Trend Research

TREND MICRO

Escalabilidad crítica

Predicciones de seguridad de Trend Micro para 2024

Contenido de este informe

Publicado por

Trend Research

Escalabilidad crítica

Tras un año actual marcado por grandes avances tecnológicos, 2024 reúne todos los ingredientes para que broten nuevos desafíos en materia de ciberseguridad. El panorama que nos rodea está marcado por las constantes fluctuaciones, tanto en el plano económico como en el político. Casi todo se ha digitalizado: desde las transacciones bancarias hasta los secuestros. Las empresas que buscan una ventaja estratégica han llegado a depender de tecnologías como la inteligencia artificial y el machine learning (IA/ML), la nube y las tecnologías Web3. Pero esas innovaciones también navegan con vientos en contra, que abren la puerta a defensores y delincuentes, así que presagiamos que, inevitablemente, se avecinan tiempos turbulentos.

En medio de los conflictos en curso en Ucrania y Oriente Medio, que condicionan fuertemente a los líderes mundiales, el panorama político se convertirá en un campo minado de ciberamenazas que pueden tener consecuencias de gran alcance, con actores de todos los bandos tratando de influir en la opinión pública y determinar el curso de los acontecimientos políticos. A medida que la UE, los Estados Unidos y Ucrania se preparan para sus respectivas próximas elecciones, los períodos electorales demostrarán ser terreno fértil para ciberataques con motivación política, campañas de desinformación cuidadosamente diseñadas y actos de espionaje orquestados a través de una red de plataformas sociales y herramientas impulsadas por la inteligencia artificial.

Para el próximo año, se prevé que se revele el verdadero potencial transformador de estos avances técnicos, convirtiéndolos en nuevos frentes de batalla para los ciberataques. De manera similar, esperamos que los ciberdelincuentes intenten explotar estos fenómenos, siempre en búsqueda de oportunidades para optimizar sus estratagemas, ampliar el impacto de las infracciones y reinventar tácticas que ya han dado pruebas de su eficacia anteriormente.

Por tanto, además de demostrar voluntad para adaptarse al devenir de los acontecimientos, los líderes empresariales también tendrán que reevaluar en qué medida es posible amoldar sus flujos y metodología de trabajo para encauzar el crecimiento. Su misión es lograr un cuidadoso equilibrio entre previsión y solidez operativa, que aproveche las inversiones tecnológicas. Y les aguarda un año lleno de pruebas que examinarán su capacidad de adaptarse y expandirse al ritmo de las necesidades comerciales.

El propósito de este informe es detallar los principales puntos de atención del panorama de amenazas de cara al próximo año, además de ofrecer información y proponer medidas de mitigación recomendadas por nuestro equipo de expertos en ciberseguridad. Medidas diseñadas para orientar a las personas responsables de tomar decisiones, para que elijan las opciones con mejor fundamento.

Entornos en la nube

Brechas de seguridad en entornos de nube: un escenario propicio para los ataques de gusanos nativos de la nube

Gracias a su capacidad para explotar vulnerabilidades a escala y automatizar ataques, los gusanos reúnen los requisitos para ser una de las tácticas favoritas de los ciberdelincuentes el próximo año: dado que emplean scripts automatizados, permiten a cualquier actor malintencionado ejecutar una amplia gama de tareas, tales como reconocimiento, explotación y establecimiento de persistencia con una mínima intervención manual durante ataques a gran escala dentro de entornos de nube.

