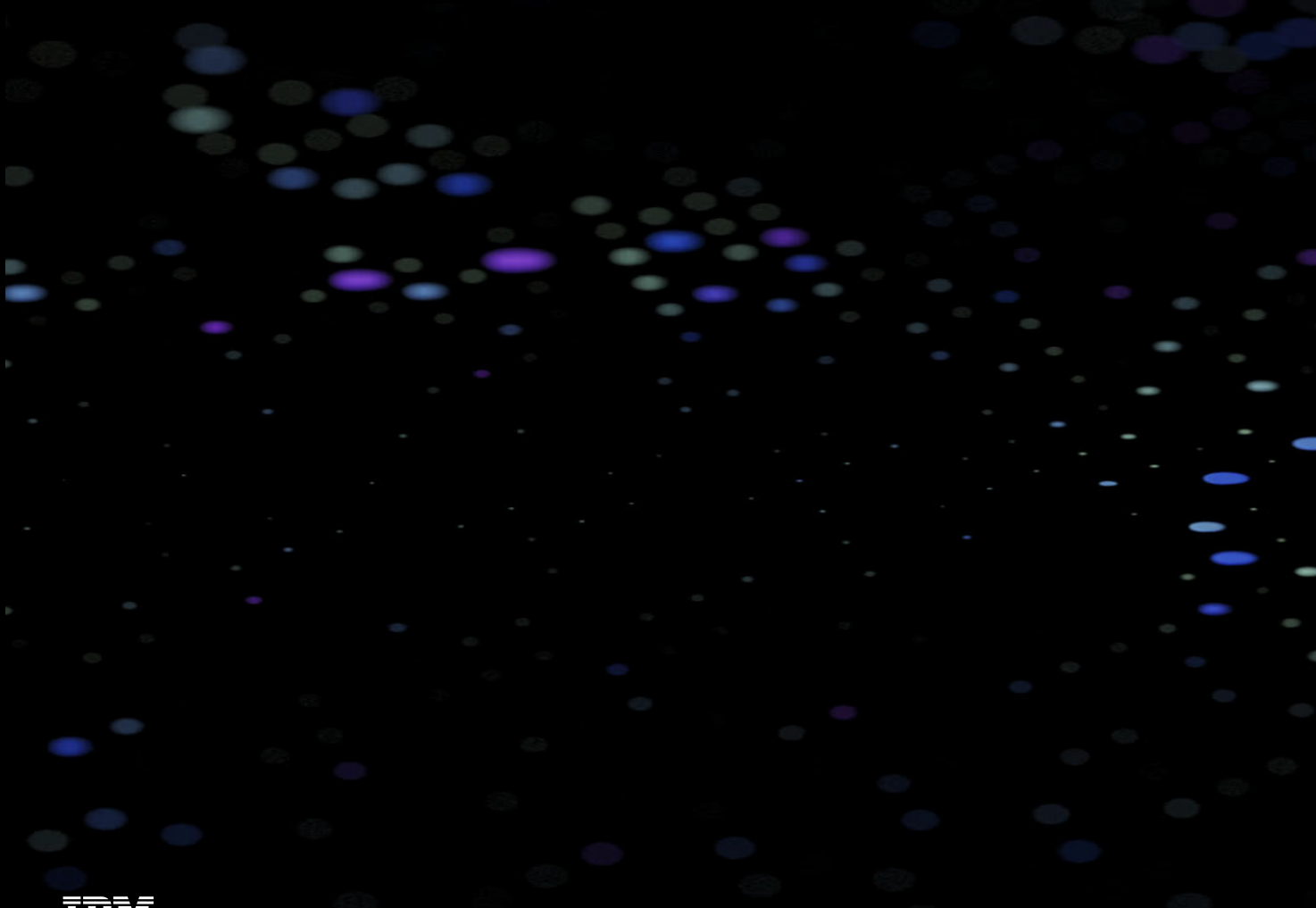
IBM Security

# X-Force Threat Intelligence Index 2020



IBM

Producido por Servicios de Inteligencia y Respuesta ante Incidentes X-Force de IBM (IRIS)

# Tabla de contenidos

# Tabla de contenidos

# Resumen y tendencias clave

## IBM Security emplea soluciones y servicios de seguridad empresarial de inteligencia para que su negocio genere resiliencia hoy ante las amenazas de seguridad cibernéticas del mañana.

A fin de actualizar a los profesionales de seguridad sobre las amenazas más relevantes, con frecuencia IBM® X-Force® lanza blogs, documentos, seminarios web y podcasts acerca de amenazas emergentes así como de tácticas, técnicas y procedimientos (TTP) de los atacantes.

Una vez al año, IBM Security® lanza el IBM X-Force Threat Intelligence Index, que resume el año anterior en términos de las amenazas más destacadas informadas por nuestros diferentes equipos de investigación a fin de proporcionarles a los equipos de seguridad información que puede ayudarles a mejorar la seguridad en sus organizaciones.

Los datos y la información que se presentan en este informe provienen de los servicios de seguridad administrada, servicios de respuesta ante incidentes, actividades de prueba de penetración y servicios de administración de vulnerabilidad de IBM Security.

Los equipos de investigación de IBM X-Force analizan datos de cientos de millones de puntos de conexión y servidores protegidos, junto con datos que se derivan de activos que no pertenecen a clientes, tales como sensores de spam y redes de vulnerabilidad intencional. IBM Security Research también ejecuta trampas para spam en todo el mundo y monitorea decenas de millones de spam y ataques de phishing diariamente, analizando miles de millones de páginas web e imágenes para detectar campañas de ataque, actividad fraudulenta y abuso de marca, a fin de proteger mejor a nuestros clientes y al mundo conectado en el que vivimos.

# X-Force Incident Response and Intelligence Services (IRIS) compiló análisis de servicios de seguridad y software de IBM Security del año pasado, que mostraron que en 2019 volvieron a surgir antiguas amenazas que se utilizaron de nuevas maneras.

— Según los datos de X-Force, un aumento del 2000 % en incidentes dirigidos a la tecnología operativa (OT) en 2019 podría presagiar un aumento de interés por parte de los actores amenazantes en atacar sistemas industriales a medida que ingresamos a 2020.

— En 2019 se afectaron más de 8,5 mil millones de registros, un 200 % más que la cantidad de registros perdidos en 2018. El invasor inadvertido puede ser en gran parte responsable por este significativo aumento. Los registros expuestos a causa de servidores mal configurados (incluido el almacenamiento en la nube de acceso público, las bases de datos en la nube inseguras y las copias de seguridad de rsync indebidamente aseguradas, o dispositivos de almacenamiento en áreas de redes conectadas a internet abierta) representaron el 86 % de los registros afectados en 2019.

— El panorama de malware cambió en 2019, cuando los actores amenazantes regresaron al ransomware y a la generación de botnets. Durante 2019, X-Force IRIS respondió a acciones de ransomware en 12 países diferentes, en 5 continentes diferentes y en 13 industrias diferentes. Además, la actividad de malware destructivo muestra que esta tendencia de malware potencialmente catastrófico sigue siendo una creciente amenaza.

— Los principales tres vectores de infección inicial que se observaron en las acciones de X-Force IRIS de 2019 fueron muy parejos entre sí: Phishing (31 %), escaneo y explotación (30 %) y credenciales robadas (29 %). El phishing, más notablemente, pasó de conformar casi la mitad de los incidentes totales de 2018 a menos de un tercio en 2019. Por el contrario, el escaneo y la explotación de vulnerabilidades aumentaron hasta casi un tercio de los incidentes, siendo que en 2018 solo representaban un 8 %.

— El análisis de X-Force de actividad de spam global indica que el correo electrónico del spam continúa usando un subconjunto de vulnerabilidades, con un enfoque particular en solo dos CVE: 2017-0199 y 2017-11882. Estas dos son vulnerabilidades emparchadas que han representado casi el 90 % de las vulnerabilidades que los actores amenazantes intentaban explotar a través de campañas de spam.

— Si bien los servicios financieros siguieron siendo el sector más atacado en 2019, el ataque específico a la industria destacó un cambio de prioridades por parte de los actores amenazantes, dado que la venta minorista, los medios, la educación y el gobierno subieron en la tabla global de los sectores más atacados.

— Este año, el X-Force Threat Intelligence Index incorporó la información geocéntrica, que proporciona datos sobre las tendencias observadas de todo el mundo. IBM Security continúa rastreando a múltiples actores amenazantes que atacan en todas las geografías, y este informe destaca a los actores amenazantes clave de cada región, los ataques observados desde 2019, y las potenciales fechas de interés para la seguridad cibernética en 2020.

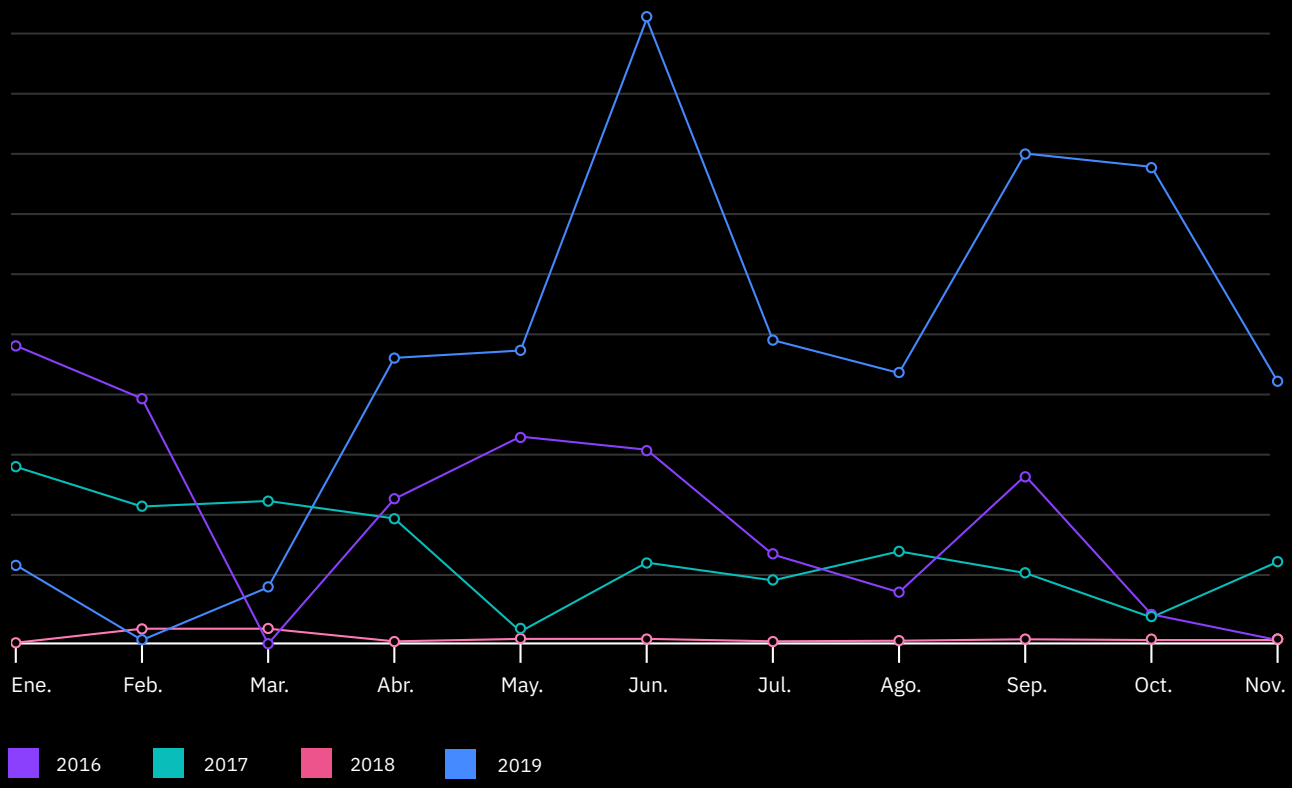
Las siguientes secciones de este informe anual pasan por las tendencias de mayor nivel y desglosan la información sobre lo qué les dio forma en 2019.

# Ataques y vectores de infección iniciales

**Figura 1:**

## Tendencias de ataques a la tecnología operativa (OT)

Volumen de ataque mensual a OT, comparación entre los años 2016-2019 (Fuente: IBM X-Force)




### Crecimiento explosivo de los ataques a la infraestructura de la tecnología operativa (OT)

Los datos de IBM X-Force indican que los eventos en los que los actores amenazantes atacaron sistemas de control industrial (ICS) y activos de tecnología operativa (OT) similares aumentaron más del 2000 % desde 2018. De hecho, la cantidad de eventos en que se atacaron activos de OT en 2019 fue superior al volumen de actividad observado en los últimos tres años.

La mayoría de los ataques observados se centraron en el uso de una combinación de vulnerabilidades conocidas dentro de los componentes de hardware de SCADA e ICS, así como ataques de pulverización de contraseñas utilizando tácticas de acceso de fuerza bruta contra objetivos de ICS.

Algunas actividades informadas centradas en ataques a ICS se han asociado con dos conocidos actores amenazantes, y coincidieron con la intensificación en la línea de tiempo de ataques que observamos en nuestra telemetría. Se llevaron a cabo dos campañas específicas por medio del grupo Xenotime y de IBM Hive0016 (APT33) quienes según se informa ampliaron sus ataques en objetivos de ICS.

La superposición entre la infraestructura de TI y la OT, como los Controladores de lógica programables (PLC) y ICS, siguieron siendo un riesgo para las organizaciones que dependían de dichas infraestructuras híbridas en 2019.

La convergencia de la infraestructura de TI/OT permite que las vulneraciones de TI apunten contra dispositivos de OT y controlen sus activos físicos, que pueden aumentar en gran medida el costo de recuperación. Por ejemplo, a principios de 2019, IBM X-Force IRIS ayudó a responder ante una vulneración en una empresa de manufactura global, donde una infección de ransomware que comenzó en un sistema de TI luego se trasladó lateralmente hasta la infraestructura de OT y detuvo las operaciones de la planta. El ataque afectó no solo las operaciones de la propia empresa, sino también provocó un efecto dominó en los mercados globales.

Las evaluaciones de seguridad de X-Force IRIS que se ofrecieron a nuestros clientes en 2019 destacaron la vulnerabilidad de los sistemas de OT, que suelen usar software y hardware heredados. Mantener sistemas de producción que ya no pueden ser actualizados con patches y están repletos de antiguas vulnerabilidades que ya se han tornado públicas implica que incluso si los sistemas de OT no están expuestas a internet, los sistemas de OT sin protección podrían ser una presa fácil. En caso de desplazamiento lateral, una vez que un atacante gana el primer paso, se puede acceder fácilmente a estos sistemas desde el interior de la red y se los puede dañar con técnicas de explotación relativamente simples.

Si bien la tendencia de ataques a la red de los ICS que se muestra en la Figura 1 se ha ido reduciendo desde inicio de octubre de 2019, X-Force espera que los ataques contra los objetivos OT/ICS continúen aumentando en 2020, dado que varios actores amenazantes planean lanzar nuevas campañas contra las redes industriales en todo el mundo. Con más de 200 nuevos CVE relacionados con ICS lanzados en 2019, la base de datos de vulnerabilidades de IBM X-Force muestra que es posible que las amenazas para ICS sigan aumentando en 2020.

X-Force prevé que los ataques contra los objetivos de ICS seguirán aumentando en 2020, dado que varios actores amenazantes planean lanzar nuevas campañas contra redes industriales en todo el mundo.

**Los registros infringidos crecen drásticamente**

La cantidad de registros infringidos aumentó significativamente en 2019 cuando más de 8,5 mil millones de registros quedaron expuestos, tres veces más que en 2018 comparando año con año. El principal motivo de este significativo crecimiento es que los registros expuestos por configuraciones deficientes aumentaron casi diez veces interanualmente. Estos registros conforman el 86 % de los registros afectados en 2019. Este es un claro desvío de lo que informamos en 2018 cuando observamos una disminución del 52 % desde 2017 en los registros expuestos debido a configuraciones deficientes y estos registros conformaban menos de la mitad de los registros totales.

Notablemente, en realidad hubo una disminución en la cantidad de incidentes por configuraciones deficientes en 2019 del 14 % interanual. Este hecho implica que cuando efectivamente hubo una vulneración por configuración deficiente, la cantidad de registros afectados fue significativamente superior en 2019. Casi tres cuartos de las vulneraciones en las que hubo más de 100 millones de registros afectados fueron incidentes con configuraciones deficientes. En dos de esos incidentes de configuración deficiente que ocurrieron en el sector de servicios profesionales, el recuento de registros expuestos fue de miles de millones por cada incidente.

Este aumento significativo de los registros perdidos entre las industrias destaca el mayor riesgo de las vulneraciones de datos, incluso para las organizaciones de sectores que generalmente no se consideraban objetivos primarios.

