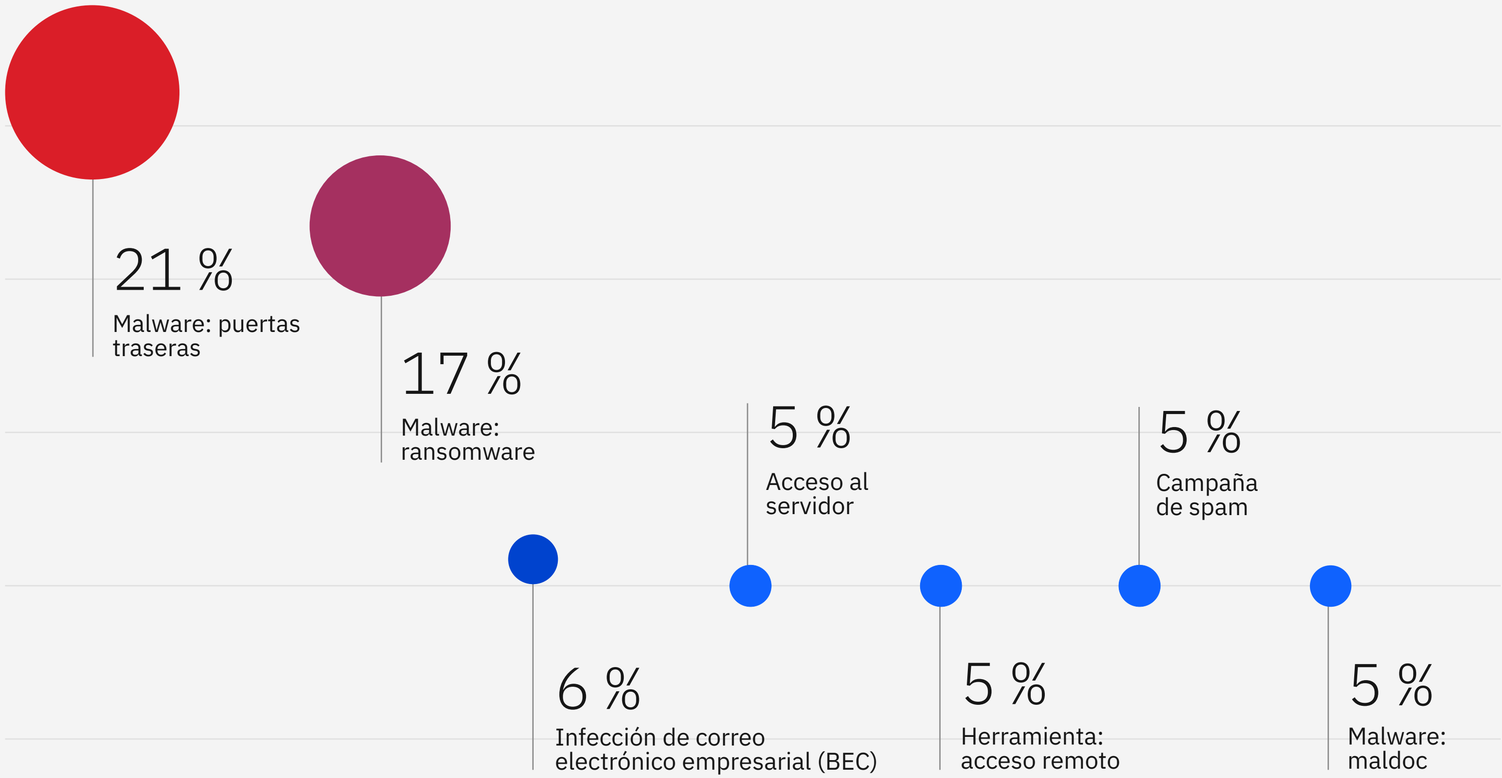


Figura 7: Principales acciones sobre objetivos observadas por X-Force en 2022. Fuente: X-Force

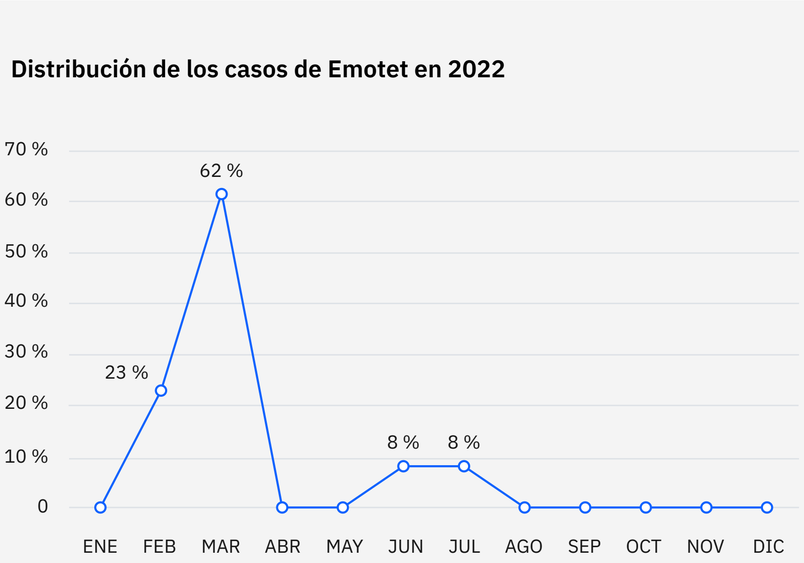


Figura 8: Gráfico que muestra el aumento de casos de Emotet a principios de 2022. Fuente: X-Force

En los casos en los que el uso de una puerta trasera se clasificó como una acción sobre el objetivo, es probable que el agente de amenaza tuviera otras intenciones cuando se puso en funcionamiento la puerta trasera. Es probable que la intervención exitosa de los equipos de seguridad o de respuesta a incidentes haya impedido que el atacante cumpliera con otros objetivos. Esta actividad maliciosa probablemente incluyó ransomware, ya que cerca de dos tercios de los casos de puertas traseras mostraban indicios de ser un ataque de ransomware.

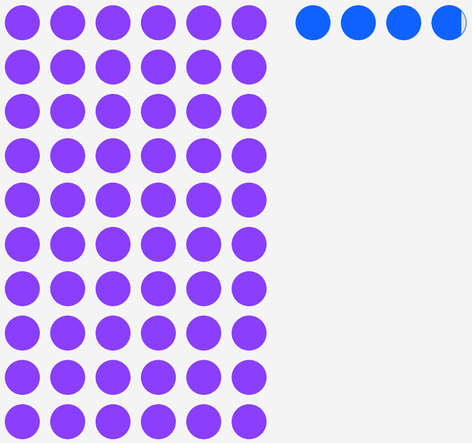
El aumento del uso de puertas traseras también puede deberse a la cantidad de dinero que este tipo de acceso puede generar en la dark web. El acceso infectado a la red corporativa de un intermediario de acceso inicial suele venderse por varios miles de USD. Este tipo de acceso puede ser buscado por agentes maliciosos que buscan obtener un beneficio rápido y evitar problemas para mantener el acceso mientras se mueven lateralmente y obtienen datos de alto valor. Aquellos agentes maliciosos que carecen de acceso al malware necesario para establecer el acceso por sí mismos también pueden buscar puertas traseras.

Los intermediarios de acceso inicial suelen intentar subastar sus accesos, los cuales X-Force ha visto por entre USD 5 000 y 10 000 aunque los precios finales pueden ser inferiores. Otros han informado de la venta de accesos por entre USD 2 000 y 4 000 y uno de ellos alcanzó los USD 50 000. Estas cantidades se comparan con el precio considerablemente inferior de algo como una tarjeta de crédito simple, que se ofrece por menos de USD 10.

Las puertas traseras provocaron un notable aumento de los casos de Emotet en febrero y marzo. Ese repunte infló significativamente la clasificación de casos de puertas traseras, ya que las implementadas en este periodo representan el 47 % de todas las identificadas a nivel mundial a lo largo de 2022. Tras el paro de Emotet de julio a noviembre, después del cual volvió a funcionar durante casi dos semanas con un volumen mucho menor, el número de casos de puertas traseras descendió significativamente.

Duración media de los ataques de ransomware

2019	2021
Más de 2 meses	Más de 3 días



Ransomware

Incluso en medio de un año caótico para algunos de los sindicatos de ransomware más prolíficos, el ransomware fue el segundo objetivo más común; el primero fue la instalación de puertas traseras, seguido de las interrupciones en las operaciones de las empresas. La proporción de incidentes de ransomware disminuyó del 21 % en 2021 al 17 % en 2022.

Un estudio de IBM Security X-Force reveló que la duración promedio de los ataques de ransomware se redujo en un 94,34 % de 2019 a 2021, de más de dos meses a menos de cuatro días. Sin embargo, el ransomware es un riesgo claro y presente que solo muestra signos de expansión, no de ralentización.

Una forma especialmente dañina de que los operadores de ransomware distribuyan su carga útil a través de una red es comprometiendo los controladores de dominio. Un pequeño porcentaje, aproximadamente el 4 %, de los resultados de las pruebas de penetración en la red realizadas por X-Force Red revelaron entidades que tenían configuraciones erróneas en Active Directory que podían dejarlas expuestas a una escalada de privilegios o a la toma total del dominio. En 2022, X-Force también observó ataques de ransomware más agresivos contra la infraestructura subyacente, como ESXi e Hyper-V. El impacto potencialmente alto de estos métodos de ataque resalta la importancia de asegurar adecuadamente los controladores de dominio y los hipervisores.

Variantes de ransomware

A medida que los grupos de ransomware y los intermediarios de acceso relacionados van y vienen, X-Force ha visto abandonos regulares en los principales grupos activos en este espacio. X-Force encontró 19 variantes de ransomware en 2022, frente a las 16 de 2021. Las variantes de LockBit comprendieron el 17 % del total de los incidentes de ransomware observados, frente al 7 % en 2021. Phobos empató con WannaCry en el segundo lugar con un 11 %. Los principales grupos en 2022 desplazaron al primer lugar de 2021, REvil, también conocido como Sodinokibi, con un 37 % de los casos en 2021, y al segundo lugar, Ryuk, con un 13 %. Ambos disminuyeron hasta llegar al 3 %.

LockBit 3.0 es la última variante de la familia de ransomware LockBit que forma parte de una operación de ransomware como servicio (RaaS) asociada a LockerGoga y MegaCortex. LockBit está en funcionamiento desde septiembre de 2019 y LockBit 3.0 se lanzó en 2022. Una parte significativa del código fuente de LockBit 3.0 parece haber sido tomada del ransomware BlackMatter.

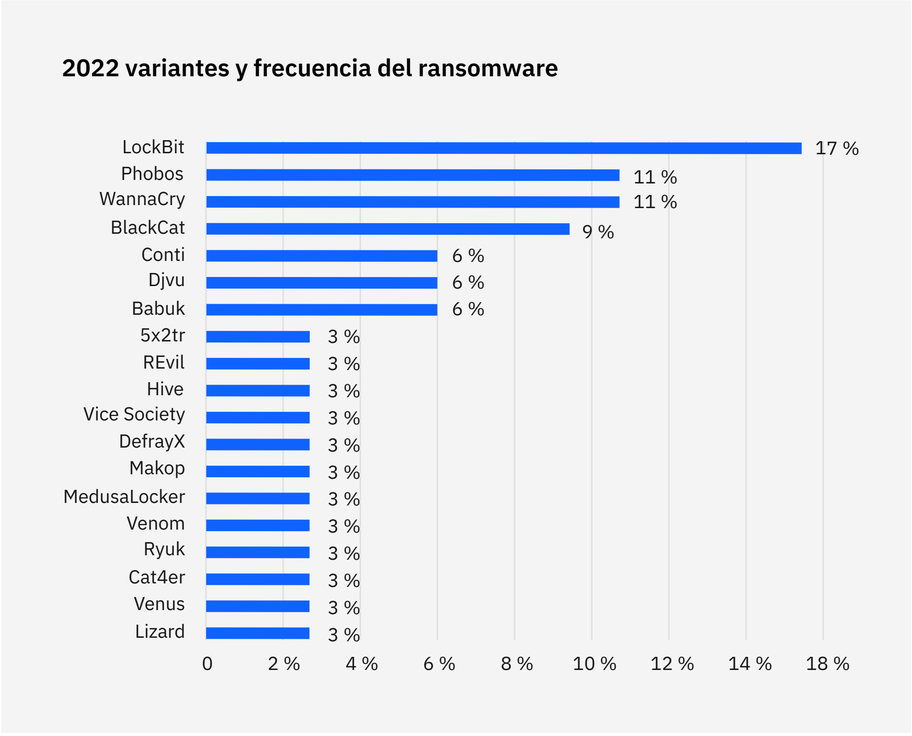


Figura 9: Variantes de ransomware y la frecuencia con la que fueron observados en las interacciones de respuesta a incidentes de X-Force en 2022. Fuente: X-Force

Los investigadores descubrieron por primera vez el ransomware Phobos a principios de 2019. Gracias a las similitudes en el código, los mecanismos de distribución, las técnicas de explotación y las notas de rescate, Phobos se identificó como una bifurcación de las conocidas familias de ransomware Crysis y Dharma. Phobos se utiliza habitualmente para ataques a menor escala, los cuales implican menores exigencias de rescate. Las campañas de phishing por correo electrónico y la explotación de puertos vulnerables del protocolo de escritorio remoto (RDP) son los principales métodos de distribución observados para Phobos.

WannaCry, visto por primera vez en 2017, se propaga utilizando EternalBlue para explotar la vulnerabilidad en el servidor Microsoft Server Message Block 1.0 (SMBv1) (MS17-010). Varios casos de WannaCry o Ryuk que X-Force observó en 2022 fueron el resultado de infecciones de hace tres o cinco años y tuvieron lugar en equipos antiguos sin parches, lo que pone de relieve la importancia de una limpieza adecuada tras este tipo de eventos.