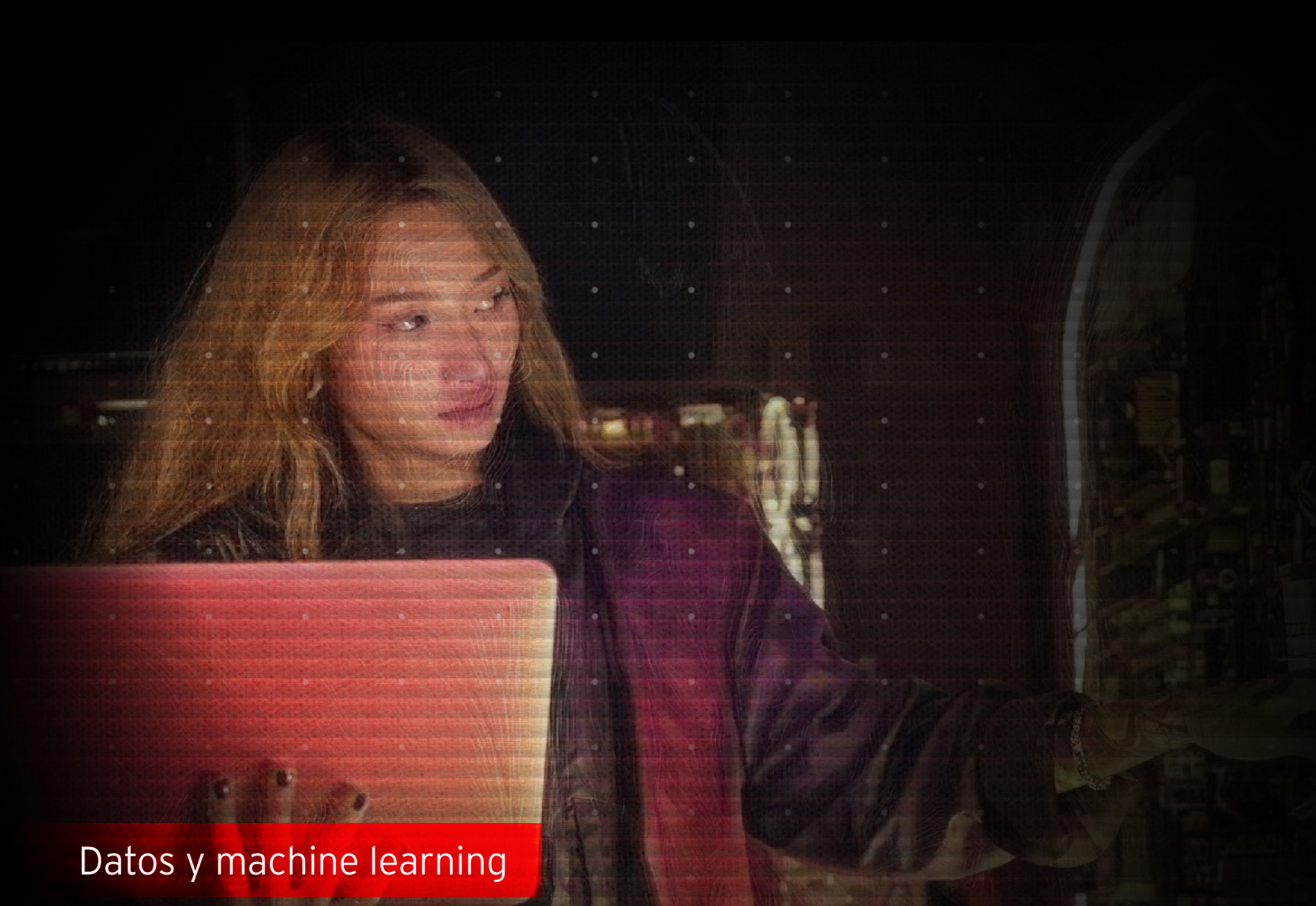
Las configuraciones erróneas de la nube sirven de puntos de entrada muy accesibles para los atacantes. Suelen ser el resultado de infraestructuras demasiado complicadas, cambios de configuración y entornos de desarrollo configurados incorrectamente. Es revelador que, según el Open Worldwide Application Security Project (OWASP), las configuraciones incorrectas también se encuentren entre los principales riesgos de seguridad de API para las organizaciones. La labor de asumir el trabajo extra de cerrar esas brechas recaerá sobre los centros de operaciones de seguridad (SOC), ya que se espera que absorban por completo la seguridad en la nube dentro de su ámbito de operaciones, con el horizonte puesto en 2026.

Para desencadenar una rápida propagación en entornos de nube bastaría un solo exploit con éxito, especialmente a través de API mal configuradas como Kubernetes, Docker y Weave Scope. Tras conseguir ese triunfo inicial y obtener acceso, los atacantes probablemente recurrirían a rootkits como medio sigiloso para lograr persistencia.

Y como los ciberdelincuentes tienen más facilidades para ejecutar técnicas posteriores a la explotación, se espera que en 2024 los ciberataques en entornos de Kubernetes se vuelvan más automatizados y especializados. Aunque Kubernetes es la plataforma de orquestación de contenedores más utilizada en la actualidad, en muchas organizaciones que ejecutan Kubernetes en la nube abundan las configuraciones erróneas. Por ese motivo, la plataforma se convierte en un objetivo codiciado, como lo demuestra un estudio reciente, que detectó que los clústeres de Kubernetes de más de 350 organizaciones y usuarios (entre ellos notables empresas que figuran en la lista Fortune 500) estaban desprotegidos.

Como era de esperar, se descubrió que al menos el 60 % de estos clústeres eran objeto de ataques de campañas de malware, incluido el gusano de nube Silentbob de TeamTNT. Además de sus funciones de escaneo, esta botnet que es similar a un gusano se comunica con un servidor de comando y control (C&C), el cual contiene herramientas y scripts diseñados para aprovecharse de infraestructuras de nube inseguras. Un excelente ejemplo de cómo los atacantes explotan las herramientas nativas de nubes infectadas para clavar sus garras en más víctimas.

Da igual en qué punto se encuentre la organización dentro de su migración a la nube: hasta podría encontrarse en el extremo donde se reciben ataques típicos de «vivir fuera de la nube», donde sus propios recursos basados en la nube se dirigen en su contra. Esto recalca algo esencial: los equipos de seguridad no deberían limitarse a los análisis habituales de malware y vulnerabilidades. Además de revisar sus políticas de seguridad, toda organización debe examinar de forma proactiva sus entornos de nube para anticiparse y prevenir estos ataques de gusanos.



