EL INFORME DE CIBERAMENAZAS

Junio de 2024

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

CONTENIDO:

Presentado por

Trellix ADVANCED RESEARCH CENTER

Una herramienta de evasión de EDR ha conseguido recientemente anular las funciones de detección y respuesta para endpoints en otra organización de su sector.

La carrera que libra la ciberseguridad para adelantarse a los atacantes y evitar que usen las herramientas de seguridad legítimas para fines malintencionados se está complicando.

Como CISO, tiene que actuar de manera ágil y veloz. Su CEO y su consejo de administración quieren saber más sobre sus herramientas de registro y alertas. Su equipo tiene asignada la tarea de identificar las brechas de seguridad y cuenta con un plan para solucionarlas.

La carrera de la ciberseguridad es un verdadero triatlón: compite en las áreas de operaciones de seguridad, tecnología e inteligencia. La carrera ha comenzado y es una prueba de resistencia.

> Los mecanismos de defensa son cada vez más sofisticados, pero también evolucionan las herramientas y tácticas de ataque de actores auspiciados por Estados y de ciberdelincuentes.

EL INFORME DE CIBERAMENAZAS

Elaborado por el Advanced Research Center de Trellix, este informe (1) destaca ideas, inteligencia y recomendaciones obtenidas de múltiples fuentes de datos críticos sobre amenazas de 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 las observaciones y los datos recogidos entre el 1 de octubre de 2023 y el 31 de marzo de 2024.

1. Cambios rápidos y significativos en el panorama de las APT
2. LockBit agita el ecosistema del ransomware
3. Aparición de los anuladores de EDR
4. Fraudes sobre el tema de las elecciones presidenciales en EE. UU.
5. La IA generativa y el submundo de la ciberdelincuencia

PRESENTACIÓN

Para los CISO, ahora es más importante que nunca contar con inteligencia sobre amenazas operativa y capacidad para añadir contexto del entorno de las amenazas globales.

Ante la necesidad de hacer más con menos, los CISO y sus equipos de SecOps necesitan inteligencia sobre amenazas para poder anticiparse, identificar y prepararse para los ataques más relevantes contra su organización, adaptar los programas y el presupuesto para actuar contra las amenazas y los atacantes más probables y, en definitiva, pasar de una estrategia reactiva a un enfoque proactivo.

Como "cliente cero" de Trellix, creo que la inteligencia nunca ha tenido más potencial para determinar la respuesta y la estrategia de los responsables.

Aquí tiene este contenido, analícelo y póngalo en práctica para la planificación estratégica, racionalización del presupuesto, concienciación del consejo de administración y soporte de las operaciones. Espero que esta información le sea realmente útil y le permita orientar adecuadamente su planificación, preparación y defensa contra las APT.

Harold Rivas
CISO, TRELLIX

ÍNDICE

PREFACIO

En este documento, como en todos nuestros informes, nuestro objetivo es proporcionar una base de inteligencia y contexto sobre lo que estamos observando.

El panorama

Los seis últimos meses no tienen precedentes; continúa el estado de policrisis y se ha acelerado la actividad de los ciberdelincuentes y actores de amenazas. Asistimos a cambios radicales en el comportamiento:

- Los operativos de las fuerzas de seguridad han dejado un ecosistema del ransomware atípico.
- Algunos grupos autónomos venden a las bandas de ransomware sus pruebas de penetración y métodos de ataque alternativos.
- La guerra en Israel ha desencadenado ataques directos financiados por Estados y hacktivismo.
- Los atacantes intentan ser más sofisticados y tienen acceso a herramientas de IA generativa baratas y de libre acceso con las que pueden convertirse en expertos de la noche a la mañana.
- Las herramientas de evasión y anulación de EDR cobran mayor importancia entre los atacantes.

Un juego del ratón y el gato

Con la implementación a mayor escala de soluciones de detección y respuesta para endpoints (EDR), el juego del ratón y el gato en ciberseguridad se complica. Nos ha llamado la atención que cada vez más actores de amenazas emplean herramientas delictivas para neutralizar las soluciones EDR. Esto representa un cambio de rumbo radical respecto al uso de herramientas tradicionales basadas en malware.

Y, como responsables de la defensa, nosotros también tenemos que cambiar la estrategia. Las soluciones EDR han demostrado su eficacia en la detección de malware, ransomware y actividades APT, pero si se desactivaran, ¿cómo deberían reaccionar las empresas y sus CISO? El CISO necesita registrar datos, crear alertas y usar inteligencia sobre amenazas operativa para disponer de visibilidad de los comportamientos no habituales en su sistema. Hace falta subir el nivel del juego.

Nosotros trabajamos con diligencia para compartir la inteligencia sobre amenazas con la comunidad -uno de nuestros valores fundamentales para adelantarnos al adversario- y realizar un seguimiento de las campañas y los grupos de amenazas a gran escala.

El panorama está más convulso que nunca. Nuestro objetivo es ayudar a nuestros clientes y al sector en su conjunto con la inteligencia necesaria para intensificar las defensas, crear contramedidas e identificar las lagunas de seguridad.

En este juego del ratón y el gato, para ganar, tenemos que actuar.

John Fokker
DIRECTOR DE INTELIGENCIA DE AMENAZAS DE TRELLIX

ÍNDICE

INTRODUCCIÓN: EL INFORME DE CIBERAMENAZAS: JUNIO DE 2024

Impacto de los eventos geopolíticos en el dominio cibernético

Las investigaciones realizadas por el Trellix Advanced Research Center sobre la actividad desde el 1 de octubre de 2023 hasta el 31 de marzo de 2024 revelan un cambio en la actividad ciberdelictiva, con un evidente incremento de las operaciones de ciberamenazas con motivaciones geopolíticas. En particular, determinados acontecimientos importantes de ámbito regional o internacional, como ejercicios militares, cumbres políticas o económicas, convenciones políticas y elecciones, han contribuido a este incremento.

Los analistas de Trellix han concluido, con un cierto nivel de certeza, que los ciberdelincuentes se centran en estos acontecimientos para recopilar inteligencia relevante sobre otros atacantes, sondear proactivamente las redes para obtener información que les permita conocer la situación o ganar posiciones estratégicas en las redes de TI para futuros ataques.

- **Los presidentes Joe Biden y Xi Jinping se reúnen en San Francisco:** en noviembre de 2023, los datos de detecciones por telemetría de Trellix señalaron un incremento de la actividad maliciosa por parte de grupos de APT asociados China solo unos días antes de que se celebrara la reunión entre el presidente de Estados Unidos, Joe Biden, y el presidente de China, Xi Jinping, en San Francisco, como parte del foro de Cooperación Económica Asia-Pacífico (APEC). El número de actividades de amenazas descendió considerablemente tras la reunión Biden-Xi y a lo largo de la cumbre de APEC.

  Al finalizar esta, el nivel de actividad de amenazas había caído a niveles mínimos en el mes de noviembre de 2023. Probablemente este patrón de actividad de grupos de actores de amenazas vinculados a China demuestre la gran influencia que tienen en ellos los acontecimientos geopolíticos, como el foro APEC. También puede apuntar a la posibilidad de que los grupos de APT de China hayan retirado deliberadamente su actividad de hacking durante un evento político destacado probablemente con el objetivo de proteger su imagen pública y su reputación internacional.
- **Guerra entre Israel y Hamás:** los acontecimientos políticos en torno a la guerra de Israel y Hamás también han dado lugar a amenazas de grupos de APT vinculados a Irán. En Estados Unidos, los datos de telemetría global de Trellix muestran incrementos periódicos de la actividad maliciosa de grupos de APT vinculados a Irán en los últimos seis meses (con la excepción de finales de noviembre y diciembre de 2023). Concretamente, nuestra telemetría global señala una reducción de la actividad de amenazas de los grupos de APT vinculados a Irán contra organizaciones estadounidenses durante los períodos de los acuerdos para el intercambio de rehenes de Israel y el alto el fuego a finales de noviembre y diciembre de 2023, cuando Estados Unidos presionó para conseguir una tregua humanitaria en la Franja de Gaza, ya que Irán apoya abiertamente a Hamás. Además, la telemetría global de Trellix indica que los grupos de APT vinculados a Irán han empleado distintas TTP, como phishing, ladrones de información, puertas traseras, downloaders, webshells maliciosos y vulnerabilidades frecuentes contra organizaciones en Israel durante el período del informe.

ÍNDICE

- **Ejercicios militares:** además, las maniobras multinacionales de preparación para el combate pueden generar un aumento de actividades maliciosas. En fechas más recientes, marzo de 2024, los datos de telemetría global de Trellix muestran incrementos repetidos de actividades de amenazas en Corea del Sur durante las maniobras militares a gran escala conjuntas de Estados Unidos y Corea, denominadas "Escudo de la Libertad", entre el 4 y el 14 de marzo de 2024. Estos ejercicios militares se han diseñado para reflejar el "campo de operaciones de Corea" y luchar contra la amenaza nuclear continua de Corea del Norte. En concreto, se detectaron más de 150 000 amenazas en Corea del Sur entre el 7 y el 13 de marzo de 2024, respectivamente, lo que multiplica aproximadamente por siete el número de detecciones diarias habituales en el país (20 000).
- **Guerra Rusia-Ucrania:** la guerra cinética que continúa en la región viene acompañada de ciberacciones de distinta envergadura. Más concretamente, se ha observado que los ciberdelincuentes vinculados a Rusia aprovechan malware nuevo y más avanzado para borrar miles de servidores y PC virtuales mediante un ataque al proveedor de telecomunicaciones ucraniano Kyivstar. El de Kyivstar es uno de los ciberataques con mayor impacto en Ucrania desde que Rusia invadió el país en 2022.

Actualidad de amenazas de un vistazo

Aunque este informe incluye investigaciones de todo nuestro sector, los temas clave siguen vigentes:

1. **Cambios rápidos y significativos en el panorama de las APT**
   a. **Escalada del grupo Sandworm vinculado a Rusia:** a medida que aumentan las tensiones geopolíticas, también se incrementa la actividad de APT en el ecosistema completo. Mientras las amenazas APT crecen de manera global, el equipo Sandworm asociado a Rusia se detectó un 40 % más en el período que analiza este informe.
   b. **China continúa su senda prolífica:** los grupos de amenazas ligados a China siguen siendo los más prolíficos en cuanto a actividades de APT. Trellix ha observado más de 21 millones de detecciones de actividades de amenazas por parte de estos grupos. En más del 23 % de los casos, las actividades maliciosas se dirigen contra el sector público en todo el mundo.
   c. **Aumenta la actividad de Volt Typhoon:** Volt Typhoon, un grupo de APT financiado por China relativamente nuevo, destaca por su particular patrón de comportamiento y sus prácticas de ataque. Desde mediados de enero de 2024, la telemetría de Trellix detectó más de 7100 actividades maliciosas asociadas a Volt Typhoon, con incrementos periódicos desde enero hasta marzo de 2024.

ÍNDICE

2. **LockBit agita el ecosistema del ransomware**
    a. **Los impostores dañan la reputación de la banda:** tras la implantación de un operativo internacional de las fuerzas de seguridad, Operation Cronos, Trellix observó a impostores que se hacían pasar por LockBit, mientras el grupo intentaba por todos los medios salvar las apariencias y restablecer la actividad lucrativa.
    b. **Estados Unidos sigue estando en el epicentro de los ataques:** este país sigue siendo el más atacado por los grupos de ransomware, seguido por Turquía, Hong Kong, India y Brasil.
    c. **Transporte y distribución, el sector más afectado:** estos han sido los sectores más atacados por el ransomware en el 4.º trimestre de 2023 y el 1.er trimestre de 2024. Generaron el 53 y el 45 % de las detecciones de ransomware, respectivamente, seguidos por la industria financiera.
    d. **La intervención de las fuerzas de seguridad acaba en condena:** antes de que se finalizara este informe, las fuerzas de seguridad revelaron la verdadera identidad del líder de la banda de LockBit. El 1 de mayo se emprendieron otras acciones contra los ciberdelincuentes de ransomware. El ciberdelincuente del grupo REvil, que atacó Kaseya y muchas otras organizaciones, fue condenado a 13 años de prisión y al pago de 16 millones de USD.
3. **Aparición de los anuladores de EDR**
    a. **Aparece la banda de ransomware D0nut:** la llegada de la banda de ransomware D0nut llama particularmente la atención por su innovador uso de una herramienta de anulación de EDR, que pone de manifiesto una táctica avanzada para sortear la detección en los endpoints y maximizar la efectividad de sus ataques.
    b. **Uso de la herramienta de evasión de EDR de Spyboy contra el sector de las telecomunicaciones:** en la campaña de enero de 2024 se usó una herramienta de anulación de EDR ("EDR killer") desarrollada por Spyboy denominada "Terminator". La herramienta permitía eludir las soluciones EDR y el 80 % de las detecciones tenían como objetivo empresas del sector de las telecomunicaciones.
4. **Fraudes sobre el tema de las elecciones presidenciales en EE. UU.**
    a. **El phishing sigue siendo popular:** mientras el mundo tiene la vista puesta en las elecciones presidenciales de noviembre en Estados Unidos, se suceden los timos que emplean imágenes de los actos electorales para obtener donaciones.

ÍNDICE

5. **La IA generativa y el submundo de la ciberdelincuencia**
    a. **Herramientas impulsadas por IA gratuitas:** Trellix observó en mercados clandestinos una herramienta Jabber para ChatGPT 4.0 que permite al desarrollador ofrecer IA generativa a los ciberdelincuentes para sus operaciones y crear una base de conocimientos de IA generativa para que puedan aprender de otros ciberdelincuentes o incluso robarles ideas y herramientas.
    b. **Aumenta la adopción de InfoStealers:** se ha observado el empleo entre los ciberdelincuentes de dos ladrones de información (o InfoStealers) con funciones basadas en IA generativa. MetaStealer y LummaStealer incluyen IA generativa para eludir la detección y detectar bots entre la lista de registros, respectivamente. Las funciones de la IA generativa complican la detección y neutralización de estas tácticas delictivas.

Metodología: cómo recopilamos y analizamos los datos

Los expertos de nuestro Trellix 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. Estos datos agregados sirven para alimentar nuestras plataformas Insights y ATLAS. Aprovechando el aprendizaje automático, la automatización y la agudeza humana, el equipo efectúa una serie de procesos intensivos, integrados e iterativos con el objetivo de normalizar los datos, analizar la información y desarrollar ideas relevantes para los responsables de la ciberseguridad y los equipos SecOps que están en primera línea de la ciberseguridad en todo el mundo. Para obtener una descripción más detallada de nuestra metodología, consulte la parte final de este informe.

ÍNDICE

ANÁLISIS, PERSPECTIVAS Y DATOS DEL INFORME

Estados y amenazas avanzadas persistentes (APT)

Desde octubre de 2023 hasta marzo de 2024, Trellix observó un incremento del 17 % en las detecciones relacionadas con APT, respecto a los seis meses anteriores. Este dato es relevante, ya que nuestro último informe identificaba un asombroso aumento del 50 % en estas detecciones. El ecosistema de APT, más agresivo, astuto y activo, es radicalmente distinto del observado hace un año.

