MANDIANT

PREDICCIONES DE SEGURIDAD PARA 2022

CATORCE PREDICCIONES DE CIBERSEGURIDAD PARA 2022 Y MÁS ALLÁ

UNA PERSPECTIVA RENOVADA Y REALISTA

Aunque nuestras vidas se vieron alteradas en 2020, la industria de la ciberseguridad volvió con fuerza en 2021. Mandiant aceptó el reto de trabajar en circunstancias siempre cambiantes sin dejar de ofrecer a los clientes servicios de primera calidad que se asocian con nuestros expertos.

En ciberseguridad, las expectativas son fundamentales. Una cosa con la que siempre podemos contar es el nivel de incertidumbre en el ámbito cibernético. Los atacantes cambian regularmente sus tácticas, técnicas y procedimientos (TTP) para evadir la detección, dejando a los defensores luchando para seguir el ritmo. Cuando Mandiant ayuda a reducir esa brecha compartiendo nuestros aprendizajes y expectativas, informados y respaldados por pruebas, también avanzamos en la misión de Mandiant: hacer que todas las organizaciones estén seguras contra las ciberamenazas y confíen en su preparación.

El informe de este año, *Catorce predicciones de ciberseguridad para 2022 y más allá*, presenta más de una docena de puntos de vista de nuestros líderes y principales expertos ubicados en todo el mundo, incluyendo a Sandra Joyce, EVP, Global Intel & Advanced Practices, y Charles Carmakal, SVP y Director de tecnología (Chief Technology Officer).

Pase la página para explorar las predicciones de seguridad de Mandiant para 2022.

EL RANSOMWARE Y LA EXTORSIÓN MULTIFACÉTICA EN EL CENTRO DE ATENCIÓN

1. No hay final a la vista: Aumento de la frecuencia y ampliación de las tácticas

La amenaza del ransomware ha crecido significativamente a lo largo de la última década y continuará su tendencia al alza. El negocio del ransomware es sencillamente demasiado lucrativo, a menos que los gobiernos internacionales y las innovaciones tecnológicas puedan alterar de manera fundamental el cálculo de la rentabilidad de los atacantes. Aunque hemos visto esfuerzos para interrumpir las operaciones y responsabilizar a los actores de las amenazas, los ciberdelincuentes simplemente se trasladan a otra plataforma, como parte del modelo de negocio del ransomware como servicio, para continuar con sus operaciones. Muchos actores del ransomware operan desde lugares que no se rigen por la legislación estadounidense y desde regiones donde sus acciones no tienen tantos costos ni repercusiones. Esperamos ver más ataques de ransomware procedentes de fuera de los EE. UU. También esperamos ver un aumento de incidentes de ransomware contra industrias críticas, donde la urgencia de pagar es mayor para evitar un impacto significativo en la salud y en el bienestar de la población civil.

Los perpetradores que se dedican a la extorsión multifacética seguirán encontrando más formas de extorsionar a sus víctimas. La extorsión multifacética comienza con el bloqueo de las víctimas de sus propios archivos a través de la encriptación (ransomware clásico), y luego añade amenazas como hacer públicos los datos sensibles. En 2022 se espera que los actores intensifiquen nuevas tácticas, como tratar de reclutar a personas con información privilegiada entre sus víctimas u objetivos. También esperamos ver más ciberdelincuentes que castiguen a las víctimas que contratan a empresas profesionales de negociación para que les ayuden a reducir el importe final del pago de la extorsión. De hecho, ya hemos visto estas tácticas en 2021, y el año que viene esperamos que evolucionen a medida que los actores de las amenazas se vuelvan más inteligentes desde el punto de vista comercial y aprendan qué tipo de situaciones quieren evitar sus víctimas.

Los perpetradores que se dedican a la extorsión multifacética seguirán encontrando más formas de extorsionar a sus víctimas.

