MANDIANT®

NOW PART OF Google Cloud

Previsión de ciberseguridad para 2023

Introducción

Nuestras previsiones sobre el año que se avecina se han denominado anteriormente "predicciones". Sin embargo, nuestras reflexiones sobre el panorama de la ciberseguridad para el año que viene se basan siempre en las tendencias que ya observamos. "Previsión" es un término que describe con mayor precisión nuestro propósito. Y así, presentamos la Previsión de ciberseguridad de Mandiant para 2023. Este informe está repleto de reflexiones sobre el futuro de varias de las mentes más brillantes de Mandiant, como Sandra Joyce, jefa de Inteligencia global, y Charles Carmakal, director de Tecnología de consultoría, así como Phil Venables, director de Seguridad de la información de Google Cloud.

Las amenazas evolucionan, los atacantes cambian constantemente sus tácticas, técnicas y procedimientos, y los defensores deben adaptarse y mantenerse implacables si quieren estar a la altura. Esta previsión tiene como objetivo ayudar a la industria de la ciberseguridad a enmarcar su lucha contra los ciberadversarios en 2023.

Previsiones globales

Más ataques por parte de atacantes no organizados y que no son Estados nación

En 2023 esperamos ver más intrusiones llevadas a cabo por atacantes no organizados y que no son Estados nación. Es probable que un mayor número de actores de amenazas que operan fuera de Norteamérica y Europa sean más jóvenes y lleven a cabo operaciones de intrusión, no porque estén interesados en ganar dinero específicamente, o porque los Gobiernos les hayan encargado hacerlo, sino para poder presumir ante sus amigos o alardear en línea de haber hackeado y avergonzado a organizaciones prominentes. Aunque les complace obtener beneficios económicos, esa no es necesariamente su principal motivación.

Europa podría superar a Estados Unidos como la región más atacada por el ransomware

El ransomware sigue teniendo un impacto significativo en las empresas de todo el mundo. Si bien los informes indican que Estados Unidos es el país más atacado por el ransomware en todo el mundo,[1] pequeños indicadores muestran que la actividad del ransomware está disminuyendo en Estados Unidos y creciendo en otras regiones.[2] En Europa, el número de víctimas está aumentando, y si ese incremento continúa, es probable que Europa se convierta en la región más atacada en 2023. Estados Unidos se ha mostrado muy firme en cuanto a las políticas, las sanciones y la posibilidad de una respuesta en el ámbito cibernético en relación con el ransomware y otros ataques. Sin embargo, es difícil concluir si la postura más agresiva frente al ransomware disuade realmente los ataques.

Más extorsión, menos ransomware

Históricamente, los ciberdelincuentes han utilizado el ransomware para obtener beneficios económicos del acceso a la red de la víctima. Debido a varias vulneraciones visibles y de alto perfil el año pasado, las organizaciones consideran que mitigar el daño a la marca es una razón mucho más convincente para pagar un rescate que para recuperar el acceso a los sistemas cifrados. Durante el próximo año, los criminales continuarán recurriendo a la extorsión, pero las implementaciones reales de ransomware podrían disminuir. Los proveedores de ransomware como servicio (RaaS) modernizarán su software para centrarse en la exfiltración de datos y en los "sitios de filtración" para avergonzar públicamente.

1. FCW (27 de septiembre de 2022). Estados Unidos es el principal blanco de los ataques de ransomware, según un informe.
2. Washington Post (17 de agosto de 2022). La disminución de las cifras de ransomware, ¿es una ilusión?

Las cuatro grandes

Rusia cibernética y la invasión de Ucrania

La invasión rusa de Ucrania creó circunstancias sin precedentes para la actividad de las ciberamenazas. Este es probablemente el primer caso en el que una gran potencia cibernética ha llevado a cabo ataques perturbadores, ciberespionaje y operaciones de información de forma simultánea a operaciones militares generalizadas y cinéticas. Mandiant anticipa futuros ataques disruptivos en Ucrania y sugiere que es probable que vayan acompañados de operaciones de información concurrentes. Esperamos que el deseo de Rusia de utilizar tácticas disruptivas, así como frentes de hacktivistas falsos o cooptados (para atribuirse la filtración y destrucción de datos) se extienda cada vez más fuera de Ucrania y sus vecinos inmediatos.