En el vertiginoso panorama de las ciberamenazas, los grupos de amenazas persistentes avanzadas (APT) siguen representando un desafío importante y sofisticado para los responsables de la ciberseguridad en todo el mundo.

Nuestro objetivo es analizar en detalle las actividades asociadas con APT detectadas entre el cuarto trimestre de 2023 y el primero de 2024. Este análisis se centra en los orígenes de estas amenazas, los objetivos principales de los atacantes y las herramientas que han empleado en sus operaciones. Comparamos estos hallazgos con datos de la primera mitad de 2023 (del 2.º y el 3.er trimestre) mediante dos métricas clave: la variación porcentual y la variación de contribución proporcional.

- Variación porcentual: esta métrica nos ayuda a ver si la actividad de un grupo de APT específico, su objetivo de ataque (países concretos) o el empleo de determinadas herramientas han aumentado, descendido o se mantienen al mismo nivel a lo largo del tiempo. Conocer estos datos nos ayuda a hacer un seguimiento del cambio de los comportamientos de estos ciberdelincuentes y descubrir cómo evoluciona el panorama de las ciberamenazas globalmente.
- Variación de contribución proporcional: esta métrica añade contexto, ya que no se limita a mostrar los datos brutos del cambio en la actividad, sino que contrasta esta información con el entorno completo de las amenazas para la ciberseguridad. Por ejemplo, aunque las detecciones de un ciberdelincuente determinado hayan aumentado considerablemente, es posible que solo representen una pequeña parte del total de ciberamenazas si el entorno global ha experimentado un enorme aumento. Por el contrario, si sus detecciones han disminuido, pero el resto del entorno de amenazas se ha ralentizado aún más, este ciberdelincuente podría tener un peso relativamente mayor.

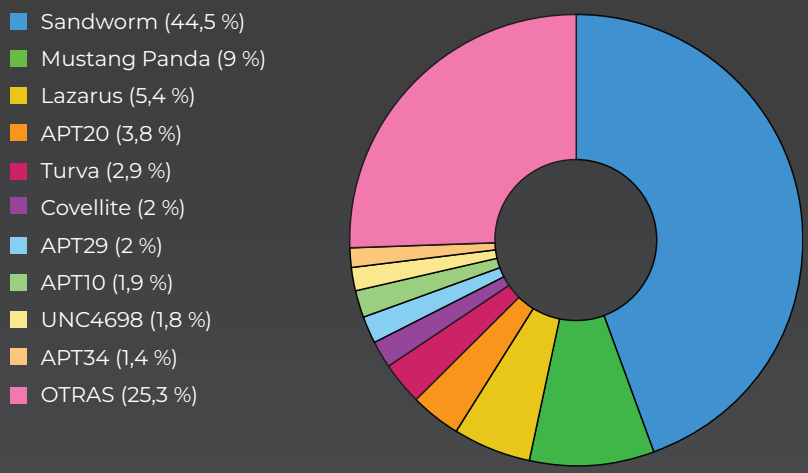
Estas métricas nos permiten conocer en detalle los cambios en las actividades de las APT y de esta forma podemos sacar conclusiones acerca de sus objetivos estratégicos, sus metodologías preferidas y los retos que implican para la ciberseguridad. En las secciones que siguen profundizaremos sobre estas conclusiones, arrojando luz sobre el intrincado mundo de las APT y el esfuerzo continuo que se requiere para garantizar la protección contra estas amenazas tan sofisticadas.

ÍNDICE

Estados y grupos de APT activos

Además, el período que va desde octubre de 2023 hasta marzo de 2024 fue testigo de fluctuaciones importantes en las actividades de varios grupos de APT. Estas fluctuaciones no solo subrayan la naturaleza dinámica de las ciberamenazas, también destacan los cambios en el enfoque operativo y las técnicas que emplean estos expertos ciberdelincuentes.

10 APT PRINCIPALES SEGÚN LAS DETECCIONES ENTRE EL ÚLTIMO TRIMESTRE DE 2023 Y EL PRIMER TRIMESTRE DE 2024.



CAMBIOS EN LA ACTIVIDAD DE GRUPOS DE CIBERAMENAZAS: VARIACIÓN Y CONTRIBUCIÓN PROPORCIONAL

Amenazas persistentes avanzadas	Variación porcentual	Variación de contribución proporcional
Sandworm	1669,43 %	40,34 %
Mustang Panda	-2,19 %	-6,14 %
Lazarus	66,87 %	0,07 %
APT28	18,67 %	-1,49 %
Turla	2,95 %	-1,74 %
Covellite	85,30 %	0,23 %
APT29	123,98 %	0,53 %
APT10	80,46 %	0,17 %
UNC4698	368,75 %	1,14 %
APT34	96,73 %	0,23 %
Otros	-28,99 %	-33,33 %

ÍNDICE

- **Cambio de táctica:** Sandworm, conocido tradicionalmente por el potencial destructivo de sus ciberoperaciones, muestra un acusado incremento de las detecciones (1669 %), con una variación de contribución proporcional del 40 %. Este impresionante crecimiento es indicativo de una escalada sin precedentes de las ciberactividades de este grupo vinculado a Rusia.
- **Incremento agresivo de la operaciones:** APT29, un grupo con un amplio historial de ciberespionaje, mostró un aumento destacado de la actividad. Las detecciones aumentaron un 124 %. De la misma forma, APT34 y Covellite también mostraron un aumento de detecciones, del 97 y el 85 % respectivamente, lo que indica un aumento del ritmo de las operaciones o bien el inicio de nuevas campañas.
- **Homeostasis:** en cambio, grupos como Mustang Panda, Turla y APT28 mostraron pocos cambios en sus niveles de actividad. Mustang Panda sufre un ligero descenso de -2 % y Turla un modesto aumento del 3 % en las detecciones.
- **Surgen nuevos actores:** es de destacar la aparición de UNC4698, con un aumento del 363 % de detecciones, lo que puede ser indicio de la incorporación al panorama de las APT de un nuevo actor con un gran peso potencial.

¿QUÉ SABEMOS DE UNC4698?

No se sabe mucho sobre este grupo, pero los investigadores han podido identificar su comportamiento como trabajo en equipo y aún no saben cómo definirlo.

Dicho esto, lo que sí se sabe de UNC4698 es que su prioridad es el espionaje industrial, la recopilación de datos operativos sensibles que podrían utilizarse para apoyar los objetivos económicos o de seguridad nacional del Estado patrocinador, muy probablemente China, por la naturaleza y el enfoque regional de los ataques.

Sus objetivos principales son organizaciones petroleras y de gas ubicadas en Asia.

También se sabe que emplean un malware específico al que llaman "SNOWYDRIVE".

UNC4698 emplea una amplia variedad de tácticas, técnicas y procedimientos (TTP) relacionados con el uso de malware distribuido a través de unidades flash USB. A continuación incluimos algunas técnicas tácticas y procedimientos asociados a este actor de amenazas:

- **Acceso inicial a través de dispositivo USB infectados:** el principal método de infección implica el uso de unidades USB que contienen software malicioso diseñado para crear una puerta trasera en el sistema host.

ÍNDICE

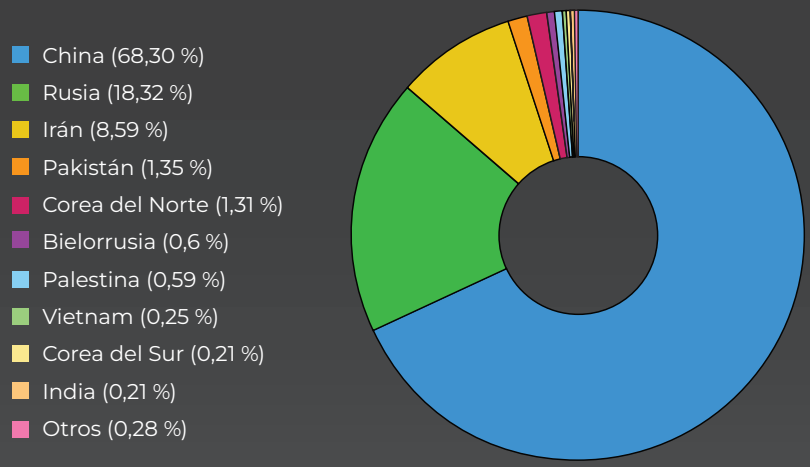
¿QUÉ SABEMOS DE UNC4698? *(continuación)*

- **Ejecución a través de archivos maliciosos:** el malware suele incluir un inyector que escribe DLL y ejecutables maliciosos en el disco. Estos archivos suelen hacerse pasar por software legítimo para evitar su detección y se ejecutan para conseguir un mayor control.
- **Persistencia y modificación del Registro:** UNC4698 se asegura la persistencia en los sistemas infectados modificando el Registro de Windows. Esto permite al malware iniciarse automáticamente al arrancar el sistema.
- **Comunicación con el servidor de mando y control:** el malware establece un método para la comunicación remota, permitiendo a los agresores emitir órdenes y controlar los sistemas comprometidos a distancia.
- **Movimiento lateral a través de soportes extraíbles:** el malware puede copiarse automáticamente en otros dispositivos USB conectados a la máquina infectada, lo que ayuda a propagar la infección a otros sistemas.

Las detecciones en el caso de los grupos menos conocidos o no identificados aumentaron un 62 %, síntoma de que existe una gama variada y creciente de amenazas, además de las entidades de APT bien documentadas. El incremento del 8 % en su contribución proporcional al total de detecciones pone de manifiesto la evolución constante y la diversificación de las ciberamenazas.

Grupos de APT y países de origen

10 PAÍSES ASOCIADOS A GRUPOS APT CON EL MAYOR NÚMERO DE DETECCIONES ASOCIADAS A CAMPAÑAS, ENTRE EL ÚLTIMO TRIMESTRE DE 2023 Y EL PRIMER TRIMESTRE DE 2024



ÍNDICE

Cuando se analizan los países de origen, la telemetría de Trellix desde octubre de 2023 hasta marzo de 2024 también indica cambios destacados en cuanto a las ciberactividades patrocinadas por Estados.

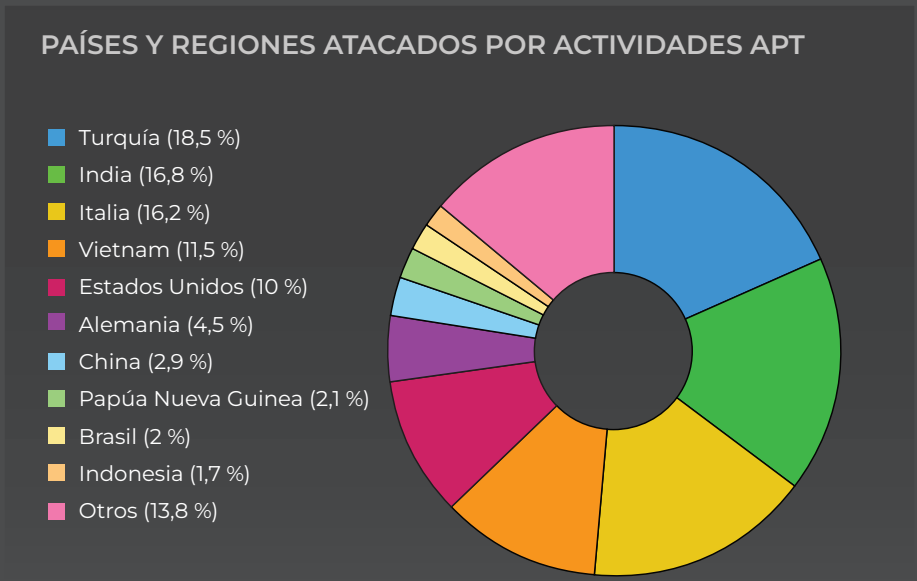
Los grupos de amenazas vinculados a China siguen siendo los más prolíficos en cuanto a actividades de APT

- **Escalada importante de las operaciones:** las motivaciones geopolíticas y la ciberseguridad están evolucionando en distintos países. Esto es lo que ha observado nuestra telemetría:
  a. Los grupos de amenazas vinculados a Rusia han mostrado un considerable incremento de detecciones de APT, hasta un 31 %, y su contribución proporcional ha subido un 4 %. Esto representa una notable escalada de las ciberoperaciones, que posiblemente refleje objetivos estratégicos más amplios o respuestas a la dinámica de la ciberseguridad a nivel mundial.
  b. Los grupos de amenazas vinculados a Irán también han incrementado enormemente las ciberactividades; un 8 % en las detecciones y un 3,89 % en la contribución proporcional. Esto pone de relieve una clara ampliación de las ciberoperaciones de Irán, en línea con sus objetivos geopolíticos y su implicación en la guerra entre Israel y Hamás.
- **Una mayor diversificación:** China sigue siendo el principal origen de actividades de APT, aunque las detecciones solo han aumentado un 1 %. Sin embargo, su contribución proporcional al total de las detecciones se ha reducido ligeramente (-1 %), lo que podría indicar una mayor diversificación de orígenes de APT durante este período. En febrero de este año aparecieron también informes sobre acciones importantes de Volt Typhoon, un grupo de APT financiado por China, contra infraestructuras críticas de Estados Unidos. En la siguiente sección se incluye más información sobre este tema.
- **Giro en la estrategia:** por el contrario, los grupos ligados a Corea del Norte, Vietnam e India han experimentado descensos significativos en sus actividades de APT. Las detecciones relacionadas con Corea del Norte han caído un -82 %, las de Vietnam un -80 % y las de India un -82 %. Es de destacar la importante disminución de la contribución proporcional de Corea del Norte (-6 %), posiblemente debida a un cambio en prioridades, estrategia o capacidades.
- **Surgen más países:** se ha observado un aumento considerable de las actividades de APT en grupos vinculados a Paquistán y Bielorrusia. Las detecciones han aumentado un 55 % y un 2019 %, respectivamente. Estos aumentos, en particular el incremento exponencial de Bielorrusia, subrayan la aparición de actores nuevos o desconocidos hasta ahora en el espacio de las APT.

  La categoría "Otras" muestra un aumento del 121 % en las detecciones, lo que indica que las actividades de APT no se limitan a los países que se citan con más frecuencia. Esta diversidad refleja el carácter global de las ciberamenazas y la necesidad de contar con una postura de ciberseguridad de amplio alcance y adaptable.

En los próximos meses haremos un seguimiento exhaustivo de estos nuevos patrones de ataque.

ÍNDICE



Regiones y países atacados

Esta sección se centra en las regiones en las que Trellix detectó actividad de grupos de APT entre el 4.º trimestre de 2023 y el 1.er trimestre de 2024 y revela cambios importantes en las prioridades y la estrategia de estos sofisticados ciberdelincuentes.

> Los datos subrayan la naturaleza global de las ciberamenazas y los distintos niveles de atención que diferentes naciones reciben de los grupos de APT.

Tras las evaluaciones, el Trellix Advanced Research Center ha concluido con un moderado nivel de confianza que los siguientes factores afectan a la actividad detectada en determinados países y regiones.