Infección de correo electrónico empresarial (BEC)

BEC mantuvo su tercer lugar en 2022 con el 6 % de los incidentes a los que respondió X-Force. Este rango es ligeramente inferior al 8 % de ataques en 2021 y al 9 % del quinto lugar en 2020. Desplazó al ataque que ocupaba el segundo lugar en 2021, que eran los ataques de acceso a servidores. Este tipo de ataques se producen cuando un atacante consigue acceder a un servidor con fines desconocidos. En 2022 estos ataques se clasificaron de forma más granular según el tipo de acceso que conseguían esos agentes. Se usaron enlaces de spear phishing en la mitad de los casos de BEC a los que respondió X-Force. Los archivos adjuntos maliciosos y el abuso de cuentas válidas se utilizaron para permitir intentos de BEC en el 25 % de los casos cada uno.

Principales impactos

X-Force también examinó con más detalle el efecto de los incidentes en las empresas víctimas para comprender mejor el impacto que los agentes de amenazas buscaban tener a través de los incidentes a los que respondió X-Force. Con esta información, las organizaciones pueden conocer mejor los impactos más comunes para planificar con mayor eficacia las respuestas a posibles incidentes futuros.

El análisis reveló que más de uno de cada cuatro incidentes tenía como objetivo extorsionar a las empresas víctimas, lo que lo convierte en el principal impacto observado en los incidentes corregidos por X-Force. Los casos de extorsión observados se ejecutaban con mayor frecuencia mediante ransomware o BEC y, a menudo, incluían el uso de herramientas de acceso remoto, cryptominers, puertas traseras, descargadores y web shells.

Principales impactos en 2022

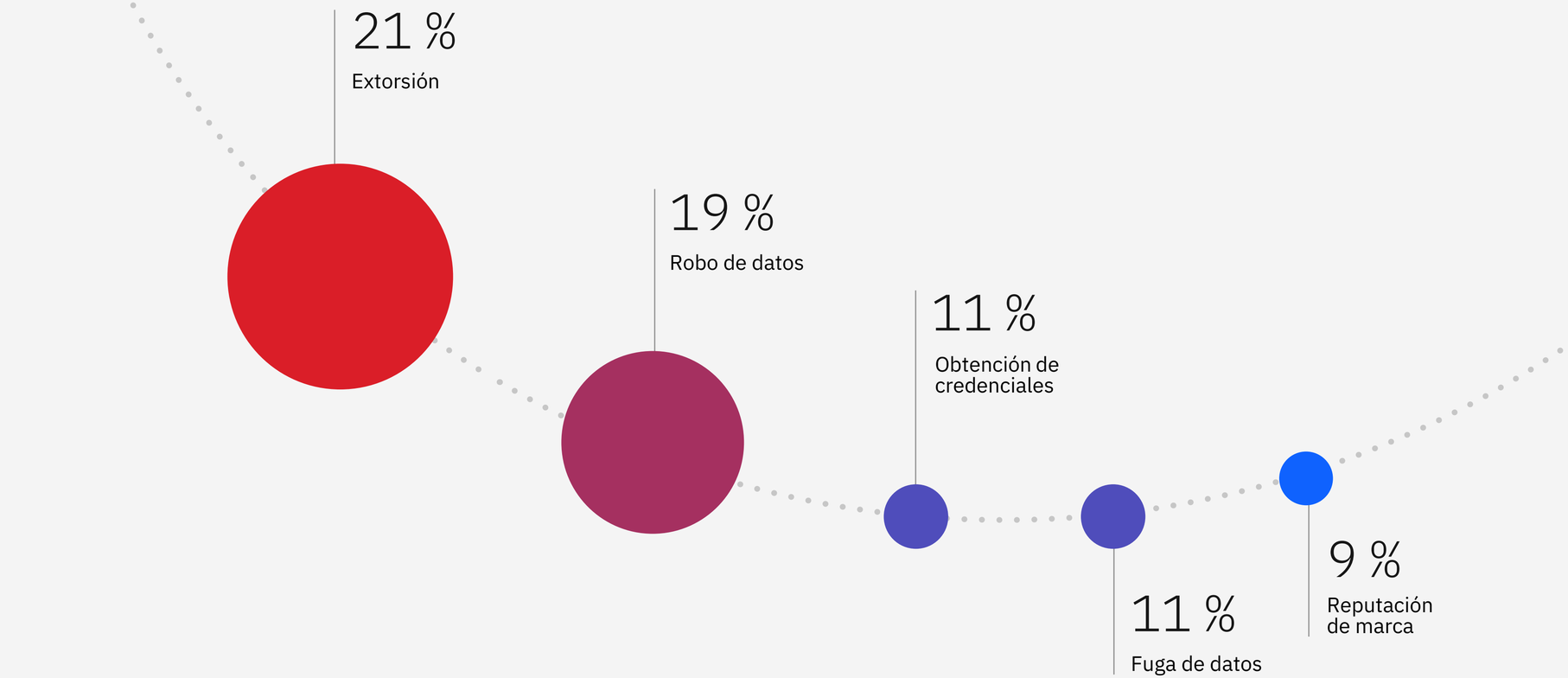


Figura 10: Principales impactos observados por X-Force en las respuestas a incidentes en 2022. Fuente: X-Force

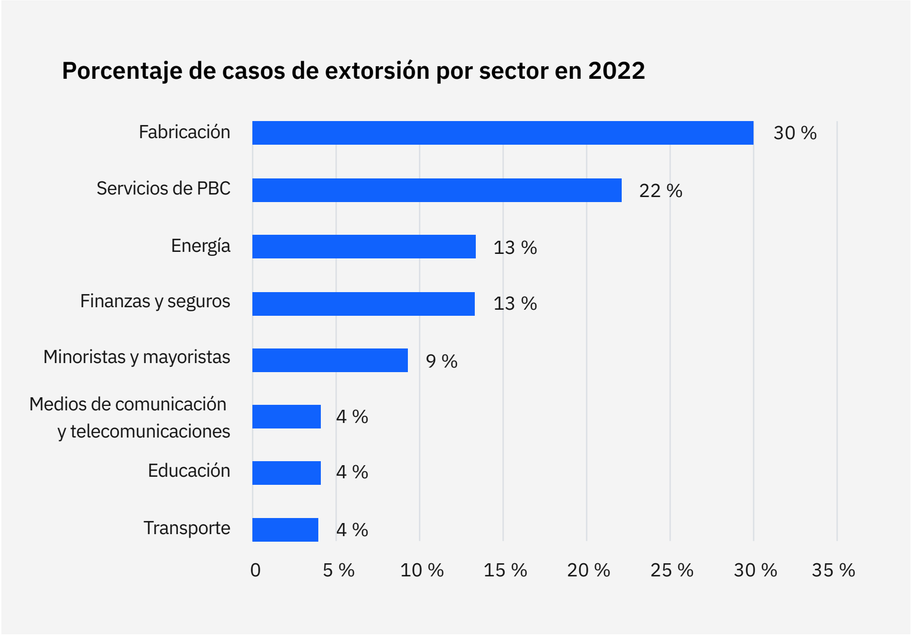


Figura 11: Porcentaje de casos de extorsión por sector observados por X-Force en las respuestas a incidentes en 2022. Las cifras no suman el 100 % debido al redondeo. Fuente: X-Force

El robo de datos ocupó el segundo lugar y representó el 19 % de todos los incidentes que corrigió X-Force. La obtención de credenciales que condujo al robo de nombres de usuarios y contraseñas y que requirió las correspondientes mitigaciones representó el 11 %. Los incidentes en los que X-Force pudo identificar información específica que realmente se filtró después de ser robada fueron menos comunes que el robo de datos, con un 11 %. Los impactos en la reputación de la marca, como la interrupción de los servicios que los clientes prestan a sus clientes, representaron el 9 % de los incidentes. Ver en el Apéndice la lista completa de impactos rastreados por X-Force. Los incidentes que afectaron a la reputación de marca de las víctimas fueron principalmente ataques de denegación de servicio distribuido (DDoS), los cuales también se utilizan con frecuencia para extorsionar a las víctimas con el fin de que paguen dinero para detener el ataque.

Avances notables en la extorsión en línea[1-9]

Año	Evento	Táctica
2013	Cryptolocker: uno de los primeros grandes brotes de ransomware	Encriptación de datos
2014	DDoS 4 Bitcoin, Armada Collective	Ransom DDoS
2015	El ransomware Chimera añade la amenaza de filtrar los datos robados en línea	Doble extorsión
2017–18	BitPaymer y SamSam	Caza mayor
2020	Caso del ransomware Vastaamo	Triple extorsión

Extorsión

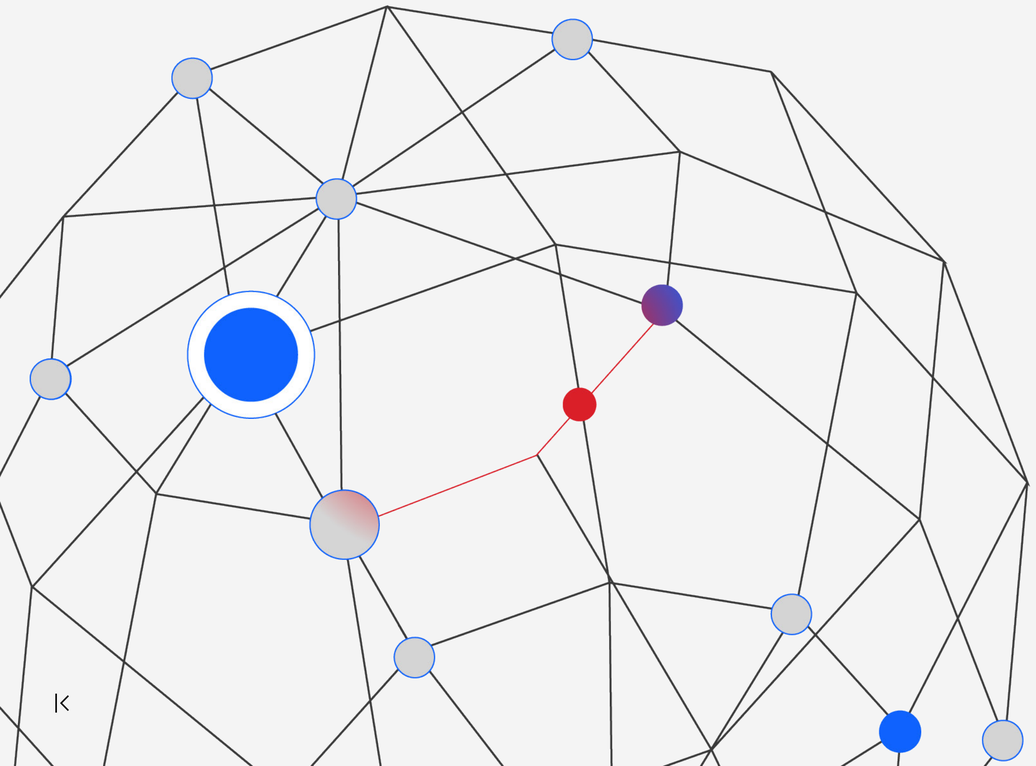
Aunque actualmente la extorsión se asocia más con el ransomware, las campañas de extorsión comprenden una variedad de métodos para ejercer presión sobre sus objetivos. Entre ellas, se incluyen las amenazas DDoS, la encriptación de datos y, más recientemente, las amenazas de doble y triple extorsión que combinan varios elementos vistos anteriormente.

Otra táctica con la que al menos un grupo de ransomware experimentó a partir de 2022 fue hacer que los datos que habían robado fueran más accesibles para las víctimas posteriores. Al facilitar a las víctimas secundarias la identificación de sus datos entre una fuga de datos, los operadores buscan aumentar la presión posterior sobre la empresa que fue objetivo del grupo o afiliada de ransomware en primer lugar. En 2023, X-Force espera que los autores de amenazas experimenten con notificaciones a las víctimas mejoradas o novedosas para aumentar los posibles costos legales y de reputación de una intrusión.

A menudo, tanto los defensores como las víctimas de los ciberataques se centran en los impactos observados en una empresa por parte de los atacantes. Sin embargo, es importante tener en cuenta las intenciones de dichos atacantes, sus capacidades y cómo evolucionan con el tiempo. Este enfoque permite discernir mejor cuál puede ser la próxima evolución de las capacidades. Dada la creciente variedad de opciones de extorsión y el objetivo principal de los autores de ransomware de obtener beneficios económicos, el equipo de X-Force considera que los atacantes seguirán evolucionando y ampliando sus metodologías de extorsión para encontrar nuevas formas de presionar a las víctimas para que paguen.

07

Desarrollos cibernéticos vinculados a la guerra de Rusia en Ucrania



La actividad cibernética patrocinada por Rusia tras su invasión a Ucrania no ha dado lugar, hasta el momento de esta publicación, a los ataques generalizados y de gran impacto que las entidades gubernamentales occidentales temían en un principio. Sin embargo, Rusia ha desplegado un número sin precedentes de wipers contra objetivos en Ucrania, lo que pone de relieve su continua inversión en capacidades de malware destructivo. Además, la invasión ha provocado el resurgimiento de la actividad de hackers emprendida por grupos simpatizantes de uno u otro bando, así como una reordenación del panorama cibercriminal de Europa del Este.

Teniendo en cuenta las capacidades avanzadas de Rusia para ejecutar ciberataques contra infraestructuras críticas desde 2015, los organismos de ciberseguridad internacionales emitieron una advertencia en abril de 2022. La advertencia mencionaba operaciones cibernéticas de posible importancia e interrupciones relacionadas en Ucrania y otros lugares. X-Force evaluó que las amenazas más importantes que surgieron incluyen el regreso de la acción de hackers y el malware wiper, así como cambios significativos en el mundo cibercriminal. La mayoría de estas operaciones tuvieron como víctimas a entidades centradas en Ucrania, Rusia y países vecinos, pero algunas se han extendido también a otras zonas.

