Presentado por

Trellix ADVANCED RESEARCH CENTER

EL INFORME SOBRE AMENAZAS

Febrero de 2023

ÍNDICE

VISIÓN DE CONJUNTO DE LAS AMENAZAS, 4.° TRIMESTRE DE 2022

Durante los meses finales del año los ciberdelincuentes han demostrado una vez más ser un formidable adversario. Por su parte, el Trellix Advanced Research Center ha contraatacado dotando con todavía más recursos de inteligencia de amenazas a nuestro equipo formado por cientos de analistas e investigadores de seguridad de élite.

"En otras palabras: hemos llevado nuestra inteligencia de amenazas a otro nivel, para aportar serenidad al caos de sus equipos de SecOps con una protección más sencilla y para ofrecer mejores resultados de seguridad con menos estrés. Las amenazas siguen evolucionando. Y usted también puede avanzar".

En este informe, compartimos nuestra privilegiada visión sobre los ciberdelincuentes, familias, campañas y técnicas que despuntaron durante el último trimestre. Pero hay más. También hemos ampliado nuestras fuentes y ahora recogemos datos de sitios en los que se publican las filtraciones de ransomware, así como de informes del sector de la seguridad. Al mismo tiempo, también hemos aumentado las categorías de investigación de amenazas que ahora incluyen seguridad de redes, incidentes en la nube, incidentes de endpoints y operaciones de seguridad.

Desde nuestro último informe sobre amenazas, el Trellix Advanced Research Center ha participado en investigaciones y estudios en todo el mundo sobre aspectos como el vínculo entre Gamaredon y el enorme incremento de ciberataques contra Ucrania durante el cuarto trimestre, y la aplicación de parches a 61 000 proyectos de código abierto vulnerables, además de publicar su análisis de los ataques del nuevo año en el informe Predicciones de amenazas para 2022.

El siguiente resumen, que incorpora las mejoras del informe sobre amenazas, es un ejemplo de cómo el trabajo del Trellix Advanced Research Center permite a los clientes y al sector de la seguridad obtener un mejor resultado en la lucha contra las amenazas:

Ransomware

- Reveladoras investigaciones sobre la prominencia de LockBit 3.0, que es el grupo de ransomware que más impacto ha tenido en el cuarto trimestre.
- La continua prevalencia del ransomware en todo el mundo y, en especial, en Estados Unidos.
- Los sectores afectados por el ransomware, como el de bienes y servicios industriales.

Ataques auspiciados por Estados

- Sectores afectados por estos ataques, como los de Administración pública y transporte y distribución.
- Empresas con sede en Estados Unidos afectadas por actividad auspiciada por Estados.

Casos de aprovechamiento de recursos locales (LOLBin)

- Análisis más detallado de la actuación de Cobalt Strike en circulación, utilizando metodología de detección del Trellix Advanced Research Center.
- El gran número de servidores de Cobalt Strike Team que alojan proveedores de la nube chinos.
- Windows Command Shell se utiliza en las campañas denunciadas para ejecutar casi la mitad de los 10 principales archivos binarios del sistema operativo.

Ciberdelincuentes

- China, Corea del Norte y Rusia encabezan la lista de países en cuanto a origen de la ciberactividad.

Tendencias de la seguridad del correo electrónico

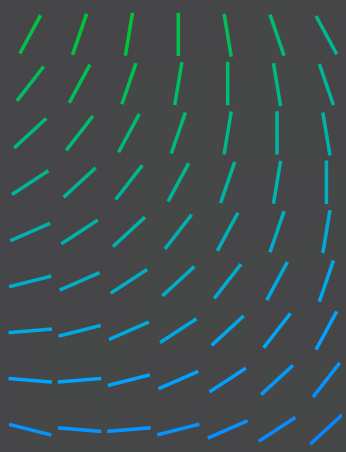
- El acusado incremento de mensajes maliciosos en países árabes observado durante el Mundial de fútbol.
- Análisis de las campañas de phishing y vishing, con información de las técnicas de suplantación y los temas habituales entre empresas que emplea el vishing.

Seguridad de redes

- Las webshells, herramientas y técnicas utilizadas, así como los ataques más relevantes, significativos y devastadores del trimestre.

Telemetría de operaciones de seguridad basada en Trellix XDR

- Alertas de seguridad, exploits, fuentes de registros y técnicas MITRE ATT&CK más destacadas
- Incidentes en la nube
- Técnicas y detecciones para Azure, AWS y GCP
- Principales técnicas y detecciones

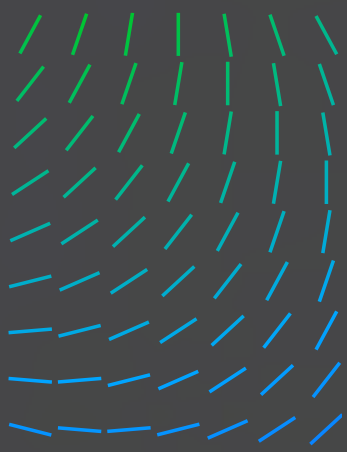


CARTA DE NUESTRO DIRECTOR DE INTELIGENCIA DE AMENAZAS

Nuestro equipo del Advanced Research Center tiene el placer de compartir los nuevos datos del informe de amenazas del 4.° trimestre de 2022, para cerrar el año. Se puede observar cómo evoluciona el informe, con la incorporación de nuevos datos procedentes de nuestros sensores de productos, combinados con análisis de otras fuentes, como los sitios de filtraciones de ransomware y nuestra infraestructura de seguimiento de ataques en circulación. En Trellix, seguimos firmes en nuestro propósito de proteger a nuestros clientes contra la ciberdelincuencia en un momento en el que los atacantes se muestran muy activos y son cada vez más multifacéticos. Ante el complicado panorama geopolítico y económico actual, y dada la inquietud que esto genera, se impone la necesidad de contar con inteligencia de amenazas a nivel mundial.

La incertidumbre financiera causada por la guerra de Ucrania ha provocado un enorme aumento del precio de la energía, que no se observaba desde los años 70, con consecuencias en todas las economías del planeta. El regreso de la guerra a Europa también ha sido utilizado como una llamada de atención por aquellos que se cuestionaban la estrategia de seguridad y defensa de la Unión Europea y su capacidad para defender sus intereses, en particular en el ciberespacio. La Administración estadounidense también ha reconocido la necesidad de abordar la competición geoestratégica, proteger las infraestructuras críticas y luchar contra la manipulación y la interferencia de otros países en la información. SolarWinds, Hafnium, la situación en Ucrania y otros eventos exigen una actuación conjunta de la Administración y el Congreso de Estados Unidos para implantar nuevas normas de seguridad y abordar la financiación de manera que se capitalice el compromiso y el trabajo realizado por gobiernos anteriores. ¿Cómo afecta esta incertidumbre a la ciberseguridad de nuestras empresas, nuestras instituciones públicas y privadas, y nuestros valores democráticos?

En el último trimestre, nuestro equipo observó ciberactividad a nivel de gobiernos, en las áreas de espionaje, estrategia militar y desinformación, al servicio de objetivos políticos, económicos y territoriales. La guerra de Ucrania ha sido escenario también de nuevas formas de ciberataques y los hacktivistas son cada vez más audaces a la hora de falsificar sitios, filtrar información y llevar a cabo ataques DDos. Por otro lado, los métodos tradicionales de ciberataque siguen vigentes. Se observan con frecuencia tácticas basadas en ingeniería social, como el phishing, para engañar y manipular al usuario con el objetivo de que divulgue información personal o confidencial.



Empresas de todo el mundo siguen sufriendo la plaga del ransomware. Como ocurrió durante la pandemia de COVID-19, los ciberdelincuentes no dudan en aprovechar los períodos de crisis e incertidumbre. Y, al igual que el panorama de las ciberamenazas, también avanzan nuestras investigaciones. Sin embargo, nuestro objetivo es siempre el mismo: mejorar sistemáticamente la eficacia de nuestros productos y proporcionar inteligencia práctica para garantizar que se pueda proteger lo que más importa. En este informe, podrá comprobar la importancia del trabajo que hacemos para todos los miembros del Trellix Advanced Research Center. Todos y cada uno de los investigadores y expertos que componen nuestro equipo ponen en nuestros proyectos todo su empeño y dedicación.

No dude en comunicarme sus impresiones sobre este informe completo y si considera que hay áreas que merecerían un análisis más detallado, contacte conmigo o con nuestro equipo @TrellixARC en Twitter. Esperamos verle en la conferencia RSA en San Francisco en abril.

John Fokker
Director de Inteligencia de amenazas

METODOLOGÍA

Los sistemas backend de Trellix proporcionan la telemetría que nos sirve como base para nuestros informes trimestrales de amenazas. Combinamos estos datos con inteligencia de acceso público sobre amenazas y con nuestras propias investigaciones sobre amenazas prevalentes, como el ransomware, la actividad auspiciada por Estados, etc.

Cuando hablamos de telemetría, nos referimos a datos relacionados con las detecciones, no a las infecciones. Una detección se registra cuando uno de nuestros productos detecta un archivo, URL, dirección IP u otro indicador y nos informa al respecto.

Por ejemplo, sabemos que cada vez más organizaciones aplican estrategias de comprobación de la eficacia que emplean muestras de malware reales. Esto aparecerá como una detección, pero sin duda, no es una infección.

El proceso para analizar y filtrar falsos positivos en telemetría está en continuo desarrollo, por lo que se pueden generar nuevas categorías de amenazas respecto a las ediciones anteriores.

Además, también se añadirán nuevas categorías cuando otros equipos de organizaciones de Trellix aporten sus datos a este informe trimestral.

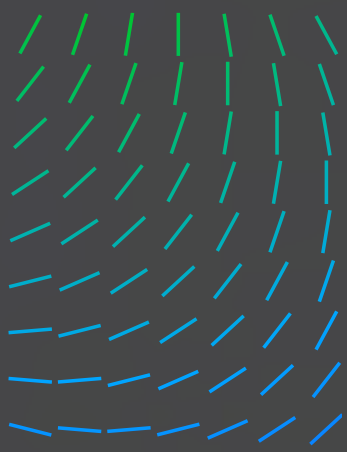
La privacidad de nuestros clientes es primordial, lo que es importante a la hora de generar datos de telemetría y asociar esta información a los sectores y países de nuestros clientes. Las bases de clientes por país varían y en ocasiones los incrementos requieren un examen más detenido de los datos. Un ejemplo: el sector de las telecomunicaciones a menudo presenta porcentajes elevados en nuestros datos. Sin embargo, esto no necesariamente significa que este sector reciba muchos ataques, ya que incluye también a los proveedores de servicios de Internet, que son propietarios de espacios de direcciones IP que las empresas pueden comprar. ¿Qué significa esto? Los envíos desde el espacio de direcciones IP del proveedor de servicios de Internet se muestran como detección del sector de las telecomunicaciones, pero podrían ser de clientes del proveedor que operan en un sector diferente.

