INFORME 2021

El IoT en la empresa: edición oficina vacía

¿Qué sucede cuando los empleados abandonan sus dispositivos inteligentes en el trabajo?

zscaler™

A lo largo de 2020 y hasta bien entrado 2021, la pandemia de la COVID-19 dejó muchas oficinas corporativas en un silencio inquietante y sin empleados. Pero a pesar de la falta de gente, estos edificios seguían bullendo de actividad bajo la superficie. Los propios edificios no eran lo único que quedaba abandonado: los relojes inteligentes, la señalización digital, las impresoras en red y muchos otros dispositivos del IoT seguían conectados a la red, actualizando datos, realizando funciones, esperando órdenes.

Los autores de amenazas se dieron cuenta y muchos intentaron aprovecharse de ello. Y esto sucedía en medio del enorme cambio global al trabajo desde cualquier lugar. Esto se traduce en la asombrosa cifra de 833 programas de malware de IoT bloqueados cada hora.

La creciente variedad de dispositivos IoT que llegan a las redes corporativas incluye de todo, desde relojes inteligentes y cámaras IP hasta automóviles y muebles musicales. El setenta y seis por ciento de las transacciones se producen en canales de texto sin cifrar, aunque todos los dispositivos utilizan SSL para al menos un subconjunto de sus comunicaciones. Las organizaciones deben emplear políticas y arquitecturas de confianza cero para proteger sus redes de ser explotadas a través de estos dispositivos. Este informe del equipo de investigación de amenazas de Zscaler ThreatLabz analiza en profundidad tanto los dispositivos IoT autorizados como los no autorizados y las tendencias de malware de IoT basadas en los datos de dos semanas de la nube de Zscaler.

Vamos a analizar los datos de dos estudios: un estudio de huellas digitales de dispositivos IoT que identifica los dispositivos IoT y el tráfico, y un estudio de malware de IoT basado en los datos de la nube Zscaler. Debido a que los dispositivos IoT (especialmente los no autorizados) no tienen agentes, todos los datos de este informe representan dispositivos y ataques a redes corporativas en ubicaciones de oficina física. Los datos para este informe se recogieron entre el 15 de diciembre y el 31 de diciembre de 2020, cuando se cerraron la mayoría de las oficinas comerciales no esenciales.

Aumento del 700 % en el malware específico de IoT con respecto al año anterior.

Hallazgos clave

- El malware de IoT en las redes corporativas ha aumentado en un 700 por ciento desde nuestro estudio de 2019, a pesar de que gran parte de la fuerza laboral de todo el mundo trabaja desde casa
- Los dispositivos de entretenimiento y automatización del hogar fueron los que plantearon el mayor riesgo debido a su variedad, al bajo porcentaje de comunicación cifrada y a las conexiones con destinos sospechosos
- Gafgyt y Mirai (familias de malware que se usan en botnets) representaron el 97 por ciento de las cargas de malware de IoT bloqueadas por la nube de Zscaler
- Los sectores de tecnología, fabricación, venta al por menor y al por mayor y sanidad representaron el 98 por ciento de las víctimas de ataques de IoT
- La mayoría de los ataques se originaron en China, Estados Unidos e India
- La mayoría de los objetivos de los ataques de IoT estaban en Irlanda, Estados Unidos y China

Huellas digitales de dispositivos IoT

Dispositivos más comunes

Al examinar más de 500 millones de transacciones de dispositivos IoT, ThreatLabz identificó 553 tipos de dispositivos diferentes de 212 fabricantes y los clasificó en 21 categorías. Las tres categorías más comunes, que representan casi el 65 por ciento del total de dispositivos, fueron decodificadores (29 por ciento), televisores inteligentes (20 por ciento) y relojes inteligentes (15 por ciento).

