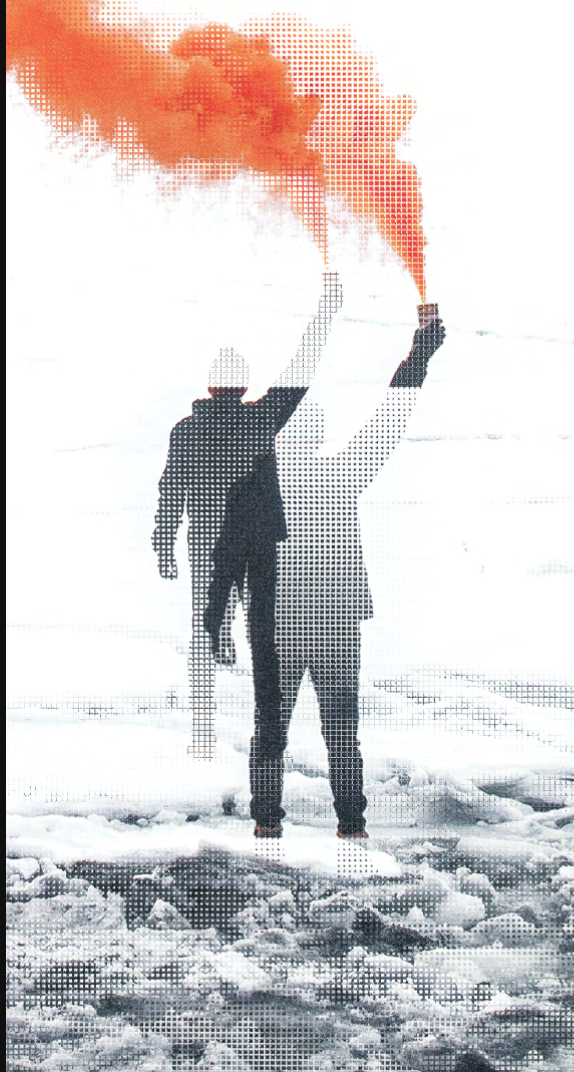
Threat Landscape

↘ 2023/2024

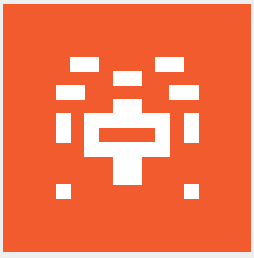
El panorama más completo de las amenazas cibernéticas en un año de transformaciones producidas por la adopción y evolución de tecnologías de inteligencia artificial. Además, las previsiones y tendencias que este 2024 guarda para la ciberseguridad.

///AXUR



¿Qué encontrará en este reporte?

Índice



Mensaje de Axur

MENSAJE DE AXUR

Sabemos que las amenazas cambian de un año para el otro. Claramente, la dimensión y el ritmo de estos cambios también varían, pero siempre hay alguna novedad que merece nuestra atención. Algunos de estos cambios permanecen y se transforman en tendencias, mientras que otros son apenas anomalías temporarias.

El año 2023 puso fin al pequeño alivio sobre los ataques de ransomware observado en 2022, reavivando las amenazas y todos los desafíos que estas representan.

La reanudación de los ataques de ransomware estuvo acompañada de dos métodos de acceso: el ataque a la cadena de suministros – supply chain – y las amenazas internas, o más conocidos como "insiders". Muchos de los nuevos ataques aprovechan los vínculos comerciales y los ecosistemas tecnológicos para alcanzar objetivos distantes del punto de entrada. Podemos considerar si aún tiene sentido el concepto limitado de amenaza interna, cuando existen tantas redes y entornos conectados.

Paralelamente, estamos viviendo transformaciones producidas por la adopción y evolución de tecnologías de inteligencia artificial. Dentro de nuestro medio de seguridad cibernética, estas tecnologías pueden generar nuevos tipos de ataques o perfeccionar amenazas antiguas, como ya está ocurriendo. Al mismo tiempo, es necesario encontrar medidas que utilicen la IA para la defensa de los datos. Esto depende de nosotros, que conocemos la necesidad de detectar y prevenir con rapidez los nuevos ataques, así como también sabemos de la falta de profesionales especializados para la tarea.

Esperamos que este informe pueda ayudar a entender el escenario en que estamos y a vislumbrar el camino a seguir.

Thiago Bordini
Head de Cyber Threat Intelligence | Axur

Resumen ejecutivo

Con la tecnología y la experiencia en inteligencia de Axur, este informe aportará un retrato del escenario de amenazas cibernéticas de 2023.

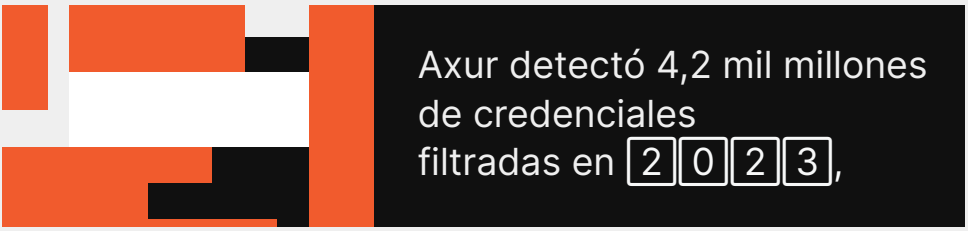
Ransomware

La disminución de la actividad de los operadores de ransomware en 2022 se revirtió este año. Los ataques volvieron a ocurrir e incorporaron nuevos abordajes de ingeniería social y ataques a terceros (en la cadena de proveedores y prestadores, o supply chain).

Aunque todavía se los denomine "ransomware", algunos ataques ya dejaron en segundo plano la criptografía de los archivos y prefieren apostar a una amenaza basada en los costos regulatorios y legales que puedan derivar de una filtración de datos.

Credenciales en el foco de los atacantes

El robo de credenciales de acceso continúa siendo elevado.



manteniendo así la tendencia establecida con el uso de malwares de credential stealers y otros ataques para reciclar credenciales robadas en filtraciones de datos. Adoptar la autenticación multifactor continúa siendo un requisito importante para dificultar el uso de estas credenciales.

Aumento en la filtración de tarjetas de débito y crédito

Detectamos un aumento significativo en el intercambio de datos de tarjetas entre los delicuentes. Nuestro monitoreo identificó

más de 13 millones de tarjetas filtradas, un crecimiento del 265%, en comparación con el volumen de 2022.

Sectores más afectados

La actividad delictiva en la Deep & Dark Web se concentró mayoritariamente en los sectores minoristas, finanzas y tecnología, que fueron los causantes del 77% de los incidentes de mención sospechosa. En detecciones de phishing, el sector de las telecomunicaciones ocupa el tercer lugar: el top 3 representa el 90% de las páginas.

Inteligencia artificial

El uso de inteligencia artificial permite que delincuentes con poco conocimiento de programación produzcan artefactos maliciosos o configuren herramientas preexistentes con mayor facilidad. Los modelo de lenguaje de gran tamaño (LLM) se han utilizado para automatizar la interacción con las víctimas en ataques de ingeniería social por medio de mensajes y aplicaciones de comunicación.

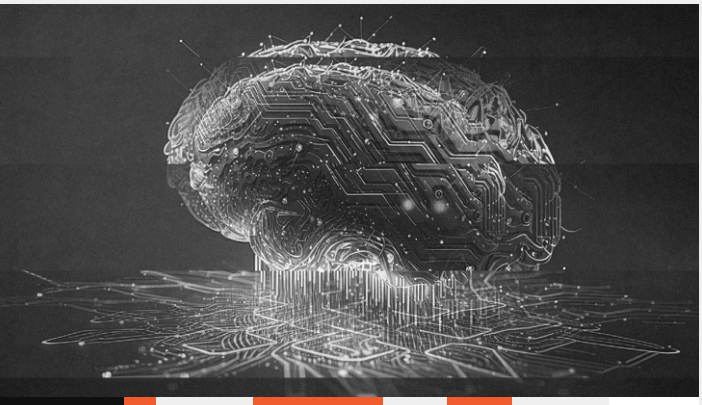
Inestabilidad geopolítica

Los conflictos entre Ucrania y Rusia e Israel y Hamas instigaron a grupos de hacktivistas, que ponen en la mira a empresas y organizaciones asociadas a cualquier país que se manifieste de forma favorable a la nación que consideran enemiga. Además, las acciones de estos grupos tienden a ser más imprevisibles que los ataques realizados por grupos delictivos motivados únicamente por la renta financiera.

Phishing

El comercio minorista y el sector financiero son los más alcanzados por los ataques de phishing.

A lo largo de 2023, identificamos más de 31 mil páginas de phishing.



Inteligencia artificial

El uso de la IA tiende a posibilitar nuevas formas de fraude y ataques. Por otro lado, la IA puede ser uma pieza fundamental para el avance de la inteligencia en amenazas cibernéticas, ya sea en la organización de la información, la velocidad de procesamiento o en el mejoramiento del monitoreo.

Ingeniería social

La ingeniería social presentó un gran desafío en los ataques ocurridos en 2023. Socios y proveedores sufren asaltos de los atacantes, que amplían el número de canales para obtener acceso a sus objetivos.

El empleo de amenazas de violencia física también sorprende, más aún en estos casos.

2023

Febrero

La banda de ransomware Cl0p aprovecha una vulnerabilidad en el software GoAnywhere y amenaza con exponer los datos de más de 130 empresas.

La red social Reddit revela haber sido objetivo de un ataque de ingeniería social sofisticado que proporcionó a los invasores acceso a documentos, códigos y sistemas internos.

Marzo

El administrador de contraseñas LastPass informa que un incidente en 2022 filtró bóvedas cifradas de los usuarios. Los analistas de blockchain creen que los delincuentes accedieron a las bóvedas para obtener claves privadas, lo que permitió el robo de más de US$ 40 millones en criptoactivos.

Un bug en ChatGPT filtra conversaciones de usuarios hacia el historial de otros usuarios, dándoles acceso a estos intercambios que pertenecían a terceros.

Abril

Un ransomware compromete sistemas e informaciones de clientes de Western Digital, fabricante de soluciones de almacenamiento de datos. El servicio My Cloud queda inactivo por diez días.

3CX, desarrollador de soluciones de comunicación empresarial, revela que delincuentes accedieron a los sistemas de la compañía e incluyeron un malware en la descarga de su software a través del canal de distribución oficial.

Mayo

Luxottica, fabricante de lentes, confirma un incidente de filtración de datos personales de 70 millones de clientes.

Junio

Cl0p aprovecha una vulnerabilidad en el software MOVEit Transfer para comprometer a más de 2.000 empresas. El ataque alcanzó a bancos, hospitales, universidades y organismos públicos, sobre todo en los Estados Unidos.

Septiembre

El Departamento de Estado de los EEUU revela que sus e-mails fueron comprometidos por hackers chinos que aprovecharon una falla en la nube de Microsoft.

El grupo Scattered Spider compromete a Caesars Entertainment y MGM Resorts y paraliza sus actividades mediante un ransomware.
MGM Resorts se niega a pagar el rescate, por lo que queda diez días inactivo y tiene pérdidas estimadas en US$ 100 millones. Informes de prensa afirman que Caesars pagó el rescate de US$ 15 millones, pero la empresa dice que "no es posible" determinar las pérdidas futuras.

Falla en Google Bard expone las conversaciones de los usuarios con el chatbot en los resultados de búsqueda, generando un problema similar al enfrentado por ChatGPT en marzo.

Octubre

Okta, un proveedor de servicios de identidad, anuncia que sufrió dos ataques cibernéticos.

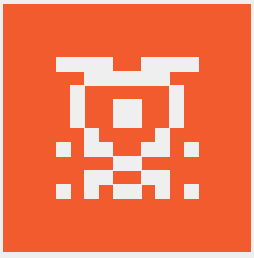
Los hackers del grupo Sandworm, de origen ruso, causan un nuevo apagón en Ucrania luego de usar un malware de tipo wiper para borrar todos los datos y softwares de los sistemas de una generadora de energía.

Noviembre

El grupo de ransomware LockBit afirma haber obtenido un paquete de 1,5 TB de datos con 24 años de información de empleados del gobierno canadiense.

Diciembre

Kyivstar, el mayor operador de telefonía móvil de Ucrania, sufre un ciberataque que provoca inestabilidad en sus servicios. El ataque se atribuyó a un grupo relacionado con la inteligencia rusa.



Panorama de ciberseguridad

Los ataques cibernéticos evolucionaron mucho en los últimos años. Las amenazas avanzadas y los grupos de ransomware conocidos por realizar movimiento lateral dentro de las redes corporativas traen la impresión de que la situación es grave. La migración hacia la nube, que se realizó precipitadamente en muchas empresas, también dejó víctimas en el camino.

Sabiendo de los riesgos y de estos ciberataques, ¿Cuál es el horizonte al que debemos apuntar?

Existe un movimiento para integrar el riesgo cibernético al riesgo del negocio. Esta perspectiva, que ya estaba siendo trabajada por algunos especialistas, se presenta como la única vía posible ante la dimensión de los perjuicios, en particular cuando los ataques paralizan las actividades de la empresa en su conjunto o generan multas millonarias por filtración de datos personales.

En la práctica, el riesgo cibernético se vuelve mucho más amplio y sujeto a algunas reglas que antes sólo existían para los llamados riesgos "tradicionales".

La estrategia de ciberseguridad de la administración Biden, en los Estados Unidos, constituye, en gran parte, una interpretación de esa perspectiva, pues entiende que los desarrolladores de software y los prestadores de servicios deben ser responsables por ciertas fallas, tal como sucede en otros sectores.

También se buscan, en gran medida, formas de reducir los costos del riesgo a través de un seguro cibernético. Según el Swiss Re Institute, el mercado del seguro cibernético duplicará su tamaño en cuatro años,

y alcanzará los $22 mil millones en 2025.