2. No hay honor entre ladrones: Más disputas entre perpetradores

Las operaciones de ransomware como servicio suelen implicar a varios actores, cada uno de los cuales realiza un elemento específico del ataque a cambio de una cuota o una parte de los beneficios. Prevemos que, a lo largo de 2022, aumentará el conflicto entre estos actores, y este puede acabar provocando malos resultados para las víctimas. Los conflictos pueden producirse cuando los objetivos no pagan, o si las fuerzas de seguridad desmantelan la capacidad de cobro de los perpetradores. También pueden surgir conflictos cuando las organizaciones de víctimas acaban pagando; un actor concreto puede sentir que no ha cobrado lo suficiente o que no está recibiendo su parte justa. Ya estamos viendo este tipo de conflictos entre los perpetradores y las víctimas podrían sufrir por ello. En los próximos 12 meses, esperamos ver muchas situaciones en las que las víctimas pagarán un millón de dólares o más para evitar que se publiquen sus datos robados. En algunas de estas situaciones, algunos o todos esos datos pueden ser publicados por uno de los actores de la operación debido a un conflicto. Conforme estos hechos aumenten, mayor será el efecto en la forma en que las organizaciones piensen sobre el pago de rescates.

3. Organizaciones atrapadas entre el gobierno de los EE. UU. y los perpetradores del ransomware

El gobierno de los Estados Unidos está enfocado en el ransomware y en cómo frenarlo, y esto puede tener consecuencias negativas para las organizaciones. Por ejemplo, las organizaciones estadounidenses (y las que no tienen sede en los Estados Unidos, pero operan en ese país) no pueden pagar a perpetradores sancionados ni a ningún grupo o individuo que figure en la lista de no pago del Departamento del Tesoro de los Estados Unidos. Aun así, en varios casos públicos, las víctimas pagaron a grupos que podían tener alguna conexión suelta con las entidades sancionadas... no necesariamente conexiones garantizadas o incluso concretas, pero sí alguna creencia leve de que podría haber una conexión. No estamos seguros de que el gobierno dé un escarmiento a una o más de las grandes organizaciones que realicen un pago a una presunta entidad sancionada, con la mera intención de intentar frenar y evitar que las organizaciones víctimas paguen grandes sumas por demandas de extorsión. Hay varias perspectivas diferentes sobre los pagos de extorsión, incluida la de prohibirlos directamente para que todo el proceso sea ilegal. En consecuencia, prevemos que probablemente habrá algún recurso negativo para una organización afectada que haya pagado una demanda de extorsión.

Muchos dispositivos de tecnología operacional (OT) no se construyen con la seguridad en la vanguardia del diseño.

4. Los sistemas ciberfísicos están cada vez más amenazados por los "n00bs"

A lo largo de 2021, observamos que los perpetradores de baja sofisticación aprendieron que podían crear grandes impactos en el espacio de la tecnología operativa (OT), quizás incluso mayores de lo que pretendían. Los actores seguirán explorando el espacio OT en 2022 y utilizarán cada vez más el ransomware en sus ataques. Esta focalización se producirá por la necesidad de mantener los entornos OT plenamente operativos, especialmente cuando los sistemas forman parte de infraestructuras críticas. Los ataques contra entornos críticos de OT pueden causar graves trastornos e incluso poner en peligro vidas humanas, lo que aumenta la presión para que las organizaciones paguen un rescate. Para agravar el problema, muchos de estos dispositivos OT no se construyen con la seguridad en la vanguardia del diseño, y actualmente estamos viendo un aumento masivo en el número de vulnerabilidades que se identifican en los entornos OT.

5. Más vulneraciones públicas en la región de Asia-Pacífico y Japón (APJ)

Históricamente, las vulneraciones en la región de la APJ no se han hecho públicas, pero es probable que esto cambie en 2022 a medida que la extorsión multifacética sea más frecuente. En el pasado, hacer pública una vulneración no beneficiaba ni al atacante ni a la organización afectada. Los atacantes querían permanecer invisibles el mayor tiempo posible, con la esperanza de mantener su acceso a las redes de las víctimas durante largos períodos. Y las víctimas querían evitar el daño a la reputación, el impacto financiero y otras consecuencias que se derivan de una vulneración.

La extorsión multifacética ha cambiado todo eso. Ahora los atacantes simplemente amenazan con exponer las vulneraciones y publicar los datos sensibles para aumentar la urgencia de pagar. Las organizaciones en la APJ deben estar preparadas para hacer frente a este tipo de operadores de extorsión, pero, lamentablemente, muchos en la región carecen de experiencia con este tipo de amenazas, o no las toman en serio. Por lo tanto, prevemos que los atacantes harán públicas muchas más vulneraciones de organizaciones en la APJ.