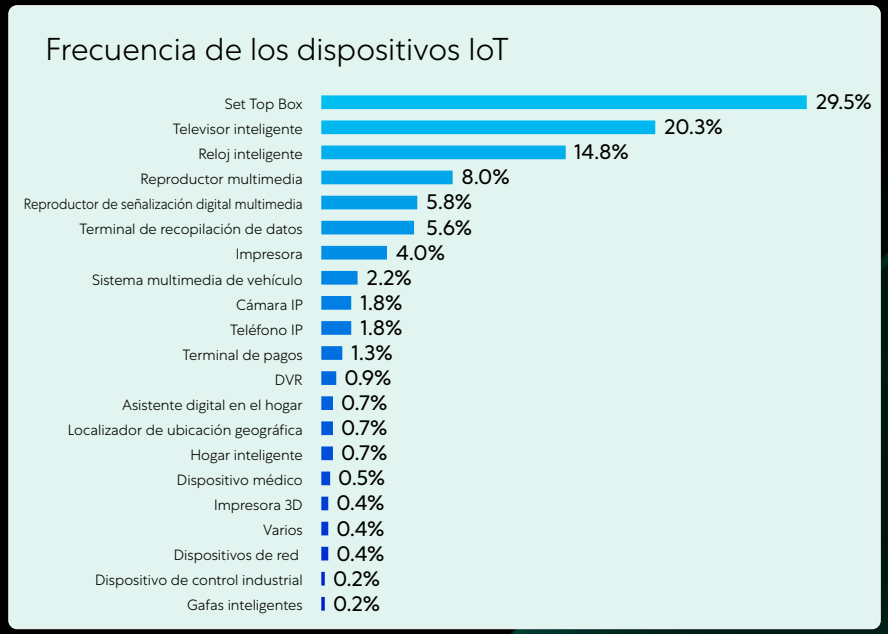
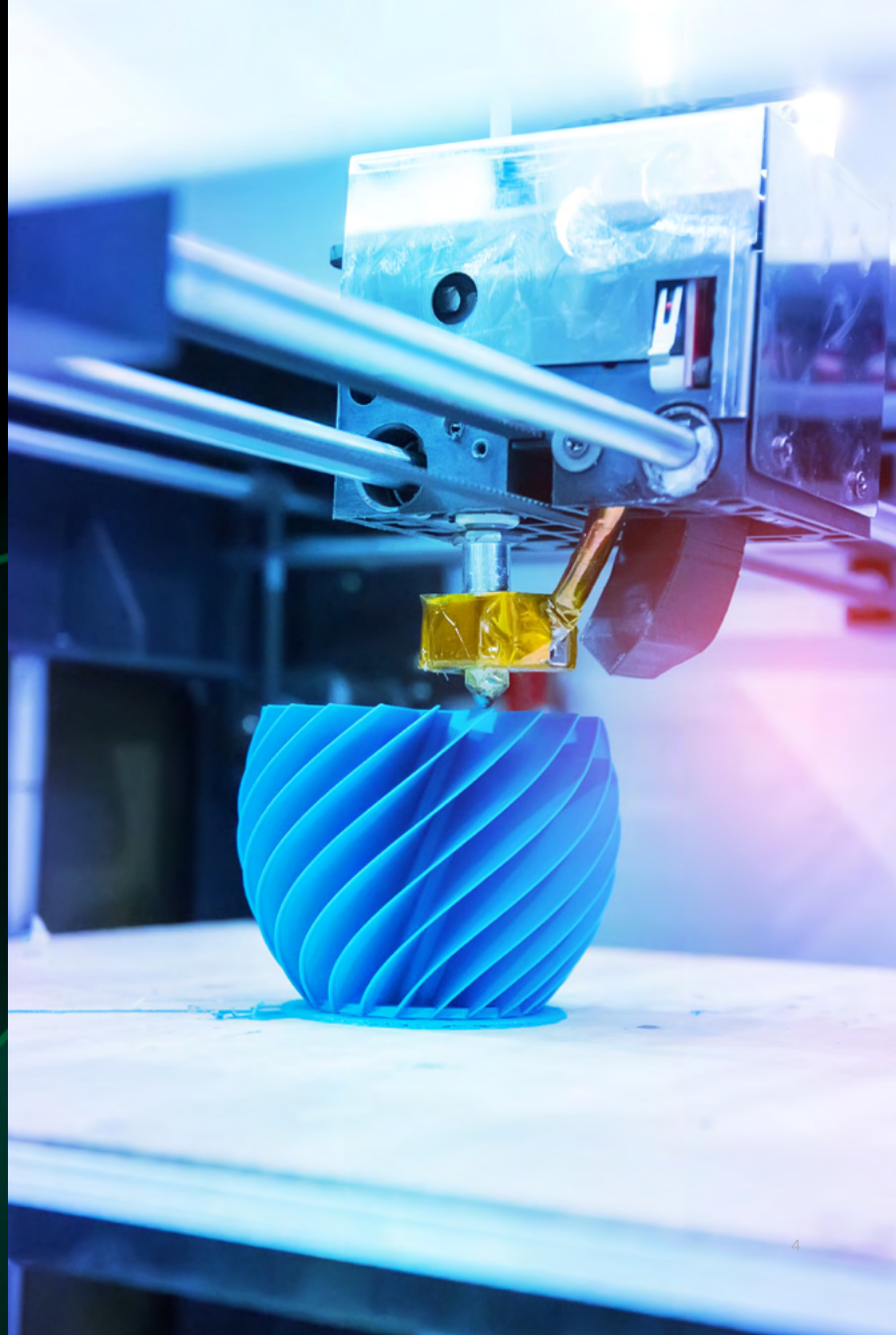