Por otra parte, los defensores están empleando hábilmente los avances en materia de detección, respuesta e intercambio de información que se han desarrollado en los últimos años. Muchos de los primeros intentos de ataques wiper fueron rápidamente identificados, analizados y divulgados. Estos ataques incluyen al menos ocho wipers identificados y el descubrimiento e interrupción de un ciberataque ruso planeado contra la red eléctrica de Ucrania en abril de 2022.

En el ciberespacio, los efectos más palpables de la guerra en curso proceden de grupos autoproclamados hackers que operan en apoyo de intereses nacionales ucranianos o rusos. Aunque desde la invasión rusa se han formado muchos grupos que operan contra las redes rusas y ucranianas para hacer política, Killnet es uno de los más prolíficos que simpatizan con Rusia. Ha reivindicado ataques DDoS contra servicios públicos, ministerios, aeropuertos, bancos y empresas energéticas con sede en la Organización del Tratado del Atlántico Norte (OTAN) estados miembros, países aliados de Europa, así como en Japón y los Estados Unidos. Las entidades que encajan en el perfil de ataque de Killnet deben contar con medidas de mitigación DDoS, como contratar los servicios de un proveedor de mitigación DDoS externo.

Cronología de determinados eventos de hackers en 2022

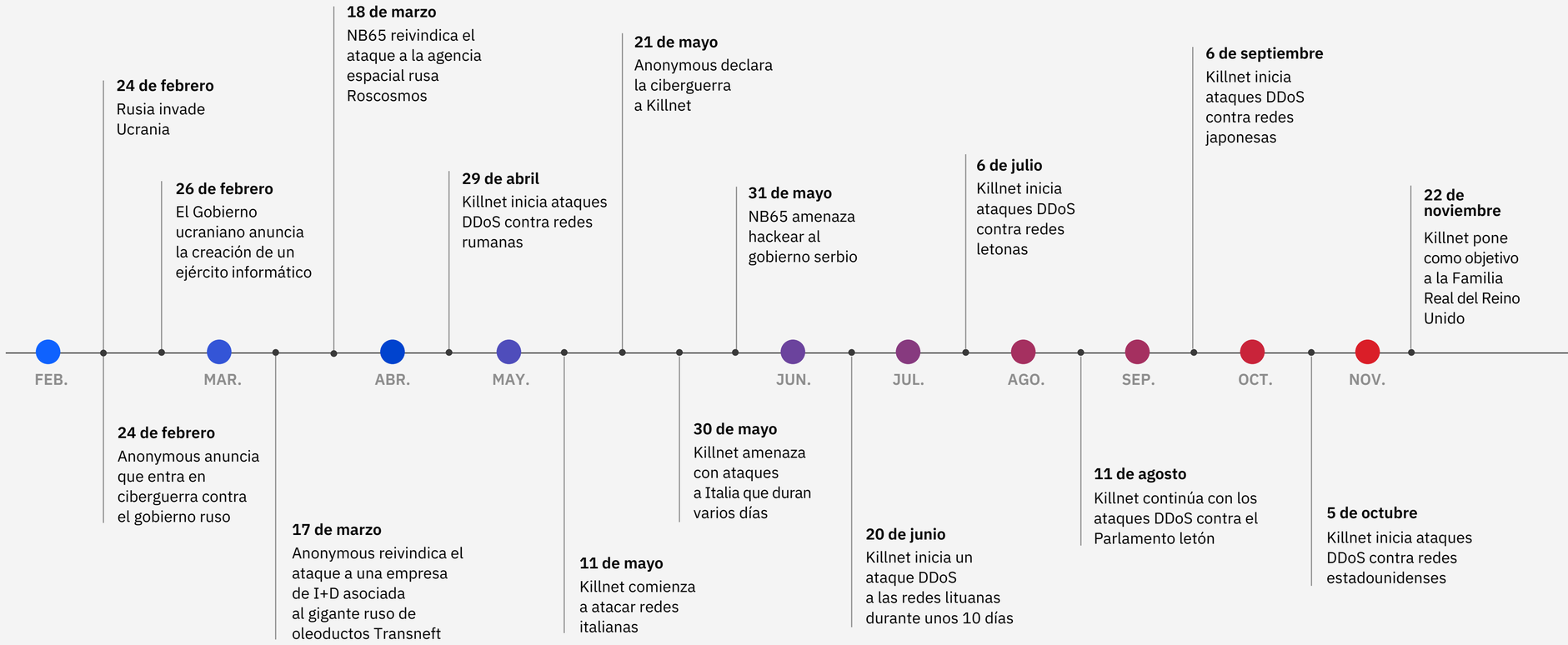


Figura 12: Imagen que muestra los eventos de ataques observados hasta la fecha durante el conflicto en Ucrania. Fuente: Análisis X-Force de informes de código abierto

Los wipers aparecieron en la guerra de Rusia en Ucrania

La guerra de Rusia en Ucrania se destaca por el uso de múltiples familias de wiper desplegadas contra múltiples objetivos en rápida sucesión y a una escala nunca vista, así como por el uso de malware junto a operaciones militares cinéticas.

Estos usos incluyen al menos nueve wipers nuevos: AcidRain, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AwfulShred, OrcShred y SoloShred. Estos wipers se utilizaron principalmente contra las redes ucranianas desde antes de la invasión inicial hasta las primeras etapas de la guerra, principalmente de enero a marzo de 2022. Aunque ya se han usado wipers en el pasado, en la mayoría de los casos se ha tratado de campañas aisladas contra un grupo limitado de objetivos. No obstante, las notables excepciones de WannaCry y NotPetya, las cuales se propagaron indiscriminadamente tras afectar a sus víctimas iniciales, hacen temer que estos wipers tengan una mayor difusión o sean reutilizados para operaciones maliciosas en otros lugares.

X-Force sigue afirmando que los agentes de ciberamenazas patrocinados por Rusia continúan siendo una amenaza significativa para las redes informáticas y las infraestructuras críticas de todo el mundo. Este juicio se basa en ciberoperaciones rusas que ocurren desde hace tiempo y están dirigidas a redes ucranianas, europeas, de la OTAN y de Estados Unidos, así como en operaciones de ataque ejecutadas por grupos de amenazas rusas desde 2015.

Conmoción entre los grupos de ciberdelincuentes rusos

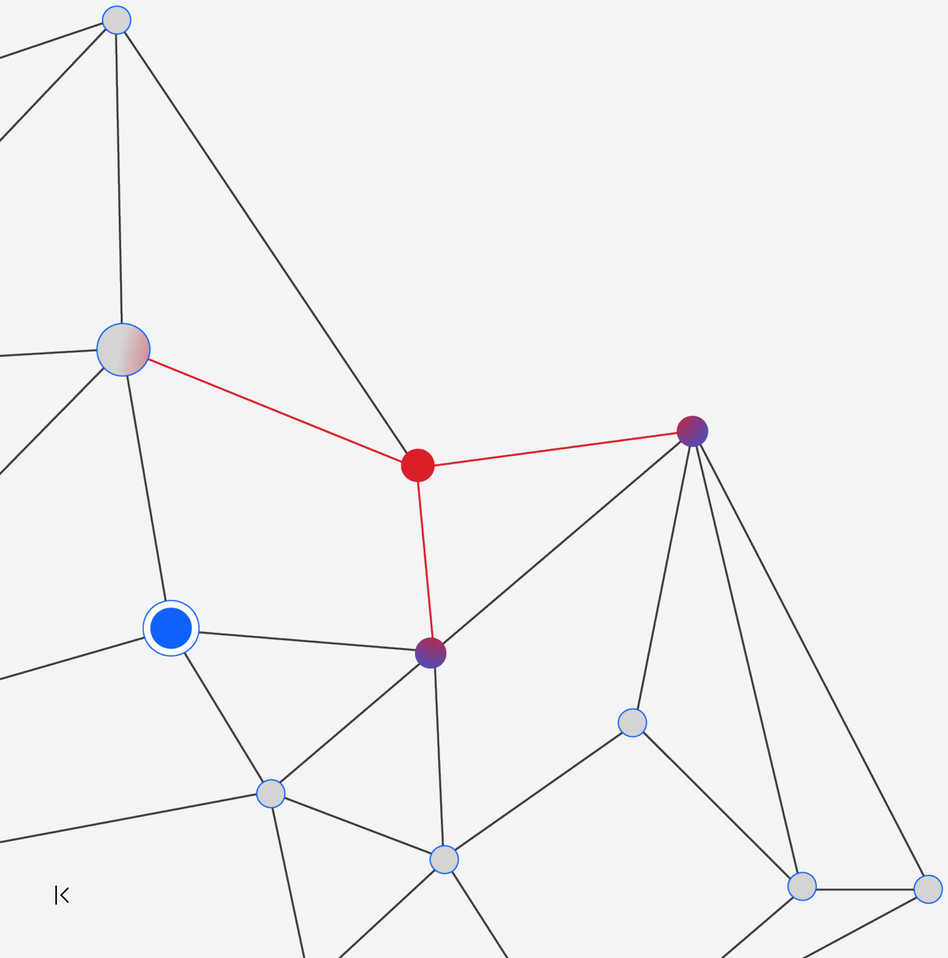
2022 fue un año tumultuoso para ITG23, uno de los sindicatos de ciberdelincuentes rusos más destacados, conocido principalmente por desarrollar el troyano bancario Trickbot y el ransomware Conti. El grupo sufrió una serie de filtraciones relevantes a principios de 2022, tras respaldar públicamente la participación de Rusia en la guerra. Conocidos como ContiLeaks y TrickLeaks, dieron lugar a la publicación de miles de mensajes de chat y al doxing de numerosos miembros del grupo. X-Force descubrió pruebas que indicaban que ITG23 comenzó a atacar sistemáticamente desde mediados de abril hasta, al menos, mediados de junio de 2022, un cambio sin precedentes, ya que el grupo no había atacado a Ucrania anteriormente.

Además, aparentemente el grupo ha retirado dos de sus familias de malware más conocidas, Trickbot y Bazar, y ha cancelado su operación de ransomware Conti. Varios informes han sugerido que podría estar produciéndose una importante reestructuración de personal, con la división del grupo en varias facciones y el cese completo de la actividad por parte de ciertos miembros.

El cierre de Trickbot y Bazar, los cuales son responsables de un número significativo de infecciones en 2021, provocó un vacío que fue llenado rápidamente por familias de malware como Emotet, IcedID, Qakbot y Bumblebee. Antes de su cierre, ITG23 seguía implementando el ransomware Conti de forma prolífica, lo cual representó un tercio de todos los casos de ransomware a los que X-Force respondió en el primer trimestre de 2022.

El grupo también publicó una nueva versión de su malware Anchor, una puerta trasera sigilosa que el grupo había desarrollado tradicionalmente contra objetivos de alto perfil. La versión actualizada descubierta por X-Force, y denominada AnchorMail, cuenta con un novedoso mecanismo de comunicación de mando y control (C2) basado en el correo electrónico. El servidor C2 emplea los protocolos Simple Mail Transfer Protocol Secure (SMTPS) e Internet Message Access Protocol Secure (IMAPS), y el malware se comunica con el servidor enviando y recibiendo mensajes de correo electrónico diseñados de forma específica.

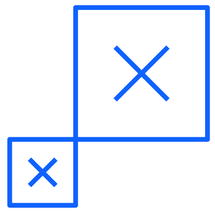
El panorama del malware



Aumento de virus propagadores de USB

Después de que X-Force observara intentos de infección de Raspberry Robin que estaban afectando a empresas a mediados de mayo de 2022, el enigmático gusano comenzó a propagarse rápidamente en las redes de las víctimas a partir de usuarios que compartían dispositivos USB (bus serie universal). Las infecciones se dispararon a principios de junio y a principios de agosto Raspberry Robin alcanzó un punto máximo del 17 % de los intentos de infección observados por X-Force. Este máximo se identificó en los sectores del petróleo y el gas, la manufactura y el transporte. El porcentaje de intentos de infección del 17 % en estos sectores es significativo, ya que menos del 1 % de los clientes de X-Force en total han visto la misma variante de malware. X-Force también observó más actividad de Raspberry Robin desde septiembre hasta noviembre de 2022.

La propagación de virus basados en USB se realiza mediante ingeniería social y requiere algún tipo de acceso físico a una red terminal para llevar a cabo una infección exitosa, ya sea por un usuario legítimo o por algún otro medio. X-Force recomienda asegurarse de que las herramientas de seguridad bloquean los malware conocidos basados en USB, impartir formación sobre seguridad y desactivar las funciones de ejecución automática de cualquier soporte de almacenamiento extraíble. En entornos especialmente delicados, como los sistemas OT o donde existan espacios de aire, lo más seguro es prohibir por completo el uso de memorias USB. Si es necesario permitirlos, se debe controlar estrictamente el número aprobado de dispositivos portátiles para uso en su entorno, además de poner en práctica las sugerencias anteriores.



El aumento de Rust

El lenguaje Rust Programming Language aumentó constantemente su popularidad entre los desarrolladores de malware durante 2022, gracias a su soporte multiplataforma y a los bajos porcentajes de detección de antivirus en comparación con otros lenguajes más comunes. Al igual que el lenguaje Go, también se beneficia de un proceso de compilación más complicado que puede hacer que el malware requiera más tiempo de análisis por los ingenieros inversos. Varios creadores de ransomware han lanzado versiones Rust de sus malware, como BlackCat, Hive, Zeon y, más recientemente, RansomExx. Además, X-Force ha analizado un crypter ITG23 escrito en Rust, junto con la familia CargoBay de puertas traseras y aplicaciones de descarga. La creciente popularidad de Rust pone de manifiesto que el ecosistema del ransomware sigue centrándose en innovar para eludir la detección.