RANSOMWARE, 4.° TRIMESTRE DE 2022

En esta sección ofrecemos la información que hemos recopilado sobre la actividad de los grupos de ransomware. Esta información se recopila de múltiples fuentes para obtener una imagen más clara y objetiva del panorama de las amenazas y nos ayuda a determinar qué familia de ransomware tuvo más impacto en el cuarto trimestre de 2022. La primera fuente es cuantitativa y representa estadísticas de campañas de ransomware extraídas de la correlación de indicadores de peligro (IoC) y telemetría de los clientes de Trellix. La segunda es cualitativa y muestra el análisis de varios informes publicados por el sector de la seguridad que han sido filtrados, analizados y depurados por el grupo de inteligencia de amenazas. Por último, la tercera fuente, que es una categoría nueva, incluye datos de víctimas del ransomware extraídos de distintos "sitios de filtraciones" de grupos de ransomware y posteriormente normalizados, completados y analizados para obtener una versión anonimizada de los resultados.

A través de estos diferentes puntos de vista pretendemos proporcionar muchas de las piezas del rompecabezas que compone el panorama de las amenazas actual. Por separado, cada uno presenta sus propias limitaciones y ninguno es suficiente. 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, combinando las distintas visiones se obtiene un mejor conocimiento de las distintas amenazas y, al mismo tiempo, se reducen los vacíos de información.

La conjunción de datos cuantitativos y cualitativos procedentes de distintas fuentes permite alcanzar una conclusión fundamentada, tomando en consideración los inconvenientes y carencias potenciales.



Datos sobre ransomware, 4.° trimestre de 2022

Grupo de ransomware con mayor impacto en el cuarto trimestre: LockBit 3.0

A través de la observación de las distintas fuentes que emplea Trellix, podemos concluir que LockBit 3.0 ha sido el grupo de ransomware con un mayor impacto en el cuarto trimestre de 2022. La destacada posición de LockBit 3.0 se basa en lo siguiente:

3.° LockBit 3.0 ocupó el tercer puesto entre los grupos de ransomware más prevalentes en el trimestre, según los análisis de telemetría de ransomware obtenidos de los sensores de Trellix en todo el mundo.

2.° LockBit 3.0 ocupa el segundo puesto, junto con el ransomware Cuba, entre los grupos de ransomware más denunciados por el sector de la seguridad, según los análisis de varias campañas obtenidos por el grupo de inteligencia de amenazas.

1.° El sitio de filtraciones de LockBit 3.0 es el que incluye más víctimas entre todos grupos de ransomware en este trimestre. LockBit ha sido el grupo que más ha presionado a las víctimas amenazándolas con exponer sus identidades con el correspondiente perjuicio para su reputación.

Estas son otras categorías de LockBit y conclusiones sobre el cuarto trimestre de 2022:

SECTORES AFECTADOS POR LOCKBIT 3.0, 4.° TRIMESTRE DE 2022

29 %

El sector de bienes y servicios industriales fue el más afectado por LockBit 3.0 en el cuarto trimestre de 2022, según el sitio de filtraciones de víctimas de LockBit 3.0.

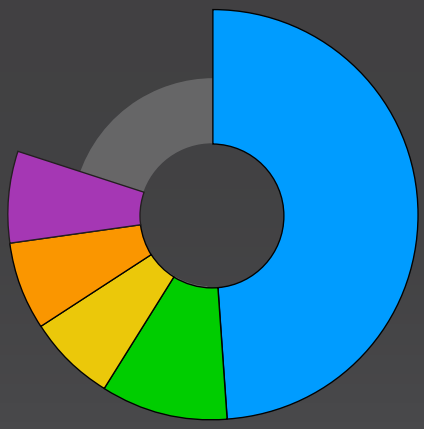
- Bienes y servicios industriales
- Comercio minorista
- Tecnología
- Atención sanitaria
- Construcción y materiales
- Artículos de uso personal y doméstico
- Administración pública

PAÍSES CON EMPRESAS AFECTADAS POR LOCKBIT 3.0, 4.° TRIMESTRE DE 2022

49 %

Las empresas de Estados Unidos fueron las más afectadas (49 %) por LockBit 3.0 en el cuarto trimestre de 2022, seguidas por las del Reino Unido, según el sitio de filtraciones de víctimas de LockBit 3.0.

- Estados Unidos
- Reino Unido
- Canadá
- Francia
- Brasil



Herramientas y exploits usados en LockBit 3.0

VULNERABILIDADES APROVECHADAS POR LOCKBIT 3.0

CVE-2018-13379
CVE-2020-0787
CVE-2021-20028
CVE-2021-34473
CVE-2021-34523

HERRAMIENTAS MALICIOSAS UTILIZADAS POR LOCKBIT 3.0

Amadey	Hakops
Blister	Neshta
BloodHound	SocGholish
Cobalt Strike	StealBit
Grabff	WinPEAS

HERRAMIENTAS NO MALICIOSAS UTILIZADAS POR LOCKBIT 3.0

BCDEdit	MiniDump	NSIS	Schtasks.exe
Cmd	MpCmdRun.exe	PCHunter	VSSAdmin
Fltmc.exe	Mshta	PowerShell	wevtutil
Fsutil	Mstsc	Process Monitor	WMIC
GMER	Netsh	Rundll32	RCLONE
MEGASYNC	Nltest		

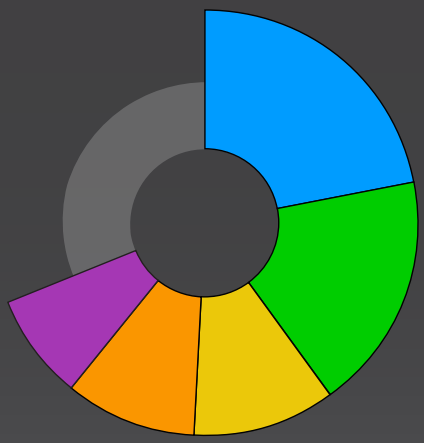
El ransomware observado a través de nuestra telemetría

Las siguientes estadísticas se basan en las correlaciones entre nuestra telemetría y nuestra base de conocimientos de inteligencia de amenazas. Tras una fase de análisis, identificamos un grupo de campañas a partir de los datos en el período de tiempo seleccionado y extraemos sus características. Las estadísticas mostradas corresponden a las campañas, no a las propias detecciones. Nuestra telemetría global mostró indicadores de peligro (IoC) que pertenecen a varias campañas de distintos grupos de ransomware. Las siguientes familias de ransomware, junto con sus respectivas herramientas y técnicas empleadas, son las más prevalentes en las campañas identificadas. Del mismo modo, los países y sectores que siguen son los más golpeados por las campañas identificadas.

FAMILIAS DE RANSOMWARE MÁS PREVALENTES, 4.° TRIMESTRE DE 2022

22 %

Cuba fue la familia de ransomware más prevalente en el cuarto trimestre de 2022. Zeppelin fue muy utilizada por Vice Society. Más información sobre las filtraciones de comunicaciones de Yanluowang



- Cuba
- Hive
- Lockbit
- Zeppelin
- Yanluowang

HERRAMIENTAS NO MALICIOSAS MÁS PREVALENTES UTILIZADAS POR GRUPOS DE RANSOMWARE, 4. TRIMESTRE DE 2022

41 %

Cobalt Strike fue la herramienta más prevalente utilizada por grupos de ransomware en el cuarto trimestre de 2022.

1.	Cobalt Strike	41 %
2.	Mimikatz	23 %
3.	BURNTCIGAR	13 %
4.	VMProtect	12 %
5.	POORTRY	11 %

TÉCNICAS MITRE-ATT&CK UTILIZADAS POR GRUPOS DE RANSOMWARE MÁS OBSERVADAS, 4.° TRIMESTRE DE 2022

1.	Cifrado de datos para causar daños	17 %
2.	Descubrimiento de información del sistema	11 %
3.	PowerShell	10 %
4.	Transferencia de herramientas a la entrada	10 %
5.	Windows Command Shell	9 %

HERRAMIENTAS NO MALICIOSAS MÁS PREVALENTES UTILIZADAS POR GRUPOS DE RANSOMWARE, 4. TRIMESTRE DE 2022

21 %

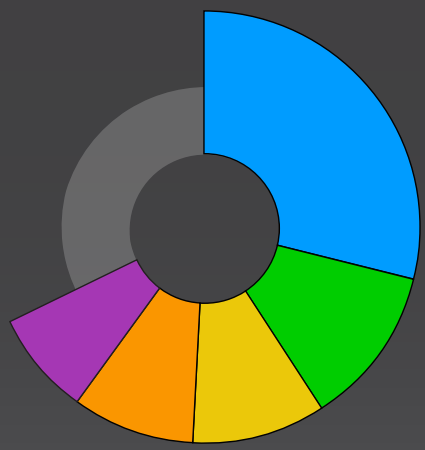
Cmd fue la herramienta no maliciosa más prevalente utilizada por grupos de ransomware en el cuarto trimestre de 2022.

1.	Cmd	21 %
2.	PowerShell	14 %
3.	Net	10 %
4.	Reg	8 %
5.	PsExec	8 %

PAÍSES MÁS AFECTADOS POR GRUPOS DE RANSOMWARE, 4.° TRIMESTRE DE 2022

29 %

Estados Unidos fue el país más afectado por el ransomware en el cuarto trimestre de 2022, según la telemetría de Trellix.

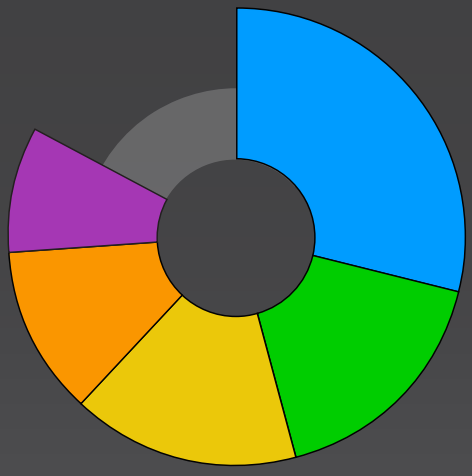


- Estados Unidos
- China
- Qatar
- Japón
- Indonesia

SECTORES MÁS AFECTADOS POR GRUPOS DE RANSOMWARE, 4.° TRIMESTRE DE 2022

29 %

El sector de externalización y alojamiento fue el más afectado por el ransomware en el cuarto trimestre de 2022, según la telemetría de Trellix. Esto guarda relación con el tamaño medio de la empresa de las víctimas incluidas en sitios de filtraciones de ransomware. Estas empresas no suelen tener un bloque de IP asignado y dependen de proveedores de alojamiento externos.