Datos y machine learning

Los datos: una nueva arma contra los incipientes modelos de machine learning basados en la nube

Mientras que las preocupaciones sobre la seguridad en el entorno de la nube en términos generales surgen de amenazas como configuraciones erróneas y ataques nativos de la nube concebidos para que los atacantes logren acceder a los datos almacenados, defender los modelos de **machine learning** (ML) presentará unos desafíos muy distintos para los equipos de seguridad. Unos desafíos que podrían hacer peligrar la integridad de los propios datos.

En 2024, el envenenamiento de datos se convertirá en una amenaza emergente para los modelos de **machine learning** basados en la nube, así que los defensores deberán cubrir una superficie muy amplia para protegerla de agresiones. Es la consecuencia de que muchos de estos modelos obtengan datos de diversos orígenes, como lagos de datos de terceros y sistemas de aprendizaje federado. Además de orquestar dichos ataques durante la fase de recopilación de datos de un modelo, los actores malintencionados también podrían orquestarlos poniendo en riesgo el almacenamiento de datos o la infraestructura de canalización de datos de un modelo.

Entre los modelos especializados entrenados con conjuntos de datos más específicos y los grandes modelos de lenguaje (LLM) y los modelos de IA generativa, que operan con conjuntos de datos masivos, los primeros serán más vulnerables al envenenamiento de datos. Y es que la cantidad de datos que utilizan los segundos provoca que resulten mucho más difíciles de influenciar por parte de sus atacantes.

Un modelo de **machine learning** cuyo rendimiento y comportamiento se hayan visto comprometidos puede abrir la puerta a graves consecuencias para las organizaciones situadas que trabajen después con el modelo. A diferencia de los ataques de «errores en el sistema», que generalmente tienen un impacto fijo y predecible, en este caso los agresores pueden envenenar datos en áreas específicas con resultados muy diversos:

- Un modelo de procesamiento de lenguaje natural que haya sido envenenado y manipulado para divulgar datos confidenciales podría servir como medio de extracción de datos.
- Los servidores de transporte de telemetría de colas de mensajes (MQTT) mal protegidos podrían permitir que los delincuentes escribiesen instrucciones maliciosas.
- Sería posible entrenar un motor de recomendaciones contaminado para que muestre contenido inapropiado o sesgado, lo cual podría provocar la insatisfacción del usuario o, peor aún, acarrear repercusiones legales.
- Si un sistema de detección de fraude se alimenta con datos de entrenamiento contaminados, podría no detectar adecuadamente actividades ilícitas, y eso podría conllevar sanciones regulatorias para una empresa.

Para mantenerse alerta contra agentes malintencionados cuyo objetivo sea contaminar los datos, en 2024 las organizaciones deberían adoptar una postura preventiva que incluya las siguientes medidas de seguridad:

- Validar y autenticar minuciosamente todos los conjuntos de datos de entrenamiento, independientemente de su origen, ya sean de fuentes internas o de proveedores externos.
- Proteger estrictamente los conjuntos de datos guardados en servicios de almacenamiento en la nube bajo un enfoque de defensa en profundidad, que implica múltiples prácticas que trabajan en conjunto y cifran los datos cuando estén en reposo.
- Usar mecanismos de transferencia más seguros como HTTPS y SFTP (Protocolo seguro de transferencia de archivos, Secure File Transfer Protocol), así como plataformas de **machine learning** como servicio (MLaaS) basadas en la nube.
- Implementar un control de accesos basado en roles (RBAC) para supervisar el acceso de los usuarios como parte de una estrategia más amplia de defensa de confianza cero.
- Emplear herramientas de gestión de la postura de seguridad en la nube (CSPM, Cloud Security Posture Management) para ayudar a identificar y rastrear cualquier cambio en sus recursos basados en la nube.
- Auditar y monitorizar periódicamente el estado de su infraestructura en la nube para detectar cualquier intento de manipulación de datos, configuraciones incorrectas y actividad sospechosa que podría representar un peligro para la red en la nube.

IA generativa

La IA generativa permitirá a los estafadores mejorar sus señuelos de ingeniería social en ataques dirigidos

En poco tiempo, empresas, organizaciones e instituciones de todos los ámbitos tendrán presupuestos destinados a la IA generativa como parte fundamental de sus estrategias comerciales en TI, publicidad y ciberseguridad. El auge imparable de la IA también ha llegado a la política y un buen ejemplo es el uso de imágenes generadas por IA con fines propagandísticos en Nueva Zelanda y Estados Unidos. En este último caso, se prevé que la IA se sumará al ruido de la desinformación política de cara a las elecciones presidenciales del próximo año. Sin embargo, es poco probable que las empresas desarrollen sus propias soluciones de IA o LLM. En cambio, buscarán proveedores que ya tengan estas tecnologías integradas en sus carteras, junto con la experiencia para implementarlas.

