EL INFORME DE CIBERAMENAZAS

Junio de 2023

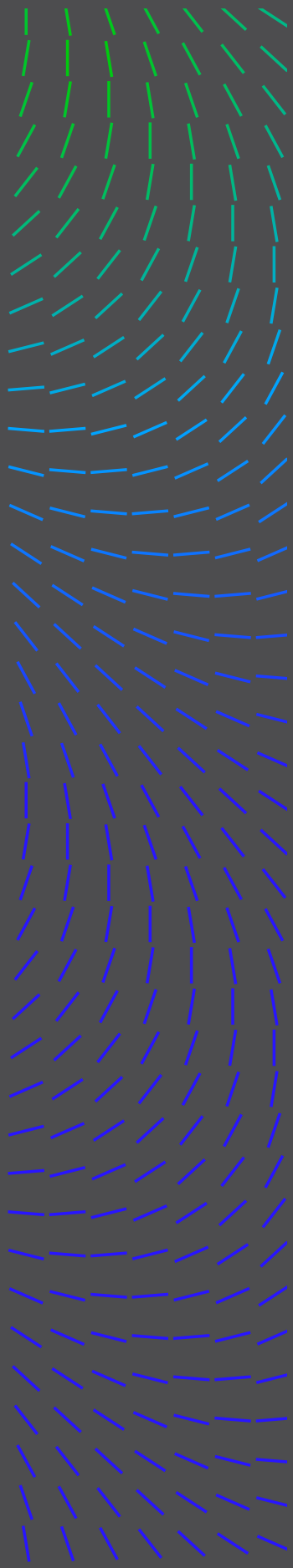
Información obtenida de una red mundial de expertos, sensores, telemetría e inteligencia

Presentado por

Trellix ADVANCED RESEARCH CENTER

EL INFORME DE CIBERAMENAZAS

Elaborado por el Advanced Research Center de Trellix, este informe (1) destaca las perspectivas, la inteligencia y la orientación obtenidas de múltiples fuentes de datos críticos sobre amenazas a la ciberseguridad, y (2) desarrolla interpretaciones expertas, racionales y razonables de estos datos para orientar y facilitar las mejores prácticas en ciberdefensa. Esta edición se centra en los datos y observaciones recogidos entre el 1 de enero y el 31 de marzo de 2023.



Las ciberamenazas siguen evolucionando y multiplicándose, a gran velocidad y a gran escala.

Mientras los equipos de operaciones de seguridad (SecOps) se apresuran a defender la información, los activos y las operaciones, todos carecen de una visión completa del panorama de las amenazas.

¿Por qué? Adquirir perspectiva requiere un horizonte amplio. Múltiples fuentes. Flujos de datos. Inteligencia en bruto. Volúmenes masivos de telemetría.

Una visión real requiere una visión estratégica de muchas organizaciones y sectores. Y regiones. Y superficies de ataque.

Bienvenido a la edición de junio de 2023 del Informe de ciberamenazas.

COMPRENDER LOS RIESGOS, AMENAZAS Y VULNERABILIDADES A LOS QUE SE DIRIGEN LOS ATACANTES Y NEUTRALIZARLOS ACTIVAMENTE

Paso mucho tiempo hablando con miembros de consejos de administración, CEO, CISO, CIO, CTO y otros líderes responsables de la ciberdefensa de países, organismos gubernamentales y empresas del sector privado de todos los sectores.

Tratamos una amplia gama de temas, desde la investigación, la innovación y la inteligencia globales hasta las últimas prácticas de ciberdefensa de sus equipos de SecOps. Hablamos de sus retos, tal y como Trellix ha documentado recientemente en nuestro informe liderazgo de pensamiento La mente del CISO: por ejemplo, demasiadas fuentes de información diferentes (35 %), mandatos normativos y requisitos legales cambiantes (35 %), superficies de ataque crecientes (34 %), escasez de personal cualificado (34 %) y falta de adopción y uso por parte de otras partes de la empresa (31 %)[1].

Casi todas estas interacciones abordan, directa o implícitamente, la naturaleza del entorno de amenazas. ¿Qué tipos de ataques se están produciendo? ¿Cuáles son los grupos de ransomware más impactantes? ¿Cuáles son las vulnerabilidades atacadas? ¿Qué países parecen ser los más activos? ¿Qué tendencias de amenazas estamos siguiendo en la seguridad del correo electrónico y de la red?

"Como miembro del consejo de administración, CEO, CISO, CIO, CTO o miembro del equipo de SecOps, este conocimiento -compartido en este informe y a través de la rica biblioteca de Trellix de orientación, información y perspectivas- es a menudo crítico para su misión.

En Trellix tenemos mucho que compartir, porque estamos en primera línea todos los días. Estamos aprovechando una enorme reserva de inteligencia de seguridad, conocimientos y datos obtenidos de más de mil millones de sensores en todo el mundo. Como miembro del consejo de administración, CEO, CISO, CIO, CTO o miembro del equipo de SecOps, este conocimiento -compartido en este informe y a través de la rica biblioteca de Trellix de orientación, información y perspectivas- es a menudo crítico para su misión.

Mi compañero John Fokker, que dirige la práctica de inteligencia de amenazas dentro del equipo de élite del Advanced Research Center de Trellix, ha recopilado un excelente informe. Utilice esta información para ayudar a centrar su equipo, reforzar sus procesos e implantar las tecnologías XDR adecuadas. Y díganos qué temas podemos abordar en futuras ediciones para ayudar a garantizar el éxito y la seguridad de su organización.

Joseph (Yossi) Tal
SVP, JEFE DEL TRELLIX ADVANCED RESEARCH CENTER

EN APOYO DE LOS HÉROES EN PRIMERA LÍNEA DE LA CIBERSEGURIDAD

Trabajo con héroes. No me refiero a mi equipo, aunque se les haya considerado con superpoderes a lo largo de sus diversas trayectorias profesionales en los sectores público y privado.

Me refiero a ustedes. Me refiero a las personas y equipos de todo el mundo que confían en las avanzadas capacidades de investigación de Trellix -nuestros sistemas, conocimientos e inteligencia- para proteger a sus organizaciones de los ciberataques. CISO, CTO y CIO, sí, así como nuestros colegas de agencias como Europol, el FBI y la NSA, la Cybersecurity and Infrastructure Security Agency (CISA), el Centro Australiano de Ciberseguridad (ACSC, Australian Cyber Security Centre). y el Centro Nacional de Ciberseguridad del Reino Unido (NCSC-UK, National Cyber Security Centre). Igual de importante -y quizá incluso más- es que me refiero a todos los miembros de su equipo de SecOps.

"Como sabe perfectamente por su trabajo diario, la ciberseguridad evoluciona con extraordinaria rapidez. Avances tecnológicos y una fuerte tendencia hacia la adopción de XDR.

¿Cuáles cree que son los elementos que realmente marcan la diferencia en su misión de SecOps? Según el informe de Trellix que mi compañero Yossi mencionó anteriormente, los líderes de ciberseguridad de todo el mundo compartieron su punto de vista sobre ellos. Entre ellos se incluyen una mejor visibilidad (44 %), una mayor priorización de lo que importa (42 %), una colaboración más amplia para abordar ataques multivectoriales (40 %) y una mayor precisión (37 %)[2].

Cada uno de estos factores depende fundamentalmente de la precisión de las perspectivas, la información y los datos, como el contenido de este informe.

Como sabe perfectamente por su trabajo diario, la ciberseguridad evoluciona con extraordinaria rapidez. Avances tecnológicos y una fuerte tendencia hacia la adopción de XDR, cambios normativos, desde las leyes hasta la responsabilidad, y cambios en el entorno de las amenazas. Se está produciendo una revolución, una transformación en la forma en que los equipos de SecOps pueden anticiparse a la próxima generación de ciberataques. El éxito siempre empieza por comprender nuestro estado actual.

Estamos juntos en esto. Con Trellix no tiene por qué preocuparse. Este informe es para usted.

John Fokker
JEFE DE INTELIGENCIA SOBRE AMENAZAS
E INGENIERO PRINCIPAL
TRELLIX ADVANCED RESEARCH CENTER

[1] Trellix, "2023 Report: The Mind of the CISO", 2023.
[2] Trellix, "2023 Report: The Mind of the CISO", 2023.

INTRODUCCIÓN

Contexto estratégico: un mundo inestable

Interpretar los datos de este informe requiere comprender "el panorama general" a escala mundial. Esto se debe a que las ciberamenazas a organizaciones de todo el mundo no se producen en un vacío técnico. Entre los principales impulsores del ciberriesgo se encuentran las guerras y otras fuerzas mayores, los cambios a gran escala en los ciclos económicos y las nuevas vulnerabilidades que pueden surgir cada vez que un equipo introduce cambios en factores como los modelos de negocio, los partners clave, los procesos básicos, la adopción de tecnología y el cumplimiento de normativas. Una muestra de los factores que influyen en nuestros datos sobre amenazas del primer trimestre de 2023 incluye:

La invasión rusa de Ucrania y la guerra asimétrica contra Occidente: la ciberactividad con fines de espionaje, guerra y desinformación al servicio de las ambiciones políticas, económicas y territoriales de los Estados más importantes sigue intensificándose. Los hackers lanzan ciberataques cada vez más sofisticados contra empresas, gobiernos e infraestructuras occidentales.

Control consolidado de Xi Jinping sobre China y sus aspiraciones geopolíticas: Los objetivos nacionalistas de China, su política exterior asertiva y sus prácticas de espionaje corporativo siguen impulsando los ciberriesgos, ya que los grupos de amenazas persistentes avanzadas (APT) afiliados a China dominan el panorama mundial.