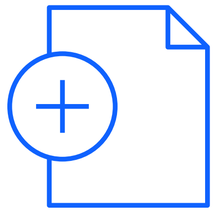
Vidar InfoStealer

X-Force observó una afluencia repentina del malware Vidar InfoStealer que comenzó en junio de 2022 y continuó hasta principios de 2023. Observado por primera vez en 2018, Vidar es un troyano malicioso que roba información y es distribuido como malware como servicio (MaaS). El troyano suele ejecutarse cuando los usuarios hacen clic en enlaces o archivos maliciosos de spam (malspam) adjuntos. Gracias a su amplio esquema de funciones, Vidar puede utilizarse para recuperar una gran variedad de información del dispositivo como datos de tarjetas de crédito, nombres de usuario, contraseñas y archivos, y para realizar capturas de pantalla del escritorio del usuario. Vidar también puede robar carteras de criptomonedas de Bitcoin y Ethereum.

Los ataques a través de un ladrón de información (info stealer) suelen tener una motivación económica. Los datos robados se analizan y cualquier información valiosa se coteja y organiza en una base de datos.

Esta base de datos puede venderse en la dark web o a través de la aplicación de mensajería privada Telegram. Los autores de las amenazas pueden usar la información para cometer diversos tipos de fraude, como solicitar préstamos bancarios o tarjetas de crédito, comprar artículos en línea o hacer reclamaciones fraudulentas al seguro médico.

Las amenazas pueden utilizar credenciales de inicio de sesión infectadas para acceder a cuentas corporativas y servicios remotos. El costo medio de utilizar un ladrón de información es de aproximadamente USD 250 al mes y depende de los usuarios implementar el malware de su elección. X-Force observa regularmente mercados que intentan vender accesos capturados por malware de robo de información por entre USD 10 y USD 75. Una vez obtenido el acceso, los atacantes pueden utilizar fácilmente los privilegios de la cuenta atacada como punto de partida para iniciar otras actividades maliciosas.



Evolución de los mecanismos de distribución de malware

Cada vez es más frecuente que el malware se distribuya a través de documentos maliciosos de Microsoft Office, normalmente adjuntos a correos electrónicos de phishing. Los desarrolladores de malware crearon estos documentos con macros maliciosas diseñadas para ejecutar malware al abrir el documento. El uso de macros con este fin se extendió tanto que los productos de Microsoft Office comenzaron a incluir advertencias de seguridad en el momento de apertura de documentos habilitados para macros. En julio de 2022, Microsoft empezó a bloquear de forma predeterminada la ejecución de macros en los documentos recibidos por correo electrónico o desde Internet.

A medida que los defensores aumentaban sus capacidades de detección y prevención, los atacantes comenzaron a alejarse de la aplicación Visual Basic (VBA) para pasar a un formato de macro existente más antiguo dentro de Microsoft Excel conocido como Macro 4.0. Los documentos Excel maliciosos se utilizan desde hace bastante tiempo. Sin embargo, la mayoría de los mecanismos de seguridad se crearon en torno a macros VBA dentro de un documento Excel. Durante un tiempo, las macros de Excel Macro 4.0 proporcionaron un buen medio para eludir la detección. Alrededor de esta misma época, algunos agentes de amenazas comenzaron a enviar enlaces dentro de un correo electrónico para llevar a la víctima a un sitio instalador de malware (dropper) para descargar los documentos maliciosos en lugar de enviarlos como un archivo adjunto de correo. Cuando Microsoft introdujo cambios para permitir a los administradores desactivar Macro 4.0 y también bloquear la ejecución de macros descargadas de Internet, los atacantes se vieron obligados a cambiar nuevamente de táctica.

Tras los cambios introducidos por Microsoft, muchos autores de malware siguen utilizando documentos de Microsoft Office habilitados para macros, pero los grupos más sofisticados adoptaron una cadena de infección más intrincada y compleja. Estas nuevas tácticas consisten en una combinación de archivos HTML con un binario incrustado o un archivo comprimido protegido por contraseña. Esos archivos también incluyen una imagen ISO que puede contener un archivo LNK o CMD, así como otros tipos de archivos que probablemente no se envíen a un destinatario de correo electrónico ni se descarguen de Internet. Otros incluyen la inyección remota de templates o la explotación de vulnerabilidades. CVE-2021-40444, una vulnerabilidad de ejecución remota de código en Microsoft HTML (MSHTML), es un ejemplo en el que se utiliza un componente de software para representar páginas web en Microsoft Windows para ejecutar el malware en lugar de depender de macros.

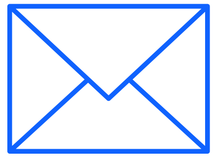
Los datos de spam destacan la amenaza del ransomware e ilustran mejor las macrotendencias

X-Force analizó las tendencias del phishing y el spam en el correo electrónico para comprender mejor su eficacia general y su uso por parte de los atacantes. En la investigación se descubrió que los mensajes de spam se utilizaron regularmente a lo largo del año para distribuir malware, como Emotet, Qakbot, IcedID y Bumblebee, los cuales a menudo conducen a infecciones de ransomware.

Malware[10-18]	**Ransomware**
Trickbot	*Conti*
Bazarloader	*Conti*, Diavol
IcedID	*Conti*, Quantum
Bumblebee	*Conti*, Diavol, Quantum
Emotet	*Conti*, BlackCat, Quantum
Qakbot	*REvil*, *Conti*, Black Basta
SocGholish	LockBit

Los datos de esta tabla abarcan el periodo comprendido entre fines de 2021 y la publicación de este informe. La cursiva indica que el malware o ransomware fue detectado en 2022, pero no ha sido observado por X-Force al menos hasta octubre de 2022.

X-Force identificó un aumento en la actividad de Qakbot en septiembre de 2022 que utilizaba el contrabando de HTML para vulnerar a las víctimas. Estas infecciones están vinculadas a una amplia actividad posterior al ataque, lo cual incluye el reconocimiento, la obtención de información y la implementación de cargas útiles adicionales. Las infecciones de Qakbot no controladas a lo largo de 2022 provocaron múltiples infecciones de Black Basta. X-Force observó que los ataques de ransomware reivindicados en el sitio de filtraciones del grupo de ransomware Black Basta disminuyeron notablemente durante la interrupción de la actividad de phishing de Qakbot en el verano de 2022. X-Force espera que la reanudación de la actividad de Qakbot se correlacione de una forma similar con un mayor número de víctimas del ransomware.



Cómo evitar las macros

El uso de archivos ISO y LNK surgió como una importante táctica para infectar empresas víctimas en respuesta a los cambios de macros de Microsoft a partir de octubre de 2021. Esta táctica incluye tanto la entrega directa de sus cargas útiles a través de esos archivos contenedores, como el encubrimiento de archivos habilitados para macros dentro de ellos.

- Los archivos ISO y los archivos comprimidos se están usando para eludir el atributo de marca de web (MOTW) que Microsoft está usando para ayudar a los objetivos a habilitar macros maliciosas. Mientras que los archivos ISO o comprimidos parecerán descargados de Internet, el archivo adjunto habilitado para macros que contienen no lo hará, lo que les permite a los agentes de amenazas continuar con este ataque.
- Otra forma de eludir las restricciones de las macros es incluir cargas útiles directamente en los archivos LNK que, al hacer clic en ellas, lanzan comandos arbitrarios que se utilizan principalmente para descargar o cargar las siguientes fases. Antes de principios de 2022, solo hubo una campaña en febrero de 2021 que empleó esta táctica. X-Force lo observó por primera vez de forma recurrente a finales de febrero-marzo de 2022 y ahora lo ve con regularidad.

Entre las tendencias adicionales detectadas por X-Force en las campañas de spam de los agentes de amenazas se incluyen el aumento del uso de archivos comprimidos encriptados como adjuntos y la apropiación de datos informáticos, como se explica aquí.

- Las extensiones comprimidas encriptadas, más difíciles de detectar y marcar como maliciosas por los software antivirus, se descubrieron con más frecuencia en 2022. El número promedio de mensajes de spam con este tipo de archivos adjuntos enviados por semana se multiplicó por nueve en 2022, en comparación con los datos de 2021 desde abril de ese año.
- La apropiación de datos informáticos, en la que los agentes de amenazas se insertan en hilos de correo electrónico existentes, es una táctica utilizada desde hace tiempo para aumentar la legitimidad del spam y atraer a las víctimas de forma más eficaz. Esta táctica experimentó un notable aumento en 2022, en comparación con la mayor parte de 2021, y disminuyó en primavera, una tendencia que X-Force considera impulsada en gran parte por el envío de spam Emotet.

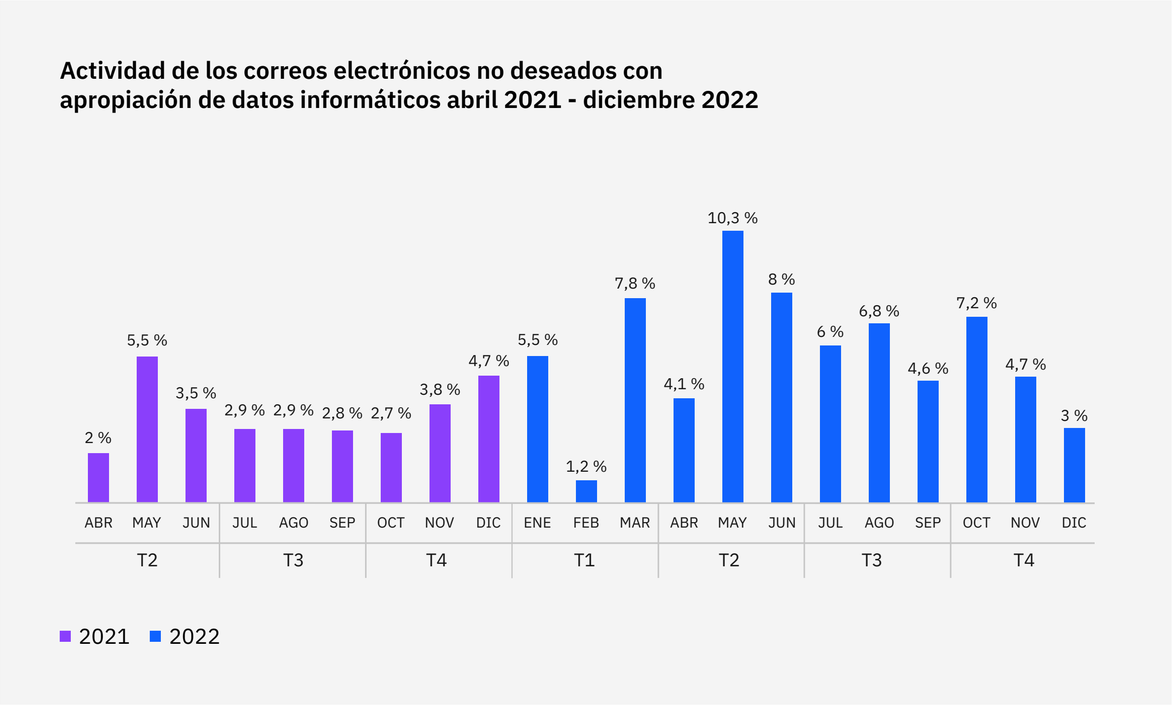


Figura 13: Las cifras muestran el porcentaje por mes del total de intentos de apropiación de datos informáticos detectados en la información de X-Force desde abril de 2021. Fuente: X-Force

– Emotet regresó en noviembre de 2021, después de que la red de bots fuera interrumpida en enero de 2021. Continuó su actividad en 2022, se tomó un descanso de casi cuatro meses a partir de mediados de julio y regresó durante casi dos semanas en noviembre de 2022.