La integración de la IA en las operaciones diarias para aprovechar al máximo su potencial no se limita únicamente a instituciones comerciales y políticas. Mientras que el **machine learning** (que constituye un apartado específico dentro de la IA general) sí suele trabajar con algoritmos fijos, los algoritmos de la IA generativa se encuentran en constante evolución. Esto explica por qué los sistemas de IA son capaces de crear nueva información basada en aprendizajes previos. Estas tecnologías están estrechamente relacionadas y si se agregan al arsenal de un agente amenazante, pueden resultar útiles por diferentes motivos: el **machine learning** por su capacidad de procesamiento de datos y la IA generativa por su producción creativa. Sin embargo, la calidad de los resultados de ambos sistemas depende directamente de la calidad de la información que se utilice para entrenarlos. De hecho, la IA generativa puede recibir datos incorrectos, ya sea por exposición accidental o maliciosa. Al igual que sucede con tantas otras tecnologías emergentes, la IA es un arma de doble filo y en 2024 se hará evidente su papel en la dimensión social de los ciberataques.

De entre todos los avances que se están produciendo en el campo de la inteligencia artificial, la IA generativa destacará como una potente herramienta para los atacantes cuando se trate de intentos de suplantación y robo de identidades, desdibujando las líneas de nuestra realidad digital en esquemas de ingeniería social como las vulneraciones del correo electrónico empresarial (BEC o Business Email Compromise), el phishing y los ataques tipo whaling.

Según el último informe anual del Centro de Quejas de Internet del FBI, los delitos cibernéticos basados en la ingeniería social figuran entre los delitos con más víctimas y se han consolidado como una de las fuentes de ingresos más rentables para los atacantes.

A la vista de cómo se están desarrollando los avances en este ámbito, parece que ser barato y parecer convincente siguen siendo factores mutuamente excluyentes para los deepfakes. De todas las herramientas que se han vuelto más sofisticadas gracias al impulso de la inteligencia artificial y que, por lo tanto, están listas para crear falsos contenidos de audio y vídeo hiperrealistas en tiempo real, predecimos que en el futuro cercano, la clonación de voz será un vehículo para más abusos y estafas. Asimismo, prevemos esta continuará siendo una amenaza más dirigida a objetivos concretos, ya que si se quiere conseguir una buena suplantación de la voz con la ayuda de la IA, es necesario recopilar numerosas fuentes de audio de personas específicas.

La accesibilidad de las tecnologías basadas en la IA despejará el camino para diseñar estafas más convincentes y generalizadas dirigidas a víctimas cuidadosamente escogidas. A raíz del cierre de WormGPT en agosto bajo el peso del escrutinio de los medios, y mientras los agentes malintencionados esperan antes de lanzar otras herramientas del tipo de WormGPT, existe la posibilidad de que otros actores se decanten rápidamente por otras alternativas. Los investigadores especializados en seguridad han demostrado que es posible engañar a los sistemas de IA generativa para que eludan sus propias reglas de censura. Por tanto, es concebible que un impostor ingenioso encuentre una solución a través de una escalada de privilegios o jailbreak que afecte a un modelo grande de lenguaje (LLM), para lo que también necesitaría credenciales de usuario robadas y conectividad a una red privada virtual (VPN) para mantener el anonimato.

Ya se ha detectado a los primeros estafadores que tratan de aprovechar lo que la Comisión Federal de Comercio de Estados Unidos llama «medios sintéticos». Combinar diversas herramientas de inteligencia artificial, como chatbots y clones de voz, podría ser el motor de amenazas polifacéticas como el secuestro virtual. Tengamos en cuenta que bastaría un puñado de ataques exitosos para que el secuestro virtual sea lucrativo, así que los ciberdelincuentes que recurran a tales herramientas no necesitarían desarrollar sus actividades a gran escala. Para evitar ser víctimas de estas estafas tan sofisticadas, los defensores deberían implementar políticas de confianza cero, acompañadas de un cambio de paradigma: será necesario aplicar una máxima fundamental, que ninguna interacción en línea se tome nunca al pie de la letra.

Cadenas de suministro de software

Los ataques a la cadena de suministro de software servirán de toque de atención para proteger los sistemas CI/CD de los proveedores.

Cuando un fragmento de software se convierte en plataforma de lanzamiento para propagar malware, se convierte en un elemento terriblemente ubicuo, con presencia por todas partes. Lo veremos en 2024. Cuando las empresas implementan software de uso común, están aprovechándose de soluciones que pueden considerarse el estándar del sector, que vienen equipadas con abundante documentación de soporte y pueden garantizar la compatibilidad e interoperabilidad con múltiples socios. Estos factores facilitan que las organizaciones en crecimiento conserven su agilidad, incluso cuando incorporan más aplicaciones, proveedores y canales de distribución de terceros a sus cadenas de suministro. Pero una vez se han identificado las vulnerabilidades del software, esos mismos programas pueden servir de arma. Y los daños resultantes llegarán en cascada a todos los participantes ligados a una red con conexiones muy estrechas.

Los ciberdelincuentes que quieran alterar o interrumpir las cadenas de suministro lo intentarán a través de cualquier punto débil de las defensas. Pensemos por ejemplo en las eSIM, la última versión de los módulos de identidad de suscriptores o tarjetas SIM. En la era 5G, no solo se han convertido en un componente integral de la gestión de flotas e inventarios, sino que también han demostrado ser útiles para el seguimiento e identificación de activos por parte de las empresas.