Figura 1: Frecuencia de dispositivos IoT



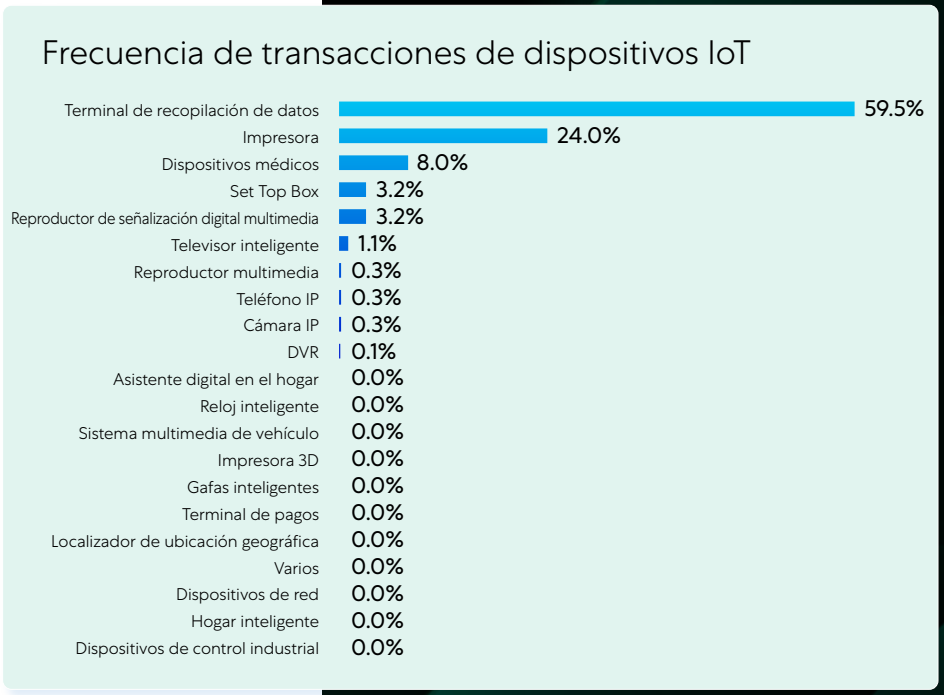
¿El Internet de los muebles musicales?

El "Internet de las cosas" sigue expandiéndose a nuevas categorías, algunas de las cuales pueden estar completamente fuera del radar de los equipos de TI. ThreatLabz descubrió una serie de dispositivos inesperados que se conectan a la nube, entre ellos:

- **Refrigeradores inteligentes:** un refrigerador inteligente de Samsung tiene la capacidad de transmitir música, videos y contenido desde el teléfono del propietario a una pantalla en la puerta del refrigerador.
- **Lámpara musical:** Ikea y Sonos han creado una lámpara de mesa combinada con un reproductor multimedia inteligente llamado Symfonisk.
- **Automóviles:** los reproductores multimedia de los automóviles Tesla y Honda se conectaban a las redes corporativas.
- **Tarjetas de memoria wifi:** las tarjetas de memoria wifi de Eye Fi, generalmente utilizadas en las cámaras para almacenar y compartir fotos, enviaban tráfico a través de la nube de Zscaler.

Dispositivos más activos

Las transacciones de dispositivos IoT representaron el 0,038 por ciento del total de transacciones en la nube de Zscaler durante el período de dos semanas. Algunos dispositivos realizaron muchas más transacciones que otros: los terminales de recogida de datos y las impresoras realizaron por sí solos más del 80 por ciento del tráfico total del IoT, tal y como se muestra en la figura 2.



Base: 575 091 158 transacciones de dispositivos IoT
Figura 2: Transacciones de dispositivos IoT

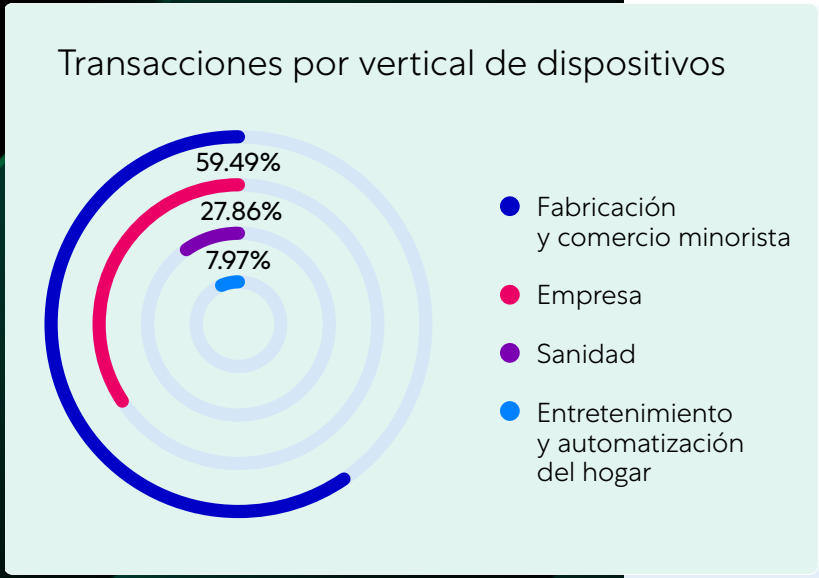


Figura 3: Dispositivos IoT por tipo

Tráfico por dispositivo: clasificación vertical

Los dispositivos IoT se agruparon en cuatro categorías en función de los sectores que los produjeron:

- **Los dispositivos de fabricación/minorista** representaron el 59 por ciento de las transacciones e incluían 57 tipos de dispositivos diferentes de 20 fabricantes; entre ellos, impresoras 3D, rastreadores de geolocalización, dispositivos de control industrial, sistemas multimedia automotrices, terminales de recopilación de datos y terminales de pago.
- **Los dispositivos empresariales** representaron el 28 por ciento de las transacciones: reproductores multimedia de señalización digital, grabadores de vídeo digital, cámaras y teléfonos IP, impresoras y dispositivos de red.
- **Los dispositivos sanitarios** representaron el ocho por ciento de las transacciones e incluyeron una serie de dispositivos médicos principalmente de tres fabricantes: GE Healthcare, Abbott Laboratories y HOLOGIC.
- **Los dispositivos de entretenimiento y automatización del hogar** supusieron el cinco por ciento de las transacciones generadas por una amplia variedad de dispositivos como asistentes digitales para el hogar, reproductores multimedia, decodificadores, gafas inteligentes, dispositivos domésticos inteligentes, televisores inteligentes y relojes inteligentes. Aunque estos representaron el porcentaje más bajo de transacciones, fueron los más variados e incluyeron numerosos dispositivos de consumo: un total de 420 dispositivos de 150 fabricantes diferentes.

Los dispositivos IoT se comunican en texto sin formato la mayor parte del tiempo

ThreatLabz observó que el 76 por ciento de las transacciones totales de los dispositivos IoT se produjeron a través de canales de texto sin formato, con solo el 24 por ciento de las transacciones a través de canales cifrados seguros. Aunque esta proporción parece inaceptablemente baja, supone una mejora triplicada con respecto a nuestro estudio de 2019, en el que solo el 8,5 por ciento de las comunicaciones de IoT estaban cifradas. No obstante, el riesgo de seguridad persiste: las comunicaciones en texto plano son mucho más fáciles de espiar para los atacantes o, peor aún, de interceptar y modificar, lo que les permite explotar los dispositivos IoT con fines maliciosos.

Los 553 dispositivos que se observaron en el estudio utilizaban SSL en alguna medida, pero el porcentaje de comunicaciones que realmente se cifraron variaba mucho según el tipo de dispositivo. Los dispositivos empresariales y de entretenimiento doméstico se comunicaron casi exclusivamente mediante texto sin formato, mientras que los dispositivos sanitarios lo hacían a través de SSL aproximadamente la mitad de las veces.