PERSPECTIVAS DE LOS PRINCIPALES ACTORES NACIONALES Y ESTATALES: LOS CUATRO GRANDES

6. Rusia

Rusia mantendrá una postura agresiva en lo que queda de 2021 y en 2022, con un énfasis sostenido en los objetivos de la OTAN, Europa del Este, Ucrania, Afganistán y el sector energético. El gobierno de los Estados Unidos atribuyó a Rusia el ataque UNC2452 (también referido como el incidente de compromiso de la cadena de suministro de SolarWinds), lo que demuestra que Rusia tiene la capacidad de lograr un impacto generalizado. Creemos que los entornos de la cadena de suministro de software y de la cadena de suministro en general seguirán siendo el objetivo de Rusia el próximo año. Además, la manipulación por parte de UNC2452 de los métodos de autenticación en entornos híbridos de nube/en el sitio pone de manifiesto tácticas innovadoras, lo que nos lleva a pensar que el nivel de sofisticación y el alcance de las operaciones rusas se ampliarán.

7. Irán

Irán utilizará sus herramientas cibernéticas de manera mucho más agresiva para promover los intereses regionales. Las operaciones de información atribuidas por los Estados Unidos a Irán en 2020 y 2021 demostraron tácticas más agresivas que las vistas anteriormente. Irán también seguirá atacando a Israel y a otros países de Oriente Medio. Han demostrado su capacidad y voluntad de utilizar malware destructivo, así que prevemos que aprovecharán cualquier oportunidad que se les presente. En última instancia, veremos a Irán tratando de crear un mayor equilibrio de poder en función de sus propios intereses. Los hemos visto con objetivos en el extranjero, pero lo más probable es que su objetivo a lo largo de 2022 sea regional.

8. China

China seguirá siendo muy agresiva, apoyando la Iniciativa del Cinturón y Ruta de la Seda utilizando el ciberespionaje. Ahora que el Ministerio de Seguridad del Estado (MSS) y el Ejército Popular de Liberación (EPL) han completado la mayor parte de su reorganización, sus operaciones van a estar mucho más centradas. China ha mostrado su voluntad de ampliar sus operaciones y tomar medidas que antes el país no estaba dispuesto a tomar. A medida que las tensiones geopolíticas siguen aumentando, la gran pregunta es: "¿Cuándo veremos a China desplegar algunas de sus capacidades destructivas conocidas, pero aún no utilizadas?"

9. Corea del Norte

Corea del Norte, frente a sus desafíos geográficos, internacionales y financieros, está dispuesta a tomar muchos riesgos. En 2022, esperamos ver a Corea del Norte flexionar sus capacidades cibernéticas para compensar su falta de otros instrumentos de poder nacional. El aparato cibernético norcoreano seguirá apoyando al régimen de Kim mediante la financiación de las ambiciones nucleares y la obtención de información estratégica.

10. LOS ACONTECIMIENTOS EN AFGANISTÁN DESENCADENAN OPERACIONES DE ESPIONAJE E INFORMACIÓN

Con la afirmación del control Talibán y la salida de las fuerzas estadounidenses de Afganistán, se pueden anticipar más operaciones de ciberespionaje e información. Empezaremos a ver a los actores habituales de las operaciones de información, Irán, China y Rusia, impulsar narrativas para apoyar sus intereses hasta finales de 2021 y principios de 2022. También harán hincapié en las percepciones negativas en torno a los acontecimientos, especialmente la percepción de que los Estados Unidos no cumplió sus compromisos con organizaciones y países. La declaración de un emirato también puede envalentonar a los perpetradores extremistas proislámicos para que amplíen sus actividades de propaganda, lo que incluye tácticas de hacktivismo, como sustituciones, la apropiación de cuentas en las redes sociales y la difusión de "listas de asesinatos" compiladas a partir de datos de código abierto o comprometidos.

Los deepfakes se han utilizado para facilitar el fraude BEC, eludir los protocolos MFA y la verificación de identidad KYC.