Sin embargo, la triste realidad es que las eSIM están expuestas a diversas amenazas que posibilitarían el secuestro de SIM, como configuraciones inadecuadas, secuestro de SIM o secuestro de flotas. Explotar las eSIM como vectores de ataque tiene el potencial de poner en peligro cadenas de suministro enteras, permitiendo que agentes malintencionados manipulen las funciones de gestión que supervisan el inventario de dispositivos habilitados para eSIM.

Las cadenas de suministro se han convertido en un objetivo atractivo para los ciberdelincuentes cuyo objetivo es actuar a través de un único proveedor para afectar a múltiples organizaciones que han elegido como víctimas: un estudio global encargado por Trend Micro confirmó que en más de la mitad de las organizaciones globales, la seguridad de su cadena de suministro ha sido puesta en riesgo por ransomware. A la mayoría de los directivos de TI encuestados también les preocupaba que su organización corriera un riesgo más alto de recibir ataques mediante ransomware debido a su red de socios y clientes. Cuando se utilizan como vector de acceso las cadenas de suministro dotadas de defensas insuficientes, los agresores pueden eliminar a los proveedores de acceso originales de los modelos comerciales de ransomware y así maximizar todavía más sus ganancias.

También predecimos que los ciberdelincuentes intentarán infiltrarse en las cadenas de suministro de software de los proveedores a través de sus sistemas de integración y entrega continuas (CI/CD). A pesar de que estos sistemas han permitido a los desarrolladores automatizar muchas etapas del desarrollo de software, cada proyecto es diferente: no existe una forma única de configurar canales de CI/CD, ya que se basan en múltiples herramientas y procesos que conllevan una serie de riesgos de dependencia. En 2024, los proveedores tendrán que anticiparse y contar con que los delincuentes intentarán atacar la fuente. O sea, el mismo código sobre el que se construyen las infraestructuras de TI. Y lo harán con ataques que se centrarán persistentemente en componentes de terceros como bibliotecas, canalizaciones y contenedores. Es cierto que esas fuentes pueden contribuir a acelerar el desarrollo y reducir los plazos de comercialización, pero no están exentas de puntos ciegos de seguridad:

- **Falta de auditorías de seguridad exhaustivas.** Aunque algunas bibliotecas y contenedores de terceros utilizan escáneres de vulnerabilidades, ciertos errores podrían pasar desapercibidos si no tienen una designación de vulnerabilidades y exposiciones comunes (CVE). Mientras no se divulguen ni se aborden estas vulnerabilidades, seguirán constituyendo una ruptura en la cadena de confianza.
- **Componentes obsoletos.** Los desarrolladores también podrían acceder sin darse cuenta a componentes obsoletos con vulnerabilidades ocultas. Que la versión actual de una biblioteca o contenedor sea segura no garantiza que siga siéndolo si en futuras actualizaciones se introducen vulnerabilidades, accidentalmente o a través de cuentas de mantenimiento comprometidas.
- **Riesgo de ataques de inyección de código.** Las bibliotecas de terceros vulnerables también pueden servir de vía para que los ciberdelincuentes les inserten código malicioso que se ejecutará tan pronto como se efectúe una llamada a la biblioteca. A continuación, sería posible aprovecharse del acceso no autorizado a sistemas y datos para recolectar credenciales, secuestrar recursos del sistema para extraer criptomonedas o lanzar ataques distribuidos de denegación de servicio (DDoS).

Las plataformas y los registros de contenedores aplican autenticación multifactor (MFA), emplean tokens cuidadosamente seleccionados y realizan escaneos secretos en repositorios y similares. Sin embargo, también es necesario que las organizaciones actúen de forma proactiva para limitar los riesgos a los que se exponen sus sistemas de CI/CD. Por eso recomendamos a sus equipos de seguridad y desarrolladores que se planteen tomar las siguientes medidas:

- Implementar herramientas de seguridad de aplicaciones que puedan reconocer rápidamente cualquier signo de comportamiento sospechoso.
- Prestar esas mismas herramientas de seguridad a todo el proceso de CI/CD.
- Realizar una investigación en profundidad sobre bibliotecas y contenedores antes de proceder a usarlos.
- Escanear todas las bibliotecas y contenedores (imprescindible al actualizar a una nueva versión) para evitar que se trabaje con cualquier código secuestrado.
- Supervisar cualquier dependencia externa, especialmente aquellas de fuentes ascendentes, para detectar vulnerabilidades ocultas.

Tecnología blockchain

Los atacantes buscarán nuevos terrenos de caza y planes de extorsión en la tecnología blockchain

La capacidad de la tecnología blockchain para crear libros de contabilidad en línea a prueba de manipulaciones y facilitar transacciones transparentes tiene diversas aplicaciones prácticas para las empresas, desde el desarrollo de plataformas de redes sociales hasta sitios web de comercio electrónico. A pesar de que es frecuente utilizar la tecnología blockchain para el mantenimiento de registros distribuidos digitalmente, continúa sigue siendo lo suficientemente flexible como para funcionar también dentro de límites predefinidos. Pensemos en las redes blockchain privadas o basadas en permisos. Cada vez son más las empresas de todo el mundo que las adoptan para reducir los gastos operativos en áreas como la gestión de cadenas de suministro y la contabilidad intraempresarial.

