Predicciones de seguridad de Trend Micro para 2020

TREND MICRO™ | research

THE FUTURE IS COMPLEX

P. 4

EXPOSED

P. 9

MISCONFIGURED

P. 13

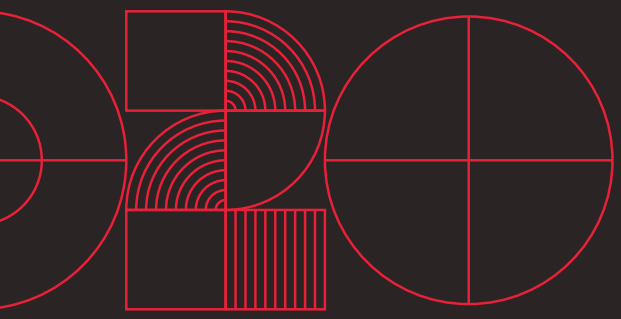
DEFENSIBLE

P. 17

CYBERSECURITY IN 2020

P. 20

Publicado por Trend Micro Research
Imágenes de stock bajo licencia de Shutterstock.com



THE NEW NORM

Predicciones de seguridad de Trend Micro para 2020

El año 2020 marca la transición hacia una nueva década, y los recientes y notables acontecimientos y tendencias significan un cambio similar en el panorama de las amenazas. La ciberseguridad a partir de 2020 tendrá que ser vista a través de muchas lentes; desde las diferentes motivaciones de los atacantes y el arsenal ciberdelictivo hasta el avance de los desarrollos tecnológicos y la inteligencia global de amenazas, solo para que los defensores puedan mantenerse al día y anticiparse a los pilares de la ciberdelincuencia, a los cambios en los papeles y a los nuevos actores.

El viejo paradigma, en el que las redes están aisladas detrás del firewall de la empresa, está detrás de nosotros. Atrás quedan los días en que se utilizaba una cantidad limitada de aplicaciones empresariales. El paradigma actual exige una amplia variedad de aplicaciones, servicios y plataformas que requerirán protección. La seguridad en capas que se aplica a diversos esfuerzos de implementación y se mantiene al día con los cambios en el ecosistema será crucial para hacer frente a la amplia gama de amenazas.

Métodos probados -extorsión, ofuscación, phishing- siguen siendo exitosos en los ataques que vemos hoy, pero inevitablemente surgirán nuevos riesgos. La creciente migración a la nube, por ejemplo, intensifica el error humano: las configuraciones erróneas contribuyen a la posibilidad de un compromiso exponencial. La gran cantidad de activos e infraestructuras conectadas crea, además, una serie de problemas que abren puertas a las amenazas. Las amenazas empresariales no serán menos complejas, ya que mezclan los riesgos tradicionales con las nuevas tecnologías, como la inteligencia artificial (IA) en los fraudes empresariales.

Nuestras predicciones de seguridad para 2020 reflejan las opiniones y puntos de vista de nuestros expertos sobre las amenazas y tecnologías actuales y emergentes. Los escenarios y desarrollos descritos son de un posible futuro, en el que los avances tecnológicos y las amenazas evolucionadas serán los principales impulsores de los cambios en el panorama. Este informe pretende capacitar a las empresas para que tomen decisiones fundadas e informadas en áreas específicas de seguridad que presentarán desafíos y oportunidades en 2020 y en las próximas décadas.

La forma en que ha evolucionado el panorama de las amenazas a lo largo de los años demuestra que los agentes de las mismas no se dejan intimidar para comprometer sistemas en su propio beneficio. Cambian y se adaptan en su elección de vectores de ataque y tácticas, lo que hace necesario que usuarios y empresas se mantengan a la vanguardia y un paso por delante.

Los atacantes pasarán por encima de los parches incompletos y precipitados.

Los administradores de sistemas deberán estar atentos no solo a la puntualidad de los despliegues de parches, sino también a la calidad de los parches que despliegan. Con la aplicación de un parche de baja calidad los sistemas críticos podría romper funcionalidades importantes o provocar fallos debido a defectos del parche. Retrasar la aplicación de un parche, por otro lado, pone a los sistemas en riesgo de compromiso debido a un ataque a una vulnerabilidad conocida.

Los problemas relacionados con los parches dejan abiertas ventanas de exposición que los atacantes utilizarán como puntos de entrada. Anticipamos más casos de sorteo o bypass del parche cuando el parche liberado es insuficiente. Por ejemplo, un atacante puede desencadenar un exploit cambiando un par de líneas al código del arreglo. El año pasado, se descubrió un parche para una vulnerabilidad zero-day en Microsoft Jet Database Engine que era "incompleto", es decir, que el fallo estaba limitado y no se eliminaba[1]. Este año, los hackers aprovecharon las vulnerabilidades de los routers Cisco que más tarde se descubrió que tenían correcciones incompletas[2].

Los atacantes contarán con los usuarios de las bibliotecas de código abierto para pasar por alto las correcciones publicadas por los mantenedores de las bibliotecas. También aprovecharán la brecha de parches, en la que se explota una vulnerabilidad antes de que el parche sea enviado a los usuarios del producto intermedio que utiliza la biblioteca vulnerable[3]

En los casos en los que el parche no elimina la vulnerabilidad o existe una brecha en su implementación, los servicios de parcheo virtual pueden ayudar al proporcionar protección inmediata y protección contra vulnerabilidades conocidas y desconocidas.

Los ciberdelincuentes recurrirán a plataformas blockchain para sus transacciones en el underground.

El ecosistema underground seguirá evolucionando a medida que proliferen las actividades de ciberdelincuencia. La confianza desempeñará un papel más importante en los mercados clandestinos, como lo demuestra la aplicación de la investigación de antecedentes y los pagos en garantía en las transacciones de alto riesgo[4]. Blockchain se considerará un nuevo medio para establecer un sistema de confianza distribuido entre compradores y vendedores; los contratos inteligentes permitirán a los ciberdelincuentes formalizar los pagos en criptomonedas y registrarlos en blockchain. Para mantener el anonimato y reducir el riesgo de estafas de salida, los ciberdelincuentes recurrirán a los mercados de blockchain que ofrecen una forma descentralizada de facilitar las transacciones[5].

El malware de productos básicos como el ransomware y el modelo de negocio del crimen como servicio seguirán siendo opciones perennes para los ciberdelincuentes que buscan beneficiarse fácilmente de los ataques.

Los sistemas bancarios estarán en el punto de mira de la banca abierta y el malware de los cajeros automáticos.