Sin embargo, esto no significa que se minimice la adopción de prácticas seguras. El seguro no cubre los daños y perjuicios secundarios, como la pérdida de la confianza de clientes y proveedores. Más allá de esto, poner precio al riego tiende a beneficiar a las empresas que actúan de forma responsable y que buscan proteger su negocio. Las aseguradoras ya observan los controles que las empresas implementan o dejan de implementar para definir el valor de los premios.

Por parte del gobierno, hemos observado casos de autoridades americanas y australianas que buscan responsabilizar a los propios encargados de seguridad por las fallas en sus empresas. Si bien la base regulatoria aún se está definiendo, el mensaje que los reguladores intentan transmitir es claro: el solo “asumir el riesgo” ya no es viable. Entramos en 2024 con incertidumbre sobre cómo será la actuación de los tribunales con respecto a esta cuestión.

De todas maneras, estos movimientos están impulsados por la madurez del sector. La balanza entre "seguridad" e "innovación" empieza a buscar un equilibrio en lugar de priorizar la evolución a cualquier costo. Como los servicios digitales están en todos lados, directa o indirectamente, el riesgo digital "contamina" los demás riesgos, así como estos también contaminan el riesgo digital.

En 2023, los ataques cibernéticos a gran escala lograron alcanzar cientos de empresas que tenían un único punto en común. Fue el caso de los ataques a MOVEit Transfer, GoAnywhere y 3CX. De instituciones financieras a universidades, todas eran igualmente vulnerables.

Ransomware:

Los ataques dirigidos a las vulnerabilidades de GoAnywhere y MOVEit Transfer, ambos de autoría del grupo Cl0p, posiblemente sean los mayores exponente de lo que significó el ransomware en 2023: acciones agresivas y en masa. Los delincuentes apostaron a la eficiencia y priorizaron amenazas que involucraban la exposición de los datos robados en vez de la criptografía.

En los países que aprobaron leyes para la protección de datos, es posible que sea más dificultoso enfrentar filtraciones en la información personal que resolver los peligros exclusivamente técnicos derivados de la criptografía de los datos. Si la multa que recibirá la empresa es significativamente superior a la cifra exigida por los estafadores, la criptografía de los archivos dejará de ser el factor decisivo para pagar el rescate.

Si bien antes se podía hablar de una "triple extorsión" (criptografía, exposición de datos y DDoS u otra amenaza), actualmente existen casos de ransomware sin la criptografía de datos característica de este tipo de estafas. Los planes de respuesta al ransomware, destinados a recuperar y proteger los datos, no logran evitar multas y otras sanciones regulatorias inherentes a la exposición de dichos datos.

Un caso que ilustra este cambio de táctica es el que tuvo como protagonista a la banda de ransomware ALPHV (también conocida como "BlackCat"), denunciado por una víctima a la Securities and Exchange Commission (SEC), organismo que regula los valores mobiliarios de los Estados Unidos. Los delincuentes alegaron que la empresa no había cumplido con su obligación legal de informar la vulneración de su sistema a las autoridades regulatorias.

Dentro de este mismo marco, los grupos de ransomware pueden divulgar declaraciones falsas sobre los ataques que realizan en sus "leak sites" (sitios de filtración) de la Deep Web. Aunque de hecho los ataques no se lleven a cabo, esto presiona a las empresas pudiendo llegar a causar daños en la imagen de sus marcas.

- Variante del ransomware CryptoMix
- Activo desde: 2019
- País de origen: Rusia
- Sectores más afectados: varios sectores y organizaciones
- Motivación: financiera

- Modelo de Ransomware como Servicio (RaaS)
- Activo desde: noviembre de 2021
- País de origen: Rusia
- Sectores más afectados: varios sectores y organizaciones
- Motivación: financiera

En caso de que ⚠ las amenazas sean infundadas, es importante que las empresas puedan evaluar rápidamente sus entornos y adoptar una postura firme en cuanto a la falsedad de las declaraciones de los delincuentes.

Evidentemente, los ataques tradicionales de doble extorsión (criptografía y exposición de datos) continuaron siendo lo habitual. De cualquier modo, las nuevas modalidades delictivas funcionaron y los grupos de ransomware volvieron a facturar más en 2023, luego de la baja de 2022.

En este sentido, la sofisticación técnica de los ataques cibernéticos permanece muy vinculada a las tácticas tradicionales. La ingeniería social continúa siendo uno de los riegos mayores, y empieza a alcanzar también a empleados de proveedores tercerizados. El grupo delictivo conocido como "the Com" (o Scattered Spider), asociado al ya mencionado ALPHV, también se destacó en el uso de estas tácticas llevando a cabo ataques exitosos contra prestadores de servicios de TI (lo que condujo al incidente en los casinos Caesars y MGM) y amenazando, al comunicarse con sus víctimas, con aplicar la violencia física.

Muchos ataques siguen llevándose a cabo a partir del modelo de Ransomware como Servicio (ransomware-as-a-service, RaaS), ya que el mismo permite que las operaciones de estos grupos se vuelvan más difusas y diversificadas. El modelo RaaS permite que muchos delincuentes puedan asociarse a la operación como afiliados. LockBit es un buen ejemplo de esta modalidad, y constituyó uno de los grupos más activos del año.

- Ransomware-as-a-Service (RaaS) model
- Activo desde: septiembre de 2019
- País de origen: Rusia
- Sectores más afectados: servicios profesionales, transporte, manufacturas
- Motivación: financiera

Del mismo modo que el RaaS no es una novedad, también debemos decir que muchas empresas sufren ataques de ransomware por equivocarse en lo básico, como no aplicar actualizaciones de software con parches de seguridad o descuidar la gestión de identidad y acceso. Es después del ataque que muchas de estas empresas advierten la falta de un plan de continuidad del negocio y de recuperación de desastres.

Por lo antedicho, cualquier escenario en el que la facturación de los grupos de ransomware esté en crecimiento se torna desfavorable. Considerando el elevado grado de profesionalidad de estas organizaciones delictivas, los recursos que ellas obtienen pueden reinvertirse en acciones delictivas, como el reclutamiento de nuevos miembros o la creación de artefactos y herramientas más sofisticadas que dificulten la detección y la atribución de la actividad.

Inteligencia artificial

Ciertamente la madurez digital y la consolidación de las tácticas de ataque no anularon la innovación por completo.

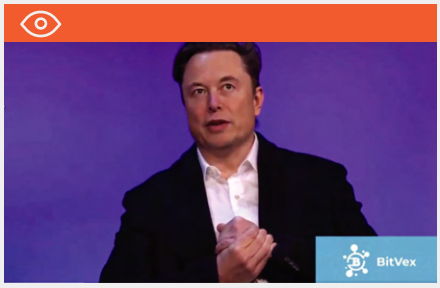
El año 2023 estuvo marcado por un acentuado avance de los algoritmos de aprendizaje automático y de la inteligencia artificial.

Como la modalidad de deep learning es muy versátil, los atacantes pueden emplear esta tecnología en los ataques más diversos. En 2023, pudimos observar los siguientes ataques:

Deepfakes: imágenes y voces manipuladas que están siendo usadas en algunos contextos. Un ejemplo son los videos falsos que promueven estafas de criptomonedas usando personalidades como el multimillonario Elon Musk y el creador de Ethereum Vitalik Buterin. Los videos utilizan imágenes de estos ejecutivos tomadas en eventos, pero los discursos originales se reemplazan por una voz sintetizada a través de IA. Las imágenes se adulteran a fin de garantizar la sincronía labial, que es otra función de este tipo de IA.

Axur Research Team también observó casos en que las imágenes manipuladas por IA -por ejemplo, las que agregan movimiento a imágenes estáticas- han sido utilizadas para burlar sistemas de autenticación biométrica remota. Aunque normalmente este tipo de autenticación exige una captura de foto o video con la cámara del smartphone, los delincuentes pueden usar aplicaciones modificadas para enviar las imágenes manipuladas por IA y provocar el error en el sistema.

Finalmente, los medios de comunicación dan cuenta de situaciones en que los estudiantes crearon deepfakes para perjudicar la imagen de sus compañeros. Si bien estos hechos no tienen una réplica directa en la seguridad corporativa, disparan una alarma sobre las posibilidades de uso de las deepfakes cuando existen conflictos en las organizaciones o como instrumento para comprometer la reputación de los ejecutivos.



Ingeniería social: así como las empresas ven la posibilidad de utilizar la IA para automatizar los procesos de atención al consumidor, los delincuentes pueden usar los modelos de lenguaje amplio (LLMs, large language models) para crear robots que interactúen con las víctimas en estafas de ingeniería social.

En estos casos, el contacto del estafador por lo general es más indirecto que en un phishing tradicional, y el convencimiento de la víctima se da poco a poco.

Desde el punto de vista del fraude, la ventaja de este tipo de interacción más personal es el mayor involucramiento de la víctima, que se vuelve susceptible de caer en engaños que no tendrían efecto en un contexto impersonal. La desventaja, para los delincuentes, reside en el trabajo de mantener varias conversaciones en paralelo, ya que la estafa no se aplica a una sola persona por vez.

La automatización de las repuestas que permite la IA es una solución a este problema para los delincuentes. Observamos que ciertos golpes hacia aplicaciones de mensajería (como WhatsApp) utilizaron este macanismo para acelerar las interacciones con las víctimas, luego de enviar los mensajes en masa.

Códigos y automatización: los LLMs tienen un gran potencial para automatizar o proyectar soluciones a las tareas de programación. Para el mundo del ciberdelito, esto significa que los agentes menos habilidosos puedan usar estas herramientas a fin de compensar la falta de conocimiento técnico.

Habitualmente, las herramientas comerciales de IA tienen restricciones a fin de evitar que produzcan códigos maliciosos. Sin embargo, hay varias brechas que permiten que el llamado "jailbreak" de la inteligencia artificial la prepare para aceptar prácticamente cualquier prompt.

Los atacantes más habilidosos pueden aprovechar la IA para ganar tiempo, ya sea en las tareas más complejas de programación como en el ajuste de archivos de configuración usados en otras herramientas.

Ante estos nuevos desafíos, y debido al panorama general que se presenta, existe la necesidad de innovar en seguridad. Es necesario aprovechar los avances que puedan mejorar la productividad y priorizar lo que más importa en el momento indicado. La inteligencia artificial y la inteligencia en amenazas cibernéticas son dos pilares importantes en este emprendimiento.

Con frecuencia, la seguridad cibernética sufre el impacto de factores externos, como la economía y la política.

Un ejemplo de esto es la popularidad de las criptomonedas y su reglamentación, o la falta de ella. En la práctica, la mayor parte de los ataques de ransomware depende de un pago realizado en criptomonedas. En este caso, una circunstancia relacionada con la política económica tiene como resultado un modelo de estafa cibernética.

En 2023, tres fenómenos geopolíticos provocaron impactos visibles en la seguridad de la información: la guerra entre Rusia y Ucrania, las sanciones comerciales impuestas por Estados Unidos a China y, más recientemente, el conflicto entre Israel y Hamas.

Rusia vs. Ucrania

- Los movimientos en Rusia tienen impacto sobre los delincuentes situados en ese país

- Las autoridades que observan el conflicto están viendo la necesidad de elaborar medidas tendientes a disminuir el riesgo cibernético de los sectores críticos

- Las sanciones económicas dificultan la relación de terceros con vínculos entre los dos países

Con la invasión de Rusia al territorio ucraniano, en 2022, hecho que dio inicio al mayor conflicto armado en suelo europeo desde la Segunda Guerra Mundial, la guerra tuvo su reflejo en internet de inmediato. Mientras se realizaban campañas para reclutar voluntarios para el "Ejército de TI de Ucrania" (IT ARMY of Ukraine), el gobierno de este país acusaba a Rusia por los ataques de denegación de servicio, que provocaban inestabilidad en sus sitios web.

El grupo de ransomware Conti protagonizó uno de los episodios más notables: luego de manifestar su apoyo a Rusia durante un duro ataque de ransomware contra el gobierno de Costa Rica, se conocieron conversaciones e informaciones internas de la banda. Se cree que la filtración, atribuida a un especialista ucraniano, agravó las tensiones dentro del grupo y contribuyó a su disolución.

- Modelo de Ransomware como Servicio (RaaS)
- Activo desde: diciembre de 2019
- País de origen: Rusia
- Sectores más afectados: grandes corporaciones y agencias gubernamentales
- Motivación: financiera

Evidentemente, esto no sucedió con todos los grupos que levantaron la bandera rusa. La banda de ransomware Stormous que también se declara pro Rusia, continuó en actividad.

- Se supone que es un ransomware, pero su modus operandi aún está siendo investigado
- Activo desde: 2021
- Sectores más afectados: gobierno, grandes empresas
- Motivación: agenda política, renta financiera
- Se centra, sobre todo, en códigos fuentes y documentos sensibles de sus objetivos

Otros ataques alcanzaron sistemas críticos en Ucrania y en Rusia desde el comienzo de la guerra. En junio de 2023, los ucranianos se atribuyeron la autoría de un ataque que provocó la caída de una red interbancaria en Rusia y generó inestabilidad en el sistema de pagos.

Del otro lado, un grupo ruso conocido como Sandworm llevó a cabo diversos ataques contra la infraestructura ucraniana. En noviembre, los invasores lograron desestabilizar el sistema eléctrico ucraniano y causaron un apagón que coincidió con un ataque físico. Fue el tercer apagón provocado por Sandworm y el primero que pareció estar vinculado con la ofensiva rusa.

- Grupo de amenazas atribuido a las fuerzas armadas de Rusia
- Activo desde: por lo menos 2009
- País de origen: Rusia
- Sectores más afectados: empresas eléctricas, organismos gubernamentales, campañas presidenciales
- Motivación: sabotaje y espionaje

Pero las repercusiones de este conflicto no se limitan a los dos países involucrado en él.

