Basque CyberSecurity Centre

Situación de la Ciberseguridad en Euskadi

4º trimestre 2022

www.ciberseguridad.eus

Basque CyberSecurity Centre

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Basque CyberSecurity Centre

Contenido

Basque CyberSecurity Centre

1. Resumen ejecutivo

Este informe, producto de la constante supervisión y evaluación llevada a cabo por el Centro Vasco de Ciberseguridad con el objetivo de identificar amenazas proactivamente con potencial impacto en Euskadi para implementar las medidas adecuadas, contiene un recopilatorio y análisis de los eventos y amenazas más significativos ocurridos durante el último trimestre de 2022. El resultado es una **información valiosa para mejorar las habilidades de prevención, detección y respuesta** ante las ciberamenazas de los organismos públicos, empresas y ciudadanía vasca.

Para comprender la situación actual de la ciberseguridad en Euskadi, es esencial adoptar una visión general de la realidad internacional en diferentes aspectos que afectan al ecosistema digital.

El conflicto entre Rusia y Ucrania sigue siendo un factor determinante en gran medida de la situación internacional, tal y como ha ocurrido durante todo el año 2022. Los ciberataques entre Rusia y Ucrania se han reducido en un 50%, reportándose 70 ciberataques contra Ucrania y 25 ciberataques contra la Federación Rusa. Sin embargo, fuera de las fronteras de los países en conflicto, estos ataques se han duplicado en relación al período anterior, reportándose un total de 239. **El ataque más frecuente continúa siendo la Denegación de Servicio Distribuido** (DDoS). También se han reportado fugas de información, malware y phishing. En este sentido, los actores maliciosos más relacionados con Rusia han sido Sandworm y Gamaredon, entre otros. Destacan nuevos aliados como el iraquí AlTahrea. Por parte de Ucrania, IT Army of Ukraine sigue siendo el más activo.

Por otro lado, desde un punto de vista normativo, **el Parlamento Europeo ha aprobado la aplicación de la directiva NIS2 y el reglamento DORA**, que formalizan el nuevo marco para la ciberseguridad y la resiliencia digital en los servicios financieros y a nivel general en la Unión Europea. Esta nueva regulación trata de armonizar las leyes anteriores, pero a la vez supone nuevas obligaciones para garantizar su cumplimiento por parte de diferentes tipos de industrias.

A nivel estatal, se han producido varias noticias relevantes, tales como un ciberataque que afectó a 3 hospitales de Barcelona, un ciberataque recibido por Telefónica o la desarticulación por parte de la Policía Nacional de una organización criminal dedicada al phishing.

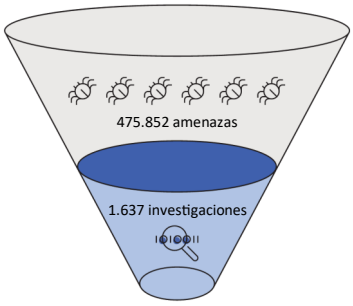
Durante el cuarto trimestre de 2022 **en Euskadi destaca el ciberataque recibido por el Grupo Noticias**, que afectó a sus ediciones impresas, así como la desarticulación de una banda en Álava que estafaba a clientes de entidades financieras mediante SMS falsos. Además, desde el Centro Vasco de Ciberseguridad se han gestionado 208 incidentes cuya tipología más habitual es el fraude.

En cuanto a las vulnerabilidades detectadas, durante este periodo se han publicado 6.751. Esto supone un decremento del 2,03% respecto al trimestre anterior, en el que se registraron 6.888. Igualmente, se percibe un decremento del 13,71% de las vulnerabilidades críticas, registrándose en este período 1.014, frente a las 1.153 clasificadas previamente. En cuanto al resto de vulnerabilidades, según la valoración CVSS v3, 2.435 tienen una valoración alta, 2.613 son medias, 123 son bajas y 566 están pendientes de asignar en el momento de obtención de la información. **La tipología más habitual de vulnerabilidad continúa siendo el cross-site-scripting** (XSS). Por otra parte, los productos más afectados por estas vulnerabilidades han sido los relativos a Google (relacionados con Android), Microsoft o Mozilla.

Así mismo, en este periodo se **han identificado 31 vulnerabilidades nuevas** que están siendo activamente explotadas por los atacantes.

Durante este periodo, se han identificado 4.129 infecciones de malware. Como tipología de malware, **el ransomware continúa siendo una amenaza muy relevante**. En este sentido, se han identificado 390 infecciones de ransomware. Los grupos criminales más activos han sido Lockbit, Bian Lian y BlackCat.

Durante el cuarto trimestre de 2022 se han identificado 475.852 indicios de amenazas que, tras un procesado y un filtrado iniciales, han generado 1.637 investigaciones con su correspondiente análisis. En este sentido, **la fuga de información continúa siendo una de las amenazas de mayor incidencia**, aunque al final del periodo analizado se ha apreciado un repunte relativo a las actividades de robo de credenciales.



FUENTE: MODELO DE INTELIGENCIA DEL BCSC

2. Hechos relevantes

Vivimos en un mundo hiperconectado, esta es una realidad que necesitan las empresas para el desarrollo de sus negocios y la sociedad en general tanto a nivel personal como profesional, en todos los ámbitos. Dentro de este contexto, **las capacidades de ciberdefensa de las organizaciones se deben construir no sólo mirando lo que sucede desde una perspectiva local, sino que teniendo en cuenta también la realidad internacional**. Para ello, es necesario analizar las tendencias que constantemente cambian la realidad de la sociedad en varios aspectos (social, económico, político, etc.), sus consecuencias en el mundo "ciber", para poder reaccionar de forma adecuada, para mitigar los riesgos existentes y adaptarse contribuyendo así a su resiliencia y sin lugar a duda a su competitividad.

Por este motivo, se resume en este informe los eventos más relevantes del cuarto trimestre del año, acontecidos a nivel internacional, estatal y local a Euskadi. De esta forma, proporcionando a las organizaciones este análisis detallado, ponemos a su disposición una información que consideramos crucial para poder prevenir riesgos futuros y mejorar, en general, sus capacidades de defensa.

2.1. Ámbito internacional

El cuarto trimestre del año 2022 ha seguido marcado por la actividad en el ciberespacio derivada del conflicto entre Rusia y Ucrania

Dentro del análisis de la situación a nivel internacional, el cuarto trimestre del año 2022 ha seguido marcado por la actividad en el ciberespacio derivada del conflicto entre Rusia y Ucrania.