Registros vulnerados en 2019

# 8,5 mil millones

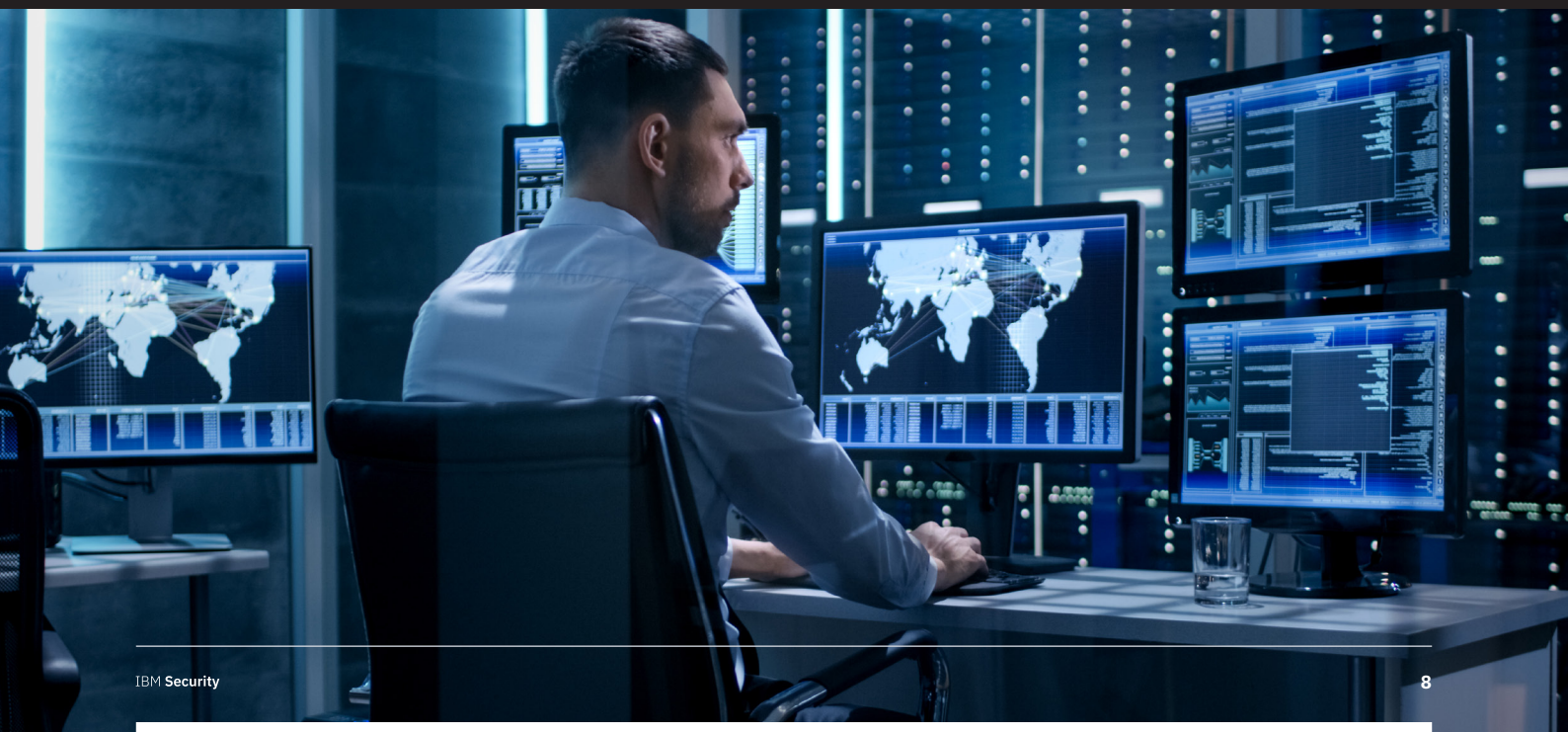
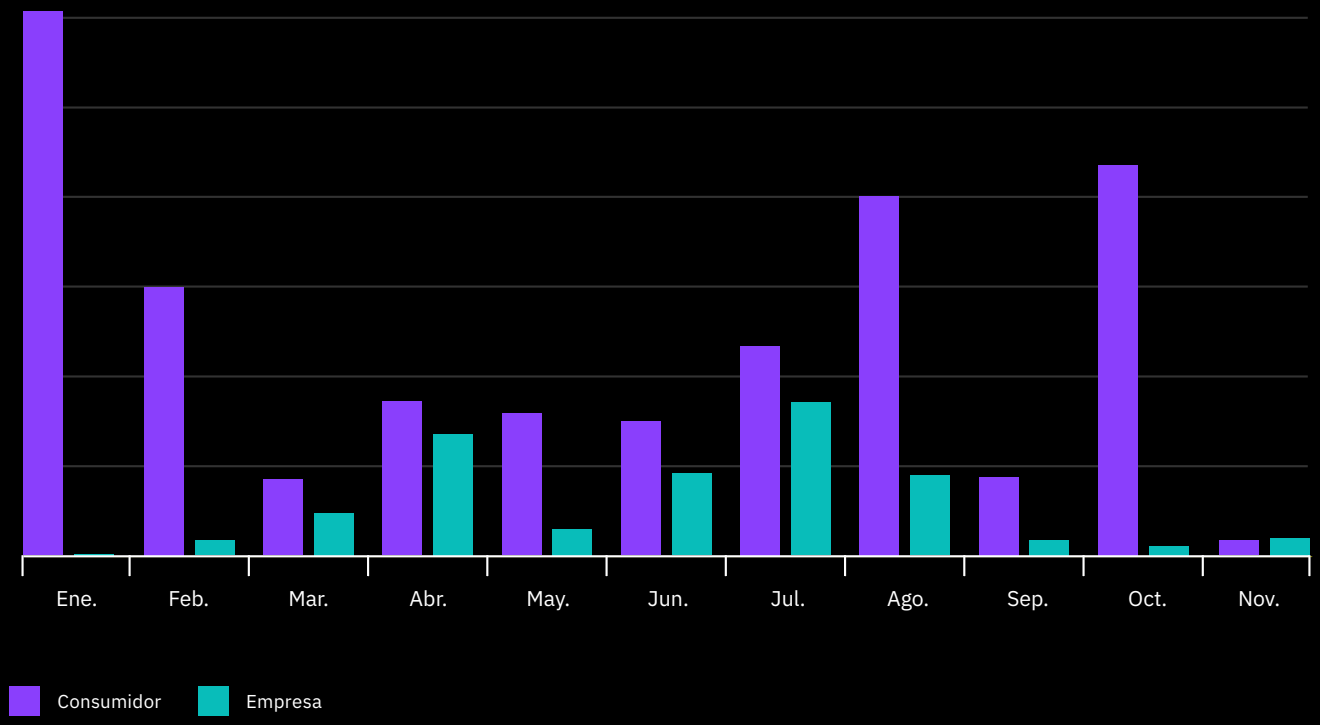


**Figura 2:**

## Ataques a consumidores en comparación con ataques a empresas

Volumen mensual de ataques a consumidores en comparación con ataques a empresas en 2019 (Fuente: IBM X-Force)




**Los ataques a los dispositivos de IoT incluyen los ámbitos empresariales**

Con más de 38 mil millones de dispositivos que se prevé que estarán conectados a internet en 2020, el panorama de amenazas de la internet de las cosas (IoT) se ha estado formando en forma gradual para ser uno de los vectores de amenazas que pueden afectar las operaciones tanto a nivel del consumidor como empresarial utilizando malware relativamente simple y ataques automatizados generalmente generados por script.

Dentro de la esfera de código malicioso que se utiliza para infectar dispositivos de IoT, la investigación de IBM X-Force ha rastreado múltiples campañas de malware Mirai en 2019 que han cambiado notablemente y pasaron de atacar productos electrónicos de consumidores a atacar hardware de nivel empresarial, actividad que no se observaba en 2018. Los atacantes pueden usar los dispositivos afectados con acceso a la red como punto de giro en potenciales intentos por establecer su posición en la organización.

Mirai es un malware de IoT prolífico que varios atacantes han utilizado desde 2016 para provocar una interrupción masiva al infectar grandes cantidades de dispositivos de IoT y usarlos en ataques de denegación del servicio distribuido (DDoS). En nuestro análisis de las campañas de 2019, hemos descubierto que los TTP de quienes manejaron el malware Mirai han cambiado notablemente desde 2018, y en 2019 se centraron en atacar hardware empresarial además de productos electrónicos de consumidores.

Analizando los ataques que afectaron a los dispositivos de IoT en 2019, hemos observado el uso generalizado de ataques por inyección de órdenes (CMDi) que contenían instrucciones de descargar cargas dañinas maliciosas dirigidas a varios tipos de dispositivos de IoT. La mayoría de estos ataques por inyección se realizan de manera automática por scripts que escanean e intentan infectar dispositivos en masa. Si el dispositivo de IoT a atacar es susceptible a estos ataques de inyección, la carga dañina se descarga y se ejecuta, y envía de manera efectiva el dispositivo a una gran botnet de IoT. Uno de los facilitadores más comunes de estos ataques son los dispositivos de IoT con contraseñas débiles o predeterminadas que se pueden adivinar fácilmente mediante un humilde ataque de diccionario.

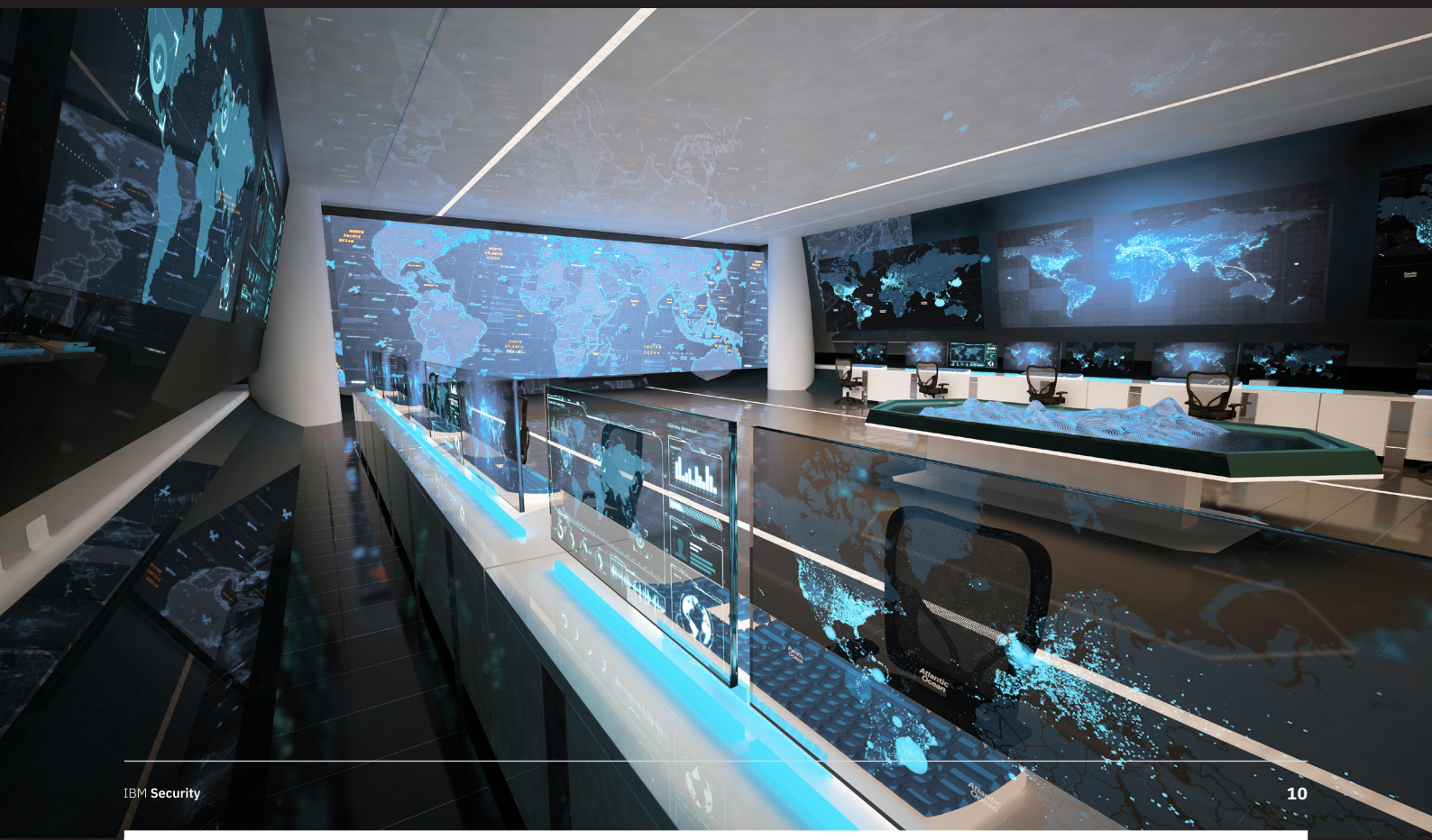
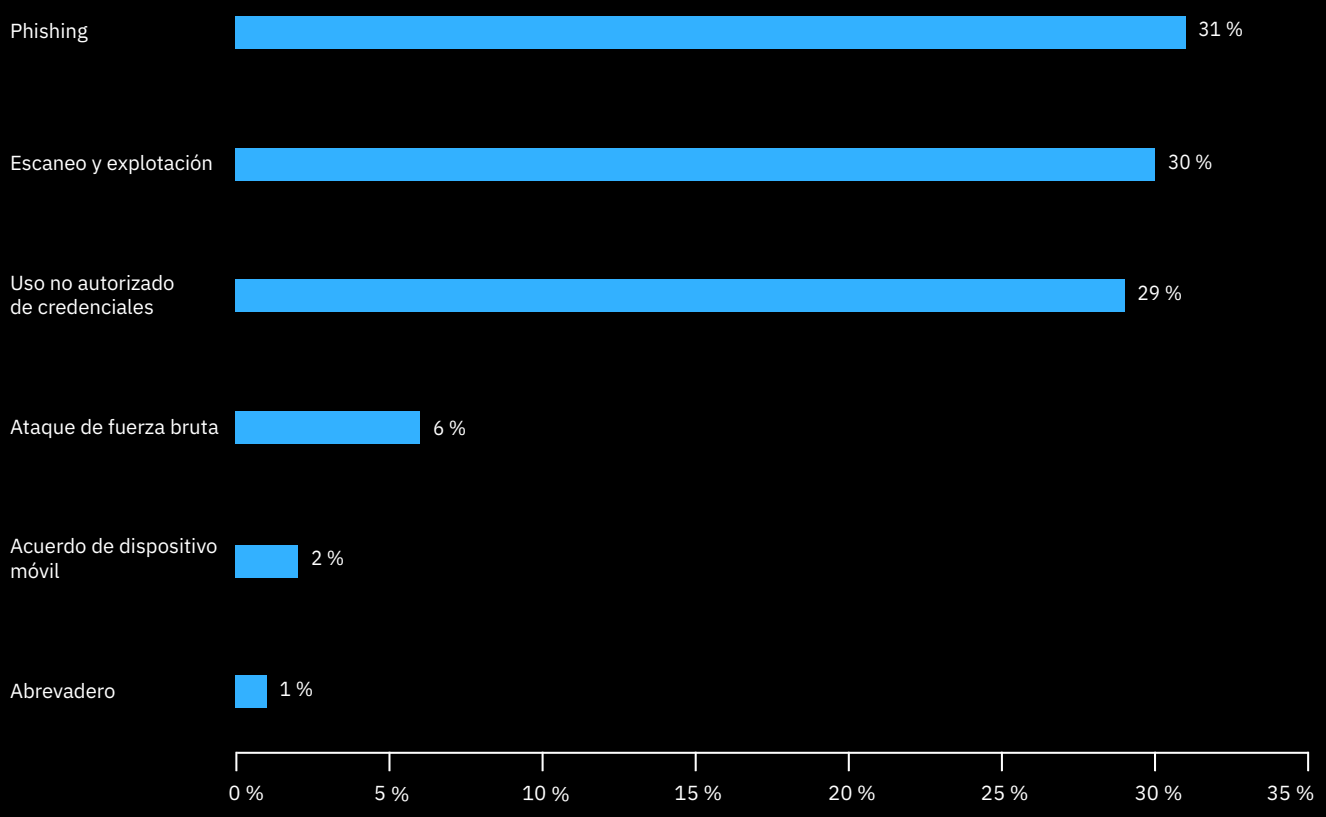


**Figura 3:**

## Principales vectores de acceso inicial

Desglose de los principales 6 vectores en ataques iniciales en 2019, como porcentaje de los seis vectores de acceso (Fuente: IBM X-Force)

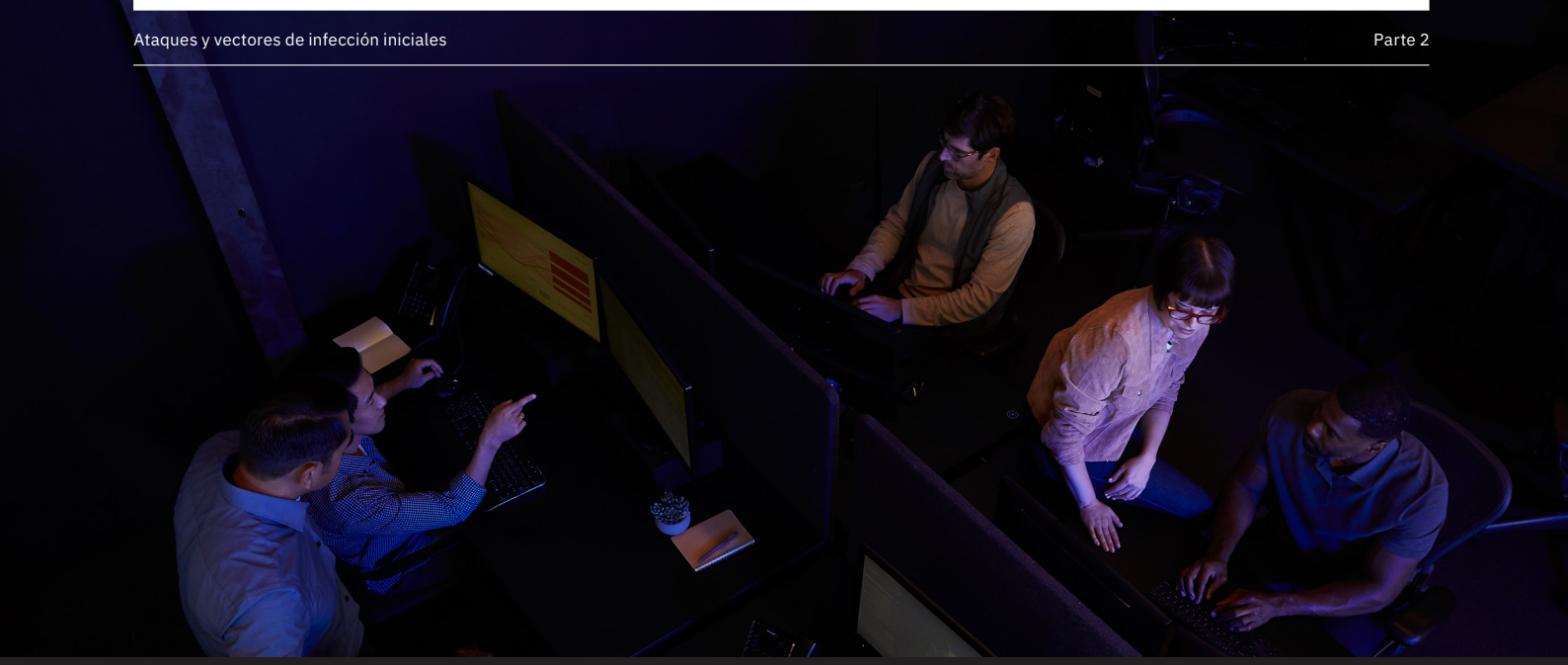



### El phishing es el principal vector para el acceso inicial en ataques en 2019

La extensiva capacidad de respuesta ante incidentes de IBM X-Force IRIS proporciona información valiosa sobre métodos y motivaciones de los atacantes.