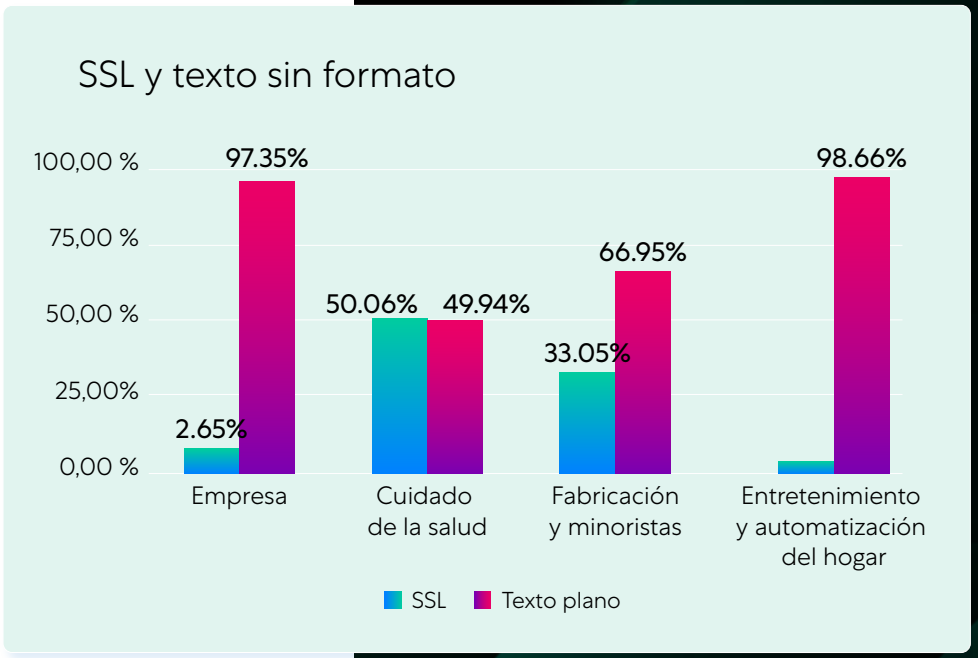


Figura 4: Porcentaje de comunicaciones cifradas por tipo de dispositivo

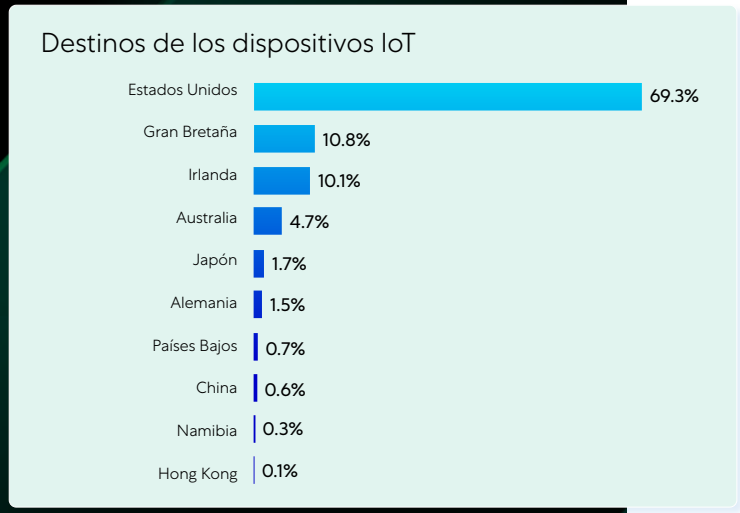


Figura 5: Principales destinos de las comunicaciones IoT

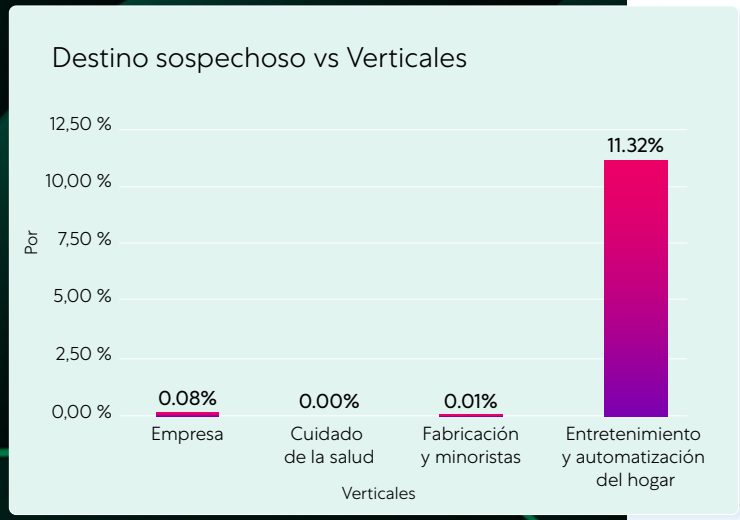


Figura 6: Porcentaje de tráfico sospechoso por tipo de dispositivo

¿Con qué países hablan los dispositivos IoT?

ThreatLabz examinó los países a los que los dispositivos IoT dirigían los datos, denominados "destinos". La mayor parte de esta comunicación es legítima, los dispositivos IoT hacen lo que están diseñados para hacer, que es enviar y recibir datos. Estados Unidos fue, con diferencia, el principal destino: recibió el 69 por ciento del tráfico, seguido de Gran Bretaña (11 por ciento) e Irlanda (10 por ciento). A continuación se muestran los diez países de destino principales.

Los dispositivos de entretenimiento y automatización del hogar tienden a dirigirse mucho más a China y Rusia

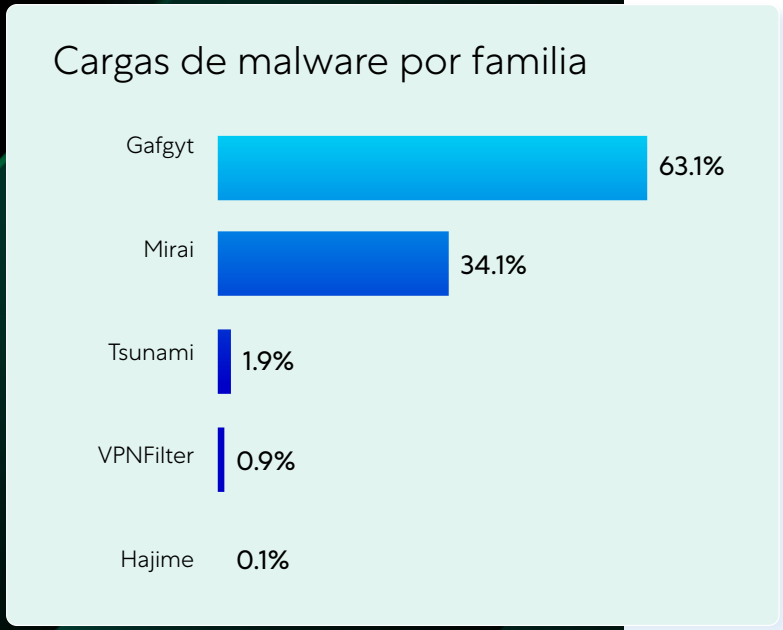
El once por ciento del tráfico proveniente de dispositivos de entretenimiento y automatización del hogar se dirigió a China y Rusia. Aunque gran parte de este tráfico es legítimo y no malicioso, se trata de destinos que ThreatLabz considera sospechosos por su potencial para el espionaje gubernamental y otras vulnerabilidades de datos. La práctica totalidad (el 99,9 por ciento) de este tráfico sospechoso provenía de televisores inteligentes y decodificadores.