Si se analiza la situación a nivel internacional, tal y como ha sucedido a lo largo de todo el año 2022, el cuarto trimestre ha seguido marcado por las consecuencias derivadas del conflicto entre Rusia y Ucrania. A pesar del aparente estancamiento del conflicto tras el repliegue ruso en las regiones de Járkov y Jerson, en el campo de batalla del ciberespacio el número de ciberataques reportados en la Federación Rusa ha sido prácticamente la mitad si se compara con el periodo anterior. Sin embargo, nuevamente el número de ciberataques reportados fuera de las fronteras de los países beligerantes se ha vuelto a duplicar, situándose la mayoría de ellos dentro de las fronteras de los países de la OTAN.

Los principales sectores que se han visto afectados han sido el sector público, financiero, energético, administrativo, así como el del transporte, seguido del sector TIC, fabricación y medios de comunicación. En lo que atañe a los ciberataques sufridos por Ucrania todo parece indicar que han ido destinados a inutilizar servicios financieros, sistemas de pago del sector energético, medios de comunicación y logísticos, así como a bloquear a las administraciones públicas. Estas acciones parecen coherentes con los ataques con misiles y drones suicidas que el ejército ruso ha realizado

en el campo de batalla físico contra la infraestructura crítica ucraniana en represalia por el devenir de los acontecimientos a medida que el conflicto ha ido evolucionando. Por su parte, los ciberataques contra objetivos rusos han sido de índole similar, pero menos intensos en volumen.

De hecho, durante el cuarto trimestre se reportaron 70 ciberataques que afectaron a Ucrania, 25 ciberataques que tuvieron como objetivo la Federación rusa y se registraron un total de 239 ciberataques que guardan relación con este conflicto en el resto del mundo.

De los 239 ataques registrados en el resto del mundo durante el último cuatrimestre de 2022, 213 han ido dirigidos a países pertenecientes a la OTAN, principalmente a países situados en el entorno del conflicto y que proveen de cobertura a Ucrania, como son Polonia con 70 ciberataques registrados, Letonia con 33, Lituania con 16 y Estonia con 11. Por otro lado, se han registrado 22 ciberataques dirigidos a los Estados Unidos y 12 a Reino Unido también vinculados al conflicto. Por último, destacan los 15 ciberataques registrados en la República Checa que afectaron a distintos sectores estratégicos del país y tuvieron lugar de manera simultánea los días 3 de octubre y 11 de noviembre.

Entre los países que no se encuentran en la OTAN y que más ciberataques han sufrido, destaca Moldavia con 11 ciberataques registrados coincidiendo con una situación interna tensionada por protestas masivas contra las políticas de su gobierno fruto de la crisis agravada sufrida por las consecuencias del conflicto armado en el país vecino.

Asimismo, en el cuarto trimestre ha continuado la tendencia detectada durante el tercer trimestre en cuanto a la tipología de ciberataques más reportados. De hecho, la casi totalidad de los ciberataques registrados son ataques por Denegación de Servicio Distribuidos (DDoS), superando en más de 100 nuevos ataques con respecto al periodo anterior. Por otro lado, se han vuelto a reportar en menor medida incidentes por Fuga de Información (Hack & Leak), Malware o Phishing. Esta consolidación de la tendencia registrada durante el cuarto cuatrimestre presupone una mejora de las capacidades defensivas de los actores implicados en la contienda en el ámbito del ciberespacio frente a amenazas como el Malware, los Wiper, el Ransomware o el principal vector de entrada, los ataques de Phishing, destinando casi la totalidad de sus capacidades ofensivas a los ataques DDoS.

Si se profundiza en los ataques DDoS, en total se han registrado 310 ciberataques, de los cuales 61 han tenido lugar contra objetivos ucranianos. Tan solo 13 han tenido como objetivo a la Federación Rusa y 236 han sido registrados en el resto del mundo, de los cuales la mayoría, como ya se ha señalado anteriormente, tuvieron lugar en países de la OTAN. Los sectores afectados han sido muy heterogéneos, pero principalmente, administraciones públicas, sector energético y financiero, así como el de transporte, TIC, medios de comunicación e industrial.

Finalmente, los actores maliciosos directamente vinculados a Rusia más activos han sido Sandworm y Gamaredon, junto con colectivos ya conocidos como People's Cyber Army, Phoenix, Anonymous Russia, XakNet, Killnet, Clowns, Russian Hackers Team, FRwL y NoName057(16). Los cuales han participado en ciberataques de manera activa a lo largo de todo el cuatrimestre. Entre los nuevos aliados de Rusia destaca el ataque del actor iraquí AlTahrea contra la infraestructura ferroviaria ucraniana el 8 de octubre. Por otro lado, el principal actor directamente vinculado a Ucrania, IT Army of Ukraine ha sido nuevamente el más activo durante el cuarto cuatrimestre de entre todos los actores que simpatizan con la causa ucraniana. No obstante, destacan diversos ataques perpetrados por colectivos contrarios al régimen de Moscú, por ejemplo, el colectivo National Republican Army, integrado por opositores a las políticas impulsadas por Putin dentro de Rusia, o Cyber Partisans, un colectivo bielorruso que también ha perpetrado ciberataques contra objetivos rusos. Además del conflicto entre Rusia y Ucrania, se han dado a conocer otros sucesos de interés en el ámbito internacional.

- El FBI, el CISA y la NSA revelan cómo los piratas informáticos atacaron una organización de la base industrial de defensa[I]. Las agencias de ciberseguridad e inteligencia de Estados Unidos revelaron el 4 de octubre que varios grupos de piratas informáticos nacionales podrían haber atacado la red empresarial de una organización del sector de la base industrial de defensa como parte de una campaña de ciberespionaje. Los hallazgos son el resultado de los esfuerzos de respuesta a incidentes de CISA en colaboración con la empresa de ciberseguridad Mandiant desde noviembre de 2021 hasta enero de 2022. No se ha atribuido la intrusión a un actor o grupo de amenaza conocido.
- Un ciberataque interrumpe los sitios web del Gobierno búlgaro por "traición a Rusia"[II]. Un ataque de denegación de servicio distribuido (DDoS) hizo caer brevemente los sitios web de la administración

presidencial, el Ministerio de Defensa, el Ministerio del Interior, el Ministerio de Justicia y el Tribunal Constitucional. Una vez restablecido el acceso, los sitios funcionaban con más lentitud de lo habitual, según la publicación búlgara en línea Dnevnik. El grupo de piratas informáticos prorruso Killnet reivindicó la autoría del ataque, afirmando que se trataba de un castigo "por la traición a Rusia y el suministro de armas a Ucrania".