Los operadores de malware móvil dedicados a atacar la banca online y los sistemas de pago serán prolíficos en 2020. Los pagos online en Europa verán más actividad a medida que más bancos confirmen su apoyo a los pagos móviles[6]. Con la Directiva de Servicios de Pago revisada (PSD2) actualmente en vigor en la Unión Europea (UE), y otros países que siguen su ejemplo con sus propias regulaciones[7], la "banca abierta" u "open banking" no está lejos de una adopción más amplia. Sin embargo, esto también significa que otras implicaciones de seguridad afectarán al paradigma bancario, desde fallos en las API bancarias hasta nuevos esquemas para campañas de phishing[8]. Los actores de la industria, tanto antiguos como nuevos, deben emplear medidas que van desde el desarrollo de software que sea seguro por diseño hasta la realización de auditorías de seguridad regulares.

La mercantilización del crimeware para cajeros automáticos seguirá ganando terreno. Ya se han encontrado a la venta variantes de Cutlet Maker, Hello World y WinPot. Esperamos que estas familias de malware para cajeros automáticos compitan por el dominio en el mercado clandestino o underground[9].

Deepfakes serán la próxima frontera para el fraude empresarial.

Durante años, las estafas por correo electrónico con técnicas evolucionadas[10] han sido perpetradas en gran medida por estafadores en África Occidental[11], y no esperamos que esto cambie. Prevemos que el fraude avanzará en 2020 con las nuevas tecnologías, en particular la inteligencia artificial (IA). La tecnología de IA se está utilizando para crear falsificaciones altamente creíbles (en formato de imagen, vídeo o audio) que representan a personas que dicen o hacen cosas que no ocurrieron, lo que se conoce comúnmente como "deepfakes"[12]. El aumento de las deepfakes es motivo de preocupación: inevitablemente pasará de crear vídeos pornográficos falsos de celebridades a manipular a los empleados y procedimientos de la empresa.

En 2019 aparecieron noticias de ciberdelincuentes que utilizaban una voz generada por IA en ingeniería social. Según se informa, una compañía de energía fue víctima de un fraude de 243.000 dólares en el que los estafadores utilizaron la IA para imitar la voz del CEO[13] de la empresa. Se realizarán más intentos de explotar la tecnología, utilizando deepfakes de los responsables de la toma de decisiones para engañar a un empleado a fin de que transfiriera fondos o tome decisiones críticas. Se producirá un cambio con respecto al tradicional compromiso del correo electrónico de las empresas (BEC)[14] y a las estafas de soporte técnico. Los agentes maliciosos ya no dependerán únicamente de la falsificación de direcciones de correo electrónico y aprovecharán el elemento audiovisual de las deepfakes para dar más credibilidad a sus planes. Los ejecutivos de nivel C serán el blanco principal de este tipo de fraude, ya que a menudo participan en llamadas, conferencias, apariciones en los medios de comunicación y vídeos online[15].

Google ya ha publicado una amplia serie de vídeos falsos para ayudar a los investigadores a detectar los fraudes y falsificaciones[16]. Si bien las "estafas de deepfake" pueden estar en su etapa inicial, los empleados tendrán que aprender a identificar signos reveladores de deepfakes, como una entonación diferente, un habla lenta y una piel de aspecto artificial en los vídeos. También serán cruciales otras medidas adicionales de verificación en los procesos relacionados con las finanzas.

Los proveedores de servicios gestionados se verán comprometidos por la distribución de malware y los ataques a la cadena de suministro.

Las organizaciones confían cada vez más en la externalización o subcontratación para sus actividades y necesidades diarias. Con ello vienen los temores de que los ataques a través de la cadena de suministro pasen por alto las medidas de seguridad y pongan en peligro los procesos[17] de negocio. El riesgo radica en depositar una confianza ilimitada en terceros, como los proveedores de servicios gestionados (MSP).

Los ataques a la cadena de suministro a lo largo de los años han tomado muchas formas, incluyendo el secuestro de una actualización de software y el compromiso de servicios de terceros para obtener código malicioso para dirigirse a las empresas objetivo[18]. Esto último es lo que prevemos que más afectará a las pequeñas y medianas empresas (PYMES) en 2020. Si las PYMES externatizan parte de su infraestructura u operaciones, estos terceros proveedores pueden convertirse en trampolines para el compromiso.

El compromiso en la cadena de suministro de un MSP puede extenderse a otras partes en sentido descendente. Los agentes maliciosos se dirigirán a proveedores de servicios y cargarán código malicioso en sus sitios con el objetivo de recoger los datos confidenciales de los clientes, entre otros. Los atacantes encontrarán distribuidores o proveedores con posturas de seguridad débiles para difundir malware a las organizaciones de los clientes. Por ejemplo, una brecha en la infraestructura de un proveedor de software permitió a los hackers desplegar ransomware en cientos de sistemas de consultorios dentales[19]. Esta tendencia continuará, si es que no se acelera.

Para evitar que se vean afectados por estos ataques de malware, las empresas deben realizar evaluaciones periódicas de vulnerabilidades y riesgos e implementar medidas preventivas, incluyendo verificaciones exhaustivas de los proveedores y empleados que tienen acceso al sistema.

Los atacantes sacarán provecho de los fallos 'wormable' y de los errores de deserialización.

En mayo, Microsoft publicó una corrección para una vulnerabilidad crítica de ejecución remota de código (RCE) designada como CVE-2019-0708 y apodada BlueKeep. Desde entonces, la compañía ha lanzado actualizaciones similares para vulnerabilidades que afectan a los Servicios de Escritorio Remoto en Windows. Como los fallos son "wormable"[20], cualquier malware que los explote puede propagarse tan velozmente como WannaCry, que saltó rápidamente por todo el mundo y tumbó cientos de miles de sistemas informáticos a su paso en 2017. Sin embargo, desarrollar un exploit para aprovechar BlueKeep es una tarea compleja que requiere un alto nivel de conocimientos técnicos. Por ejemplo, un módulo Metasploit que explota la vulnerabilidad fue liberado pero resultó ser difícil de manejar, a diferencia del exploit EternalBlue[21].

Oiremos más de BlueKeep, y se producirán intentos de explotación sobre otras vulnerabilidades conocidas de alta gravedad. Los protocolos ampliamente utilizados, como Server Message Block (SMB) y Remote Desktop Protocol (RDP), serán el centro de atención de los atacantes que deseen explotar sistemas no protegidos. El protocolo SMB fue el vehículo para los perversos ataques de WannaCry y NotPetya. RDP tampoco es ajeno a los problemas de seguridad. Además de ser accedido por BlueKeep para ejecutarse, también es un vector de entrada común para el ransomware[22]; los atacantes detrás del ransomware SamSam exploran en busca de dispositivos con conexiones RDP expuestas[23].