Ahora bien, aunque la tecnología blockchain promete integridad de datos, ahorro de costes y resistencia a fallos de un solo punto, también oculta una serie de dificultades para la implementación y la seguridad, especialmente en la época actual del Internet de las cosas (IoT). Los blockchain son bien conocidos por sus problemas de latencia y además, generan tantos datos que necesitan un sistema de gestión propio dedicado. Dejando a un lado estas preocupaciones, tampoco son inmunes a los ataques de denegación de servicio (DoS) y de almacenamiento en la nube, que podrían bloquear a los usuarios.

Pero aunque restringir el acceso de los usuarios sea grave, no es la peor de las estratagemas que pondrán en práctica los delincuentes el año que viene: a la vista de cómo crece el número de empresas que recurre a blockchains privadas, es mera cuestión de tiempo que alguien se fije en ellas, porque contienen datos y activos muy valiosos. Habrá una corriente constante de ciberdelincuentes empeñada en atacar no solo los blockchains públicos, sino también en intensificar los ataques a las redes de blockchains privadas. Generalmente, se tiende a pensar (equivocadamente) que los sistemas internos son más seguros por defecto. Pero aquí sucede lo contrario, porque habitualmente los blockchains privados se someten a menos pruebas de estrés y carecen del nivel de resiliencia que tienen los blockchains públicos, más curtidas porque deben defenderse de ataques constantes.

Debido a su naturaleza centralizada, los blockchains resultan muy atractivos para las instituciones sujetas a una supervisión estrecha, especialmente en el sector financiero. Aun así, ese mayor nivel de control sería un consuelo muy pobre para las empresas si los delincuentes empiezan a desarrollar modelos de negocio de extorsión que apunten específicamente a blockchains privados. Sabiendo que los operadores de blockchains privados pueden modificar, anular o borrar cualquier entrada, sin duda los atacantes también intentarán apoderarse de estos derechos administrativos.

El próximo año aparecerán también casos de extorsión donde los agresores intentarán robar claves que les permitan alterar aspectos de los blockchains de sus víctimas, como escribir datos maliciosos o editar registros existentes. Así luego podrían exigir un rescate a cambio de guardar silencio sobre la magnitud del daño que hayan logrado infligir.

Si los extorsionadores consiguiesen tomar el control de suficientes nodos clave, podrían cifrar todo el blockchain e impedir que funcione hasta obtener una recompensa considerable. Desafortunadamente, en comparación con sus contrapartidas públicas, los blockchains privados suelen tener menos nodos que validen transacciones. Eso significa menos trabajo para los atacantes que planeen poner en riesgo toda la red. Por eso las organizaciones que ofrecen servicios que dependen de redes blockchain autorizadas deben verificar que su red de nodos esté distribuida adecuadamente, porque así será capaz de resistir ciberataques e interrupciones.

Los delincuentes prestan más atención a las tecnologías Web3 y así, en 2024 se sentarán las bases para que aparezcan los primeros grupos criminales que trabajen por completo y exclusivamente con organizaciones autónomas descentralizadas (DAO), que se rigen por contratos inteligentes autoejecutables alojados en redes blockchain. Ya se ha observado la evolución hacia esos nuevos grupos de amenazas entre elementos sospechosos, que han encontrado formas de utilizar contratos inteligentes como armas para agregar capas de complejidad a los delitos relacionados con criptomonedas contra plataformas financieras descentralizadas. Por ejemplo, usar contratos falsos o abiertamente maliciosos.

Desarrollar competencias en tecnologías innovadoras como es el blockchain exige tiempo. Así que, por ahora, empresas y organizaciones tendrán que depender de proveedores externos para ejecutar sus blockchains. Quizás en el futuro haya un mercado mayor para productos capaces de monitorizar implementaciones de blockchains en busca de vulnerabilidades y ataques, que ayuden a las empresas a administrar sus blockchains internamente. Hasta entonces, habrá que colaborar a fondo con los proveedores en las siguientes consideraciones de seguridad:

- **Sopesar las necesidades de seguridad de las soluciones basadas en la nube en comparación con las locales.** Por ejemplo, la segunda opción requeriría que la propia empresa alojase el blockchain y configurase adecuadamente los nodos de la red. Las soluciones basadas en la nube ayudan a simplificar el proceso de configuración de redes blockchain, pero es poco probable que puedan ofrecer el mismo nivel de control o libertad para la personalización que aportan las blockchains dotadas de infraestructura local tangible.
- **Desarrollar adecuadamente cualquier contrato inteligente.** La mayoría de los contratos inteligentes están escritos en Solidity, de modo que las organizaciones deberán estar al tanto de cualquier riesgo de seguridad específico de este lenguaje de programación.

¿Qué nos espera en el futuro?