- **Hackean la web del Parlamento Europeo tras aprobar una resolución crítica con Rusia**[III]. El sitio web del Parlamento Europeo sufrió un ataque cibernético de denegación de servicio distribuido (DDoS, lo que impidió el acceso a la página durante al menos una hora. Los equipos de la Eurocámara trabajan para resolver la situación. El grupo prorruso Killnet se ha atribuido la autoría del ataque en su canal de Telegram. Se sospecha que este mismo grupo está detrás de otros ataques recientes contra servicios informáticos de la Casa Blanca, la casa real británica y algunas administraciones francesas. Aunque las fuentes parlamentarias no han podido verificar la identidad de los atacantes.
- **Hackers atacan con ransomware una plataforma de comunicaciones de defensa australiana**[IV]. Agentes de amenazas han llevado a cabo un ataque de ransomware contra una plataforma de comunicaciones utilizada por el personal militar y de defensa australiano. La empresa, denominada ForceNet, es uno de los proveedores de servicios externos del Departamento de Defensa contratados para gestionar uno de sus sitios web.
- **Piratas informáticos indios atacan ordenadores de políticos y generales paquistaníes**[V]. Varios de los objetivos políticos parecen haber surgido de las continuas tensiones entre India y Pakistán. El 10 de enero, la banda recibió el encargo de entrar en la cuenta de correo electrónico de Fawad Chaudhry, entonces ministro de Información del gobierno del primer ministro Imran Khan. Hicieron una captura de pantalla de la bandeja de entrada de Fawad Chaudhry, que ha sido vista por el Sunday Times y el Bureau.
- **A finales de octubre, un ciberataque provocó la parada de los trenes en Dinamarca**[VI]. El ataque afectó a un proveedor de servicios informáticos externo. Un ciberataque provocó la parada de la formación de los trenes operados por DSB en Dinamarca el pasado fin de semana, los actores de la amenaza golpearon a un proveedor de servicios de TI de terceros. El ataque afectó a la empresa danesa Supeo, que proporciona soluciones de gestión de activos empresariales a compañías ferroviarias, operadores de infraestructuras de transporte y autoridades públicas de pasajeros. DSB es la mayor empresa ferroviaria de Dinamarca.

2.2. Ámbito estatal

Durante el cuarto trimestre han acontecido numerosas noticias a nivel estatal que se consideran relevantes desde un punto de vista de ciberseguridad y cómo actúan los actores actualmente. A continuación, se indica un resumen de estos hechos relevantes:

- **Un ciberataque afecta a tres hospitales de Barcelona**[VII]. Varios hospitales de Barcelona sufrieron un ciberataque que dejó inutilizados sus sistemas informáticos. Tres hospitales y diferentes ambulatorios sufrieron afectaciones y residencias, con incidencias en el uso de diversos de sus dispositivos necesarios para las visitas a los especialistas.
- **Telefónica sufrió un ciberataque en octubre**[VIII]. Telefónica comunicó a sus clientes que, a causa de un ciberataque, debían modificar las contraseñas de sus routers WiFi, tanto si son de uso doméstico como empresarial. Se vieron comprometidas las claves de acceso de los routers residenciales y empresariales. Aunque el ciberataque no ha comportado la revelación de datos personales como el nombre, dirección, DNI, historial de llamadas o los datos bancarios.
- **La Policía Nacional desmantela organización criminal dedicada al phishing**[IX]. La Policía Nacional ha desarticulado una organización criminal especializada en cometer estafas utilizando el engaño del "fraude del CEO" y ha detenido a 15 de sus integrantes: nueve de ellos en Madrid, cinco en Albacete y uno más en Valencia. La investigación policial ha logrado relacionar a esta red con numerosas transferencias de origen fraudulento, con un valor aproximado de 850.000 euros, así como un entramado empresarial dedicado a la recepción y posterior blanqueo del dinero que recibían.

2.3. Ámbito Euskadi

Durante el cuarto trimestre de 2022 han sido relevantes los siguientes incidentes de ciberseguridad en el entorno geográfico de Euskadi:

- **Ciberataque contra el Grupo Noticias**[X]. Un ataque cibernético realizado causó problemas en la generación de las páginas impresas del periódico Grupo Noticias. Como resultado, los servidores del periódico se bloquearon y afectaron a las cuatro ediciones impresas que componen el Grupo Noticias, incluyendo Diario de Noticias de Álava, Nafarroa (Diario de Noticias), Gipuzkoa (Noticias de Gipuzkoa) y Bizkaia (DEIA). Esto generó incertidumbre sobre la disponibilidad puntual de las ediciones impresas del periódico en los kioscos, aunque Diario de Noticias de Álava logró estar presente y ofrecer información puntualmente.
- **Desarticulan una banda en Álava que estafaba a clientes de entidades financieras con SMS falsos**[XI]. La Policía Nacional ha desarticulado una banda en Álava que estafaba a clientes de entidades financieras mediante SMS falsos. Según las investigaciones, el grupo criminal estaba dirigido por dos individuos que se encontraban encarcelados en el centro penitenciario de Basauri, desde donde supuestamente daban instrucciones al resto de los miembros del grupo. La operación fue liderada por la Brigada Provincial de Policía Judicial de la Policía Nacional en Vitoria y permitió poner fin a las actividades de este grupo, que cometía estafas en todo el país.