Otros fallos que esperamos que se conviertan en una preocupación importante para las empresas son los errores de deserialización. Los fallos que implican la deserialización de datos no confiables son una clase

de vulnerabilidades altamente críticas que, cuando se explotan contra aplicaciones empresariales, pueden modificar datos que se supone que están a salvo de la modificación y permiten la posible ejecución de código controlado por el atacante[24]. La serialización es una técnica que muchos lenguajes de programación utilizan para traducir un objeto a un formato que pueda almacenarse o transmitirse. La deserialización es lo contrario de ese proceso. Uno de los riesgos radica en cómo las aplicaciones que aceptan objetos serializados no validan la entrada no confiable antes de *deserializarla*. Los atacantes expertos continuarán aprovechándose de esto insertando un objeto malicioso en un flujo de datos y ejecutándolo en el servidor de aplicaciones.

En lugar de encontrar varios defectos para encadenarlos para la ejecución del código, los atacantes pueden explotar los errores de deserialización para obtener fácilmente un control remoto completo y ejecutar el código automáticamente incluso en entornos complejos. La serialización y deserialización son conceptos importantes en las aplicaciones Java y son comunes a muchas aplicaciones web y productos de middleware. Las empresas que utilizan plataformas que soportan estos mecanismos deberían practicar la aplicación inmediata de parches y parches virtuales[25] , así como tener conocimiento de la explotabilidad del sistema o del software.

El futuro convergente marca el comienzo de ataques y técnicas antiguas y nuevas que exponen los activos de la tecnología de la información (TI) y tecnología operativa (OT).

Los ciberdelincuentes utilizarán dispositivos IoT para el espionaje y la extorsión.

Prevemos que los ciberdelincuentes y los protagonistas de las amenazas utilizarán el machine learning y la IA para espiar en dispositivos conectados en entornos empresariales, como televisores y altavoces inteligentes. Pueden utilizar el reconocimiento de idiomas y la identificación de objetos para espiar conversaciones personales y de negocios. A partir de ahí, pueden identificar un conjunto de objetivos para la extorsión o conseguir un punto de apoyo para el espionaje corporativo.

En cuanto a otras formas de monetización de los ataques contra Internet de las Cosas (IoT), los ciberdelincuentes todavía no han encontrado un modelo de negocio escalable que aproveche la amplia superficie de ataque que ofrece IoT, por no hablar de los cambios de panorama, como por ejemplo, en el caso de las redes 5G. La monetización de los ataques IoT, aunque todavía está en su infancia, será puesta a prueba de diferentes maneras por los ciberdelincuentes. La extorsión digital[26] es el más probable de estos métodos.

En las comunidades underground, los ciberdelincuentes han estado debatiendo cómo comprometer varios tipos de dispositivos conectados en sus métodos para ganar dinero. Estos métodos se probarán en dispositivos de consumo al principio, con la maquinaria industrial conectada como siguiente objetivo lógico. Ya hemos visto conversaciones relacionadas con los controladores lógicos programables (PLC) que se utilizan para controlar equipamiento[27] de fabricación a gran escala.

Los dispositivos IoT, como los routers, se monetizarán a través de botnets, que podrán utilizarse posteriormente como red distribuida para los servicios ofrecidos a los ciberdelincuentes. No es descabellado sospechar que el hacking de routers también se presentará en forma de botnets utilizados para el secuestro de Servidores de Nombre de Dominio (DNS), que se venden como software malicioso de tipo crimeware o como un servicio, principalmente para phishing. Otras ofertas en el underground incluyen el acceso a transmisiones de vídeo de webcams y a medidores inteligentes con firmware modificado. Estos dispositivos expuestos pondrán las conversaciones sobre la seguridad IoT en un primer plano, sobre todo porque no todos los dispositivos IoT tienen seguridad incorporada y se encuentran equipados para estar debidamente protegidos contra diversos ataques.

Los usuarios de 5G se enfrentarán a las implicaciones de seguridad de pasar a redes definidas por software.

A medida que el lanzamiento de 5G gane impulso en 2020, esperamos una variedad de vulnerabilidades simplemente debido a la novedad de la tecnología, incluyendo sus códigos y la conmutación dinámica entre entornos. Incluso con la automatización, la tecnología seguirá planteando desafíos no solo por los inevitables defectos de código, sino también porque los proveedores no están bien equipados para hacer frente a las amenazas relacionadas con la tecnología.

Dado que el entorno 5G es una red definida por software que permite conectividad de alto ancho de banda y baja latencia para usuarios y dispositivos conectados, se espera que las redes sirvan a una amplia gama de aplicaciones y verticales. Las amenazas relacionadas con las redes 5G provendrán de operaciones de software vulnerables (es decir, la red 5G está gestionada por un software o proveedor potencialmente vulnerable) y de la topología distribuida que permiten (es decir, vías de ataque más amplias, un gran número de dispositivos IoT conectados). Los atacantes tratarán de obtener el control del software que gestiona las redes 5G para controlar la propia red. Además, las actualizaciones que involucran 5G serán muy parecidas a las actualizaciones de software de los smartphones y conllevarán vulnerabilidades[28]. Los investigadores ya han demostrado cómo las vulnerabilidades 5G pueden ser explotadas de diferentes maneras utilizando plataformas de hardware y software de bajo coste[29], y es seguro asumir que los ciberdelincuentes no estarán muy por detrás. La falta de seguridad en las redes 5G también agravará las amenazas posibles relacionadas con la confidencialidad (por ejemplo, espionaje de datos/tráfico), integridad (por ejemplo, modificación de datos transmitidos) y disponibilidad (por ejemplo, interrupción de la red que afecta a sectores interdependientes)[30].

La medida actual del éxito de los países y los proveedores parece ser quién consigue construir primero 5G, sacrificando la seguridad por la velocidad. Poner la seguridad 5G como una ocurrencia tardía, debido a la migración apresurada y a las configuraciones deficientes, planteará desafíos, especialmente a medida que más servicios se vuelvan dependientes de la tecnología. Aplicar la seguridad a las infraestructuras habilitadas para 5G después del despliegue será más complejo que incorporar la seguridad desde el principio[31]. Para mitigar las consecuencias de las protecciones inadecuadas se necesitarán profesionales de seguridad capaces de identificar los problemas específicos de las redes definidas por software[32]. Si las funciones de la red permiten un cambio dinámico, entonces la seguridad también debe ser dinámica. Por ejemplo, en el despliegue dinámico de servicios de red a través de la virtualización de funciones de red (NFV) y la virtualización de aplicaciones, la seguridad también debe ser capaz de mantenerse al día con el despliegue rápido de aplicaciones.

Las infraestructuras críticas se verán afectadas por más ataques y paradas de producción.