Turquía ha experimentado un aumento sin precedentes en detecciones relacionadas con APT

Objetivos operativos:
las detecciones de amenazas dirigidas contra Turquía sufrieron un impresionante aumento (1458 %), lo que implica un ascenso del 16 % en su contribución proporcional al total de detecciones. Este asombroso incremento indica un cambio significativo en el enfoque de las ciberamenazas contra Turquía, que probablemente refleje tensiones geopolíticas más amplias u objetivos operativos concretos de los grupos de APT.

- **Importancia estratégica:** India e Italia también han experimentado aumentos importantes en las detecciones, que alcanzan el 614 % y el 308 %, respectivamente. Es posible que la mayor prevalencia de estos países en la lista de objetivos de ataque esté relacionada con su creciente importancia estratégica en el ciberdominio, ya sea debido a factores económicos, políticos o tecnológicos.

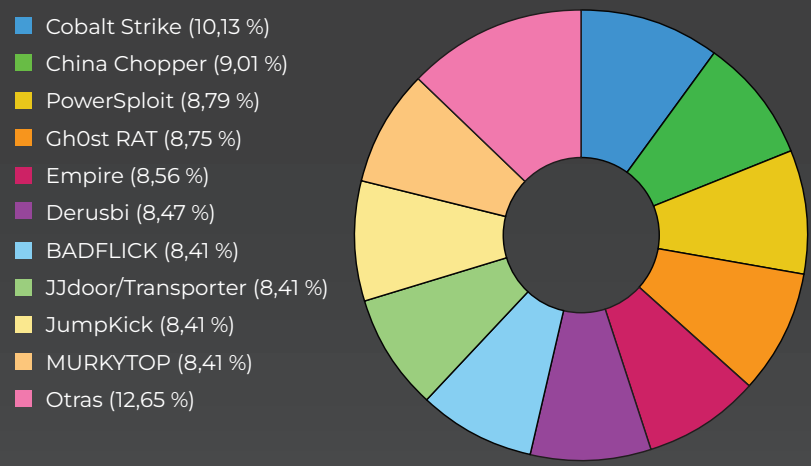
ÍNDICE

- **Ampliación del panorama:** es curioso destacar que Vietnam y Estados Unidos, aunque continúan generando detecciones de APT significativas, muestran tendencias diferentes. Las detecciones de Vietnam aumentaron un 9 %, sin embargo su contribución proporcional descendió un -9 %, lo que indica un aumento de objetivos de ataques. Estados Unidos experimentó un moderado incremento de las detecciones (15 %), pero una caída del -7 % en la contribución proporcional, lo que indica una diversificación de las estrategias de los grupos de APT.
- **Acontecimientos geopolíticos:** en Alemania, China, Papúa Nueva Guinea y Brasil se observan incrementos en las detecciones, y en Alemania y China, cambios significativos en la contribución proporcional. Esta diversificación en los objetivos refleja los ajustes estratégicos y oportunísticos que aplican los grupos de APT como repuesta al estado de la ciberseguridad mundial y a los acontecimientos geopolíticos.
- **Mejora de la seguridad nacional:** por el contrario, Indonesia ha experimentado un notable descenso de las detecciones (48 %), junto con una caída del -4 % de la contribución proporcional. Esta caída podría ser indicio de un cambio de prioridades temporal o síntoma de una mejora de las medidas de ciberseguridad nacional.
- **Consolidación del enfoque:** la categoría "Otros", que representa a un colectivo de otros países distintos en los que Trellix detectó actividad relacionada con las APT, muestra un descenso del 23 % en las detecciones y del 21 % en la contribución proporcional. Este descenso posiblemente se deba a una consolidación del enfoque por parte de los grupos de APT en determinados objetivos que concentran un gran nivel de interés durante este período.

Observamos potencial para que el panorama siga cambiando rápidamente impulsado por las tendencias geopolíticas.

Herramientas maliciosas

10 HERRAMIENTAS MALICIOSAS DETECTADAS ENTRE EL ÚLTIMO TRIMESTRE DE 2023 Y EL PRIMER TRIMESTRE DE 2024.



ÍNDICE

El análisis de la herramientas maliciosas utilizadas en campañas de APT entre el 4.º trimestre de 2023 y el 1.er trimestre de 2024 revela tendencias claras en cuanto a las preferencias y tácticas operativas de los ciberdelincuentes. La variación de las tasas de detección y su contribución proporcional ofrece datos sobre la evolución del panorama de las ciberamenazas y la dinámica de uso de las herramientas entre estos sofisticados grupos.

Se observaron las siguientes tendencias:

- **Se refuerza la eficacia de las herramientas de ataque:** Cobalt Strike sigue siendo la herramienta preferida para muchos grupos de amenazas, a pesar del descenso del 17 % en las detecciones. El descenso relativamente pequeño que muestra en la variación de contribución proporcional (-1 %) es síntoma de su popularidad y eficacia en ciberoperaciones, y subraya el reto que supone defenderse contra herramientas de ataque versátiles y de uso generalizado.
- **Dependencia de shells web, PowerShell y ataques de acceso remoto:** Las detecciones de las herramientas China Chopper, PowerSploit y Gh0st RAT también sufrieron un marcado descenso, 23 %, 24 % y 24 %, respectivamente. A pesar de esto, los ligeros cambios que muestran en la variación de contribución proporcional indican que siguen siendo parte integral del kit de herramientas del actor de amenazas. Estas herramientas, conocidas por su eficacia en ataques de shells web, PowerShell exploits y acceso remoto, son prueba de que se sigue confiando en herramientas versátiles de eficacia demostrada para las ciberoperaciones.
- **Herramientas menos detectables:** Empire, Derusbi, BADFLICK, JJdoor/Transporter, JumpKick y MURKYTOP experimentaron tendencias a la baja similares en las detecciones. Todas ellas superan un 25 % de disminución. Este retroceso uniforme podría reflejar un cambio más amplio en la preferencia de herramientas entre los grupos de amenazas o bien una adaptación a las contramedidas y técnicas de detección que impone la necesidad de utilizar nuevas herramientas, menos detectables.
- **Innovación constante:** las detecciones de la categoría de herramientas maliciosas "Otras" se incrementaron considerablemente (30 %) y la variación de contribución proporcional aumentó de forma importante (6 %). Este incremento subraya la innovación constante y la adaptación entre los ciberdelincuentes, que exploran nuevas herramientas y técnicas para evitar ser detectados y lograr sus objetivos.

El cambio en las preferencias en cuanto a uso de herramientas maliciosas pone de relieve la capacidad de adaptación de los ciberdelincuentes para responder a los avances en ciberseguridad.

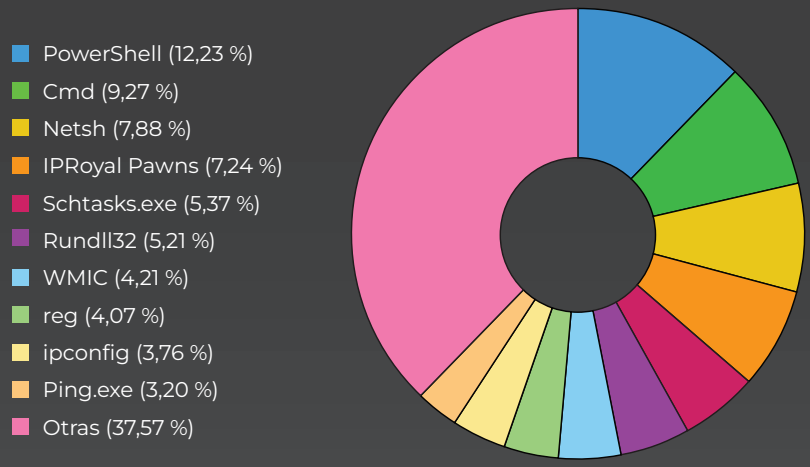
> A medida que aumenta la sofisticación de los mecanismos de defensa, también lo hacen las herramientas y tácticas ofensivas de los grupos de APT.

El cambio hacia una gama más amplia de herramientas, como indica el aumento de detecciones en la categoría "Otras", confirma la necesidad de investigaciones continuas, inteligencia sobre amenazas y estrategias de defensa adaptables para mitigar el riesgo que implican estas ciberamenazas en evolución.

ÍNDICE

Herramientas no maliciosas

10 PRINCIPALES HERRAMIENTAS NO MALICIOSAS DETECTADAS ENTRE EL ÚLTIMO TRIMESTRE DE 2023 Y EL PRIMER TRIMESTRE DE 2024.



> Esta práctica, conocida como aprovechamiento de recursos locales (Living of The Land, LOTL), complica las tareas de detección y demuestra lo sofisticados que son estos ciberdelincuentes.

El empleo de herramientas no maliciosas en las ciberoperaciones por parte de grupos de APT entre el 4.º trimestre de 2023 y el 1.er trimestre de 2024 revela un importante aspecto de las ciberamenazas modernas: el aprovechamiento de herramientas del sistema legítimas para fines malintencionados. Esta práctica, conocida como aprovechamiento de recursos locales (Living of The Land, LOTL), complica las tareas de detección y demuestra lo sofisticados que son estos ciberdelincuentes. Las estadísticas relevan variaciones significativas en el uso de estas herramientas, lo que refleja su importancia estratégica en las ciberoperaciones.

- **Versatilidad:** las detecciones de PowerShell han aumentado considerablemente, hasta un 105 %, con una variación de contribución proporcional del 1 %. Este aumento subraya su versatilidad y capacidad al automatizar una amplia variedad de actividades maliciosas, desde el reconocimiento hasta la entrega de la carga útil.
- **La manipulación de las redes en el punto de mira:** las detecciones de Netsh y IPRoyal Pawns han aumentado enormemente, 99 % y 102 %, respectivamente. Estas herramientas suelen utilizarse para la configuración de la red y el tráfico proxy, lo que indica una tendencia estratégica hacia las técnicas de evasión y manipulación de la red.
- **Automatización a gran escala:** Schtasks.exe ha experimentado el máximo porcentaje de varianza entre las herramientas que se incluyen (un 138 %). Esto refleja un mayor uso de las tareas programadas para la persistencia y ejecución de cargas útiles maliciosas, sin la intervención directa del usuario.

ÍNDICE

- **Giros tácticos:** por el contrario, en el caso de Rundll32 y WMIC, se ha observado un aumento de uso, acompañado de descensos en la variación de contribución proporcional, lo que indica un giro en las preferencias tácticas de los grupos de APT, a pesar de que estas herramientas siguen siendo útiles.
- **Diversificación de herramientas:** el uso de Cmd, el legendario intérprete de línea de comandos de los sistemas Windows, también experimentó un incremento sustancial, con un aumento de las detecciones de hasta el 65 %. A pesar del aumento de uso, su variación de contribución proporcional ha descendido (-2,5 %), probablemente debido a una mayor diversificación de las herramientas utilizadas por los grupos de APT.

  En el caso de la categoría "Otras", que representa una variedad de herramientas que se usan menos o son más especializadas, las detecciones aumentaron un 42 %. Sin embargo, esta categoría experimentó un descenso importante de la variación de contribución proporcional (-21 %), que indica la ampliación del arsenal de herramientas a disposición de los ciberdelincuentes.

La evolución del uso de herramientas no maliciosas por parte de grupos de APT ilustra la complejidad de detectar y proteger frente a ciberamenazas sofisticadas. La selección estratégica de estas herramientas y su posterior aplicación revela un profundo conocimiento de los entornos atacados y el esfuerzo por evitar ser detectados.

> **CONSEJO PARA LOS CISO:** las defensas de la ciberseguridad no pueden limitarse a la tradicional detección de malware y tienen que incluir análisis comportamentales y detección de anomalías a fin de contrarrestar el uso ilícito de herramientas legítimas en las ciberoperaciones.

Los datos que se obtienen de los sensores globales Trellix ATLAS, junto con la información estratégica procedente del análisis de informes del sector, que proporciona el Trellix Advanced Research Center permiten a nuestros clientes identificar a los ciberdelincuentes que tienen en el punto de mira a sus respectivos sectores y utilizar nuestro análisis comportamental para detectar comportamientos anómalos en su entorno.

ÍNDICE

Conclusión

El análisis de actividades de amenazas persistentes avanzadas (APT) entre el 4.° trimestre de 2023 y el 1.er trimestre de 2024 arroja luz sobre el carácter dinámico y cada vez más complejo del panorama de las ciberamenazas. Nuestro examen de las estadísticas relacionadas con los orígenes, países atacados y herramientas maliciosas y no maliciosas utilizadas por los grupos de APT revela varias tendencias clave que subrayan la evolución de las estrategias empleadas por los ciberdelincuentes.

Los grupos de APT siguen mostrando un alto grado de:

1. Adaptabilidad y sofisticación
2. Aprovechamiento de una combinación de herramientas maliciosas
3. Uso de funciones legítimas de los sistemas para llevar a cabo acciones de espionaje, interrumpir las operaciones y robar información confidencial.

Los importantes cambios observados en cuanto a tácticas operativas y de ataque de estos grupos no solo reflejan sus objetivos estratégicos, sino también su respuesta ante los avances en las medidas de defensa y ciberseguridad a nivel mundial.

Los cambios drásticos en las prácticas de ataque, con un incremento notable de actividades relacionadas con las APT en determinados países, denotan las motivaciones geopolíticas de estas ciberoperaciones. Asimismo, los cambios en las herramientas utilizadas, con un evidente aumento de tácticas que aprovechan los recursos existentes (LOTL), ponen de relieve la dificultad permanente de detectar y combatir las amenazas APT en un panorama en el que las actividades legítimas y las maliciosas están cada vez más interrelacionadas.

Además, la diversificación de orígenes de APT y la ampliación de sus estrategias de ataque son síntoma de la proliferación mundial de las cibercapacidades y la necesidad de contar con un enfoque de la ciberseguridad unificado y cooperativo.

> Es evidente que ningún país u organización está a salvo del impacto de estos ciberdelincuentes.

ÍNDICE

Volt Typhoon: actor de amenazas APT vinculado a China

Los grupos de ciberdelincuentes auspiciados por Estados siguieron representando una grave amenaza para empresas del sector público y privado en todo el mundo durante el último trimestre de 2023 y el primero de 2024. Estos adversarios, normalmente bien equipados y expertos en ciberamenazas, atacan las redes sin descanso durante períodos prolongados, con un nivel de competencia y unos recursos superiores a los de los ciberdelincuentes o hacktivistas.

23 %

Más del 23 % de las detecciones de actividades maliciosas se dirigen contra el sector público en todo el mundo

Más de 21 millones de detecciones de actividad de amenazas de grupos de ciberdelincuentes vinculados con China

Concretamente, según los datos de telemetría de Trellix, los grupos de actores de amenazas auspiciados por Estados vinculados a China han aumentado las amenazas contra el sector público en todo el mundo. Nuestros datos dejan constancia de más de 21 millones de detecciones de actividad de amenazas por parte grupos vinculados con China, entre octubre de 2023 y marzo de 2024.