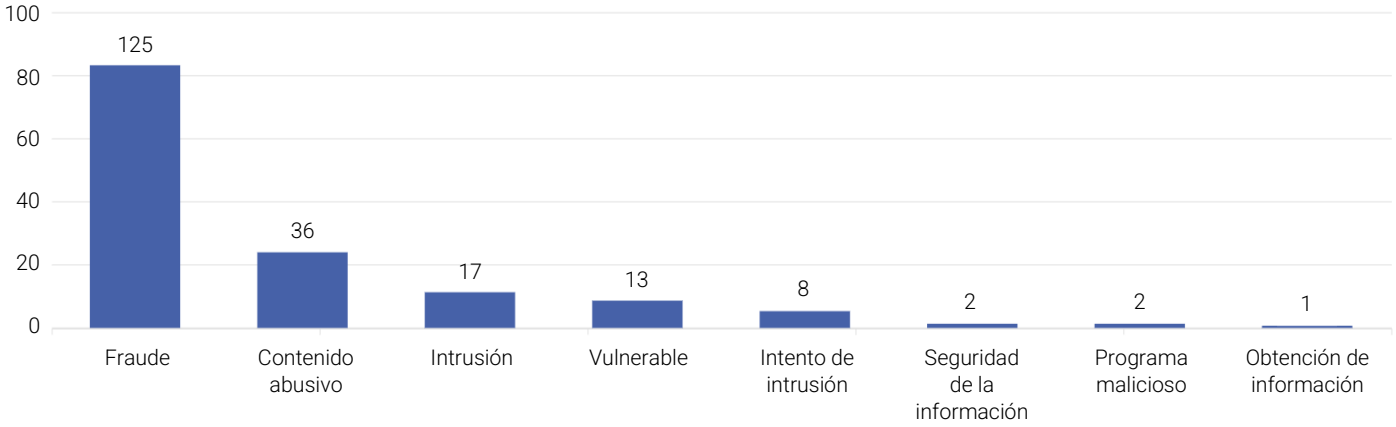
3. Incidentes gestionados por el BCSC

Durante el cuarto trimestre de 2022, se han gestionado 204 incidentes, siendo la tipología más habitual la de fraude.

Durante el cuarto trimestre de 2022, se han gestionado 204 incidentes, cuya tipología es la siguiente:

Estos incidentes provienen de ciudadanía, empresas y organismos públicos que reportan al servicio de asesoramiento del Centro. En el caso de identificar cualquier actividad sospechosa agradecemos que se nos reporte a través del email incidencias@bcsc.eus o llamando al **900 104 891** y así poder tomar las medidas técnicas oportunas para mitigar la amenaza.

Tipologías de incidentes gestionados por el BCSC



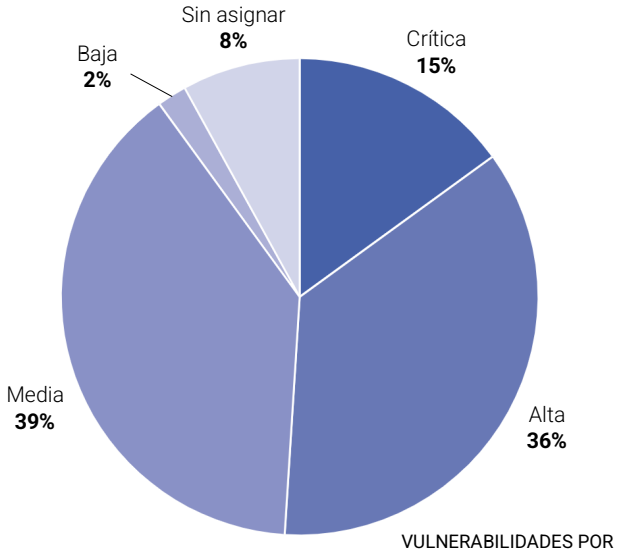
TIPOLOGÍA DE INCIDENTES GESTIONADOS POR EL BCSC. FUENTE: BCSC

4. Vulnerabilidades

Durante este periodo se han publicado 6.751 nuevas vulnerabilidades, lo cual supone un decremento del 2,03% respecto al trimestre anterior.

Durante este periodo se han publicado 6.751 nuevas vulnerabilidades, lo cual supone un decremento del 2,03% respecto al trimestre anterior, en el que se registraron 6.888. Igualmente, se percibe un decremento del 13,71% de las vulnerabilidades críticas, registrándose en este período 1.014, frente a las 1.153 registradas en el trimestre anterior. En cuanto al resto de vulnerabilidades, 2.435 tienen una valoración alta, 2.613 son medias, 123 son bajas según la valoración CVSS v3, mientras 566 están pendientes de asignar en el momento de obtención de la información.

Vulnerabilidades por severidad

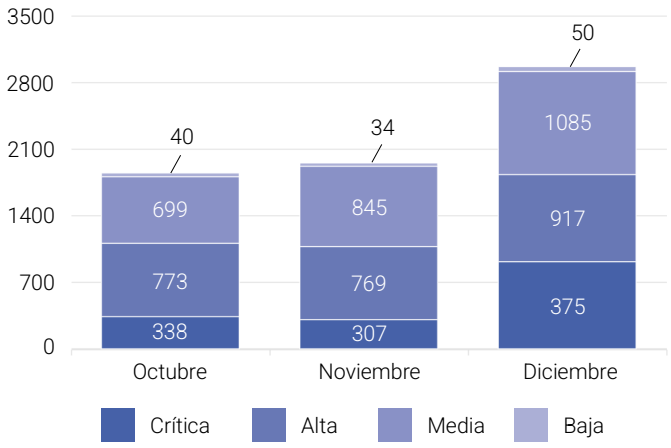


VULNERABILIDADES POR SEVERIDAD. FUENTE: MITRE

Cada vulnerabilidad es diferente y afecta a los activos de distinta forma. Algunas permiten ejecutar código remoto, otras inyectar código o instrucciones y afectar al comportamiento de un programa, otras permiten escalar privilegios, etc.

Esta criticidad y el número total de vulnerabilidades, ha evolucionado a lo largo de este trimestre según se indica a continuación:

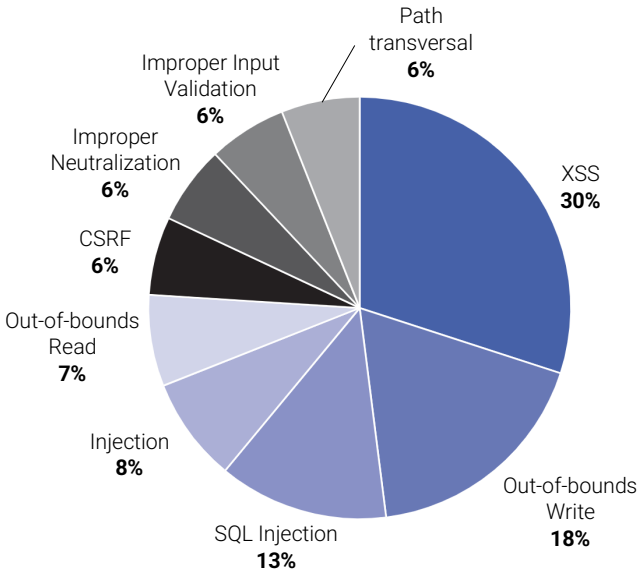
Evolución de criticidad por mes



EVOLUCIÓN DE VULNERABILIDADES POR MES. FUENTE: MITRE

Tomando como base el estándar CWE (Common Weakness Enumeration), analizando el tipo de vulnerabilidades, estas se distribuyen de la siguiente forma:

TOP 10 tipos de vulnerabilidades

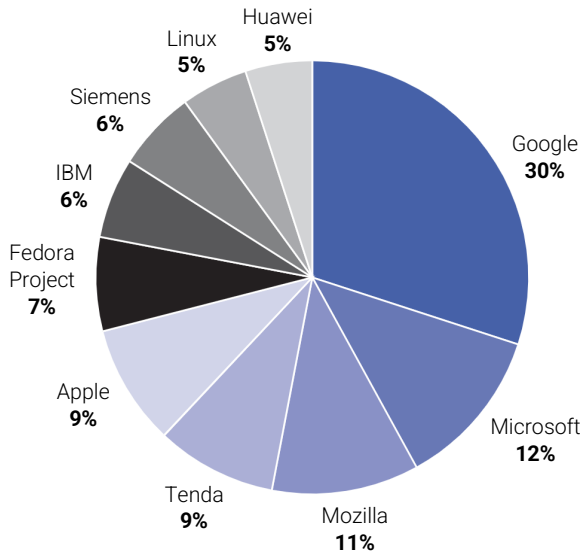


TOP 10 DE TIPOLOGÍA DE VULNERABILIDADES. FUENTE: MITRE

Como se puede ver, en el trimestre en análisis, el tipo de vulnerabilidad más común continúa siendo el cross-site-scripting (XSS).

Respecto a los fabricantes afectados, en el siguiente gráfico se muestra el TOP 10 de afectados por las vulnerabilidades publicadas en este trimestre:

Vulnerabilidades por fabricante

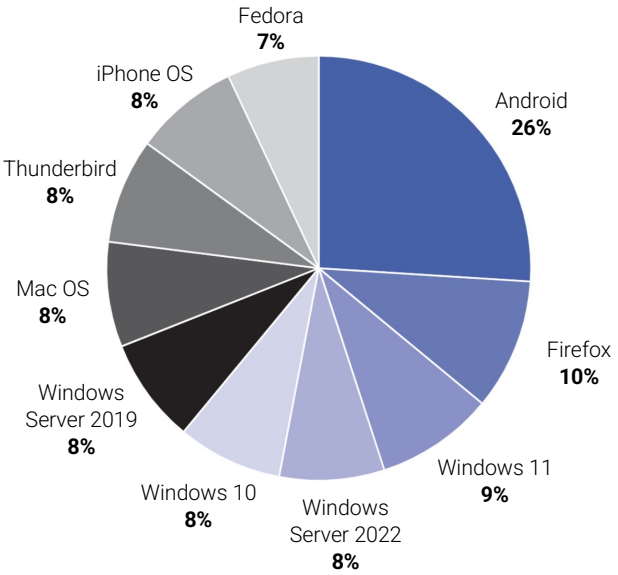


TOP 10 FABRICANTES AFECTADOS POR VULNERABILIDADES. FUENTE: MITRE

Como se puede ver, los fabricantes de algunos de los productos más usados están en este top, como son Google (por productos como Android), Microsoft o Mozilla.

La relación de vulnerabilidades por producto afectado se refleja en el siguiente gráfico:

Vulnerabilidades por producto



TOP 10 PRODUCTOS AFECTADOS POR VULNERABILIDADES. FUENTE: MITRE

Como se puede ver, se mantiene correlación con el gráfico anterior de fabricantes.

Así mismo, en este periodo se han identificado **31 vulnerabilidades nuevas** que están siendo activamente explotadas por los atacantes.

De todas las vulnerabilidades identificadas en este trimestre, y atendiendo a distintos criterios como la propia severidad, su explotación activa y potencial impacto, se destacan las siguientes:

CVE-2022-4116

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-4116
- CWE: 94
- Productos afectados: Quarkus
- Valoración CVSS: 9.8 CRITICAL CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Vector ataque: Red
- Complejidad: Bajo
- Privilegios requeridos: Ninguno
- Interacción de usuario: Ninguna
- Alcance: Sin cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

Se ha encontrado una vulnerabilidad en Quarkus. Este fallo de seguridad se produce en Dev UI Config Editor, que es vulnerable a ataques drive-by localhost que conducen a la ejecución remota de código.

CVE-2022-42856

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-42856
- CWE: 843
- Productos afectados: Safari, tvOS, macOS Ventura, iOS, iPadOS
- Valoración CVSS: 8.8 ALTA CVSS: 3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
- Vector ataque: Red
- Complejidad: Bajo
- Privilegios requeridos: Ningunos
- Interacción de usuario: Requerida
- Alcance: Sin cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

Se ha solucionado un problema de confusión de tipos con una gestión de estados mejorada. Este problema se ha corregido en Safari 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 15.7.2 y iPadOS 15.7.2, iOS 16.1.2. El procesamiento de contenido web maliciosamente diseñado puede conducir a la ejecución de código arbitrario. Apple es consciente de un informe de que este problema puede haber sido explotado activamente contra versiones de iOS lanzadas antes de iOS 15.1.

CVE-2022-31705

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-31705, https://www.ciberseguridad.eus/ultima-hora/vulnerabilidades-en-productos-vmware
- CWE: 787
- Productos afectados: VMware vRealize Network Insight (vRNI), VMware ESXi, VMware Workstation y VMware Fusion.
- Valoración CVSS: 8.2 HIGH CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
- Vector ataque: Local
- Complejidad: Bajo
- Privilegios requeridos: Altos
- Interacción de usuario: Ninguna
- Alcance: Con cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

VMware ESXi, Workstation y Fusion contienen una vulnerabilidad de escritura fuera de límites en el controlador USB 2.0 (EHCI). Un actor malicioso con privilegios administrativos locales en una máquina virtual puede explotar este problema para ejecutar código como el proceso VMX de la máquina virtual que se ejecuta en el host. En ESXi, la explotación está contenida dentro del sandbox de VMX mientras que, en Workstation y Fusion, esto puede llevar a la ejecución de código en la máquina donde está instalado Workstation o Fusion.