- Externalización y alojamiento
- Banca/finanzas/ administración del patrimonio
- Administración pública
- Distribución mayorista
- Industria farmacéutica

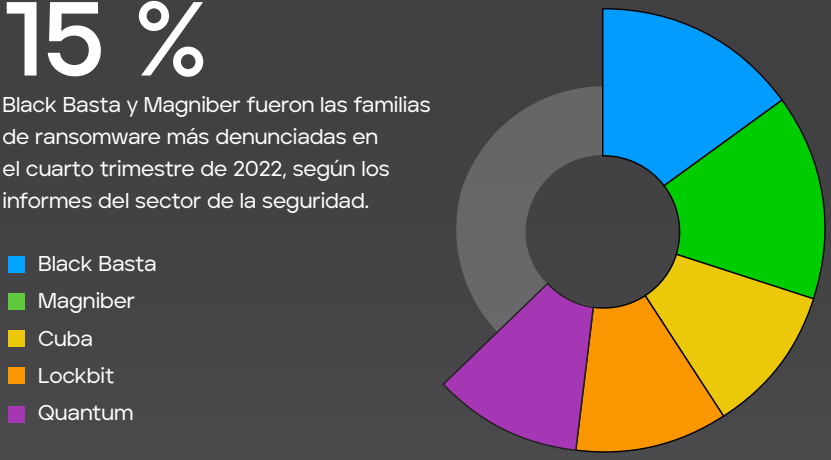
Ransomware denunciado por el sector de la seguridad

Las estadísticas siguientes se basan en informes públicos, así como en investigaciones realizadas internamente. Tenga en cuenta que no todos los incidentes de ransomware son denunciados. Muchas familias de ransomware ya llevan un tiempo activas y en determinados períodos obtienen menos atención que las familias nuevas. Según estos criterios, estos datos se refieren a las familias de ransomware que, según el sector de la seguridad, tuvieron más impacto y relevancia durante el trimestre.

FAMILIAS DE RANSOMWARE MÁS DENUNCIADAS, 4.° TRIMESTRE DE 2022

15 %

Black Basta y Magniber fueron las familias de ransomware más denunciadas en el cuarto trimestre de 2022, según los informes del sector de la seguridad.



PRINCIPALES TÉCNICAS DE ATAQUE POR FAMILIAS DE RANSOMWARE, 4. TRIMESTRE DE 2022

19 %

La técnica de ataque más denunciada en el cuarto trimestre de 2022 fue el cifrado de datos para causar daños, según los informes del sector de la seguridad.

1.	Cifrado de datos para causar daños	19 %
2.	Windows Command Shell	11 %
3.	Descubrimiento de información del sistema	10 %
4.	Transferencia de herramientas a la entrada	10 %
5.	PowerShell	10 %

PRINCIPALES SECTORES ATACADOS POR FAMILIAS DE RANSOMWARE, 4. ° TRIMESTRE DE 2022

16 %

El sector sanitario fue el más atacado por familias de ransomware en el cuarto trimestre de 2022, según los informes del sector de la seguridad.

- Atención sanitaria
- Finanzas
- Administración pública
- Fabricación
- Transporte

PAÍSES MÁS ATACADOS POR FAMILIAS DE RANSOMWARE, 4. ° TRIMESTRE DE 2022

19 %

Estados Unidos fue el país más atacado por familias de ransomware en el cuarto trimestre de 2022, según los informes del sector de la seguridad.

- Estados Unidos
- Alemania
- Brasil
- Argentina
- Canadá
- India
- Países Bajos
- Corea del Sur
- Suiza
- Reino Unido

CVE UTILIZADAS EN FAMILIAS DE RANSOMWARE, 4.° TRIMESTRE DE 2022

1.	CVE-2021-31207	16 %
	CVE-2021-34474	16 %
	CVE-2021-34523	16 %
2.	CVE-2021-34527	13 %
3.	CVE-2021-26855	9 %
	CVE-2021-27065	9 %

HERRAMIENTAS MALICIOSAS UTILIZADAS POR FAMILIAS DE RANSOMWARE, 4.° TRIMESTRE DE 2022

44 %

Cobalt Strike fue la herramienta maliciosa más utilizada por las familias de ransomware denunciadas en el cuarto trimestre de 2022, según los informes del sector de la seguridad.

1.	Cobalt Strike	44 %
2.	QakBot	13 %
3.	IcedID	9 %
4.	BURNTCIGAR	7 %
5.	Carbanak SystemBC	7 % 7 %

HERRAMIENTAS NO MALICIOSAS UTILIZADAS POR FAMILIAS DE RANSOMWARE, 4.° TRIMESTRE DE 2022

21 %

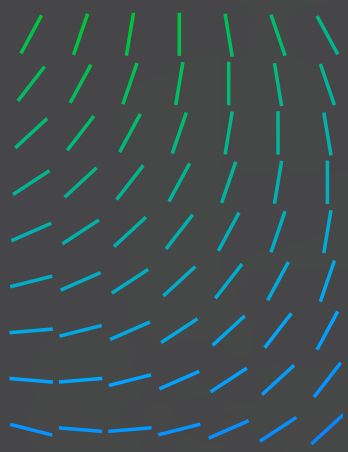
PowerShell fue la herramienta no maliciosa más utilizada por las familias de ransomware denunciadas en el cuarto trimestre de 2022, según los informes del sector de la seguridad.

1.	PowerShell	21 %
2.	Cmd	18 %
3.	Rundll32	11 %
4.	VSSAdmin	10 %
5.	WMIC	9 %

Víctimas en "sitios de filtraciones" de ransomware, 4.° trimestre de 2022

Los datos de esta sección se han recopilado a partir de "sitios de filtraciones" que utilizan los distintos grupos de ransomware para divulgar datos de sus víctimas. Estos grupos extorsionan a las víctimas publicando su información en estos sitios web. Cuando se estancan las negociaciones o las víctimas no acceden a pagar el rescate en la fecha tope que establece el grupo de ransomware, los ciberdelincuentes hacen pública la información que les han robado. Nosotros usamos la herramienta de código abierto RansomLook para obtener la información publicada y procesamos internamente los datos para normalizar y completar los resultados y ofrecer una versión anonimizada del análisis victimiológico.

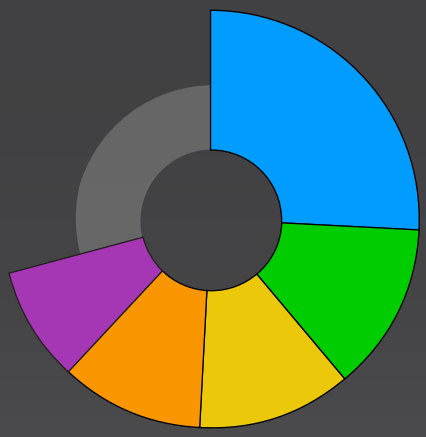
Es importante destacar que no todas las víctimas de ransomware aparecen en los sitios de filtraciones correspondientes. Muchas pagan el rescate y su información no se divulga. Estos datos reflejan las víctimas que han sufrido extorsiones o represalias por parte de los grupos de ransomware y no deben confundirse con la cantidad total de víctimas.



GRUPOS DE RANSOMWARE CON MÁS VÍCTIMAS, 4.° TRIMESTRE 2022

26 %

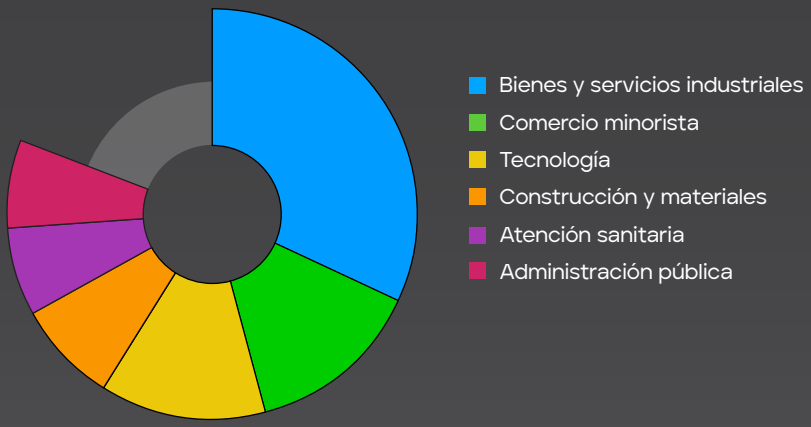
LockBit 3.0 representó el 26 % de los 10 principales grupos de ransomware con mayor número de víctimas según sus respectivos sitios de filtraciones, en el cuarto trimestre de 2022.



SECTORES AFECTADOS POR GRUPOS DE RANSOMWARE SEGÚN SUS SITIOS DE FILTRACIONES, 4.° TRIMESTRE DE 2022

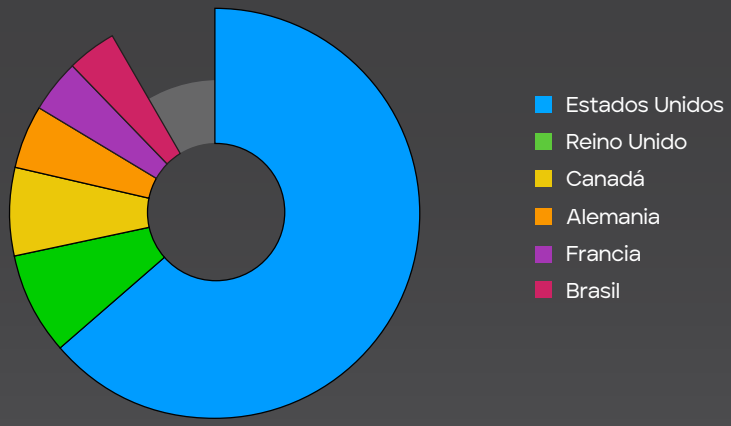
32 %

El sector de bienes y servicios industriales fue el más afectado por grupos de ransomware según sus sitios de filtraciones, en el cuarto trimestre de 2022. El sector de bienes y servicios industriales engloba todos los productos materiales y servicios intangibles que se emplean principalmente en construcción y fabricación.