DETECCIONES A NIVEL MUNDIAL DE GRUPOS DE APT VINCULADOS A CHINA

(Fuente: ATLAS)

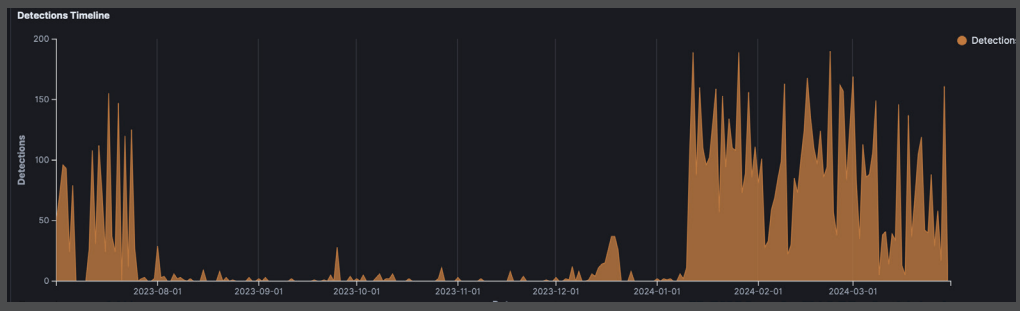
ÍNDICE

Descripción

Volt Typhoon, un grupo de APT auspiciado por China relativamente nuevo, destaca por un patrón de comportamiento distinto y por sus perfiles de ataque, que se desvían del ciberespionaje convencional y la recopilación de inteligencia de otros grupos de APT asociados a dicho país. Según otros informes de código abierto anteriores, este grupo de APT chino se ha posicionado en redes de TI de control industrial para facilitar el movimiento lateral e interrumpir el funcionamiento de los recursos y funciones de tecnología operativa en caso de crisis geopolítica o guerra. Los datos de telemetría de Trellix indican que, desde que retomó las operaciones en enero de 2024, Volt Typhoon ha atacado repetidamente al sector público en todo el mundo, incluido Estados Unidos, mediante el empleo de técnicas de aprovechamiento de recursos existentes (LOTL).

Cronología

Los datos de telemetría de Trellix muestran que Volt Typhoon se detectó por primera vez a mediados de 2021, pero permaneció inactivo, con poca o ninguna actividad, desde agosto de 2023 hasta enero de 2024. Este período de descanso podría estar relacionado con la culminación de las investigaciones sobre amenazas en los meses que siguieron al primer informe de proveedores sobre Volt Typhoon, publicado en mayo de 2023, que atrajo mucha atención en todo el mundo. También podría deberse a un cambio de la infraestructura de ataque de Volt Typhoon durante este período, motivado por la exposición pública, lo que provocó un descenso del número de actividades de amenazas detectadas.



Cronología de detecciones de Volt Typhoon desde julio de 2023 a marzo de 2024 (Fuente: Trellix ATLAS)

Volt Typhoon reanudó las operaciones aproximadamente a mediados de enero de 2024, según los datos de telemetría de Trellix. Desde mediados de enero de 2024, la telemetría de Trellix detectó más de 7100 actividades maliciosas asociadas a Volt Typhoon, con incrementos periódicos desde enero hasta marzo de 2024.

Detalles de detecciones de Volt Typhoon de enero a marzo de 2024

ÍNDICE

Tácticas, técnicas y procedimientos (TTP)

Nuestros datos de detecciones indican que desde que retomó las operaciones a mediados de enero de 2024, Volt Typhoon ha aprovechado sistemáticamente algunas herramientas y funciones nativas de Windows para ejecutar comandos con fines maliciosos. El uso malintencionado de herramientas y funciones legítimas del sistema, lo que se conoce como Living of The Land (LOTL), es cada vez más popular entre los grupos de atacantes asociados con China, como Volt Typhoon. Netsh.exe es una de estas herramientas de uso dual, que se puede usar para distintos fines maliciosos, como desactivar la configuración del firewall o configurar un túnel proxy para permitir el acceso remoto a un host infectado. Ldifde es otra herramienta que utiliza Volt Typhoon para recopilar información.

Tras lograr el acceso a un controlador de dominio, los atacantes pueden usar Ldifde.exe para exportar datos confidenciales o para realizar cambios autorizados en el directorio. Asimismo, los actores de amenazas de Volt Typhoon usan ntdsutil con fines malintencionados. Ntdsutil es una herramienta legítima que permite a los administradores realizar tareas de mantenimiento de bases de datos. Sin embargo, también sirve para crear un volcado de Active Directory con el fin de obtener credenciales y filtrar datos confidenciales.

Volt Typhoon siguió utilizando en sus operaciones herramientas de código abierto, como FRP, Impacket y Mimikatz. La telemetría de Trellix detectó también que Volt Typhoon utilizó las herramientas y comandos LOTL siguientes, entre febrero y marzo de 2023:

- Comsvcs
- Dnscmd
- Ldifde
- MiniDump
- Net
- Netsh
- Ntdsutil
- reg
- ping
- PowerShell
- PsExec

ÍNDICE

Según nuestra telemetría, estas son las herramientas de MITRE ATT&CK que utilizó Volt Typhoon:

- Acceso inicial – T1190: Exploit de aplicaciones públicas
- Ejecución – T1106: API nativa
- Persistencia – T1546: Ejecución desencadenada por evento
- Elevación de privilegios - T1546: Ejecución desencadenada por evento
- Evasión de defensas – T1070.001: Borrado de registros de eventos de Windows
- Evasión de defensas – T1070: Eliminación de archivos
- Evasión de defensas – T1027: Ofuscación de archivos o información
- Acceso a credenciales – T1003.003: NTDS
- Acceso a credenciales – T1003: Volcado de credenciales del sistema operativo
- Acceso a credenciales – T1110: Fuerza bruta
- Acceso a credenciales – T1555: Credenciales extraídas de almacenes de contraseñas
- Descubrimiento – T1069.002: Grupos de dominios
- Descubrimiento – T1069.001: Grupos locales
- Descubrimiento – T1083: Descubrimiento de archivos y directorios
- Descubrimiento – T1057: Descubrimiento de procesos
- Descubrimiento – T1010: Descubrimiento ventanas de aplicaciones
- Recopilación – T1560: Archivado de datos recopilados
- Recopilación – T1560.001: Archivado mediante utilidad
- Mando y control – T1090.002: Proxy externo
- Mando y control – T1105: Transferencia de herramientas a la entrada
- Mando y control – T1132: Codificación de datos

Evolución del panorama del ransomware

En el 4.º trimestre de 2023, el panorama de las ciberamenazas asistió a una escalada de ataques de ransomware, con un impacto cada vez mayor de nuevas familias aparecidas ese año.

- **Herramientas de anulación de EDR:** entre ellas, la aparición de la banda de ransomware D0nut es particularmente destacable debido a su innovador uso de una herramienta de anulación de EDR, que pone de manifiesto una táctica avanzada para sortear la detección en los endpoints y maximiza la efectividad de sus ataques. En la siguientes sección se incluye más información sobre este tema.
- **Aprovechamiento de vulnerabilidades:** en este período también se constató que continúa la tendencia de aprovechar vulnerabilidades críticas para facilitar el despliegue del ransomware. En concreto, CVE-2023-4966, conocida como Citrix Bleed, es una vulnerabilidad que aprovecharon los afiliados a LockBit 3.0. Esto constata que la infraestructura crítica sigue siendo vulnerable ante ciberataques sofisticados. Además, el aprovechamiento de la vulnerabilidad CVE-2023-22518 en Confluence Data Center y Confluence Server ilustra el interés de los atacantes por infiltrarse en plataformas empresariales muy utilizadas con fin de desplegar el ransomware.

ÍNDICE

La campaña de ransomware Cactus, dirigida contra las instalaciones de Qlik Sense, que aprovecha vulnerabilidades recién descubiertas, pone además de manifiesto la agilidad de los atacantes para adaptarse al panorama de seguridad y sacar partido de vulnerabilidades emergentes. Con todo esto el 4.° trimestre ha sido muy prolífico en cuanto a grupos de ransomware.

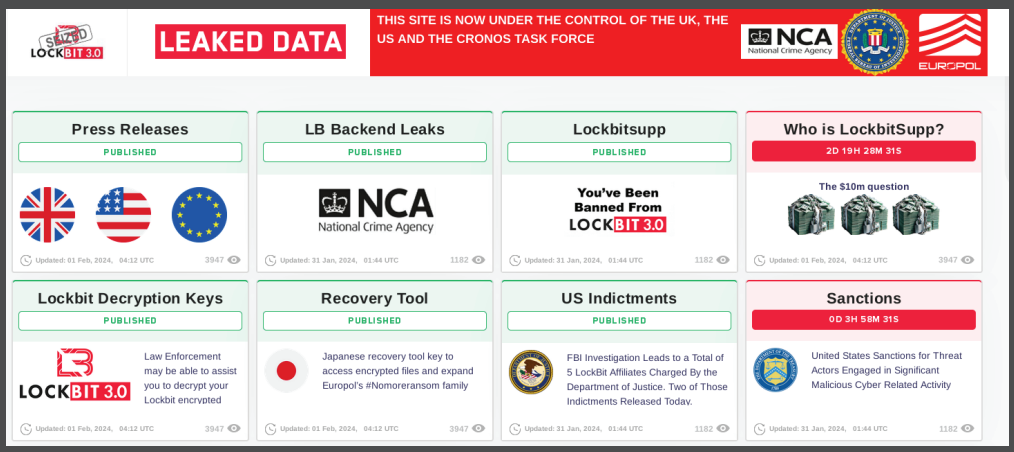
Sin embargo, en el primer trimestre de 2024, con la intervención de un extraordinario operativo de las fuerzas de seguridad, se iba a cuestionar el statu quo.

Operation Cronos: acciones de las fuerzas de seguridad para desmantelar LockBit

El 19 de febrero de 2024 se puso en marcha un operativo internacional de las fuerzas de seguridad, al que denominaron Operation Cronos, y que consiguió desmantelar las actividades de la tristemente célebre banda LockBit, poniendo en jaque a este grupo de ciberdelincuentes de larga tradición. Las fuerzas del orden no solo publicaron avisos del desmantelamiento, sino que acabaron tomando el control del sitio de divulgación del colectivo y también filtraron información para exponer al mundo al grupo ciberdelictivo. Se presentaron varios cargos y los afiliados activos recibieron un amistoso mensaje de bienvenida cuando se conectaron al sistema backend de LockBit, en el que se indicaba muy claramente que se conocía su identidad.

El objetivo de estas operaciones no so fue solo perturbar la actividad de LockBit, sino también dañar su reputación y socavar la confianza dentro de la banda.

Al término de la redacción de este informe, Operation Cronos dio un nuevo giro. Las fuerzas de seguridad a nivel mundial dieron un nuevo golpe revelando la verdadera identidad del líder del grupo LockBit. Esta no fue la única victoria de las fuerzas de seguridad: el 1 de mayo, el ciberdelincuente de REvil, que atacó Kaseya y muchas otras empresas, fue condenada a 13 años de prisión y a pagar 16 millones de dólares de indemnización. Encontrará más información sobre cómo Trellix Advanced Research Center ayudó en el caso de REvil en este artículo.



ÍNDICE

El año pasado, nuestro informe de febrero identificó al ransomware LockBit como el más agresivo en cuanto a las peticiones de rescate. Los ciberdelincuentes utilizan una gran variedad de técnicas para lanzar sus campañas, incluida la explotación de vulnerabilidades encontradas incluso en 2018. A lo largo de 2023, LockBit siguió siendo en todo momento el grupo de ransomware más prevalente con el mayor número de víctimas publicadas en su sito de divulgación. Su objetivo principal fueron organizaciones europeas y norteamericanas en distintos sectores, siendo el de los bienes y servicios industriales el más afectado. En 2023, LockBit continuó evolucionando continuamente e introduciendo nuevas herramientas y métodos a su programas de ransomware. En particular, el grupo ha estado trabajando en el desarrollo de la herramienta de cifrado LockBit Green, basado en el código filtrado del ransomware Conti, así como variantes de LockBit dirigidas a macOS. Además, en 2023 observamos que LockBit RaaS ofrecía refugio a miembros de otros programas RaaS, como ALPHV y NoEscape, cuyas operaciones había sido desmanteladas.

A raíz de las acciones de desmantelamiento, observamos a LockBit intentando por todos los medios salvar las apariencias y restablecer la actividad lucrativa. Esto era de esperar dada la publicidad de las actividades delictivas de LockBit. Sin embargo, en el submundo de la ciberdelincuencia es más fácil restaurar un servidor que años de confianza. Queda por ver la cantidad de información que las fuerzas de seguridad han conseguido obtener de las operaciones, el perfil y los afiliados de LockBit.

> Esta incertidumbre crea un riesgo considerable para los ciberdelincuentes que deseen colaborar con LockBit y su (antiguo) equipo.

Las acciones de las fuerzas de seguridad dejaron bien a las claras que la ciberdelincuencia es un mundo de todos contra todos. El Trellix Advanced Research Center observó que otros ciberdelincuentes utilizaban la versión filtrada de LockBit Black para suplantar a la conocida marca para su propio beneficio económico.

Impostores o no, las víctimas que generaron eran reales; sin duda los eventos de estos dos últimos trimestres dan para un guion cinematográfico.

Una visión global del ransomware

Durante nuestra investigación sobre la actividad de ransomware en el primer trimestre de 2023, investigamos múltiples fuentes: sitios de filtraciones, telemetría, e informes públicos. Breves comentarios sobre cada una de las categorías.

- **Sitios de filtraciones:** estos sitios están diseñados para mostrar pruebas de víctimas extorsionadas que no han pagado el rescate exigido, ofreciendo así una perspectiva de la actividad de la banda de ciberdelincuentes. Además, es importante destacar que los sitios de filtraciones no necesariamente reflejan fielmente el panorama de ciberamenazas. El hecho de que estén controlados por delincuentes,

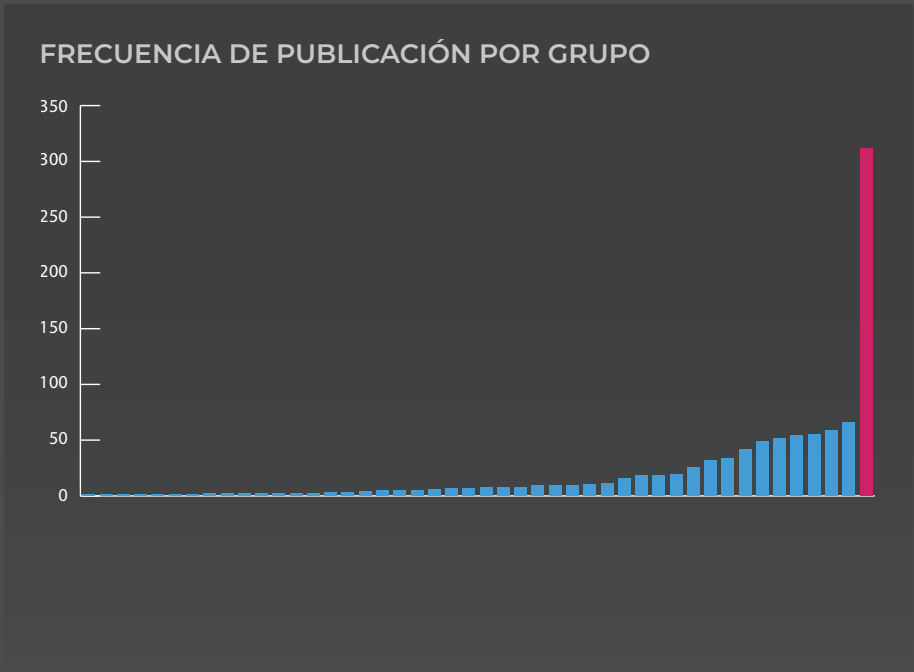
ÍNDICE

hace imposible fiarse de todas las afirmaciones. Además, si las bandas son fieles a su palabra, las víctimas que pagan el rescate no aparecen en los sitios, lo que deja una imagen incompleta de la situación. Los datos que se utilizan en este informe se refieren a las tendencias globales de los sitios de filtraciones y sí ofrece una imagen significativa.