Economías en desarrollo y rápida expansión de las infraestructuras: en el desarrollo de muchas regiones que amplían sus infraestructuras y tecnologías a medida que crecen sus economías, la ciberseguridad no suelen ser una prioridad, lo que da lugar a muchas vulnerabilidades relacionadas con la seguridad de infraestructuras críticas.

Inflación mundial y sus repercusiones económicas y políticas: este trimestre incluyó volatilidad de los mercados, crisis financieras y políticas, y presiones sobre las prioridades de gasto y los presupuestos de ciberseguridad.

Interrupciones continuas en la cadena de suministro tras la crisis: las nuevas vías de comercialización entre regiones exigieron cambios en los partners, las redes de transporte, el intercambio de información y, por extensión, los ciberriesgos. Dado que las ciberamenazas afectan diariamente a la cadena de suministro, la necesidad de contar con capacidades de confianza cero (Zero-Trust) sigue siendo fuerte en todos los sectores.

El mito del entorno de seguridad superior de Apple: esto persiste a pesar del hecho de que los entornos macOS ya no pueden considerarse seguros a medida que los actores de amenazas comienzan a aprovechar el malware basado en Golang a gran escala y amplían los vectores de ataque para cubrir numerosos sistemas operativos.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

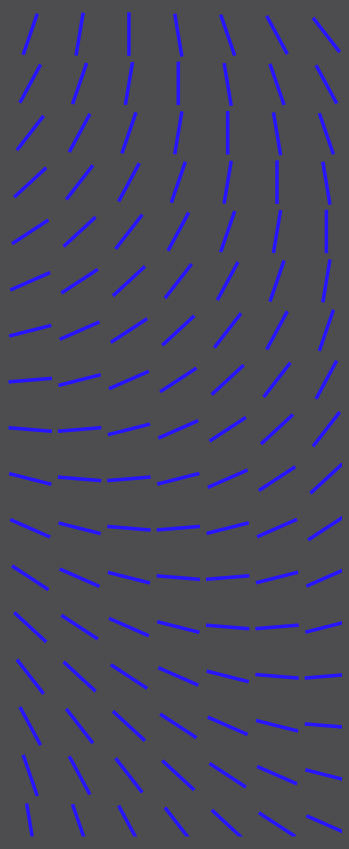
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



La inteligencia artificial llega al escenario mundial, prometiendo trastornos: la ciberdefensa se ve favorecida y perjudicada por la mejora del aprendizaje automático, el procesamiento del lenguaje natural y otros avances. A medida que las ciberamenazas globales evolucionan y se producen a una escala mucho más rápida de lo que los equipos humanos pueden gestionar, las soluciones de inteligencia artificial se convierten en vitales para la ciberdefensa empresarial.

Ciberseguridad: retos de los CISO y la revolución de los SecOps

¿Cuál es uno de los retos más importantes para los profesionales de la ciberseguridad y los equipos de SecOps? Digerir la información sobre amenazas –a gran velocidad y a gran escala– y proporcionar información práctica de inmediato a los equipos de caza de amenazas y a los grupos de trabajo de todas las organizaciones.

¿El objetivo de Trellix? Simplificar ese proceso.

¿Cómo? Proporcionando el nivel de automatización necesario para llegar a las respuestas en las que las organizaciones necesitan centrarse, utilizando nuestras capacidades superiores de inteligencia sobre amenazas, caza de amenazas y operaciones de seguridad integradas en nuestros productos XDR, de protección de host, de red y de correo.

El entorno de amenazas del primer trimestre de este año también se vio influido por factores internos, muchos de los cuales reflejan las continuas adversidades a las que se enfrentan los responsables de la ciberseguridad y los equipos de primera línea.

Tecnología obsoleta: Muchas organizaciones siguen confiando en tecnología antigua como SOAR y SIEM. De hecho, el 96 % de los CISO afirman que necesitan mejores soluciones para proteger a su entidad de las ciberamenazas[3].

Mar de herramientas de seguridad: los equipos de SecOps están inundados de alertas y carecen de lo necesario para priorizar su tiempo. De media, las organizaciones emplean una confusa variedad de 25 soluciones y herramientas de seguridad[4].

Fatiga de alertas: inundados de alertas, los equipos de SecOps luchan con la priorización, los falsos positivos y las alertas perdidas. Según IDC, el 35 % ignora las alertas, quizás, en parte, porque el 45 % son falsos positivos[5].

Recursos insuficientes: con recursos y experiencia limitados en operaciones de seguridad, es difícil contrarrestar las amenazas con eficacia. ¿Cuál es la antigüedad media de un analista SOC? Aproximadamente dos años[6].

Metodología: cómo recopilamos y analizamos los datos

Los expertos de talla mundial de nuestro Advanced Research Center recopilan las estadísticas, tendencias y datos que componen este informe a partir de una amplia gama de fuentes globales, tanto cautivas como abiertas. Los datos agregados se introducen en nuestras plataformas Insights y ATLAS. Aprovechando el aprendizaje automático, la automatización y la agudeza humana, el equipo realiza un ciclo a través de un conjunto de procesos intensivos, integrados e iterativos, normalizando los datos, analizando la información y desarrollando ideas importantes para los líderes de la ciberseguridad y los equipos SecOps en primera línea de la ciberseguridad en todo el mundo. Para obtener una descripción más detallada de nuestra metodología, consulte el final de este informe.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

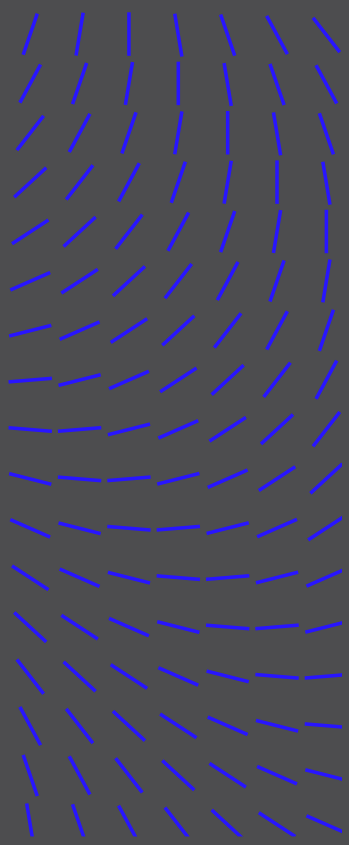
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



Aplicación: cómo utilizar esta información

Es imperativo que todo equipo de evaluación líder del sector comprenda, reconozca y, en la medida de lo posible, mitigue el efecto de la parcialidad: la inclinación natural, implícita o invisible a aceptar, rechazar o manipular los hechos y su significado. El mismo precepto es válido para los consumidores de contenidos.

A diferencia de una prueba o experimento matemático altamente estructurado y con base de control, este informe es intrínsecamente una muestra de conveniencia, un tipo de estudio no probabilístico que se utiliza a menudo en pruebas médicas, sanitarias, psicológicas y sociológicas y que hace uso de datos disponibles y accesibles.

En resumen, nuestras conclusiones se basan en lo que podemos observar y, evidentemente, no incluyen pruebas de amenazas, ataques o tácticas que hayan eludido la detección, la notificación y la recopilación de datos.

A falta de una información "completa" o una visibilidad "perfecta", este es el tipo de estudio que mejor se adapta al objetivo de este informe: identificar las fuentes conocidas de datos críticos sobre amenazas a la ciberseguridad y desarrollar interpretaciones racionales, expertas y éticas de estos datos que informen y permitan las mejores prácticas en ciberdefensa.

Un aspecto central de esta ética de investigación es el siguiente:

Una instantánea en el tiempo: nadie tiene acceso a todos los registros de todos los sistemas conectados a Internet, no se denuncian todos los incidentes de seguridad y no todas las víctimas sufren extorsión ni son incluidas en sitios de filtraciones. Sin embargo, rastrear lo que se puede permite comprender mejor las distintas amenazas, al tiempo que se reducen los puntos ciegos analíticos y de investigación.

Falsos positivos y falsos negativos: entre las características técnicas de alto rendimiento de los sistemas especiales de rastreo y telemetría de Trellix para recopilar datos se encuentran mecanismos, filtros y tácticas que ayudan a contrarrestar o eliminar los resultados de falsos positivos y negativos. Estos ayudan a elevar el nivel de análisis y la calidad de nuestros hallazgos.

Detecciones, no infecciones: cuando hablamos de telemetría, hablamos de detecciones, no de infecciones. Una detección se registra cuando uno de nuestros productos descubre un archivo, URL, dirección IP u otro indicador y nos informa al respecto.

Captura irregular de datos: algunos conjuntos de datos requieren una interpretación cuidadosa. Los datos de telecomunicaciones, por ejemplo, incluyen telemetría de clientes ISP que operan en muchas otras industrias y sectores.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

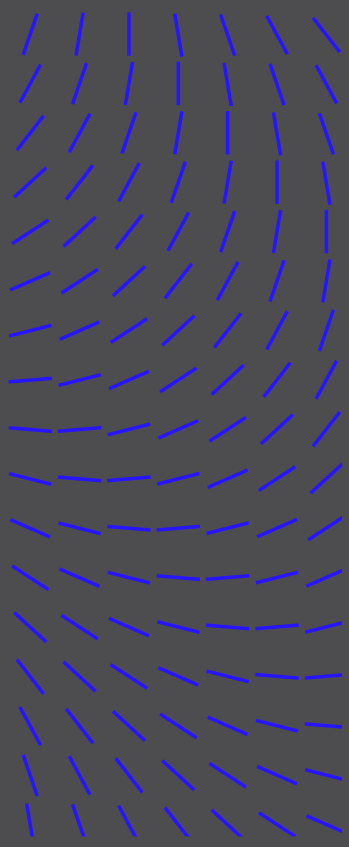
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



Atribución a Estados: del mismo modo, determinar la responsabilidad de un Estado en varios ciberataques y amenazas puede ser muy difícil, dada la práctica común entre los hackers y ciberdelincuentes vinculados con Estados de suplantarse unos a otros, o disfrazar la actividad maliciosa como si procediera de una fuente de confianza.