Las empresas de servicios públicos y otras infraestructuras críticas (IC) continuarán siendo objetivos viables para los extorsionadores en 2020. La extorsión a través del ransomware seguirá siendo el arma preferida de los ciberdelincuentes, ya que el riesgo para las empresas es alto. El tiempo de inactividad prolongado en la producción se traduce en cuantiosas pérdidas económicas; las líneas de producción pueden debilitarse durante semanas, dependiendo del tiempo que tarde la restauración del sistema. Los atacantes también pueden configurar botnets para montar un ataque distribuido de denegación de servicio (DDoS) contra redes de tecnología operativa (OT). Las empresas manufactureras que emplean proveedores de servicios en la nube estarán en riesgo de ataques a la cadena de suministro; los proveedores inseguros podrían servir como puntos de partida para que los agentes de las amenazas ataquen e inmovilicen la producción. Los ciberataques ponen en peligro la disponibilidad, que es la máxima prioridad en estas infraestructuras, y la presión para reforzar la ciberseguridad de las empresas que emplean la Internet industrial de las cosas (IIoT) no hará más que aumentar[33].

En los últimos años, diferentes agentes de amenazas se han dirigido a varias instalaciones energéticas de todo el mundo en campañas de reconocimiento[34]. Estas actividades de ataques de ransomware dirigido se centran en obtener acceso a las credenciales de los sistemas de control industrial (ICS) y de los sistemas de control de supervisión y adquisición de datos (SCADA), así como en recopilar información sobre el

funcionamiento de las instalaciones. El impacto de estos compromisos se propagará no solo dentro del sistema de IC afectado, sino también a través de sus interdependencias, con consecuencias generalizadas (por ejemplo, la interrupción de las centrales eléctricas locales y el suministro de energía[35]).

Esto no quiere decir que el fallo del sistema debido a los ataques afectará solo a la industria de los servicios públicos. Las instalaciones de producción, transporte y fabricación de alimentos también estarán en peligro, ya que utilizan cada vez más aplicaciones de IoT e interfaces hombre-máquina (HMI) como centro principal para la gestión de los módulos de diagnóstico y control.

Las IC públicas y las infraestructuras de TI gubernamentales estarán expuestas a ataques durante más tiempo que los entornos industriales privados, ya que estas áreas del sector público tienden a estar infrafinanciadas. La información reunida en las campañas de reconocimiento brindará a los actores de amenazas la oportunidad de realizar intentos de ataque más coordinados para perturbar no solo las infraestructuras, sino también los servicios públicos y los procesos políticos.

Las oficinas domésticas y otras estructuras de trabajo remoto redefinirán los ataques a la cadena de suministro.

Las organizaciones tendrán que ser cautelosas ante los riesgos introducidos por los acuerdos de teletrabajo y los dispositivos domésticos conectados a Internet que desdibujan las líneas de la seguridad de la empresa. Después de todo, trabajar en entornos domésticos no es tan seguro como estar en la red corporativa. Además, la débil seguridad Wi-Fi agrava los riesgos en el trabajo a distancia, como los espacios de trabajo compartidos o públicos. Una red abierta deja los archivos e información sensibles expuestos para que otros usuarios de la misma red puedan fisgonear[36]. Los dispositivos remotos pueden infectarse con malware que puede entrar en la red corporativa y obtener información valiosa.

La fuerza laboral móvil de hoy en día ya no está atada a un ordenador en un entorno de oficina tradicional. A diferencia de lo que sucede en la configuración de bring-your-own-device (BYOD), los empleados que trabajan desde casa pueden moverse entre varios dispositivos conectados para acceder a apps en la nube y software de comunicación. Los dispositivos domésticos conectados que sirven como puerta de entrada para ataques empresariales son un despliegue inevitable, teniendo en cuenta cómo los empleados pueden encontrar que estos dispositivos (por ejemplo, televisores inteligentes, altavoces y asistentes) también son adecuados para su uso en el trabajo. Las empresas tendrán que decidir qué políticas de seguridad de la información aplicar para hacer frente a tales situaciones.

Utilizando las reservas de información personal que ya han acumulado, los ciberdelincuentes diseñarán ataques empresariales empleando redes domésticas y públicas haciéndose pasar por empleados. Estos ataques cada vez más sofisticados extenderán el compromiso del correo electrónico y los procesos de negocio, más allá de la simple redirección de fondos o la infección por malware. El entorno familiar del empleado se convertirá en un punto de partida para los ataques a la cadena de suministro.


MISCONFIGURED
THE FUTURE IS
Las migraciones Cloud y DevOps presentan riesgos y recompensas para quienes las adopten, lo que pone de relieve la necesidad de seguridad a lo largo de todo el proceso de implementación.

Las vulnerabilidades en los componentes del contenedor serán las principales preocupaciones de seguridad para los equipos DevOps.

El espacio del contenedor[37] es acelerado. Los lanzamientos son rápidos, las arquitecturas se integran continuamente y las versiones de software se lanzan regularmente. Las prácticas de seguridad tradicionales no podrán seguir el ritmo.

Esto resalta la importancia de los principios de DevSecOps para los equipos DevOps, ya que los contenedores vuelcan más convenciones y asumen más roles que son críticos para las organizaciones. Los rápidos ciclos de desarrollo pueden dejar poco espacio para las pruebas de seguridad y vulnerabilidad. Una aplicación puede ahora requerir que una organización proteja cientos de contenedores repartidos en múltiples máquinas virtuales en diferentes plataformas de servicios cloud. Las organizaciones estarán totalmente ocupadas con diferentes componentes de la arquitectura del contenedor, incluyendo las vulnerabilidades en tiempos de ejecución (por ejemplo, Docker, CRI-O, Containerd y runC[38]), orquestadores (por ejemplo, Kubernetes), y entornos de construcción (por ejemplo, Jenkins). Los atacantes encontrarán formas de aprovechar cualquier eslabón débil para comprometer la canalización de DevOps.

Las vulnerabilidades en las imágenes de contenedores ampliamente utilizadas tienen un efecto perjudicial en el pipeline de la empresa si se descargan posteriormente. Parchear contenedores será particularmente complicado si las organizaciones confían en un tercero para la reparación de la imagen, confiando en que es seguro. Las vulnerabilidades en las aplicaciones contenerizadas afectarán no solo al código o al motor del contenedor, sino también a muchos otros elementos en el stack, a los que los agentes maliciosos pueden acceder para obtener acceso y control.

Las plataformas sin servidor introducirán una superficie de ataque por la configuración incorrecta y los códigos vulnerables.

Cada vez más empresas están adoptando plataformas sin servidor para integrar aplicaciones en la nube y reducir costes. Gartner pronostica que más del 20% de las empresas globales tendrán tecnologías de computación serverless para 2020[39]. Las plataformas Serverless, o sin servidor, ofrecen “función como servicio”, permitiendo a los desarrolladores ejecutar códigos sin que la organización tenga que pagar por servidores o contenedores enteros[40]. Sin embargo, el hecho de no tener servidores no significa inmunidad frente a los problemas de seguridad.