- **Telemetría:** la telemetría se extrae del ecosistema de sensores de Trellix y las detecciones se producen cuando uno de nuestros productos detecta un archivo, URL, dirección IP u otro indicador y nos informa al respecto. Esto no quiere decir que cada detección sea una infección, ya que los clientes prueban la detección de determinados archivos para ajustar sus reglas internas, lo que también se reflejan en el registro agregado. Por lo tanto, estos datos siguen siendo útiles al considerar el panorama general, ya que las tendencias siguen estando ahí.
- **Informes públicos:** informes de proveedores y de particulares procesados por nuestro Advanced Research Center para analizar funciones e identificar tendencias. Cada informe tiene un sesgo inherente, debido por ejemplo a la presencia dominante de un proveedor en una región geográfica sobre otra. Esta diferencia también se reflejará en los tipos de incidentes notificados. Debido a los diferentes sesgos de los informes incluidos, no aplicamos un filtro específico.

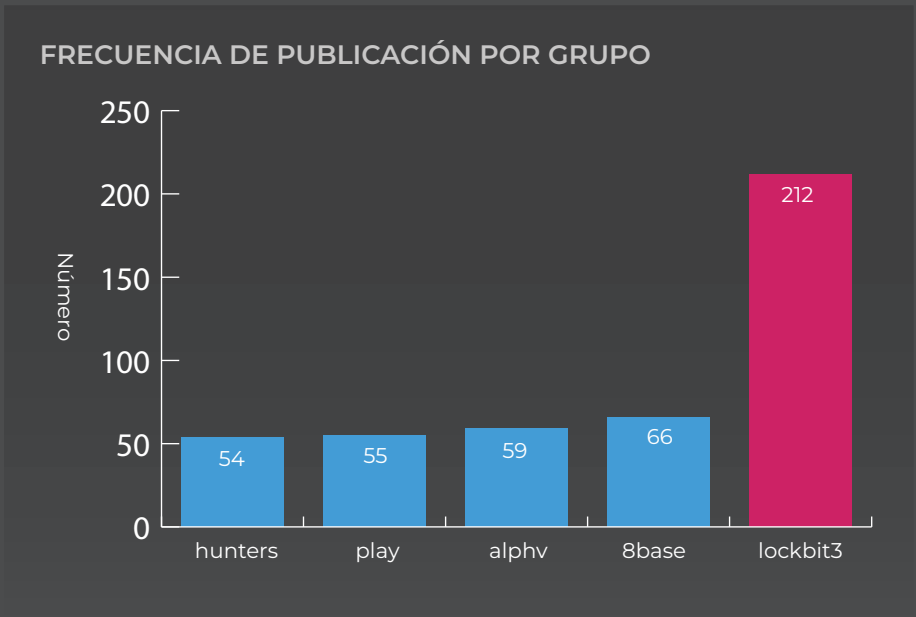
Grupos de ransomware activos

Muchas de las publicaciones agregadas de los sitios de filtraciones del primer trimestre de 2024 muestran signos de actividad. A veces, vemos que los sitios publican anuncios generales, pero la mayoría son "pruebas" de extorsiones o filtraciones de datos de la víctima. También suelen publicar una víctima varias veces, lo que puede provocar que se inflen las cifras porque se contará más de una vez en los datos.



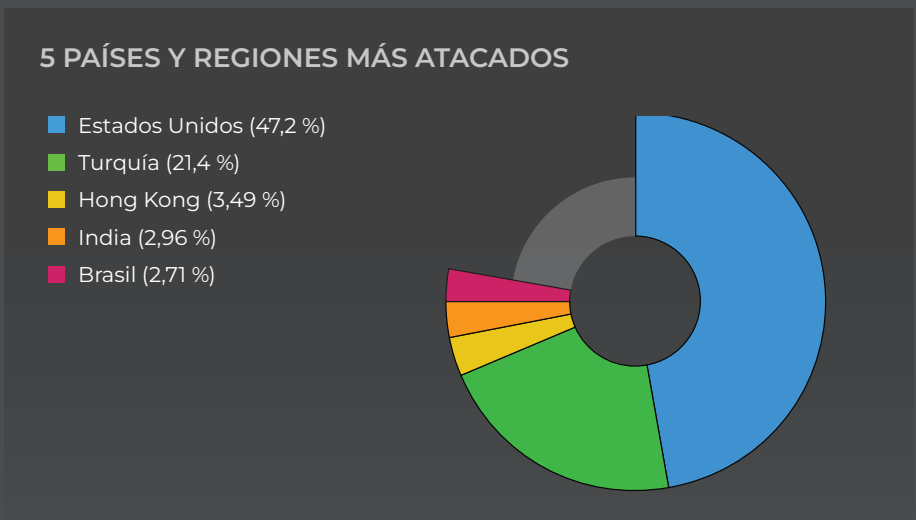
ÍNDICE

Cuando examinamos la frecuencia de los cinco sitios de filtraciones de bandas de ransomware activos, la actividad de LockBit destaca claramente en los gráficos. La actividad de las bandas, excluyendo a LockBit, es de una media de 50 publicaciones por trimestre, lo que significa que por término medio, transcurren menos de dos días entre la publicación de dos víctimas. Como se indicó anteriormente, estos números corresponden a las víctimas que no pagaron, lo que significa que el número real de víctimas es probablemente mayor, aunque no hay forma de determinar el número exacto.



Regiones y países atacados

Dada la actividad constante de las bandas de ransomware, podemos observar las detecciones de ransomware en la telemetría de Trellix. Estados Unidos genera la mayor parte de las detecciones, seguido de Turquía, Hong Kong, India y Brasil.



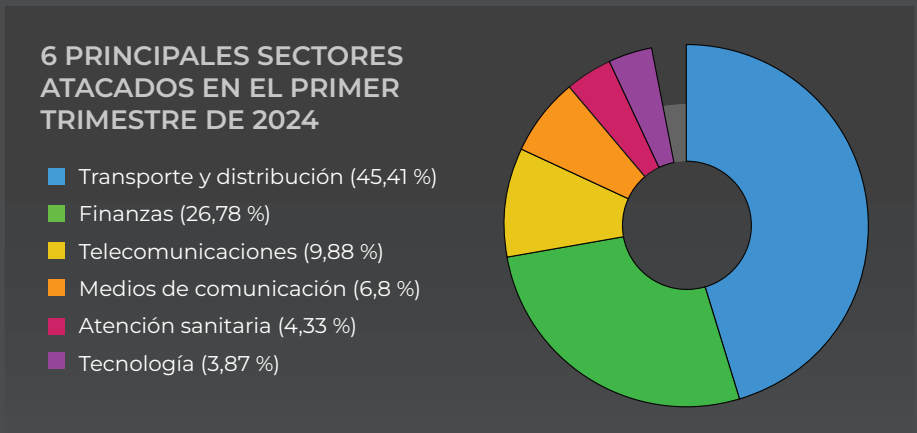
ÍNDICE

Puesto que el ransomware representa una amenaza para todos los sectores en prácticamente cualquier parte del mundo, las métricas de detección son representativas en relación con la base de clientes.

En el trimestre anterior, la telemetría era similar, excepto por el aumento de detecciones en India y China. No tenemos constancia de que hubiera una campaña específica contra estas regiones y sospechamos que el mayor número de detecciones en dichas áreas podría deberse a pruebas de malware.

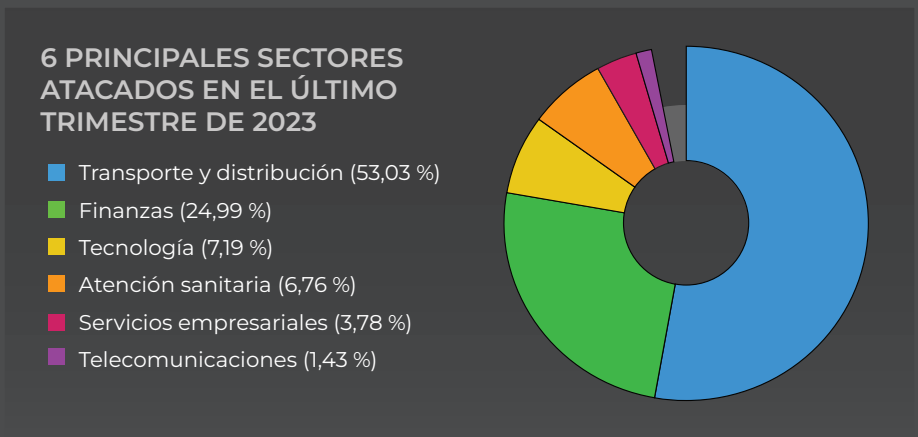
Sectores atacados

La agregación de la telemetría mundial por sector muestra que la mitad de las detecciones provienen del sector del transporte y la distribución (logística), y poco más de una cuarta parte proviene de los servicios financieros. Estos dos sectores acumulan más del 72 % de todas las detecciones, lo que no deja de ser lógico: la disponibilidad de sus servicios es de vital importancia. Si una empresa de transporte no puede operar debido a un ataque de ransomware que bloquea el movimiento de mercancías, podría sufrir enormes pérdidas económicas. De igual forma, sector financiero se basa en la confianza, y la filtración de datos confidenciales y/o la paralización de la actividad de la empresa debido a un ataque de ransomware, perjudican fundamentalmente a las empresas del sector.



Durante el último trimestre de 2023, los principales sectores atacados fueron ligeramente distintos, aunque sin diferencias en los dos primeros. Ambos fueron responsables de una proporción aún mayor, sumando un total combinado del 78 % de todas las detecciones durante el período mencionado. La incidencia en los sectores de la tecnología y la atención sanitaria disminuyó durante el primer trimestre de 2024 respecto al trimestre anterior, pero la diferencia en sí no puede atribuirse a uno o varios de estos incidentes específicos.

ÍNDICE



Herramientas y técnicas

Las última de las tres fuentes mencionadas son los informes públicos. Según los informes recopilados, pueden identificarse las técnicas MITRE, las herramientas asociadas y las líneas de comandos.

> **CONSEJO PARA LOS CISO:** los equipos azules de las organizaciones, responsables de la protección frente a ataques, pueden utilizar esta información desde una perspectiva de detección: al centrarse en las técnicas y herramientas más utilizadas, se pueden mitigar múltiples tipos de ataques de diferentes actores de amenazas, comenzando por los más eficaces. Asimismo, los ejercicios de los equipos de ataque y coordinación de defensa (red-teaming y purple teaming) pueden orientarse hacia estas técnicas para comprobar las medidas de detección en vigor.

La siguiente tabla muestra las técnicas más frecuentes, en orden descendente.

Técnicas MITRE ATT&CK	Campañas únicas
Datos cifrados por impacto	31
Descubrimiento de archivos y directorios	23
PowerShell	23
Transferencia de herramientas a la entrada	21
Descubrimiento de información del sistema	21
Ofuscación de archivos o información	19
Modificación del Registro	18
Windows Command Shell	17
Anulación de ocultación/descodificación de archivos o información	16
Parada del servicio	16

Debido al objetivo del ransomware, las técnicas de cifrado de datos y descubrimiento de archivos y directorios, se encuentran, como era de esperar, en los primeros lugares. La comparación de estas técnicas con

ÍNDICE

las más prevalentes del cuarto trimestre de 2023, revela que la mayoría de las principales técnicas en la lista son similares, aunque su posición específica puede variar.

Técnicas MITRE ATT&CK	Campañas únicas
Datos cifrados por impacto	45
PowerShell	29
Ofuscación de archivos o información	25
Descubrimiento de archivos y directorios	24
Windows Command Shell	24
Inhibición de la recuperación del sistema	23
Exploit de aplicaciones públicas	21
Transferencia de herramientas a la entrada	21
Descubrimiento de procesos	21
Parada del servicio	21

Al igual que en la sección anterior sobre las ATP, los ciberdelincuentes siguen aprovechando herramientas legítimas para sus actividades delictivas. Las herramientas utilizadas influyen en las técnicas observadas, en la medida en que una herramienta es un medio para un fin, que en este caso es una herramienta. Por ejemplo, PowerShell y Windows Command Shell se suelen utilizar para ejecutar comandos adicionales en el sistema, como la eliminación de instantáneas, que es el factor determinante de la técnica "Inhibición de la recuperación del sistema". Esta es también la razón por la que son las herramientas más utilizadas, como se muestra en la imagen siguiente.

Nombre de la herramienta de línea de comandos (attr)	Campañas únicas
Cmd	7
PowerShell	6
VSSAdmin	5
wevtutil	4
curl	4
Rundll32	4
reg	4
Schtasks.exe	3
BCDEdit	3
wget	2

ÍNDICE

El uso de VSSAdmin, BCDEdit, y wevtutil son indicios de que el ransomware se está asegurando de que el sistema de la víctima no pueda recuperarse a un estado normal, tal y como estaba antes del ataque. El uso de la herramienta reg muestra los cambios realizados en el Registro, que pueden realizarse por varias razones. El malware suele utilizar el Registro para asegurar la persistencia, pero al ransomware le da importancia, ya que su función concluye cuando finaliza el cifrado. En cambio, puede ajustar otras configuraciones para permitir ciertas acciones que de otro modo no serían posibles. Rundll32 se utiliza a menudo para cargar y ejecutar una DLL, pero también es blanco de inyección de procesos.

Al igual que en el trimestre anterior, PowerShell y el símbolo de comandos encabezan la lista precisamente por la misma razón. VSSAdmin y BCDEdit también están presentes, aunque la utilidad Windows Event Util (wevtutil) no se encuentra en la lista de principales herramientas. Dada la escasa presencia de todas las herramientas mencionadas, con una frecuencia máxima de 13 en cada uno de los trimestres, no sorprende que no todas las campañas utilicen las mismas herramientas . Una ligera variación puede dar lugar a la exclusión de esas herramientas.