El camino por recorrer: orientación y recursos

¿Qué significa la información contenida en este informe para los héroes de la ciberseguridad en primera línea? La información y los datos sobre ciberseguridad solo son útiles si se transforman en acción y se traducen en un menor riesgo, una mejor toma de decisiones o actividades de operaciones de seguridad más eficaces o rentables. Para obtener más información y recursos, visite www.trellix.com.

[3] Trellix, "2023 Report: The Mind of the CISO", 2023
[4] Trellix, "2023 Report: The Mind of the CISO", 2023
[5] The Voice of the Analysts, IDC, 2021
[6] Ponemon Institute, 2020

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

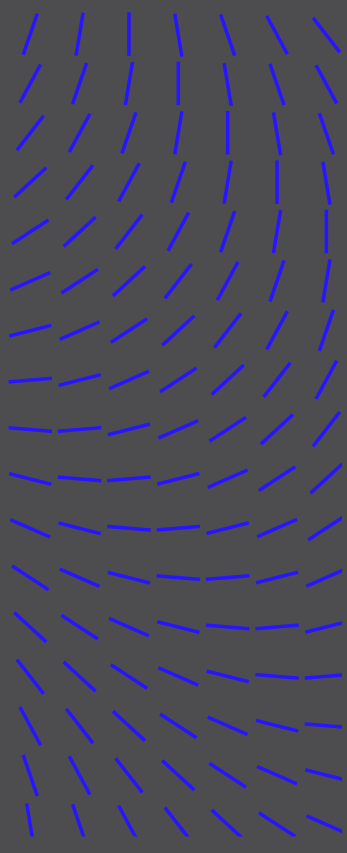
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

El panorama de ransomware

- **La ola ransomware:** el ransomware sigue siendo el principal tipo de ciberataque en todo el mundo. Las tácticas de ingeniería social para engañar y manipular a las personas para que divulguen información confidencial o personal, como el phishing, son más frecuentes que nunca, incluso a medida que se vuelven más sofisticadas.
- **Dominio de Cuba y Play:** aunque observamos un descenso de la actividad ciberdelictiva relacionada con los rescates a principios de año, las familias de ransomware más frecuentes en el primer trimestre fueron Cuba (9 %) y Play (7 %).
- **LockBit persiste:** a pesar de haber reducido su actividad dos trimestres seguidos, LockBit sigue siendo el ransomware más agresivo a la hora de presionar a sus víctimas para que cumplan las peticiones de rescate.
- **Magecart Group, ¿en alza?** Los informes públicos indican que la actividad de este grupo de robo de tarjetas de crédito y reventa de comercio electrónico aumentó enormemente en el primer trimestre de 2023. Esta amenaza rara vez opera a la misma escala de actividad que otras grandes APT afiliadas a Estados, lo que podría indicar una reaparición el Magecart Group en todo el mundo.

Evolución de las tácticas del ransomware

- **Objetivos económicos:** no sorprende que las motivaciones del ransomware sigan siendo principalmente financieras; los sectores de seguros (20 %) y servicios financieros (17 %) registraron el mayor número de detecciones de posibles ataques.
- **Las medianas empresas, las más afectadas:** la evaluación de los datos de nuestros sitios de filtraciones revela que las víctimas de estos ataques suelen ser empresas medianas con solo entre 51 y 200 empleados (32 %) y unos ingresos de entre 10 y 50 millones de dólares (38 %).
- **Estados Unidos como principal objetivo:** Estados Unidos (15 %) fue el país más afectado por los grupos de ransomware. También fue el país con el mayor porcentaje de víctimas corporativas (48 %) que decidieron "recomprar sus datos" a los atacantes, una tasa seis veces mayor que la siguiente nación de la lista, el Reino Unido.
- **Cobalt Strike como arma favorita:** la telemetría de Trellix identifica esta herramienta como una de las favoritas de los autores de ransomware (28 % de los incidentes). Su popularidad y uso parecen estar creciendo entre estos grupos, a pesar de los intentos del proveedor Fortra a finales del cuarto trimestre de 2022 de dificultar su uso a los ciberdelincuentes.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

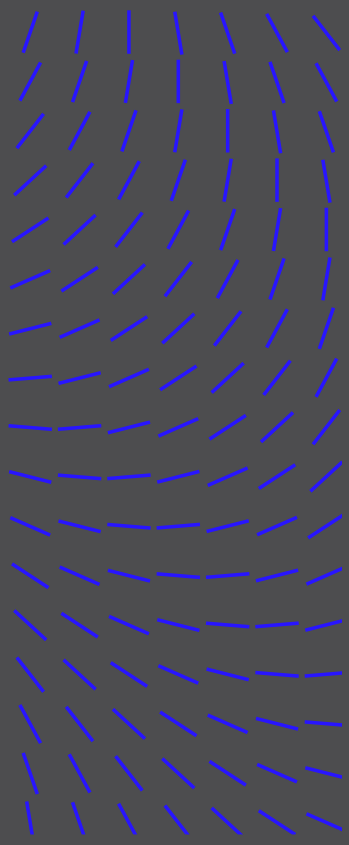
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



Señales de alerta de los Estados

- **Ciberdelincuentes más relevantes:** en los últimos seis meses, las APT vinculadas a China, como Mustang Panda y UNC4191, fueron las más activas en sus ataques contra Estados en el primer trimestre. Los actores de amenazas vinculados a China dominaron la escena mundial, generando el 79,3 % de toda la actividad contra países, seguidas de los vinculados a Corea del Norte, Rusia e Irán.
- **Grupo de APT más activo:** Mustang Panda se mantuvo por tercer trimestre consecutivo como el grupo de APT más activo en todo el mundo (72 %), lo que denota los continuos y crecientes esfuerzos ciberdelictivos de China con fines de espionaje y alteración.

Información sobre vulnerabilidades

- **Falta de respuesta a las vulnerabilidades conocidas:** la mayoría de las vulnerabilidades más críticas de este trimestre consistían en vulnerabilidades conocidas aún no resueltas.
- **Noticias de ayer:** en el caso de una vulnerabilidad de Apple revelada en febrero de este año, el fallo tenía raíces tan lejanas como el exploit FORCEDENTRY, que fue utilizado por el NSO Group como parte de su spyware Pegasus revelado en 2021.

Seguridad del correo electrónico

- **Nuevas vías de ataque:** aunque Microsoft ha empezado a bloquear los adjuntos de macros para la plataforma Office, los actores de amenazas han adoptado rápidamente otros medios de infección para seguir atacando los dispositivos Windows, como el envenenamiento de SEO, OneNote y los adjuntos zip.
- **Marcas poco fiables:** además de los mensajes de correos electrónicos de phishing genéricos, los ciberdelincuentes utilizan cada vez más marcas y servicios legítimos, como los de PayPal, Google, DWeb e IPFS, para estafar a las víctimas y robar sus credenciales online.

Acceso no autorizado a la nube

- **Un cambio de táctica:** los ataques a la infraestructura en la nube siguen aumentando a medida que más y más empresas migran de una infraestructura in situ a opciones más asequibles y escalables de Amazon, Microsoft, Google y otros.
- **Cuentas válidas:** aunque los ataques más sofisticados con autenticación multifactor, proxies y ejecución de API están en ascenso, la técnica de ataque dominante sigue siendo a través de cuentas válidas, con más del doble de frecuencia que el segundo vector de ataque más utilizado. Esto pone de relieve que el riesgo de acceso fraudulento es real, ya que los ciberdelincuentes acceden y venden inicios de sesión de cuentas o sitios web legítimos para infiltrarse y realizar ataques.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

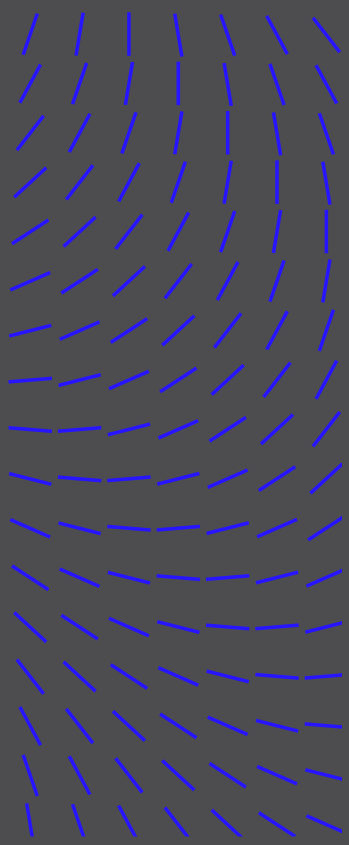
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

Incidentes de seguridad

Los incidentes de seguridad analizados en esta sección se basan en informes públicos. En el primer trimestre de 2023, los archivos binarios de Windows, las herramientas de terceros, el malware personalizado y las herramientas de pruebas de penetración siguieron afectando a las operaciones, ya que los actores de amenazas explotaron las vías de menor resistencia. Se siguió abusando de PowerShell y Windows Command Shell para generar tareas que conducen a la persistencia, el despliegue y la extracción.