En 2022, no hubo una explicación aceptable para la baja en la actividad de ransomware que se registró en el mundo. En 2023, al reanudarse los ataques de ransomware, se desestimaron algunas explicaciones, como por ejemplo la posibilidad de que las empresas simplemente estuvieran más protegidas.

Analizando lo que sucedió de diferente en 2022, deberemos reconocer que la disminución en los ataques puede haberse dado como una posible consecuencia de la guerra.

Vale destacar -inclusive considerando la acción de Conti contra Costa Rica- que muchos delincuentes involucrados en ataques a través de ransomware son rusos. A comienzos de 2022, Rusia se reorganizó con el fin de adaptarse al conflicto y generó una inestabilidad que puede haber impactado también en los hábitos de los threat actors.

En el panorama interno, Rusia iniciaba sus campañas de reclutamiento. En el panorama externo, las sanciones económicas dificultaban la situación económica del país y el acceso al sistema bancario mundial. Ambos factores pueden haber perjudicado la actividad delictiva.

El impacto se agrava por el accionar de los grupos de hacktivismo. Un ejemplo es Killnet, que realiza ataques de denegación de servicio (DDoS) y provocó la caída de varios sitios web en Estados Unidos y en países europeos vinculados a la Organización del Tratado del Atlántico Norte (OTAN). A comienzos de 2023, pasó a orquestar ataques contra organizaciones de salud.

- Grupo hacktivista prorruso
- Activo desde: 2021
- País de origen: Rusia
- Sectores más afectados: aeropuertos, bancos, contratistas de defensa, salud, proveedores de servicios de internet y gobiernos
- Motivación: Política, justificaciones ideológicas

De todas maneras, es indudable que muchas naciones empezaron a revisar sus planes de seguridad nacional. En la actualidad, los sistemas informáticos son esenciales para el funcionamiento de la sociedad, y, por ello, la tecnología y la comunicación digital asumen un papel fundamental.

Con la prolongación del conflicto y de los intercambios de ataques físicos y cibernéticos, han surgido ideas y preocupaciones nuevas, tanto en la esfera digital como en el mundo de los negocios.

Los economistas prevén la finalización del llamado "dividendo de la paz", término acuñado por el presidente George H. W. Bush y la primera ministra Margaret Thatcher para describir el escenario que se siguió a la disolución de la Unión Soviética y que permitió reducir los gastos en defensa. Para muchos gobiernos, pensar en "adversarios" volvió a tener sentido a fin de justificar las medidas a tomar.

La Estrategia Cibernética del Departamento de Defensa de los Estados Unidos menciona a Rusia y China como adversarios. El conflicto con Ucrania también se cita como una demostración de la capacidad de ataque de Rusia, cuya ofensiva, según los documentos de la Casa Blanca, podría alcanzar la infraestructura norteamericana.

En la práctica, esto significa que los movimientos regulatorios y los incentivos económicos que el gobierno norteamericano planea elaborar estarán en concordancia con la realidad del conflicto, y las nuevas reglamentaciones que llegarán a los sectores críticos – salud, finanzas e infraestructura – también podrán etenderse como una consecuencia de las lecciones que dejó el conflicto.

Como varios de los principales prestadores de servicios de tecnología e infraestructura tecnológica están ubicados en Estados Unidos, estos cambios tendrán impacto en todo el mundo.

Otro punto que debe considerarse es los efectos que tendrán las sanciones económicas y los riesgos del negocio relacionados con la cadena de suministros que dichas sanciones imponen.

Las autoridades están aplicando distintas multas por violación a las normas. En tal sentido, en abril Microsoft recibió una multa por US$ 3 millones por haber prestado servicios irregularmente.

La tensión generada se alimenta desde ambos lados. Más allá de las acciones llevadas adelante para aislar la red del país y evitar la dependencia de software foráneo, Rusia multó a tres empresas extranjeras – UPS, Airbnb y Spotify – alegando que violaron las leyes que exigen el almacenamiento de datos en territorio ruso.

A medida que los prestadores de servicios de tecnología abandonan Rusia para cumplir sus obligaciones legales (incluyendo Microsoft, Atlassian y Amazon), las empresas que todavía dependen de proveedores de ese país corren riesgos con respecto a la disponibilidad, integridad o confidencialidad de los datos que están bajo la responsabilidad de estos terceros.

China y la guerra de los semiconductores

- EE.UU. busca ampliar su liderazgo en semiconductores, generando disputas geopolíticas con China
- EE.UU. argumenta que el software y hardware hechos en China representan un riesgo para la seguridad nacional
- Los países ya formularon programas de reemplazo de equipos chinos

En 2022, Estados Unidos aprobó el CHIPS and Science Act. Esta legislación expresaba la voluntad de ampliar el liderazgo tecnológico con respecto a China.

Las relaciones geopolíticas que plantearon esta necesidad son complejas. Además de un posible enlace con los problemas en la cadena global de sumunistros surgidos durante la pandemia de Covid-19, también existen intereses militares, como por ejemplo, las dificultades que enfrentó Estados Unidos para reponer chips de equipos antiguos.

Ante la información de que chips piratas provenientes de China llegaron a las Fuerzas Armadas estadounidenses, se comprende el alineamiento en las necesidades de seguridad nacional y de independencia en la fabricación de los semiconductores.

Las autoridades norteamericanas vienen repitiendo que el uso de equipos de origen chino genera riesgos en la seguridad nacional, tanto de los Estados Unidos como de sus aliados. Respecto a países como Reino Unido y Australia reemplazaron e incluso prohibieron el uso de cámaras de seguridad fabricadas en China.

Algo similar ocurre con la disputa por las redes 5G. A finales de 2022, se prohibió la venta de equipos de las marcas Huawei, ZTE e Hikvision en Estados Unidos. Desde entonces, algunos países europeos anunciaron en sus redes planes para reemplazar los equipos chinos.

De cualquier manera, no todos los países son propensos a adoptar este tipo de medidas y no está claro si habrá consecuencias a largo plazo, especialmente para empresas que no actúan en infraestructura crítica.

Aunque se sostenga que la discusión y negociación se debe basar en hechos y evidencias, el hecho más importante es que se trata de una disputa geopolítica, lo que significa que los intereses involucrados en ella no siempre sean claros.

Por este motivo, las empresas que actúan en el sector de infraestructura crítica o que habitualmente trabajan con organizaciones impactadas deben continuar prestando atención a estas repercusiones, tanto apagar la perspectiva del cumplimiento como desde los riesgos concretos que corre la seguridad de la conectividad y los equipos.

Israel vs. Hamas

- Existen grupos de hacktivistas en ambos lados del conflicto
- Los hacktivistas realizan ataques simbólicos contra organizaciones vistas como aliadas del adversario
- Aunque los ataques sean de escala reducida, hay riesgo de compliance y de perjuicios para los negocios
- El comportamiento y la respuesta de las organizaciones pueden perfeccionarse con Cyber Threat Intelligence

Con la manifestación del conflicto entre Israel y Hamas en octubre de 2023, entraron en escena diversos grupos de hacktivismo y declararon su apoyo a uno de los involucrados en la guerra.

El mapeo realizado por el equipo de Cyber Threat Intelligence de Axur identificó

por lo menos 52 grupos hacktivistas que manifestaron su apoyo a Palestina, mientras que 16 lo hicieron a Israel.

Es importante destacar que existen vínculos entre este enfrentamiento y el llevado a cabo entre Rusia y Ucrania. Algunos países de la región, como Irán y Siria, son aliados de Rusia. Las alianzas se reflejan también en los alineamientos de los grupos de hacktivismo, con el Ejército de TI de Ucrânia, del lado de Israel, y Killnet, del lado palestino.

Tal como sucedió en el caso ucraniano, estos grupos direccionaron sus ataques a los países que manifestaron su apoyo al bando contrario, aun cuando los países no se involucraran directamente en el conflicto.

En este sentido, podemos nombrar el caso de Ganosec Team, que atacó a la India por haber dado su apoyo a Israel y como represalia contra hacktivistas indios que se habían manifestado a favor del estado judío. Otro caso es el de Moroccan Ghosts, que dirigió sus ataques contra Sudáfrica, alegando que ese país apoyaba a Israel -aunque históricamente Sudáfrica ha apoyado a Gaza-, y acompañó el embargo diplomático contra el Estado de Israel.

Algunas empresas brasileñas también fueron blanco de ataques de los grupos hacktivistas, luego de que Brasil llevara al Consejo de Seguridad de la ONU una propuesta para clasificar los actos de Hamas como terroristas. Aunque Brasil se haya expresado con mucha prudencia con respecto al conflicto y proponga una resolución pacífica del mismo, el solo hecho de condenar los ataques fue suficiente para sufrir represalias.

Las acciones de los grupos hacktivistas no siempre poseen um vínculo concreto con el objetivo que persiguen. Esto termina por representar un riesgo para organizaciones, empresas y hasta para los individuos, quienes pueden volverse víctimas del “fuego cruzado”.

Inclusive las pequeñas empresas → son atacadas si estos grupos encuentran una vulnerabilidad fácil de explotar.

El propósito de los ataques suele ser simbólico: lo importante es demostrar que se ataca a un objetivo que se considera enemigo. Siempre que la empresa u organización esté vinculada al objetivo de los hacktivistas, cualquier tipo de ataque – DDoS o filtración de datos – es suficiente para mostrar su compromiso con la causa.

Aunque la intención de muchos ataques sea provocar caídas en los sitios web para compartir en las redes (principalmente, en Telegram) capturas de pantalla con el texto del error "sitio web inaccesible", existen casos en que realmente se exponen los datos de los individuos y se modifica la apariencia de los sitios web (defacement).
Las filtraciones de datos generan riesgos para las personas, ya que es posible que los ciberdelincuentes aprovechen la información para otros fines. Con todo, también existe un riesgo de compliance para las empresas que tengan la obligación legal de resguardar los datos como medida de seguridad.

Los incidentes de defacement pueden ser igualmente complejos. Si bien muchos hacktivistas no tienen interés en provocar otro tipo de daños, la organización atacada deber llevar a cabo un proceso de respuesta al incidente y de peritaje a fin de garantizar la integridad del entorno. Además de esto, potencialmente el defacement puede generar inconvenientes para la institución o la marca, lo cual es compatible con el objetivo de estos grupos.

La aplicación de Cyber Threat Intelligence tiene la capacidad de ayudar a acelerar al proceso de respuesta, pues a menudo los grupos dejan un "sello" y tienen tendencia a realizar ataques similares a las acciones anteriores.

De todos modos, la variedad de los ataques y la dificultad de prever las acciones de los hacktivistas generan una gran incertidumbre, y es importante destacar que nadie está "libre" de recibir un ataque. Los grupos actúan de ambos lados, y atacan a cualquier organización que aparezca como "aliada" o que "apoye" a los adversarios, aun cuando no se haya manifestado a favor o en contra de los protagonistas del conflicto.

↪ Aunque los hacktivistas no siempre logren provocar daños prolongados a las redes nacionales, una empresa que no esté preparada para enfrentar estos ataques se expone a diversos riesgos ⚠ y expone también a sus clientes y empleados.

2023 en números

La plataforma Axur siempre utiliza rastreadores de datos y sensores configurados para detectar incidentes de diferentes categorías, como filtración de credenciales, filtración de tarjetas, páginas de phishing y estafas, entre las cuales, el uso indebido de la marca, perfiles falsos en redes sociales y aplicaciones móviles falsas.
En el año 2023 se repitió considerablemente lo que observamos en 2022. Sin embargo, la modalidad de las filtraciones cambió de forma significativa,

↳ y el número de tarjetas filtradas ascendió a más del triple.

Credenciales

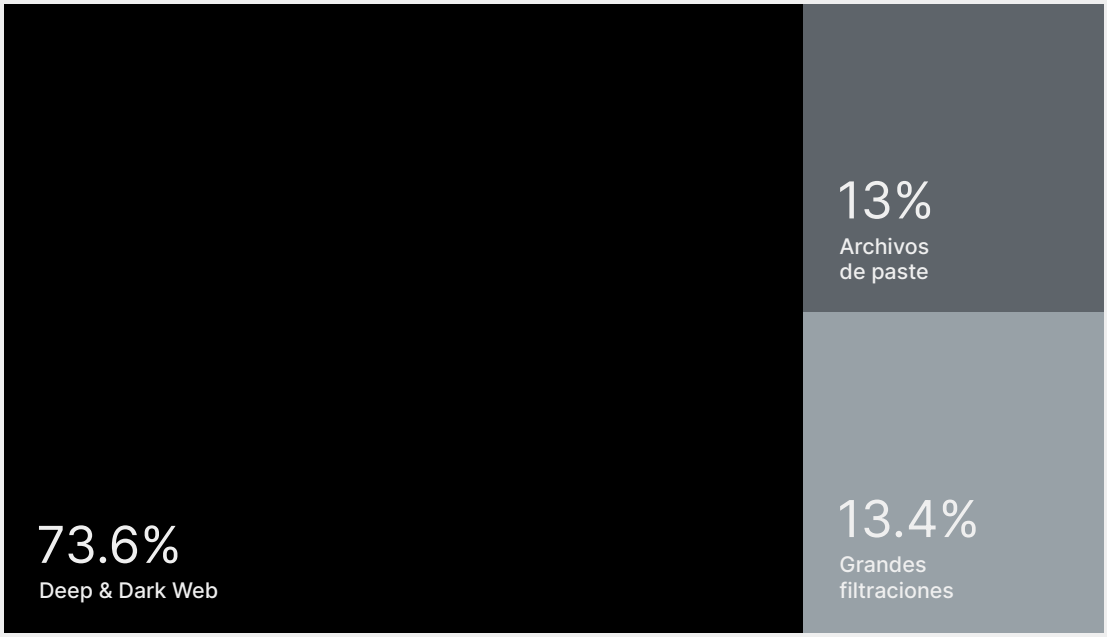
La plataforma Axur monitorea filtraciones y publicaciones en la Deep, Dark & Surface Web para identificar la fuga de credenciales.