Nombre de la herramienta de línea de comandos (attr)	Campañas únicas
PowerShell	13
Cmd	9
WMIC	6
Net	6
echo	5
VSSAdmin	4
msiexec	3
Schtasks.exe	3
Rundll32	3
BCDEdit	3

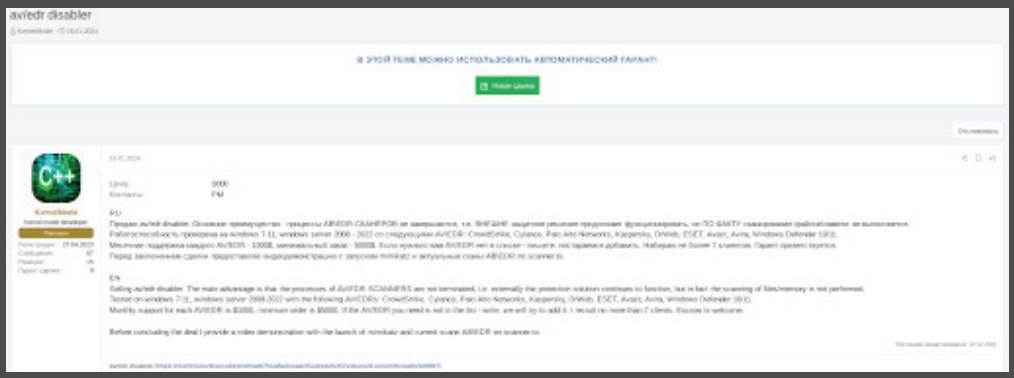
La amenaza del ransomware continúa.

ÍNDICE

La aparición de las herramientas de anulación y evasión de EDR

La adopción global de soluciones de detección y respuesta para endpoints (EDR) por parte de muchas organizaciones ha contribuido a mejorar la detección, comprensión y respuesta a más ataques sofisticados. Los ciberdelincuentes actuales suelen recurrir a técnicas LOLBin (archivos binarios que aprovechan recursos locales) y otros métodos de ataque más complejos, pero la presencia de tecnología EDR ha complicado a los atacantes sus esfuerzos por pasar desapercibidos.

La seguridad, sin embargo, sigue siendo una suerte de juego del ratón y el gato, y los ciberdelincuentes intentan encontrar formas de eludir o desactivar las soluciones EDR. Este fenómeno ha provocado el desarrollo de una gran cantidad de herramientas y técnicas destinadas a eludir y anular las herramientas EDR, algunas de las cuales se comercializan en los foros clandestinos de ciberdelincuentes. Hemos visto anteriormente, por ejemplo, que la banda de ransomware D0nut ha ganado notoriedad gracias a su herramienta de anulación de EDR.



Anuncio de anulación de herramienta de anulación de EDR en el foro clandestino XSS

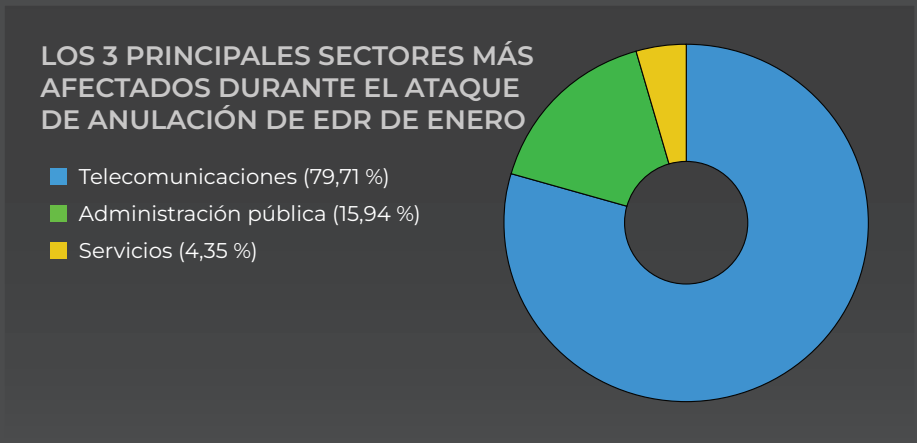
Campaña de enero que utilizaba la herramienta de Terminator de Spyboy

Una técnica habitual, bautizada como BYOVD (Bring Your Own Vulnerable Driver) consiste en explotar controladores vulnerables para ejecutar código con privilegios elevados.

Un ejemplo de este método es la herramienta de anulación de EDR "Terminator", desarrollada por el actor de amenazas llamado Spyboy. La herramienta "Terminator" aprovecha un controlador de Windows legítimo pero vulnerable que pertenece a la herramientas antimalware Zemana para ejecutar código arbitrario dentro del kernel de Windows probablemente explotando la vulnerabilidad CVE-2021-31728. Terminator apareció online a mediados de 2023 y Trellix publicó un artículo detallado en su base de datos de conocimientos sobre los productos afectados, que puede leerse aquí.

Del 11 al 17 de enero de 2023, el Trellix Advanced Research Center detectó un conjunto inusual de detecciones de Terminator de Spyboy en la telemetría de Trellix, lo que sugiere el lanzamiento de una nueva campaña. Esta campaña de Terminator alcanzó su punto máximo durante tres días y se detectó varias veces en un organismo gubernamental, una empresa de servicios públicos y una empresa de comunicaciones por satélite. Dado los objetivos específicos, Trellix considera con un alto nivel de confianza que el ataque está relacionado con el conflicto ruso-ucraniano.

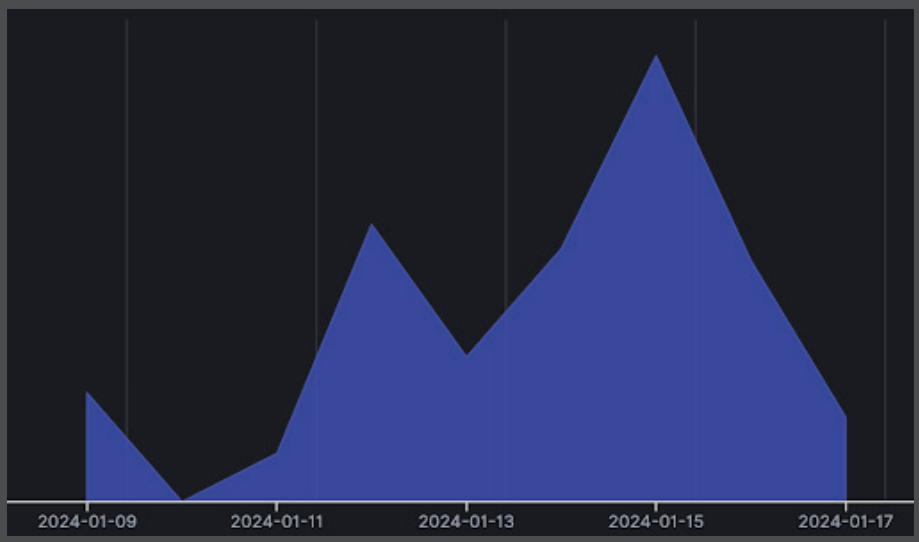
ÍNDICE



Detecciones de Trellix ATLAS de ataques contra Ucrania durante la campaña Terminator de enero

Proliferación de herramientas de anulación de EDR

A principios de 2023, Sophos describió una herramienta con un propósito similar: AuKill. También utilizaba un controlador vulnerable (BYOVD). Los controladores que se utilizaban en los casos de EDR Terrminator y AuKill son diferentes, pero ambos son inofensivos. Sin embargo, en algunas campañas de 2022 se emplearon herramientas similares con controladores maliciosos personalizados que había que cargar.



ÍNDICE

La explotación de controladores inofensivos para este fin complica la detección de estos ataques, y coincide con el uso de archivos LOLBin mencionado anteriormente. Aunque un archivo binario y un controlador son técnicamente distintos, la intención y las motivaciones son similares, sino idénticas. El malware HermeticWiper, aparecido en 2022, es otro ejemplo de uso de un controlador inofensivo. En ese caso, el controlador se utilizó para borrar una máquina, en lugar para desactivar el antivirus. Otra coincidencia entre la herramienta Terminator mencionada anteriormente, y HermeticWiper, es que ambos se atribuyen a un actor de amenazas proruso.

También hemos observado un ejemplo de uso de la red Discord para la distribución de malware en uno de nuestros clientes en Latinoamérica. Nuestro equipo ha observado que Discord sigue utilizándose de esta forma en ataques de malware.

> **CONSEJO PARA LOS CISO:** es absolutamente esencial que todos los SOC supervisen de cerca su solución EDR. Es necesario configurar alertas y registros para que, en caso de que se desactiven las herramientas EDR, se notifique al SOC inmediatamente y se actúe de manera adecuada. La desactivación de herramientas EDR puede ser un indicio de manipulación, y una respuesta rápida es clave para limitar el acceso del atacante a su red. También es de suma importancia utilizar una estrategia de defensa en profundidad, permitiendo que otras herramientas, como su plataforma de detección y respuesta para red (NDR), detecten posibles incidentes.

ÍNDICE

El correo electrónico sigue siendo terreno abonado para los ciberdelincuentes

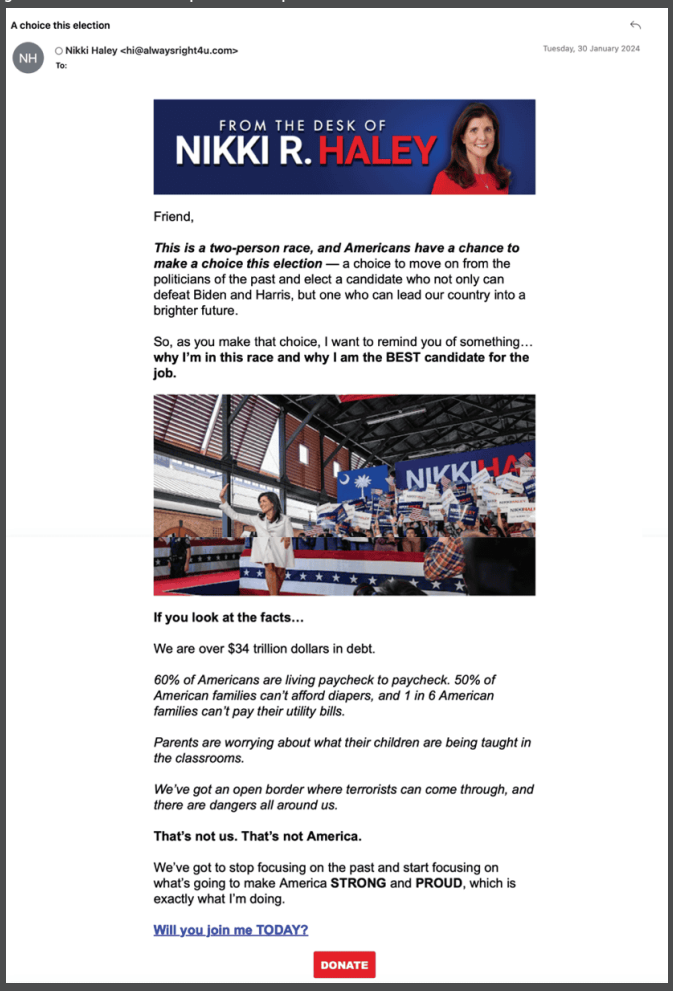
Trellix procesa 2000 millones de muestras de correo electrónico y 93 millones de adjuntos de correo electrónico al día. Esto genera una gran cantidad de datos y la posibilidad de identificar nuevas técnicas empleadas por los ciberdelincuentes que utilizan el correo electrónico como vector de ataque.

Estafas de donaciones electorales

Las estafas de phishing de donaciones electorales se aprovechan de la buena voluntad y el apoyo de los ciudadanos a los candidatos políticos aprovechando los sentimientos patrióticos y utilizando nombres de candidatos políticos conocidos. En el primer trimestre de 2024, nuestros investigadores descubrieron a ciberdelincuentes explotando servicios de marketing legítimos para crear páginas de donación convincentes, adornadas con imágenes de candidatos junto con banderas americanas, instando a los destinatarios a donar.

Estas estafas utilizan URL de servicios de marketing auténticos para engañar a los destinatarios, haciéndoles creer que los mensajes de correo electrónico son legítimos. Sin embargo, los mensajes se envían para aprovecharse de la generosidad de los ciudadanos. Los enlaces incluidos en los mensajes dirigen a los usuarios a páginas de donación, donde se les invita a introducir sus datos financieros o enviar contribuciones a las cuentas o direcciones de billeteras de los destinatarios.

Nuestros investigadores de correo electrónico observaron los siguientes mensajes maliciosos para supuestas donaciones electorales.



A choice this election

NH Nikki Haley <hi@alwaysright4u.com>
To:

Tuesday, 30 January 2024

FROM THE DESK OF
NIKKI R. HALEY

Friend,

This is a two-person race, and Americans have a chance to make a choice this election — a choice to move on from the politicians of the past and elect a candidate who not only can defeat Biden and Harris, but one who can lead our country into a brighter future.

So, as you make that choice, I want to remind you of something… **why I'm in this race and why I am the BEST candidate for the job.**

If you look at the facts…

We are over $34 trillion dollars in debt.

60% of Americans are living paycheck to paycheck. 50% of American families can't afford diapers, and 1 in 6 American families can't pay their utility bills.

Parents are worrying about what their children are being taught in the classrooms.

We've got an open border where terrorists can come through, and there are dangers all around us.

That's not us. That's not America.

We've got to stop focusing on the past and start focusing on what's going to make America **STRONG** and **PROUD**, which is exactly what I'm doing.

Will you join me TODAY?