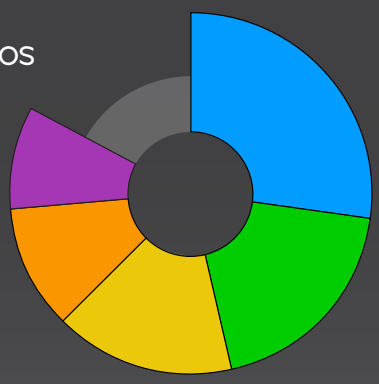
PRINCIPALES ARCHIVOS BINARIOS UTILIZADOS EN INCIDENTES DEL 1.ER TRIMESTRE DE 2023

1. PowerShell
2. Windows CMD
3. Tarea planificada
4. RunDLL32
5. WMIC

La programación de tareas, la inserción de archivos DLL maliciosos y los comandos ejecutados a través del instrumental de administración de Windows completaron los cinco primeros puestos. Tanto si se ejecutan mediante secuencias de comandos como si se introducen manualmente por teclado, los autores de las amenazas siguieron haciendo uso de los archivos binarios desprotegidos y no supervisados que ya tenían a su disposición.

En muchos casos, las herramientas de terceros, el software gratuito y las herramientas de pruebas de penetración desempeñan un papel en el ciclo de vida de un ataque, ayudando a los autores de amenazas a establecer la persistencia, ejecutar secuencias de comandos, descubrir y recopilar información específica y escalar privilegios para acceder a activos o datos que, de otro modo, serían inaccesibles para cuentas restringidas. Además, cuando se utiliza para la escalación de privilegios, un atacante puede ejecutar procesos de instalación con privilegios elevados y acceder a áreas, activos o datos que de otro modo serían inaccesibles para cuentas restringidas.

PRINCIPALES HERRAMIENTAS DE TERCEROS EN INFORMES PÚBLICOS EN EL 4.° TRIMESTRE DE 2023



INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

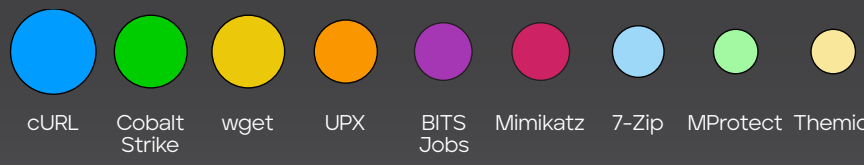
METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX

PRINCIPALES HERRAMIENTAS DE TERCEROS EN INFORMES PÚBLICOS EN EL 1.ER TRIMESTRE DE 2023

HERRAMIENTAS ESPECÍFICAS



Las herramientas de terceros más maliciosas, como Cobalt Strike, Mimikatz y Sharphound, son utilizadas tanto legítimamente como por los actores de amenazas para recopilar contraseñas, establecer balizas o elevar privilegios. Una vez que un atacante compromete un entorno, puede utilizar herramientas de transferencia de archivos como cURL para acceder a cargas útiles remotas, o Rclone para filtrar datos al almacenamiento en la nube.

En el primer trimestre de 2023, Magecart Group, APT29 y APT41 fueron los tres grupos de amenazas y APT más activos en atacar a usuarios por ubicación geográfica y sectores como métodos para recaudar valor monetario, descubrir secretos de estado o inhibir el uso de infraestructuras. Nos sorprendió descubrir que el Magecart Group encabezaba la lista, ya que rara vez opera a la escala de las otras grandes APT afiliadas a Estados. Vigilaremos la actividad de este grupo en los próximos meses para determinar si los datos de este periodo indican su reaparición en la escena mundial.

Las técnicas menos sofisticadas de "spray-and-pray" o envíos masivos de mensajes, diseñadas para atrapar a cualquiera que pudiera hacer clic o descargar, plagaron los sectores en campañas globales pasadas. Los ataques dirigidos han evolucionado en sofisticación, aumentando su persistencia contra los sectores industrial, financiero y sanitario. Aunque los dos sectores restantes, telecomunicaciones y energía, parecen haber sido atacados con menor frecuencia en los eventos globales, ambos son igualmente importantes y es posible que las organizaciones de estos no hayan informado de un incidente o sigan sin ser conscientes de su existencia.

PRINCIPALES ACTORES DE AMENAZAS ACTIVOS EN DENUNICAS PÚBLICAS EL 1.ER TRIMESTRE DE 2023

1.	Magecart Group	5 %
2.	APT29	4 %
3.	APT41	4 %
4.	Blind Eagle	4 %
5.	Gamaredon Group	4 %
6.	Lazarus	4 %
7.	Mustang Panda	4 %
8.	Sandworm Team	4 %

PRINCIPALES SECTORES ATACADOS EN DENUNICAS PÚBLICAS EL 1.ER TRIMESTRE DE 2023

1.	Fabricación	8 %
2.	Finanzas	7 %
3.	Atención sanitaria	6 %
4.	Telecomunicaciones	5 %
5.	Energía	5 %

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

INCIDENTES DE SEGURIDAD

RANSOMWARE

ACTIVIDAD RELACIONADA CON ESTADOS

INFORMACIÓN SOBRE VULNERABILIDADES

SEGURIDAD DEL CORREO ELECTRÓNICO

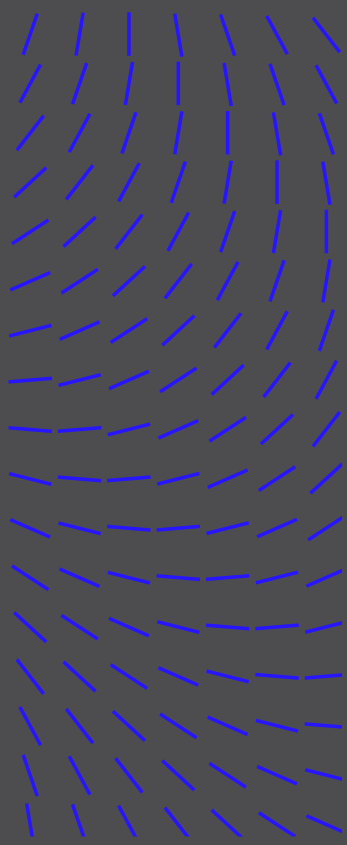
SEGURIDAD DE LA RED

INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



Los sucesos notificados analizados y examinados por nuestro equipo de investigación contienen abundante información, correlaciones o atribuciones de un actor de amenazas individual, un grupo de amenazas o una APT más sofisticada. Las herramientas, técnicas y procedimientos, junto con las familias de malware, incluyen programas maliciosos cargadores y descargadores, RAT, ladrones de información y ransomware. En los eventos del primer trimestre de 2023 analizados y disponibles a través de Insights, determinamos que Ucrania fue el objetivo más frecuente, seguida de cerca por Estados Unidos.

Las familias de ransomware Royal Ransom, Trigona y Maui fueron las más atacadas en el primer trimestre de 2023. Trellix publicó recientemente un análisis detallado de Royal Ransom y su funcionamiento interno con ejecutables de Windows y Linux. Aunque las estadísticas representadas surgieron específicamente de nuestra plataforma Insights, se produjeron muchos eventos adicionales en toda la infraestructura conectada globalmente, incluidos eventos conocidos notificados o mantenidos en privado y eventos que aún deben identificarse y corregirse.

PRINCIPALES PAÍSES ATACADOS EN DENUNICAS PÚBLICAS EL 1.ER TRIMESTRE DE 2023

7 %

En los incidentes públicos disponibles para el análisis, determinamos que Ucrania era el país más atacado por los actores de amenazas, seguido de cerca por Estados Unidos.

1.	Ucrania	7 %
2.	Estados Unidos	7 %
3.	Alemania	4 %
4.	Corea del Sur	3 %
5.	India	3 %

PRINCIPALES RANSOMWARE EN INCIDENTES PÚBLICOS EL 1.ER TRIMESTRE DE 2023

1.	Royal Ransom	7 %
2.	Trigona	4 %
3.	Maui	4 %
4.	Magniber	3 %
5.	LockBit	3 %

Ransomware

Las estadísticas que se muestran a continuación corresponden a las campañas, no a las detecciones en sí. Nuestra telemetría global reveló indicadores de peligro (IoC) pertenecientes a varias campañas de distintos grupos de ransomware.

Es bastante común ver un descenso de la actividad cibercriminal a principios de año, especialmente en enero. Esta tendencia podría explicar la notable disminución de la actividad tanto de Hive como de Cuba. Además, la interrupción de las actividades de Hive por parte del FBI y Europol a finales de enero habría interferido significativamente en sus operaciones. LockBit sigue siendo una de las principales familias de ransomware, especialmente agresiva y aparentemente exitosa a la hora de presionar a las víctimas para que paguen sus rescates.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX

PRINCIPALES RANSOMWARE UTILIZADOS EN INCIDENTES, 1.ER TRIMESTRE DE 2023

8 %

Cuba fue el grupo de ransomware más activo, seguido de Play y LockBit.