En 2023, detectamos la filtración de 4,2 mil millones de credenciales, número que se mantuvo estable con respecto al período anterior.

Muchas credenciales se extraen de sistemas atacados por malwares de tipo credential stealer. Estos softwares maliciosos recolectan cualquier tipo de credencial, por lo que son capaces de escanear datos de navegadores para robar cookies y buscar softwares de billeteras digitales instalados para robar claves criptográficas que dan acceso a criptoactivos

Aunque el volumen de credenciales filtradas se haya mantenido estable, hubo un cambio en el origen de las mismas. En 2022, el 96% de las credenciales se recolectaron en la Deep Web. En 2023, observamos un número mucho más significativo de credenciales en los llamados pastes y en grandes filtraciones, aumentando la diversidad de las fuentes de las credenciales.

Origen de las credenciales en 2023



Canales, grupos y foros de la Deep & Dark Web siguieron siendo las principales fuentes de credenciales filtradas en 2023.

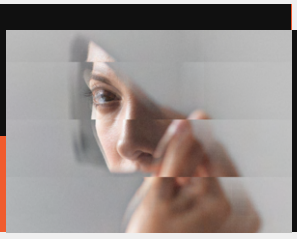
Para entender

Pastes: Son archivos de texto de tamaño variado que contienen colecciones de datos muchas veces indefinidas. El término hace referencia al formato de los archivos de texto que puede ser compartido en los llamados "paste sites".

Grandes filtraciones: Las colecciones de datos con denominación o cuyo origen es más específico son tratadas por Axur como "grandes filtraciones". En general, son bancos de datos voluminosos que se pueden atribuir a una fuente (filtraciones de una empresa) o a una acción delictiva (recopilación de filtraciones menores).

El análisis realizado por Axur indicó que cerca del 15% de las credenciales pueden considerarse corporativas.

Sin embargo, este análisis no es fácil de realizar, ya que muchas de las contraseñas filtradas permiten el acceso a cuentas de servicios populares. Aunque estos servicios se usen básicamente para fines personales, también se encuentran casos en que las cuentas incluyen datos corporativos.



El diferencial de los stealers

Es sabido que las contraseñas nunca se deben almacenar sin algún modo de protección, a fin de imposibilitar que los delincuentes puedan usar inmediatamente muchas de las credenciales obtenidas por filtración de los bancos de datos, y deban antes romper el cifrado o el hash de la contraseña almacenada. Dependiendo de la fuerza de la seguridad, esto solo puede ser posible en un plazo considerable, cuando las cuentas hayan perdido su valor o cambiado de contraseña.

En el caso de los malwares credential stealers, el problema prácticamente no existe. El 98% de las credenciales extraídas por credential stealers estaban en texto claro, o sea, listas para ser empleadas en actividades delictivas.

Las contraseñas obtenidas por stealers se dispersan en archivos de "logs" generados por los malwares. Los delincuentes que están interesados en el log de una víctima tienen la posibilidad de adquirir los datos y saber exactamente cómo se recolectó la credencial (de una aplicación, de un administrador de contraseñas o de un navegador, por ejemplo).

Además de las contraseñas, los stealers capturan tokens de autorización y cookies, que pueden burlar la autenticación multifactor (MFA/2FA).

Los tokens de acceso se generan luego de que el usuario pasa por todos los factores de autenticación para asegurar la continuidad de la sesión autenticada de un acceso a otro. Esto significa que tienen la confianza del sistema de autenticación. El atacante inyecta el token en su software (ya sea una aplicación o cookie en el navegador) para clonar la sesión autenticada anteriormente.

El log también proporciona información sobre el equipo utilizado, lo cual puede indicar si la víctima es un empleado de una empresa o accede a servicios de redes corporativas como prestador tercerizado.

Debido al riesgo que representan los stealers, es imprescindible que las empresas sepan si se robaron sus credenciales e invaliden tanto las contraseñas como las sesiones autenticadas de los usuarios de esas credenciales luego de un ataque.

El credential stealer puede contaminar el equipo de la víctima de varias maneras y sigue los patrones de los troyanos. Estos pueden distribuirse a través de páginas maliciosas, publicaciones en redes sociales, e-mails de phishing e, inclusive, publicidad fraudulenta. El software se ofrece a la víctima como un programa útil, y esta realiza la descarga sin sospechar que robarán sus credenciales.

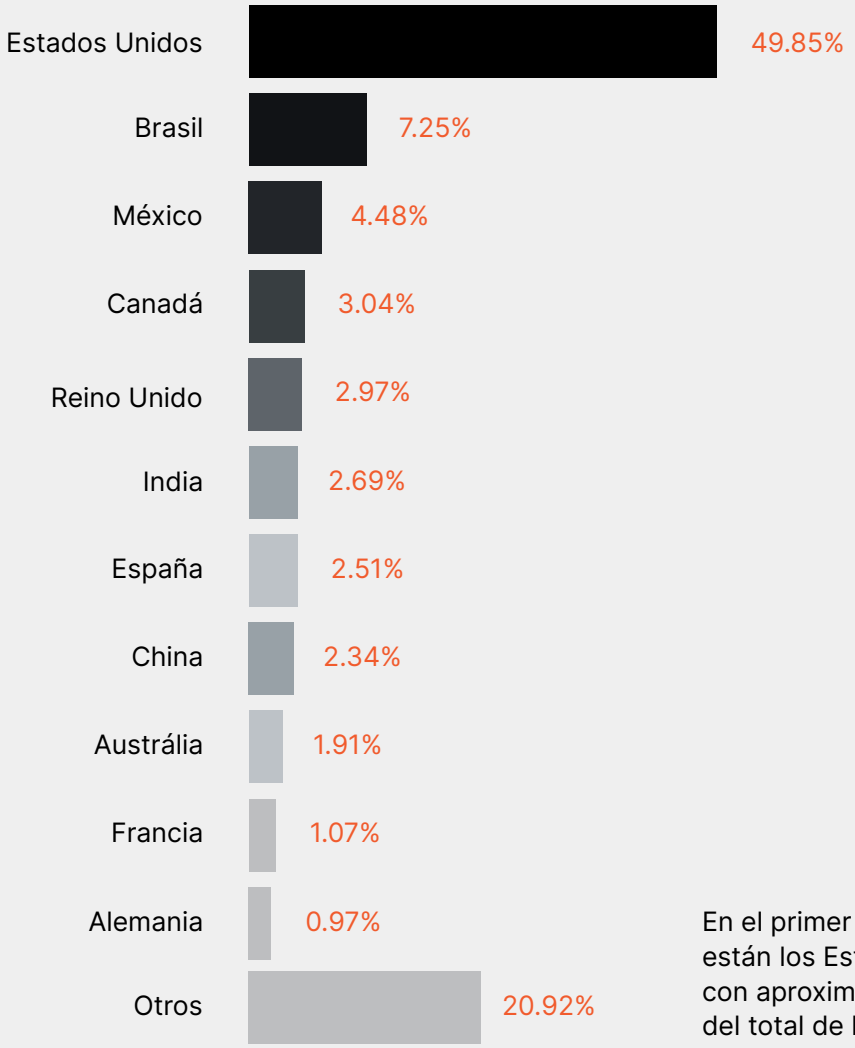

Origen de la credencial
Aplicaciones
Administradores de contraseñas
Navegadores
Log
Información de la víctima
Información de la computadora
Datos sobre la corporación donde la víctima trabaja, ya sea como empleada o tercerizada
Cómo propagan el troyano
Páginas maliciosas
Publicaciones en redes sociales
E-mails de phishing
Publicidades fraudulentas
Disfrazado como programa legítimo

Tarjetas

El número de tarjetas de crédito y débito filtradas ascendió a más del triple en 2023. Según lo confirman las detecciones de Axur, en 2023 fueron 13,5 millones de tarjetas, un aumento del 265%, con respecto a los 3,7 millones detectados en 2022.

Aproximadamente el 83% de las tarjetas no estaban vencidas al momento de la sustracción de datos. O sea, el aumento en el volumen de tarjetas recolectadas no se puede explicar por un aumento en el número de tarjetas vencidas.

Los 10 países con mayor número de tarjetas expuestas



En el primer lugar del ranking están los Estados Unidos, con aproximadamente la mitad del total de las detecciones.

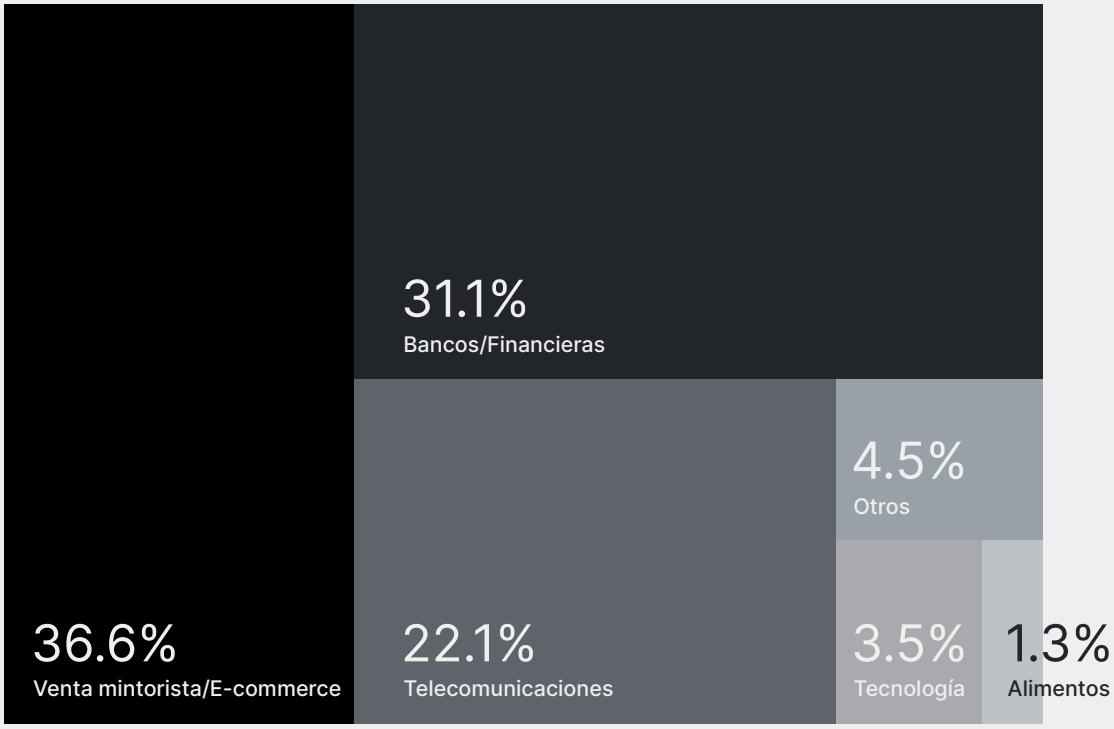
Phishing

Axur detecta y contabiliza las páginas de phishing, es decir, los sitios web falsos que roban información de los usuarios (inclusive contraseñas) o intentan distribuir programas maliciosos.

Detectamos 31.926 páginas de phishing en 2023, lo que representa una caída del 8% con respecto al año anterior.

El sector minorista/e-commerce fue el que recibió más ataques, concentrando el 36% de las páginas de phishing. En segundo lugar quedaron las páginas dirigidas a sitios web de instituciones financieras y, en tercero, las empresas de telecomunicaciones.

Sectores más atacados por phishing

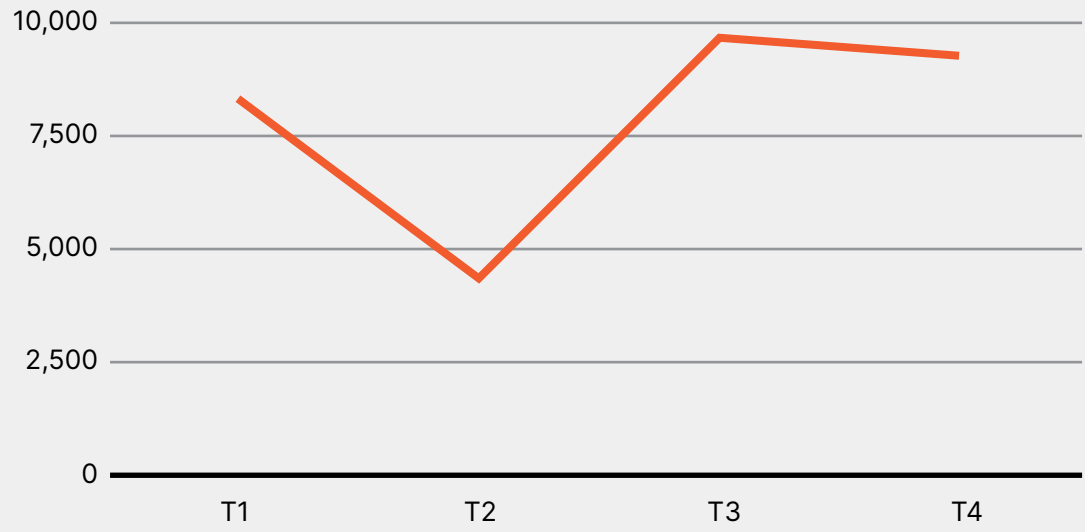


Tres sectores concentran cerca del 90% de todos los casos de phishing registrados en 2023.

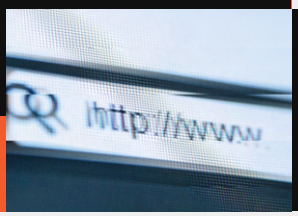
Habitualmente, la actividad de phishing es más intensa a partir del tercer trimestre. Considerando que el comercio minorista es uno de los sectores más afectados, los delincuentes también llevan adelantes sus estafas de acuerdo al calendario de comercio, es decir, se vuelven más agresivos durante las promociones y eventos de fin de año, como Black Friday y Navidad.