CVE-2022-44710

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-44710, https://www.ciberseguridad.eus/ultima-hora/actualizaciones-de-seguridad-de-microsoft-de-diciembre-de-2022
- CWE: 269
- Productos afectados: DirectX Graphics Kernel
- Valoración CVSS: 7.8 HIGH
- CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
- Vector ataque: Local
- Complejidad: Alta
- Privilegios requeridos: Bajo
- Interacción de usuario: Ninguna
- Alcance: Con cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

Vulnerabilidad de elevación de privilegios en el núcleo de gráficos DirectX.

CVE-2022-20419

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-20419, https://www.ciberseguridad.eus/ultima-hora/boletin-de-seguridad-de-android-de-octubre-de-2022
- CWE: Información insuficiente
- Productos afectados: Android
- Valoración CVSS: 7.8 HIGH
- CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- Vector ataque: Local
- Complejidad: Bajo
- Privilegios requeridos: Bajo
- Interacción de usuario: Ninguna
- Alcance: Sin cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

En setOptions de ActivityRecord.java, existe la posibilidad de cargar cualquier código Java arbitrario en el proceso de lanzamiento debido a un error lógico en el código. Esto podría conducir a una escalada local de privilegios sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.

A continuación, se indican las **vulnerabilidades más relevantes en relación a entornos y productos industriales.**

CVE-2022-3156

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-3156, https://www.ciberseguridad.eus/ultima-hora/control-de-acceso-inadecuado-en-rockwell-automation-studio-5000-logix-emulate
- CWE: 287
- Productos afectados: Rockwell Automation Studio 5000 Logix Emulate software
- Valoración CVSS: 7.8 HIGH CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- Vector ataque: Local
- Complejidad: Bajos
- Privilegios requeridos: Bajos
- Interacción de usuario: Ninguna
- Alcance: Sin cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

Existe una vulnerabilidad de ejecución remota de código en el software Rockwell Automation Studio 5000 Logix Emulate. A los usuarios se les conceden permisos elevados en ciertos servicios del producto cuando se instala el software. Debido a esta configuración incorrecta, un usuario malintencionado podría potencialmente lograr la ejecución remota de código en el software objetivo.

CVE-2022-43509

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-43509, https://www.ciberseguridad.eus/ultima-hora/escritura-fuera-de-limites-en-omron-cx-programmer
- CWE: 787
- Productos afectados: CX-Programmer v.9.77 y anterior
- Valoración CVSS: 7.8 HIGH CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
- Vector ataque: Local
- Complejidad: Baja
- Privilegios requeridos: Ninguna
- Interacción de usuario: Requerida
- Alcance: Sin cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

Existe una vulnerabilidad de escritura fuera de los límites en CX-Programmer v.9.77 y anteriores, que puede conducir a la divulgación de información y/o a la ejecución de código arbitrario haciendo que un usuario abra un archivo CXP especialmente diseñado.

CVE-2022-3087

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-3087, https://www.ciberseguridad.eus/ultima-hora/ejecucion-de-codigo-arbitrario-en-productos-de-fuji-electric
- CWE: 787
- Productos afectados: Fuji Electric Tellus Lite V-Simulator versiones 4.0.12.0 y anteriores
- Valoración CVSS: 7.8 HIGH CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
- Vector ataque: Local
- Complejidad: Baja
- Privilegios requeridos: Ninguno
- Interacción de usuario: Requerida
- Alcance: Sin cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

Fuji Electric Tellus Lite V-Simulator versiones 4.0.12.0 y anteriores son vulnerables a una escritura fuera de límites que puede permitir a un atacante ejecutar código arbitrario.

CVE-2022-40263

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-40263, https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-de-credenciales-sin-cifrar-en-bd-totalys-multiprocessor
- CWE: 798
- Productos afectados: BD Totalys MultiProcessor, versión 1.70 y anteriores.
- Valoración CVSS: 7.8 HIGH CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- Vector ataque: Local
- Complejidad: Baja
- Privilegios requeridos: Baja
- Interacción de usuario: Ninguno
- Alcance: Sin cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

BD Totalys MultiProcessor, versiones 1.70 y anteriores, contienen credenciales codificadas. Si se aprovechan, las amenazas pueden acceder a información confidencial, modificarla o eliminarla, incluida la información sanitaria electrónica protegida (ePHI), la información sanitaria protegida (PHI) y la información de identificación personal (PII). Los clientes que utilizan BD Totalys MultiProcessor versión 1.70 con Microsoft Windows 10 tienen configuraciones adicionales de endurecimiento del sistema operativo que aumentan la complejidad del ataque requerido para explotar esta vulnerabilidad.

CVE-2022-33324

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-33324, https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-dos-en-productos-mitsubishi-electric
- CWE: 404
- Productos afectados: Mitsubishi Electric Corporation MELSEC iQ-R Series R00/01/02CPU
- Valoración CVSS: 7.5 HIGH CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- Vector ataque: Red
- Complejidad: Baja
- Privilegios requeridos: Ninguno
- Interacción de usuario: Ninguno
- Alcance: Sin cambios
- Confidencialidad: Ninguna
- Integridad: Ninguna
- Disponibilidad: **Alta**

Permite a un atacante remoto no autenticado provocar una denegación de servicio en la comunicación Ethernet del módulo mediante el envío de paquetes especialmente diseñados. Se requiere un reinicio del sistema del módulo para la recuperación.

Del mismo modo, también existen productos del ámbito de ciberseguridad que son afectados por vulnerabilidades. Es importante estar al corriente de estas ya que, si son los productos en los que delegamos la seguridad de nuestros sistemas, una vulnerabilidad en ellos podría exponerlos a un atacante. A continuación, se muestran las **vulnerabilidades de productos y tecnologías de seguridad** más relevantes publicadas en este trimestre:

CVE-2022-27518

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-27518, https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-critica-en-citrix-adc-y-citrix-gateway
- CWE: 664
- Productos afectados: Citrix ADC, Citrix Gateway
- Valoración CVSS: 9.8 CRITICAL
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Vector ataque: Red
- Complejidad: Bajo
- Privilegios requeridos: Ninguno
- Interacción de usuario: Ninguno
- Alcance: Sin cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

Ejecución remota no autenticada de código arbitrario.