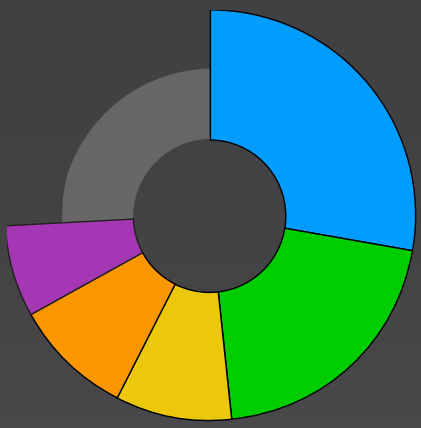
- Cuba
- Play
- LockBit 3.0
- Clop
- Hive

HERRAMIENTAS DE RANSOMWARE UTILIZADAS, 1.ER TRIMESTRE DE 2023

28 %

CobaltStrike se utilizó en casi un tercio de todos los incidentes de ransomware del trimestre, y su uso no ha hecho más que crecer a pesar de las recientes actualizaciones para dificultar el abuso de la herramienta por parte de los ciberdelincuentes.

- Cobalt Strike
- Mimikatz
- Empire
- BloodHound
- SystemBC



PAÍSES MÁS AFECTADOS POR GRUPOS DE RANSOMWARE, 1.ER TRIMESTRE DE 2023

15 %

Este trimestre, Estados Unidos sigue siendo el país más afectado por el ransomware, seguido de cerca por Turquía.

1.	Estados Unidos	15 %
2.	Turquía	14 %
3.	Portugal	10 %
4.	India	9 %
5.	Canadá	9 %

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX

SECTORES MÁS AFECTADOS POR GRUPOS DE RANSOMWARE, 1.ER TRIMESTRE DE 2023

1.	Seguros	20 %
2.	Servicios financieros	17 %
3.	Farmacia	7 %
4.	Telecomunicaciones	4 %
5.	Externalización y alojamiento	4 %

Los grupos de ransomware extorsionan a las víctimas publicando su información en sitios web conocidos como "sitios de filtración", utilizando la exposición para impulsar negociaciones estancadas con las víctimas o cuando se rechaza el pago del rescate. Nuestros expertos de Trellix utilizan RansomLook, una herramienta de código abierto, para recopilar datos de las publicaciones y, a continuación, normalizar y enriquecer los resultados para proporcionar un análisis anónimo de la victimología.

Es importante destacar que no todas las víctimas de ransomware aparecen en los sitios de filtraciones correspondientes. Muchas pagan el rescate y su información no se divulga. Las métricas que figuran a continuación son un indicador de los grupos de víctimas de ransomware a los que se dirige la extorsión o las represalias, y no deben confundirse con el número total de víctimas.

GRUPOS DE RANSOMWARE CON MÁS VÍCTIMAS SEGÚN SUS SITIOS DE FILTRACIONES, 1.ER TRIMESTRE DE 2023

1.	LockBit	30 %
2.	Hive	22 %
3.	Clop	12 %
4.	Royal Ransom	7 %
5.	ALPHV	5 %

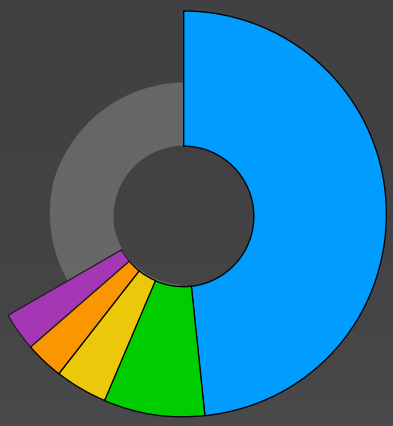
SECTORES MÁS AFECTADOS POR GRUPOS DE RANSOMWARE SEGÚN SUS SITIOS DE FILTRACIONES, 1.ER TRIMESTRE DE 2023

1.	Bienes y servicios industriales	25 %
2.	Comercio minorista	14 %
3.	Tecnología	11 %
4.	Atención sanitaria	8 %
5.	Servicios financieros	6 %

PRINCIPALES PAÍSES DE EMPRESAS INCLUIDAS EN SITIOS DE FILTRACIONES DE RANSOMWARE, 1.ER TRIMESTRE DE 2023

48 %

de las empresas víctimas que aparecen en los sitios de filtraciones de los grupos de ransomware tenían su sede en Estados Unidos.



- Estados Unidos
- Reino Unido
- Alemania
- Canadá
- India

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

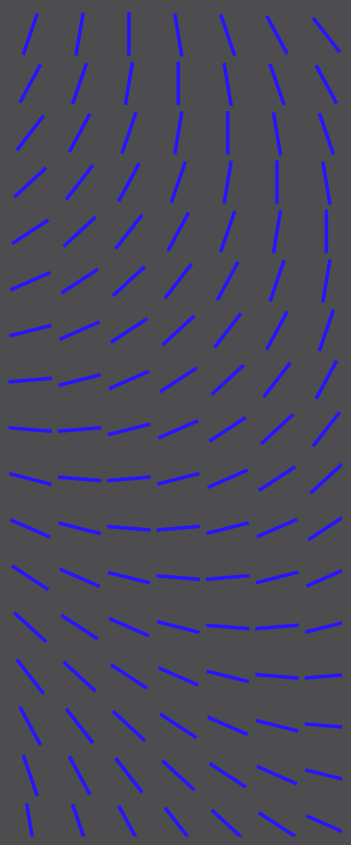
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



TAMAÑO DE EMPRESAS INCLUIDAS EN SITIOS DE FILTRACIONES DE RANSOMWARE, 1.ER TRIMESTRE DE 2023

RANGO DE EMPLEADOS		INGRESOS ANUALES	
1.	51- 200 (32 %)	1.	10-50 M$ (38 %)
2.	1001- 5000 (22 %)	2.	1000-10 000 M$ (23 %)
3.	11- 50 (15 %)	3.	1-10 M$ (21 %)
4.	201- 500 (15 %)	4.	100- 250 M$ (11 %)
5.	501- 1000 (15 %)	5.	500-1000 M$ (7 %)

Actividad relacionada con Estados

La información sobre la actividad de los grupos afiliados por Estados recopilada de múltiples fuentes crea una mejor imagen del panorama de las amenazas y ayuda a reducir el sesgo de observación. En primer lugar, representamos los datos extraídos al correlacionar los indicadores de peligro de grupos relacionados con Estados con telemetría de clientes de Trellix. En segundo lugar, aportamos datos de los distintos informes publicados por el sector de la seguridad previamente filtrados, analizados y depurados por el grupo de inteligencia de amenazas.

Como se ha indicado anteriormente, estas estadísticas que se muestran a continuación corresponden a las campañas, no a las detecciones en sí. Debido a que se agregan varios tipos de registros, al uso que hacen nuestros clientes de las estrategias de simulación de amenazas y al elevado nivel de correlaciones con la base de conocimientos de inteligencia de amenazas, los datos se filtran manualmente para cumplir nuestros objetivos de análisis.

Seguimos observando que los actores de amenazas afiliados a China dominan el panorama mundial, en particular con Mustang Panda como responsable de una mayoría significativa de las detecciones en el primer trimestre de 2023. Dado que dependen en gran medida de la carga local y otras técnicas de ocultación, es posible que los grupos de APT afiliados a China roten sus herramientas de malware con menos frecuencia que otros actores de amenazas. De ser así, esta práctica podría provocar un "sesgo de proyección" o una estimación inflada de las detecciones de hashes afiliados a China.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

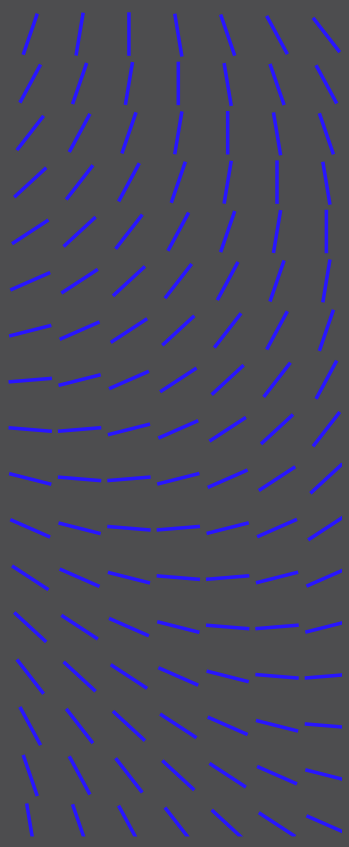
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX

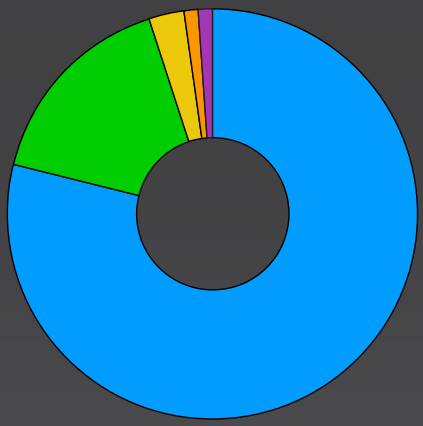


PAÍSES MÁS PREVALENTES EN CUANTO A CIBERACTIVIDAD AUSPICIADA POR ESTADOS, 1.ER TRIMESTRE DE 2023

79 %

China representó una mayoría dominante de la ciberactividad auspiciada por Estados en el 1.er trimestre de 2023.