Con el 31 %, el phishing fue el vector usado con mayor frecuencia para el acceso inicial en 2019, pero se ha reducido desde 2018 cuando representaba casi la mitad del total.[1]

1 El X-Force Threat Intelligence Index de 2019 informó que casi un tercio (el 29 %) de los ataques analizados por X-Force IRIS incluían ataques a través de correos electrónicos de phishing. Esta cantidad se ha ajustado para justificar la evidencia adicional que surgió tras la publicación de diversos incidentes que aumentaron el porcentaje al 44 % para 2018.



Lo que es más notable es que en 2019, los atacantes escanearon cada vez más entornos, en busca de vulnerabilidades para explotar, y los especialistas encuestados sobre el incidente notaron que esta técnica se utilizó en el 30 % de los incidentes, mucho más que solo el 8 % de los incidentes totales del año anterior.

Los actores amenazantes tenían muchas opciones para escanear y explotar, dado que IBM X-Force rastreó más de 150.000 vulnerabilidades que se habían divulgado públicamente. Si bien los adversarios sofisticados pueden desarrollar explotaciones desde el día cero, a menudo se suele confiar en las explotaciones conocidas ya que dichas explotaciones les permiten a los adversarios obtener un posicionamiento inicial sin tener que emplear recursos para crear nuevos TTP, lo que les permite reservar sus mejores armas para las redes con más defensas. Además, los atacantes cubren las organizaciones que no se actualizan con la aplicación de parches, incluso con vulnerabilidades cuyos parches ya han estado disponibles por algún tiempo. Por ejemplo, se siguen observando algunas instancias de infección Wanna Cry a más de dos años desde la infección inicial y de que el parche (MS17-010) estuviera ampliamente disponible.

El uso de credenciales robadas donde los actores amenazantes usan credenciales obtenidas con anterioridad para acceder a organizaciones que tenían en la mira, entró en un cerrado tercer puesto con el 29 %. A menudo estas credenciales podrían robarse de un sitio externo u obtenerse a través de un intento de phishing contra la organización a atacar. Los actores amenazantes pueden usar credenciales robadas para camuflarse con el tráfico legítimo, lo que hace que la detección sea aún difícil.

Los ataques de fuerza bruta disminuyeron interanualmente hasta una cuarta y distante posición con el 6 % de todos los casos, seguido de los dispositivos de BYOD con el 2 % como punto de acceso inicial en las organizaciones que estaban en la mira.

Los investigadores de X-Force observaron notable repunte en la actividad de los actores amenazantes en junio y julio de 2019, cuando la cantidad de eventos eclipsó los totales de todo 2019 para ese punto. Si bien se desconoce el motivo de este repentino resurgimiento de la actividad, los meses de verano parecen ser más activos también en términos de spam, ya que se registró un pico en el volumen de spam en agosto de 2019. Es posible que los actores amenazantes simplemente hayan sido más ruidosos y más fácilmente detectados, o que un cambio en las tácticas o las herramientas de dichos actores hayan generado una actividad significativa. En menos probable que los picos de actividad de corto plazo sean el resultado de nuevos actores amenazantes que ingresan al mercado, dado que se esperaría que estas nuevas entradas creen un aumento sostenido en la actividad en lugar de un pico temporal.

# Tendencias de malware

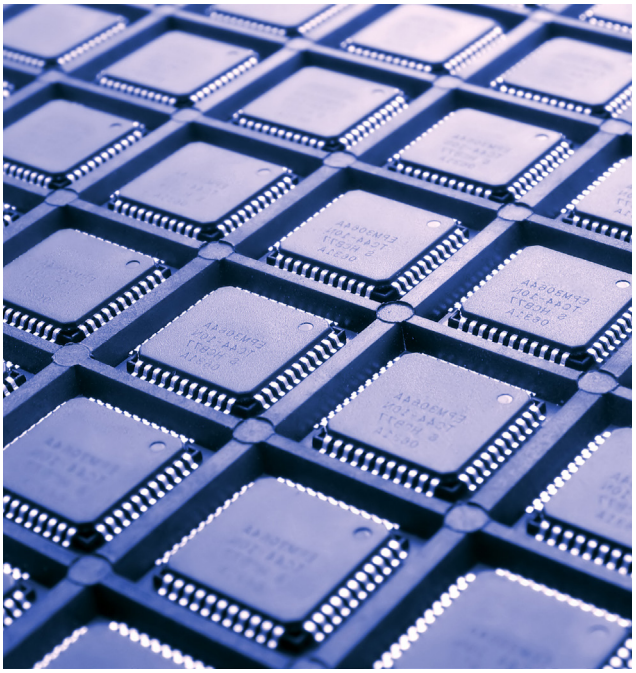
**Los ataques de malware destructivos aumentan drásticamente**

Las investigaciones de IBM X-Force IRIS indican que los ataques de malware destructivo se tornaron más frecuentes y aumentaron tanto en geografía como en alcance durante 2019.

Usado tanto por criminales cibernéticos como por actores del estado nacional, el malware destructivo es un software malicioso con la capacidad de hacer que los sistemas afectados queden inoperables y desafía su reconstitución. Las variantes de malware más destructivas causan la destrucción mediante la eliminación o la sobreescritura de archivos que son críticos para que el sistema operativo pueda funcionar. En algunos casos, el malware destructivo puede enviar mensajes adaptados a equipos industriales para que dejen de funcionar. En nuestra definición de malware destructivo se incluye el tipo de ransomware que es capaz de borrar datos de las máquinas o de cifrar datos de manera irreversible en una máquina.

Entre la segunda mitad de 2018 y la segunda mitad de 2019, X-Force IRIS respondió a la misma cantidad de ataques destructivos en términos interanuales, destacando que esta tendencia de malware potencialmente catastrófica sigue poniendo a las organizaciones en riesgo.

Históricamente, los ataques destructivos suelen provenir de adversarios del estado nacional. Sin embargo, hemos observado una tendencia en la que más variedades de ransomware motivados por cuestiones financieras están incorporando elementos destructivos en el ataque, con variantes tales como LockerGoga y MegaCortex que debutaron con su ataque destructivo a fines de 2018 y comienzos de 2019.

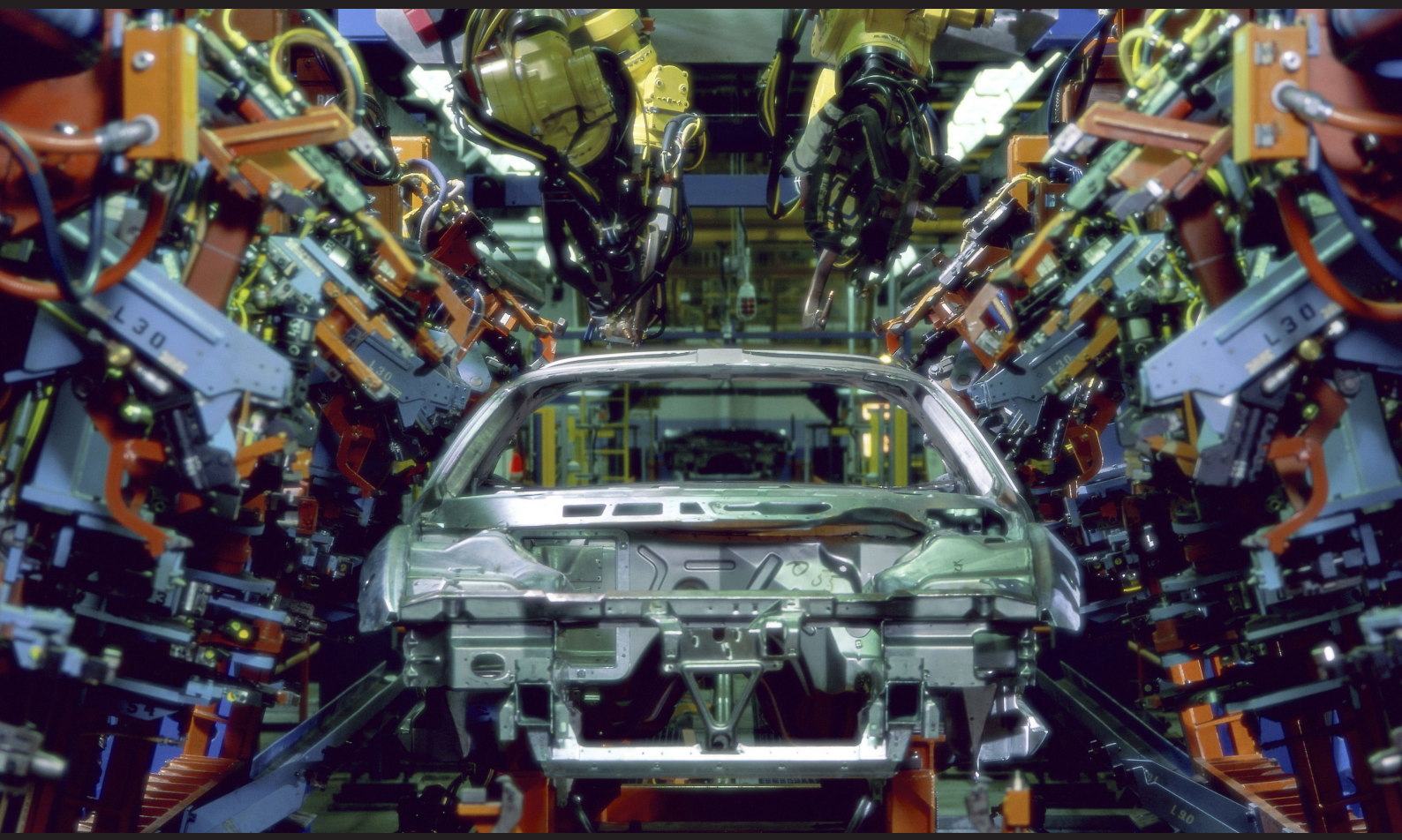


Se calcula que los ataques destructivos cuestan en promedio USD 239 millones, 60 veces más que el costo promedio de una vulneración de datos.

A fines de 2019, X-Force IRIS destacó el descubrimiento de un nuevo malware destructivo que denominamos ZeroCleare. Este ataque se dirigió al sector energético de Medio Oriente e IBM se lo atribuyó al grupo de APT afiliado a Irán ITG13[2], también conocido como APT34/OilRig.

X-Force IRIS calcula que el costo de un ataque de malware destructivo para las empresa puede ser particularmente alto, y grandes empresas multinacionales incurrieron en un costo de USD 239 millones por incidente, en promedio. Se estima que este costo es más de 60 veces superior que el costo promedio de 2019 de vulneración de datos tal como lo calculó el Ponemon Institute.

A diferencia de las vulneraciones de datos que roban o exponen datos, los ataques destructivos generalmente implican la destrucción de hasta tres cuartos o más de los dispositivos de las redes de la organización victimizada.



2 ITG es la sigla para IBM Threat Group (Grupo de Amenazas de IBM), un término que se analiza con mayor profundidad en Las industrias atacadas con mayor frecuencia. X-Force utiliza nombres de ITG, con los nombres alternativos para los grupos de amenazas entre paréntesis después del nombre de ITG.

**Ransomware y cryptominers agresivos en 2019**

El recuento de variantes de malware y los ataques que utilizan malware aumenta y disminuye durante el año, pero a pesar de eso, la información sobre los tipos de amenazas que deberían tener prioridad puede ayudar a las organizaciones a administrar mejor el riesgo.

En la primera mitad de 2019, aproximadamente el 19 % de los ataques observados estaban relacionados con incidentes de ransomware, en comparación con solo el 10 % de los ataques de la segunda mitad de 2018. En el T4 de 2019 hubo un aumento del 67 % en actividades de ransomware en comparación con el T4 del año anterior. Durante 2019, X-Force IRIS respondió a acciones de ransomware en 12 países diferentes, en 5 continentes diferentes y en 13 industrias diferentes.

Este resurgimiento se puede atribuir a los números cada vez mayores de actores amenazadores y de campañas lanzadas contra diversas organizaciones en 2019. Se destacaron las instituciones municipales y públicas que padecieron ataques de ransomware, así como organismos gubernamentales locales y proveedores de atención sanitaria. Los ataques a estos tipos de organizaciones suelen sorprenderlas sin preparación para responder, con mayores probabilidades de pagar un rescate y, en ciertos casos, bajo un estrés extremo por recuperarse del ataque debido a la amenaza a la seguridad pública y la vida humana.

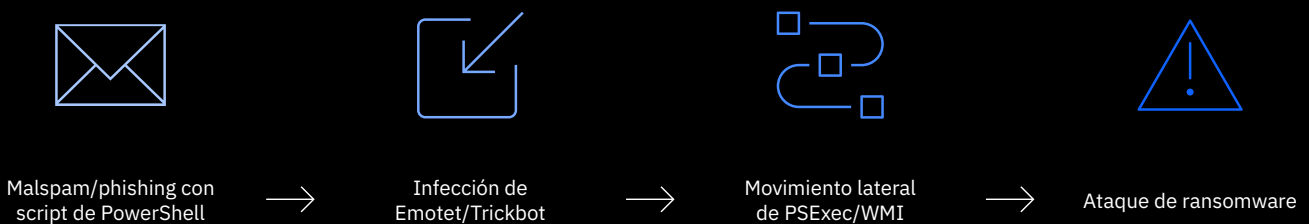
Los datos de X-Force muestran que en los casos de ataques de ransomware, el principal vector de ataque en 2019 fue a través de los intentos por explotar las vulnerabilidades del protocolo de Bloqueo de mensajes del servidor de Windows (SMB) para propagarse por la red. Esta táctica, que se usó anteriormente en los ataques de WannaCry, representó más del 80 % de los intentos de ataque observados.

En el T4 de 2019 hubo un aumento del 67 % en las actividades de ransomware en comparación con el cuarto trimestre de 2018.

**Figura 4:**

## Infección de ransomware en varios pasos

Ataque de ransomware a través de una rutina de infección de varios pasos (Fuente: IBM X-Force)




Los ataques contra las versiones vulnerables del protocolo de SMB pueden ser automáticos, lo que los convierte en una opción de bajo costo para que los actores amenazantes intenten y escalen fácilmente en su búsqueda por afectar a tantos sistemas como sea posible en un ataque.

Los actores amenazantes también suelen usar gestores de descarga de productos, como Emotet y TrickBot, para ejecutar un ransomware en un sistema objetivo. Esta técnica suele aprovechar PowerShell para descargar el malware y distribuirlo utilizando funciones nativas, tales como PSExec o Windows Management Instrumentation (WMI), que pueden ser más difíciles de detectar.

Los atacantes utilizan múltiples etapas para infectar a los usuarios, en lugar de un solo golpe directo con ransomware, para tener un mayor control sobre el ataque, para evitar los controles y la detección y para plantar la semilla de una operación de ransomware que pudiera abarcar suficientes dispositivos como para instar a las víctimas a pagar. El retorno de su inversión de paciencia y planificación es grande: en cinco meses, los ataques Ryuk amasaron más de USD 3,7 millones para su banda criminal. En otra instancia, un ataque a asilos de ancianos en EE. UU. llevó a un pedido de rescate de USD 14 millones de los operadores de Ryuk.

El ransomware no es el único tipo de malware en repuntar en 2019. Otro tipo de malware que fue extremadamente popular en 2019 fue el código de minería de la criptomoneda.

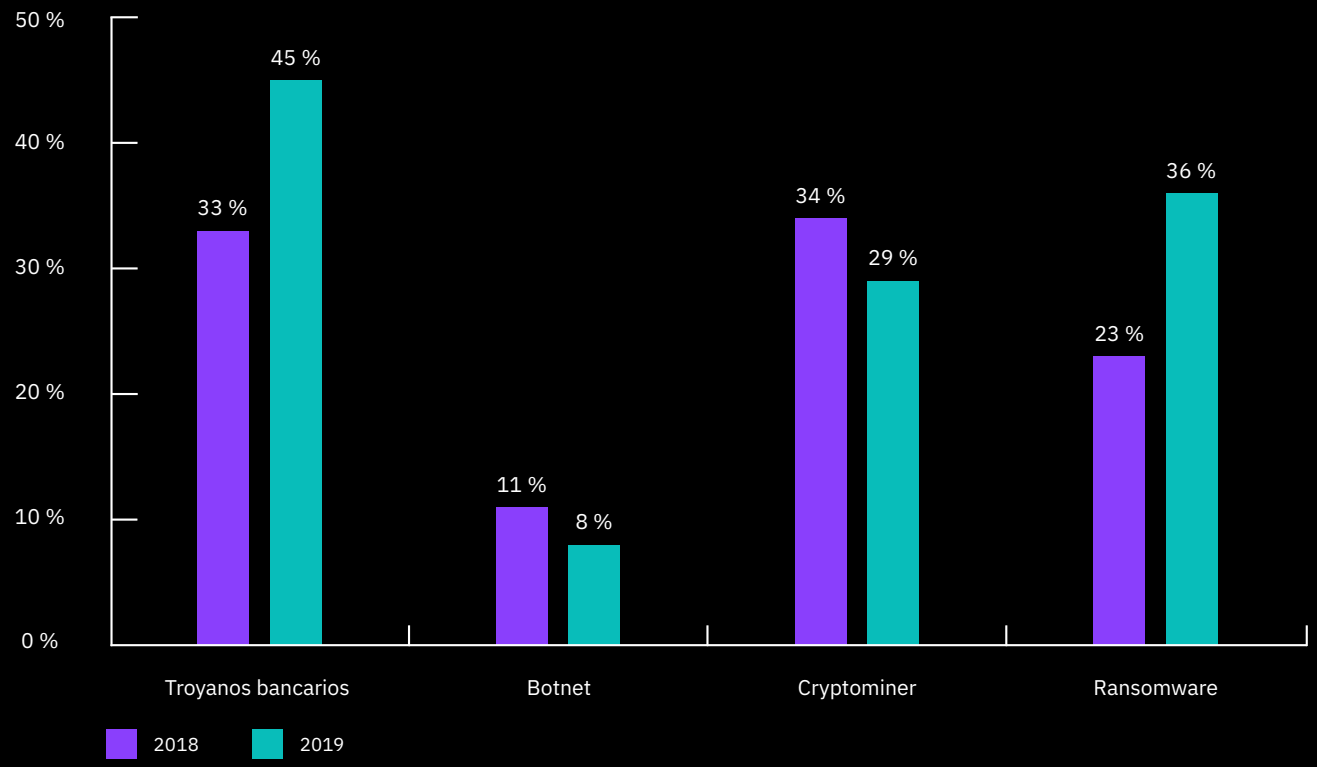
Según la telemetría de X-Force, la actividad de cryptomining aumentó a niveles sin precedentes a mediados de 2019, con un volumen de actividad en junio que casi excede toda otra actividad de cryptomining para el resto del año.