Las empresas que apuestan con valentía por los modelos de **machine learning**, las herramientas de inteligencia artificial generativa, las redes blockchain y la nube con la esperanza de obtener réditos en productividad deben mantenerse alerta. Porque inevitablemente, esos mismos motores de innovación nos traerán realidades crueles y puntos débiles inesperados. Cuando una organización adopta cada vez más soluciones de software, aumenta su grado de interconexión y dependencia de los datos. Por lo tanto, en ese avance constante en pos del crecimiento, es fundamental que conserve la capacidad de gestionar cargas de trabajo más altas y aplicar medidas de defensa a las superficies sensibles a los ataques, porque estas también se expanden.

A medida que las empresas amplíen sus operaciones, deben priorizar la protección de los activos digitales, los datos confidenciales y la integridad general de su infraestructura tecnológica. En última instancia, se trata de una postura de seguridad sólida, que se instaura para respaldar la expansión llamada a sentar las bases de cara al futuro para la pila de TI de esa organización. Y la empresa debe seguir el ritmo de las nuevas tecnologías, cuya aceleración acentuará ciertos riesgos cibernéticos o provocará que surjan otros nuevos. Si los defensores aspiran a mantener firmes sus líneas frente a las ciberamenazas en constante evolución que les esperan el próximo año, necesitarán garantizar la protección en cada punto del ciclo de vida de la amenaza, además de emplear una estrategia de seguridad multidimensional, basada en información fidedigna y previsión sobre las amenazas.

Notas finales

1 Rob Picheta y Gul Tuysuz. (5 de noviembre de 2023). *CNN*. "Tensions grow in Kyiv over status of war, as Zelensky insists conflict with Russia is not at a 'stalemate'". Consultado el 6 de noviembre de 2023, en Enlace.

2 BBC. (15 de noviembre de 2023). *BBC*. "Israel Gaza war: History of the conflict explained". Consultado el 22 de noviembre de 2023, en Enlace.

3 Parlamento Europeo. (25 de octubre de 2023). *Parlamento Europeo*."European elections 2024: MEPs' proposals for the lead candidate system". Consultado el 6 de noviembre de 2023, en Enlace.

4 Robert Costa. (5 de noviembre de 2023). *CBS News*. "Election 2024: One year to the finish line". Consultado el 6 de noviembre de 2023, en Enlace.

5 Yulia Dysa. (3 de noviembre de 2023). *Yahoo! News*. "Ukraine's Zelenskiy ponders idea of 2024 election during war". Consultado el 6 de noviembre de 2023, en Enlace.

6 Michael Langford. (21 de febrero de 2023). *Trend Micro*. "Common Cloud Configuration Errors & Fixes". Consultado el 13 de noviembre de 2023, en Enlace.

7 Equipo del proyecto de seguridad API de OWASP. (2023). *Proyecto abierto de seguridad de aplicaciones a nivel mundial (OWASP)*."OWASP Top 10 API Security Risks – 2023". Consultado el 13 de octubre de 2023, en Enlace.

8 Trend Micro. (9 de junio de 2023). *Trend Micro*. "Trend Micro Predicts Cloud Security Will Be Consumed by the SOC by 2026". Consultado el 9 de noviembre de 2023, en Enlace.

9 Magno Logan y David Fiser. (25 de mayo de 2021). *Trend Micro*. "TeamTNT Targets Kubernetes, Nearly 50,000 IPs Compromised in Worm-like Attack". Consultado el 13 de octubre de 2023, en Enlace.

10 Aqua Security. (8 de agosto de 2023). *Aqua Security Software Ltd*. "Aqua Nautilus Researchers Find Kubernetes Clusters Under Attack in Hundreds of Organizations". Consultado el 10 de octubre de 2023, en Enlace.

11 Lucian Constantin. (13 de julio de 2023). *CSO Online*. "Silentbob worm attack targets multiple cloud technologies". Consultado el 13 de octubre de 2023, en Enlace.

12 Bloomberg Intelligence. (1 de junio de 2023). *Bloomberg*. "Generative AI to Become a $1.3 Trillion Market by 2032, Research Finds". Consultado el 13 de octubre de 2023, en Enlace.

13 Tess McClure. (24 de mayo de 2023). *The Guardian*. "New Zealand's National party admits using AI-generated people in attack ads". Consultado el 6 de noviembre de 2023, en Enlace.

14 Matt Novak. (25 de abril de 2023). *Forbes*. "GOP Releases First Ever AI-Created Attack Ad Against President Biden". Consultado el 6 de noviembre de 2023, en Enlace.

15 Ali Swenson y Matt O'Brien. (3 de noviembre de 2023). *Time*. "Poll Shows Most U.S. Adults Think AI Will Add to Election Misinformation in 2024". Consultado el 6 de noviembre de 2023, en Enlace.

16 Greg Young. (1 de junio de 2023). *Trend Micro*. "Generative AI: What Every CISO Needs to Know". Consultado el 19 de noviembre de 2023, en Enlace.

17 Internet Crime Complaint Center (Centro de denuncias de delitos en Internet). (2023). *FBI, Federal Bureau of Investigation*. "2022 Internet Crime Report". Consultado el 20 de octubre de 2023, en Enlace.

18 Jon Healey. (11 de mayo de 2023). *Los Angeles Times*. "Real-time deepfakes are a dangerous new threat. How to protect yourself". Consultado el 13 de octubre de 2023, en Enlace.