11. DEEPFAKES: NO SOLO PARA LAS OPERACIONES DE INFORMACIÓN

La eficacia de las deepfakes (videos falsos con apariencia muy real) en las operaciones de información se ha debatido en la comunidad de seguridad, pero los actores patrocinados por el estado y con motivaciones financieras también han demostrado un creciente interés en esta tecnología. Mandiant observó publicaciones y anuncios sobre la tecnología deepfake en foros criminales clandestinos en ruso e inglés a lo largo de 2020 y 2021. Los usuarios de estos foros clandestinos anunciaban vídeos e imágenes deepfake personalizados, así como formación para que los usuarios crearan sus propios medios manipulados. El audio deepfake ha facilitado esquemas de fraude del tipo de correo electrónico comercial (BEC).

Las fuentes abiertas ponen de relieve cómo los perpetradores han utilizado medios de comunicación manipulados para eludir los protocolos de seguridad de la autenticación multifactorial (MFA) y las medidas de verificación de identidad de Conozca a su Cliente (KYC). Prevemos que a medida que aumente la disponibilidad de la tecnología deepfake en 2022 en adelante, los perpetradores de delitos y de espionaje integrarán cada vez más medios manipulados en sus operaciones para hacer más convincente la ingeniería social, adaptar fácilmente el contenido a objetivos específicos y derrotar algunos sistemas de verificación de identidad automatizados.

12. LA SUBCONTRATACIÓN CIBERNÉTICA AUMENTA LA VELOCIDAD Y EL IMPACTO DE LAS OPERACIONES MALICIOSAS

La subcontratación de las operaciones maliciosas a través de distintos mecanismos, como los programas de afiliación de ransomware, los vendedores de exploits, los contratistas comerciales, los vendedores de malware y los autónomos, contribuye tanto a la creciente frecuencia como a la complejidad de la actividad de las ciberamenazas. No vemos indicios de que esto merme en 2022. La difuminación de las distinciones entre las operaciones con motivación financiera y las patrocinadas por el estado, tanto en lo que respecta a las herramientas como al talento, la maduración de los mercados legítimos e ilegítimos de herramientas y servicios de terceros, y la creciente especialización y mercantilización de las competencias en materia de ciberamenazas (en particular en las comunidades de ciberdelincuentes) contribuyen a que las capacidades más sofisticadas sean accesibles para un grupo más amplio de naciones patrocinadoras y perpetradores de delitos. Para los defensores, esto se traduce en un aumento del riesgo cibernético general a medida que aumenta la cantidad, la calidad y la adaptabilidad de las operaciones maliciosas. También complica la atribución, el seguimiento y la distinción de conjuntos de actividades, así como el desarrollo de estrategias defensivas centradas en los motivos y las TTP de los perpetradores.

La proporción de investigaciones de respuesta a incidentes de Mandiant que involucran recursos en la nube ha crecido en los últimos años.

13. LA NUBE Y LOS TERCEROS INTRODUCEN NUEVOS PUNTOS DE ESTRANGULAMIENTO

Las organizaciones seguirán confiando cada vez más en la nube y en los proveedores de terceros alojados en la nube para las principales tareas empresariales, lo que supone una mayor presión para que esos terceros mantengan tanto la disponibilidad como la seguridad. Si cualquiera de estas características se deteriora, las organizaciones deben estar preparadas para trabajar en torno a las alteraciones y diagnosticar, abordar y recuperarse de un incidente cuando pueden no haber sido el objetivo principal y pueden no tener acceso a la imagen completa del ciclo de vida del ataque en los registros internos. La proporción de investigaciones de respuesta a incidentes de Mandiant que involucran recursos en la nube ha crecido en los últimos años. Prevemos que vulneraciones y abusos en la nube seguirán creciendo junto con la adopción de la nube por parte de las empresas durante 2022. Sospechamos que las organizaciones que utilizan la nube y los proveedores alojados en ella pueden ser más vulnerables a los ataques, así como a los errores, las vulnerabilidades, las desconfiguraciones o las interrupciones que afecten a los recursos de la nube.