La asertividad cibernética china

El ciberespionaje chino supone una amenaza de alta frecuencia y magnitud para las organizaciones de todo el mundo, tanto del sector público como del privado. Los principales motores de la actividad de las ciberamenazas chinas serán la integridad territorial y la estabilidad interna, la hegemonía regional y la expansión de la influencia política y económica mundial. La actividad de operaciones de ciberespionaje e información en apoyo de los intereses económicos y de la seguridad nacional de China continuará intensificándose. En 2022, una campaña de operaciones de información a favor de la República Popular China se dirigió directamente a entidades comerciales de una industria de importancia estratégica para Pekín.[3] Consideramos que este ataque más amplio a entidades del sector privado es notable, y es posible que veamos a competidores globales de empresas chinas en otras industrias como objetivo de tales operaciones de información.

Escalada iraní

Mandiant prevé que los grupos de ciberespionaje iraníes continuarán llevando a cabo una amplia actividad de recopilación de información, especialmente contra objetivos gubernamentales y de Oriente Medio, así como contra entidades de telecomunicaciones, transporte y otras. Prevemos que la intención de los actores de la amenaza iraní de utilizar ciberataques disruptivos y destructivos continuará intacta, a falta de un cambio significativo en el actual aislamiento internacional de Irán.

Corea del Norte desea ingresos e inteligencia

Evaluamos con gran confianza que Corea del Norte continuará realizando operaciones que apoyen al régimen tanto con fuentes de ingresos como con inteligencia estratégica. El aislamiento político y económico internacional, junto con los problemas de salud pública, probablemente informarán del ciberespionaje norcoreano contra objetivos diplomáticos, militares, financieros y farmacéuticos. Creemos que la actividad se centrará principalmente en Corea del Sur, Japón y Estados Unidos, y que también se llevarán a cabo operaciones en Europa, Oriente Medio y el Norte de África, así como en el sur de Asia.

3. Mandiant (28 de junio de 2022). Campaña de influencia de DRAGONBRIDGE a favor de la República Popular de China apunta a compañías de minería de tierras raras con la intención de desbaratar la competencia por el dominio del mercado que detenta este país.

Las operaciones de información dependerán más de las organizaciones de terceros para una negación plausible

Históricamente, las operaciones de inteligencia siempre han tenido una motivación política y han sido patrocinadas por el Estado, como observamos en las elecciones de 2016 en Estados Unidos.[4] Desde entonces, hemos observado una mayor externalización del trabajo de las operaciones de inteligencia por parte de los actores estatales. Esta podría ser una tendencia creciente en 2023, a medida que las contrataciones de "hackers por encargo" sean más comunes. En 2019, los investigadores de la inteligencia de fuentes abiertas (Open Source Intelligence, OSINT) observaron una campaña en las redes sociales a favor de las operaciones de inteligencia indonesias, llevada a cabo por la empresa de medios de comunicación InsightID, con sede en Yakarta.[5] Esta campaña tenía como objetivo distorsionar la verdad sobre los acontecimientos en la conflictiva provincia indonesia de Papúa. Coincidiendo con esta observación, Meta testificó a mediados de 2021 sobre el incremento de la contratación de empresas de marketing o relaciones públicas en las campañas de operaciones de inteligencia, para reducir la barrera de entrada de algunos actores de amenazas y ofuscar las identidades de los más sofisticados.[6]

Las empresas se inclinarán por la autenticación sin contraseña

El robo de credenciales corporativas continúa siendo una de las principales formas de acceso de los ciberdelincuentes a las víctimas. Además, en 2022, se han producido varios ejemplos de atacantes que han encontrado formas de eludir las tecnologías de autenticación multifactor. Apple, Google y Microsoft se han comprometido a crear recursos sin contraseña para el consumidor basados en los estándares de la FIDO Alliance y el World Wide Web Consortium.[7] La implementación inicial de estas tecnologías se centrará en los recursos sin contraseña para el consumidor, pero los directores de seguridad de la información exigirán plataformas de identidad empresarial para ampliar los conceptos sin contraseña al mercado empresarial. Durante el próximo año, busque soluciones sin contraseña centradas en la empresa.

La identidad primero, la identidad perdida

Los actores de las amenazas han pasado de obtener el control de un endpoint a acceder a las credenciales y la cuenta de un usuario. La identidad de un usuario dentro de una organización se ha vuelto más crítica que el acceso al endpoint del usuario. Durante el próximo año, veremos que los actores de las amenazas encontrarán nuevas formas de robar las identidades de los usuarios utilizando una combinación de ingeniería social, robos de información de productos básicos y la recopilación de información de fuentes de datos internas después del ataque. Combinarán las credenciales robadas con nuevas técnicas para eludir la autenticación multifactorial y utilizar de forma abusiva los sistemas de gestión de la identidad y el acceso.