19 David Sancho y Vincenzo Ciancaglini. (15 de agosto de 2023). *Trend Micro*. "Hype vs. Reality: AI in the Cybercriminal Underground". Consultado el 13 de octubre de 2023, en Enlace.

20 Matt Burgess. (13 de abril de 2023). *Wired*. "The Hacking of ChatGPT Is Just Getting Started". Consultado el 13 de octubre de 2023, en Enlace.

21 Michael Atleson. (20 de marzo de 2023). *Comisión Federal de Comercio de EE. UU. (Federal Trade Commission)*."Chatbots, deepfakes, and voice clones: AI deception for sale". Consultado el 13 de octubre de 2023, en Enlace.

22 Craig Gibson y Josiah Hagen. (28 de junio de 2023). *Trend Micro*. "Virtual Kidnapping: How AI Voice Cloning Tools and ChatGPT are Being Used to Aid Cybercrime and Extortion Scams". Consultado el 22 de octubre de 2023, en Enlace.

23 Craig Gibson. (15 de noviembre de 2019). *Trend Micro*. "From SIMjacking to Bad Decisions: 5G Security Threats to Non-Public Networks." Consultado el 6 de noviembre de 2023, en Enlace.

24 Trend Micro. (6 de septiembre de 2022). *Trend Micro*. "Over Half of Global Firms' Supply Chains Compromised by Ransomware". Consultado el 18 de noviembre de 2023, en Enlace.

25 Feike Hacquebord, Stephen Hilt y David Sancho. (15 de diciembre de 2022). *Trend Micro*. "The Future of Ransomware". Consultado el 18 de noviembre de 2023, en Enlace.

26 Trend Micro. (24 de octubre de 2023). *Trend Micro*. "CI/CD Pipeline: How to Overcome Set-Up Challenges". Consultado el 9 de noviembre de 2023, en Enlace.

27 Trend Micro. (29 de agosto de 2023). *Trend Micro*. "How to Protect Your CI/CD Pipeline". Consultado el 9 de noviembre de 2023, en Enlace.

28 Trend Micro. (13 de enero de 2022). *Trend Micro*. "Blockchain 101: What Is It? How Does It Work? And What Are Its IIoT Applications?". Consultado el 20 de noviembre de 2023, en Enlace.

29 Trend Micro. (17 de mayo de 2018). *Trend Micro*. "Blockchain: The Missing Link Between Security and the IoT?". Consultado el 20 de noviembre de 2023, en Enlace.

30 Departamento de investigación de Statista. (6 de septiembre de 2023). *Statista*. "Size of the blockchain technology market worldwide in 2018 and 2019, with forecasts from 2020 to 2025". Consultado el 13 de octubre de 2023, en Enlace.

31 María Korolov. (16 de julio de 2018). *CSO Online*. "5 ways to hack blockchain in the enterprise". Consultado el 13 de octubre de 2023, en Enlace.

32 Eric Piscini, David Dalton y Lory Kehoe. (n. d.). *Deloitte EMEA Grid Blockchain Lab*. "Blockchain & Cybersecurity Point of View". Consultado el 13 de octubre de 2023, en Enlace.

33 Matt Wixey. (29 de agosto de 2023). *Sophos*. "For the win? Offensive research contests on criminal forums". Consultado el 10 de octubre de 2023, en Enlace.

34 Fyodor Yarochkin, Vladimir Kropotov y Jay Liao. (18 de enero de 2023). *Trend Micro*. "'Payzero' Scams and The Evolution of Asset Theft in Web3". Consultado el 9 de noviembre de 2023, en Enlace.

35 Cifer Fang et al. (24 de marzo de 2022). *Trend Micro*. "An Investigation of Cryptocurrency Scams and Schemes". Consultado el 9 de noviembre de 2023, en Enlace.

Escalabilidad crítica

Predicciones de seguridad de Trend Micro para 2024

TREND MICRO™

Trend Micro, líder mundial en ciberseguridad, contribuye a que el mundo sea un lugar seguro para el intercambio de información digital. Gracias a décadas de experiencia en seguridad, investigación de amenazas globales e innovación continua, nuestra plataforma de ciberseguridad unificada protege a más de medio millón de organizaciones y a millones de personas en nubes, redes, dispositivos y terminales.

La plataforma unificada de ciberseguridad Trend Micro One ofrece técnicas avanzadas de defensa contra amenazas, potentes funciones de detección y respuesta (XDR) e integración en todo el ecosistema de TI, incluidos AWS, Microsoft y Google, lo que permite a las organizaciones comprender, comunicar y mitigar mejor el riesgo cibernético.

El equipo de investigación de amenazas globales de Trend Micro ofrece un repertorio inigualable de información y conocimientos que impulsa nuestra plataforma de ciberseguridad y ayuda a proteger a organizaciones de todo el mundo de cientos de millones de amenazas diarias.

Contamos con 7000 empleados en 65 países, especializados en la seguridad y extraordinariamente motivados por hacer del mundo un lugar mejor y más seguro.

Trend Micro permite a las organizaciones simplificar y proteger su mundo conectado.

trendmicro.com