DONATE

ÍNDICE

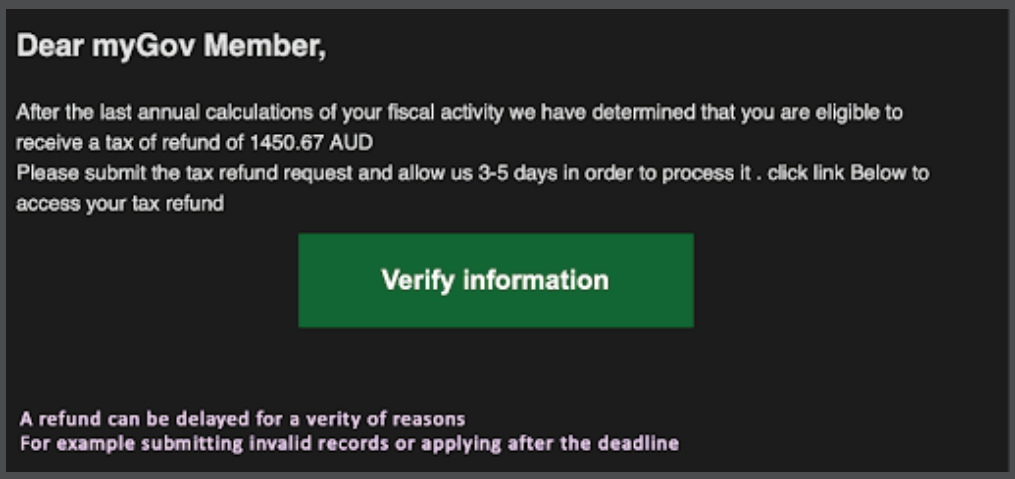
Phishing fiscal

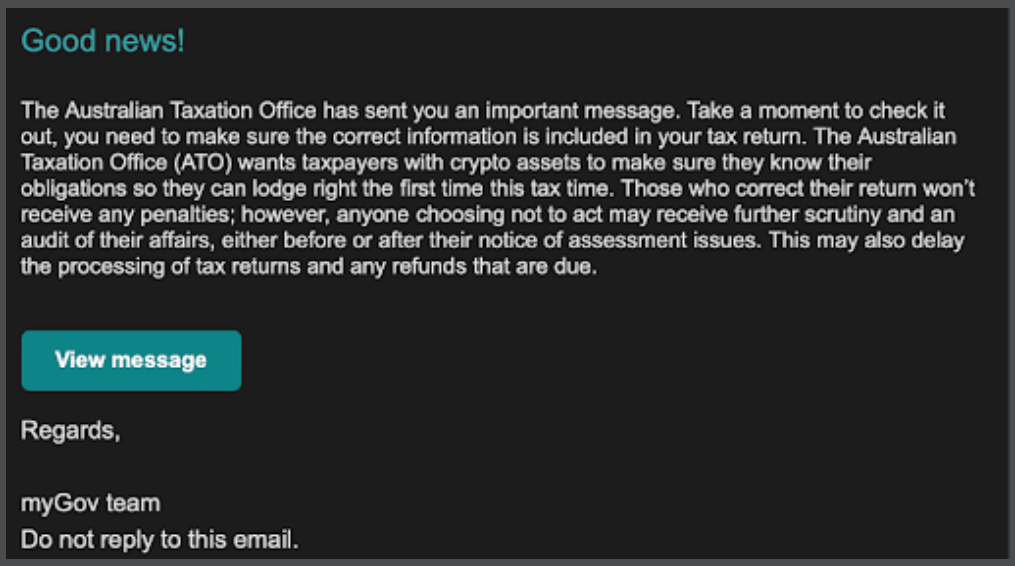
En el contexto de los impuestos, los ataques de phishing son especialmente preocupantes. Los estafadores se hacen pasar por agencias gubernamentales, autoridades fiscales o servicios de preparación de impuestos de buena reputación para engañar a las personas y conseguir que divulguen información personal. Es posible que usen como pretexto que debe impuestos atrasados, tiene declaraciones no presentadas o que le corresponde una devolución de impuestos. Su objetivo final es conseguir el número del documento nacional de identidad o los detalles de la cuenta bancaria, u otros datos valiosos. El mensaje contiene enlaces que parecen dirigir a sitios web oficiales de la administración o servicios fiscales, pero en realidad lo hacen a sitios fraudulentos diseñados para robar datos.

Trellix también observó un aumento de este tipo de mensajes supuestamente procedentes de la autoridad tributaria de Australia en el primer trimestre de 2024, y consiguió detectarlos correctamente.

ÍNDICE

A continuación puede ver una muestra de la campaña donde queda claro que los atacantes dan la sensación urgencia para convencer a los destinatarios a hacer clic en el enlace relacionado con el reembolso de impuestos.





La IA generativa protagonista de una carrera armamentística: hallazgos del submundo de la ciberdelincuencia

La inteligencia artificial y el aprendizaje automático han dejado de estar al alcance exclusivamente de los que tienen más dinero. ChatGPT y herramientas similares pueden ser utilizadas por cualquiera, incluidos los ciberdelincuentes: por eso la inteligencia artificial se ha convertido en una carrera armamentística entre ciberdelincuentes y profesionales de la seguridad. La IA es una herramienta poderosa y debe utilizarse de forma responsable para alcanzar los objetivos empresariales, pero es fundamental que las organizaciones no permitan que los atacantes ganen terreno. Debemos utilizar nuestras nuevas capacidades para superar a los ciberdelincuentes, a medida que sus tácticas se vuelven más precisas y sus armas más peligrosas.

ÍNDICE

CONSEJO PARA LOS CISO: la función de CISO ha adquirido incluso más importancia, ya que debe guiar a la empresa a través de este panorama en constante cambio. Con el incremento de los ciberataques, la creciente presión de la IA y el aumento de las responsabilidades, no sorprende que 90 % de los CISO se encuentre bajo una presión cada mayor. Seguir el ritmo de la IA y la IA generativa es esencial, y casi todos los CISO admiten que sus organizaciones podrían hacer más. Encontrará más información en el último informe de Trellix, Mind of the CISO: Decoding the GenAI Impact.

Los actores de amenazas adoptan la IA generativa por sus funciones de aprendizaje aceleradas y su coste asequible. Además, es extremadamente potente, ya que permite crear correos electrónicos de phishing en cualquier idioma, con una gramática impecable, logotipos y datos de acceso. Los ciberdelincuentes pueden encontrar, escribir y probar exploits 10 veces más rápido sin tener grandes conocimientos en la materia.

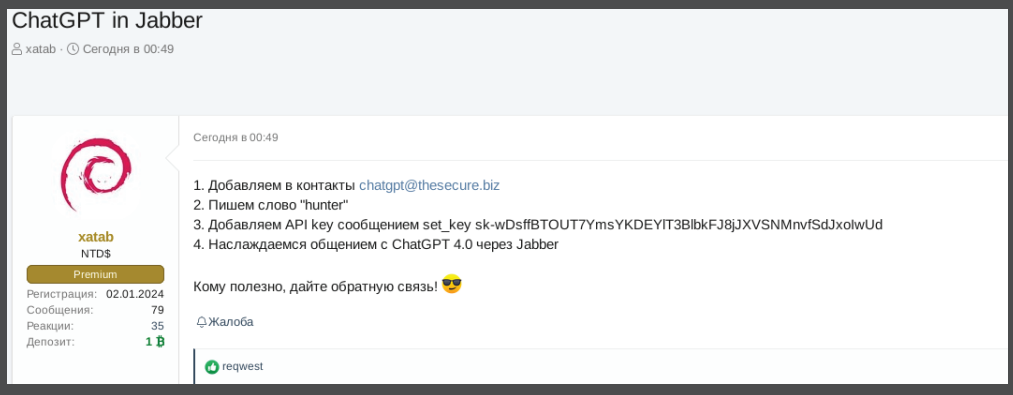
Nuestro equipo del Advanced Research Center investiga regularmente el submundo de la ciberdelincuencia para seguir las tendencias. La IA generativa está ganando terreno entre los ciberdelincuentes, que comparten su éxitos y vender sus herramientas. Desde nuestro último informe, hemos observado lo siguiente desde principios de 2024.

Proyecto "ChatGPT in Jabber", posiblemente utilizado por un grupo de APT ruso.

En enero, observamos a **xatab**, un actor maliciosos importante del foro clandestino XSS, buscando un desarrollador para crear un proyecto "ChatGPT 4.0 en Jabber", junto con una API e instrucciones sobre cómo utilizarlo.

Además de la adopción por parte de los ciberdelincuentes de las integraciones LLM, también es posible que la intención/motivación de **xatab** detrás del proyecto "ChatGPT in Jabber" sea interceptar y recopilar la correspondencia de los actores de amenazas, espiar sus solicitudes para conseguir inteligencia y conocimiento sobre lo que interesa a los ciberdelincuentes y cuáles son los principales temas y alcance de sus actividades ilícitas impulsadas por IA generativa.

Observamos lo siguiente:



Instrucciones y clave API del proyecto "ChatGPT in Jabber " compartidas por **xatab** en el foro XSS

ÍNDICE

```python
1. Add to your contacts chatgpt@thesecure.biz
2. Write a keyword "hunter"
3. Add API key in the message: set_key <OPENAI_API_KEY>
4. Enjoy the conversation with  ChatGPT 4.0 via Jabber

If useful share your feedback!
```

El 31 de enero de 2024, **xatab** ofreció 2000 dólares por su proyecto "ChatGPT in Jabber' en el foro XSS. Si creemos las alegaciones sobre XSS del ciberdelincuente **germans**, que había desarrollado el bot solicitado pero que fue inicialmente ignorado por **xatab**, parece que **germans** aceptó finalmente desarrollar un bot por 1500 dólares. El bot se creó para los servidores Jabber de los foros Exploit (@exploit[.]im) y XSS (@thesecure[.]biz), y fue publicado por **xatab** en los foros clandestinos Exploit y XSS, supuestamente para probarlo y recibir comentarios de los miembros del foro. El robot podría basarse en el proyecto xmppgpt.

En los mensajes publicados en los foros Exploit y XSS, **xatab** se presenta como un equipo de APT (conocidos en algunos círculos como especialistas en pruebas de penetración) interesado en contratar un agente de acceso a empresas de EE. UU./Reino Unido/Canadá/Australia para una colaboración fructífera. Ofreció pagar el 20 % de los ingresos generados por cada acceso y depositó un bitcoin en cada foro de Exploit y XSS para demostrar la seriedad de su oferta.

Ofreciendo una herramienta gratuita ChatGPT 4.0 a la comunidad de ciberdelincuentes, **xatab** consigue dos objetivos:

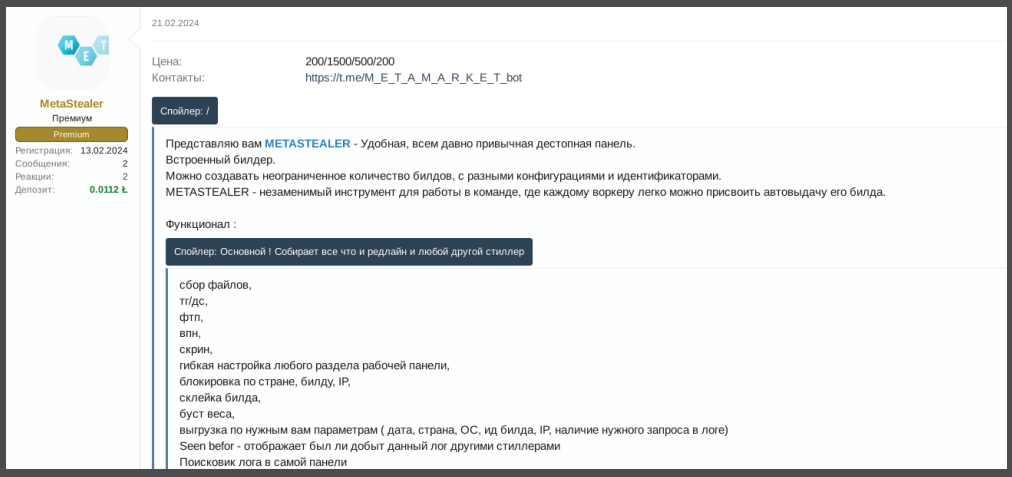
1. Actúa como catalizador y facilitador, deseoso de ayudar a los actores de amenazas a innovar y adoptar la IA generativa en sus operaciones.
2. Pretende crear un caldo de cultivo/base de conocimientos de IA generativa para beneficiarse de los conocimientos de otros ciberdelincuentes, o incluso apropiarse de sus ideas y herramientas innovadoras.

Trellix ha probado el proyecto "ChatGPT in Jabber" de acuerdo con las instrucciones proporcionadas , y parece que funciona según lo previsto por el actor de amenazas.

Integración de la IA generativa en los ladrones de información

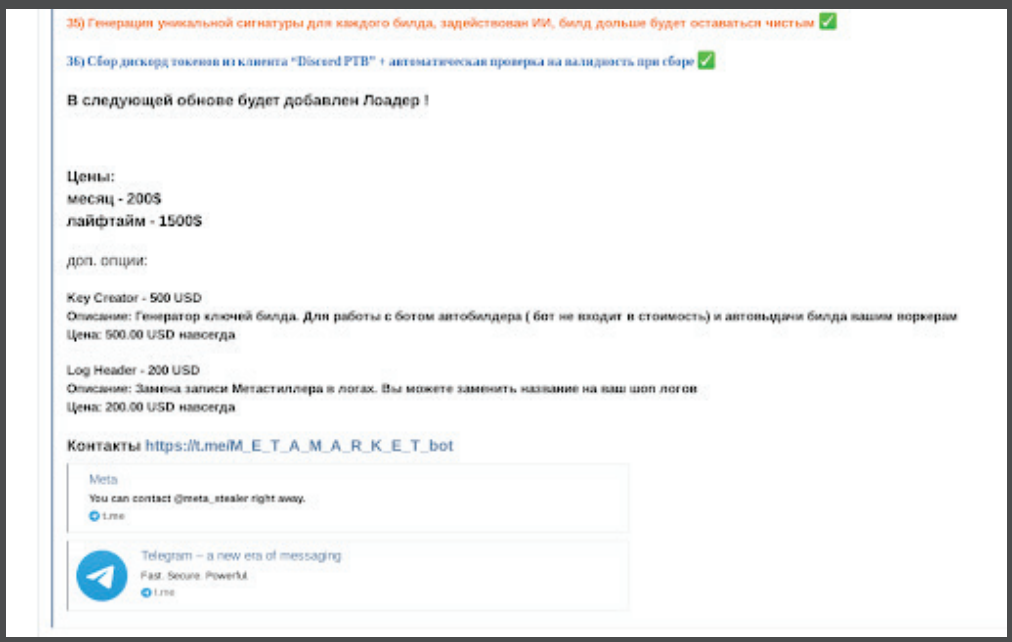
El 21 de febrero de 2024, el ciberdelincuente MetaStealer anunció una nueva versión renovada de **MetaStealer** en el foro XSS. MetaStealer es una herramienta para robar de información (infostealer) que apareció por primera vez en 2021; se cree que es una variante del célebre Redline. Se han observado muchas versiones de **MetaStealer** en entornos reales. Sin embargo, la n nueva versión identificada por Trellix cuenta con una función basada en IA generativa para eludir la detección.

ÍNDICE



Publicación de la versión mejorada de **MetaStealer** por el actor malicioso MetaStealer en el foro XSS

En la captura de pantalla siguiente, el texto naranja bajo el punto 35) significa "Generación de firmas únicas para cada compilación, se utiliza inteligencia artificial, la compilación permanece clara (o no detectada) durante más tiempo", lo que sugiere que los desarrolladores de MetaStealer incorporaron una nueva función basada en IA generativa en su programa para crear compilaciones únicas de MetaStealer, con el fin de evadir la detección y permanecer fuera del alcance de los sistemas de antivirus/detección y respuesta ante amenazas durante más tiempo.

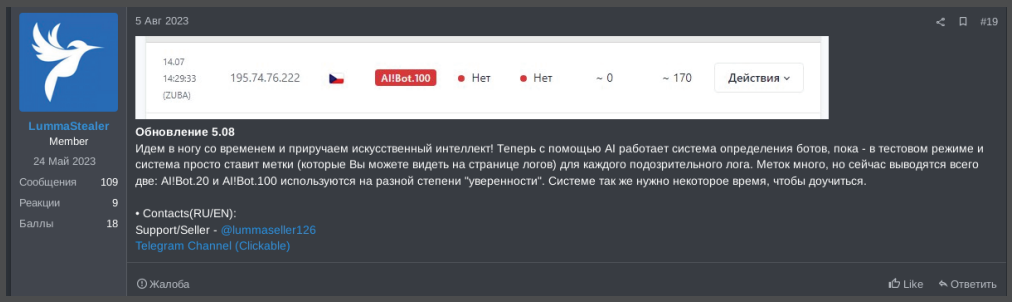


Integración de una función basada en IA generativa de la versión mejorada de MetaStealer para eludir defensas

Otro ejemplo es un ladrón de información arraigado LummaStealer. Desde agosto de 2023, hemos observado al equipo de LummaStealer probando una función basada en IA que permite a los usuarios de su ladrón de información detectar bots entre la lista de registros. El sistema basado en IA integrado en LummaStealer puede ser una red neuronal personalizada entrenada para detectar si un registro de usuario sospechoso es un bot o no. LummaStealer utiliza una etiqueta **AI!Bot.<número>** para clasificar el registro detectado como un bot.