Esperamos que las bibliotecas obsoletas, las configuraciones erróneas y las vulnerabilidades conocidas y desconocidas sean puntos de entrada de amenazas para las aplicaciones sin servidor. Los atacantes pueden aprovecharlas para recopilar información confidencial o penetrar en las redes corporativas[41].

Las plataformas sin servidor también incluyen contenedores, funciones sin servidor y otras dependencias, lo que subraya aún más la complejidad del origen de una amenaza. Dado que la computación sin servidor presta funciones, especialmente aquellas que son de código abierto, como sin estado, monitorización de permisos y almacenamiento de datos sensibles serán además una de las principales preocupaciones en 2020. Además de aumentar la visibilidad de la red, la mejora de los procesos y la documentación de los flujos de trabajo serán esenciales para la ejecución de aplicaciones sin servidor.

Al igual que en las aplicaciones basadas en contenedores, DevSecOps también debe estar a la vanguardia de la implementación sin servidor. Los entornos sin servidor también se beneficiarán de la integración continua y la facilidad de uso a la que aspira DevSecOps[42]. Las herramientas de seguridad que abordan las infraestructuras sin servidor, incluidas las dependencias y vulnerabilidades de las aplicaciones de código abierto, serán importantes para la adopción sin servidor y el despliegue de funciones específicas.

Las configuraciones incorrectas de los usuarios y la participación insegura de terceros agravarán los riesgos en las plataformas cloud.

Una organización puede seguir corriendo riesgos a pesar de la actualización regular de los sistemas y de la adopción de las medidas adecuadas si existen problemas de autenticación y aplicaciones mal configuradas en la implementación. Los controles de seguridad básicos que no se implementan correctamente serán una gran amenaza para la seguridad de los datos de las organizaciones.

Prevemos más incidentes de redes comprometidas debido a los puntos débiles de los servicios en la nube. Las configuraciones incorrectas en el almacenamiento en la nube que causan fugas de datos seguirán siendo un problema de seguridad común para las organizaciones en 2020. Las restricciones de acceso insuficientes, los controles de permisos mal gestionados, la negligencia en las actividades de registro y los activos expuestos públicamente son solo algunos de los errores que las empresas cometerán al configurar sus redes en la nube. Los errores y fallos relacionados con los servicios en la nube expondrán un número significativo de registros de la empresa e incluso conducirán a la imposición de multas y penalizaciones. Estos riesgos pueden reducirse mejorando la situación general de seguridad en la nube (es decir, configurando e implementando adecuadamente las infraestructuras) y garantizando que se respeten las mejores prácticas y los estándares de la industria.

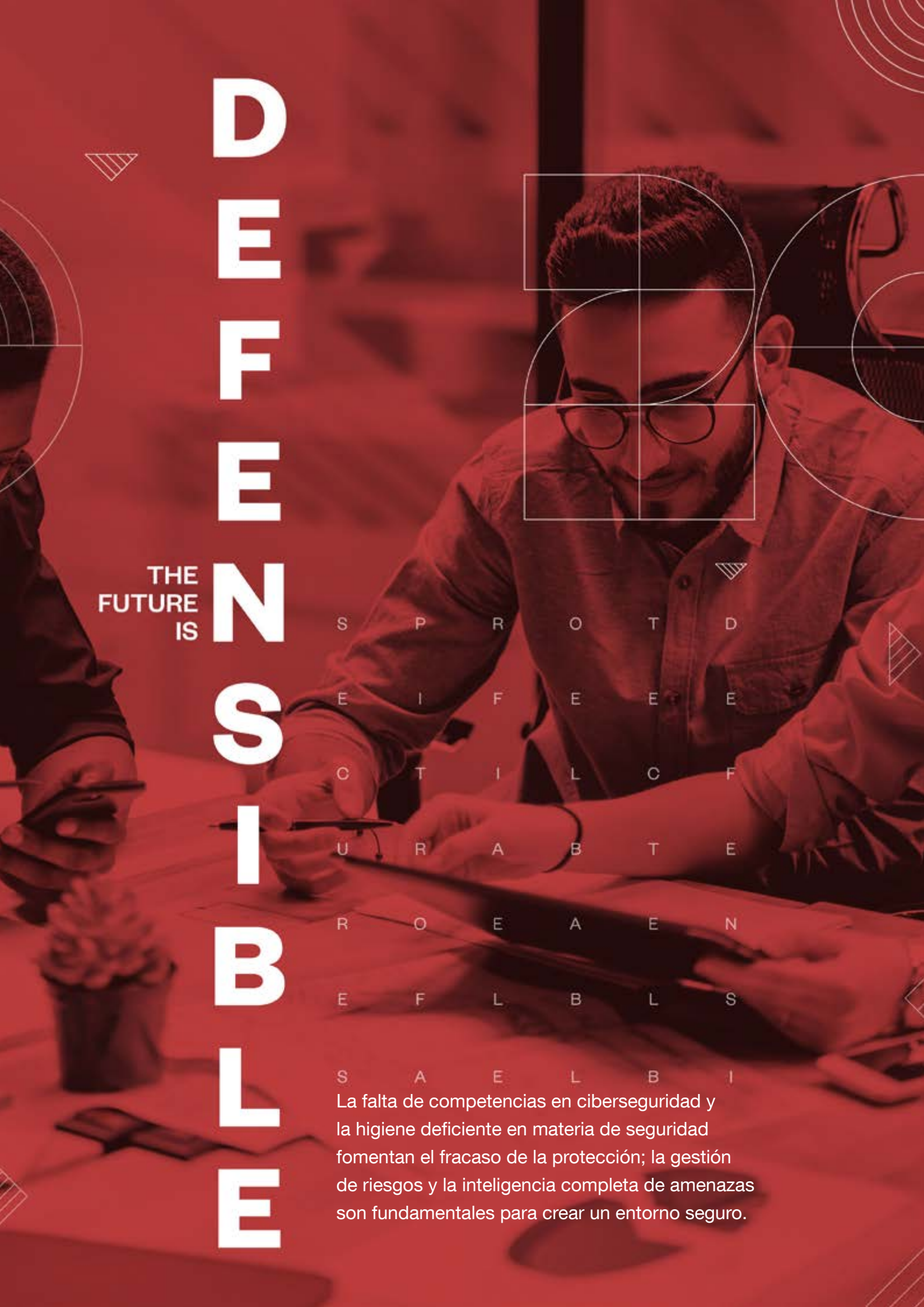
A medida que más empresas y producciones (por ejemplo, instalaciones de fabricación)[43] se trasladen a la nube, los proveedores de servicios externos estarán cada vez más involucrados. Sin embargo, también existe el riesgo de que estos proveedores no tengan experiencia con la nube (es decir, estén acostumbrados a los procesos y sistemas tradicionales) y que no estén equipados para proteger la infraestructura. Los atacantes estarán motivados para lanzar ataques DDoS contra los proveedores de servicios a través de botnets para interrumpir los servicios en la nube.