Si bien el malware tiende a aumentar y caer según los motivos y los recursos de quienes operan las botnets, este aumento podría estar relacionado con la triplicación del valor de Monero, una criptomoneda que suelen usar los mineros de malware.

**Figura 5:**

## Innovación del código genético de malware

Porcentaje del nuevo código (anteriormente no observado) por categoría, 2018-2019 (Fuente: Intezer)




### Principales innovadores en la evolución del código de malware de 2019

Aprovechando la anterior colaboración de X-Force en la detección de nuevas variantes de malware, Intezer utilizó su tecnología de análisis de malware genético que revela el origen genético de todo el código de software para identificar similitudes y volver a utilizar el código para medir la "innovación" del malware. Esta medición de la innovación muestra hasta que punto los actores amenazantes invirtieron en el desarrollo de un nuevo código, lo que sugiere que los adversarios buscan expandir sus capacidades de amenazas y evadir la detección.

Los datos de Intezer muestran que, en 2019, los actores amenazadores se centraron principalmente en desarrollar y evolucionar la base de códigos de

Esta sección del informe se escribió en colaboración entre IBM X-Force e investigadores de Intezer. Intezer realiza un análisis genético sobre el código binario del malware.

En 2019, los troyanos bancarios tenían el mayor nivel de código nuevo (45 %), seguido del ransomware (36 %). Históricamente, IBM ha visto el interés y la inversión de los actores amenazantes en tipos de malware eficaces contra los usuarios empresariales, lo que sugiere que estas familias de malware podrían atacar a las empresas en 2020. A menos que evolucionen constantemente, los troyanos bancarios y los operadores de ransomware se extinguirán, ya que el malware se detectará más rápidamente y con el tiempo se reducirá el retorno de la inversión de los ataques.

Los cryptominers mostraron una caída en innovación en 2019, pero el volumen de actividad minera aún era alto, lo que sugería que los actores amenazadores seguían desarrollando nuevas versiones de criyptominers pero dependen cada vez más del código anterior. Según la experiencia de IBM, estos códigos simplistas de malware suelen depender de otros antecesores, no maliciosos, como XMRig por ejemplo, modificados para obtener monedas de forma ilegítima. Los nuevos mineros también se escriben para diferentes fines, como obtener monedas en dispositivos de IoT, o en el otro extremo, en servidores infectados, donde la potencia del CPU es mayor que en dispositivos más pequeños y PC individuales.

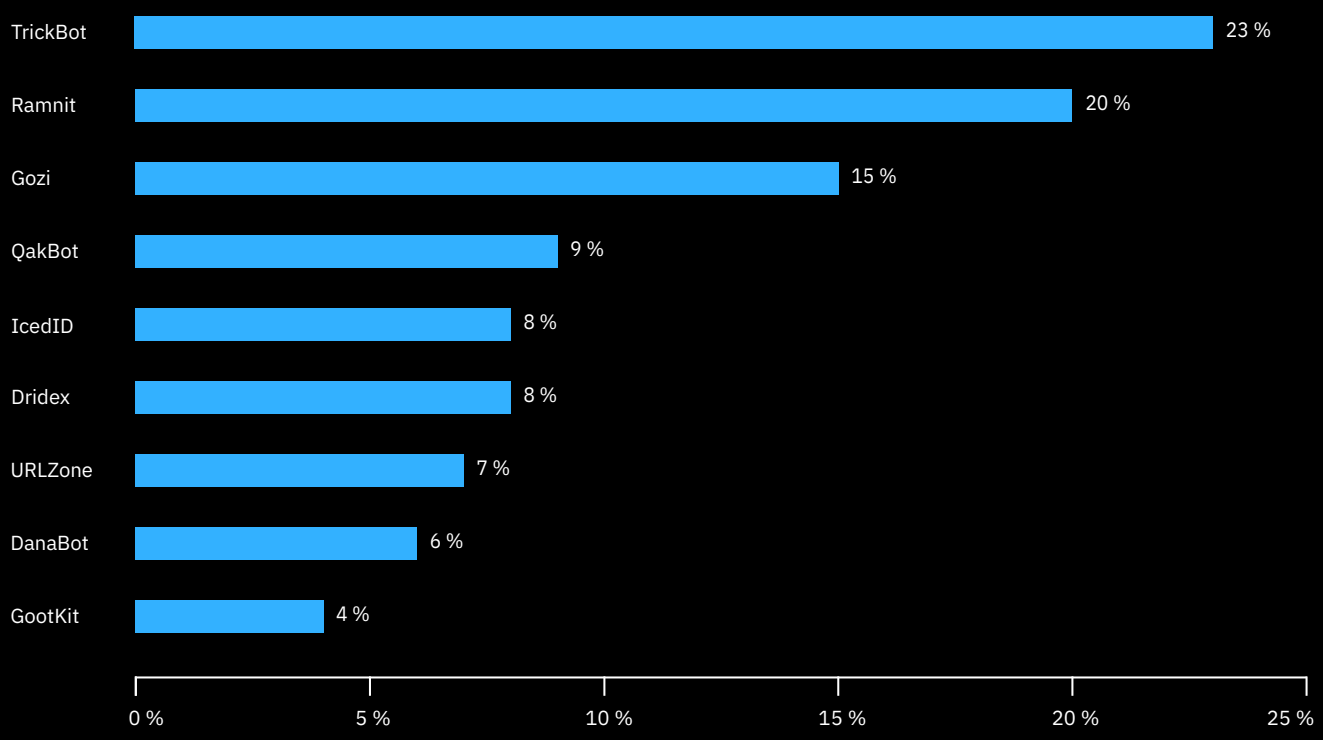
Por contraste, el malware de botnet genérico (11 %) tuvo menos innovación de código interanual, lo que indica una reducción en la inversión para modificar sus capacidades. IBM ha observado que estos tipos de códigos llegan a los usuarios a través de spam o publicidad maliciosa. El rol principal del malware de botnet genérico es obtener cierto posicionamiento en un dispositivo infectado, pero su funcionalidad sigue siendo mínima, lo que puede explicar por qué no ven un mayor nivel de evolución del código.

Al entrar al 2020, estas tendencias de innovación del código pueden indicar tipos de malware que serán más difíciles de identificar y contener debido a la constante inversión para que este código evolucione.

En 2019, los actores amenazadores se centraban en desarrollar y hacer evolucionar la base de códigos de troyanos bancarios y ransomware.

**Figura 6:**
## Principales familias de troyanos bancarios

Desglose de las principales familias de troyanos bancarios en 2019, como porcentaje de las nueve familias de troyanos que se muestran (Fuente: IBM X-Force)




### Troyanos bancarios y ransomware: un matrimonio engañoso que sigue empeorando

El campo del malware financiero se convirtió en un problema corriente hace un poco más de una década, con el aumento del malware como el troyano Zeus, que a la vez fue el primer troyano bancario comercial en disponibilidad general del mundo del delito cibernético. Una revisión del panorama del delito financiero de 2019 marca una clara tendencia para las principales bandas criminales de troyanos bancarios: estos botnets de malware se están utilizando cada vez más para abrir la puerta para los ataques de ransomware de alto interés.

Un gráfico de las familias de troyanos más activos en esta categoría para 2019 se ve similar al producido en la conclusión anual de 2018. TrickBot, Gozi y Ramnit siguen en las tres posiciones superiores. Estos troyanos se operan y organizan en grupos que ofrecen diversos modelos comerciales a otros actores de delito cibernético, como esquemas de botnet como servicio y la distribución a través de activos afectados.

La pandilla que opera TrickBot ha sido, por mucho, el grupo de crimeware más activo en el campo del delito cibernético en 2019. Esta actividad se expresó en diversos aspectos:

— Frecuencia de actualizaciones y reparaciones de códigos (código, versión y evolución de las características)

— Frecuencia y escalada de campañas de infección

— Frecuencia y volumen de actividad de ataque

Los delincuentes que crearon titulares de periódicos con ataques de ransomware de alto impacto en 2019 son también las que introdujeron los ataques de fraude electrónico de alto interés en el campo del delito cibernético en 2015. En un sentido, la estrategia general es la misma, solo se modifica la táctica con el tiempo: se apunta a empresas para obtener una mayor recompensa.

Además, los informes de finales de 2019 indican que ITG08, (FIN6) que históricamente se ha enfocado en el robo masivo de datos de tarjetas de pago, también ha ido diversificando sus TTP. Ahora intenta incluir la implementación de ransomware a las redes empresariales. La acumulación, y luego la venta o el uso de datos de tarjetas robadas puede llevar tiempo y esfuerzo para monetizarse, mientras que un ataque de ransomware tiene el potencial de millones netos en un solo golpe, lo que atrae a más bandas criminales a seguir la ruta del ransomware o la extorsión cibernética.

**Los principales ejemplos de troyanos bancarios que se diversifican al ransomware son:**

**Dridex**
Anteriormente distribuía LokiBot a dispositivos de usuario, ahora implementa BitPaymer/DopplePaymer en redes empresariales.

**GootKit**
Se sospecha que implementa LockerGoga en redes empresariales. LockerGoga surgió a principios de 2019 y desde entonces ha sido parte de ataques paralizantes a negocios.

**QakBot**
Implementa MegaCortex en redes empresariales.

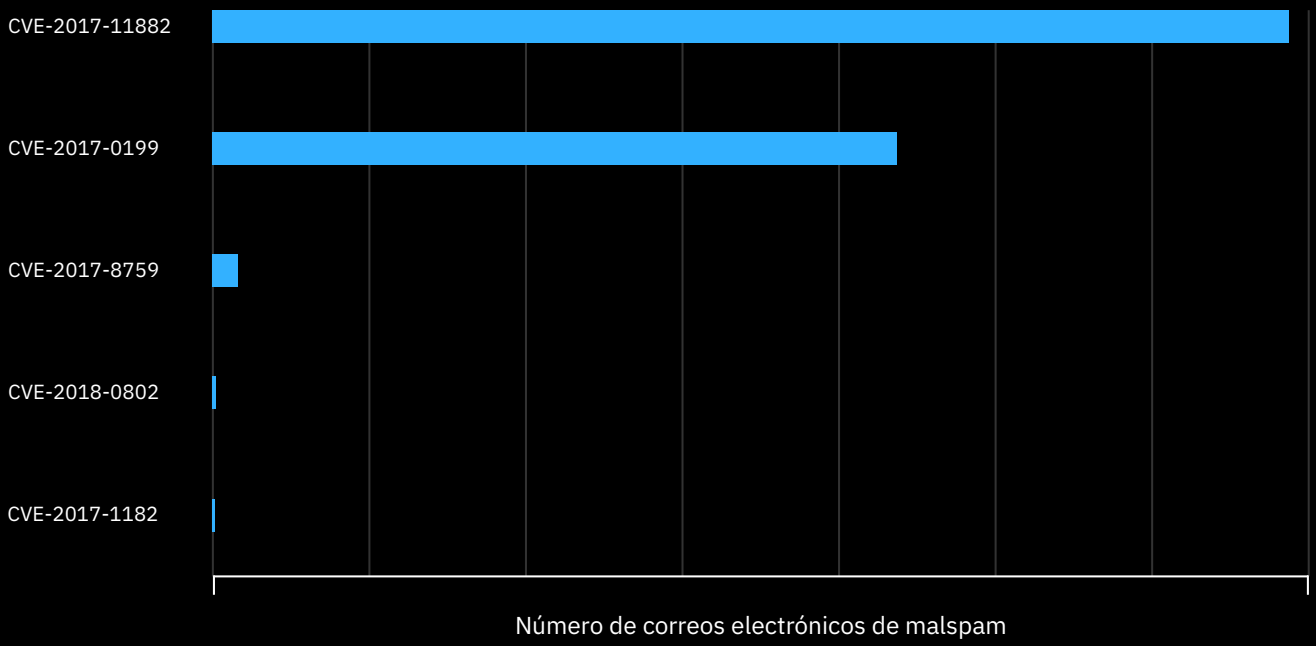
**TrickBot**
Implementa Ryuk en redes empresariales.

# Tendencias de spam y phishing

**Figura 7:**

## Principales vulnerabilidades aprovechadas en malspam

Desglose de las principales vulnerabilidades aprovechadas en los adjuntos de malspam en 2019, por volumen (Fuente: IBM X-Force)




**Las vulnerabilidades de 2017 siguen siendo las estrellas en el spam de 2019**

IBM X-Force ejecuta trampas para spam en todo el mundo y monitorea decenas de millones de mensajes de spam y correos electrónicos de phishing al día. Nuestros equipos y tecnología analizan miles de millones de páginas web e imágenes para detectar actividad fraudulenta y abuso de marca.

El análisis de X-Force de actividad de spam global indica que el correo electrónico del spam continúa usando un subconjunto de vulnerabilidades, con un enfoque particular en solo dos CVE: 2017-0199 y 2017-11882. Estas dos son vulnerabilidades emparchadas que han representado casi el 90 % de las vulnerabilidades que los actores amenazantes intentaban explotar a través de campañas de spam. Ambos CVE afectan Microsoft Word y no requieren la interacción del usuario más allá de abrir un documento con trampa.

Los datos de nuestros eventos muestran que la frecuencia con la que se usaron estas dos vulnerabilidades por parte de los atacantes en 2019 excedió el uso de cualquier otra vulnerabilidad de ejecución del código remoto de Microsoft Word en una proporción de casi 5 a 1.

Si bien estas dos vulnerabilidades aparecieron en cantidades considerables de correos electrónicos de spam, no hay indicaciones de qué tan exitosas podrían ser para explorar a los usuarios. Dicho eso, el spam suele ser un juego de números; con suficiente volumen, incluso un índice de éxito pequeño es suficiente para generar valor para los actores amenazantes. Dado que muchos usuarios e incluso organizaciones pueden estar atrasados con los parches de ciertas cuestiones, aún es posible ver dispositivos afectados por errores más antiguos.

Es posible que haya muchas explicaciones en relación con la popularidad de las vulnerabilidades anteriores, incluida la facilidad de incorporación y la disponibilidad de generadores de documentos gratuitos, su efectividad continua o su versatilidad para dejar una variedad de cargas dañinas maliciosas.

El uso continuo de vulnerabilidades anteriores destaca el extenso rastro de actividad maliciosa y cómo aún se pueden aprovechar las vulnerabilidades significativas contra los usuarios, años después de la divulgación y el lanzamiento del parche.