PAÍSES DE EMPRESAS AFECTADAS POR GRUPOS DE RANSOMWARE SEGÚN SUS SITIOS DE FILTRACIONES, 4.° TRIMESTRE DE 2022

63 % de las 10 principales empresas mostradas por los grupos de ransomware en sus respectivos sitios de filtraciones en el cuarto trimestre de 2022 tienen sede en Estados Unidos, seguidas por las del Reino Unido (8 %) y Canadá (7 %).



ESTADÍSTICAS POR ESTADOS, 4.° TRIMESTRE DE 2022

Este apartado ofrece información recopilada sobre la actividad de los grupos patrocinados por Estados. Esta información se obtiene de múltiples fuentes con el fin de crear una imagen más precisa del panorama de las amenazas y reducir los sesgos en la observación. En primer lugar, representamos los datos extraídos al correlacionar los IoC de grupos relacionados con Estados con telemetría de clientes de Trellix. En segundo lugar, aportamos datos de los distintos informes publicados por el sector de la seguridad previamente filtrados, analizados y depurados por el grupo de inteligencia de amenazas.

Datos destacados de actividad auspiciada por Estados, 4.° trimestre de 2022

- Estados Unidos y Alemania experimentaron aumentos importantes en el número de ataques por Estados.
- China y Vietnam aparecen en el cuarto trimestre por vez primera para este tipo de ataques.

Estadísticas a nivel de Estados observadas a través de nuestra tecnología

Estas estadísticas se basan en las correlaciones entre nuestra telemetría y nuestra base de conocimientos de inteligencia de amenazas. Tras una fase de análisis, identificamos un grupo de campañas a partir de los datos en el período de tiempo seleccionado y extraemos sus características. Las estadísticas mostradas

corresponden a las campañas, no a las propias detecciones. Debido a que se agregan varios tipos de registros, al uso que hacen nuestros clientes de las estrategias de simulación de amenazas y al elevado nivel de correlaciones con la base de conocimientos de inteligencia de amenazas, los datos se filtran de forma manual para ajustarse a los criterios necesarios.

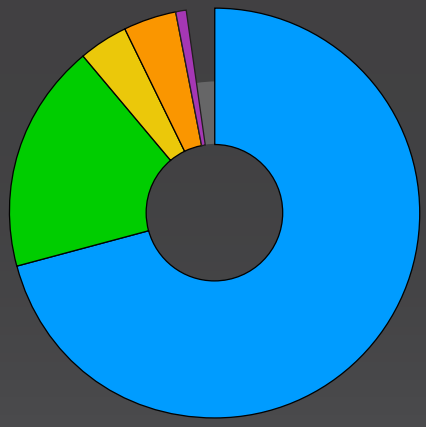
Nuestra telemetría global mostró indicadores de peligro (IoC) relacionados con varias campañas de grupos que emplean amenazas persistentes avanzadas (APT). Los siguientes países y ciberdelincuentes, junto con las herramientas y técnicas empleadas, son los más frecuentes en las campañas identificadas. Del mismo modo, los datos sobre los países y sectores equivalen a los más golpeados por las campañas identificadas

Datos de telemetría de actividad auspiciada por Estados

PAÍSES MÁS PREVALENTES EN CUANTO A CIBERACTIVIDAD AUSPICIADA POR ESTADOS, 4.° TRIMESTRE DE 2022

71 %

China fue el país más prevalente en cuanto a ciberactividad auspiciada por Estados en el cuarto trimestre de 2022.

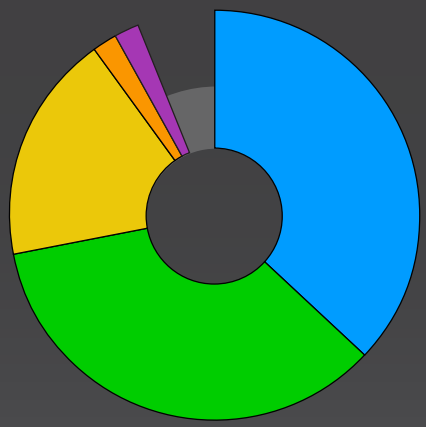


- China
- Corea del Norte
- Rusia
- Irán
- Líbano

GRUPOS DE CIBERATACANTES MÁS PREVALENTES, 4.° TRIMESTRE DE 2022

37 %

Mustang Panda fue el grupo de ciberatacantes más prevalente en el cuarto trimestre de 2022, según la telemetría de actividad auspiciada por Estados.



- Mustang Panda
- UNC4191
- Lazarus
- MuddyWater
- Kimsuky

TÉCNICAS MITRE ATT&CK MÁS PREVALENTES EMPLEADAS EN ACTIVIDAD RELACIONADA CON ESTADOS, 4.° TRIMESTRE DE 2022

1.	Carga lateral de DLL	14 %
2.	Rundll32	13 %
3.	Ofuscación de archivos o información	12 %
4.	Windows Command Shell	11 %
5.	Claves de ejecución del Registro/carpeta de inicio	10 %

HERRAMIENTAS MALICIOSAS MÁS PREVALENTES EMPLEADAS EN ACTIVIDAD RELACIONADA CON ESTADOS, 4.° TRIMESTRE DE 2022

1.	PlugX	24 %
2.	BLUEHAZE	23 %
3.	DARKDEW	23 %
4.	MISTCLOAK	23 %
5.	Troyano de acceso remoto JSX	2 %

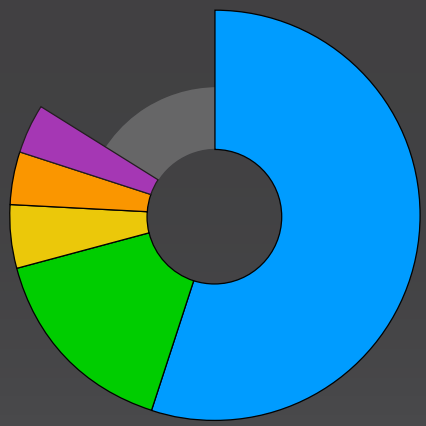
HERRAMIENTAS NO MALICIOSAS MÁS PREVALENTES EMPLEADAS EN ACTIVIDAD AUSPICIADA POR ESTADOS, 4.° TRIMESTRE DE 2022

1.	Rundll32	22 %
2.	Cmd	19 %
3.	Reg	17 %
4.	Ncat	12 %
5.	Regsvr32	6 %

PAÍSES MÁS AFECTADOS POR ACTIVIDAD AUSPICIADA POR ESTADOS, 4.° TRIMESTRE DE 2022

55 %

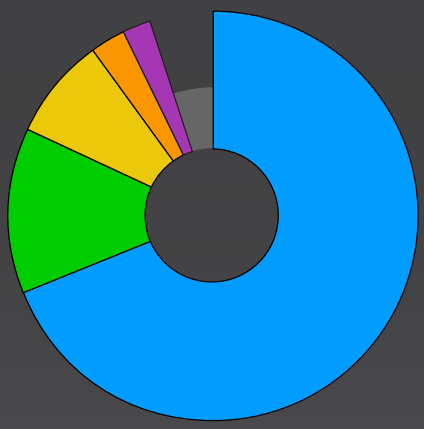
Estados Unidos fue el país más afectado por actividad auspiciada por Estados en el 4.° trimestre de 2022.



SECTORES MÁS AFECTADOS EN CUANTO A CIBERACTIVIDAD AUSPICIADA POR ESTADOS, 4.° TRIMESTRE DE 2022

69 %

El sector de transporte y distribución fue el más afectado en cuanto a ciberactividad auspiciada por Estados en el cuarto trimestre de 2022.



- Transporte y distribución
- Energía/Gas y petróleo
- Distribución mayorista
- Comercio minorista
- Banca/finanzas/ administración del patrimonio

Incidentes por Estados según informes públicos, 4.° trimestre de 2022

Estas estadísticas se basan en informes públicos y en investigaciones realizadas internamente; no proceden de telemetría de registros de los clientes. Tenga en cuenta que no todos los incidentes a nivel de Estados se comunican. Muchas campañas emplean las TTP conocidas y habituales y su divulgación es menos atractiva. La industria tiende a escoger las campañas más novedosas en las que el ciberdelincuente ha intentado algo nuevo o bien ha cometido un fallo. Estos datos son un indicador de lo que el sector ha considerado relevante y significativo durante el cuarto trimestre de 2022.

PAÍSES MÁS DENUNCIADOS EN CAMPAÑAS AUSPICIADAS POR ESTADOS, 4.° TRIMESTRE DE 2022

37 %

de las campañas auspiciadas por Estados denunciadas públicamente en el cuarto trimestre de 2022 se originaron en China.

1.	China	37 %
2.	Corea del Norte	24 %
3.	Irán	1 %
4.	Rusia	1 %
5.	India	1 %

CIBERDELINCUENTES MÁS PREVALENTES EN DENUNCIAS DE ACTIVIDAD AUSPICIADA POR ESTADOS, 4.° TRIMESTRE DE 2022

33 %

Lazarus fue el ciberdelincuente más prevalente en cuanto a actividad patrocinada por Estados en el cuarto trimestre de 2022.

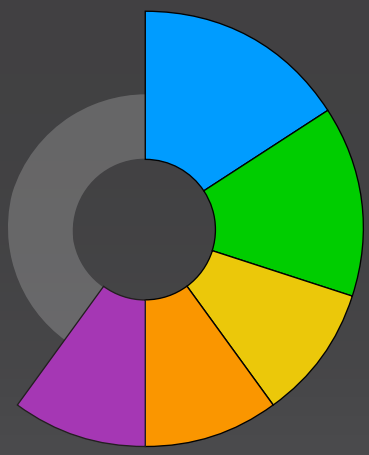
1.	Lazarus	33 %
2.	Mustang Panda	17 %
3.	APT34 APT37 APT41 COLDRIVER Patchwork Polonium SideWinder Winnti Group	cada uno un 1 %

PAÍSES MÁS ATACADOS EN CAMPAÑAS RELACIONADAS CON ESTADOS DENUNCIADAS, 4.° TRIMESTRE DE 2022

16 %

Estados Unidos fue el país más atacado en campañas auspiciadas por Estados denunciadas en el cuarto trimestre de 2022.