Las plataformas en la nube serán presa de ataques de inyección de código a través de bibliotecas de terceros.

En 2020 se producirán más compromisos en las plataformas cloud mediante ataques de inyección de código, ya sea directamente en el código o a través de una biblioteca de terceros. La inyección de malware se puede hacer en un intento de espiar o tomar el control de los archivos e información de un usuario en

la nube. Las formas más comunes de estos ataques en las aplicaciones web de los servicios cloud son los ataques cross-site scripting y ataques de inyección SQL. Los ataques exitosos permiten a los hackers recuperar de forma remota datos confidenciales y manipular el contenido de la base de datos. Por otro lado, los atacantes pueden ir por una ruta diferente con bibliotecas de terceros que, al ser descargadas por los usuarios, ejecutan código malicioso inyectado[44].

Mientras tanto, prevemos que más atacantes seguirán los datos hasta la nube. Se espera que se produzcan brechas en la nube a medida que se vayan adoptando modelos de computación cloud de software, infraestructura y plataforma como servicio. Cuantos más datos corporativos residan en la nube, más se interesarán los actores maliciosos. La prevención de compromisos en la nube requerirá la debida diligencia por parte de los desarrolladores, una cuidadosa consideración de los proveedores y las plataformas ofrecidas, y mejoras en la gestión de la postura de seguridad cloud.



La falta de competencias en ciberseguridad y la higiene deficiente en materia de seguridad fomentan el fracaso de la protección; la gestión de riesgos y la inteligencia completa de amenazas son fundamentales para crear un entorno seguro.

La detección predictiva y de comportamiento será crucial contra las amenazas persistentes y sin archivo.

Las amenazas que "viven de la tierra" continuarán evadiendo las técnicas tradicionales de listas negras[45]. Las empresas tendrán que considerar soluciones con indicadores de comportamiento, sandboxing y monitorización de tráfico. Dado que estas amenazas se plantan en el registro, residen en la memoria de un sistema, o abusan normalmente de herramientas de listas blancas como PowerShell y Windows Management Instrumentation (WMI), el seguimiento de indicadores no basados en archivos como eventos o comportamientos de ejecución específicos será importante para la detección. Las técnicas sin archivos también seguirán destacando para otras formas de ataque que despliegan troyanos bancarios[46] , malware de minería de criptomonedas maliciosos de criptomoneda[47] y ransomware[48].

Aparte de las amenazas de Linux que se centran en infectar dispositivos IoT para convertirlos en parte de una botnet DDoS[49], el malware basado en Linux también experimentará un aumento sostenido a medida que el sistema de código abierto se convierta en un componente importante, sino el principal[50], en las plataformas empresariales. Además, las variantes de malware con capacidad para robar información aumentarán, ya que son fiables para recopilar información que puede utilizarse para penetrar más profundamente en las redes. Esperamos que estas amenazas persistan en los sistemas empresariales a través de diversos medios -incluidas las técnicas sin archivos- listas para volver a generar sus procesos para nuevos ataques.

El framework MITRE ATT&CK desempeñará un papel más importante en la forma en que las empresas evalúan la seguridad.

El framework MITRE ATT&CK proporciona una matriz completa para la evaluación de la seguridad. Su base de conocimiento público utiliza ataques conocidos para clasificar y explicar tácticas y técnicas adversarias[51]. Esperamos que más empresas evalúen modelos de amenazas, productos de seguridad y riesgos organizativos a través de la lente del framework. Además de que los cazadores de amenazas puedan controlar mejor los ataques y los patrones, los defensores también se beneficiarán de la medición de la eficacia de las medidas de mitigación y las herramientas de seguridad. La base de conocimiento MITRE ATT&CK puede actuar como un recurso común para los responsables de seguridad y los proveedores de ciberseguridad, agilizando el intercambio de información sobre técnicas de ataque y medidas defensivas.

La inteligencia de amenazas deberá complementarse con experiencia en análisis de seguridad para la protección en todas las capas de seguridad.

Anticipamos que los ataques en 2020 y en adelante serán planeados, distribuidos y variados en términos de tácticas. La inteligencia de amenazas y los análisis de seguridad ayudarán a las organizaciones a defender sus entornos de forma proactiva mediante la identificación de brechas de seguridad, la eliminación de eslabones débiles y la comprensión de las estrategias de los atacantes. La inteligencia integral de amenazas infundida en la seguridad y los respectivos procesos de gestión de riesgos será de un valor incalculable para las organizaciones que buscan mitigar los peligros antes de que ocurra cualquier ataque.

El compromiso a través de las amenazas avanzadas, el malware persistente, el phishing común, los posibles ataques zero-day y otros ataques se pueden evitar si se dispone fácilmente de información y protección. Tener una visibilidad completa del entorno permite a las organizaciones disponer de una metodología de prevención eficaz para detectar amenazas y desviar ataques en tiempo real. Esto significa tener un mejor contexto más allá del endpoint, que abarque el correo electrónico, el servidor, las cargas de trabajo en la nube, así como las redes.

Las organizaciones reconocerán que la brecha de habilidades de ciberseguridad y una deficiente higiene de seguridad siguen siendo factores importantes en el panorama de las amenazas de 2020. Los responsables de la toma de decisiones y los administradores de TI reconocerán la necesidad de tener una visión más amplia de lo que está ocurriendo en sus entornos empresariales. Los expertos en seguridad, como los analistas del centro de operaciones de seguridad (SOC), ayudarán a obtener ese punto de vista consolidado y a correlacionar los hallazgos con la inteligencia global de amenazas.


CYBERSECURITY
IN 2020
INFORM
CNOITA
ONNECT
CYBERS
TIRUCE
Y2020202
DATA00

La colaboración con expertos en seguridad será esencial para mitigar los riesgos en todas las áreas de la infraestructura cibernética de la empresa. Esto permitirá a los defensores y desarrolladores obtener mayor visibilidad y control sobre sus dispositivos conectados y abordar sus puntos débiles. La detección en tiempo real y de hora cero también será crucial para identificar proactivamente las amenazas conocidas y desconocidas.