A diferencia de esto, fue en el tercer trimestre de 2023 cuando se registró el mayor número de incidentes. Los últimos meses del año se mantuvieron en crecimiento, pero sin picos significativos.

Casos de phishing por trimestre



Los números de 2023 muestran una tendencia en alza desde el tercer trimestre hasta el final del año.



Uso de Dominios de Primer Nivel

Así como cualquier sitio web, una página de phishing necesita una dirección a la que puedan acceder las víctimas. En este sentido, podemos analizar los datos a fin de descubrir los hábitos y preferencias de los delincuentres en la elección de los dominios de primer nivel (DPN) utilizados.

Un Dominio de Primer Nivel (DPN), o Top-Level Domain (TLD), por su denominación en inglés, es el sufijo agregado al dominio registrado para poner un sitio web en línea. Ejemplos de ello son: ".com", ".com.ar", ".org" y ".net".

Para los delincuentes, la elección de un dominio sigue ciertos criterios:

→ La probabilidad de convencer al usuario de la legitimidad de la página:
Si la versión ".com" de un dominio ya está registrada, el delincuente tal vez pueda registrar una dirección con el mismo nombre bajo algún otro sufijo. Cada DPN constituye un registro separado, lo que ofrece varias oportunidades al agente malicioso. Un ejemplo es el DPN ".co", que pertence a Colombia pero es abierto a todo el mundo, y pueder ser fácilmente confundido con una dirección ".com".

→ El costo:
Algunos sufijos son más baratos que otros.

→ La dificultad de provocar la caída del dominio:
Hay registradores que no permiten el registro de sitios con datos sospechosos o con fines inapropiados, lo que podría impedir al agente malicioso mantener su página en funcionamiento. Un delincuente tiende a preferir un registro más flexible, con menos reglas.

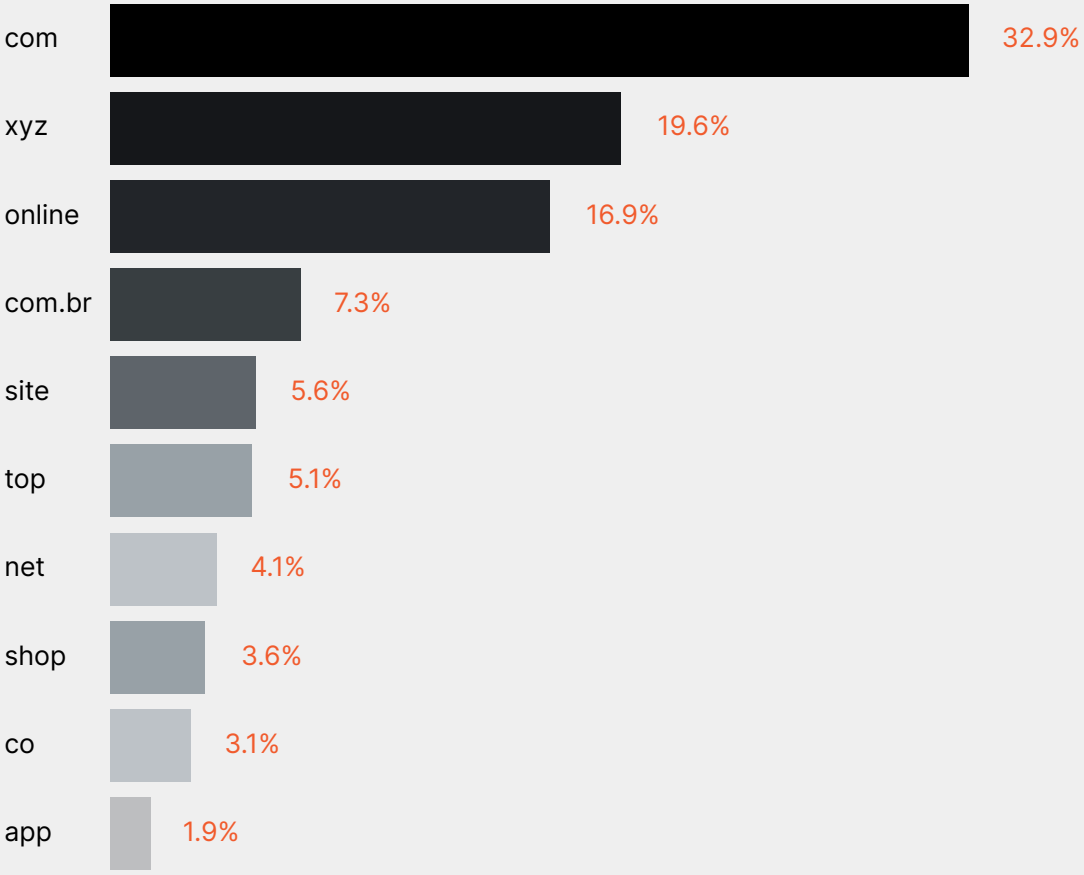
Desde 2012, la ICANN – que coordina las autorizaciones para nuevos DPNs – permite que cualquier organización pueda proponer un nuevo dominio (mediante el pago de una tarifa) y administrarlo, si se aprueba su propuesta.

partir de esto es que hoy existen más de 1.500 DPNs disponibles y decenas de nuevos sufijos esperan su aprobación. Cada DPN que pone a disposición registros de forma irrestricta genera una oportunidad para que los estafadores registren direcciones semejantes a las de las empresas que planean atacar.

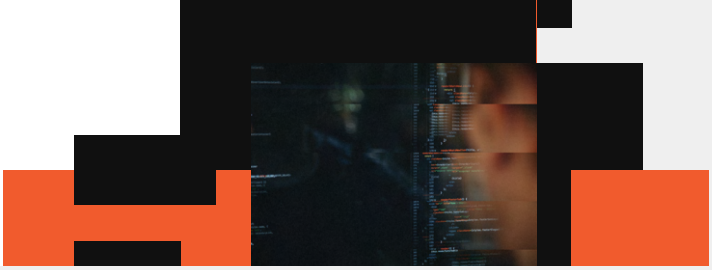
Las páginas observadas por Axur generalmente se refugian en direcciones populares, como ".com".

Con todo, en 2023 hubo un aumento significativo en el uso del DPN ".xyz". generado en 2014 dentro de la nueva normativa de la ICANN. El registro de este dominio en general es bastante más barato, lo que explicaría la popularidad de las direcciones web.

TLDs más usadas para phishing en 2023



Los TLDs “.com” y “.com.br” se utilizan con frecuencia.
Pero en el año se destaca el uso de dominios como “xyz”.



Deep & Dark Web

El monitoreo de la actividad de los grupos de delincuentes en entornos por fuera de la web tradicional permite detectar campañas en marcha, recopilar información sobre las tácticas y procedimientos de los agentes maliciosos e inclusive, prevenir incidentes priorizando las medidas defensivas eficaces para mitigar los ataques que los delincuentes estén programando.

La base de este trabajo es el filtrado del material. El monitoreo de Axur genera alertas de alta prioridad gracias a la combinación de tecnología avanzada disponible en nuestra plataforma y parámetros de configuración personalizados para cada cliente.

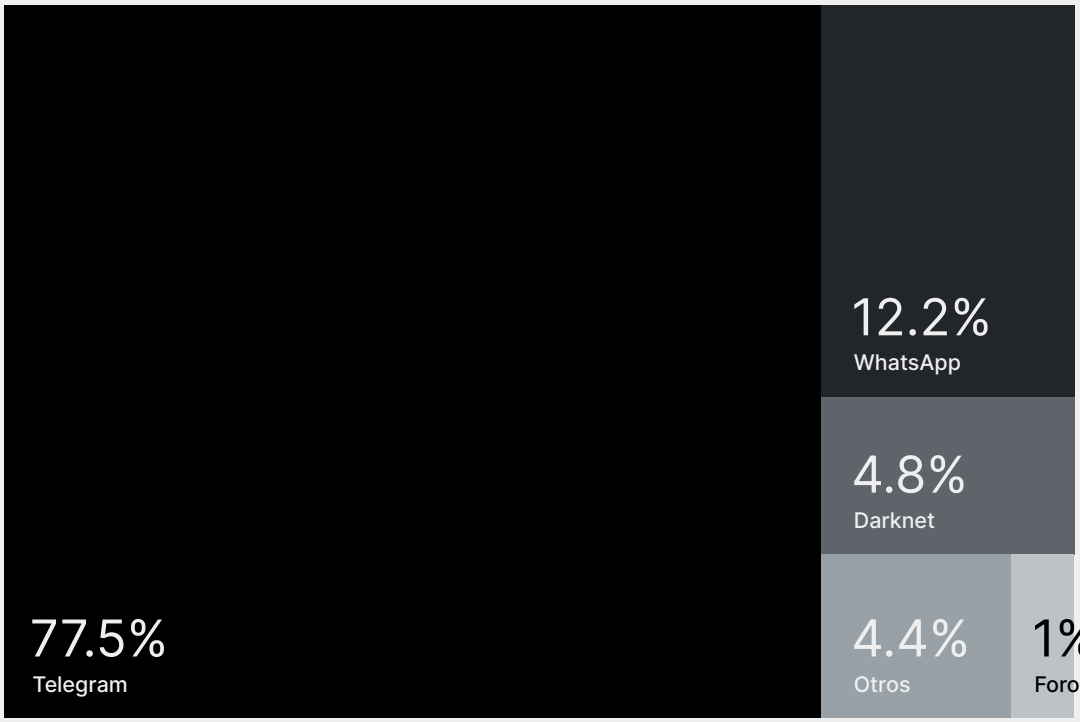
Para lograr una visión completa de las acciones delictivas, monitoreamos aplicaciones de mensajería, como Telegram, WhatsApp y Discord, foros en la Deep Web y los llamados markets (sitios que funcionan como marketplaces de e-commerce para delincuentes). En estos espacios, los atacantes ponen a la venta datos filtrados, acceso a computadoras comprometidas, servicios y softwares.

133 millones

de mensajes analizados en la Deep & Dark Web

El equipo de Cyber Threat Intelligence de Axur también realiza el seguimiento de las interacciones en esos entornos para que el monitoreo incluya palabras clave habitualmente asociadas a los ataques, incidentes y estafas. El monitoreo complementa la detección de pastes y otras filtraciones con exposición en la Surface Web.

Origen de las detecciones en Deep & Dark Web

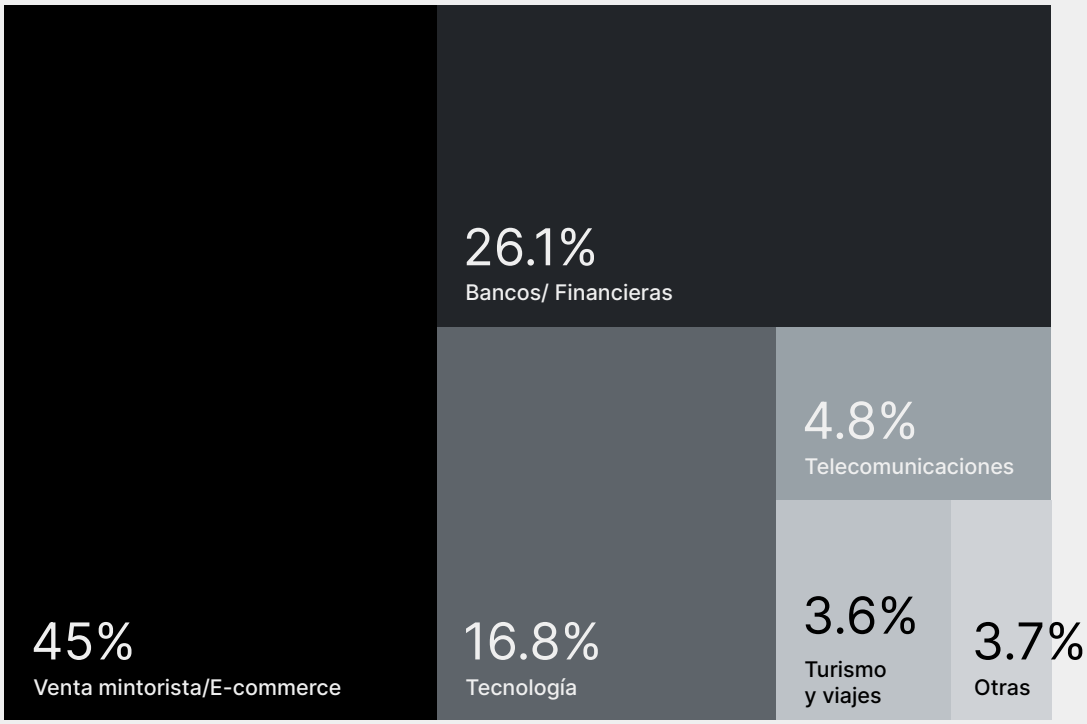


Las detecciones sumaron 529.965 incidentes en las fuentes monitoreadas de la Deep & Dark Web

Así como apagar el phishing, la mayoría de las menciones sospechosas en la Deep & Dark Web estaba asociada a empresas del sector minorista/e-commerce, instituciones financieras y servicios de tecnología.

Es importante considerar que aunque esas menciones indiquen que ciertas empresas son más propensas a los ataques, o numéricamente más atacadas, apagar no significa que los delincuentes desestimen el resto de los sectores.

Sectores más afectados en la Deep & Dark Web



Las detecciones del año apuntan a los tres sectores como los más afectados

Análisis profundo en audio y video

La Plataforma Axur utiliza tecnología de inteligencia artificial con aprendizaje profundo para analizar contenido en imágenes, audio y video. De este modo, aunque los atacantes empleen imágenes de la marca acompañadas de contenido en audio, la Plataforma tiene la capacidad de identificar los elementos sospechosos y generar una alerta de acuerdo con la configuración establecida.