- China
- Corea del Norte
- Rusia
- Irán
- Pakistán



GRUPOS DE CIBERATACANTES MÁS PREVALENTES, 1.ER TRIMESTRE DE 2023

1.	Mustang Panda	72 %
2.	Lazarus	17 %
3.	UNC4191	1 %
4.	Common Raven	1 %
5.	APT34	1 %

TÉCNICAS MITRE ATT&CK MÁS PREVALENTES EMPLEADAS EN ACTIVIDAD RELACIONADA CON ESTADOS, 1.ER TRIMESTRE DE 2023

1.	Carga lateral de LDLL	14 %
2.	Anulación de ocultación/ descodificación de archivos para información	11 %
3.	Transferencia de herramientas a la entrada	10 %
4.	Datos del sistema local	10 %
5.	Descubrimiento de archivos y directorios	10 %

HERRAMIENTAS MALICIOSAS MÁS PREVALENTES EMPLEADAS EN ACTIVIDAD RELACIONADA CON ESTADOS, 1.ER TRIMESTRE DE 2023

38 %

PlugX fue responsable del 38 % de la ciberactividad auspiciada por Estados, 1.er trimestre de 2023.

1.	PlugX	38 %
2.	Cobalt Strike	35 %
3.	Raspberry Robin	14 %
4.	BLUEHAZE/DARKDEW MISTCLOAK	3 %
5.	Mimikatz	3 %

India es uno de los principales países de Asia y regiones vecinas con programas cibernéticos capaces. Algunos grupos, predominantemente actores de amenazas vinculados a China, han demostrado un gran interés por los avances tecnológicos, militares y políticos de la India. Un número notable de detecciones en la India puede atribuirse a Mustang Panda.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

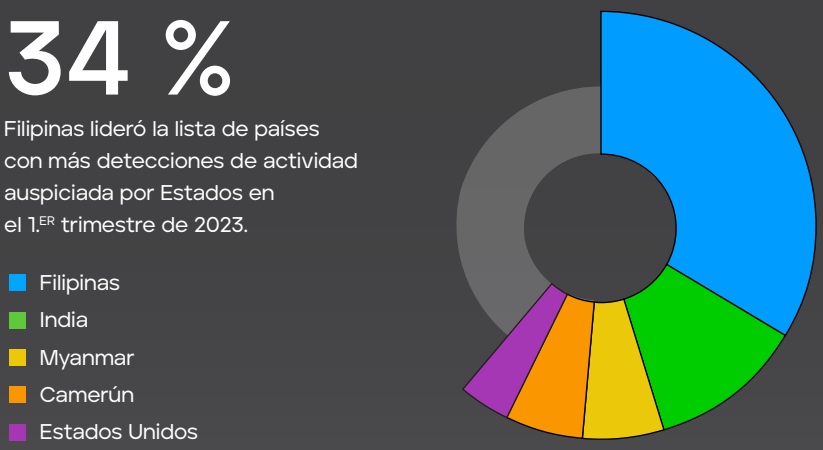
RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX

PAÍSES CON MÁS DETECCIONES DE ACTIVIDAD AUSPICIADA POR ESTADOS, 1.ER TRIMESTRE

34 %

Filipinas lideró la lista de países con más detecciones de actividad auspiciada por Estados en el 1.ER trimestre de 2023.



SECTORES CON MÁS DETECCIONES DE ACTIVIDAD AUSPICIADA POR ESTADOS, 1.ER TRIMESTRE

Información sobre vulnerabilidades

Los expertos en ingeniería inversa y análisis de vulnerabilidades del Trellix Advanced Research Center supervisan continuamente las vulnerabilidades más recientes con el fin de orientar a los clientes sobre cómo las están aprovechando los actores de amenazas y cómo mitigar la probabilidad y el impacto de estos ataques.

Uno de nuestros hallazgos más críticos, aunque no sorprendentes, para el primer trimestre de 2023 es que muchas de las vulnerabilidades más críticas de este periodo consistían en eludir parches para CVE antiguas, fallos en la cadena de suministro resultantes de la utilización de bibliotecas obsoletas o vulnerabilidades corregidas hace tiempo que persisten mucho más allá de sus esperados cinco minutos de fama.

Consideremos CVE-2022-47966 por ejemplo, una vulnerabilidad crítica (9,8) en los productos ManageEngine de Zoho que hizo las rondas este enero. ManageEngine lo utilizan miles de empresas en todo el mundo, por lo que no nos sorprendió cuando se detectó en circulación la explotación de esta vulnerabilidad. Lo que nos asombró fue la causa raíz: la utilización de Apache Santuario 1.4.1 -una versión casi lo suficientemente antigua como para votar- que contenía un problema conocido que permitía la inyección de XML.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX

Zoho corrigió la vulnerabilidad en toda su gama de productos en octubre y luego, casi tres meses más tarde, en el primer trimestre, CISA publicó un aviso advirtiendo de la explotación de la vulnerabilidad e instando a los proveedores a aplicar el parche correspondiente.

Otro ejemplo es CVE-2022-44877, una vulnerabilidad crítica en Control Web Panel (CWP). Aunque no está directamente relacionada, esta vulnerabilidad tiene muchas de las características de nuestro ejemplo anterior: es otra vulnerabilidad de ejecución remota de código de 9,8 que vio una explotación activa generalizada en enero a pesar de haber sido corregida en octubre. La causa raíz tampoco era exactamente digna de una charla en Black Hat: inyección de comandos usando expansión de variables shell estándar en un parámetro URL.

Un tercer ejemplo es CVE-2021-21974, una vulnerabilidad en el servicio OpenSLP de VMware ESXi corregida en febrero de 2021, casi exactamente dos años antes de su repentino resurgimiento debido a una explotación en entornos reales. Cuando informamos sobre esta vulnerabilidad en nuestro Informe de errores de febrero, observamos que alrededor de 48 000 servidores accesibles a través de Internet seguían ejecutando versiones vulnerables de ESXi según Shodan. Hoy, esa cifra sigue siendo superior a 38 000, lo que supone un cambio de menos del 22 %.

Fecha	Número de servidores ESXI vulnerables según Shodan
Finales de febrero de 2023	48 471
Finales de abril de 2023	38 047

Encontramos algunos ejemplos propios cuando investigábamos los dispositivos de Apple a principios de este año: CVE-2023-23530 y CVE-2023-23531. Estas dos vulnerabilidades difieren de los ejemplos anteriores en que su impacto se limita a la elevación local de privilegios y no a la ejecución remota de código. Sin embargo, esta no es una razón para pasar por alto su importancia, ya que una vulnerabilidad muy similar fue aprovechada por el exploit FORCEDENTRY, que fue utilizado por el NSO Group para desplegar su spyware Pegasus en 2021. De hecho, las dos vulnerabilidades CVE que hemos descubierto utilizan el mismo componente primitivo que sirvió de base para el exploit FORCEDENTRY: una clase inocua llamada NSPredicate. Desafortunadamente, el enfoque de Apple para mitigar FORCEDENTRY implicó el uso de una extensa lista de denegación para apuntalar las formas en que NSPredicate estaba siendo abusado, una mitigación que no abordó el problema de fondo y nos permitió eludirlo.

Resulta tentador señalar este tipo de tendencias y concluir que los proveedores no se toman en serio la seguridad o lamentar la reaparición de antiguos exploits por parte de los actores de amenazas y los investigadores, pero esta no es la conclusión correcta. Los investigadores de vulnerabilidades se dedican al análisis de variantes porque un investigador de vulnerabilidades eficaz emula las prioridades de los actores de amenazas reales, y encontrar una forma de eludir la mitigación o una vulnerabilidad CVE antigua en

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

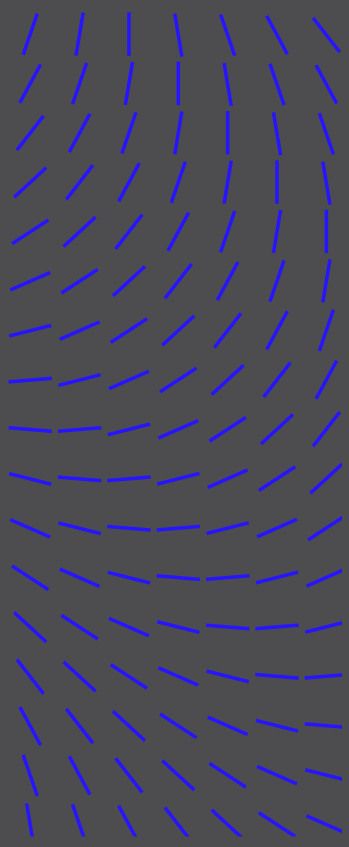
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



un producto rara vez parcheado produce sistemáticamente una mayor rentabilidad que reinventar la rueda. Para las organizaciones que reconocen legítimamente esta tendencia, la conclusión debería ser la siguiente: aunque las tecnologías punteras de detección de amenazas son insustituibles en el panorama moderno de las amenazas, se pueden obtener muchas victorias en los aspectos fundamentales, como los procesos de aplicación de parches y la investigación de la cadena de suministro.

Seguridad del correo electrónico

Las estadísticas de seguridad del correo electrónico se basan en la telemetría generada a partir de varios dispositivos de seguridad del correo electrónico desplegados en redes de clientes de todo el mundo.

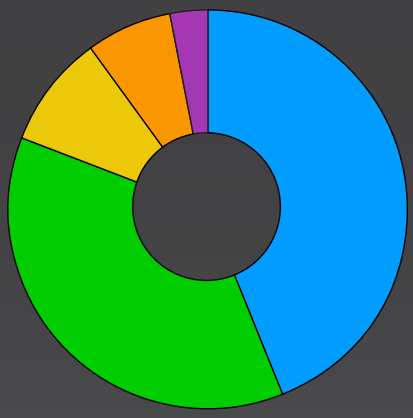
Los ataques de phishing que aprovechan marcas legítimas para estafar a los usuarios y robar sus credenciales van en aumento, con DWeb, IPFS y Google Translate muy utilizados en los ataques por correo electrónico. Los atacantes también hicieron uso ilegítimo del correo gratuito y otros servicios similares, como las dos aplicaciones PayPal Invoicing and Google Forms, para montar ataques de vishing y evitar ser detectados. Durante este periodo también se atacaron nuevas marcas como Scribd, LesMills y las tarjetas regalo de Google Play.