Por el contrario, menos del 1 por ciento del tráfico de ida y vuelta de los dispositivos diseñados para casos de uso empresarial, sanitario y de fabricación y comercio minorista se dirigía a destinos sospechosos.

Estudio de malware de IoT

Durante ese mismo período de dos semanas de nuestro estudio de huellas digitales de IoT, ThreatLabz también analizó las actividades específicas del malware de IoT en la nube de Zscaler.

ThreatLabz observó aproximadamente 300 000 transacciones bloqueadas relacionadas con malware, vulnerabilidades y comunicaciones de comando y control de IoT, lo que representa un aumento de casi el 700 por ciento con respecto al año anterior. En cuanto al volumen de transacciones de malware, observamos un total de 18 000 hosts únicos y aproximadamente 900 entregas de cargas útiles únicas en un plazo de 15 días.



Base: 900 cargas útiles
Figura 7: Cargas útiles únicas de malware por familia

Principales amenazas de IoT

Las familias de malware Gafgyt y Mirai fueron, con diferencia, las dos familias de malware de IoT más prolíficas en nuestro estudio. De hecho, el 97 por ciento de las 900 entregas de cargas útiles únicas que observamos pertenecían a estas dos familias. Otras familias activas fueron Tsunami, VPNFilter y Hajime.

Mientras que Gafgyt fue la que tenía la mayor cantidad de cargas útiles únicas, las cargas útiles del malware Mirai se utilizaron con más frecuencia en los ataques de IoT durante nuestro estudio. Si se observa el volumen de transacciones, el 76 por ciento de los ataques bloqueados procedían de la familia de malware Mirai, el 5 por ciento de Gafgyt y el 19 por ciento de otros.

Botnets de IoT
Las vulnerabilidades de dispositivos IoT pueden proporcionar a los atacantes acceso tanto al dispositivo como a las redes conectadas, lo que permite todo tipo de actividades maliciosas. Mirai y Gafgyt son particularmente conocidos por usar dispositivos para crear redes de bots: redes de dispositivos bajo el control de un atacante que permiten ataques coordinados a gran escala. Se han utilizado las redes de bots para ataques de denegación de servicio distribuidos (DDoS), infracciones financieras, minería de criptomonedas e intrusiones selectivas, por citar algunos. La red de bots de Mirai es conocida por lanzar el que fuera el mayor ataque DDoS de la historia en 2016, que provocó interrupciones generalizadas de Internet. ThreatLabz evaluó los intentos de devolución de llamadas de redes de bots como parte de este estudio de malware y descubrió que los atacantes se dirigían no solo a los dispositivos IoT, sino también a una serie de routers populares y otros dispositivos de red para llevar a cabo estos ataques:

Los mejores dispositivos de devolución de llamada de red de bots	
CCTV y DVR de más de 70 proveedores	DVR MVPower
Múltiples dispositivos que utilizan el SDK de Realtek con el daemon miniigd	Dispositivos Linksys
Huawei HG532	Dispositivos Netgear R7000/R6400
Router ZyXEL	Routers Netgear DGN1000
Routers Dasan GPON	Dispositivos D-Link
Routers Eir D1000	Dispositivos Vacron NVR
Dispositivos D-Link	

Sectores más atacados

Las empresas tecnológicas fueron las que sufrieron el mayor índice de ataques de malware de IoT, con un 40 % de las infecciones. Los siguientes sectores más afectados fueron la industria manufacturera (28 por ciento) y el comercio minorista y mayorista (24 por ciento).

Países con más ataques de malware

En nuestro estudio, se descubrió que el 88,5 por ciento de los dispositivos IoT comprometidos reenviaban los datos a servidores de uno de estos tres países: China (56 por ciento), Estados Unidos (19 por ciento) o India (14 por ciento). Estos se conocen como países de "destino de malware" y en cada caso entregan el malware directamente o se conectan a él después de la infección. Algunos atacantes configurarán servidores de comando y control dentro del país al que están dirigidos, por lo que es posible que la ubicación del servidor no necesariamente indique la ubicación real del atacante.