4. Departamento de Justicia de los EE. UU. (Marzo de 2019). Informe sobre la investigación de la injerencia rusa en las elecciones presidenciales de 2016.
5. Instituto Australiano de Política Estratégica (ASPI) (15 de octubre de 2019). Investigación conjunta BBC-ASPI sobre las operaciones de información en Papúa Occidental.
6. ZDNET (29 de julio de 2021). Desinformación por encargo: Las empresas de relaciones públicas son el nuevo campo de batalla de Facebook.
7. Apple (5 de mayo de 2022). Apple, Google y Microsoft se comprometen a ampliar el apoyo al estándar de la FIDO para acelerar la disponibilidad de los inicios de sesión sin contraseña.

Los atacantes leerán más investigaciones sobre seguridad para aprender tácticas ofensivas y defensivas

Se espera que la tendencia observada en 2022 vaya en aumento: Los actores de las amenazas continuarán estudiando los blogs y las investigaciones de los analistas de la comunidad de seguridad. Lo harán para aprender tácticas y técnicas ofensivas, estrategias defensivas y cómo aprovechar las vulnerabilidades. Es posible que descubran formas ingeniosas de irrumpir en las organizaciones, o tal vez aprendan técnicas sobre las que se escribió en un post de seguridad hace dos o tres años, pero que no se han utilizado realmente en la práctica. Ya pudimos advertir que los actores de las amenazas leen los blogs de seguridad de los defensores para saber cómo pueden ser detectados.

El ciberseguro será más difícil de obtener y la cobertura puede ser restringida

A lo largo de los años, más empresas han confiado en el ciberseguro para cubrir sus riesgos cibernéticos, ya que la dirección es más consciente de los riesgos de ciberseguridad. Sin embargo, los reclamos también se han disparado, obligando a las empresas aseguradoras a reevaluar su capacidad de riesgo y reducir la cobertura en consecuencia. Muchas empresas que intentan renovar su ciberseguro, o que acaban de entrar en el mercado de los ciberseguros, pueden encontrar dificultades para obtener la cobertura que desean.

Incremento generalizado de los infostealers y de la recopilación de credenciales

El robo de credenciales conduce a intrusiones de gran impacto. Mandiant constató que las credenciales utilizadas en las intrusiones están disponibles a través de infostealers como REDLINESTEALER, VIDAR y RACOONSTEALER. Estos programas stealers están ampliamente disponibles en la red y la compra de credenciales es una alternativa barata a tratar de robarlas a las víctimas. Cada vez habrá más denuncias de intermediarios de acceso inicial en foros y otros lugares (donde los atacantes venden el acceso una vez que han explotado con éxito un punto de entrada), así como la venta de credenciales o cookies, que serán cada vez más utilizadas para obtener acceso a las organizaciones con menor costo, complejidad y tiempo.

Cuando el mundo real y el mundo virtual se encuentran

Hasta ahora hemos observado y encontrado ataques por SMS, correo electrónico y redireccionamiento de aplicaciones. Ahora vemos surgir un nuevo modelo: un enfoque que consiste en engañar a las víctimas en el mundo real. Por ejemplo, en 2022 observamos una campaña en la que las víctimas recibían un recibo de entrega de paquetes en sus buzones de correo físico. El recibo contenía un código QR que les dirigía a un sitio de robo de identidad y de números de tarjetas de crédito. En 2023, esperamos ver más esquemas similares, donde el atacante utiliza elementos físicos cotidianos para engañar a sus víctimas. Publicidades falsas, llaves USB falsas, recibos falsos: las posibilidades para los atacantes son infinitas. Educar a los empleados y al público es la mejor defensa contra este tipo de amenazas.

Mayor énfasis federal para proteger la infraestructura técnica nacional contra actividades maliciosas

En 2023, esperamos que el Gobierno de Biden ponga en marcha una serie de políticas coherentes tras la Orden Ejecutiva de *2021 sobre cómo mejorar la ciberseguridad de la nación*[8] *y el Memorándum de Seguridad Nacional de 2022.*[9] Aunque la colaboración entre el sector público y el privado haya crecido en los últimos tiempos, es necesario profundizar en la coordinación entre las agencias y las grandes organizaciones tecnológicas. Esperamos que el Gobierno pueda implementar más puntos de control de seguridad para que las organizaciones reflexionen sobre el progreso que han hecho para cumplir con los requisitos regulatorios. A medida que se establezcan estas oportunidades, podemos esperar ver un mayor intercambio de conocimientos entre las organizaciones públicas y privadas, lo que aumenta la transparencia y la protección en torno a las amenazas de impacto más recientes.