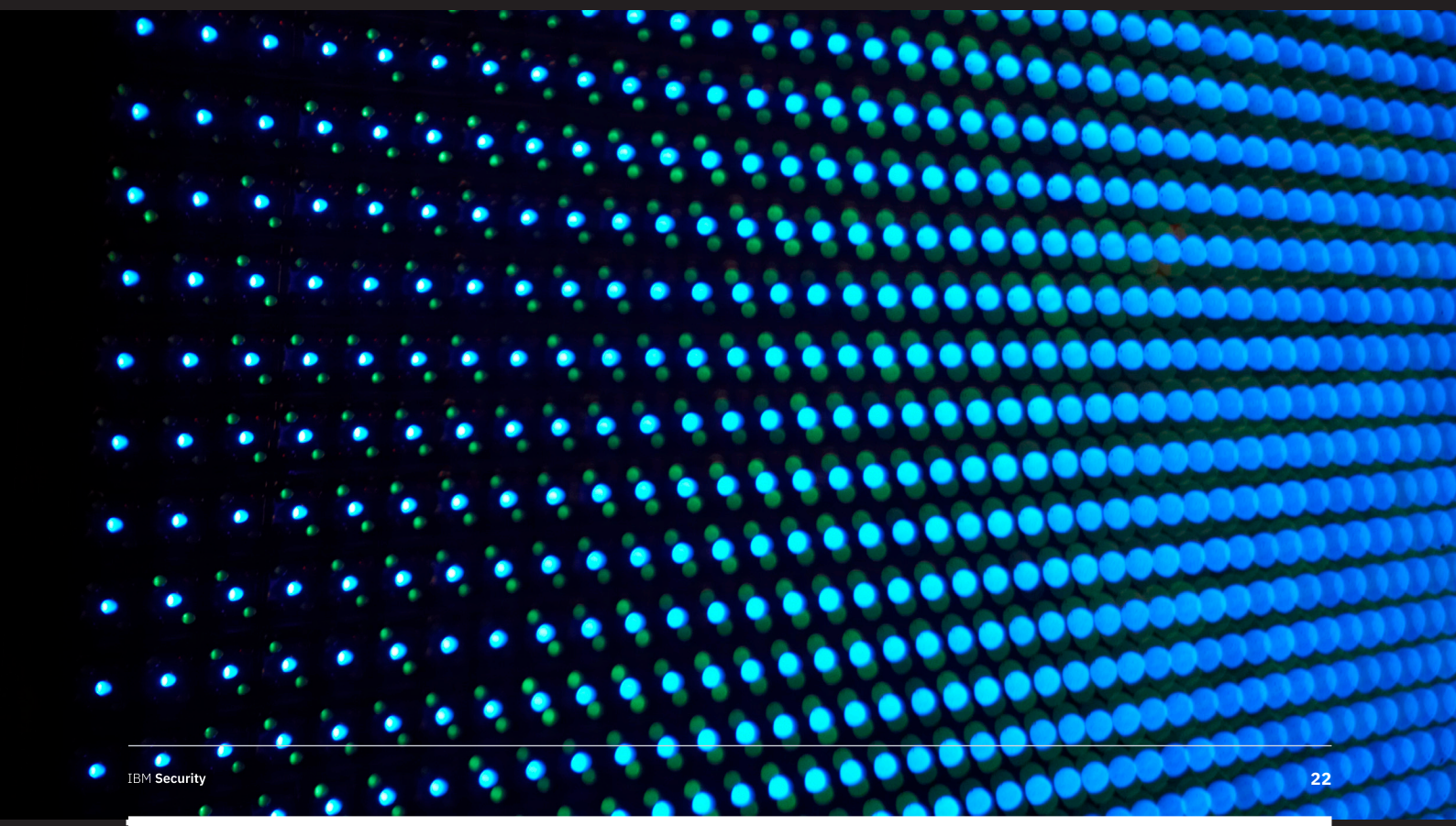
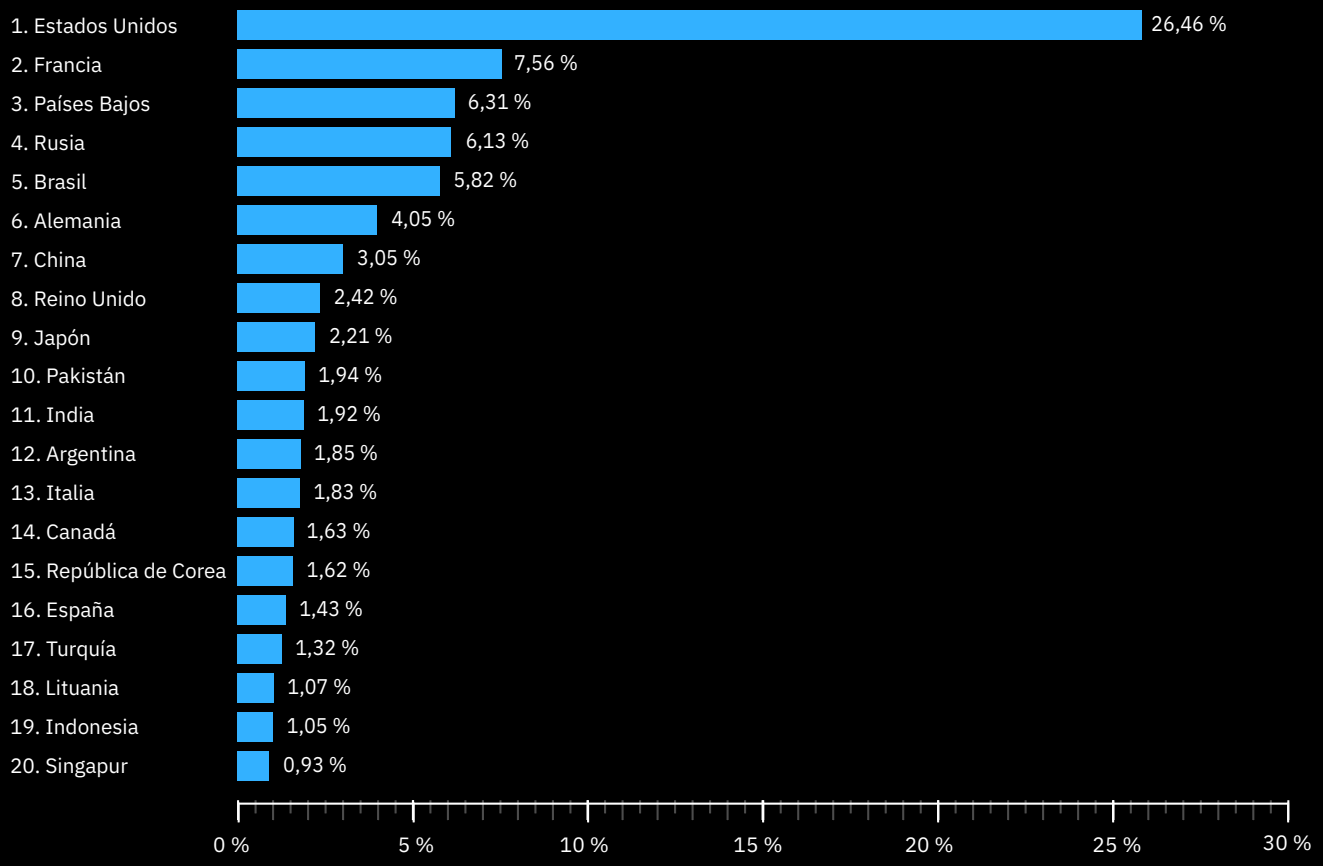


**Figura 8:**

## Principales 20 países que alojaron C2 de spam

Desglose de los principales 20 países que alojaron comando y control de spam en 2019, como porcentaje de los 20 países mostrados (proporción del total de servidores C2 en los principales 20 países = 80,6 %) (Fuente: IBM X-Force)




### Las botnets de spam alojadas en occidente tienen un impacto a nivel mundial

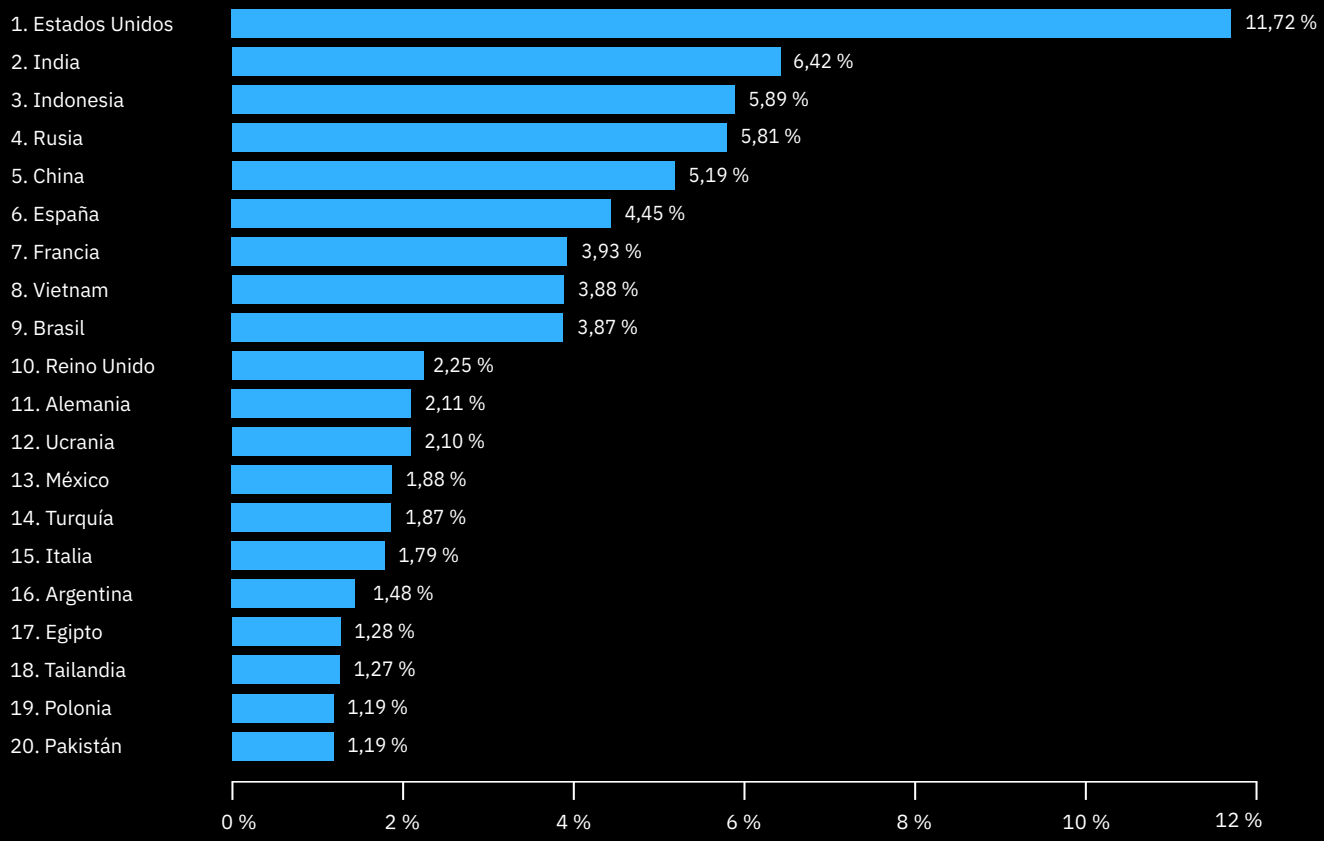
La investigación de IBM X-Force sobre botnets de spam observa una variedad de puntos de datos geoespecíficos vinculados con la infraestructura de comando y control (C2) para botnets de spam. Uno de los parámetros que observamos es la geolocalización en la que se alojan las botnet C2. En 2019, notamos que los C2 se alojaban principalmente en los países de América del Norte y Europa Occidental, lo que representaba más de la mitad de las instancias C2 observadas en 2019. El alojamiento C2 restante se distribuía por una gran variedad de regiones.

En muchos casos, la infraestructura de C2 de botnet de spam se alojaba en servidores afectados, y el uso de servidores de América del Norte y Europa se alinea con la comprensión común de que estos países generalmente tienen un tiempo de producción de servidor más consistente. Además, los delincuentes cibernéticos prefieren alojar sus ataques en recursos locales que tienen menores probabilidades de levantar sospechas cuando el tráfico de estos servidores interactúa con los dispositivos y las redes de la geografía a atacar.

**Figura 9:**

## Principales 20 países para víctimas de botnet de spam

Desglose de los principales 20 países para el total de clientes de botnet (víctimas) en 2019, como porcentaje de los 20 países mostrados (proporción del total de clientes de botnet en los principales 20 países = 69,6%) (Fuente: IBM X-Force)




### Víctimas del spam por región geográfica

Las víctimas de botnets de spam en 2019 se distribuyeron por todo el mundo, pero Estados Unidos fue el país con mayor cantidad de víctimas, seguido de India, Indonesia, Rusia y China. La distribución de objetivos se alinea con la motivación de los piratas informáticos de llegar a la mayor cantidad posible de destinatarios con campañas de spam de alto volumen. Como es de esperar, los países con mayor población observan una mayor cantidad de correos electrónicos de spam.

**Los dominios maliciosos bloqueados destacan la prevalencia de los servicios de anonimato**

Cuando se trata de mantener las redes a salvo de las amenazas en línea, es muy común evitar que los usuarios y los activos se comuniquen con dominios maliciosos confirmados o que se sospeche que pueden serlo. A fin de minimizar el riesgo, la mayoría de las organizaciones usan listas para bloquear direcciones de IP sospechosas. Con la misma idea a nivel global, Quad9, un servicio de servidor de nombre de dominio (DNS) disponible de manera gratuita[3], bloquea en promedio 10 millones de solicitudes de DNS de sitios maliciosos a diario.

Según una muestra de datos de Quad9 que se correlacionan con la inteligencia de amenazas de IBM Security, las URL que se encontraban en el correo electrónico de spam eran las que conformaban la mayoría de las solicitudes de DNS sospechosas, con el 69 % de todas las solicitudes de 2019. Si bien disminuyeron desde el 77 % en 2018, la categoría de URL de spam sigue representando la categoría más significativa de dominios maliciosos en general. Se puede atribuir una disminución del 8 % a la categoría de servicios de anonimato, que conforma el 24 % de las solicitudes de DNS.

El spam de correo electrónico sigue siendo uno de los modos más efectivos para llegar a la mayor cantidad de potenciales víctimas gracias a las grandes botnets de spam, como botnet Necurs, que puede diseminar docenas de millones de correos con spam por día. Los dominios maliciosos suelen distribuir malware para distribuir ransomware, scripts de robo de credenciales o enlaces a estafas más grandes, y están diseñados para engañar al usuario final al parecer o personificar a una marca que ellos conocen.

Una vasta mayoría de actores motivados por cuestiones financieras también eligen colocar enlaces de URL maliciosos en correos de spam, ya que esto les permite cubrir toda la red con mínimo esfuerzo, u optar por un ataque geoespecífico que pueda limitar la exposición a sus estafas.

El gráfico de la Figura 10 muestra las distribuciones de tipos de dominios maliciosos registrados por IBM Security en 2019.

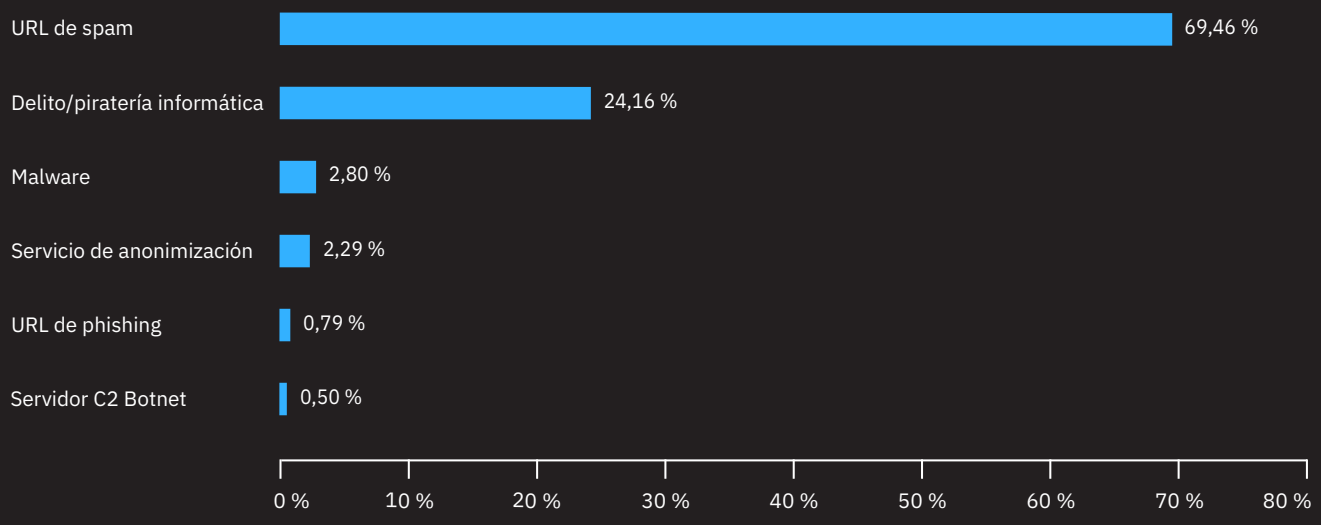
El spam de correo electrónico sigue siendo uno de los modos más efectivos para llegar a la mayor cantidad de potenciales víctimas.

3 Quad9 se creó y patrocinó mediante una colaboración entre IBM, Packet Clearing House (PCH) y Global Cyber Alliance (GCA).

**Figura 10:**

## Principales tipos de amenazas de dominios maliciosos

Desglose de los principales tipos de amenazas de dominios maliciosos, como porcentaje de los seis tipos conocidos, en 2019 (Fuente: IBM X-Force y Quad9)




**URL de spam:**
Dominios que llevan a sitios afiliados con campañas de spam, a menudo son una molestia pero no están afiliadas a ninguna actividad criminal

**Servicio de anonimato:**
Dominios que llevan a proveedores de anonimato que ocultan tráfico para que no se siga viendo

**Delito/piratería informática:**
Dominios específicamente identificados como involucrados en conductas delictivas, como sitios que alojan scripts de explotación del navegador web

**URL de phishing:**
Dominios que simulan ser otros dominios legítimos, generalmente en un intento por obtener datos de credenciales u otra información sensible del usuario

**Comando y control de botnet:**
Dominios vinculados a la actividad de botnet y que potencialmente infecta a los visitantes

**Malware:**
Dominios que alojan malware conocido

Los proveedores de anonimato, como por ejemplo Tor, permiten que los usuarios hagan anónima la fuente de su tráfico de internet navegando por nodos operados por otros actores. Si bien los servicios de anonimato pueden servir al propósito legítimo, y a menudo así es, de proporcionarles a los usuarios mayor privacidad para su actividad de exploración web, esta actividad también puede dificultar o imposibilitar el rastreo y bloqueo de actividad maliciosa.