14. MÁS DISPOSITIVOS DEL INTERNET DE LAS COSAS, MÁS VULNERABILIDADES, MÁS SUPERFICIE DE ATAQUE

En los próximos años, esperamos ver un crecimiento continuo de los dispositivos de la Internet de las Cosas (IoT), muchos de los cuales serán baratos y se crearán sin tener realmente en cuenta la seguridad. El número de vulnerabilidades que introducen, tanto en el software como en el hardware, hará que sea difícil para los cazadores de errores mantenerse al día. Dado que todos estos dispositivos están conectados, veremos cómo se amplía la superficie de ataque general con el potencial de un impacto grave. Lamentablemente, no se ha hecho suficiente hincapié en la seguridad en el diseño fundamental de los dispositivos del IoT para solucionar estos problemas, por lo que la situación no hará más que empeorar en los próximos años. Cuando se publican correcciones para las vulnerabilidades recién descubiertas, el usuario debe tomar la iniciativa de actualizar sus dispositivos. Es posible que la mayoría de los usuarios nunca se dé cuenta de que es necesaria una actualización, y si lo hacen, puede que ni siquiera les importe. No ha habido ninguna iniciativa coordinada de seguridad para los dispositivos IoT. Tecnologías como Secure Boot están ayudando, pero solo están siendo implementadas por organizaciones más grandes y en productos más nuevos. Es cierto que empresas como Microsoft y Amazon están creando plataformas que ofrecerán a las empresas más pequeñas la oportunidad de construir dispositivos IoT más seguros. Estos son pasos en la dirección correcta, pero pasarán varios años antes de que se logre un panorama de IoT seguro.

No ha habido ninguna iniciativa coordinada de seguridad para los dispositivos IoT.

EN BUSCA DE UN FUTURO MÁS SEGURO

Puede que las "predicciones" tengan más fuerza, pero en ciberseguridad quizá sea más apropiado hablar de "pronóstico". Eso es porque nuestras expectativas de futuro se basan en las tendencias que vemos ahora. Y no se trata solo de los comportamientos de los atacantes; tenemos en cuenta todo lo demás, desde la tecnología y las tendencias en el lugar de trabajo hasta los cambios en la legislación y en la normativa.

Todos los informes recientes de Mandiant sobre predicciones han incluido una sección sobre el ransomware. Este año no es una excepción; de hecho, nuestras perspectivas sobre la amenaza para 2022 son quizá más sombrías. Los actores del ransomware son cada vez más agresivos, convirtiendo estos ataques, antes relativamente sencillos, en operaciones multifacéticas de extorsión más elaboradas —y lucrativas. Los esfuerzos estadounidenses e internacionales contra el ransomware están en marcha, pero no han afectado al modelo de negocio del ransomware como servicio. En un giro cruel, los esfuerzos del gobierno podrían conducir a resultados negativos para las organizaciones.

El ransomware no va a ir a ninguna parte, y tampoco el espionaje y las operaciones de información. En 2022, seguiremos viendo la actividad regional e internacional de los cuatro grandes: Rusia, Irán, China y Corea del Norte. También veremos este tipo de actividad derivada de los recientes acontecimientos en Afganistán. El aumento del uso de la tecnología deepfake no hará más que agravar las amenazas.

Las organizaciones tienen mucho que considerar en 2022, pero permanecer atentas les permitirá defenderse de las próximas amenazas y responder a las que inevitablemente se produzcan. Mandiant, que incorpora la más amplia y profunda experiencia cibernética e inteligencia sobre amenazas en tecnologías dinámicas de ciberdefensa, ayudará a empoderar a las organizaciones.

Más información en **www.mandiant.com**

Mandiant
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

Acerca de Mandiant
Desde 2004, Mandiant® ha sido un socio de confianza para las organizaciones preocupadas por la seguridad. En la actualidad, la inteligencia y la experiencia de Mandiant, líderes en el sector, impulsan soluciones dinámicas que ayudan a las organizaciones a desarrollar programas más eficaces e infundir confianza en su preparación cibernética.

MANDIANT

2021 Mandiant, Inc. Todos los derechos reservados. Mandiant es una marca registrada de Mandiant, Inc. Todas las demás marcas, productos o nombres de servicios son o pueden ser marcas comerciales o marcas de servicio de sus respectivos propietarios. M-EXT-RT-US-EN-000410-01