- Estados Unidos
- Reino Unido
- Pakistán
- Rusia
- Ucrania

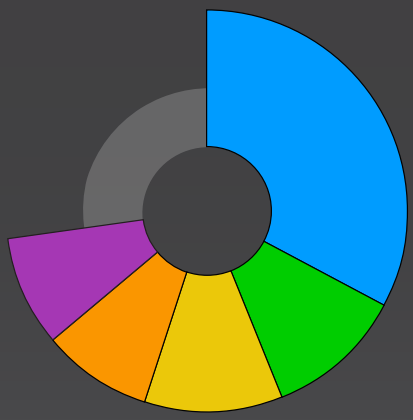


SECTORES MÁS ATACADOS EN CAMPAÑAS AUSPICIADAS POR ESTADOS, 4.° TRIMESTRE DE 2022

33 %

La Administración pública fue el sector más atacado en las campañas auspiciadas por Estados en el cuarto trimestre de 2022, seguido por el de Industria militar (11 %) y Telecomunicaciones (11 %).

- Administración pública
- Industria militar
- Telecomunicaciones
- Energía
- Finanzas



HERRAMIENTAS MALICIOSAS MÁS POPULARES EMPLEADAS EN CAMPAÑAS AUSPICIADAS POR ESTADOS, 4.° TRIMESTRE DE 2022

1.	PlugX	22 %
2.	Cobalt Strike	17 %
3.	Metasploit	13 %
4.	BlindingCan	9 %
5.	Scanbox ShadowPad ZeroCleare	cada uno un 9 %

HERRAMIENTAS NO MALICIOSAS MÁS POPULARES EMPLEADAS EN CAMPAÑAS AUSPICIADAS POR ESTADOS, 4.° TRIMESTRE DE 2022

1.	Cmd	32 %
2.	Rundll32	20 %
3.	PowerShell	14 %
4.	Reg	8 %
5.	Schtasks.exe	7 %

TÉCNICAS MITRE ATT&CK MÁS POPULARES EMPLEADAS EN CAMPAÑAS AUSPICIADAS POR ESTADOS, 4.° TRIMESTRE DE 2022

1.	Transferencia de herramientas a la entrada	13 %
2.	Descubrimiento de información del sistema	13 %
3.	Ofuscación de archivos o información	12 %
4.	Protocolos web	11 %
5.	Anulación de ocultación/descodificación de archivos o información	11 %

VULNERABILIDADES APROVECHADAS OBSERVADAS EN CAMPAÑAS AUSPICIADAS POR ESTADOS, 4.° TRIMESTRE DE 2022

CVE-2017-11882	CVE-2020-17143
CVE-2021-44228	CVE-2021-21551
CVE-2018-0802	CVE-2021-26606
CVE-2021-26855	CVE-2021-26857
CVE-2021-27065	CVE-2021-26858
CVE-2021-34473	CVE-2021-28480
CVE-2021-34523	CVE-2021-28481
CVE-2015-2545	CVE-2021-28482
CVE-2017-0144	CVE-2021-28483
CVE-2018-0798	CVE-2021-31196
CVE-2018-8581	CVE-2021-31207
CVE-2019-0604	CVE-2021-40444
CVE-2019-0708	CVE-2021-45046
CVE-2019-16098	CVE-2021-45105
CVE-2020-0688	CVE-2022-1040
CVE-2020-1380	CVE-2022-30190
CVE-2020-1472	CVE-2022-41128
CVE-2020-17141	

APROVECHAMIENTO DE RECURSOS LOCALES (LOLBIN) Y HERRAMIENTAS DE TERCEROS, 4.° TRIMESTRE DE 2022

Las observaciones y el seguimiento realizados a través de nuestra plataforma Trellix Insights Global Threat Intelligence nos han permitido recopilar la siguiente información sobre el panorama de amenazas durante el 4.° trimestre de 2022:

DATOS DESTACADOS SOBRE LOLBIN, 4.° TRIMESTRE DE 2022

- El aprovechamiento de recursos locales sigue jugando un papel importante en las etapas de un ataque: acceso inicial, ejecución, descubrimiento, persistencia e impacto.

- Los datos del 4.° trimestre de 2022 muestran una tendencia sostenida de técnicas de ejecución de comandos y scripts mediante Windows Command Shell o PowerShell.
- Su uso fue prevalente por parte de los ciberdelincuentes, incluidas las sofisticadas APT, los grupos con motivaciones financieras y los hacktivistas.

Los recién llegados, los ciberdelincuentes puntuales o los principiantes que irrumpen en el panorama de amenazas también hacen uso de archivos binarios ya presentes incorporados en infraestructuras de ataques populares, en su intento de pasar desapercibidos e infiltrarse en un sistema o aprovechar una vulnerabilidad.

Las técnicas de aprovechamiento de recursos locales siguen utilizándose en las fases de un ataque: acceso inicial, ejecución, descubrimiento, persistencia e impacto. Los datos del 4.° trimestre de 2022 muestran una tendencia sostenida de técnicas de ejecución de comandos y scripts mediante Windows Command Shell o PowerShell.

ARCHIVOS BINARIOS DEL SISTEMA OPERATIVO MÁS PREVALENTES, 4.° TRIMESTRE DE 2022

47 %

Windows Command Shell representó el 47 % (casi la mitad) de los 10 binarios del sistema operativo más prevalentes del 4.° trimestre de 2022, seguido de PowerShell (32 %) y Rundl32 (27 %).

1.	Windows Command Shell	47 %
2.	PowerShell	32 %
3.	Rundl32	27 %
4.	Schtasks	23 %
5.	WMI	21 %

El uso es prevalente entre los actores de amenazas, incluidas las sofisticadas APT, los grupos con motivaciones financieras y los hacktivistas.

Los eventos procesados a través de la plataforma Trellix Insights indican que los actores de amenazas utilizaron binarios de Windows para facilitar el despliegue de malware adicional, como un ladrón de información, un troyano de acceso remoto o ransomware. Archivos binarios como MSHTA, WMI o WScript pueden haberse ejecutado para recuperar cargas útiles adicionales de recursos controlados por el atacante.

PRINCIPALES HERRAMIENTAS DE TERCEROS, 4.° TRIMESTRE DE 2022

1.	Herramientas de acceso remoto	58 %
2.	Transferencia de archivos	22 %
3.	Herramientas posexplotación	20 %
4.	Descubrimiento de la red	16 %
5.	Descubrimiento de AD	10 %

Las herramientas de acceso remoto y control se encuentran sistemáticamente entre las más utilizadas por los actores de amenazas. Sin embargo, las herramientas que utilizan los profesionales de la seguridad siguen empleándose con fines maliciosos. Los actores de amenazas pueden utilizarlas para mantener balizas activas, automatizar la filtración o recopilar y comprimir la información perseguida.

Entre las herramientas gratuitas y de código abierto, los actores de amenazas utilizaron los empaquetadores de software para modificar el software legítimo e incluir malware con la intención de eludir las detecciones y dificultar el análisis.

DATOS DE COBALT STRIKE DEL 4.° TRIMESTRE DE 2022

El grupo de inteligencia sobre amenazas del Advanced Research Center supervisa el uso de los servidores del Cobalt Strike Team (Cobalt Strike C2) en entornos reales, mediante la combinación de metodologías detección de cargas útiles y caza de amenazas. Aquí presentamos las principales novedades identificadas durante el análisis de las balizas de Cobalt Strike recopiladas:

15 % LICENCIAS DE PRUEBA DE COBALT STRIKE

Solo el 15 % de las balizas de Cobalt Strike identificadas en circulación tenían una licencia de prueba de Cobalt Strike. Esta versión de Cobalt Strike incluye la mayoría de las funciones conocidas de esta infraestructura posexplotación. Sin embargo, añade "avisos" y elimina el cifrado en tránsito para facilitar a los productos de seguridad la detección de la carga útil.

87 % RUNDLL32.EXE

Rundll32.exe, el proceso predeterminado utilizado para crear las sesiones y ejecutar tareas posexplotación, se detectó en el 87 % de las balizas identificadas.

5 % ENCABEZADO HTTP DE HOST

Al menos el 5 % de las balizas de Cobalt Strike observadas utilizaban encabezado HTTP de host que facilita el *domain fronting* con Cobalt Strike. El Domain Fronting es una técnica que abusa de las redes de entrega de contenido (CDN, Content Delivery Networks) que albergan múltiples dominios. Los atacantes ocultan una solicitud HTTPS a un sitio web malicioso bajo una conexión TLS a un sitio web legítimo.

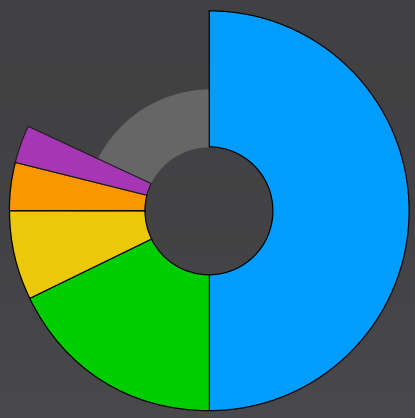
22 % BALIZAS DNS

Las balizas DNS representaron el 22 % de las balizas de Cobalt Strike identificadas. Este tipo de carga útil se comunica con el servidor de Cobalt Strike Team, que es un servidor autoritativo del dominio, a través de consultas DNS para ocultar su actividad.

PRINCIPALES PAÍSES QUE ALOJAN SERVIDORES DE COBALT STRIKE TEAM, 4.° TRIMESTRE DE 2022

50 %

La mitad de los servidores de Cobalt Strike Team detectados en el 4.° trimestre de 2022 se alojaban en China, sobre todo por el tamaño del alojamiento de nube disponible en este país.



GOOTLOADER, 4.° TRIMESTRE DE 2022

Gootloader es un malware modular que en ocasiones puede denominarse indistintamente como otro malware identificado como "GootKit" o "GootKit Loader". Las funciones modulares actuales del malware Gootloader se utilizan para distribuir cargas útiles de malware, como REvil, Kronos, Cobalt Strike e Icedid.

En incidentes recientes se ha observado a Gootloader utilizando la optimización de motores de búsqueda (SEO) para dirigir a usuarios desprevenidos a sitios web comprometidos o falsos utilizados para alojar un archivo comprimido con una carga útil de archivos de JS (JavaScript). Sin embargo, esta técnica requiere que el usuario abra el archivo y ejecute el contenido que a su vez ejecuta el código JS malicioso a través de Windows Scripting Host. Tras la ejecución, Gootloader iniciará comunicaciones de mando y control y recuperará malware adicional.

Gootloader es un presunto malware como servicio (MaaS) ofrecido a suscriptores, que permite a los actores de amenazas incorporar varias cargas útiles adicionales, por lo que supone una importante amenaza para los entornos empresariales.