CVE-2022-42475

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-42475, https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-critica-en-fortios
- CWE: 787
- Productos afectados: FortiOS SSL-VPN, FortiProxy SSL-VPN
- Valoración CVSS: 9.8 CRITICAL CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Vector ataque: Red
- Complejidad: Baja
- Privilegios requeridos: Ninguno
- Interacción de usuario: Ninguno
- Alcance: Sin cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

Una vulnerabilidad de desbordamiento de búfer basada en heap [CWE-122] en FortiOS SSL-VPN 7.2.0 a 7.2.2, 7.0.0 a 7.0.8, 6.4.0 a 6.4.10, 6.2.0 a 6.2.11, 6.0.15 y anteriores y FortiProxy SSL-VPN 7.2.0 a 7.2.1, 7.0.7 y anteriores puede permitir a un atacante remoto no autenticado ejecutar código o comandos arbitrarios a través de solicitudes específicamente diseñadas.

CVE-2022-33873

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-33873, https://www.ciberseguridad.eus/ultima-hora/inyeccion-de-comando-no-autenticado-en-fortitester
- CWE: 78
- Productos afectados: FortiTester, versiones: 7.1.0 y 7.0.0; 4.2.0, 4.1.0 hasta 4.1.1 y 4.0.0; 3.9.0 hasta 3.9.1, 3.8.0, 3.7.0 hasta 3.7.1, 3.6.0, 3.5.0 hasta 3.5.1, 3.4.0, 3.3.0 hasta 3.3.1, 3.2.0, 3.1.0 y 3.0.0; 2.9.0, 2.8.0, 2.7.0, 2.6.0, 2.5.0, 2.4.0 hasta 2.4.1 y 2.3.0.
- Valoración CVSS: 9.8 CRITICAL CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Vector ataque: Red
- Complejidad: Bajo
- Privilegios requeridos: Ninguno
- Interacción de usuario: Ninguno
- Alcance: Sin cambios
- Confidencialidad: **Alta**
- Integridad: **Alta**
- Disponibilidad: **Alta**

Una neutralización incorrecta de elementos especiales utilizados en un comando OS ('OS Command Injection') vulnerabilidades [CWE-78] en los componentes de inicio de sesión de consola de FortiTester 2.3.0 a 3.9.1, 4.0.0 a 4.2.0, 7.0.0 a 7.1.0 puede permitir a un atacante no autenticado ejecutar un comando arbitrario en el shell subyacente.

CVE-2022-40684

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-40684, https://www.ciberseguridad.eus/ultima-hora/aviso-de-seguridad-fortios-y-fortiproxy
- CWE: 306
- Productos afectados: FortiOS: versiones 7.0.0 a 7.0.6 y desde la 7.2.0 a la 7.2.1. FortiProxy: versiones 7.0.0 a 7.0.6 y 7.2.0
- Valoración CVSS: 9.8 CRITICAL CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Vector ataque: Red
- Complejidad: Baja
- Privilegios requeridos: Ninguno
- Interacción de usuario: Ninguno
- Alcance: Sin cambios
- Confidencialidad: Alta
- Integridad: Alta
- Disponibilidad: Alta

CVE-2022-0030

- Referencia: https://nvd.nist.gov/vuln/detail/CVE-2022-0030, https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-en-pan-os-de-palo-alto-cve-2022-0030
- CWE: 290
- Productos afectados: Palo Alto Networks PAN-OS 8.1
- Valoración CVSS: 8.1 HIGH
- CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
- Vector ataque: Red
- Complejidad: Alta
- Privilegios requeridos: Ninguno
- Interacción de usuario: Ninguno
- Alcance: Sin cambios
- Confidencialidad: Alta
- Integridad: Alta
- Disponibilidad: Alta

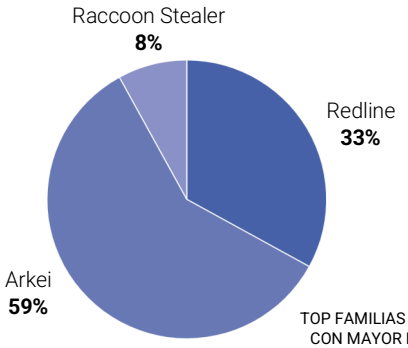
Una vulnerabilidad de omisión de autenticación en la interfaz web de PAN-OS 8.1 de Palo Alto Networks permite a un atacante basado en red con conocimientos específicos del cortafuegos o dispositivo Panorama de destino hacerse pasar por un administrador de PAN-OS existente y realizar acciones privilegiadas.

5. Malware

Durante el cuarto trimestre de 2022 se han identificado 356 infecciones de familias de malware diferentes.

El BCSC monitoriza las familias de malware con más tasa de afectación en Euskadi. Durante el cuarto trimestre de 2022 se han identificado 356 infecciones de familias de malware diferentes, con la siguiente distribución:

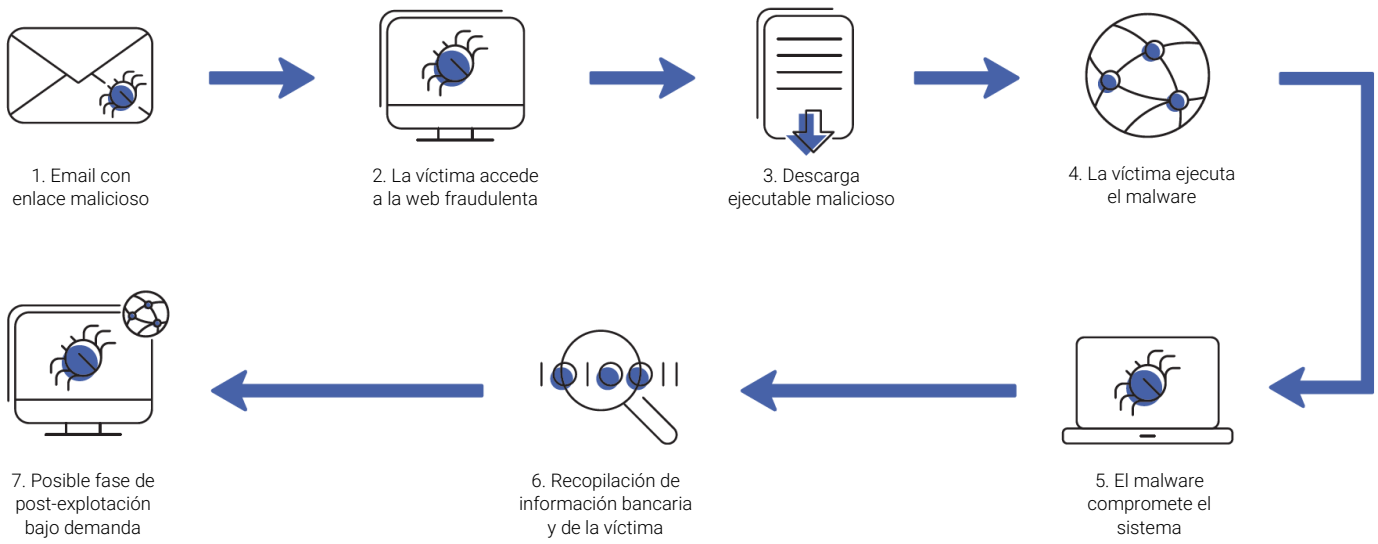
Familias de malware con mayor impacto en Euskadi