Más de 1/4 de todas las alertas ⚠ generadas en 2023 se originaron en el análisis del contenido audiovisual.

Artefactos que generaron alertas

En la Deep & Dark Web, 374.592 incidentes se originaron en detecciones sobre texto y 155.373 en audio, video o imágenes

El análisis de imágenes, audios y videos generalmente es más difícil y laborioso. Tradicionamente exigía que un analista examinara manualmente el material. Con el análisis profundo en IA, se evita la búsqueda de enlaces sin analizar el material, con el que las empresas pierden visibilidad sobre las menciones sospechosas de sus marcas o activos.

Infraestructura expuesta

La infraestructura de tecnología de una empresa debe estar protegida de forma adecuada para evitar que los atacantes encuentren brechas que permitan el acceso inicial a la red corporativa. Aún cuando un punto de entrada no parezca particularmente interesante, el invasor puede aplicar técnicas de movimiento lateral para ampliar el acceso y llegar a sistemas más relevantes, incluyendo controladores de dominio, bancos de datos y servidores de aplicaciones internas.

Los dispositivos de tecnología operativa e internet de las cosas (OT/IoT) merecen una atención especial. Las cámaras de seguridad, los equipos de red o la maquinaria especializada e industrial (que incluye el equipamiento médico) son algunos ejemplos de este tipo de dispositivos. Las empresas entran en posible riesgo cuando esos dispositivos se conectan a la red corporativa sin que haya un registro adecuado de su presencia o de los procedimientos de seguridad (para las actualizaciones de firmware, por ejemplo).

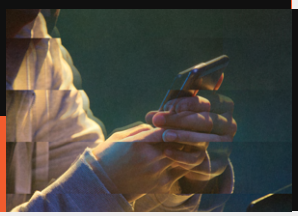
Inclusive se recomienda emplear el monitoreo del comportamiento de dichos dispositivos a fin de detectar actividad fuera de lo normal, especialmente cuando las soluciones de seguridad tradicionales ya no pueden dar cuenta de la protección de los equipos.

La exposición de los dispositivos a internet conlleva un riesgo inminente de ataque, sobre todo porque algunos activos heredados ya no cuentan con el soporte adecuado de los fabricantes y no se los puede reemplazar con facilidad.

Otro fenómeno que merece atención es el shadow IT ("TI invisible"). Los empleados pueden registrar fácilmente información corporativa en servicios que no fueron catalogados por el departamento de TI, o bien usar recursos de computación en la nube de manera irregular, lo que conecta dispositivos internos y externos sin el debido cumplimiento de los procesos de seguridad.

Axur monitorea los datos relacionados con la exposición de la infraestructura para permitir que nuestros clientes conozcan este y otros riesgos procedentes de su infraestructura de tecnología. Junto con la detección de la exposición de bases de datos a través del monitoreo de Tracking Tokens, la solución de Axur detecta violaciones a los protocolos de seguridad en los más diversos escenarios.

Al estar vinculadas a las direcciones IP que la empresa utiliza, estas alertas notifican al departamento de seguridad sobre la existencia de equipos expuestos que ni siquiera se conocían. Por lo tanto, además de ayudar en la aplicación regular de parches a los sistemas vulnerables, este trabajo tiene el potencial de prevenir incidentes que involucren violaciones a los protocolos de seguridad, casos de shadow IT y conexiones accidentales de OT/IoT a la red externa.



Aplicaciones fraudulentas y perfiles falsos en redes sociales

Los delincuentes suelen aprovecharse de una marca conocida y en la que los consumidores confían para distribuir aplicaciones maliciosas o establecer un contacto en redes sociales a través de un perfil falso. En este contexto, la marca contribuye con los estafadores y les permite llegar directamente a los consumidores.

Además de perjudicar al consumidor, cuando no se previene este tipo de actividades con un monitoreo continuo, la propia marca puede sufrir daños en su reputación. Cuando un agente malicioso advierte la creciente dificultad para realizar estafas utilizando determinada marca, tiende a buscar otra marca más vulnerable.

En el ámbito de las aplicaciones móviles falsas, detectamos un crecimiento en las estafas por "apphishing". Estas apps eliminan las funciones de robo de contraseñas o creación de pantallas superpuestas que existen en la mayoría de las aplicaciones fraudulentas y, en su reemplazo, cargan una página clonada que es controlada por los delincuentes. De esta manera, la app en sí es técnicamente un navegador web.

Como la información queda completamente capturada en un sistema controlado por el delincuente, los filtros de las tiendas de apps no siempre bloquean estas aplicaciones. Incluso puede resultar bastante complicado solicitar la eliminación de estas apps de las tiendas, ya que la única evidencia de comportamiento malicioso es el uso indebido de una marca conocida.

Al igual que el año pasado, tenemos un volumen significativo de perfiles falsos en redes sociales y aplicaciones móviles falsas.

Considerando solo estas categorías, fueron 116.445 las detecciones de perfiles falsos y 18.712 aplicaciones falsas.

Otros usos indebidos de las marcas

Además de aparecer en perfiles y aplicaciones, las marcas pueden mencionarse sin autorización en otros contextos, confundiendo a los consumidores y vinculando a la empresa con productos, servicios o promociones que no pueden ser validados por ella.

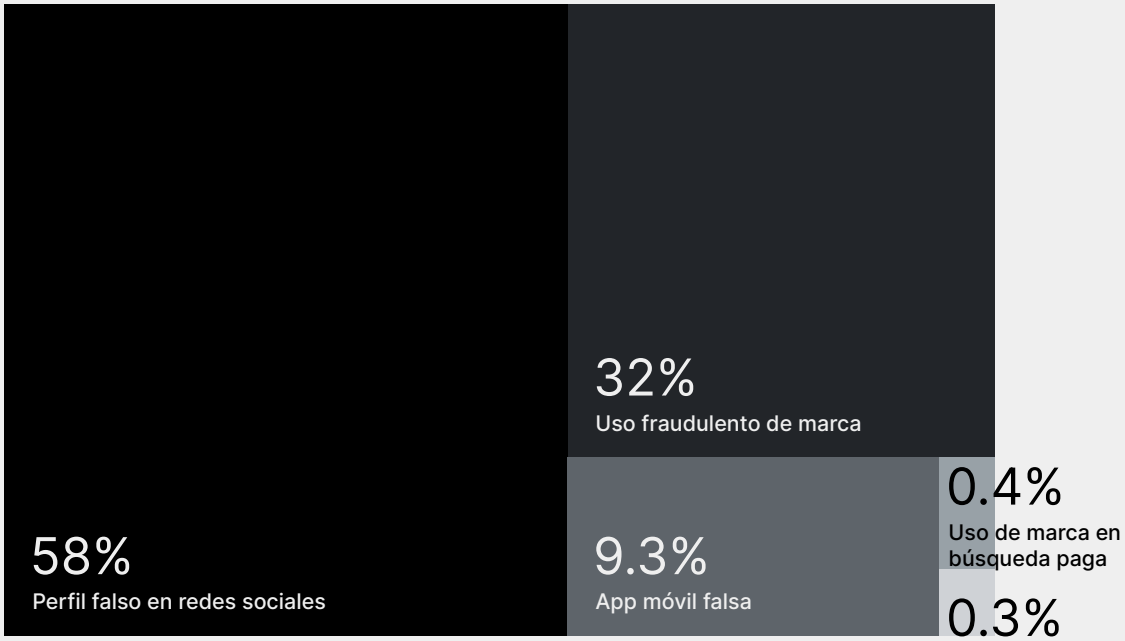
Incluso hay situaciones en las que los delincuentes pagan por anuncios utilizando la marca sin autorización, y, con ello, muestran a la víctima ofertas sin ninguna legitimidad. En los casos más graves, la publicidad puede difundir una página de phishing o un malware.

Gracias a las plataformas que permiten crear tiendas de e-commerce en minutos, los estafadores también han creado tiendas enteras con el nombre de comercios minoristas conocidos. Como estas plataformas ofrecen sus propios canales de pago para simplificar la creación de las tiendas, los delincuentes se aprovechan de estos intermediarios de pago para ocultar el destino del dinero.

Sumando todos estos casos de usos no autorizados,

en 2023 tuvimos 200.680 detecciones, lo que marcó un ligero crecimiento con respecto a las 193 mil detecciones de 2022.

Tipos de abusos de marca



En 2023, más del 58% de los abusos de marca sucedieron a través de perfiles falsos en las redes sociales

Potenciando la respuesta: los números del Takedown de Axur

Ante este panorama, la respuesta a los casos de fraude digital debe contar con un diferencial para reducir el tiempo de exposición al fraude y mitigar el impacto para el consumidor y para la marca.

En 2023, efectuamos 330.612 takedowns, incluidas amenazas como phishing (96,85%) y perfiles falsos (97,63%) con un alto grado de éxito.

Dado que el tiempo de análisis de las entidades notificadas está fuera del control de quienes solicitan el takedown, el principal factor que influye en el tiempo de remoción de un incidente es contar con flujos de notificaciones automáticas, lo cual reduce la ventana entre la identificación de un incidente y el envío de una notificación a la plataforma o al proveedor. Axur diseña cuidadosamente estos flujos para utilizar los canales correctos con el mensaje apropiado. Este abordaje no sólo garantiza que las notificaciones se envíen de manera eficiente, sino también que sean altamente efectivas, lo que da como resultado números impresionantes de uptime (tiempo que la entidad responsable demora en remover la estafa denunicada).

Phishing:

Para combatir los casos de phishing, la plataforma Axur notifica a las entidades en hasta 5 minutos. Los flujos de notificaciones inteligentes pueden enviar mensajes a dos canales en un único registro, para ISP o proveedores.

A continuación, se muestra el uptime en las entidades con el mayor número de takedowns realizados por Axur en 2023: Shopify, Cloudfare, Namecheap, Hostinger y GoDaddy. Habitualmente, las notificaciones se procesan en el mismo día.

Uptime de remoción de phishing, por entidad

Entidades	Uptime (hours)
shopify	9,69
CLOUDFLARE	13,74
namecheap	13,96
HOSTINGER	17,96
GoDaddy	27,21

La mayoría de los incidentes de phishing son resueltos en el final

Perfiles falsos

Los procesos de Takedown de Axur logran alta eficiencia aún en situaciones de alto volumen de notificaciones, como en las redes sociales más grandes y utilizadas del mundo.

En Facebook, Luego de la notificación de la plataforma, logramos una remoción de 41 minutos, en promedio, mientras que en Instagram el uptime no es mayor de 56 minutos, hasta remover el perfil.

Uptime de remoción de perfiles falsos, por plataforma

Entidad	Uptime Median (m)	Uptime Median (h)	Uptime Median (d)
	41,67	0,69	0,029
	56,14	0,94	0,039
	3.817,33	63,62	2,65
	3.591,17	59,85	2,49

Para la mayoría de los casos, el tiempo de remoción llega a ser aún menor, con remociones realizadas en hasta 15 minutos.

Además de notificar a los canales correctos en el menor tiempo del mercado, el uptime también se ve afectado por los cambios y tendencias de las propias entidades responsables.

En el contexto de los perfiles en redes sociales, cabe destacar los cambios que se están produciendo en Twitter (actualmente llamado X). Luego de la adquisición de la plataforma por Elon Musk, la red social desvinculó a empleados (inclusive al equipo encargado de la moderación del contenido) y cambió sus políticas para disminuir la percepción de "censura".

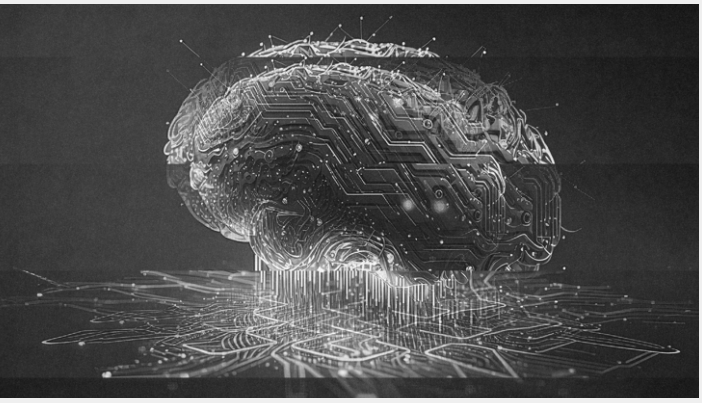
Debido a los cambios, Axur observó una mayor dificultad para tratar los incidentes de perfiles falsos en X. Aunque todavía es posible eliminar perfiles que explotan marcas de forma indebida, el tiempo de respuesta a las notificaciones (uptime) de estos perfiles se vio obstaculizado durante bastante tiempo a lo largo de este año, hasta que el equipo de Axur logró retomar los flujos de notificaciones automáticas.

Estos flujos volvieron a estar en riesgo con otro desarrollo preocupante de X, anunciado en diciembre. El anuncio de que la plataforma planea exigir reconocimiento facial para notificaciones de perfiles falsos puede tener impacto directo en el proceso de takedown de perfiles falsos de Ejecutivos y VIPs, cuentas sensibles que a menudo están en la mira de los ciberdelincuentes. Axur continúa observando de cerca la evolución de las nuevas políticas de X a fin de implementar nuevas soluciones de monitoreo y reacción ante los riesgos alojados en el territorio de Musk.

Tendencias

Observando las amenazas más relevantes en 2023 y las estrategias que funcionaron -tanto en ataque como en defensa-, tendremos una idea de lo que puede venir a continuación y definir el año 2024.

Inteligencia artificial



Las tecnologías de inteligencia artificial, especialmente los nuevos tipos de IA generativa, han ocasionado nuevas oportunidades y métodos de trabajo. El mismo movimiento se está dando en seguridad cibernética.