A través de nuestro rastreador de Gootloader interno, hemos identificado una variante reciente, detectada en circulación el 18 de noviembre de 2022, y variantes antiguas que pasaron a estar inactivas el 13 de noviembre de 2022. Las modificaciones en las últimas variantes son las siguientes:

- Eliminación de la funcionalidad de manipulación del registro.
- Aumento de las solicitudes remotas de red a 10 URL en lugar de 3.

- Capacidad de invocar directamente scripts de PowerShell a través de CScript.
- Persistencia para cada inicio de sesión de usuario.

Nuestro proceso de rastreo de Gootloader

La nueva variante de Gootloader ha evolucionado empleando múltiples capas de ofuscación. Cada etapa anidada tras el desempaquetado utiliza variables cargadas de su etapa anterior, lo que complica más el análisis. Las muestras recopiladas obtenidas por nuestros esfuerzos de caza mediante reglas YARA se incorporan a un análisis estático de JavaScript y PowerShell para extraer los indicadores de peligro (IOC), como servidores de mando y control (C&C, C2) y firmas de ID exclusivas. Estos indicadores de peligro pueden utilizarse para identificar y rastrear instancias específicas de Gootloader en circulación.

Los indicadores de peligro de Gootloader extraídos se procesan entonces realizando una consulta en la base de datos del equipo de reputación de URL de Trellix para identificar cuáles son maliciosas, los dominios legítimos potencialmente comprometidos y los dominios legítimos que se utilizan como señuelos para obstaculizar el análisis.

Datos de telemetría de Gootloader

Las estadísticas que se muestran pertenecen a las campañas identificadas a partir de la correlación de los indicadores de peligro extraídos de los registros de nuestros clientes, no de las propias detecciones. En el caso de Gootloader, la mayoría de las detecciones se basan en resultados de dominios. Puesto que Gootloader utiliza dominios de señuelo, las estadísticas que se muestran podrían interpretarse como maliciosas con un nivel medio de confianza.

PAÍSES MÁS AFECTADOS POR GOOTLOADER, 4° TRIMESTRE DE 2022

37 %

Estados Unidos fue el país más afectado por Gootloader en el 4.° trimestre de 2022.

1.	Estados Unidos	37 %
2.	Italia	19 %
3.	India	11 %
4.	Indonesia	9 %
5.	Francia	5 %

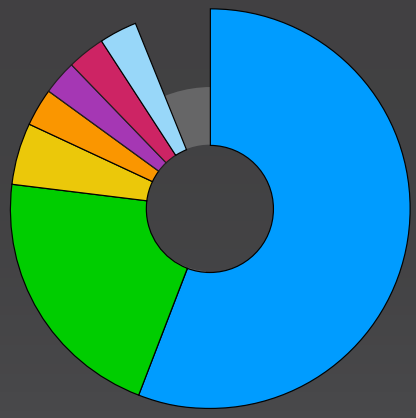
TÉCNICAS MITRE ATT&CK MÁS POPULARES EMPLEADAS POR GOOTLOADER, 4.° TRIMESTRE DE 2022

1. Desofuscación/ descodificación de archivos o información
2. JavaScript
3. Ofuscación de archivos o información
4. PowerShell
5. Vaciado del proceso

SECTORES MÁS AFECTADOS POR GOOTLOADER, 4° TRIMESTRE DE 2022

56 %

El sector de las telecomunicaciones fue el más afectado por Gootloader en el 4.° trimestre de 2022.



Técnicas MITRE ATT&CK más populares empleadas por Gootloader, 4.° trimestre de 2022

Desofuscación/descodificación de archivos o información
JavaScript
Ofuscación de archivos o información
PowerShell
Vaciado del proceso
Carga reflexiva de código
Claves de ejecución del Registro/carpeta de inicio
Rundll32
Tarea programada

INTELIGENCIA SOBRE VULNERABILIDADES, 4.° TRIMESTRE DE 2022

Nuestro panel de vulnerabilidades reúne el análisis de las últimas vulnerabilidades de gran impacto. El análisis y clasificación corre a cargo de los expertos en vulnerabilidades sectoriales del Trellix Advanced Research Center. Estos investigadores, especializados en ingeniería inversa y análisis de vulnerabilidades, supervisan permanentemente las últimas vulnerabilidades y el uso que hace de ellas los actores de amenazas en sus ataques, para ofrecer orientación sobre las medidas correctivas. Gracias al alto nivel técnico y precisión de las recomendaciones, puede separar el grano de la paja y centrarse en las vulnerabilidades de mayor impacto que pueden afectar a su organización, acelerando así la reacción.

DATOS DESTACADDOS DE INTELIGENCIA SOBRE VULNERABILIDADES, 4.° TRIMESTRE DE 2022

41 % Lanner representó el 41 % de los productos vulnerables y proveedores afectados por vulnerabilidades CVE únicas en el 4.° trimestre de 2022.

29 % IAC-AST2500A, versión de firmware 1.10.0 fue la CVE más utilizada por producto en el 4.° trimestre de 2022

PRODUCTOS VULNERABLES, PROVEEDORES Y CVE DE MAYOR IMPACTO, 4.° TRIMESTRE DE 2022

1.	Lanner	41 %
2.	Microsoft	19 %
3.	BOA	15 %
4.	Oracle	8 %
5.	Apple Chrome Citrix Fortinet Linux	5 % (cada una)

VULNERABILIDADES CVE POR PRODUCTO, 4.° TRIMESTRE DE 2022

29 %

IAC-AST2500A, versión de firmware 1.10.0 fue la vulnerabilidad CVE más utilizada por productos en el 4.° trimestre de 2022, seguida del servidor BOA (10 %), IAC-AST2500A (6 %) y Exchange (6 %).

Vulnerabilidades CVE por producto	CVE únicas
IAC-AST2500A, versión de firmware 1.10.0	9
Servidor BOA	3
Exchange	3
IAC-AST2500A	2
tvOS	1
iPadOS	1
iOS	1
Windows	1
Safari	1
SQLite hasta la versión 3.40.0 (incluida)	1
Oracle Access Manager, 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0	1
MacOS	1
Linux Kernel, anterior a la versión 5.15.61	1
Internet Explorer	1

Vulnerabilidades CVE por producto	CVE únicas
FortiOS (sslvpnd)	1
Citrix ADC/Citrix Gateway	1
Chrome, versiones anteriores a 108.0.5359.94/.95	1
Servidor BOA, BOA 0.94.13	1

VULNERABILIDADES CVE, 4.° TRIMESTRE DE 2022

CVE-2022-1786
CVE-2022-26134
CVE-2022-27510
CVE-2022-27518
CVE-2022-31685
CVE-2022-32917
CVE-2022-32932
CVE-2022-33679
CVE-2022-34718
CVE-2022-35737
CVE-2022-3602
CVE-2022-3786
CVE-2022-37958
CVE-2022-40684
CVE-2022-41040
CVE-2022-41080
CVE-2022-41082
CVE-2022-41128
CVE-2022-41352
CVE-2022-42468
CVE-2022-42475
CVE-2022-4262
CVE-2022-42856
CVE-2022-42889
CVE-2022-43995
CVE-2022-46908
CVE-2022-47939

TENDENCIAS DE SEGURIDAD DEL CORREO ELECTRÓNICO, 4.° TRIMESTRE DE 2022

Las estadísticas de seguridad del correo electrónico se basan en datos de telemetría generados de varios appliances de seguridad del correo electrónico desplegados en redes de clientes de todo el mundo. Los registros de las detecciones se agregaron y analizaron para generar las siguientes conclusiones:

TENDENCIAS DE SEGURIDAD DEL CORREO ELECTRÓNICO, 4.° TRIMESTRE DE 2022

100 % El volumen de mensajes de correo electrónico en países árabes descendió un 100 % en octubre, en comparación con los meses de agosto y septiembre.

40 % Qakbot fue la táctica de malware más utilizada, ya que representó el 40 % de las campañas dirigidas contra países árabes.

42 % El sector de las telecomunicaciones fue el más afectado por mensajes de correo electrónico maliciosos en el 4.° trimestre de 2022, el 42 % de las campañas de correo electrónico maliciosas dirigidas contra sectores concretos.

87 % Los mensajes de correo electrónico de phishing que utilizan URL maliciosas fue de manera destacada el vector de ataque más prevalente en el 4.° trimestre de 2022.

64 % Los casos de suplantación aumentaron un 64 % respecto al 3.er trimestre de 2022.

82 % de los mensajes de fraude del CEO se enviaron utilizando servicios de correo electrónico gratuitos.

78 % de los ataques Business Email Compromise (BEC) utilizaban frases habituales asociadas al CEO.

142 % Los ataques de vishing ocuparon un lugar destacado en el 4.° trimestre de 2022, con un aumento del 142 % respecto al trimestre anterior.

TÁCTICAS DE MALWARE DE CORREO ELECTRÓNICO MÁS PREVALENTES, 4. TRIMESTRE DE 2022

40 %

Qakbot fue la táctica de malware de correo electrónico más prevalente utilizada en el 4.° trimestre de 2022.

1.	Qakbot	40 %
2.	Emotet	26 %
3.	Formbook	26 %
4.	Remcos	4 %
5.	QuadAgent	4 %

PRODUCTOS Y MARCAS MÁS AFECTADAS POR PHISHING POR CORREO ELECTRÓNICO, 4.° TRIMESTRE DE 2022

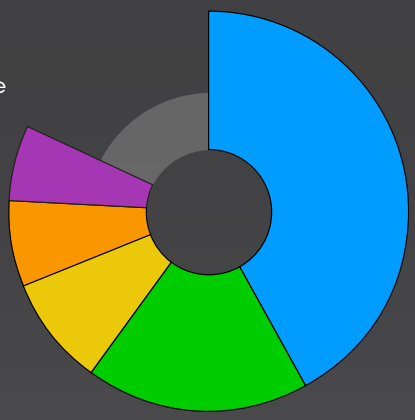
1.	Genéricos	62 %
2.	Outlook	13 %
3.	Microsoft	11 %
4.	Ekinet	8 %
5.	Cloudfare	3 %

SECTORES MÁS AFECTADOS POR MENSAJES DE CORREO ELECTRÓNICO MALICIOSOS, 4.° TRIMESTRE DE 2022

42 %

El sector de las telecomunicaciones fue el más afectado por correo electrónico malicioso en el 4.° trimestre de 2022.

- Telecomunicaciones
- Administración pública
- Educación
- Finanzas
- Servicios/Consultoría



TENDENCIAS DE SUPLANTACIÓN DEL CORREO ELECTRÓNICO, 4.° TRIMESTRE DE 2022

82 % de los mensajes de fraude del CEO se enviaron utilizando servicios de correo electrónico gratuitos.