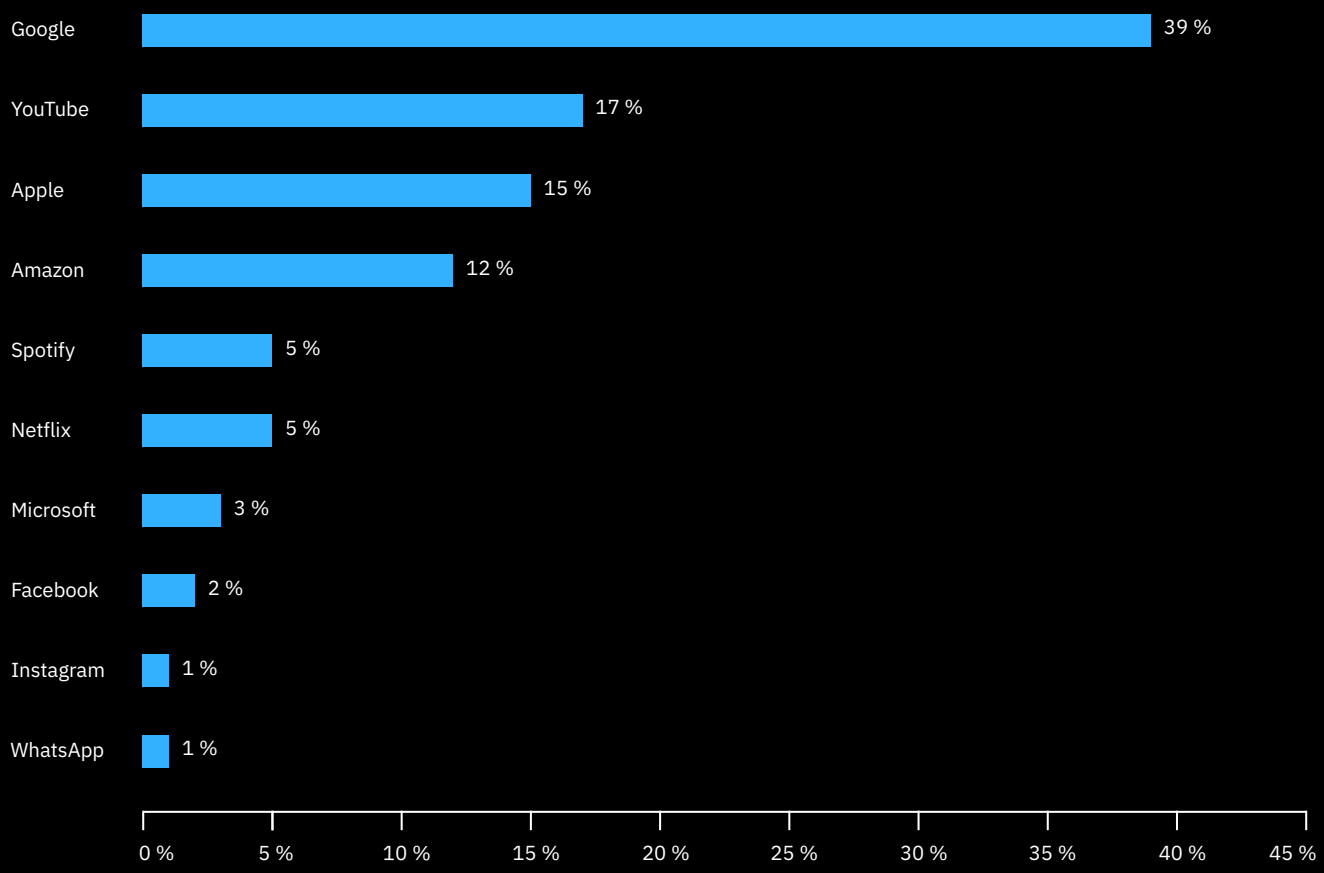
EL anonimato es una táctica común utilizada por los delincuentes cibernéticos para intentar cubrir sus rastros ya que puede usarse para ofuscar enlaces maliciosos, filtrar datos sin accionar las reglas de la Prevención de pérdida de datos (DLP), o dejar cargas dañinas maliciosas antes de que el IP del servidor remoto se bloquee.

El 4 % de las solicitudes de DNS maliciosas se categorizaron como delito informático o páginas web de hackeo de blackhat, donde se sabe que algunos criminales intentan la explotación de navegadores web, distribuyen información sobre fraudes o participan de otros tipos de delitos en línea. Este número relativamente bajo quizás se deba al hecho de que estos enlaces se dirigen mediante nodos de anonimato o se detectan y bloquean a través de proxies y firewalls de empresas, y posteriormente se cierran.

**Figura 11:**

## Principales 10 marcas falsificadas

Desglose de las principales 10 marcas falsificadas en spam en 2019, como porcentaje de las 10 marcas que se muestran (Fuente: IBM X-Force)




### El phishing simuló ser empresas de tecnología y medios sociales

El phishing sigue siendo un vector de amenazas clave en 2019, y los datos de X-Force muestran que las marcas que más se falsificaron en las campañas de phishing estaban en plataformas de tecnología y medios sociales. Para los usuarios puede ser difícil identificar dominios falsos, y con frecuencia se usan dominios que se ven como legítimos para hacerse pasar por la empresa. Un sitio web con aspecto auténtico puede ayudar a convencer a un usuario de divulgar datos personales en un sitio web malicioso si se parece mucho al original.

Estos datos se obtuvieron analizando todos los dominios maliciosos bloqueados por Quad9 en 2019 y en función de la detección de dominios ocupados ilegalmente de IBM X-Force.

Atacar medios sociales o sitios de transmisión de contenido, como Instagram y Spotify, podría no proporcionarles a los actores amenazantes datos listos para monetizar, como robar cuentas de Google o de Amazon. Sin embargo, los actores amenazantes pueden esperar que las personas vuelvan a usar contraseñas entre cuentas y servicios e intentarán usar las credenciales obtenidas para obtener acceso a cuentas más valiosas del mismo usuario.

# Industrias atacadas con mayor frecuencia

## En el escenario de amenazas actual, la especificidad de ciertos tipos de ataques según las motivaciones del actor amenazante significa que la administración de riesgos de seguridad cibernética puede verse muy diferente de un sector a otro.

Para obtener una vista aérea de las industrias más atacadas cada año, los investigadores de X-Force clasificaron el volumen de ataques que observamos en cada sector. Las industrias atacadas con mayor frecuencia se determinaron en función de los datos de incidentes de ataques y seguridad de las redes administradas de X-Force, los datos y la información derivaron de nuestros servicios de respuesta ante incidentes e incidentes divulgados públicamente.

**Figura 12:**

### Las 10 industrias más atacadas

Las 10 industrias más atacadas clasificadas por volumen de ataques, 2019 en comparación con 2018 (Fuente: IBM X-Force)

| Sector | Clasificación de 2019 | Clasificación de 2018 | Cambio |
|---|---|---|---|
| Servicios Financieros | 1 | 1 | – |
| Ventas al por menor | 2 | 4 | 2 |
| Transporte | 3 | 2 | -1 |
| Medios Electrónicos | 4 | 6 | 2 |
| Servicios profesionales | 5 | 3 | -2 |
| Gobierno | 6 | 7 | 1 |
| Educación | 7 | 9 | 2 |
| Manufactura | 8 | 5 | -3 |
| Energía | 9 | 10 | 1 |
| Sector sanitario | 10 | 8 | -2 |

La Figura 12 es un gráfico comparativo de las industrias más agredidas en 2019 y su posición en comparación con 2018.

Se puede ver fácilmente que, si bien no hubo sorpresas en el sector de servicios financieros, la industria de ventas minoristas ha estado despertando un mayor interés de los atacantes. Lo mismo ocurrió con las empresas de entretenimiento y multimedia, educación y organismos gubernamentales.

Las siguientes secciones se dividen en la frecuencia relativa de ataques en función de diversas fuentes de datos y nuestros hallazgos para cada una de estas industrias en 2019. Las descripciones de ciertas industrias destacan actores amenazadores que estuvieron particularmente activos en ataques al sector en años recientes, pero esta lista no es exhaustiva e incluye datos anteriores a 2019. X-Force IRIS rastrea y perfila docenas de grupos de delincuentes cibernéticos y patrocinados por estados nacionales. La actividad no atribuida y las campañas descubiertas en estado salvaje se rastrean dentro de la actividad “HIVE”. Una vez que la actividad ha alcanzado un umbral de análisis estricto hace la transición a un IBM Threat Group (ITG), que se basan en la recopilación de TTP, infraestructura, ataques y oficios.

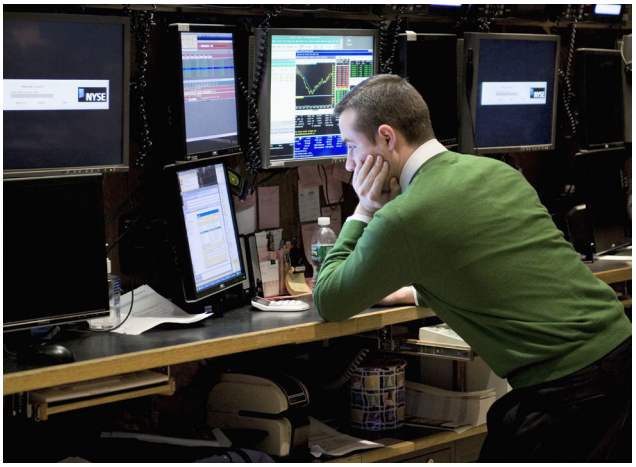
**Finanzas y seguro**

Sumando cuatro años consecutivos, el sector de finanzas y seguro fue el más atacado en 2019. Los ataques a este sector representaron el 17 % de todos los ataques de las 10 industrias más atacadas.

Es probable que los delincuentes cibernéticos motivados por las finanzas conformen la mayor parte de actores amenazantes cibernéticos activos que atacan a entidades financieras, y la atracción de las empresas financieras para un delincuente cibernético es clara: pagos potencialmente significativos y rápidos, en millones por un ataque exitoso.

Los datos las actividades de respuesta ante incidentes de X-Force mostraron que las financieras y las aseguradoras estaban primeras entre las industrias más atacadas, a pesar de la pequeña cantidad de vulneraciones de datos divulgada públicamente.

Esto sugiere que las empresas de finanzas y seguros tienden a experimentar un mayor volumen de ataques en relación con otras industrias, pero suelen tener herramientas y procesos más efectivos para detectar y contener las amenazas antes de que se conviertan en mayores incidentes. Las empresas financieras también se ven más inclinadas a probar sus planes de respuesta bajo amenaza y conforman el grupo de organizaciones que utiliza IBM Security Command Centers para prepararse y practicar para un ciberataque. Probar de manera extensiva los planes y equipos de respuesta ante incidentes en escenarios relevantes demostró ser eficaz en la mitigación de daños financieros de una vulneración de datos, según el Informe del costo de las vulneraciones de datos de 2019[4] realizado por el Ponemon Institute y patrocinado por IBM Security. Las organizaciones vulneradas que probaron de manera extensiva su plan de respuesta ante incidentes (en un entorno cibernético, por ejemplo) perdieron en promedio USD 320.000 menos que el costo medio general de una vulneración de datos de USD 3,92 millones.




Los grupos amenazadores dominantes de 2019 que atacaron organizaciones del sector financiero fueron ITG03 (Lazarus), ITG14 (FIN7) y varias facciones de Magecart. Los troyanos bancarios como TrickBot, Ursnif y URLZone fueron algunos de las principales amenazas que pagaron los bancos en 2019 al tomar y defraudar las cuentas de sus clientes.

4 El informe anual de costo de las vulneraciones de datos fue llevado a cabo por Ponemon Institute y patrocinado por IBM.

**Ventas al por menor**

La industria de la venta minorista fue la segunda industria más atacada, según los datos de X-Force de 2019. Este sector recibió el 16 % de todos los ataques de las 10 industrias más atacadas, un marcado aumento desde el cuarto lugar y el 11 % de los ataques de 2018. Esta industria experimentó la segunda mayor cantidad de ataques a la red en 2019.

La industria de ventas minoristas quedó en segundo lugar en 2019 en función de los datos de X-Force IRIS y la información divulgada públicamente de la vulneración de datos. El tipo de actor amenazante más común en atacar a las organizaciones de ventas minoristas fueron los delincuentes motivados financieramente, quienes atacaron a la industria para obtener información personal identificable del cliente (PII), datos de tarjetas de crédito, datos financieros, historial de compras e información de programa de lealtad. Los delincuentes cibernéticos generalmente usan estos datos para apropiarse de las cuentas de los clientes, estafar a los clientes y reutilizar los datos de diversos escenarios de robo de identidades.

Una técnica de ataque popular utilizada por los delincuentes cibernéticos para atacar a las ventas minoristas en 2019 fue malware de puntos de venta (POS) y remoción de tarjetas de pago de comercio electrónico, cada una destinada a desviar información de la tarjeta de pagos durante una transacción a través de terminales de pago físicas o en línea, respectivamente.

En particular, un conjunto de facciones de delincuentes cibernéticos agrupados bajo el término general Magecart, ha estado atacando plataformas de pago de terceros y vendedores minoristas en línea reconocidos directamente para inyectar un código JavaScript malicioso en las páginas de pago con tarjeta de sus sitios web. El código se ejecuta como parte del proceso de compra para transmitir la información de la tarjeta de pago de la víctima a los delincuentes cibernéticos, además de llegar al proveedor previsto.

Los que informaron incidentes en X-Force IRIS observaron estos tipos de ataques de primera mano en las múltiples vulneraciones en 2019 y notan que si bien los fragmentos de código malicioso podían ser básicos, el acuerdo de back-end de las plataformas subyacentes puede causar un impacto adicional donde los criminales pudieron atacar a miles de tiendas utilizando la misma técnica.

**Los grupos amenazantes prominentes que han atacado el sector minorista incluyen:**

| | |
|---|---|
| ITG14 (FIN7)HIVE0065 | Hive0062 (Magecart 11) |
| (TA505)ITG08 (FIN6) | Hive0066 (Magecart 12) |
| Hive0038 (FIN6) | Hive0067 (FakeCDN) |
| Hive0040 (Cobalt Gang) | Hive0068 (GetBilling) |
| Hive0053 (Magecart 2) | Hive0069 (Illum Group) |
| Hive0054 (Magecart 3) | Hive0070 (PostEval) |
| Hive0055 (Magecart 4) | Hive0071 (PreMage) |
| Hive0056 (Magecart 5) | Hive0072 (Qoogle) |
| Hive0057 (Magecart 6) | Hive0073 (ReactGet) |
| Hive0058 (Magecart 7) | Hive0083 (Inter Skimmer) |
| Hive0059 (Magecart 8) | Hive0084 (MirrorThief) |
| Hive0060 (Magecart 9) | Hive0085 (TA561) |
| Hive0061 (Magecart 10) | |

Además de los eliminadores de comercio electrónico en línea, el malware del punto de venta sigue siendo una técnica popular que los delincuentes cibernéticos usan contra los vendedores minoristas en las tiendas físicas para desviar datos de la tarjeta de pagos de las máquinas del punto del venta y los servidores back-end durante una transacción o cuando se graban los datos en la memoria.

## Transporte

El sector de transporte se considera parte de la infraestructura crítica de cualquier país. Las empresas de este sector movilizan la economía a través de tres tipos principales de transporte, incluido el transporte terrestre, el marítimo y el aéreo, para los servicios tanto industriales como de consumidor. Este sector fue el tercero más atacado en 2019, con ataques que disminuyeron en frecuencia del 13 % en 2018 al 10 % en 2019.

La clasificación de la industria del transporte en tercer lugar, luego de las finanzas y las ventas minoristas destaca el creciente atractivo de los datos y la infraestructura operada por las empresas de transporte. Estos activos atraen a los delincuentes cibernéticos y a los actores amenazadores del estado nacional por igual. La información con la que cuentan las empresas de transporte presenta un objetivo atractivo para los delincuentes cibernéticos, que potencialmente incluyen PII, información biográfica, números de pasaporte, información de programas de lealtad, datos de tarjetas de pago e itinerarios de viaje.

Dentro de este sector, las aerolíneas y los aeropuertos, en particular, están siendo atacados cada vez más por delincuentes cibernéticos y adversarios de estado nación que buscan rastrear a viajeros de interés o monetizar la información personal de los viajeros vendiéndola en la web oscura.

Las amenazas cibernéticas para la industria del transporte tienen un riesgo adicional en comparación con otros sectores, dado el potencial efecto cinético que puede tener un ataque, que pone en riesgo vidas humanas, así como el potencial de impactar también a otras industrias que dependen de los servicios de transporte que llevan a cabo sus operaciones.

Los grupos de actores amenazantes que atacan al sector del transporte fueron variados en 2019, ya que tanto grupos de delincuentes cibernéticos como adversarios de estado nación lanzaron ataques sobre las organizaciones en todo el mundo.

**Los grupos amenazantes prominentes que han atacado el sector de transporte incluyen:**

| | |
|---|---|
| ITG07 (Chafer) | ITG17 (Muddywater) |
| ITG09 (APT40) | Hive0016 (APT33) |
| ITG11 (APT29) | Hive0044 (APT15) |
| ITG15 (Energetic Bear) | Hive0047 (Patchwork) |

## Multimedia y entretenimiento

La cuarta industria más atacada de la clasificación de X-Force para 2019 fue el sector de los medios, que ha experimentado el 10 % de todos los ataques de las 10 principales industrias. El sector de medios subió en comparación con el 8 % del 2018 y escaló de la sexta posición a la cuarta.

El sector de medios incluye subindustrias de alto perfil tales como telecomunicaciones, así como empresas que producen, procesan y distribuyen medios de noticias y entretenimiento. La industria de los medios y el entretenimiento es un objetivo de gran valor para los atacantes cibernéticos que buscan influenciar la opinión del público, controlar los flujos de información o proteger la reputación de su organización o del país. En particular, los grupos de un estado nación pueden ver el contenido multimedia negativo como una amenaza importante para su seguridad nacional, mientras que para los delincuentes cibernéticos los ataques a los medios y al entretenimiento son financieramente lucrativos dado que pueden robar información antes de que salga al aire y pedir rescate.

Los delincuentes cibernéticos oportunistas y los adversarios de estado nación que generalmente atacaron este sector en 2019.

**Los grupos amenazantes prominentes que han atacado el sector de multimedia y entretenimiento incluyen:**

ITG03 (Lazarus)

Hive0003 (Newscaster)

Hive0047 (Patchwork)

**Servicios profesionales**

La industria de servicios profesionales presenta varias empresas que proporcionan servicios de consultoría especializada a otros sectores. Algunos ejemplos son las firmas que brindan apoyo jurídico, contable, de RR. HH. y a clientes especializados, por nombrar algunas. Este sector experimentó el 10 % de todos los ataques de las 10 industrias principales según los datos de X-Force, que fue un descenso desde los 12 % de 2018.

La información de vulneración de datos divulgada públicamente indica que los servicios profesionales también tenían la mayor cantidad de registros vulnerados de todas las industrias de nuestra clasificación. Muchas de estas firmas adquieren datos altamente sensibles de sus clientes, incluidos datos de demandas jurídicas, contables e impositivos, que pueden convertirse en un blanco lucrativo para los atacantes que buscan ganancias monetarias o información interna.