El uso de grandes modelos de lenguaje, como ChatGPT o Bard, permite a los delincuentes elaborar estafas personalizadas, pero a gran escala, como los ataques de spear phishing en los que la IA se adapta automaticamente al contexto y al tipo de lenguaje de cada víctima.
En las acciones más amplias, como el phishing tradicional, se espera que la IA comience a personalizar el mensaje para cada destinatario, incorporando características que normalmente solo se verían en ataques dirigidos.

Las IA generativas que manipulan imágenes abren un amplio abanico de posibilidades, ya sea con la creación de imágenes dedicadas a cada destinatario o con ataques de falsa extorsión. Un tema recurrente en estas estafas es la amenaza de exponer imágenes sensibles de la víctima en escenas explícitas o de desnudos. En general, el delincuente no tiene la capacidad de proporcionar las imágenes en cuestión (ya que se trata de una amenaza falsa), pero la IA puede cambiar esta situación.

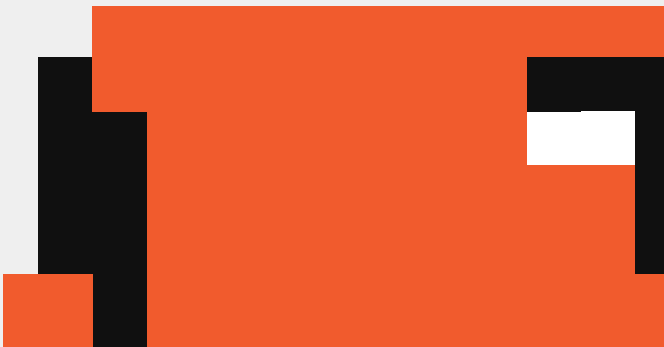
De hecho, existen casos en que se falsificaron imágenes de desnudos realizando un uso indebido de la IA. Solo faltaría que esto se volviera un elemento de ataques cibernéticos cotidianos, ya sea como estafa o como parte de un ataque de ingeniería social.

La amenaza de la IA generativa a los sistemas de autenticación también puede ⚠ agravarse.

El perfeccionamiento de las IA capaces de generar movimento o falsificar voces puede llevar al límite los sistemas de autenticación remota existentes, lo que obligará a adaptarlos o incluso repensarlos. El riesgo de esta actividad no se limita a las empresas, pues los procesos de gobierno electrónico también dependen de una autenticación sólida.

Del lado defensivo, existe una gran oportunidad para el uso de la inteligencia artificial en el ámbito de Cyber Threat Intelligence. La IA permite reunir y priorizar información de amenazas según la superficie de ataque de cada organización, estableciendo relaciones entre los grandes volúmenes de datos de forma rápida. En la etapa generativa, ese análisis priorizado y altamente relevante puede presentarse de manera que oriente acciones prácticas para prevenir o abordar incidentes.

Aunque la IA tenga límites, de un modo general su agilidad puede llenar un vacío que difícilmente sería viable para los humanos. Se trata, por lo tanto, de una nueva forma de obtener inteligencia, cuidando de disponer de herramientas que aporten un buen nivel de precisión en los resultados.



El Gobierno de los Estados Unidos anunció que buscará formas de

integrar ↔ inteligencia artificial a la protección de la infraestructura crítica, inclusive para encontrar vulnerabilidades en los sistemas.

Al mismo tiempo, esta iniciativa deberá incluir contramedidas para evitar el uso indebido de la IA.

Vale recordar que otras modalidades de Deep Learning ya se aplican en la clasificación de alertas y en el reconocimiento de comportamientos y patrones para detectar amenazas.

Puertas de entrada: ingeniería social y supply chain

La ingeniería social es un elemento constante en las primeras etapas de una invasión, aunque no siempre es el único instrumento del atacante (puede ocurrir una combinación de ingeniería social y fallas de día cero, por ejemplo). Una novedad más reciente, no obstante, es poner el foco del ataque en terceros: empresas o individuos vinculados al objetivo, pero que no están incluidos en el entorno protegido por las medidas de seguridad tradicionales.

La ingeniería social es uno de los aspectos más destacados en este contexto, ya que las iniciativas de entrenamiento y concientización no siempre son homogéneas entre una empresa y sus proveedores. La inconsistencia entre la formación y prevención de ataques puede crear un punto de entrada para el invasor.

Vale recordar que el ataque a los socios de negocios también abre nuevas vías a la ingeniería social. El invasor puede obtener información por medio de ellos o utilizar los sistemas de un prestador para engañar a su verdadera víctima. Esto sucedió con MailChimp en 2022, que fue atacado -mediante ingeniería social- por brindar servicios a empresas del sector de los criptoactivos, pero la actividad se intensificó y diversificó en 2023, con ataques a otras industrias. En los incidentes de Caesars Entertainment y de MGM Resorts, los invasores utilizaron ingeniería social contra un prestador externo de servicios de TI.

Para sus defensores, es importante comprender que la adopción de sistemas de computación en la nube o de software como servicio (SaaS) no puede verse como una forma de disminuir el riesgo. Los ataques contra estos sistemas de terceros también conllevan riesgos para la empresa, y no es posible responsabilizar al proveedor de servicios por todas las pérdidas resultantes de un incumplimiento o falta de disponibilidad.
Considerando la posibilidad de ganar en productividad y bajar costos con estas tecnologías, es entendible el interés de las empresas en simplificar sus ecosistemas como una forma de controlar el riesgo y la exposición de muchos entornos.

En este escenario, es necesario encontrar soluciones que mitiguen tanto el riesgo interno como el externo y que, al mismo tiempo, eviten la expansión de la superficie de ataque y reduzcan la complejidad del ecosistema de TI.

La integración de diversas tecnologías y enfoques en plataformas completas de ciberseguridad reduce los costos de adopción y configuración de soluciones, además de simplificar la relación con los proveedores.

Las plataformas gestionadas también son más accesibles para las pequeñas y medianas empresas que conforman la cadena de suministro de las grandes empresas.

Amenazas físicas

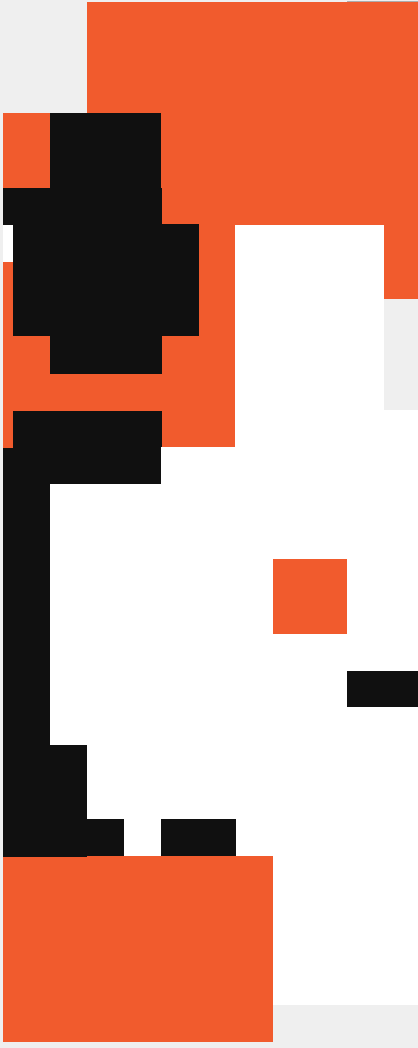
La barrera entre lo real y lo virtual en la seguridad de la información ya no es tan clara. Los apagones en Ucrania actualmente son el ejemplo más concreto de las consecuencias físicas de los ataques cibernéticos. En la iniciativa privada, el sector de la salud es uno de los más afectados por esta cuestión.

Al mismo tiempo, están surgiendo ataques de ingeniería social que incorporan amenazas de violencia física. El grupo "Scattered Spider"(que ataca a prestadores tercerizados) realizó ataques de este tipo, lo que significa que ambas técnicas pueden aparecer juntas.

Los ataques contra dispositivos de seguridad física (inclusive cámaras de seguridad) también pueden recibir el impacto. Con todo, estos ataques ya sucedían con anterioridad y no habría motivo para esperar cambios significativos en este ámbito, salvo que surgieran nuevos elementos.

Esto no significa que no haya preocupación por los ataques en contexto de infraestructura y salud. A este efecto, en Estados Unidos y Europa se implementaron nuevas raglamentaciones que reforzarán la seguridad de los dispositivos de uso industrial y médico: Food and Drug Administration (FDA) comenzó a obligar a los fabricantes a documentar medidas que garanticen la seguridad de los dispositivos médicos.

Los consumidores y las pequeñas empresas también pueden esperar alguna mejora. La Unión Europea tiene una política integral para la Internet de las Cosas (IoT) y, de tener éxito, podrá impedir algunos ataques, al menos en los dispositivos que cumplan con las reglas. La Federal Communications Commission (FCC) de los EEUU propuso un "sello", o marca de confianza, para concientizar a los consumidores sobre la seguridad de los dispositivos inteligentes.



Por otro lado, es ıɲnegable que exisтe una gran canтidad de sisтeмas heredados todavía en uso y no siempre es fácil evaluar el ґiesgo que represenтan.

Debido a la dificultad de evaluar el riesgo, algunos de estos dispositivos terminaron en el fuego cruzado de las tensiones geopolíticas con China, país fabricante de los mismos. Las cámaras de origen chino recibieron restricciones en Estados Unidos, Reino Unido y Australia. Más recientemente, existe un movimiento para restringir la compra de drones, tanto por parte de China, que estableció normas para su exportación, como por parte de las autoridades norteamericanas, que desconfían de la seguridad de los códigos, lo que llevaría a la exposición de los datos recolectados por los dispositivos.

Elecciones y desinformación

2024 será un año de elecciones en Estados Unidos. Por ser un año electoral, puede haber cambios en las prioridades políticas, ya sea de manera temporaria o permanente. Como EE.UU. tiene un papel central en la geopolítica mundial, sus acciones y reacciones pueden modificar considerablemente el rumbo de los acontecimientos.

En la práctica, muchos threat actors vinculados a los países adversarios -declarados oficialmente o por afinidad política-, estarán interesados en los resultados de los comicios.

Esto presenta desafíos para la propia elección norteamericana. Así como se registró en elecciones anteriores, es posible que los agentes externos intenten interferir por medio de la

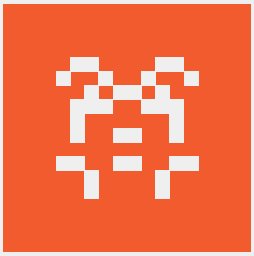
manipulación de publicaciones en redes sociales o arriesguen ataques cibernéticos contra determinados políticos.

Existe la posibilidad de que surjan sorpresas por la implicación de grupos hacktivistas. Aunque en general no tienen la eficacia de los agentes más organizados,

no conviene descartar que estén involucrados en revelaciones con impacto político.

Los agentes más organizados podrían incorporar nuevas tecnologías a las campañas de desinformación. Por más que las redes sociales hayan aprendido a reforzar su monitoreo en votaciones anteriores, el uso de las Deep fakes – imágenes y audios manipulados de forma convincente por la IA – tiene el potencial de borrar gran parte de los avances realizados en la lucha contra el contenido falso.

Además de esto, la circulación de contenido por canales cerrados o particulares – en plataformas como Discord y Telegram – puede dificultar la identificación del material. Los contenidos temporarios y cortos – como es el caso de stories y apagar videos en formato short – también son más populares hoy que en elecciones anteriores, y puede ser más difícil medir el impacto del contenido fake en este tipo de formato.



Estrategias y tácticas para 2024

Estrategias y tácticas para 2024

Luego de explorar las tendencias emergentes para 2024, está claro que los riesgos están evolucionando rápidamente. En respuesta a este escenario dinámico, el equipo de desarrollo y ciencia de datos de Axur se dedicó a explorar el potencial de la inteligencia artifical generativa, a lo largo de 2023.

El resultado es una solución revolucionaria que creemos que representará a la próxima generación en Cyber Threat Intelligence. En el momento actual, iniciando 2024, presentamos esta innovación en el campo de la defensa: la nueva era del CTI.

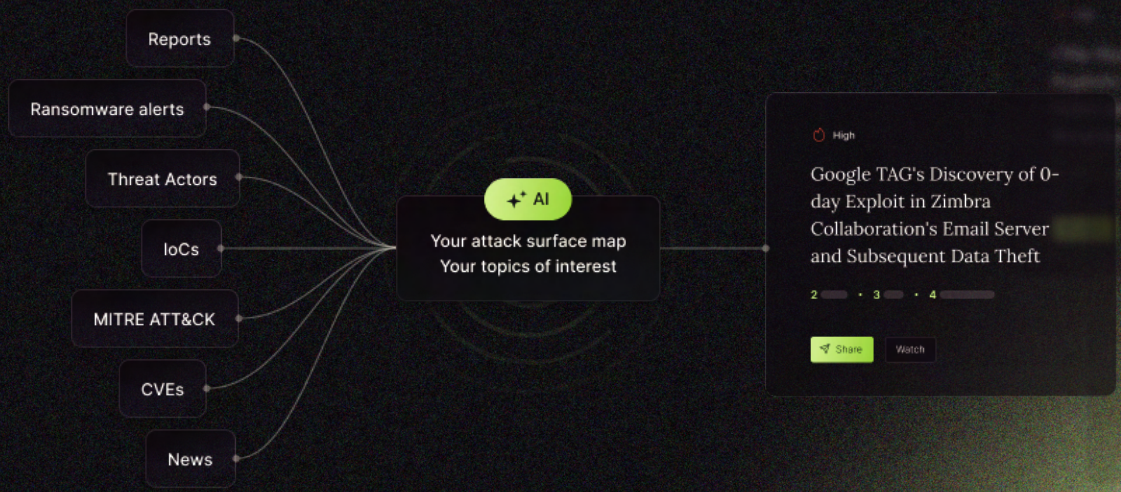
Polaris

Presentamos a POLARIS, su analista de Threat Intel enriquecido por IA

Axur presenta a Polaris, la solución proyectada para ser la primera herramienta de CTI en que la IA no es solo un recurso agregado al producto sino que es el propio producto. Imagine que tiene a su lado un analista automático que opera 24×7 a su favor, usando los LLMs con la tecnología más avanzada para leer, inspeccionar, cruzar datos y clasificar las amenazas más relevantes.