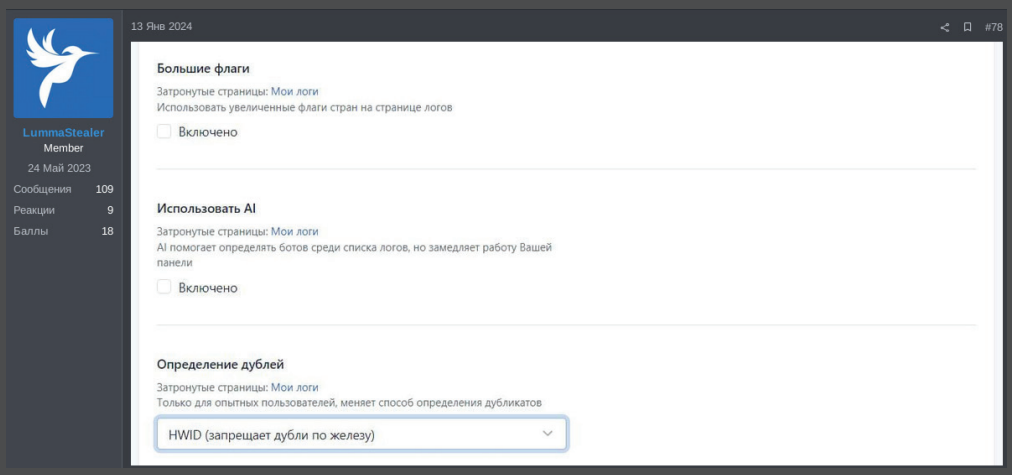
ÍNDICE

La variable <número>, cuyo rango parece estar entre 0 y 100, representa la certeza de detección de un bot:



Mensaje de LummaStealer en el foro RAMP en el que el actor de amenazas anuncia la integración de una función basada en IA para detectar bots en la lista de registros del ladrón de información.

LummaStealer anunció a sus usuarios que la red neuronal seguía en proceso de entrenamiento y que llevará tiempo mejorar la precisión en la detección. Además, en enero de 2024, **LummaStealer** informó que la función basada en IA generativa está desactivada de manera predeterminada ya que ralentiza el trabajo del panel de LummaStealer.

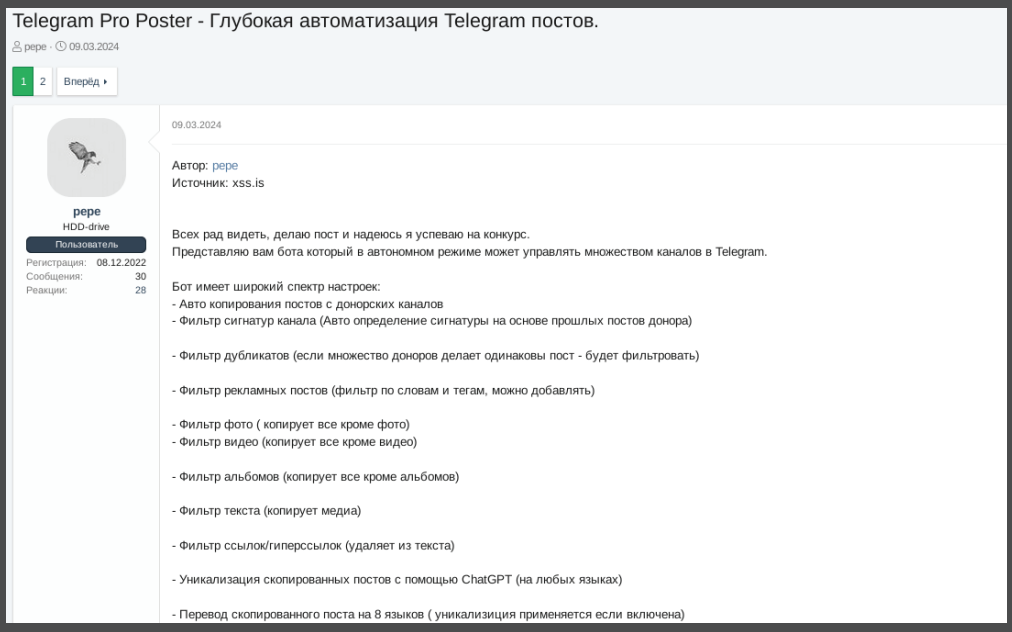


Mensaje de LummaStealer en el foro RAMP en el que el actor de amenazas informa de que la función de detección de bots está desactivada de forma predeterminada

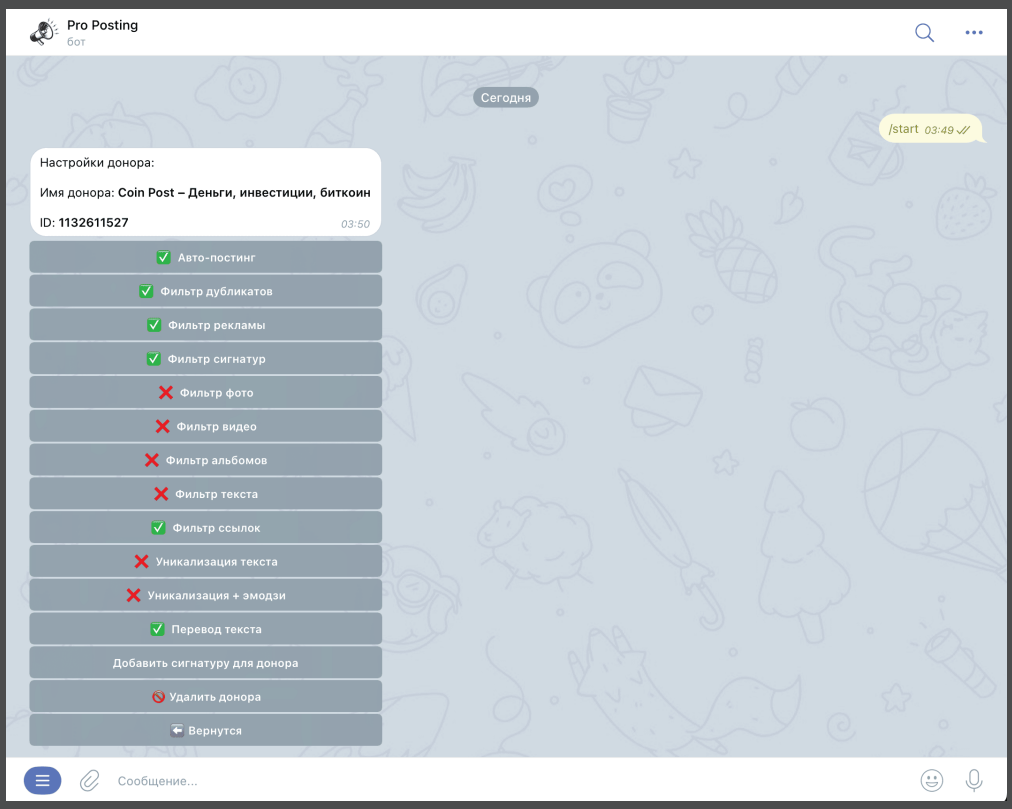
Proyecto "Telegram Pro Poster"

A principios de marzo de 2024, el ciberdelincuente pepe publicó su proyecto "Telegram Pro Poster " en el foro XSS como parte de un concurso de herramientas/software malicioso. Telegram Pro Poster es un bot destinado a "la automatización avanzada de los mensajes de Telegram". Este robot, desarrollado con Python, permite a los usuarios gestionar un gran número (o incluso ilimitado) de canales de Telegram de forma autónoma, copiando automáticamente los mensajes de los canales de Telegram "distribuidores" a los canales de destino. Entre sus muchas funciones de filtrado de mensajes, este robot tiene incorporadas dos funciones de IA generativa, diseñadas para traducir mensajes de Telegram y parafrasear un mensaje dado utilizando ChatGPT.

ÍNDICE



Mensaje en el foro XSS sobre el bot basado en IA generativa del proyecto "Telegram Pro Poster"



Funciones de filtrado de Telegram Pro Poster, incluida la función de personalización/paráfrasis, desactivad de manera predeterminada

Trellix ha obtenido el código fuente de la herramienta Telegram Pro Poster y ha identificado los segmentos de código que se indican a continuación, que son los responsables de traducir los mensajes copiados de los canales de los distribuidores a través de la API ChatGPT a los ocho idiomas indicados antes de enviarlos a los canales de Telegram de destino:

ÍNDICE

```
Unset
API_ID = 99999999 #APP TELEGRAM ID
API_HASH = "HASH" # APP TELEGRAM HASH
BOT_TOKEN = "API" # BOT API
DATABASE_PATH = 'database.db'
OPEN_AI_KEY = 'API KEY' # OPEN AI KEY


language_codes = {
    'Ukranian': 'украинский',
    'Russian': 'русский',
    'English': 'английский',
    'Indian': 'индийский',
    'Italian': 'итальянский',
    'Brasilian': 'бразильский',
    'Germany': 'немецкий',
    'Indonesian': 'индонезийский'
}
...
def gpt_translate(input_text, language):
    print(f'Перевожу этот текст: {input_text}')
    if len(input_text) > 10:
        openai.api_key = OPEN_AI_KEY
        language = language_codes[language]

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": f"Когда ты получаешь текст то ты
должен перевести его на {language}."},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        return unique_text
    else:
        return input_text
```

La segunda función, diseñada para personalizar el mensaje, está desactivada por defecto. Sin embargo, cuando está activada, utiliza OPEN_AI_KEY para solicitar a ChatGPT parafrasear el texto en el idioma deseado y, si es necesario, añadir un emoji.

```
Python
def unique_text(input_text, is_emoji_need):
    print(f'Уникализирую этот текст: {input_text}')
    if len(input_text) > 5:
        openai.api_key = OPEN_AI_KEY

        if is_emoji_need:
            content_text = "Перефразируй текст и добавь эмодзи: "
        else:
            content_text = "Перефразируй текст:"

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": content_text},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        token_count = response['usage']['total_tokens']
        return unique_text

    else:
        return input_text
```

ÍNDICE

Los comentarios de la comunidad de ciberdelincuentes XSS son muy positivos sobre el proyecto "Telegram Pro Poster", afirmando que es interesante y que, en las manos adecuadas, sin duda será útil. En un hilo del foro XSS, otro ciberdelincuente informó de que se había percatado de la adopción de este bot en varios canales de Telegram.

CONCLUSIONES

La carrera contrarreloj

La inteligencia sobre amenazas operativa proporciona información sobre la naturaleza, la intención y los periodos de actividad de ciberamenazas específicas. Es más detallada y contextual que la inteligencia sobre amenazas táctica, ya que proporciona información relevante sobre las tácticas, técnicas y procedimientos (TTP) utilizados por los ciberdelincuentes.

Las organizaciones pueden utilizar la inteligencia operativa para comprender el contexto general de los ciberataques, como las motivaciones o los métodos utilizados, lo que ayuda a los equipos de seguridad a anticiparse y prepararse para tipos específicos de ataque.

Mi trabajo con los clientes me ha demostrado que el objetivo primordial de un CISO es limitar el riesgo para su organización. El uso de inteligencia sobre amenazas operativa es una forma tangible de limitar este riesgo, ya que permite a los CISO y a sus equipos de SecOps anticiparse y sentar las bases necesarias. Les permite identificar las vulnerabilidades de sus medidas de seguridad en toda la superficie de ataque de la empresa y ponerse en la piel de sus adversarios para desestabilizarlos mejor.

Compartimos nuestra inteligencia sobre amenazas para ofrecerle una plataforma sólida y basada en hechos que respalde algunas de las decisiones más importantes que tomará. Nuestro propósito es ayudarle a mejorar sustancialmente sus capacidades de ciberdefensa e ir un paso por delante de los ciberdelincuentes.

¡Vamos!

Ashok Banerjee,
DIRECTOR DE TECNOLOGÍA, TRELLIX

ÍNDICE

METODOLOGÍA

Recopilación: los 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 de su propiedad.

Normalización: los datos agregados se introducen en nuestras plataformas Insights y ATLAS. Aprovechando el aprendizaje automático, la automatización y la agudeza humana, el equipo efectúa una serie de procesos intensivos, integrados e iterativos con el objetivo de normalizar los datos, analizar la información y desarrollar ideas relevantes para los responsables de la ciberseguridad y los equipos SecOps en primera línea de la ciberseguridad en todo el mundo.

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 responsables de ciberseguridad y a los equipos de que su SecOps a (1) conocer las últimas tendencias en el entorno de ciberamenazas, y (2) utilizar esta perspectiva para mejorar su capacidad para anticipar, prevenir y defender a su organización de ciberataques en el futuro.

Aplicación: cómo utilizar esta información

Es imperativo que todo equipo y en cualquier proceso de evaluación vanguardista se conozca, se admita y, en la medida de lo posible, se 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.

ÍNDICE

- 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.

Cómo entender el análisis de este informe

Para comprender los datos y conclusiones de este informe, es preciso tener en cuenta las siguientes consideraciones:

- **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 hay disponible 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 minimizar o eliminar los resultados de falsos positivos y negativos. De esta forma se eleva el nivel de análisis y la calidad de los 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.
- **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.

ÍNDICE

RECURSOS

Archivo de informes sobre amenazas

The Mind of the CISO

SIGA A TRELLIX ARC EN X

Trellix ARC

Ver archivo de informes sobre ciberamenazas

Trellix Advanced Research Center

ÍNDICE

ACERCA DEL TRELLIX ADVANCED RESEARCH CENTER

El Trellix Advanced Research Center está la vanguardia en cuanto a la investigación de nuevos métodos, tendencias y herramientas utilizados por los actores de amenazas en el panorama mundial de las ciberamenazas. Nuestro equipo de analistas de élite es el partner ideal para CISO, responsables de la seguridad y sus equipos de SecOps en todo el mundo. Trellix Advanced Research Center proporciona una inteligencia sobre amenazas operativa y estratégica de vanguardia a los analistas de seguridad. Impulsa nuestra plataforma XDR optimizada por IA, y ofrece productos y servicios de inteligencia sobre amenazas a nuestros clientes en todo el mundo. Más información en https://www.trellix.com/es-es/advanced-research-center.html.

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, aceleran las innovaciones tecnológicas mediante IA automatización y análisis, para reforzar la protección de más de 40 000 empresas privadas y clientes del sector público. Más información en https://trellix.com/es-es.

Trellix

ÍNDICE