Además, esta industria incluye empresas de tecnología, que han sido cada vez más atacadas dado el acceso de terceros que poseen y pueden ser aprovechados por atacantes que intentan violar las organizaciones más grandes y potencialmente más seguras a las que sirven.

Sumado a esto, el flujo de trabajo diario de las firmas de servicios profesionales tiende a crear vectores de ataque naturales para los delincuentes a través de correos electrónicos de phishing y macros maliciosos. Muchas firmas de servicios profesionales dependen en gran medida de archivos de productividad, tales como adjuntos de documentos Word o Excel, para escribir contratos, comunicarse con clientes y completar tareas diarias. El uso de macros es uno de los vectores de ataque más notorios que los delincuentes cibernéticos explotan para plantar scripts maliciosos en los tipos de archivos que ninguna organización puede bloquear por completo.

Grupos de actores amenazadores notables que atacaron servicios profesionales en 2019: ITG01 (APT10, Stone Panda), un grupo patrocinado por un estado nación que parece originarse en China.

**Gobierno**

El sector gubernamental es la sexta industria más atacada de nuestra clasificación, con el 8 % de los ataques de las 10 industrias principales, sin cambios interanuales pero que ha subido en la clasificación general desde la séptima posición en 2018.

El sector gubernamental es un objetivo de alto valor para los actores cibernéticos de un estado nación que buscan obtener una ventaja por encima de sus adversarios percibidos, hacktivistas que buscan exponer información afectada o probar su proeza técnica, y delincuentes cibernéticos que buscan recompensas monetarias mediante la extorsión y el robo de datos.

Muchos gobiernos municipales han estado bajo ataque en los últimos años, dado que los delincuentes cibernéticos buscan recopilar dinero de las organizaciones que probablemente sean menos seguras que aquellas del sector privado. Las entidades gubernamentales poseen activos de valor para actores amenazantes, principalmente información confidencial y posibles secretos de estado, que pueden incluir PII sobre empleados y agentes del gobierno, información financiera, comunicaciones internas y la funcionalidad de redes críticas.

Los actores del estado nacional han demostrado un interés a largo plazo en atacar entidades del sector gubernamental, y X-Force IRIS evalúa que son muy capaces de hacerlo. Sin embargo, cada vez más en 2019, los grupos de delincuentes cibernéticos también atacaron entidades gubernamentales, buscando

cifrar y retener datos para rescate que los gobiernos necesitan para operar, particularmente a nivel municipal o provincial.

En 2019, más de 70 entidades gubernamentales fueron atacadas con ransomware solo entre enero y julio. Los delincuentes cibernéticos también robaron datos, incluidos datos de los sitios web de defensa, y luego los filtraron a la web oscura. Obviamente, los hacktivistas encontraron en el gobierno un objetivo atractivo, particularmente si hay un problema controvertido sobre el que desean realizar una declaración. A menudo las organizaciones gubernamentales no tienen el mismo nivel de financiación en seguridad cibernética que los sectores privados, pero aún deben mantener un servicio consistente para sus electores, exacerbando aún más el desafío que estos actores amenazantes representan para estas organizaciones.

Grupos de actores amenazantes notables que atacaron organismos gubernamentales en 2019. Diferentes delincuentes cibernéticos y grupos patrocinados por un estado nación.

## Educación

El sector de la educación experimentó un 8 % de todos los ataques de las 10 industrias principales, un aumento del anterior 6 % de 2018, que lo convierten en la séptima industria más atacada de nuestra clasificación.

La industria de la educación presenta una variedad de activos valiosos para los actores motivados en sentido financiero y del estado nacional. Desde Propiedad intelectual (IP) hasta PII, las organizaciones educativas son un amplio objetivo para diferentes tipos de actores amenazantes.

Cada uno con una motivación diferente, los actores adversarios han utilizado una variedad de vectores de infección inicial para vulnerar las redes de instituciones académicas, pero el método más comúnmente observado siguen siendo los correos electrónicos de phishing, que se suelen adaptar a instituciones académicas o áreas de investigación específicas.

Las organizaciones del sector de la educación suelen tener una presencia digital y una infraestructura de TI grande y variada. Operan diferentes activos que sirven a un gran número de usuarios que van desde el personal hasta los estudiantes y contratistas. Esta vasta superficie de ataque que los actores amenazantes pueden aprovechar para diversas actividades maliciosas es más difícil de asegurar. Informes publicados en octubre de 2019 Indicaron que al menos 500 escuelas resultaron atacadas por ataques cibernéticos, mayormente ransomware, en 2019, solo en EE. UU.

Algunos ejemplos notables de ataques más sofisticados en este sector incluyen actores amenazantes de un estado nación que afectan las redes de la universidad y luego las usan como punto de partida para infectar organizaciones multimedia y contratistas militares. De modo similar, los atacantes que buscan investigación financiada por EE. UU., suelen buscar modos de vulnerar las redes de la universidad para robar propiedad intelectual que en ocasiones puede ser inestimable.

**Los grupos amenazantes prominentes que han atacado el sector de educación incluyen:**

ITG05 (APT28)
ITG12 (Turla Group)
ITG13 (APT34)
ITG15 (Energetic Bear)
ITG17 (Muddywater)
Hive0075 (DarkHydrus)

IBM X-Force IRIS evalúa con confianza que esta industria seguirá siendo atacada por actores motivados por las finanzas como por actores afiliados al estado que busquen obtener acceso a información valiosa.

Los grupos de actores amenazantes notables que atacaron este sector en 2019 incluyeron facciones de delincuentes cibernéticos y adversarios de estado nación de China, Rusia e Irán.

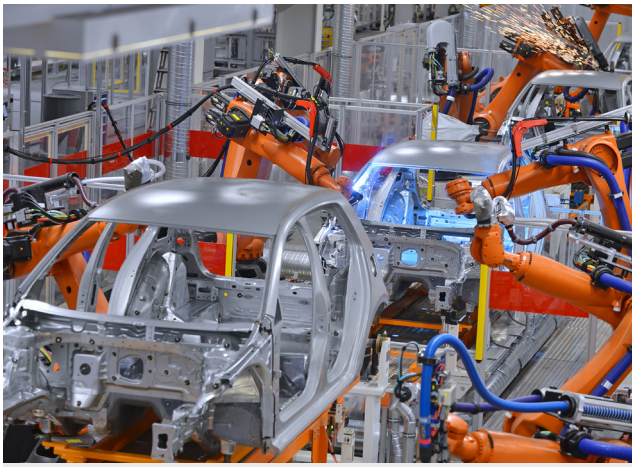
**Manufactura**

Al mover la economía a través de metales, químicos, bienes de capital y productos electrónicos, los fabricantes no están exentos de las amenazas de TI y las amenazas que afectan el piso de OT conectado. Con el 8 % de todos los ataques de las 10 industrias más atacadas, la manufactura aparece como la octava industria más atacada de nuestra clasificación, disminuyendo del 10 % de 2018.

Si bien es posible que este sector haya padecido año a año menos ataques, la disminución en la cantidad podría reflejar el hecho de que en muchos casos, la vulneración de datos del sector de manufactura no incluye información necesariamente sujeta a divulgación legal y a las reglamentaciones. Como resultado, los ataques no siempre se divulgan públicamente, lo que hace que parezca que los fabricantes reciben menos ataques de los que realmente reciben.

Los fabricantes también son organizaciones que operan entornos de TI y de OT, y por lo tanto están sujetos a las mismas amenazas que afectan a los sistemas ICS y SCADA. Pero si bien la seguridad de información de este sector se ha quedado rezagada en el pasado, la exitosa respuesta pública de un fabricante noruego a un importante ataque de ransomware en 2019 podría ser un indicativo de los cambios de enfoque en la seguridad cibernética de esta industria.

Los delincuentes cibernéticos o los actores de un estado nación que buscan una ganancia financiera y datos de IP probablemente sean las mayores amenazas cibernéticas para las empresas del sector de manufactura. Una de las técnicas de ataque más comúnmente usadas contra los fabricantes en 2019 fue el fraude de acuerdo de correo empresarial (BEC), especialmente si suelen hacer negocios con proveedores extranjeros. En dichos casos, los servidores de correo electrónico de la empresa, o incluso solo las cuentas de correo, se ven afectadas por atacantes que se insertan en hilos de comunicación existentes para ir desviando millones de dólares a cuentas que ellos controlan.



**Los grupos de amenaza notables que atacaron la industria de la manufactura incluyeron:**

ITG01 (APT10)
ITG09 (APT40)
HIVE0006 (APT27)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0076 (Tick)

Los fabricantes también son propensos a los ataques de cadenas de suministro y los adversarios del estado nación los pueden explotar para plantar puertas falsas o malware en los productos que fabrican y envían a otros países.

Del lado de la motivación financiera, los atacantes podrían acudir a los fabricantes por secretos comerciales y propiedad intelectual. Una investigación de años de una organización puede representar una ganancia rápida para los delincuentes cibernéticos en la web oscura o impulsar una ventaja de defensa o económica del estado nacional, especialmente en el caso de fabricantes de equipos militares o de defensa.

Los ataques de ransomware, phishing e inyección de SQLi también tendieron a sacudir con frecuencia la industria de manufactura, según los datos de X-Force.

## Energía

El sector de la energía es la novena industria más atacada de nuestra clasificación, ya que recibió el 6 % de todos los ataques e incidentes de las 10 industrias principales en 2019. La posición de este sector permanece sin cambios desde 2018, cuando también padeció el 6 % de los ataques.

Las empresas del sector energético demuestran ser objetivos ricos para los ataques cibernéticos en parte debido a su importancia como columna vertebral de la infraestructura crítica de cada país. La energía, en sus diversas formas, es esencial para la seguridad nacional y económica, y el funcionamiento diario de las ciudades e industrias.

Los objetivos de los ataques del sector energético son variados. Algunos activos lucrativos dentro de las empresas de energía, tales como los datos de clientes, material financiero, secretos comerciales e información de la tecnología del propietario son similares en valor a los que se encuentran en las empresas de otras industrias.

Lo que diferencia a la industria energética de las demás es la posibilidad de una interrupción y destrucción física de los sistemas de ICS y los sistemas de SCADA que ellos administran. Estos sistemas pueden ser objetivos altamente valiosos para los adversarios que desean monitorear o incluso controlar las operaciones de una instalación en particular, especialmente cuando se trata de situaciones de guerra informática y se cubren instalaciones nucleares de países rivales, por ejemplo. Esta industria también ha sido objetivo de malware destructivo, como ZeroCleare.

Un ataque exitoso en el sistema de ICS diseñado para interrumpir las operaciones puede tener efectos devastadores en los clientes que dependen de la electricidad, el gas, el petróleo o cualquier otro recurso que provenga del sector energético. Algunos ejemplos de dichos ataques y sus efectos perjudiciales se han observado en el pasado en una serie de incidentes que tuvieron como objetivo a las plantas de energía de Ucrania, supuestamente llevados a cabo por Rusia y destinados a la destrucción física.

**Los grupos amenazantes notables que han atacado este sector incluyen:**

ITG01 (APT10)
ITG09 (APT40)
ITG07 (Chafer)
ITG11 (APT29)
ITG12 (Turla Group)
ITG13 (APT34)
ITG15 (Energetic Bear)
ITG17 (Muddywater)
Hive003 (APT35)
HIVE0006 (APT27)
Hive0016 (APT33)
Hive0044 (APT15)
Hive0045 (Goblin Panda)
Hive0047 (Patchwork)
Hive0076 (Tick)
Hive0078 (Sea Turtle)
Hive0081 (APT34)

**Sector sanitario**

La décima industria más atacada, la industria sanitaria, representa el 3 % de todos los ataques de las 10 industrias más atacadas, que ha descendido desde la posición ocho y del 6 % de los ataques de 2018.

La preponderancia de la evidencia sugiere que los delincuentes cibernéticos con motivación económica son los principales atacantes de las redes del sector sanitario y de los dispositivos médicos, ya sea para robar y luego vender registros médicos en la web oscura, o para cifrar la red conectada a los dispositivos a fin de interrumpir la actividad y pedir rescate a las empresas.

La interrupción de las redes de asilos para ancianos y hospitales ha sido capaz de presionar a las organizaciones de atención sanitaria a pagar los ataques de ransomware a fin de restablecer sus operaciones lo antes posible y proteger las vidas humanas. En algunos casos, el rescate es simplemente irracional, como un pedido de USD 14 millones luego de un ataque de Ryuk en 2019.

A medida que nos introducimos al año 2020, el sector sanitario deberá seguir evolucionando su postura de seguridad para proteger los datos. Frente a los frecuentes ataques de ransomware, los hospitales deben fortalecer las capacidades de respuesta ante incidentes, y buscar ataques emergentes en dispositivos médicos inseguros que pudieran explotarse y conducir a un riesgo fácil y pivotante por parte de atacantes motivados.

Los grupos de actores amenazantes notables que atacaron este sector incluyeron grupos delictivos cibernéticos con motivación económica tales como los que operan ransomware Ryuk. Si bien los ataques de ransomware destacan la crisis que se podría desarrollar cuando los hospitales resultan afectados, no vemos que haya un interés de un estado nación persistente en este sector.

# Información geocéntrica

## Los actores amenazantes atacaron todas las regiones geográficas en 2019, pero los niveles más altos de actividad se observaron en América del Norte, Asia y Europa.

Los investigadores de X-Force también notaron actividad del actor amenazante hacia el Medio Oriente y Sudamérica en 2019, que en el primer caso consiste más en ataques de hacktivistas y de estado nación, mientras que Sudamérica se vio principalmente afectada por actores con motivaciones financieras.

En esta sección profundizaremos en estas geografías para comprender mejor la naturaleza de los ataques que observó X-Force, los actores amenazantes clave centrados en cada área y las fechas clave para que estemos alertas en 2020 por potenciales riesgos en la actividad del actor amenazante. Algunas geografías destacan los actores amenazadores que estuvieron particularmente activos en ataques en el área en años recientes, pero esta lista no es exhaustiva e incluye datos anteriores a 2019. Esta sección utiliza la nomenclatura de Grupo de Amenaza de IBM tal como se describió anteriormente, y aprovecha los datos de la respuesta ante incidentes globales de IBM así como los datos de vulneración divulgados públicamente.

## América del Norte

América del Norte clasificó como la región más alta en todas las categorías de ataques de actores amenazantes, y constituyó el 44 % de los incidentes en 2019.

América del Norte alberga potenciales blancos y mantiene una cantidad significativa de infraestructura de internet, lo que la convierte en un objetivo fácil para los actores delictivos. En 2019, América del Norte tuvo más de 5 mil millones de registros afectados.

IBM respondió ante múltiples incidentes en América del Norte en 2019 que utilizaron malware generalizado, códigos que se pueden comprar en mercados clandestinos o se pueden obtener en forma gratuita. El malware generalizado puede ser difícil de atribuir, pero puede ser muy efectivo para alcanzar objetivos delictivos.

La actividad de los actores del estado nación que atacan a América del Norte siguen siendo los mismos, pero no se observaron incidentes importantes en 2019. Las recientes negociaciones comerciales entre Estados Unidos y China podrían llevar a un aumento de ataques a las organizaciones que hacen negocios en ambas regiones, y estas organizaciones deberían mantenerse atentas siempre que estas negociaciones permanezcan inconclusas.

**Próximos eventos con significado histórico para la seguridad cibernética:**

13 de julio
(Convención Nacional Democrática, Estados Unidos)

24 de agosto
(Convención Nacional Republicana, Estados Unidos)

3 de noviembre
(Elección Presidencial de EE. UU.)

**Los grupos de actores amenazantes que han atacado este sector incluyen:**

ITG05 (APT28)
ITG08 (FIN6)
ITG11 (APT29)
ITG15 (Energetic Bear)
Hive0082 (Cobalt Dickens)
Hive0042 (Kovter)
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0006 (APT27)
Hive0003 (APT35)
ITG01 (APT10)
ITG03 (Lazarus)
ITG04 (APT19)
ITG09 (APT40)
ITG07 (Chafer)

**Actividad de ataque más notable observada en actividades de respuesta ante incidentes de X-Force en 2019:**

Acuerdo de Correo Electrónico Comercial, Ransomware, ataque de un estado nación sobre el sector financiero.

## Asia

Asia recibió el segundo mayor puntaje en el análisis de X-Force, ya que cuenta con el segundo mayor número de incidentes en vulneraciones públicas y representa el 22 % de los incidentes de 2019. Asia tuvo más de 2 mil millones de registros vulnerados en 2019, y es el segundo únicamente de América del Norte durante este año.

Una cantidad significativa de actores amenazadores centró sus ataques en organizaciones afiliadas a Asia, especialmente en la península de Corea, Japón y China. Muchos de los ataques observados dentro de esta región siguieron los TTP de los actores de un estado nación. Un ejemplo fue ITG10, donde posiblemente los actores fueron norcoreanos que atacaron entidades de Corea del Sur. Otro ejemplo es ITG01, donde posiblemente fueron actores chinos que atacaron Japón.

Los eventos geopolíticos recientes en Asia han aumentado la probabilidad de actividad afiliada a un estado nación en esta región. Las protestas democráticas de Hong Kong y las posteriores medidas severas han puesto a China al límite. Las tensiones cada vez mayores entre Corea del Norte y sus vecinos han envalentonado al régimen. La absorción de india de la región de Kashmir ha conducido de modo similar a elevar las tensiones en la región.

A medida que ingresamos al año 2020, es esencial controlar estos intereses geopolíticos potencialmente volátiles a fin de comprender el riesgo que presentan para las organizaciones que operan en esta región.