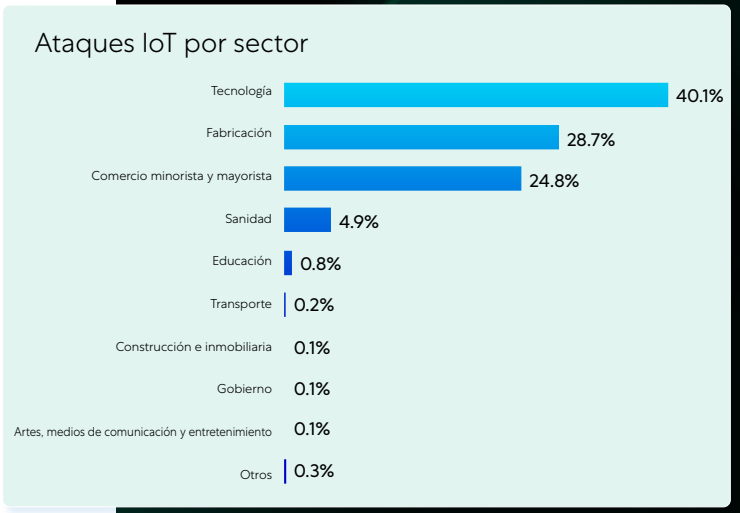


Figura 8: Ataques de IoT por sector

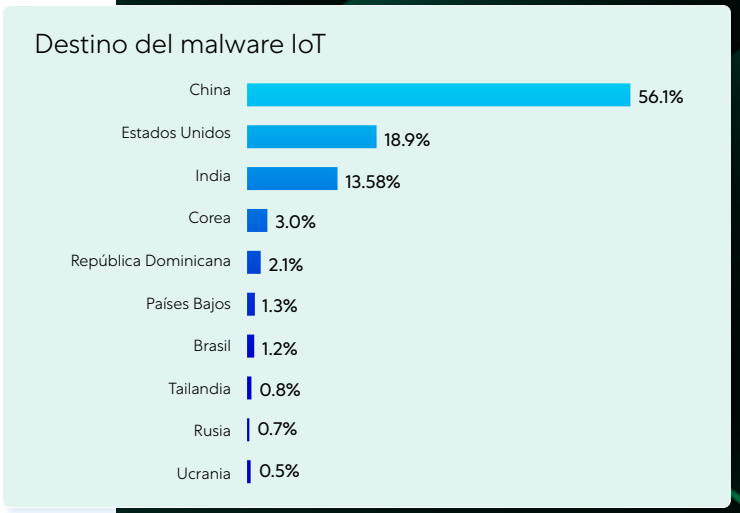


Figura 9: Principales destinos del malware de IoT

Principales ASN de autores de amenazas

Centrándonos en los destinos del malware, a continuación se muestran los principales números de sistema autónomo (ASN) y direcciones IP que ThreatLabz observó que se conectaban al malware de IoT:

ASN	IP	Nombre AS
16276	158.69.0.77	OVH, FR
398468	193.42.137.107	VMSNETWORKS, US
213035	193.239.147.144	SERVERION-AS Serverion B.V., NL
36352	107.173.125.167	AS-COLOCROSSING, US
202448	86.105.252.203	MVPS https://www.mvps.net, CY
46606	162.241.126.53	UNIFIEDLAYER-AS-1, US
53667	198.251.81.249	PONYNET, US
212953	46.102.106.25	MRS-BILISIM, TR
35913	45.15.143.175	DEDIPATH-LLC, US
213371	37.49.230.52	SQUITTER-NETWORKS, NL
35913	45.15.143.140	DEDIPATH-LLC, US
42864	45.95.169.218	GIGANET-HU GigaNet Internet Service Provider Co, HU
63916	103.42.214.181	IPTELECOM-AS-AP IPTELECOM Global, HK
134520	103.42.214.181	GIGSGIGSCLOUD-AS-AP GigsGigs Network Services, HK
3462	111.248.163.38	HINET Data Communication Business Group, TW
36352	107.173.181.189	AS-COLOCROSSING, US
36352	192.227.147.157	AS-COLOCROSSING, US
212369	45.155.125.116	TRDESERVER, TR
206898	185.172.110.205	BLADESERVERS, AU
213035	193.239.147.245	SERVERION-AS Serverion B.V., NL

Figura 10: Principales ASN de los actores de amenazas

Principales objetivos de malware de IoT

ThreatLabz también evaluó los "países de origen"—los objetivos del malware—basándose en la dirección IP del cliente. Los tres países más afectados por los ataques de IoT fueron Irlanda (48 por ciento), Estados Unidos (32 por ciento) y China (14 por ciento).