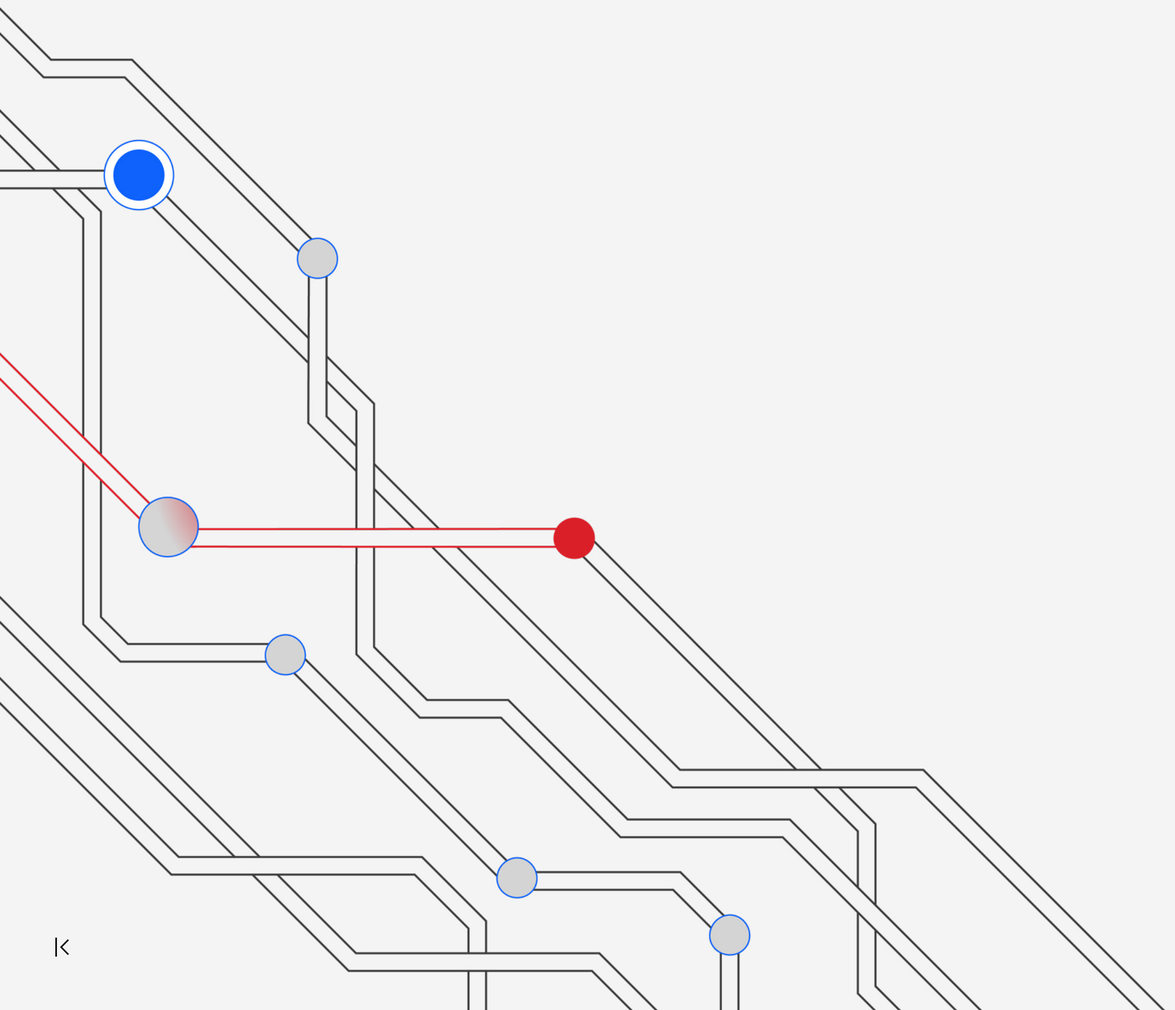
– Los datos mostraron casi el doble de intentos regulares al mes en 2022, en comparación con los datos disponibles desde abril de 2021. La apropiación de datos informáticos siguió una pendiente inestable hasta mayo de 2022 y su descenso en la segunda mitad del año coincide aproximadamente con la inactividad de Emotet.

– Los correos electrónicos no deseados que conducen a Emotet, Qakbot e IcedID hacen un uso intensivo de la apropiación de datos informáticos. El regreso de Emotet en noviembre de 2021 contribuyó al aumento inestable hasta mayo de 2022. El descenso general en la segunda mitad del año coincide con el paro de Emotet de julio a octubre y su breve regreso en noviembre de 2022.

– Rastrear la apropiación de datos y distinguirla con precisión de los casos de agentes que simplemente añaden el asunto de la respuesta en el encabezado a un correo electrónico no deseado es difícil y es probable que lo siga siendo. Por ejemplo, algunos atacantes han empezado a eliminar los encabezados “Re:”, probablemente porque son conscientes de que pueden utilizarse para rastrear su actividad.

09

Amenazas a los sistemas OT y de control industrial



Amenazas para la tecnología operativa

En 2022 se descubrieron dos nuevos malware específicos de OT, Industroyer2 y INCONTROLLER, también conocido como PIPEDREAM, y se revelaron muchas vulnerabilidades de OT denominadas OT: ICEFALL. El panorama de las ciberamenazas en el ámbito de la tecnología de la operación u OT se está ampliando drásticamente, y los propietarios y operadores de activos de OT deben ser muy conscientes de los cambios que se están produciendo.

X-Force examinó más detenidamente los datos de ataques a la red e IR específicos de OT para obtener información sobre cómo los agentes de amenazas están tratando de atacar a los clientes en los sectores relacionados con OT. Los datos sobre ataques a la red muestran que los ataques por fuerza bruta, el uso de estándares de encriptación débiles y obsoletos y las contraseñas débiles o predeterminadas son alertas comunes en los entornos de TI y OT de estos sectores.

Las alertas que indicaban probables intentos de fuerza bruta fueron las más comunes entre los datos de ataques a la red específicos del Sistema de Mando de Incidentes (ICS), seguidas de cerca por las alertas de encriptado débil. Las alertas más comunes por encriptación deficiente se referían al uso continuo de Transport Layer Security (TLS) 1.0, un método de encriptación antiguo e inseguro que quedó obsoleto en marzo de 2021. Aunque el gobierno de EE. UU. recomienda la reconfiguración para utilizar TLS 1.2 o 1.3, las directrices del Instituto Nacional de Estándares y Tecnología (NIST) abordan en mayor profundidad la realidad común. La realidad es que es posible que los sistemas más antiguos tengan que seguir utilizando versiones más débiles de encriptación para garantizar la continuidad de su funcionalidad. Las alertas de contraseñas débiles o predeterminadas también fueron notables, sobre todo teniendo en cuenta que se trata de vulnerabilidades básicas

que hacen que los atacantes puedan llevar a cabo los ataques por fuerza bruta con mayor facilidad. El intento de ataque más común contra los sectores relacionados con OT fue el escaneo de vulnerabilidades interno y externo, generalizado y probablemente indiscriminado. Los datos revelaron que las antiguas vulnerabilidades y amenazas siguen siendo relevantes hoy en día. Un grupo de vulnerabilidades descubiertas en 2021 por Cisco Talos en el software de supervisión Advantech R-SeeNet desencadenó una escasa mayoría de alertas de exploración de vulnerabilidades en todos los sectores de OT en 2022. Estas vulnerabilidades podrían permitir a los atacantes ejecutar códigos o comandos arbitrarios.

La segunda vulnerabilidad más común, sin embargo, se remonta a 2016: una vulnerabilidad de omisión de filtro en la aplicación Trihedral VTScada, CVE-2016-4510, que podría permitir a usuarios no autenticados enviar solicitudes HTTP para acceder a archivos. Los tipos de ataques, como WannaCry and Conficker, que siguen planteando amenazas significativas para la OT, ponen aún más de relieve los riesgos de las amenazas más antiguas.

El sector de la manufactura sigue siendo el más sensible a las OT

Si nos fijamos en el subconjunto de incidentes en sectores relacionados con OT, el de la manufactura fue el más atacado en 2022, según los datos. El sector fue víctima del 58 % de los incidentes que X-Force ayudó a solucionar. La implementación de puertas traseras fue la principal acción que se llevó a cabo en los objetivos, la cual fue detectada en el 28 % de los casos en el sector de la manufactura. En particular, los creadores de ransomware encuentran en este sector un objetivo atractivo, probablemente debido a la escasa tolerancia de estas empresas al tiempo de inactividad.

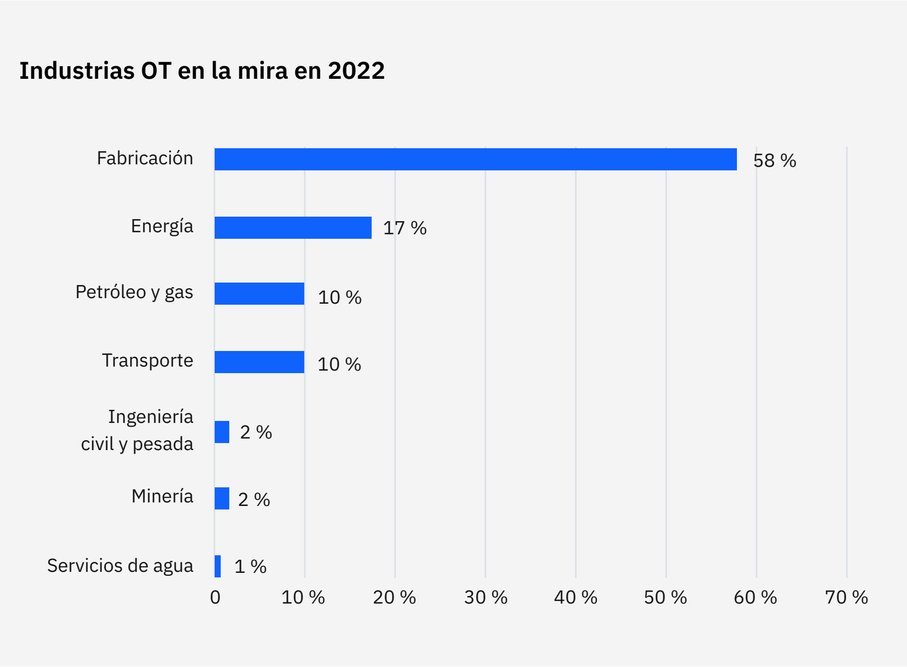


Figura 14: Proporción de casos de IR por sector relacionado con OT a los que respondió X-Force en 2022. Fuente: X-Force

En cuanto a los vectores de acceso iniciales en los casos de sectores relacionados con OT, el spear phishing representó el 38 % de los casos, lo cual incluía el uso de archivos adjuntos en un 22 % de ellos, el uso de enlaces en un 14 % y el spear phishing como servicio en un 2 %. La explotación de aplicaciones de cara al público ocupó el segundo lugar, con un 24 %, siguiendo la tendencia general del sector. La detección de puertas traseras también lideró los incidentes de estos sectores en un 20 % de los casos, seguida del ransomware con un 19 %. La extorsión también se mantiene en primer lugar entre los impactos, con un 29 %, y el robo de datos le sigue de cerca con un 24 % de los casos.

Otra de las principales vulnerabilidades explotadas en OT es la falta de una segmentación adecuada entre las redes OT y TI. El equipo de X-Force Red Adversary Simulation Services se centra regularmente en la segmentación débil para obtener acceso a entornos OT aislados. Estos entornos incluyen servidores de salto de destino, estaciones de trabajo de operador de doble alojamiento y servidores de informes, como historiadores de datos que exponen servicios web y SQL desde OT a redes de TI corporativas. Segmentar correctamente estas partes de sus redes y supervisar de cerca la comunicación entre ellas puede mantener los activos a salvo.

Evolución geográfica

Por segundo año consecutivo, la región Asia Pacífico ocupa el primer puesto como región más atacada en 2022, con el 31 % de los incidentes a los que respondió X-Force IR. Europa le siguió de cerca, con el 28 % de los ataques, y en América del Norte se produjo el 25 % de los incidentes. Asia Pacífico y Europa registraron mayores proporciones de casos, aumentando cinco y cuatro puntos porcentuales respectivamente a las cifras de 2021, con un descenso significativo en Medio Oriente del 14 % al 4 %.

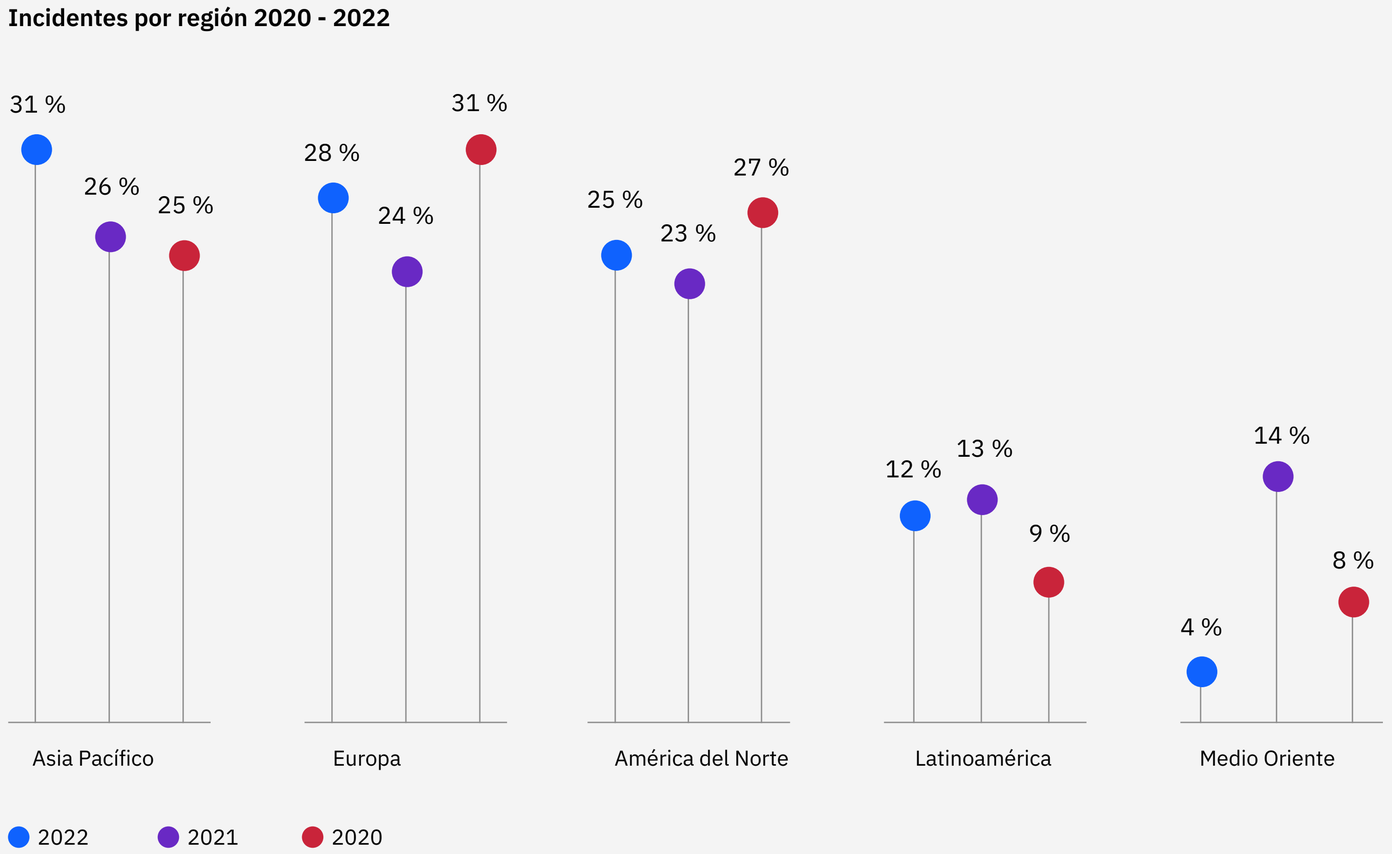


Figura 15: Proporción de casos de IR por región a los que respondió X-Force entre 2020 y 2022. Fuente: X-Force

#1 | Asia Pacífico

La región Asia Pacífico, concretamente Japón, fue el epicentro del repunte de Emotet en 2022. Aunque no está directamente relacionado con la guerra en Europa, el aumento de casos de Emotet en Japón se produjo junto con la invasión rusa de Ucrania. Otros investigadores de la comunidad de ciberseguridad señalaron que esto ayudó a aumentar la actividad de Emotet en ese momento. Se detectaron campañas de spam en varios sectores, y la mayoría de los casos se produjeron en los sectores de manufactura, finanzas y seguros. Emotet se distribuye principalmente a través de campañas de spam que utilizan titulares que llaman la atención.