Además, en términos del malware específico utilizado para estos ataques, Formbook y Agent Tesla experimentaron notables aumentos en el primer trimestre de 2023, en comparación con finales del año pasado. Esto puede deberse al hecho de que ambos ejemplares de malware son más fáciles de adquirir y desplegar, en comparación con Remcos, Emotet y Qakbot.

TÁCTICAS DE MALWARE DE CORREO ELECTRÓNICO MÁS PREVALENTES, 1.ER TRIMESTRE DE 2023

44 %

Formbook representó casi la mitad del malware de correo electrónico en el primer trimestre, seguido de cerca por Agent Tesla.



- Formbook
- Agent Tesla
- Remcos
- Emotet
- Qakbot

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX

PAÍSES MÁS ATACADOS POR PHISHING DE CORREO ELECTRÓNICO, 1.ER TRIMESTRE DE 2023

30 %

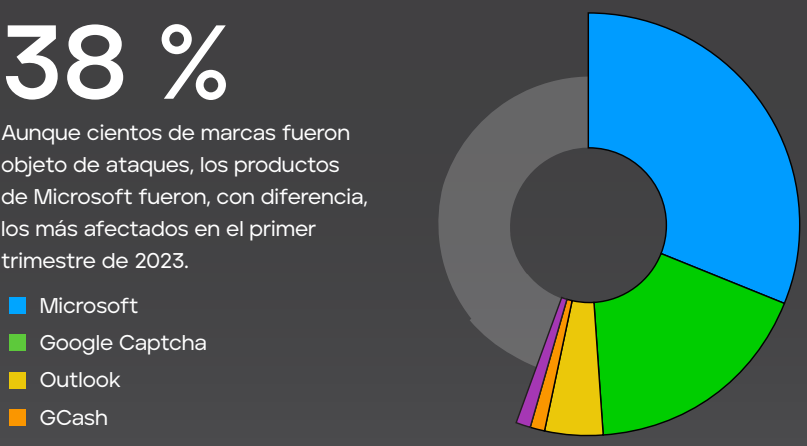
Estados Unidos y Corea fueron las principales víctimas de los intentos de phishing por correo electrónico en el primer trimestre, recibiendo casi dos tercios de todos los intentos de phishing a escala mundial.

1.	Estados Unidos	30 %
2.	Corea del Sur	29 %
3.	Taiwán	10 %
4.	Brasil	8 %
5.	Japón	7 %

PRODUCTOS Y MARCAS MÁS AFECTADAS POR PHISHING POR CORREO ELECTRÓNICO, 1.ER TRIMESTRE DE 2023

38 %

Aunque cientos de marcas fueron objeto de ataques, los productos de Microsoft fueron, con diferencia, los más afectados en el primer trimestre de 2023.



SECTORES MÁS AFECTADOS POR MENSAJES DE CORREO ELECTRÓNICO MALICIOSOS, 1.ER TRIMESTRE DE 2023

1.	Administración pública	11 %
2.	Servicios financieros	8 %
3.	Fabricación	6 %
4.	Tecnología	6 %
5.	Entretenimiento	5 %

PROVEEDORES DE ALOJAMIENTO WEB MÁS ABUSADOS, 1.ER TRIMESTRE DE 2023

1.	IPFS	41 %
2.	Google Translate	33 %
3.	Dweb	16 %
4.	AmazonAWS Appforest	3 %
5.	Firebase OWA	3 %

TÉCNICAS DE EVASIÓN MÁS UTILIZADAS EN ATAQUES DE PHISHING, 1.ER TRIMESTRE DE 2023

79 % La evasión basada en la redirección 302 fue la ténica de evasión más prevalente utilizada por los ataques de phishing en el 1.er trimestre de 2023.

46 % Los ataques basados en captcha aumentaron de manera importante en el 1.er trimestre respecto al 4.° trimestre de 2022.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX

Seguridad de redes

En el curso de la detección y el bloqueo de ataques basados en la red que amenazan a nuestros clientes, el equipo de investigación de redes del Advanced Research Center de Trellix inspecciona diferentes áreas de la cadena de ataque, desde el reconocimiento y el compromiso inicial hasta la comunicación de mando y control y las técnicas, tácticas y procedimientos de movimiento lateral.

TENDENCIAS DE DEVOLUCIÓN DE LLAMADAS DE MALWARE MÁS PREVALENTES, 1.ER TRIMESTRE DE 2023

La actividad del ransomware STOP ha disminuido un	94 %
El ransomware LockBit distribuido por Amadey ha aumentado un	25 %
La actividad de malware para Android ha aumentado un	12,5 %
La actividad de Ursnif ha aumentado un	10 %
La actividad de Smoke Loader se ha multiplicado por	7X
La actividad Amadey se ha multiplicado por	4X
La actividad de Cobalt Strike se ha multiplicado por	3X
Las actividad de Emotet se ha multiplicado por	2X

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

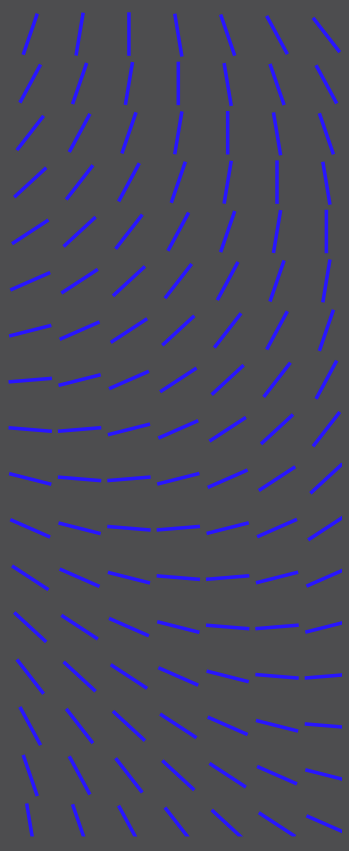
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

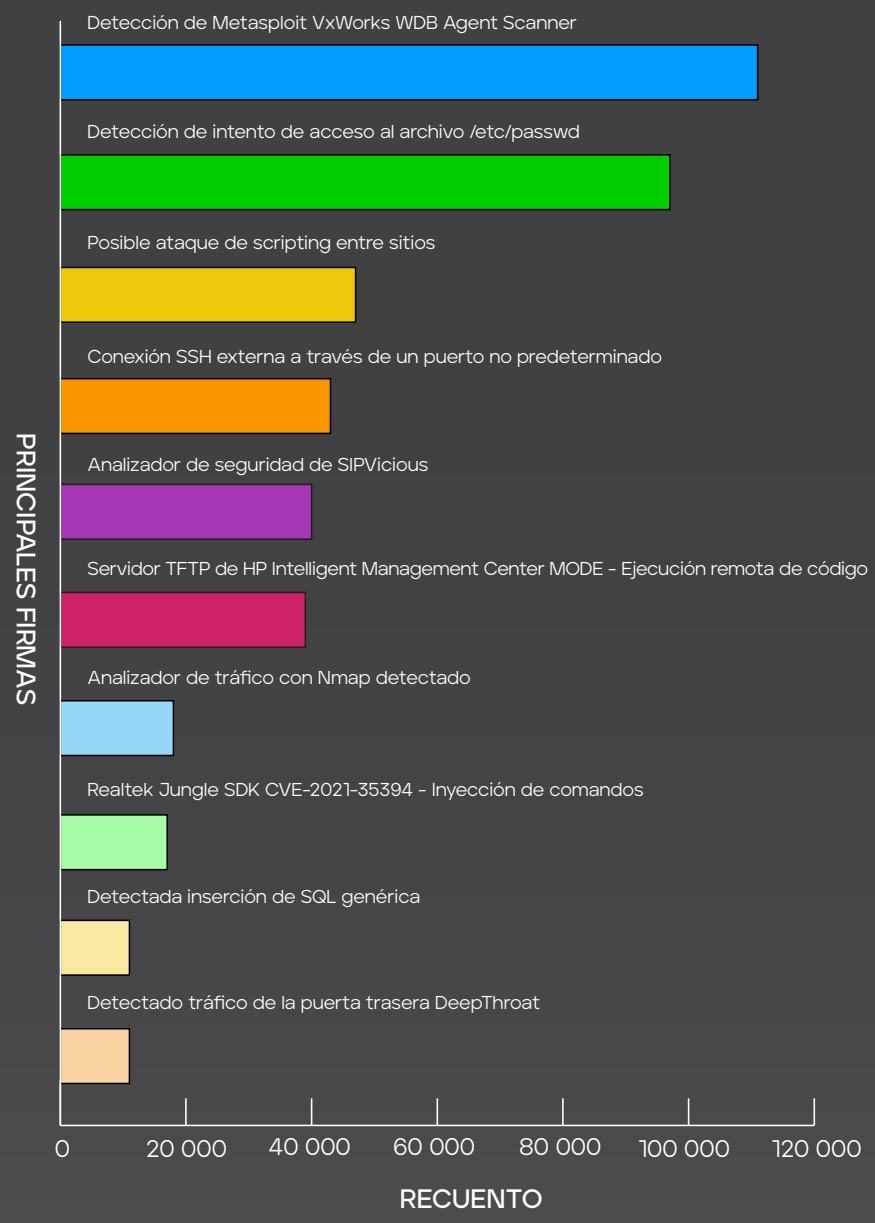
METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



ATAQUES DE MAYOR IMPACTO EN SERVICIOS EXTERNOS, 1.ER TRIMESTRE DE 2023



INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX

Incidentes en la nube

Siguen aumentando los ataques a infraestructuras en la nube contra servicios desarrollados y prestados por Amazon, Microsoft, Google y otros. La siguiente tabla describe los datos de telemetría de ataques basados en la nube por cliente y proveedor de nube.