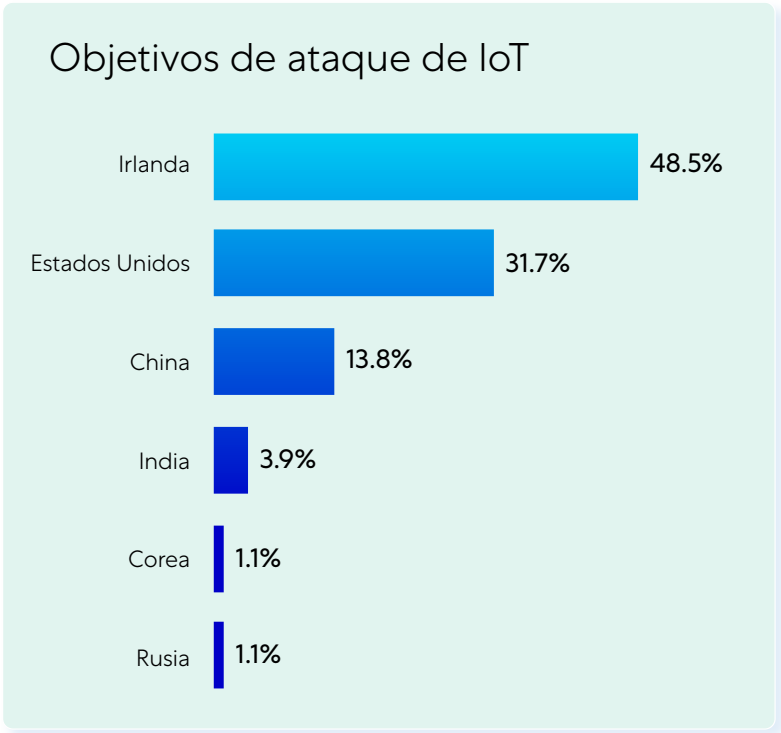


Figura 12: Principales países de origen de malware de IoT

Aspectos fundamentales para protegerse frente al malware de IoT

A medida que la lista de dispositivos "inteligentes" en el mundo crece diariamente, es casi imposible evitar que accedan a su organización, por lo que es fundamental promulgar políticas de acceso que eviten que estos dispositivos funcionen como una puerta abierta a sus datos y aplicaciones confidenciales.

Las siguientes mejores prácticas le ayudarán a garantizar que puede mitigar la amenaza de malware de IoT, tanto con dispositivos autorizados como sin autorización:

- **Haga un seguimiento y gestione sus dispositivos de red.** Muchos dispositivos IoT no están gestionados, por lo que no puede confiar solo en los datos de los agentes de punto final para obtener visibilidad de los dispositivos que están en uso en sus instalaciones. Implemente una solución que analice los registros de red para saber qué dispositivos se están comunicando actualmente en toda su red y qué hacen. Implemente arquitecturas que le permitan inspeccionar tanto el tráfico de red cifrado como el no cifrado para las comunicaciones de los dispositivos de los que podría no estar al tanto si no lo hace. Finalmente, implemente protecciones.

- **Cambie las contraseñas predeterminadas.** Es un consejo tan antiguo como la propia informática, pero una de las formas más fáciles y comunes para los atacantes de explotar sus dispositivos es usar sus contraseñas predeterminadas. Puede que el control de contraseñas no sea posible para los dispositivos IoT no autorizados, pero es un primer paso básico para implementar dispositivos IoT que sean propiedad de la empresa y debe formar parte de su formación en materia de seguridad para cualquier dispositivo que los empleados traigan al trabajo.

- **Manténgase al tanto de las revisiones y actualizaciones.** Muchos sectores, especialmente la fabricación y la atención médica, dependen de los dispositivos IoT para sus flujos de trabajo cotidianos. Para estos dispositivos autorizados, asegúrese de estar al tanto de cualquier vulnerabilidad nueva que se descubra y de mantener la seguridad de su dispositivo actualizada con parches.

- **Implemente una arquitectura de seguridad de confianza cero.** Aplique políticas estrictas para sus activos corporativos, de modo que los usuarios y dispositivos puedan acceder exclusivamente a lo que necesitan y solo después de someterse a autenticación. Restrinja la comunicación a las IP, ASN y puertos relevantes necesarios para el acceso externo. Los dispositivos IoT no autorizados que requieren acceso a Internet deben pasar por una inspección de tráfico y ser bloqueados de todos los datos corporativos, idealmente a través de un proxy. La única manera de evitar que los dispositivos IoT en la sombra supongan una amenaza para las redes corporativas es eliminar las políticas de confianza implícita y controlar estrictamente el acceso a los datos sensibles mediante una autenticación dinámica basada en la identidad, también conocida como confianza cero.

Acerca de ThreatLabZ

ThreatLabz es la división de investigación de seguridad de Zscaler. Este equipo de primera clase es responsable de buscar nuevas amenazas y garantizar que las miles de organizaciones que utilizan la plataforma global Zscaler Zero Trust Exchange™ estén siempre protegidas. Además de la investigación de malware y el análisis de comportamiento, los miembros del equipo participan en la investigación y el desarrollo de nuevos módulos prototipo para la protección avanzada contra amenazas en la plataforma Zscaler y realizan regularmente auditorías de seguridad internas para garantizar que los productos y la infraestructura de Zscaler cumplen con los estándares de cumplimiento de seguridad. ThreatLabz publica regularmente análisis detallados de amenazas nuevas y emergentes en su portal, research.zscaler.com.

Sobre Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.com** o síganos en Twitter **@zscaler**.