**Próximos eventos con significado histórico para la seguridad cibernética:**

24 de julio
(Juegos Olímpicos de Tokio 2020)

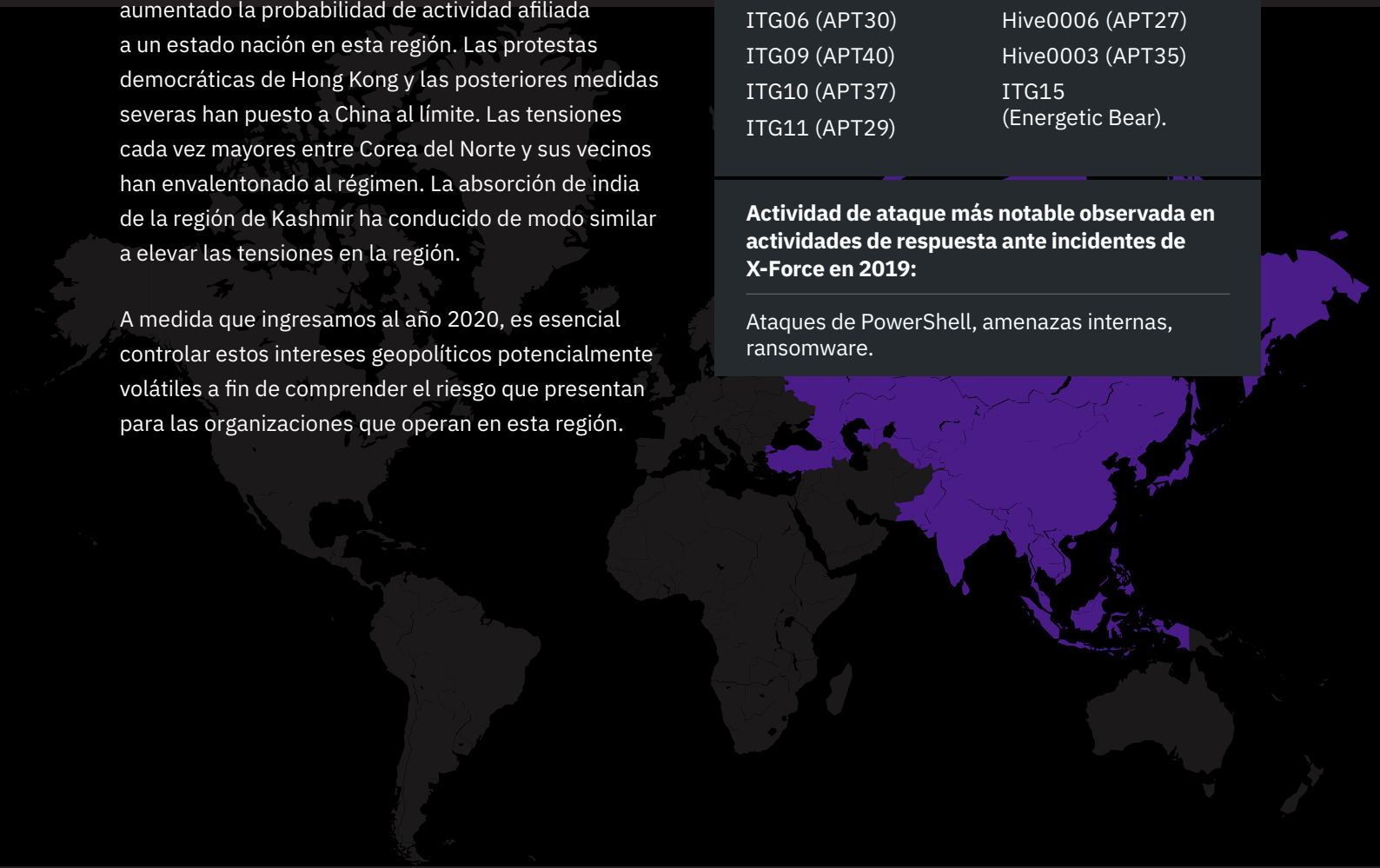
10 de octubre
(Día de la Independencia de Taiwán).

**Los grupos de actores amenazantes que han atacado este sector incluyen:**

Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0045 (Goblin Panda)
Hive0049 (Samurai Panda)
ITG01 (APT10)
ITG03 (Lazarus)
ITG05 (APT28)
ITG06 (APT30)
ITG09 (APT40)
ITG10 (APT37)
ITG11 (APT29)
ITG16 (Kimsuky)
Hive0016 (APT33)
Hive0040 (Cobalt Gang)
Hive0047 (Patchwork)
Hive0063 (DNSpionage)
Hive0076 (Tick)
Hive0079 (Labryinth Cholima)
Hive0006 (APT27)
Hive0003 (APT35)
ITG15 (Energetic Bear).

**Actividad de ataque más notable observada en actividades de respuesta ante incidentes de X-Force en 2019:**

Ataques de PowerShell, amenazas internas, ransomware.



## Europa

Europa cayó víctima de niveles de actividades maliciosas similares a Asia, con el 21 % de los incidentes.

A diferencia de Asia, que se ve mayormente afectada por estados nacionales rivales, Europa parece ser el blanco principalmente de actores amenazadores con motivación económica. Esta diferencia se puede explicar por un mayor potencial para el robo en empresas con base en Europa en función de las tasas de cambio de las divisas. Alternativamente, las motivaciones delictivas podrían buscar propiedades intelectuales, que se pueden vender a la competencia por una cifra significativa.

La salida de Gran Bretaña de la Unión Europea (Brexit) puede tener repercuciones en los círculos hacktivistas al comienzo del año 2020, pero no se han observado casos en 2019. Además, las próximas elecciones en importantes países de la Unión Europea (Alemania, Francia) podrían ser blanco de actores de un estado nación que buscan influir en las políticas de estos países.

**Próximos eventos con significado histórico para la seguridad cibernética:**

31 de enero
(Reino Unido sale de la Unión Europea bajo el artículo 50)

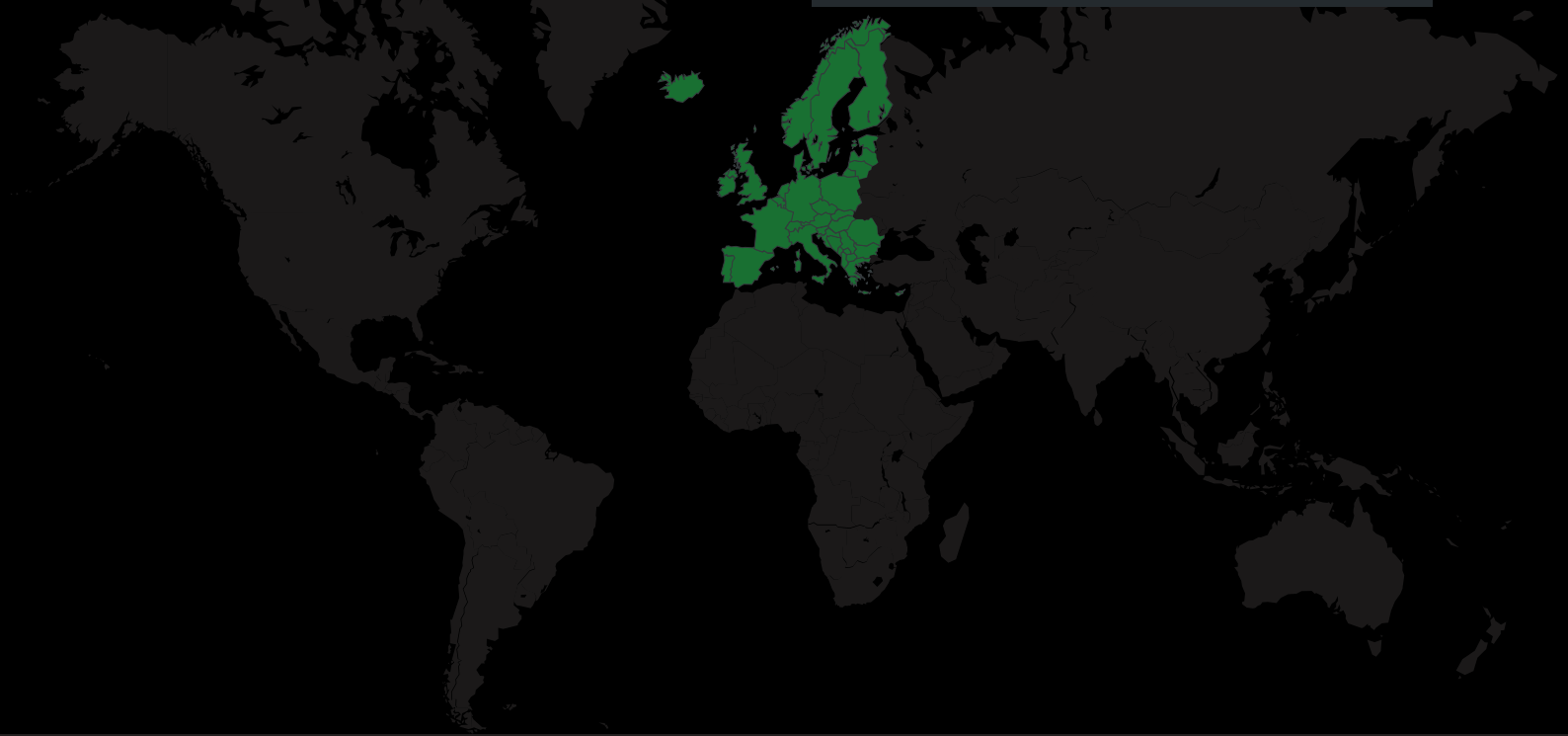
28 de junio
(Día de la Constitución de Ucrania/Aniversario de NotPetya).

**Los grupos de actores amenazantes que han atacado este sector incluyen:**

ITG05 (APT28)
ITG08 (FIN6)
ITG12 (Turla)
ITG15 (Energetic Bear)
ITG09 (APT40)
ITG07 (Chafer)
ITG11 (APT29)
ITG14 (FIN7)
ITG17 (Muddywater)
Hive0006 (APT27)
Hive0003 (APT35)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0063 (DNSpionage)

**Actividad de ataque más notable observada en actividades de respuesta ante incidentes de X-Force en 2019:**

Acuerdo RDP, malware POS, amenazas internas.



## Medio Oriente

X-Force IRIS observó una cantidad de incidentes afiliados a un estado nación que afectaron a las organizaciones en el Medio Oriente en 2019, pero las métricas generales para la actividad de actores amenazantes fueron relativamente bajas en 2019, con un 7 % de incidentes en esta región.

Podría haber muchas explicaciones para este descenso en la actividad, como que otras geografías proporcionan un mayor retorno de la inversión para la actividad delictiva cibernética. Sin embargo, a diferencia de otras geografías, el Medio Oriente tuvo una proporción mayor de hacktivistas y actividad de un estado nación, en comparación con otras partes del mundo.

La actividad hacktivista podría relacionarse con la agitación política en la región en 2019, con múltiples incidentes importantes que involucraron a Irán. De manera similar, la actividad del estado nación, como TIG13 que persigue intereses del estado iraní, siguieron objetivos del estado al atacar las organizaciones del sector energético en esta región con ataques destructivos.

La agitación política y la guerra informática cinética en Yemen siguen produciendo riesgos de actividad de amenazas cibernéticas, en la que los actores de todos los lados del conflicto están usando ataques cibernéticos para distribuir su mensaje y generar ingresos. Es posible que estos riesgos sigan durante 2020 dado que las diferentes partes siguen amenazándose públicamente entre sí sobre ese conflicto.

**Próximos eventos con significado histórico para la seguridad cibernética:**

21 de noviembre
(Torneo de la Copa Mundial de Fútbol 2022, Qatar)

**Los grupos de actores amenazantes que han atacado este sector incluyen:**

Hive0044
ITG07 (Chafer)
ITG13
Hive0081 (APT34)
Hive0078 (Sea Turtle)
Hive0075 (DarkHydrus)
Hive0063 (DNSpionage)
Hive0047 (Patchwork)
Hive0022 (Gaza Cybergang)
Hive0016 (APT33)
Hive0006 (APT27)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG10 (APT37)
ITG09 (APT40)
ITG05 (APT28)
ITG01 (APT10)

**Actividad de ataque más notable observada en actividades de respuesta ante incidentes de X-Force en 2019:**

Malware destructivo, ataque de DDOS, script web.

## Sudamérica

Sudamérica luchó contra una importante actividad delictiva cibernética en 2019, pero no recibió el mismo nivel de enfoque que las tres principales regiones geográficas, y representa solo el 5 % de los incidentes. Sin embargo, año tras año la actividad sigue aumentando en esta región, y X-Force observa un repunte en actividades significativas de respuesta ante incidentes en los sectores de servicios financieros y de ventas minoristas.

Los incidentes observados en esta región incluyeron actividad de ransomware, que creció en popularidad durante todo 2019.

**Próximos eventos con significado histórico para la seguridad cibernética:**

12 de junio
(Torneo de Fútbol Copa América 2020, Colombia y Argentina).

**Los grupos de actores amenazantes que han atacado este sector incluyen:**

Hive0081 (APT34)
Hive0044 (APT15)
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG05 (APT28)
ITG03 (Lazarus)
ITG01 (APT10)

**Actividad de ataque más notable observada en actividades de respuesta ante incidentes de X-Force en 2019:**

Acuerdo de Correo Electrónico Comercial, Ransomware, ataque de un estado nación sobre el sector financiero.

# Preparación para la resiliencia en 2020

## En función de los hallazgos de IBM X-Force en este informe, estar al tanto de la inteligencia de amenazas y crear capacidades de respuesta sólidas son modos impactantes para mitigar las amenazas en el panorama evolutivo, independientemente de la industria o el país en que uno opere.

Nuestro equipo recomienda una cantidad de pasos que cada organización puede seguir a fin de prepararse mejor para las amenazas cibernéticas en 2020:

- Aprovechar la inteligencia de amenazas para comprender mejor las motivaciones y las tácticas del actor amenazador a fin de priorizar los recursos de seguridad.
- Crear y capacitar un equipo de respuesta ante incidentes dentro de su organización. Si eso no es posible, establezca una capacidad efectiva de respuesta ante incidencias para garantizar una rápida acción ante incidentes de alto impacto. En 2019, IBM Security observó que los impactos contenidos redujeron considerablemente los costos asociados, con la pronta intervención de nuestro equipo en una infección MegaCortex para detener el ataque de ransomware a mitad de camino y evitar miles de dólares en daños.
- Poner a prueba el plan de respuesta ante incidentes de su organización a fin de desarrollar la memoria muscular. Los ejercicios teóricos o las experiencias de rango cibernético pueden proporcionarle a su equipo una experiencia crítica para mejorar el tiempo de reacción, reducir el tiempo de inactividad y por último ahorrar dinero en caso de vulneración.
- La implementación de la autenticación multifactor (MFA) sigue siendo una de las prioridades de seguridad más eficientes para las organizaciones. En 2019, el robo o la reutilización de credenciales fue uno de los métodos más comunes de ataques observados que utilizaron los actores amenazadores, y MFA puede inhibir de manera efectiva este ataque antes de que se lleve a cabo.
- Asegurar que la organización tiene una solución implementada para detectar y bloquear dominios falsificados, tales como Quad9, debido a la prevalencia de phishing como vector de ataque.
- Tener copias de seguridad, ponerlas a prueba y almacenarlas sin conexión. No solo garantizar la presencia de copias de seguridad sino también su efectividad mediante pruebas del mundo real marca una diferencia crítica para garantizar la seguridad de la organización.

# Avance con aportes clave

## En 2020, las organizaciones deberán preocuparse por las amenazas nuevas y antiguas.

- La superficie del riesgo seguirá creciendo en 2020, con más de 150.000 vulnerabilidades actuales y casos nuevos que se informan regularmente.
- Con más de cuatro veces la cantidad de registros vulnerados en 2019 en comparación con 2018, el año 2020 podría ver otro gran número de registros perdidos debido a vulneraciones y ataques.
- Los actores amenazadores siguen cambiando sus perspectivas a diferentes vectores de ataque, con mayores ataques a dispositivos de IoT, tecnología operativa (OT) y sistemas médicos e industriales conectados, por nombrar algunos.
- El malware que utilizan los actores amenazadores sigue fluctuando, y el ransomware, los crytominers y las botnets llevan la delantera en diferentes puntos en 2019. Se espera que esta tendencia continúe en 2020, es decir que las organizaciones deberán protegerse contra diferentes amenazas que van cambiando con el tiempo.
- Los altos niveles de innovación de código para el ransomware y los cryptominers podrían implicar la continuidad en la evolución de estas amenazas en 2020, por lo que se requerirán mejores capacidades de detección y contención.
- La actividad de spam continúa incesante, lo que requiere que las organizaciones creen una lista negra minuciosa, coloquen parches para la vulnerabilidad y monitoreen amenazas.
- Año tras año el cambio en ataques específicos a la industria destaca el riesgo de todos los sectores de la industria y una necesidad de avances y madurez significativos en programas de ciberseguridad en todos los ámbitos.
- Las organizaciones pueden usar su ubicación geográfica para ayudar a identificar a los atacantes y las motivaciones de ataque más probables a fin de calcular y mitigar algunos riesgos relevantes que podrían enfrentar.

# Acerca de X-Force

IBM X-Force estudia y controla las últimas tendencias de amenazas, asesora a los clientes y al público en general sobre las amenazas emergentes y críticas, y ofrece contenido de seguridad para ayudar a proteger a los clientes de IBM.

Desde la protección de las aplicaciones, la infraestructura y los datos hasta servicios de seguridad en la nube y administrados, IBM Security Servicies cuenta con la experiencia para ayudar a proteger sus activos críticos. IBM Security protege algunas de las redes más sofisticadas del mundo y emplea a algunas de las mejores mentes del negocio.

Conozca más acerca de IBM Security →

## Colaboradores

Michelle Alvarez
Dave Bales
Joshua Chung
Scott Craig
Kristin Dahl
Charles DeBeck
Ari Eitan (Intezer)
Brady Faby (Intezer)
Rob Gates
Dirk Harz
Limor Kessem
Chenta Lee
Dave McMillen
Scott Moore
Georgia Prassinos
Camille Singleton
Mark Usher
Ashkan Vila
Hussain Virani
Claire Zaboeva
John Zorabedian

**IBM Security**
New Orchard Rd
Armonk, NY 10504
Producido en los Estados Unidos de América
Febrero de 2020

Producido en los Estados Unidos de América
Febrero de 2020



IBM **Security**