La manufactura encabeza la lista de los principales sectores atacados en esta región en un 48 % de los casos, con finanzas y seguros en un distante segundo lugar con 18 %.

El spear phishing por medio de archivos adjuntos fue el principal vector de infección en esta región, con un 40 %, seguido de la explotación de aplicaciones de cara al público, con un 22 %. Los casos de servicios remotos externos y los enlaces de spear phishing empatan en el tercer lugar con un 12 %.

La implementación de puertas traseras fue la acción más común sobre el objetivo en el 31 % de los casos en la región. El ransomware ocupó el segundo lugar con un 13 % y los maldocs el tercero con un 10 %. La extorsión fue el impacto más común observado en el 28 % de los casos. El impacto en la reputación de la marca ocupa el segundo lugar, con un 22 %, y el robo de datos el tercero, con un 19 %.

Japón representó el 91 % de los casos de Asia Pacífico, Filipinas el 5 %, y Australia, India y Vietnam, el 1,5 % cada uno.

La región Asia Pacífico vio a la manufactura como el sector más atacado en el 48 % de los casos.

#2 | Europa

Europa experimentó un repunte significativo en el despliegue de puertas traseras a partir de marzo de 2022, justo después de que Rusia invadiera Ucrania. Los despliegues de puertas traseras representaron el 21 % de los casos en la región y el ransomware el 11 %. Se identificaron herramientas de acceso remoto en el 10 % de los incidentes a los que respondió X-Force. En cuanto al impacto en los clientes, el 38 % de los casos observados por X-Force en Europa estaban relacionados con la extorsión, el 17 % con el robo de datos y el 14 % con el robo de credenciales. Europa fue la región más afectada por la extorsión, ya que fue víctima del 44 % de todos los casos de extorsión observados.

La explotación de aplicaciones de cara al público fue el principal vector de infección utilizado contra las organizaciones europeas, lo cual representó el 32 % de todos los incidentes que corrigió X-Force en la región, varios de los cuales dieron lugar a infecciones de ransomware. El abuso de cuentas locales válidas se situó en segundo lugar, con un 18 %, seguido de los enlaces de spear phishing, con un 14 %, un porcentaje significativamente más bajo que el 42 % de 2021. Esta disminución de los enlaces de spear phishing puede deberse a una mayor toma de conciencia de los usuarios, a la solidez de las defensas de seguridad del correo electrónico o al empleo de defensas más eficaces que detectan los malware después de su instalación.

Los servicios profesionales, empresariales y de consumo empataron con el sector de finanzas y seguros en el puesto de sector más atacado, con un 25 % de los casos a los que respondió X-Force. La manufactura se situó en segundo lugar, con un 12 % de los casos, y los sectores energéticos y sanitarios empataron en tercer lugar, con un 10 %.

El Reino Unido fue el país más atacado de Europa, con un 43 % de los casos. Alemania representa el 14 %, Portugal el 9 %, Italia el 8 % y Francia el 7 %. “X-Force también respondió a un número menor de casos en Noruega, Dinamarca, Suiza, Austria, Grecia, Groenlandia, España y Serbia”.

El Reino Unido fue la región más atacada en Europa, ya que representa el 43 % de los casos.

#3 | América del Norte

X-Force observó un ligero aumento del número de incidentes en América del Norte, pasando del 23 % de todos los casos en 2021 al 25 % en 2022.

Las empresas energéticas encabezaron la lista de víctimas en América del Norte, ya que constituyen el 20 % de todos los ataques a los que respondió X-Force en 2022. La manufactura y el sector minorista-mayorista empataron en el segundo lugar con un 14 % de los casos cada uno. Mientras que el comercio minorista-mayorista mantuvo una posición similar en 2021, las cifras del sector de la manufactura experimentaron un descenso del 50 % con respecto a 2021. Los servicios profesionales, empresariales y de consumo ocuparon el tercer lugar en 2022 con un 12 %, en medio de un aumento del ransomware y otros casos relacionados con el malware.

Los principales vectores de infección identificados fueron la explotación de aplicaciones de cara al público, con un 35 %, y los archivos adjuntos de spear phishing, con un 20 %. Los incidentes de ransomware representaron el 23 % de los casos, algunos de los cuales fueron el resultado de detecciones de infecciones persistentes de WannaCry o Ryuk que datan de 2018 o 2019, lo que destaca la importancia de una limpieza adecuada después de estos eventos. En la región, el 12 % de los casos fueron redes de bots, con puertas traseras y BEC empatando en el tercer lugar con un 10 % cada uno.

En cuanto al mayor impacto de las amenazas, el robo de credenciales fue el más destacado, con un 25 % de los incidentes que corrigió X-Force en América del Norte. La fuga y el robo de datos empataron en segundo lugar, con un 17 % cada uno, y la extorsión representó el 13 % de los casos.

Estados Unidos fue responsable del 80 % de los ataques de la región, frente al 20 % de Canadá.

Las organizaciones más atacadas en América del Norte fueron las empresas energéticas, con un 20 % de los casos.

#4 | Latinoamérica

A efectos de información, IBM considera que Latinoamérica incluye México, Centroamérica y Sudamérica.

Los incidentes en Latinoamérica resistieron a las tendencias globales, volviendo a ser el sector minorista-mayorista el más atacado, con un 28 % de los casos que corrigió X-Force, y subiendo desde el segundo lugar en 2021. El sector de finanzas y seguros fue el segundo más afectado, con un 24 % de los casos, seguido del energético, con un 20 %.

El ransomware superó a otros ataques en Latinoamérica, representando el 32 % de los casos a los que respondió X-Force. El despliegue de puertas traseras fue la segunda acción más identificada en el objetivo, con un 16 %, mientras que BEC y la apropiación de datos de correo electrónico empataron en el tercer lugar, con un 11 % cada uno. La extorsión y el robo de datos fueron los impactos más frecuentes en la región, con un 27 % de los casos, así como las pérdidas económicas, con un 20 %. La destrucción de datos y las filtraciones empataron en el tercer lugar, con un 13 % de los casos cada una.

Los principales vectores de acceso inicial fueron los servicios remotos externos, con un 30 %, y la explotación de aplicaciones de cara al público, con un 20 %. Los ataques a unidades drive-by, las adiciones de hardware, las cuentas de dominio válidas, las cuentas locales válidas y los archivos adjuntos de spear phishing representaron el 10 % cada uno.

En todos los casos a los que X-Force respondió en Latinoamérica, Brasil representó el 67 %, Colombia el 17 % y México el 8 %. Perú y Chile se reparten el 8 % restante.

En Latinoamérica, Brasil representó el 67 % de los casos a los que respondió X-Force.

#5 | Medio Oriente y África

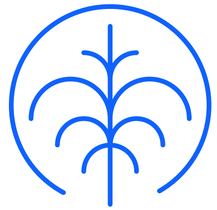
A efectos de información, IBM considera que Medio Oriente y África incluyen el Levante, la Península Arábiga, Egipto, Irán e Irak, y todo el continente africano.

El despliegue de puertas traseras se detectó en el 27 % de los casos a los que respondió X-Force en esta región en 2022. El ransomware y los virus empataron en el segundo puesto, con un 18 % cada uno. La extorsión y las pérdidas económicas representaron cada una la mitad de los impactos identificados en incidentes en toda la región en 2021.

Los enlaces de spear phishing se utilizaron para el acceso inicial en dos tercios de los casos, y los medios extraíbles representaron el otro tercio de los incidentes que corrigió X-Force en Medio Oriente y África. Las finanzas y los seguros fueron el sector más atacado en Medio Oriente y África en 2022, con un 44 % de los incidentes y un ligero descenso con respecto a 2021, con un 48 %. Los servicios profesionales, empresariales y de consumo representaron el 22 % de los ataques, y la manufactura y la energía empataron en el tercer lugar con un 11 %.

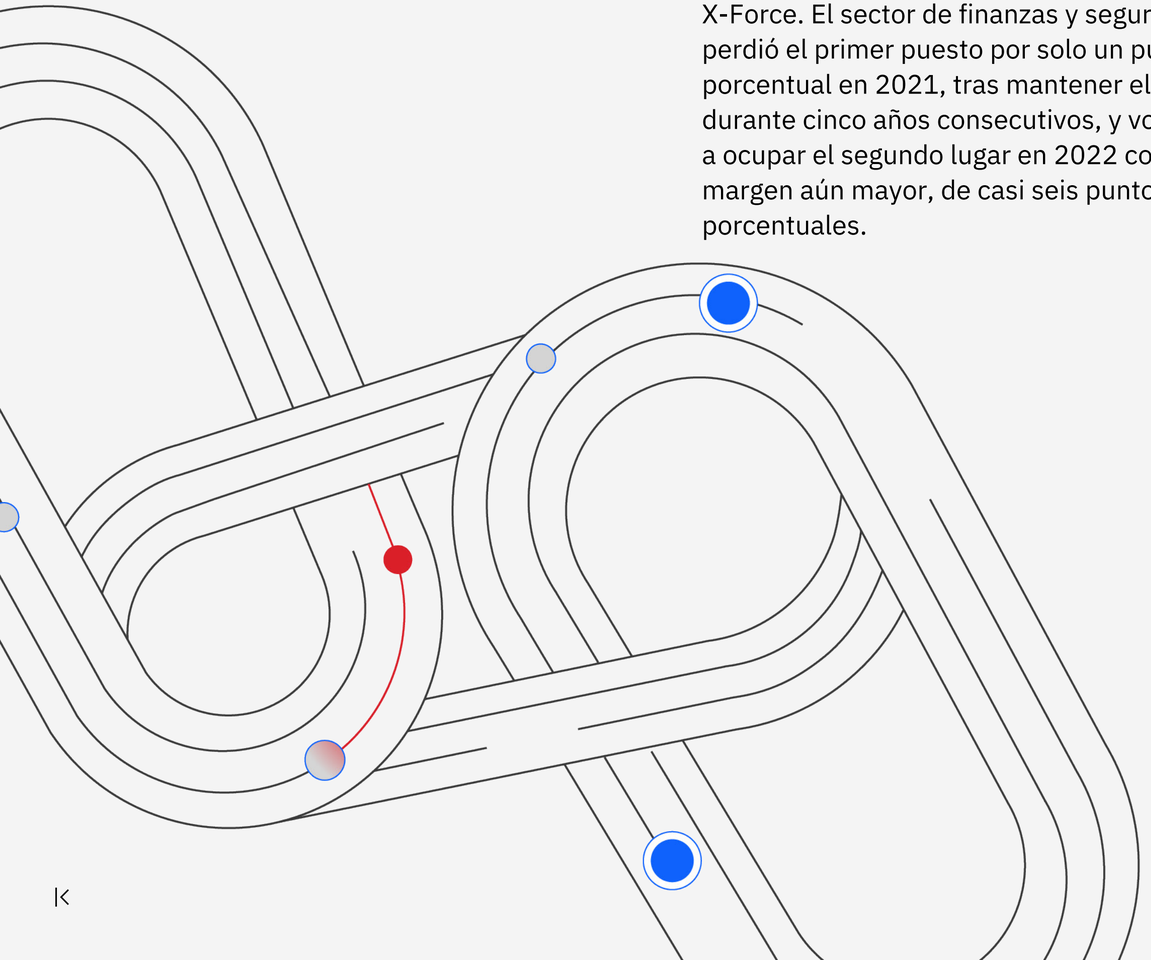
Arabia Saudita representó dos tercios de los casos de la región a los que respondió X-Force. Los casos restantes se repartieron entre Qatar, Emiratos Árabes Unidos y Sudáfrica.

El ataque más común en esta región fue el despliegue de puertas traseras en el 27 % de los casos.



Tendencias del sector

Por segundo año consecutivo, el sector de la manufactura fue el más atacado, según los datos de respuesta a incidentes de X-Force. El sector de finanzas y seguros perdió el primer puesto por solo un punto porcentual en 2021, tras mantener el título durante cinco años consecutivos, y volvió a ocupar el segundo lugar en 2022 con un margen aún mayor, de casi seis puntos porcentuales.



Proporción de ataques por industria 2018 - 2022

Industria	2022	2021	2020	2019	2018
Manufactura	24,8 %	23,2	17,7	8	10
Finanzas y seguros	18,9 %	22,4	23	17	19
Servicios profesionales, empresariales y para el consumidor	14,6 %	12,7	8,7	10	12
Energía	10,7 %	8,2	11,1	6	6
Venta minorista y mayorista	8,7 %	7,3	10,2	16	11
Educación	7,3 %	2,8	4	8	6
Asistencia sanitaria	5,8 %	5,1	6,6	3	6
Administración pública	4,8 %	2,8	7,9	8	8
Transporte	3,9 %	4	5,1	13	13
Medios de comunicación y telecomunicaciones	0,5 %	2,50	5,7	10	8

24,8 %

de los casos de respuesta a incidentes de X-Force se produjeron en el sector de manufactura.