78 % de los ataques Business Email Compromise (BEC) utilizaban frases habituales asociadas al CEO.

64 % de aumento de los mensajes maliciosos que suplantaban al CEO y otros líderes de las empresas entre el 3.er y el 4.° trimestre de 2022.

Principales frases del CEO utilizadas en ataques BEC en el 4.° trimestre de 2022:

"Necesito que me ayudes con algo inmediatamente".

"Necesito que hagas algo; por favor, envíame tu número de teléfono móvil".

"Envíame tu número de teléfono; hay algo urgente que necesito que hagas".

"Envíame tu número de móvil y mira el mensaje de texto que te voy a enviar. Necesito que hagas algo inmediatamente".

"Por favor, mira y confirma tu número de móvil y lee el mensaje con instrucciones que te voy a enviar".

"¿Recibiste mi mensaje de correo electrónico anterior? Tengo un negocio rentable que ofrecerte".

SUPLANTACIÓN (COMPARATIVA), 4.° TRIMESTRE DE 2022

64 % Los casos de suplantación aumentaron un 64 % respecto al 3.er trimestre de 2022

DATOS SOBRE CAMPAÑAS DE PHISHING, 4° TRIMESTRE DE 2022

Los proveedores de alojamiento web utilizados cada vez más para estafar y robar

En el 4.° trimestre, observamos un aumento del uso de proveedores de alojamiento web legítimos para estafar a los usuarios y robar las credenciales. Los tres proveedores de servicios más utilizados fueron: dweb.link, ipfs.link, translate.goog. También hemos observado importantes volúmenes de otros dominios de proveedores de servicios como ekinet, storageapi_fleek y selcdn.ru. Los ciberdelincuentes siguen utilizando proveedores de servicios nuevos y populares para alojar páginas de phishing y eludir los motores antiphishing. Una razón por la que los ciberdelincuentes han aumentado su interés en proveedores de alojamiento web legítimos: ningún sistema de detección puede incluir estos servicios en listas de bloqueo, ya que su principal objetivo es alojar archivos legítimos y compartir contenido.

VECTORES DE ATAQUE MÁS UTILIZADOS EN MENSAJES DE PHISHING

87 %

Los mensajes de correo electrónico de phishing que utilizan URL maliciosas fueron de largo el vector de ataque más prevalente en el 4.° trimestre de 2022.

1.	URL	87 %
2.	Adjuntos	7 %
3.	Encabezados	6 %

PROVEEDORES DE ALOJAMIENTO WEB MÁS ABUSADOS, 4.° TRIMESTRE DE 2022

154 %

Si bien Dweb fue el proveedor de alojamiento web más afectado en el 4.° trimestre de 2022, Google Translate experimentó el mayor aumento (154 %) entre el 3.er y el 4.° trimestre de 2022.

1.	Dweb	81 %
2.	Ipfs	17 %
3.	Google Translate	10 %

TÉCNICAS DE EVASIÓN MÁS UTILIZADAS EN ATAQUES DE PHISHING, 4.° TRIMESTRE DE 2022

63 %

La evasión basada en la redirección 302 fue la más prominente en el 4.° trimestre de 2022.

- Los ataques de phishing de evasión basados en geolocalización aumentaron de manera importante en el 4.° trimestre.
- Los ataques basados en captcha también aumentaron en el 4.° trimestre.

DATOS SOBRE VISHING, 4°. TRIMESTRE DE 2022

El vishing es otra forma de phishing, y está diseñado para inducir a las víctimas a interactuar con los atacantes, sobre todo mediante un mensaje de correo electrónico, de texto, una llamada de teléfono o mensajes de chat directo.

142 % Los ataques de vishing ocuparon un lugar destacado en el 4.° trimestre de 2022, con un aumento del 142 % respecto al trimestre anterior.

85 % Los servicios de correo electrónico gratuitos se han convertido en los favoritos entre los ciberdelincuentes que utilizan el vishing. Un alto porcentaje de los ataques de vishing del 4° trimestre de 2022 detectados (85 %) se enviaron a través de un servicio de correo electrónico gratuito.

Norton, McAfee, Geek Squad, Amazon y PayPal fueron los temas más populares utilizados en las campañas de vishing detectadas en el 4°. trimestre.

SEGURIDAD DE REDES, 4.° TRIMESTRE DE 2022

El equipo de investigación de Trellix ARC se centra en detectar y bloquear los ataques basados en la red que amenaza a nuestros clientes. Inspeccionamos distintas áreas de la cadena de ataque (*cyber kill chain*): reconocimiento, compromiso inicial, comunicación de mando y control, así como las tácticas, técnicas y procedimientos para el movimiento lateral. Nuestra capacidad para aprovechar al máximo nuestras tecnologías combinadas nos ofrece visibilidad para detectar mejor las amenazas desconocidas.

Técnicas MITRE ATT&CK más populares empleadas contra la seguridad de las redes, 4.° trimestre de 2022

- T1083 - Descubrimiento de archivos y directorios
- T1573 - Canal cifrado
- T1020 - Filtración automatizada
- T1210 - Aprovechamiento de servicios remotos
- T1569 - Servicios del sistema
- T1059 - Intérprete de comandos y scripts Windows Command Shell
- T1047 - Instrumental de administración de Windows
- T1087 - Descubrimiento de cuentas
- T1059 - Intérprete de comandos y scripts
- T1190 - Exploit de aplicaciones públicas

Ataques de mayor impacto en servicios externos, 4.° trimestre de 2022

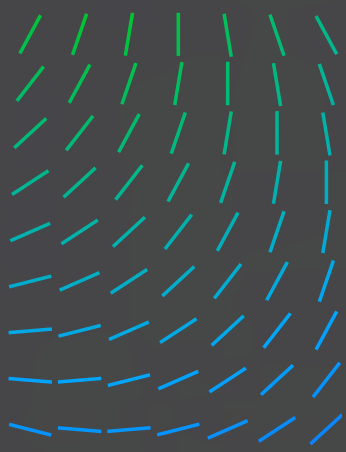
Realizamos a diario una gran cantidad de análisis de red para sondear las máquinas externas y buscar un umbral potencial en el entorno de un cliente. Los exploits antiguos buscan constantemente sistemas sin parches.

- Detección de intento de acceso al archivo /etc/passwd
- Posible ataque de scripting entre sitios
- Analizador de seguridad de SIPVicious
- Analizador de tráfico con Nmap detectado
- Actividad de análisis - Shellshock, sondeo de servidores web
- Ejecución remota de código Bash (Shellshock) HTTP CGI (CVE-2014-6278)
- Oracle WebLogic CVE-2020-14882, Vulnerabilidad de ejecución remota de código
- Intento transversal de directorios
- Inserción de secuencia de comandos OGNL ConversionErrorInterceptor en Apache Struts 2
- Ejecución remota de código CVE-2021-44228 en Log4j de Apache.

Las webshells más relevantes utilizadas como acceso inicial a la red, 4.° trimestre de 2022

Las siguientes webshells suelen utilizarse para intentar controlar un servidor web vulnerable.

- China Chopper
- JFolder
- ASPXSpy
- C99
- Tux
- B374K / Familia RootShell



Herramientas, técnicas y procedimientos más relevantes tras acceder a la red, 4.° trimestre de 2022

Las siguientes webshells suelen utilizarse para intentar controlar un servidor web vulnerable.

Hemos observado un gran volumen de herramientas, técnicas y procedimientos que utilizan los atacantes durante un movimiento lateral, incluido el empleo de vulnerabilidades y herramientas antiguas, como SCShell y PSExec.

- SCshell: movimiento lateral sin archivos usando el administrador de servicios
- Llamada a procedimiento remoto de WMI de Windows
- Invocación del shell de comandos a través de WMIEXEC en el protocolo SMB
- Exploit EternalBlue detectado
- Intento de aprovechar CVE-2020-0796, Microsoft SMBv3
- Ejecución remota de código CVE-2021-44228 - Log4j de Apache
- Enumeración remota de cuentas de administración de empresa/dominios
- Acceso remoto a PowerShell sospechoso
- Reconocimiento de red sospechoso mediante WMIC
- Comando de enumeración detectado en archivo por lotes
- Actividad PsExec en SMB

TELEMETRÍA DE OPERACIONES DE SEGURIDAD BASADA EN TRELLIX XDR

Estas estadísticas se apoyan en telemetría generada de distintos sensores de nuestra base de clientes. Los registros de las detecciones se agregan y se analizan para elaborar las siguientes secciones:

Incidentes de seguridad de mayor impacto, 4.° trimestre de 2022

A continuación se muestran las alertas de seguridad más prevalentes del 4.° trimestre de 2022:

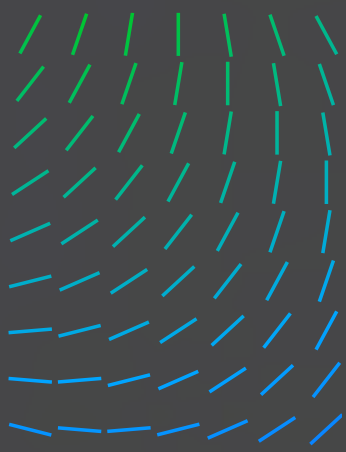
EXPLOIT - LOG4J [CVE-2021-44228]

OFFICE 365 ANALYTICS [Inicio de sesión anormal]

OFFICE 365 [Ataque de phishing permitido]

EXPLOIT - FORTINET [CVE-2022-40684]

EXPLOIT - APACHE SERVER [CVE-2021-41773 - Intento]



WINDOWS ANALYTICS [Ataque por fuerza bruta]

EXPLOIT - ATLASSIAN CONFLUENCE [CVE-2022-26134]

EXPLOIT - F5 BIG-IP [CVE-2022-1388 - Intento]

TÉCNICAS MITRE ATT&CK MÁS UTILIZADAS, 4.° TRIMESTRE DE 2022

1.	Explotación de aplicaciones públicas (T1190)	29 %
2.	Protocolo de capa de aplicaciones: DNS (T1071.004) Phishing (T1566)	14 % 14 %
3.	Manipulación de cuentas (T1098.001) Fuerza bruta (T1110) Compromiso por descarga desapercibida (T1189) Ejecución por usuario: Archivo malicioso (T1204.002) Cuentas válidas: Cuentas locales T1078,003)	7 % cada una

DISTRIBUCIÓN DE LOS PRINCIPALES ORÍGENES DE REGISTROS, 4.° TRIMESTRE DE 2022

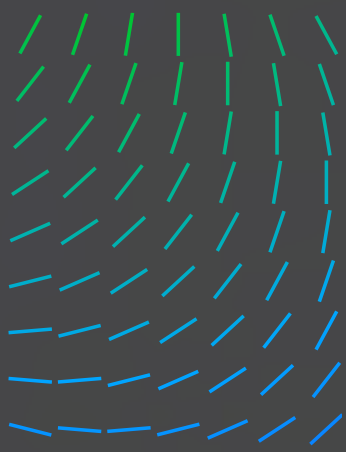
1.	Red	40 %
2.	Correo electrónico	27 %
3.	Endpoint	27 %
4.	Firewall	6 %

EXPLOITS OBSERVADOS EN EL 4.° TRIMESTRE DE 2022

EXPLOITS MÁS PREVALENTES OBSERVADOS, 4.° TRIMESTRE DE 2022

30 % Log4j fue el exploit más prevalente observado en el 4.° trimestre de 2022.