El panorama en constante cambio requerirá una combinación intergeneracional de defensa multicapa y conectada, impulsada por mecanismos de seguridad tales como:

- **Visibilidad completa.** Proporciona un examen priorizado y optimizado de las amenazas con herramientas y experiencia que mitigan el impacto y remedian los riesgos.
- **Prevención de amenazas con mitigación efectiva.** Mitiga automáticamente las amenazas una vez visualizadas e identificadas, junto con antimalware, machine learning e IA, control de aplicaciones, reputación web y técnicas antispam.
- **Detección y respuesta gestionadas.** Proporciona experiencia en seguridad que puede correlacionar alertas y detecciones para la identificación de amenazas, análisis exhaustivos y remediación inmediata utilizando herramientas optimizadas de inteligencia de amenazas.
- **Monitorización del comportamiento.** Bloquea el malware y las técnicas avanzadas de forma proactiva y detecta comportamientos anómalos y rutinas asociadas con el malware.
- **Seguridad endpoint.** Protege a los usuarios a través del sandboxing, la detección de brechas y las capacidades de sensores de endpoint que evitan ataques y protegen los datos.
- **Detección y prevención de intrusiones.** Frena el tráfico sospechoso como las comunicaciones de comando y control (C&C) y extracción de datos.

Referencias

1. Catalin Cimpanu. (13 October 2018). ZDNet. “Microsoft JET vulnerability still open to attacks, despite recent patch.” Last accessed on 8 October 2019 at https://www.zdnet.com/article/microsoft-jet-vulnerability-still-open-to-attacks-despite-recent-patch/.
2. Ionut Arghire. (29 March 2019). Security Week. “Cisco Improperly Patched Exploited Router Vulnerabilities.” Last accessed on 30 October 2019 at https://www.securityweek.com/cisco-improperly-patched-exploited-router-vulnerabilities.
3. Catalin Cimpanu. (9 September 2019). ZDNet. “Security researchers expose another instance of Chrome patch gapping.” Last accessed on 8 October 2019 at https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping/.
4. Vladimir Kropotov, Fyodor Yarochkin, and Michael Ofiaza. (7 January 2019). Trend Micro Security News. “Your Word is Your Bond: Trust and Ethics in Underground Forums.” Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/your-word-is-your-bond-trust-and-ethics-in-underground-forums.
5. Europol. (9 October 2019). Europol. “Cybercrime Is Becoming Bolder With Data At The Centre Of The Crime Scene.” Last accessed on 11 October 2019 at https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene.
6. Apple. (1 October 2019). Apple. “Apple Pay participating banks in Europe and the Middle East.” Last accessed on 8 October 2019 at https://support.apple.com/en-gb/HT206637.
7. PwC. (n.d.). PwC Italia. “Open Banking... so what?” Last accessed on 28 October 2019 at https://www.pwc.com/it/en/industries/banking/future-open-banking.html.
8. Feike Hacquebord, Robert McArdle, Fernando Mercês, and David Sancho. (17 September 2019). Trend Micro Security News. “The Risks of Open Banking.” Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-risks-of-open-banking-are-banks-and-their-customers-ready-for-psd2.
9. Numaan Huq, Vladimir Kropotov, Mayra Rosario, David Sancho, and Fyodor Yarochkin. (28 June 2019). Trend Micro Security News. “Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground.” Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crimeware-for-sale-the-commoditization-of-atm-malware-in-the-cybercriminal-underground.
10. Europol. (2018). Europol. “Internet Organised Crime Threat Assessment 2018.” Last accessed on 16 October 2019 at https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf.
11. The United States Department of Justice. (10 September 2019). US Department of Justice. “281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes.” Last accessed on 16 October 2019 at https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds.
12. J.M. Porup. (10 April 2019). CSO Online. “How and why deepfake videos work — and what is at risk.” Last accessed on 11 October 2019 at https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html.
13. Catherine Stupp. (30 August 2019). The Wall Street Journal. “Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case.” Last accessed on 11 October 2019 at https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.
14. Trend Micro. (n.d.). Trend Micro. “Business Email Compromise (BEC).” Last accessed on 11 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec).
15. Liam Tung. (4 September 2019). ZDNet. “Forget email: Scammers use CEO voice ‘deepfakes’ to con workers into wiring cash.” Last accessed on 16 October 2019 at https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/.
16. Nick Dufour and Andrew Gully. (24 September 2019). Google AI Blog. “Contributing Data to Deepfake Detection Research.” Last accessed on 23 October 2019 at https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html.
17. Trend Micro. (n.d.). Trend Micro. “Business Process Compromise (BPC).” Last accessed on 11 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/business-process-compromise.
18. Chaoying Liu and Joseph C. Chen. (16 January 2019). Trend Micro Security Intelligence Blog. “New Magecart Attack Delivered Through Compromised Advertising Supply Chain.” Last accessed on 11 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/.
19. Catalin Cimpanu. (29 August 2019). ZDNet. “Ransomware hits hundreds of dentist offices in the US.” Last accessed on 24 October 2019 at https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/.
20. Simon Pope. (13 August 2019). Microsoft Security Response Center. “Patch new wormable vulnerabilities in Remote Desktop Services (CVE-2019- 1181/1182).” Last accessed on 8 October 2019 at https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote- desktop-services-cve-2019-1181-1182/.
21. Dan Goodin. (7 September 2019). Ars Technica. “Exploit for wormable BlueKeep Windows bug released into the wild.” Last accessed on 24 October 2019 at https://arstechnica.com/information-technology/2019/09/exploit-for-wormable-bluekeep-windows-bug-released-into-the-wild/.
22. Jay Yaneza. (9 February 2017). Trend Micro Security Intelligence Blog. “Brute Force RDP Attacks Plant CRYSIS Ransomware.” Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-rdp-attacks-plant-crysis-ransomware/.
23. Trend Micro. (23 March 2018). Trend Micro Security News. “SAMSAM Ransomware Suspected in Atlanta Cyberattack.” Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/samsam-ransomware-suspected-in-atlanta-cyberattack.
24. MITRE. (19 September 2019). Common Weakness Enumeration. “CWE-502: Deserialization of Untrusted Data.” Last accessed on 8 October 2019 at https://cwe.mitre.org/data/definitions/502.html.
25. Trend Micro. (25 October 2018). Trend Micro Security News. “Virtual Patching: Patch Those Vulnerabilities before They Can Be Exploited.” Last accessed on 24 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited.
26. Trend Micro. (n.d.). Trend Micro. “Digital Extortion.” Last accessed on 7 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/digital-extortion.