#1 | Manufactura

La manufactura fue el sector más atacado y por un margen ligeramente superior al de 2021. En 2022, las puertas traseras se desplegaron en el 28 % de los incidentes, superando al ransomware, que apareció en el 23 % de los incidentes corregidos por X-Force. El porcentaje de despliegues de puertas traseras también se vio impulsado por el máximo de infecciones de Emotet. Algunos de estos casos podrían haber dado lugar a ataques de ransomware, entre otras actividades más maliciosas, pero se detectaron con la suficiente antelación para corregirlos.

Los archivos adjuntos de spear phishing y la explotación de aplicaciones de cara al público empataron en los dos primeros vectores de infección, con un 28 % cada uno. Los servicios remotos externos ocuparon el segundo lugar con un 14 %, mientras que los enlaces de spear phishing y las cuentas predeterminadas válidas empataron en el tercer lugar como acceso inicial en el 10 % de los casos.

La extorsión fue el principal impacto para las empresas de manufacturas, observada en el 32 % de los casos. Los fabricantes no toleran el tiempo de inactividad y esta intolerancia hace que la extorsión sea una estrategia lucrativa para los atacantes. El robo de datos fue el segundo más común, con un 19 % de los incidentes, seguido de las filtraciones de datos, con un 16 %. La región Asia Pacífico registró el mayor número de incidentes en el sector de manufactura, en aproximadamente el 61 % de los casos. Europa y América del Norte empatan en segundo lugar con un 14 %, mientras que Latinoamérica constituyó el 8 % y Medio Oriente y África el 4 %.

18,9 %

de los casos de respuesta a incidentes de X-Force se produjeron en el sector de finanzas y seguros.

#2 | Finanzas y seguros

Las compañías de finanzas y seguros representaron menos de uno de cada cinco ataques a los que respondió X-Force en 2022, lo que les valió el segundo lugar. Este porcentaje indica un ligero descenso en los últimos años, ya que otras sectores empezaron a atraer la atención de los atacantes, en particular la manufactura.

En comparación con otros sectores, las compañías de finanzas y seguros tienden a estar más avanzadas tanto en la transformación digital como en la adopción de la nube. Como resultado, es posible que los atacantes tengan que esforzarse más para llevar a cabo ataques exitosos contra estas empresas.

Los ataques de puerta trasera fueron la acción más comúnmente observada en el objetivo, con un 29 %, seguidos por el ransomware y los maldocs, con un 11 % cada uno. El principal vector de infección fueron los archivos adjuntos de spear phishing, los cuales se usaron en el 53 % de los ataques contra este sector. La explotación de aplicaciones de cara al público ocupó el segundo lugar, con un 18 % de los ataques, y los enlaces de spear phishing fueron el vector de acceso inicial en el 12 % de los casos.

Europa registró el mayor volumen de ataques contra compañías de finanzas y seguros, con aproximadamente el 33 % de todos los ataques, mientras que Asia Pacífico ocupó un cercano segundo lugar, con aproximadamente el 31 %. Latinoamérica experimentó aproximadamente el 15 % de los incidentes a los que respondió X-Force, mientras que América del Norte y Medio Oriente y África experimentaron aproximadamente el 10 % cada uno.

14,6 %

de los casos de respuesta a incidentes de X-Force se produjeron en el sector de los servicios profesionales, empresariales y de consumo.

#3 | Servicios profesionales, empresariales y de consumo

El sector de servicios profesionales incluye consultorías, empresas de gestión y bufetes de abogados. Estos servicios representan el 52 % de las víctimas en este segmento. Los servicios a las empresas, por el contrario, incluyen empresas como servicios informáticos y tecnológicos, relaciones públicas, publicidad y comunicaciones. Estos servicios representan el 37 % de las víctimas. Los servicios al consumidor, que engloban la construcción de viviendas, el sector inmobiliario, las artes, el ocio y el entretenimiento representaron el 11 % de los casos. Juntos, forman la categoría de servicios profesionales, empresariales y de consumo del Índice de inteligencia de amenazas de X-Force de 2023.

Los servicios profesionales, empresariales y de consumo experimentaron ataques de ransomware y de puertas traseras con mayor frecuencia, en un 18 % de los casos cada uno. Los dos principales vectores de infección fueron la explotación de aplicaciones de cara al público y los servicios remotos externos, con un 23 % cada uno. Los archivos adjuntos de spear phishing y las cuentas locales válidas fueron la causa del 15 % de los casos cada uno.

La extorsión fue el impacto más común en el 28 % de los casos, con el robo de datos, el robo de credenciales y la filtración de datos con el 17 % cada uno. X-Force respondió al 47 % de los casos en Europa, al 33 % en América del Norte, al 10 % en Asia Pacífico, al 7 % en Medio Oriente y África y al 3 % en Latinoamérica.

10,7 %

de los casos de respuesta a incidentes de X-Force se produjeron en el sector energético.

#4 | Energía

Las empresas del sector energético, incluidas las compañías eléctricas y las empresas petroleras y de gas, fueron el cuarto sector más atacado, igual que en 2021, y representaron el 10,7 % de los ataques. La explotación de una aplicación de cara al público fue el vector de infección más común, con un 40 %. Los enlaces de spear phishing y los servicios remotos externos representaron el 20 % de los casos cada uno. El uso de bots de redes fue la acción más frecuente en el objetivo en el 19 % de los casos, mientras que el ransomware y el BEC empataron en el segundo lugar con un 15 %.

El robo de datos y la extorsión se observaron en el 23 % de los casos, seguidos de la obtención de credenciales y las infecciones con bots de redes, con un 15 % cada una. En todos los casos a los que respondió X-Force en todo el mundo, las empresas norteamericanas fueron las víctimas más comunes, con un 46 % de los casos, en comparación con Europa y Latinoamérica, con un 23 % cada una, y algo menos del 5 % en Asia Pacífico y Medio Oriente y África.

El sector energético sigue sometido a la presión de diversas fuerzas mundiales, especialmente las exacerbadas por la guerra de Rusia en Ucrania y cómo esta ha afectado a un comercio energético mundial ya de por sí agitado.

8,7 %

de los casos de respuesta a incidentes de X-Force se produjeron en el sector minorista y mayorista.

#5 | Venta minorista y mayorista

Los minoristas son responsables de la venta de bienes a consumidores y mayoristas. Los mayoristas suelen encargarse del transporte y la distribución de estos bienes directamente desde los fabricantes a los minoristas o a los consumidores. El sector minorista y mayorista fue el quinto más atacado, según los datos de X-Force IR, igual que en 2021.

El vector de acceso inicial más común en los ataques a minoristas y mayoristas fueron los correos electrónicos de spear phishing con un enlace malicioso, con un 33 % de los casos. Los servicios remotos externos infectados, el spear phishing con archivos adjuntos maliciosos y las adiciones de hardware representaron el 17 % cada uno.

El ransomware, las puertas traseras y los BEC fueron las acciones más comunes de los atacantes, con un 19 % de las actividades cada una. Se identificaron virus en el 10 % de los casos. Las víctimas sufrieron extorsión en el 50 % de los casos, y robo de credenciales y pérdidas económicas en el 25 % cada uno. América del Norte y Latinoamérica registraron el mayor número de casos, con un 39 % cada una, frente al 22 % de Europa.

7,3 %

de los casos de respuesta a incidentes de X-Force se produjeron en el sector educativo.

#6 | Educación

El 20 % de los ataques a los que respondió X-Force eran casos de puertas traseras. El ransomware, el adware y los correos no deseados representaron el 13 % cada uno. La explotación de aplicaciones de cara al público fue el acceso inicial más comúnmente observado en el 42 % de los casos, seguido de los archivos adjuntos de spear phishing en el 25 %. El phishing a través de servicios, de enlaces y el abuso de cuentas locales y en la nube válidas constituyeron el 8 % de los vectores de acceso iniciales cada uno. El robo y la fuga de datos, así como la extorsión y el reconocimiento, fueron los puntos de impacto con un 25 % cada uno. Asia Pacífico representó el 67 % de los casos, América del Norte el 27 % y Latinoamérica el 6 %.

5,8 %

de los casos de respuesta a incidentes de X-Force se produjeron en el sector sanitario.

#7 | Atención médica

El sector de la salud retrocedió al séptimo lugar entre las 10 principales industrias, descendiendo aún más desde el sexto lugar que ocupaba en 2021. La proporción de casos en la atención médica a los que ha respondido X-Force se mantuvo en torno al 5 % o 6 % en los últimos tres años. Se produjeron ataques de puerta trasera en el 27 % de los casos, y web shells en el 18 %. Adware, BEC, criptomineros, cargadores, herramientas de reconocimiento y escaneado y herramientas de acceso remoto representaron el 9 % cada uno. Los casos de reconocimiento constituyeron la mayor parte de los impactos observados, con un 50 %, mientras que el robo de datos y la minería de monedas digitales se identificaron en un 25 % de los casos cada uno.

Los objetivos con sede en Europa representaron el 58 % de los incidentes, mientras que los casos en América del Norte representaron el 42 % restante.

4,8 %

de los casos de respuesta a incidentes de X-Force se produjeron en el sector gubernamental.

#8 | Gobierno

Los objetivos gubernamentales fueron otro de los principales objetivos de las puertas traseras, con un 25 % de los casos de IR de X-Force. Este porcentaje empató con los ataques DDoS, que también representaron una cuarta parte de los casos. La valiosa información confidencial de las redes del sector público es un objetivo habitual de las campañas de ciberespionaje. Esta información puede incluir extensas bases de datos de información personal e información de otro tipo que podría ser utilizada por grupos patrocinados por el estado o vendida con fines lucrativos por ciberdelincuentes. Los maldocs fueron identificados en el 17 % de los casos, mientras que los criptomineros, las herramientas de obtención de credenciales, el ransomware y los web shells se repartieron el resto de los casos con un 83 %.

Entre los casos en este sector, X-Force pudo relacionar los incidentes con ciberdelincuentes, amenazas internas que provocaron la destrucción de datos, acciones de hackers y grupos de amenazas patrocinados por el estado que realizan espionaje, cada uno de ellos en la misma proporción.

La explotación de las aplicaciones de cara al público y los archivos adjuntos de spear phishing fueron los principales vectores de infección, con un 40 % cada uno, mientras que el abuso de cuentas válidas predeterminadas representó un 20 % de los casos. Las entidades gubernamentales de Asia Pacífico fueron las más afectadas, con un 50 % de los casos. Le siguieron Europa con un 30 % y América del Norte con un 20 %.

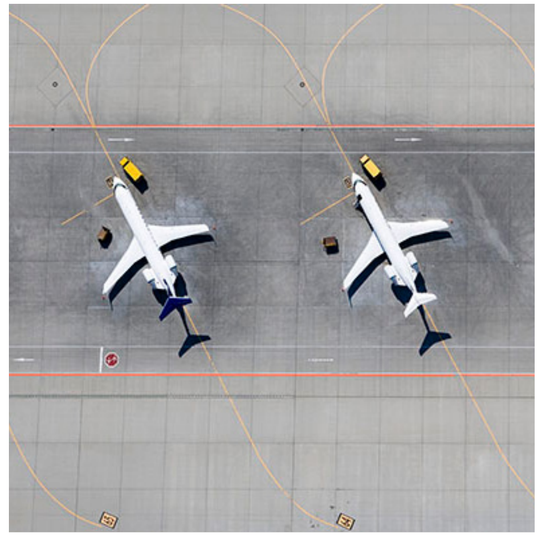
3,9 %

de los casos de respuesta a incidentes de X-Force se produjeron en el sector del transporte.

#9 | Transporte

El transporte, que se encontraba en el séptimo lugar en 2021, ha vuelto al noveno lugar, el cual ocupaba en 2020. Sin embargo, el sector siguió representando aproximadamente el mismo porcentaje de incidentes a los que respondió X-Force. El phishing fue el vector de acceso inicial más común en el 51 % de los casos, dividido a partes iguales entre enlaces, archivos adjuntos y spear phishing como servicio. El abuso de cuentas locales válidas constituyó el 33 % de los vectores de acceso iniciales, y las cuentas válidas en la nube sirvieron de punto de entrada en el 17 % de los casos. Las principales acciones sobre los objetivos fueron el acceso a servidores y el uso de herramientas de acceso remoto, con un 25 % cada una, seguidas de campañas de spam, ransomware, puertas traseras y supresión en un 13 % de los casos cada una.

El robo de datos fue el más común en el 50 % de los casos, con la extorsión y los impactos en la reputación de la marca en el 25 % cada uno. Las entidades de transporte europeas fueron el grupo más afectado, con un 62 % de los casos, y Asia Pacífico ocupó el segundo lugar, con un poco más del 37 %.