DETECCIONES POR TÉCNICAS MITRE ATT&CK, 1.ER TRIMESTRE DE 2023

	AWS	Microsoft Azure	GCP
Cuentas válidas	3437	4312	997
Modificación de la infraestructura del servicio de proceso de la cuenta en la nube	4268	0	17
Puerto no estándar	115	0	17
Autenticación multifactor	190	1,534	22
Descubrimiento de servicios de red	141	93	0
Fuerza bruta	25	1869	22
Proxy	299	2744	135
Descubrimiento de cuentas	264	68	787
Regla de reenvío de correo electrónico	25	0	22
Ejecución a través de API	1143	0	252

METODOLOGÍA

Recopilación: los avezados expertos del Advanced Research Center recopilan las estadísticas, tendencias y datos que componen este informe a partir de una amplia gama de fuentes globales.

- **Fuentes cautivas:** en algunos casos, la telemetría la generan las soluciones de seguridad de Trellix en las redes de ciberseguridad de los clientes y los marcos de defensa desplegados en todo el mundo en redes tanto del sector público como del privado, incluidas las que prestan servicios de tecnología, infraestructuras o datos. Estos sistemas, que se cuentan por millones, generan datos procedentes de mil millones de sensores.
- **Fuentes abiertas:** En otros casos, Trellix aprovecha una combinación de herramientas patentadas, propias y de código abierto para rastrear sitios, registros y repositorios de datos en Internet, así como en la web oscura, como los "sitios de filtraciones" donde los actores maliciosos publican información sobre sus víctimas de ransomware o perteneciente a ellas.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

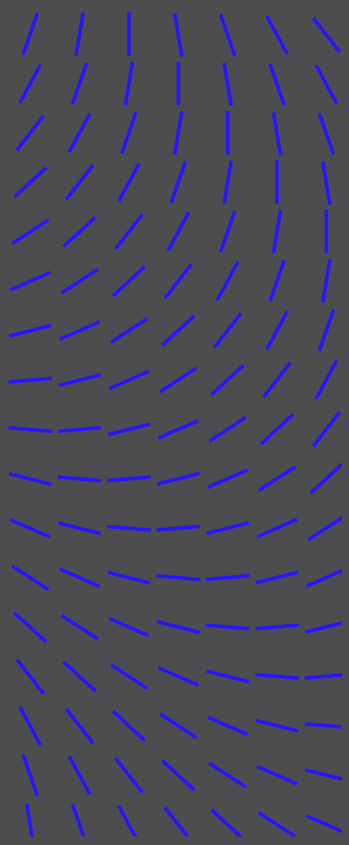
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



Normalización: los datos agregados se introducen en nuestras plataformas Insights y ATLAS. Aprovechando el aprendizaje automático, la automatización y la agudeza humana, el equipo realiza ciclos a través de un conjunto de procesos intensivos, integrados e iterativos: normalización de los datos, enriquecimiento de los resultados, eliminación de información personal e identificación de correlaciones entre métodos de ataque, agentes, sectores, regiones, estrategias y resultados.

Análisis: a continuación, Trellix analiza esta vasta reserva de información, en relación con (1) su amplia base de conocimientos de inteligencia sobre amenazas, (2) informes del sector de la ciberseguridad de fuentes muy respetadas y acreditadas, y (3) la experiencia y los conocimientos de los analistas de ciberseguridad, investigadores, especialistas en ingeniería inversa, investigadores forenses y expertos en vulnerabilidades de Trellix.

Interpretación: Por último, el equipo de Trellix extrae, revisa y valida información relevante que puede ayudar a los líderes de ciberseguridad y a los equipos de SecOps a (1) comprender las tendencias más recientes en el entorno de las ciberamenazas, y (2) utilizar esta perspectiva para mejorar su capacidad de anticipar, prevenir y defender a su organización de ciberataques en el futuro.

RECURSOS

Archivo de informes sobre amenazas

The Mind of the CISO

Trellix Advanced Research Center Discovers a New Privilege Escalation Bug Class on macOS and iOS

A Royal Analysis of Royal Ransom

Feeding Gophers to Ghidra

TWITTER

Trellix ARC

Ver archivo de informes sobre ciberamenazas

Trellix Advanced Research Center

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

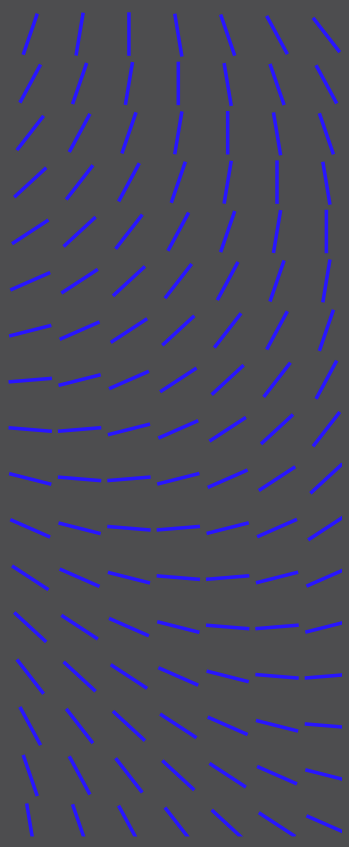
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



ACERCA DEL TRELLIX ADVANCED RESEARCH CENTER

Trellix Advanced Research Center posee la carta de ciberseguridad más completa del sector y está a la vanguardia de los métodos, tendencias y ciberdelincuentes emergentes en el panorama mundial de las amenazas y es partner ineludible de los equipos de operaciones de seguridad en todo el mundo. El Trellix Advanced Research Center ofrece inteligencia y contenido avanzado a los analistas de seguridad, mientras fomenta nuestra plataforma XDR. Además, el grupo de inteligencia de amenazas del Trellix Advanced Research Center ofrece productos y servicios de inteligencia sobre amenazas a clientes de todo el mundo.

ACERCA DE TRELLIX

Trellix es una empresa mundial que tiene como vocación redefinir el futuro de la ciberseguridad. Su plataforma de detección y respuesta ampliadas (eXtended Detection and Response, XDR), abierta y nativa, ayuda a organizaciones que se enfrentan a las amenazas más avanzadas en la actualidad a conseguir confianza en la protección y la resiliencia de sus operaciones. Trellix, junto con un nutrido ecosistema de partners, acelera las innovaciones tecnológicas gracias al aprendizaje automático y a la automatización, para reforzar la protección de más de 40 000 clientes de los sectores privado y público mediante una seguridad evolutiva.

INTRODUCCIÓN

LO MÁS DESTACADO DEL 1.ER TRIMESTRE DE 2023 DE UN VISTAZO

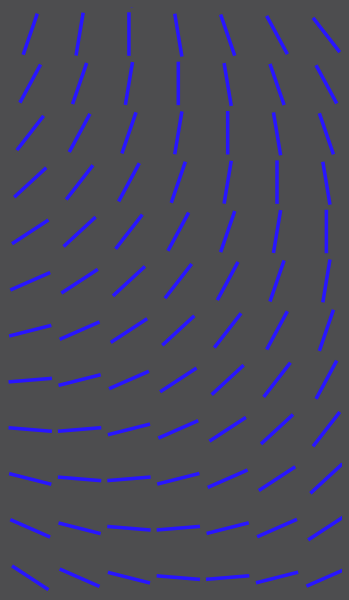
ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

- INCIDENTES DE SEGURIDAD
- RANSOMWARE
- ACTIVIDAD RELACIONADA CON ESTADOS
- INFORMACIÓN SOBRE VULNERABILIDADES
- SEGURIDAD DEL CORREO ELECTRÓNICO
- SEGURIDAD DE LA RED
- INCIDENTES EN LA NUBE

METODOLOGÍA

RECURSOS

ACERCA DE TRELLIX ADVANCED RESEARCH CENTER Y TRELLIX



Este documento y la información que contiene describen investigaciones en el campo de la seguridad informática, con fines informativos y para la conveniencia de los clientes de Trellix. Las investigaciones de Trellix se llevan a cabo de acuerdo con su Política de divulgación razonable de vulnerabilidades | Trellix. El riesgo por cualquier intento de recrear una parte o la totalidad de las actividades descritas será asumido exclusivamente por el usuario, y ni Trellix ni ninguna de sus empresas filiales asumirá responsabilidad alguna.

Trellix es una marca comercial registrada o marca registrada de Musarubra US LLC o sus empresas filiales en EE. UU. y otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros.

Para obtener más información, visite Trellix.com.

Trellix

Acerca de Trellix

Trellix es una empresa mundial que redefine el futuro de la ciberseguridad. Su plataforma de detección y respuesta ampliadas (eXtended Detection and Response, XDR), abierta y nativa, ayuda a organizaciones que se enfrentan a las amenazas más avanzadas en la actualidad a conseguir confianza en la protección y la resiliencia de sus operaciones. Los expertos en seguridad de Trellix, junto con un nutrido ecosistema de partners, aceleran las innovaciones tecnológicas mediante el aprendizaje automático y la automatización, para proteger a más de 40 000 clientes del sector privado y público.

Copyright © 2023 Musarubra US LLC

072022-05