8. La casa blanca (12 de mayo de 2021). Orden Ejecutiva para mejorar la ciberseguridad del país.
9. La Casa Blanca (19 de enero de 2022). HOJA DE DATOS: El presidente Biden firma un memorándum de seguridad nacional para mejorar la ciberseguridad de los sistemas de seguridad nacional, del Departamento de defensa y de la comunidad de inteligencia.

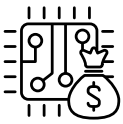
Previsiones de la APJ

Actividad cibernética en torno a las elecciones en el sudeste asiático en 2023

Varios países del sudeste asiático celebran elecciones generales en 2023, o se espera que lo hagan. Nos estamos preparando para las elecciones generales de Camboya, Malasia, Myanmar y Tailandia. Los grupos de ciberespionaje han tenido interés en anteriores elecciones del sudeste asiático y las de 2023 pueden resultar un blanco atractivo. También se prevé que estas elecciones se utilicen como señuelo para el phishing y la ingeniería social. Las elecciones filipinas se celebraron en 2022, y el Gobierno denunció 20 000 intentos de ataque a los sistemas electorales automatizados.[10]

Los países de Asia-Pacífico podrían sufrir más ataques de represalia por parte de grupos hacktivistas prorrusos

En 2023, se espera que Rusia ataque más a las entidades de Asia-Pacífico. Desde la invasión rusa a Ucrania a principios de 2022, varios países de Asia-Pacífico decidieron imponer sanciones a Rusia y, en respuesta, este país catalogó a varios países de Asia-Pacífico como "no amistosos". Cuando eso ocurrió, suscitó preocupación en la región de Asia-Pacífico porque se sabía que los actores del nexo ruso realizaban ciberataques de represalia contra organizaciones internacionales, los Juegos Olímpicos de PyeongChang en 2018 fue uno de esos casos. El ataque a organizaciones de Asia-Pacífico representa un incremento y expansión significativos de los ataques, y las organizaciones con sede en Asia-Pacífico también deberían prepararse para recibir este tipo de ataques en los próximos meses.



Elevados niveles de amenaza e interrupciones para los fabricantes de semiconductores en Asia-Pacífico

Si se interrumpen las cadenas de suministro, los fabricantes de semiconductores pueden correr más riesgos de seguridad, como ser más vulnerables ante una infección de ransomware. Los datos disponibles[11] resaltan que la industria manufacturera crítica, que incluye la industria de los semiconductores, sigue siendo un objetivo constante del ransomware. Los productores de semiconductores son más propensos a pagar rescates para evitar pérdidas económicas por interrupciones de la producción o paralizaciones del trabajo a gran escala. Estos riesgos, sumados a los conflictos geopolíticos actuales entre China y Estados Unidos, pueden provocar nuevas perturbaciones cibernéticas en la industria de los semiconductores en 2023.

10. CNN Filipinas (11 de mayo de 2022). El Gobierno bloquea más de 20 000 intentos de hackear las elecciones, según Esperon.
11. Recorded Future (29 de septiembre de 2022). Compañías de semiconductores en el punto de mira del ransomware.

Previsiones para la región de EMEA

Rusia ampliará sus objetivos en toda Europa

Una parte importante de la actividad cibernética rusa se centró en Ucrania desde el inicio del conflicto, pero en 2023 Rusia podría ampliar aún más sus operaciones cibernéticas en toda Europa. Lo más probable es que los meses de invierno desaceleren el ritmo de los conflictos físicos, lo que podría permitir que los actores rusos tengan mayor capacidad de amenaza. En el último año, Rusia solía realizar campañas de recopilación de información contra organizaciones europeas fuera de Ucrania, mientras que la mayoría de sus ataques perturbadores y destructivos se centraban en Ucrania. Esto podría cambiar en 2023, con el uso por parte de Rusia de más de sus capacidades cibernéticas disruptivas (potencialmente aumentadas) contra las organizaciones europeas. Esto podría afectar a distintas organizaciones, como proveedores de energía y militares, empresas de logística que participan en el suministro de bienes a Ucrania y organizaciones que participan en la introducción e implantación de regímenes de sanciones.