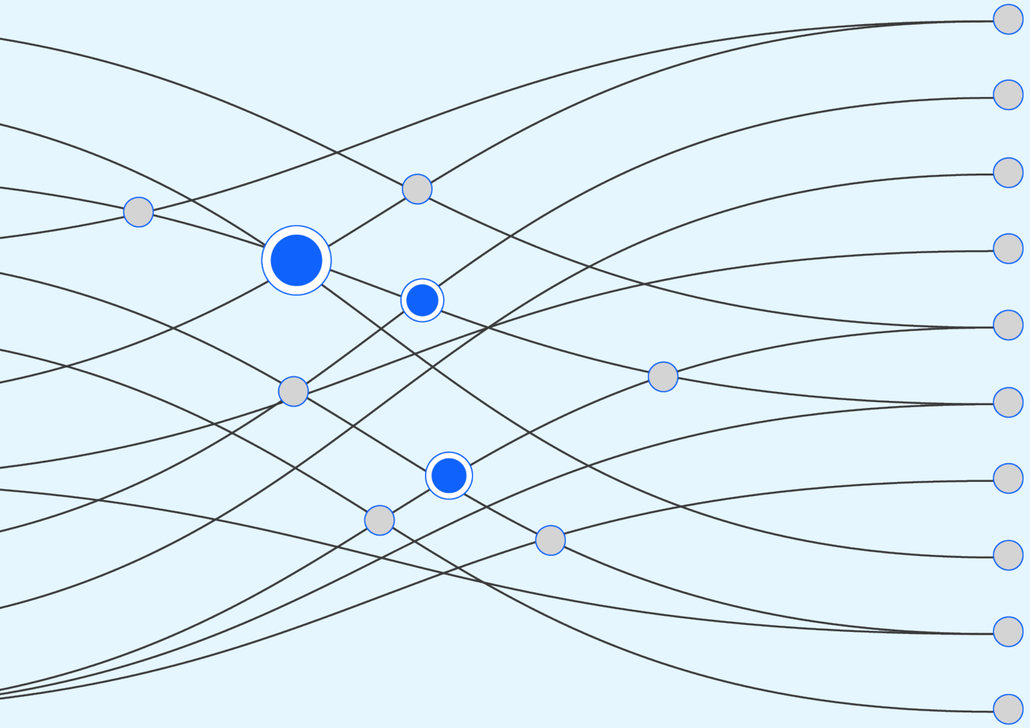
0,5 %

de los casos de respuesta a incidentes de X-Force se produjeron en el sector de los medios de comunicación y las telecomunicaciones.

#10 | Medios de comunicación y telecomunicaciones

Los medios de comunicación y las telecomunicaciones representaron una pequeña fracción de los incidentes a los que respondió X-Force y ocuparon el último lugar por segundo año consecutivo. El abuso de servicios remotos externos, como VPN y otros mecanismos de acceso, así como de cuentas de dominio válidas, fueron los vectores de infección observados. Estos vectores dieron lugar a ataques de ransomware. Las acciones observadas en estos casos incluyeron el despliegue de ransomware y herramientas de exfiltración de datos. Estas acciones, a su vez, condujeron al robo, a la filtración, destrucción y extorsión de datos.

Recomendaciones



Las siguientes recomendaciones son medidas que usted debería tomar para proteger su empresa contra amenazas maliciosas, lo cual incluye las presentadas en este informe.

Gestione sus activos: “¿Qué tenemos? ¿Qué defendemos? ¿Qué datos son críticos para nuestra empresa?” Estas son las primeras preguntas que cualquier equipo de seguridad debe responder para construir una defensa eficaz. Dar prioridad al descubrimiento de activos en su perímetro, comprender su exposición a los ataques de phishing y reducir esas superficies de ataque contribuyen aún más a la seguridad holística. Por último, las empresas deben ampliar sus programas de gestión de activos para incluir el código fuente, las credenciales y otros datos que ya podrían existir en Internet o en la dark web.

Conozca a su adversario: Mientras que muchas empresas tienen una visión amplia del panorama de las amenazas, X-Force les recomienda que adopten una visión que haga énfasis en los agentes de amenazas específicas que tienen más probabilidades de dirigirse a su sector, organización y geografía. Esta perspectiva abarca comprender cómo operan los atacantes, identificar su nivel de sofisticación y saber cuáles son las tácticas, técnicas y los procedimientos que suelen emplear.

Gestione la visibilidad: Tras conocer mejor a los adversarios con más probabilidades de atacar, las empresas deben confirmar que disponen de la visibilidad adecuada de las fuentes de datos que indicarían la presencia de un atacante. Mantener la visibilidad en los puntos clave de toda la empresa y garantizar que las alertas se generen a tiempo y, como consecuencia, se actúe rápidamente, es fundamental para detener a los atacantes antes de que puedan causar daños.

Desafíe las suposiciones: Las empresas deben asumir que su seguridad ya ha sido comprometida. Al hacerlo, los equipos pueden reexaminar en forma continua:

- Cómo pueden infiltrarse los atacantes en sus sistemas
- Cuál es su capacidad de detección y respuesta frente a tácticas, técnicas y procedimientos emergentes.
- El nivel de dificultad para que un probable adversario ponga en riesgo sus datos y sistemas más críticos.

Los equipos de seguridad eficaces llevan a cabo pruebas ofensivas con regularidad que incluyen la caza de amenazas, las pruebas de penetración y de equipo rojo basado en objetivos para detectar o validar rutas de ataque oportunistas en sus entornos.

Actúe de forma inteligente: Implemente la inteligencia de amenazas en todas partes. La aplicación eficaz de la inteligencia sobre amenazas le permitirá analizar las rutas de ataque habituales e identificar oportunidades clave para mitigar ataques comunes, además de permitirle desarrollar oportunidades de detección de alta fidelidad. La aplicación de la inteligencia de amenazas debe ir acompañada de la comprensión de sus adversarios y de cómo operan.

Prepárese: Los ataques son inevitables, pero el fracaso no tiene por qué serlo. Las empresas deben desarrollar planes de respuesta a incidentes personalizados para su entorno. Estos planes deben aplicarse y modificarse periódicamente a medida que cambia la empresa, centrándose en mejorar los tiempos de respuesta, corrección y recuperación.

Contar con un proveedor de IR de confianza reduce el tiempo que se tarda en conseguir que el personal de respuesta especializado se centre en mitigar un ataque. Además, incluir a su proveedor de IR en el desarrollo y las pruebas del plan de respuesta es fundamental y contribuye a una respuesta más eficaz y eficiente. Los mejores planes de IR incluyen una respuesta transversal a lo largo de la empresa, incorporan a partes interesadas ajenas a la TI y ponen a prueba las líneas de comunicación entre los equipos técnicos y los altos directivos. Por último, poner a prueba su plan en un ejercicio de rango cibernético de inmersión y alta presión puede mejorar enormemente su capacidad de respuesta ante un ataque.

Aumente la seguridad con estas medidas:

- ☐ Gestione sus activos
- ☐ Conozca a su adversario
- ☐ Gestione la visibilidad
- ☐ Desafíe las suposiciones
- ☐ Actúe de forma inteligente
- ☐ Prepárese

Quiénes somos

IBM Security X-Force

IBM Security X-Force es un equipo de hackers, especialistas en respuesta a ataques, investigadores y analistas centrado en las amenazas. El portafolio de X-Force incluye productos y servicios ofensivos y defensivos, diseñados a partir de un enfoque de 360 grados de las amenazas.

En una era plagada de ciberataques permanentes, un todo conectado y crecientes mandatos normativos, las empresas necesitan un enfoque centrado en la seguridad. X-Force cree que la amenaza debería ser el punto focal. A través de pruebas de penetración, gestión de vulnerabilidades y servicios de simulación de adversarios, el equipo de hackers de X-Force Red asume el papel de agentes de amenazas para encontrar vulnerabilidades de seguridad, exponiendo sus activos más importantes. Gracias a los servicios de preparación, detección y respuesta ante incidentes y gestión de crisis, el equipo de respuesta ante incidentes de X-Force sabe dónde pueden esconderse las amenazas y cómo detenerlas. Los investigadores de X-Force crean técnicas de ataque para detectar y prevenir amenazas, mientras que los analistas de X-Force recopilan datos sobre amenazas que luego traducen a información útil para reducir riesgos.

Al contar con conocimientos profundos sobre cómo piensan, trazan sus estrategias y atacan los agentes de amenazas, X-Force puede ayudarle a evitar, detectar, responder y recuperarse de los incidentes, para que usted pueda centrarse en las prioridades de su empresa.

Si su empresa necesita ayuda para reforzar su postura de seguridad, programe una consulta personalizada con un experto de IBM Security X-Force.

Programe una consulta →

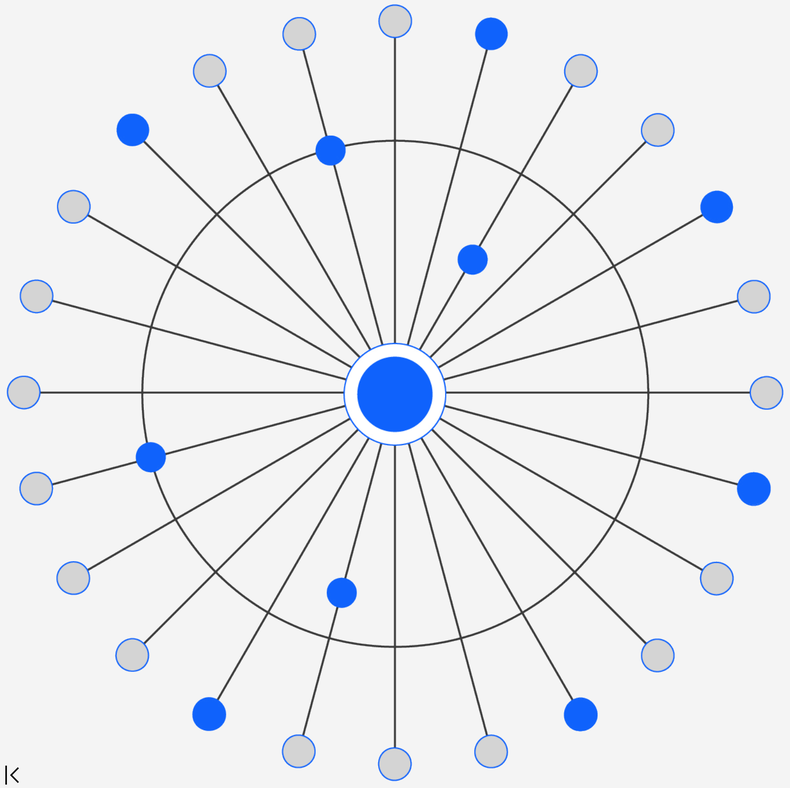
IBM Security

IBM Security se adapta a su huella en constante expansión y trabaja con usted para que pueda seguir avanzando de forma segura. Ayudamos a su empresa para ir siempre un paso adelante, con mayor rapidez y precisión, gracias a nuestras capacidades dinámicas de IA y automatización. No dude de estar tomando las decisiones correctas hoy y mañana con la información de nuestro equipo de confianza de expertos líderes del sector. Desde predecir amenazas hasta proteger los datos; trabajar con distintos proveedores o en todo el mundo; independientemente de hacia dónde se dirija su empresa, IBM Security puede ayudarle a alcanzar ambiciosos objetivos empresariales, mientras explora nuevas tecnologías esenciales y ayuda a minimizar las amenazas inesperadas.

Más información →

14

Colaboradores



Michael Worley
Christopher Caridi
Michelle Alvarez
Karlina Bakken
Yannick Bedard
Michele Brancati
Christopher Bedell
Joshua Chung
Scott Craig
Joseph DiRe
John Dwyer
Emmy Ebanks
Richard Emerson
Charlotte Hammond
Kevin Henson
Guy-Vincent Jourdan
Vio Onut
Mitch Mayne
Dave McMillen
Kat Metrick
Scott Moore
Golo Mühr
Andy Piazza
Benjamin Shipley
Christopher Thompson
Ole Villadsen
Reginald Wong
John Zorabedian

15

Apéndice

Lista de impactos

Impactos	Impactos
Robots de redes	Minería de monedas digitales
Reputación de marca	Espionaje
Obtención de credenciales	Extorsión
Destrucción de datos	Pérdida financiera
Fuga de datos	Paralización de la producción (OT)
Robo de datos	Reconocimiento

1. “A timeline of the biggest ransomware attacks”, CNET, 15 de noviembre de 2021
2. “International action against DD4BC cybercriminal group”, Europol, 12 de enero de 2016
3. “DD4BC, Armada Collective, and the Rise of Cyber Extortion”, Recorded Future, 7 de diciembre de 2015
4. “A Brief History of Ransomware”. Varonis, 10 de noviembre de 2015
5. “Inside Chimera Ransomware - the first ‘doxingware’ in wild”, MalwardBytes Labs, 8 de diciembre de 2015
6. “Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware”, Crowdstrike, 14 de noviembre de 2018
7. “Operators of SamSam Continue to Receive Significant Ransom Payments”, Crowdstrike, 11 de abril de 2018
8. “Triple Extortion Ransomware: The DDoS Flavour”, PacketLabs, 12 de mayo de 2022
9. “They Told Their Therapists Everything. Hackers Leaked It All”, Wired, 4 May 2021
10. “BazarCall to Conti Ransomware via Trickbot and Cobalt Strike”, The DFIR Report, 1 de agosto de 2021
11. “Diavol Ransomware”, The DFIR Report, 13 de diciembre de 2021
12. “Quantum Ransomware”, The DFIR Report, 25 de abril de 2022
13. “Bumblebee Loader Linked to Conti and Used In Quantum Locker Attacks”, Kroll, 6 de junio de 2022
14. “This isn’t Optimus Prime’s Bumblebee but it’s Still Transforming”, Proofpoint, 28 de abril de 2022
15. “Understanding REvil: REvil Threat Actors May Have Returned (Updated)”, Unit 42, 3 de junio de 2022
16. “AdvIntel’s State of Emotet aka ‘SpmTools’ Displays Over Million Compromised Machines Through 2022”, AdvIntel, 13 de septiembre de 2022
17. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack”, NCC Group, 19 de agosto de 2022
18. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack” NCC Group, 19 de agosto de 2022

Alfonso Nápoles Gandara 3111
Col. Parque corporativo de Peña Blanca
C.P. 01210
México D.F.

Producido en los Estados Unidos de América
Febrero de 2023

Este documento se actualizó por última vez en la fecha inicial de publicación e IBM puede modificarlo en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.