27. Stephen Hilt, Vladimir Kropotov, Fernando Mercês, Mayra Rosario, and David Sancho. (10 September 2019). Trend Micro Security News. "Uncovering IoT Threats in the Cybercrime Underground." Last accessed on 7 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-internet-of-things-in-the-cybercrime-underground.
28. Tom Wheeler and David Simpson. (3 September 2019). The Brookings Institution. "Why 5G requires new approaches to cybersecurity." Last accessed on 16 October 2019 at https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.
29. Altaf Shaik and Ravishankar Borgaonkar. (2019). Black Hat. "New Vulnerabilities in 5G Networks." Last accessed on 16 October 2019 at https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf.
30. Trend Micro. (14 October 2019). Trend Micro Security News. "EU Report Highlights Cybersecurity Risks in 5G Networks." Last accessed on 17 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/eu-report-highlights-cybersecurity-risks-in-5g-networks.
31. Tom Wheeler and David Simpson. (3 September 2019). The Brookings Institution. "Why 5G requires new approaches to cybersecurity." Last accessed on 6 November 2019 at https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.
32. Craig Gibson, Vladimir Kropotov, Philippe Lin, Rainer Vosseler, and Fyodor Yarochkin. (4 April 2019). Trend Micro Security News. "Securing Enterprises for 5G Connectivity." Last accessed on 16 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-enterprises-for-5g-connectivity.
33. Trend Micro. (15 August 2019). Trend Micro Security News. "Securing the Industrial Internet of Things: Protecting Energy, Water and Oil Infrastructures." Last accessed on 30 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-the-industrial-internet-of-things-protecting-energy-water-and-oil-infrastructures.
34. Trend Micro. (11 April 2019). Trend Micro Security News. "New Critical Infrastructure Facility Hit by Group Behind TRITON." Last accessed on 24 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/new-critical-infrastructure-facility-hit-by-group-behind-triton.
35. Trend Micro. (22 December 2017). Trend Micro Security News. "TRITON Wielding Its Trident – New Malware Tampering with Industrial Safety Systems." Last accessed on 7 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems/.
36. Alfred Ng. (19 September 2019). CNET. "WeWork's weak Wi-Fi security leaves sensitive documents exposed." Last accessed on 31 October 2019 at https://www.cnet.com/news/weworks-weak-wi-fi-security-leaves-sensitive-documents-exposed/.
37. Trend Micro. (n.d.). Trend Micro. "Container." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/container.
38. Trend Micro. (28 February 2019). Trend Micro Security News. "CVE-2019-5736: RunC Container Escape Vulnerability Provides Root Access to the Target Machine." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-5736-runc-container-escape-vulnerability-provides-root-access-to-the-target-machine.
39. Gartner, Inc. (4 December 2018). Gartner. "Gartner Identifies the Top 10 Trends Impacting Infrastructure and Operations for 2019." Last accessed on 24 October 2019 at https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras.
40. Scott Fulton III. (9 April 2019). ZDNet. "What serverless computing really means, and everything else you need to know." Last accessed on 24 October 2019 at https://www.zdnet.com/article/what-serverless-computing-really-means-and-everything-else-you-need-to-know/.
41. Guy Podjarny. (15 May 2018). The Register. "Hey cool, you went serverless. Now you just have to worry about all those stale functions." Last accessed on 10 October 2019 at https://www.theregister.co.uk/2018/05/15/stale_serverless_functions/.
42. Trend Micro. (13 April 2018). Trend Micro Security News. "Serverless Applications: What They Mean in DevOps." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/serverless-applications-what-they-mean-in-devops.
43. Willem Sundblad. (18 July 2019). Forbes. "Smart Manufacturing: Creating a Hybrid Cloud-Edge Strategy." Last accessed on 10 October 2019 at https://www.forbes.com/sites/willemsundbladeurope/2019/07/18/smart-manufacturing-creating-a-hybrid-cloud-edge-strategy/#77fc5816af5a.
44. Trend Micro. (29 November 2018). Trend Micro Security News. "Hacker Infects Node.js Package to Steal from Bitcoin Wallets." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets.
45. Trend Micro. (29 July 2019). Trend Micro Security News. "Risks Under the Radar: Understanding Fileless Threats." Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats.
46. Henry Alarcon Jr. and Raphael Centeno. (4 March 2019). Trend Micro Security Intelligence Blog. "Fileless Banking Trojan Targeting Brazilian Banks Downloads Possible Botnet Capability, Info Stealers." Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-banking-trojan-targeting-brazilian-banks-downloads-possible-botnet-capability-info-stealers/.
47. Augusto Remillano II and Arvin Macaraeg. (12 April 2019). Trend Micro Security Intelligence Blog. "Miner Malware Spreads Beyond China, Uses Multiple Propagation Methods Including EternalBlue, Powershell Abuse." Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/miner-malware-spreads-beyond-china-uses-multiple-propagation-methods-including-eternalblue-powershell-abuse/.
48. Erika Mendoza, Jay Yaneza, Gilbert Sison, Anjali Patil, Julie Cabuhat, and Joelson Soares. (29 March 2019). Trend Micro Security Intelligence Blog. "Emotet-Distributed Ransomware Loader for Nozelesn Found via Managed Detection and Response." Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response/.
49. Mark Vicente, Byron Galera, and Augusto Remillano II. (3 April 2019). Trend Micro Security Intelligence Blog. "Bashlite IoT Malware Updated with Mining and Backdoor Commands, Targets WeMo Devices." Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices/.
50. Steven Vaughan-Nichols. (1 July 2019). ZDNet. "Microsoft developer reveals Linux is now more used on Azure than Windows Server." Last accessed on 30 October 2019 at https://www.zdnet.com/article/microsoft-developer-reveals-linux-is-now-more-used-on-azure-than-windows-server.
51. The MITRE Corporation. (n.d.). MITRE. "ATT&CK." Last accessed on 11 October 2019 at https://attack.mitre.org/.

Para Raimund Genes (1963-2017)

TREND MICRO™ | research

Predicciones de seguridad de Trend Micro para 2020

TREND MICRO™ RESEARCH

Trend Micro, líder global en ciberseguridad, ayuda a hacer del mundo un lugar seguro para el intercambio de información digital. Nuestras innovadoras soluciones proporcionan a nuestros clientes seguridad en capas para centros de datos, cargas de trabajo en la nube, redes y endpoints.

En el corazón de nuestro liderazgo, Trend Micro Research cuenta con expertos apasionados por descubrir nuevas amenazas, intercambiar información clave con el público y apoyar los esfuerzos para detener a los ciberdelincuentes. Nuestro equipo global ayuda a identificar millones de amenazas diariamente, lidera la industria en la revelación de vulnerabilidades y publica investigaciones innovadoras sobre ataques dirigidos, inteligencia artificial, Internet de las Cosas (IoT), ciberdelincuencia y mucho más. Trabajamos continuamente para anticipar la próxima ola de amenazas y realizar investigaciones que inviten a la reflexión y que puedan dar forma a la dirección estratégica de la industria.

www.trendmicro.com