1.	Log4j (CVE-2021-44228)	30 %
2.	Fortinet (CVE-2022-40684)	16 %
3.	Servidor Apache (CVE-2021-41773)	15 %
4.	Atlassian Confluence (CVE-2022-26134)	14 %
5.	F5 BIG- IP (CVE-2022-1388 - Intento]	13 %
6.	Microsoft Exchange (intento de exploit de ProxyShell)	11 %



INCIDENTES EN LA NUBE EN EL 4.° TRIMESTRE DE 2022

Los ataques contra la infraestructura de nube no dejan de aumentar en una coyuntura en la que muchas empresas transicionan desde infraestructuras in situ. Los analistas de Gartner predicen que más del 85 % de las empresas adoptarán el principio de uso prioritario de la nube para 2025.

Durante el análisis de la telemetría del 4.° trimestre de 2022, hemos observado:

- Las detecciones relacionadas con AWS se sitúan a la cabeza debido a la condición de líder del mercado de la nube de AWS.
- La mayoría de los ataques se centraron en el acceso inicial mediante ataques por fuerza bruta/difusión de contraseñas contra cuentas válidas, lo que apunta al vector de infección inicial en la superficie de ataque de la nube.
- La mayoría de las cuentas empresariales tenían activada la autenticación multifactor, por lo que los ataques por fuerza brutal que tienen éxito permiten a los ciberdelincuentes acceder a plataformas MFA, generando un enorme repunte en las detecciones relacionadas con la MFA.

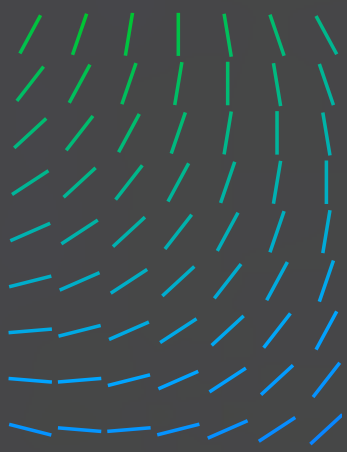
Las siguientes secciones describen brevemente los datos de telemetría de ataques basados en la nube de nuestra base de clientes desglosada por los distintos proveedores de nube.

DISTRIBUCIÓN DE LAS TÉCNICAS MITRE ATT&CK PARA AWS, 4.° TRIMESTRE DE 2022

1.	Cuentas válidas (T1078)	18 %
2.	Modificación de la infraestructura del servicio de proceso de la cuenta en la nube (T1578)	12 %
3.	Manipulación de cuentas (T1098)	9 %
4.	Cuentas en la nube (T1078.004)	8 %
5.	Fuerza bruta (T1110) Obstaculización de defensas (T1562)	6 % cada una

PRINCIPALES TÉCNICAS MITRE ATT&CK PARA AZURE, 4.° TRIMESTRE DE 2022

1.	Cuentas válidas (T1078)	23 %
2.	Autenticación multifactor (T1111)	19 %
3.	Fuerza bruta (T1110)	14 %
4.	Proxy (T1090)	14 %
5.	Manipulación de cuentas (T1098)	5 %

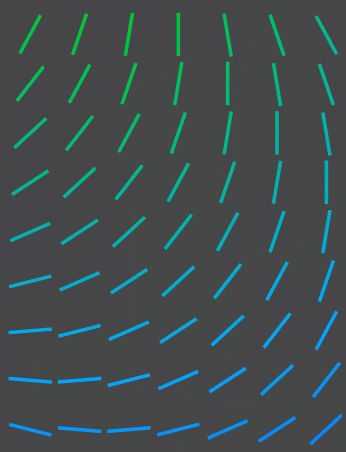


PRINCIPALES DETECCIONES DE AWS POR TÉCNICAS MITRE ATT&CK, T4 2022

Técnicas MITRE	Regla
Manipulación de cuentas (T1098)	Política de privilegios de AWS asociada a identidad IAM AWS S3 - Eliminar políticas de bucket
Cuentas válidas (T1078)	Inicio de sesión en consola anormal en servicio AWS Analytics Uso de clave API anormal en el servicio de AWS Analytics Comportamiento de usuario anormal en AWS GuardDuty Acceso anónimo a AWS GuardDuty concedido
Obstaculización de defensas (T1562)	AWS CloudTrail - Cambios en políticas en CloudTrail AWS CloudTrail - Eliminar registro de seguimiento
Credenciales en archivos (T1552.001)	Alerta de posible robo de claves secretas de AWS
Modificación de la infraestructura del servicio de proceso de la cuenta en la nube (T1578)	AWS CloudTrail - Eliminación de bucket S3 AWS CloudTrail - Definición de ACL de bucket de S3 AWS CloudTrail - Definición de ACL de objeto

PRINCIPALES DETECCIONES DE AZURE POR TÉCNICAS MITRE ATT&CK, T4 2022

Técnica MITRE ATT&CK	Regla
Cuentas válidas (T1078)	Inicio de sesión peligroso en Azure AD Inicio de sesión en Azure desde ubicación inusual Inicio de sesión en Azure por una cuenta inactiva durante 60 días
Fuerza bruta (T1110)	Múltiples errores de autenticación en Azure Graph - Ataque de fuerza bruta contra el portal de Azure Graph - Intentos de descifrado de contraseñas distribuidas
Autenticación multifactor (T1111)	MFA en Azure denegada por alerta de fraude MFA en Azure denegada porque el usuario está bloqueado MFA en Azure denegada por código de fraude MFA en Azure denegada por app de fraude
Servicios remotos externos (T1133)	Inicio de sesión en Azure desde la red TOR
Manipulación de cuentas (T1098)	Restablecimiento de contraseñas de usuario inusual en Azure

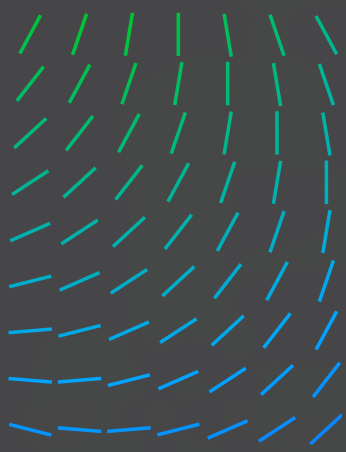


DISTRIBUCIÓN DE LAS TÉCNICAS MITRE ATT&CK PARA GCP, 4.° TRIMESTRE DE 2022

1.	Cuentas válidas (T1078)	36 %
2.	Ejecución a través de API (T0871)	18 %
3.	Descubrimiento de cuentas (T1087.001) Manipulación de cuentas (T1098) Obstaculización de defensas (T1562) Modificación de la infraestructura del servicio de proceso de la cuenta en la nube (T1578) Servicios remotos (T1021.004)	9 % cada una

PRINCIPALES DETECCIONES DE GCP POR TÉCNICAS MITRE ATT&CK, T4 2022

Técnica MITRE ATT&CK	Regla
Cuentas válidas (T1078)	GCP - Creación de cuenta de servicio GCP Analytics - Actividad anormal GCP - Creación de clave de cuenta de servicio
Servicios remotos (T1021.004)	GCP - Regla de firewall permite todo el tráfico en el puerto SSH
Manipulación de cuentas (T1098)	GCP - Modificación de directivas de IAM de la empresa
Descubrimiento de cuentas (T1087.001)	Alerta ["gcps net user"]
Transferencia de datos a cuenta en la nube (T1527)	GCP - Enrutador de registros modificado
Modificación de la infraestructura del servicio de proceso de la cuenta en la nube (T1578)	GCP - Protección de eliminación desactivada



REDACCIÓN E INVESTIGACIÓN

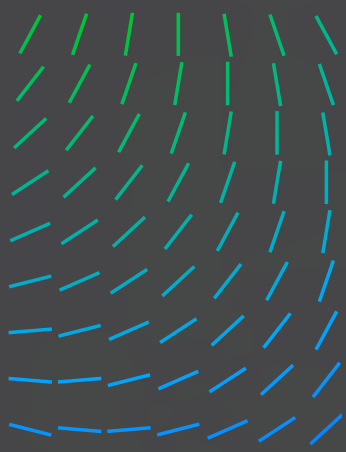
Alfred Alvarado
Henry Bernabe
Adithya Chandra
Dr. Phuc Duy Pham
Sarah Erman
John Fokker
Lennard Galang
Sparsh Jain
Daksh Kapoor
Maulik Maheta
João Marques
Tim Polzer
Srini Seethapathy
Rohan Shah
Vihar Shah
Swapnil Shashikantpa
Shyava Tripathi
Leandro Velasco

RECURSOS

Para estar al tanto de las amenazas más recientes y que más impacto han producido identificadas por el Trellix Advanced Research Center, consulte estos recursos:

TWITTER

Trellix ARC

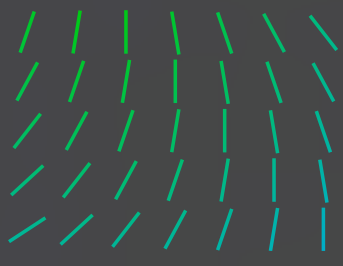


ACERCA DEL TRELLIX ADVANCED RESEARCH CENTER

El Trellix Advanced Research Center posee la carta de ciberseguridad más completa del sector y está a la vanguardia en cuanto al estudio de métodos, tendencias y ciberdelincuentes emergentes en el panorama de las amenazas. Partner ineludible de los equipos de operaciones de seguridad en todo el mundo, el Trellix Advanced Research Center ofrece inteligencia y contenido avanzado a los analistas de seguridad, mientras fomenta nuestra plataforma XDR.

ACERCA DE TRELLIX

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



Para obtener más información, visite Trellix.com.

Trellix

Acerca de Trellix

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

072022-05