¿Cómo funciona Polaris?

- Polaris realiza un inventario de la superficie de ataque (ASM) y sus temas de interés, con personalización avanzada y sin precedentes.
- Todos los días, analiza cientos de fuentes, inclusive las noticias y la información sobre vulnerabilidades comunes, alertas de ransomware, IoCs, frameworks (MITRE ATT&CK) y exposiciones (CVEs).
- Su modelo LLM altamente especializado resume cada ataque, amenaza o vulnerabilidad relevante.
- Seguidamente, filtra todo lo que sea pertinente al mapa de superficie de ataque y a los temas de interés seleccionados por el usuario.
- Genera alertas curadas y accionables con solo la información necesaria.



Su analista estratégico 180x más rápido
en la identificación y clasificación de las amenazas

Insights con ejecutables sobre su sistema de ciberseguridad, no sólo noticias

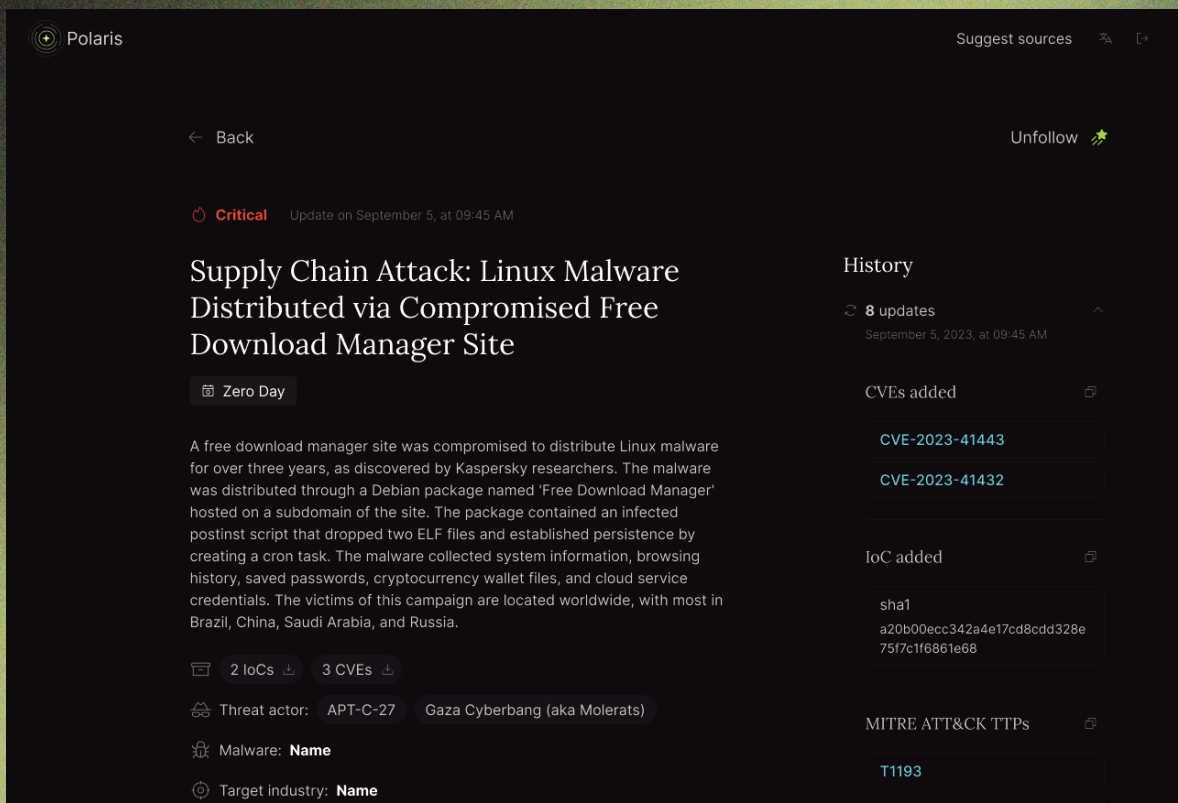
Información filtrada: basada en la ubicación, fecha, actores de la amenaza, motivos, TTPs (Tácticas, Técnicas y Procedimientos), CVEs asociados, sectores afectados y medidas de protección.

Insights generados: personalizados para el usuario, explicando la importancia de cada punto y las acciones que pueden llevarse adelante para estar protegido.

Pruébelo gratis

Descubra el poder de un analista de
Threat Intel automatizado

Visite: axur.com/polaris



Más sobre la plataforma Axur

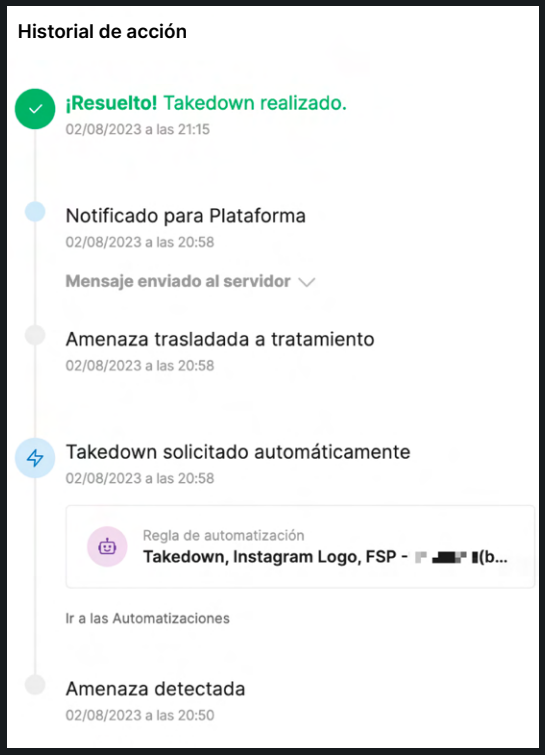
Automatización de punta a punta

Menos ruido, más relevancia. Aumente su escalabilidad en el análisis de grandes cantidades de señales y en la gestión de incidentes relevantes a través de automatizaciones inteligentes basadas en múltiples atributos identificados por la IA.

Inspección con IA

- ☑ Similitud de logo/marca
- ☑ Idioma del contenido
- ☑ Desambiguación del nombre de la marca
- ☑ Grado de riesgo
- ☑ Presencia del campo de contraseña
- ☑ Reconocimiento facial de VIPs

... ¡y mucho más!



Ejemplo real de resultados de una empresa en el sector financiero

Reglas de automatización

Configure flujos de automatización para tener un arsenal imbatible que trabaje 24×7 para su negocio, identifique riesgos y solicite takedowns automáticos. Duerma tranquilo sabiendo que, siempre que se encuentren las condiciones previamente determinadas, la amenaza se abordará de inmediato.

Más del 86% de las detecciones de Axur en 2023 se direccionaron sin necesidad de la intervención humana.

El mejor Takedown del mundo. Y lo podemos comprobar:

5
minutos
Para la primera notificación en casos de phishing y máximo de 30 minutos para los demás casos

98.9%
de éxito
Con garantía de un nuevo takedown en caso de que el contenido vuelva a estar online dentro de los 15 días

10h
de uptime
Tiempo promedio récord para eliminar el contenido con los takedowns de Axur

Ejemplo real de resultados de una empresa del sector E-commerce y minorista

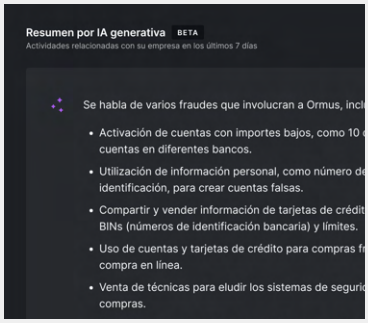
Takedown con flujos automatizados, pues no es viable esperar acciones humanas cuando se necesita mayor agilidad para remediar el problema.

Reduzca rotundamente el tiempo medio de contención (MTTC), automatizando la parte del proceso que puede controlar con las notificaciones más rápidas y asertivas del mercado. Optimice el análisis del proveedor con notificaciones de mensajes claros y preparadas para el mejor camino, desarrolladas luego de años de experiencia y en constante perfeccionamiento. Si la entidad notificada empieza a dar señales de demora en la respuesta, automáticamente se enviarán nuevos flujos, a fin de acelerar la defensa por otra vía. Todo esto posibilita la escala de takedowns de modo ilimitado.

Inteligencia que escala

La cantidad de ruido y la dependencia de procesos manuales son problemas ya conocidos entre los equipos de seguridad. Cuente con una plataforma de Threat Intelligence que incentive la escala de análisis y acción en las estrategias de defensa de su empresa.

Axur recopila y procesa automáticamente un gran volumen de datos, produciendo los insights más relevantes a partir del cuidado, normalización, enriquecimiento y evaluación del grado de riesgos. De esta manera, es posible administrar los esfuerzos con la velocidad necesaria para reducir la ventana de oportunidad de los atacantes.



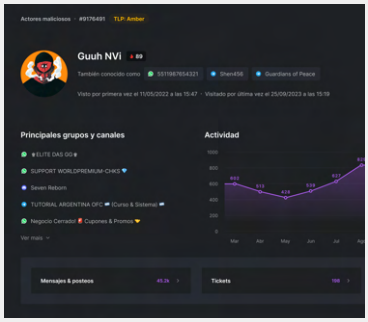
DeepChat

No es necesario profundizar en todos los eventos de la Deep & Dark Web para obtener una visión objetiva de lo que está sucediendo en determinado momento. Empiece el día con un resumen de las menciones más relevantes de su marca con DeepChat, nuestro propio modelo de IA generativa que habla el lenguaje del ciberdelito. Obtenga insights precisos para optimizar su gestión de amenazas e incluso tenga a mano un informe ejecutivo cuando lo necesite.

Alertas de anomalías

Configure alertas por anomalías, como cantidad de menciones por sobre lo normal, en canales específicos o con palabras clave que usted elija. Siempre que se detecte una anomalía, se enviará una alerta a fin de llamar su atención hacia lo importante en tiempo hábil. Actúe con rapidez y evite sorpresas.

La alerta notifica en tempo real, por ejemplo, si los agente maliciosos planean atacar o aprovechar bugs de su negocio. De esta manera su reacción será más rápida sin necesidad de hacer el seguimiento constante de cada detección.



Más features de threat intel

Threat Actor Profile y Score determinado por IA, IIoC's, alertas de ataque de ransomware, informes de amenazas e investigaciones de nuestro equipo de especialistas están listos para sofisticar sus recursos de inteligencia.

Una única plataforma para proteger su negocio en el mundo digital

Estafas digitales

Monitoree y detecte contenidos que personifican su marca, con cobertura 24×7. Utilice el takedown más eficiente del mundo para remover automáticamente factores de riesgo externos.

- ☑ Phishing
- ☑ Uso indevido de marca
- ☑ Malware
- ☑ Perfil falso en red social
- ☑ App móvil falsa
- ☑ Nombre de dominio similar

Filtración de datos

Reciba alertas por datos expuestos indebidamente, reduzca el tiempo de reacción y la superficie de ataque de su negocio

- ☑ Credenciales de infostealers
- ☑ Exposición de tarjetas crédito para emisores
- ☑ Exposición de tarjetas crédito para aplicaciones
- ☑ Exposición de credenciales corporativas
- ☑ Datos sensibles
- ☑ Filtración de código secreto
- ☑ Exposición de bases de datos

Inteligencia Deep & Dark Web

Utilice la base integrada más grande de datos sin procesar de la Deep & Dark Web para monitorear la actividad delictiva, detectar menciones a su negocio e interrumpir ataques en el menor tiempo de reacción.

- ☑ Las menciones a su negocio, socios, industria o cualquier palabra clave que quiera monitorear, inclusive en imágenes (utilizando OCR) o audios, con transcripción
- ☑ Indicadores de compromiso (IoCs)
- ☑ Boletines de seguridad
- ☑ Búsquedas dirigidas y Threat Hunting con Explorar
- ☑ Alerta de anomalías
- ☑ Apoyo inmediato para investigación

Ejecutivos y VIPs

Monitoree la exposición de datos de las cuentas más sensibles de su empresa y reduzca el riesgo de spear phishing, ransomware y ataques utilizando Ingeniería Social.

- ☑ Perfil falso en red social
- ☑ Exposición de información personal, credenciales, teléfonos o tarjetas de crédito

Piratería de contenido

Rescate sus ingresos que están desapareciendo por la piratería y las ventas irregulares.

- ☑ Producto falso o venta irregular
- ☑ Piratería de contenido

Evaluación de seguridad

Evalúe y fortalezca su posición de seguridad eliminando riesgos externos y de terceros.

Sobre

///AXUR

Axur permite la escalabilidad y la automatización de la gestión de las ciberamenazas para apoyar a los equipos de seguridad de la información y ofrecer experiencias digitales más seguras. Nuestra plataforma de Cyber Threat Intelligence posee el tiempo de reacción más rápido del mercado, solicitando Takedowns automáticos 24×7.

Esto es posible porque la plataforma Axur trabaja en cuatro capas: además de la detección, las tecnologías de inspección, automatización y eliminación reducen en gran medida el tiempo medio de contención (MTTC) para los equipos de seguridad. Además, nuestros expertos en Ciber Inteligencia amplían la investigación tanto en la Surface como en la Deep & Dark Web, convirtiendo a Axur en la empresa líder en Cyber Threat Intelligence de Latinoamérica.

Comience gratuitamente

Agende una demostración


///AXUR
Digital
experiences
made safe
axur.com