Las inquietudes europeas sobre la energía se desarrollan en el ámbito cibernético

Es probable que la inquietud por el suministro y los precios energéticos en Europa se manifieste en forma de operaciones cibernéticas maliciosas. Mandiant afirma haber observado un aumento de las campañas de phishing con temática energética. Se sabe que los grupos de ransomware se dirigen a sectores bajo presión, como se demostró con el implacable ataque al sector de la atención médica durante la pandemia.[12] Las empresas energéticas europeas podrían enfrentarse a una mayor cantidad de ataques durante los próximos meses de invierno.

Los proveedores de energía europeos también son un objetivo para los actores patrocinados por el Estado ruso que buscan ejercer más presión sobre los países involucrados en los regímenes de sanción rusos o que buscan reducir su dependencia de la energía rusa. La presión sobre el suministro energético europeo también aumentará el interés por los proveedores de energía no europeos. La disponibilidad de petróleo y gas, los movimientos de precios planificados por organizaciones como la OPEP y el desarrollo de políticas energéticas gubernamentales se convertirán en un objetivo de recopilación más importante para las agencias de inteligencia estatales.

La crisis energética en Europa también puede dar lugar a una mayor atención a las infraestructuras críticas. Las infraestructuras críticas ya corren el riesgo de sufrir ciberataques destructivos cuando las naciones están en conflicto, pero la crisis energética amplía la amenaza. Podríamos ver cómo las infraestructuras críticas son objeto de campañas de ransomware centradas en la interrupción del suministro de energía y electricidad.

12. The Verge (19 de agosto de 2021). La pandemia reveló los riesgos de salud que suponen los ataques de ransomware en los hospitales.

Conclusión

El ransomware ocupa un lugar destacado en los informes de Mandiant desde hace varios años, y con razón. Aunque está bien establecido como parte de los conjuntos de herramientas de muchos actores, los datos muestran más bien un descenso en los incidentes de ransomware en Estados Unidos y un aumento en los incidentes de ransomware en Europa. Aunque las entidades de regiones europeas deben mantenerse atentas, las organizaciones de todo el mundo deben estar preparadas para recibir más intentos de extorsión. Los actores dedicados a la extorsión no se detendrán ante nada para lograr sus objetivos, incluido el uso de dispositivos físicos y tipos de ingeniería social menos comunes.

También se espera que el próximo año aumente la cantidad de atacantes motivados simplemente por el derecho a presumir. Estos actores suelen ser más jóvenes y no están vinculados a un Estado nación o a un grupo organizado. Sin embargo, eso no significa que no vayamos a ver actividad de los Estados nación. Las Cuatro Grandes, Rusia, China, Irán y Corea del Norte, serán muy activas en 2023, utilizando ataques destructivos, operaciones de información, amenazas financieras y más.

El camino hacia una mejor defensa cibernética nunca fue fácil, especialmente para los profesionales de la seguridad. Las organizaciones tienen mucho que tener en cuenta para 2023. Como siempre, el incesante trabajo de Mandiant en primera línea recopila información y desarrolla las mejores prácticas que compartimos regularmente con los responsables de seguridad, para que puedan tomar las medidas necesarias para prevenir estas amenazas y responder rápida y eficazmente ante los ataques que invariablemente se producen.

Colaboradores

En los últimos años de publicación de Mandiant Cyber Security Forecast (antes Security Predictions), Sandra Joyce, jefa de Inteligencia Global, y Charles Carmakal, CTO Consultor, lideraron el informe. Este año agregamos las opiniones de Phil Venables, CISO de Google Cloud. Muchos otros expertos de Mandiant también colaboraron en este informe, entre ellos:

Geoff Ackerman
Jamie Collier
Vivek Chudgar
David Grout
Emiel Haeghebaert
Sarah Hawley
Scott Henderson
John Hultquist
Isif Ibrahima
Jeff Johnson
Igors Konovalovs
Steve Ledzian
Yihao Lim
Keith Lunden
Brendan McKeague
Jens Monrad
Jake Nicastro
Parnian Najafi
Dan Perez
Fred Plan
Clayton Quinlan
Alice Revelli
Nick Richard
Marcin Siedlarz
Matt Shelton
Lindsay Smith
Genevieve Stark
Josh Stern
Van Ta
Kelli Vanderlee

Más información en www.mandiant.com

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

Acerca de Mandiant

La experiencia e inteligencia sobre amenazas de Mandiant, líderes en la industria, impulsan soluciones de seguridad dinámicas que ayudan a las organizaciones a desarrollar programas más eficaces e infundir confianza en su preparación cibernética. Mandiant ahora forma parte de Google Cloud.

MANDIANT
NOW PART OF Google Cloud