TOP FAMILIAS DE MALWARE CON MAYOR IMPACTO EN EUSKADI. FUENTE: BCSC

REDLINE

RedLine Stealer (también conocido como RedLine) es un software malicioso que puede comprarse entre 150 y 200 dólares, dependiendo de la versión, en foros de hackers. RedLine puede robar datos e infectar sistemas operativos con malware. En general, los ciberdelincuentes intentan infectar los ordenadores con software malicioso como RedLine Stealer para crear dinero mediante el uso indebido de la información robada a la que se ha accedido e infectar los sistemas con software adicional de este tipo con el mismo objetivo. es capaz de recolectar datos sobre los siguientes elementos: equipo y sistema operativo, ficheros, navegadores, clientes VPN, clientes FTP, clientes de mensajería, clientes de juegos y carteras de criptomonedas.



CADENA DE ATAQUE DE REDLINE. FUENTE: BCSC

De acuerdo a las muestras analizadas, y los ataques típicos vistos, las técnicas usadas durante la infección de este malware se muestran a continuación:

Initial Access	Execution	Credential Access	Discovery	Collection	Command and Control	Exfiltration
Phishing	User Execution	Credentials from Password Stores	Account Discovery	Data from local system	Non-Standard Port	Exfiltration Over C2 Channel
Spearphishing Attachment		Credentials from Web Browsers	Process Discovery	Screen Capture		
Spearphishing Link		Password Managers	Software Discovery			
Spearphishing via Service		Window Credential Manager	Security Software Discovery			
		OS Credential Dumping	System Time Discovery			
		Steal Web Session Cookie				
		Unsecured Credentials				
		Credentials In Files				
		Credentials In Registry				
		Group Policy Preferences				
		Private Keys				

TTPS DEL MALWARE REDLINE. FUENTE: BCSC

ARKEI

Arkei es un malware, conocido desde mayo del año 2018, especializado en el robo de información. Recoge datos de los navegadores, monederos de criptomonedas y ficheros que coincidan con un patrón definido por el atacante (cada atacante puede definir sus propios patrones).

Debido a su capacidad de personalización, salen nuevas variantes continuamente y es complicado identificar un mecanismo de ataque definido.

Los TTP del malware que son comunes en sus diferentes se indican a continuación:

Execution	Credential Access	Discovery
Command and Scripting Interpreter	OS Credential Dumping	Query Registry

TTPS DEL MALWARE ARKEI. FUENTE: BCSC

RACCOON STEALER:

Raccoon Stealer fue uno de los ladrones de información más prolíficos en 2021, siendo utilizado por múltiples actores cibercriminales. Anteriormente se vendía como un malware como servicio en foros clandestinos desde principios de 2019, pero su funcionamiento se detuvo repentinamente el 25 de marzo de 2022. El 10 de junio de 2022, mientras buscaban paneles de administración de ladrones en el motor de búsqueda Shodan, los analistas de SEKOIA.IO se toparon con servidores activos que alojaban una página web llamada "Raccoon Stealer 2.0".

Las capacidades de este software se basan en adquirir información de sus víctimas, siendo capaz de conseguir: el historial del navegador, carteras de criptomonedas, direcciones de correo electrónico, contraseñas, cookies, capturas de pantalla, información del sistema. Este este su flujo de infección:

CADENA DE ATAQUE DE RACCOON STEALER. FUENTE: BCSC

Las TTPs usadas por este malware se muestran en la siguiente imagen:

Initial Access	Execution	Defense Evation	Credential Access	Discovery	Collection	Command and Control	Exfiltration
Drive-by Compromise	Command and Scripting Interpreter	Deobfuscate/ Decode Files or Information	Credentials from Password Stores	Account Discovery	Archive Collected Data	Application Layer Protocol	Exfiltration Over C2 Channel
Phishing	Exploitation for Client Execution	Obfuscated Files or Information	Credentials from Web Browsers	File and Directory Discovery	Automated Collection	Data Encoding	
	Native API		Input Capture	Process Discovery	Data from Local System	Non-Application Layer Protocol	
			OS Credential Dumping	Query Registry	Email Collection		
			Unsecured Credentials	Remote System Discovery	Input Capture		
			Credentials in Files	System Information Discovery	Screen Capture		
				System Network Configuration Discovery			
				System Owner/ User Discovery			
				System Time Discovery			

TTPS DE RACCOON STEALER. FUENTE: BCSC

5.1. Técnicas usadas

Tomando como base las técnicas utilizadas por el TOP de familias de malware, se ha procedido a comparar todas ellas identificando aquellas que más se repiten.

En el siguiente gráfico se especifican, con arreglo a la matriz de Mitre Att&ck, los TTPs comunes localizados en los malware con mayor impacto en Euskadi durante el último trimestre. Cada técnica se puntúa con un valor entre 1 (verde) y 4 (rojo). Una mayor puntuación significa que la técnica es utilizada por un mayor número de familias de malware.

TTPS COMUNES EN LOS MALWARE DE MAYOR IMPACTO EN EUSKADI. FUENTE: BCSC

A continuación, se indica una descripción detallada de cada una de las técnicas más utilizadas; esta descripción se realizará para aquellas técnicas vistas en, por lo menos, la mitad de las familias de malware analizadas:

Execution

- T1059 - Command and Scripting Interpreter: Los adversarios pueden abusar de los intérpretes de comandos y de scripts para ejecutar comandos, scripts o archivos binarios. Estas interfaces y lenguajes brindan formas de interactuar con los sistemas y son una característica común en muchas plataformas diferentes. La mayoría de los sistemas vienen con una interfaz de línea de comandos integrada y capacidades de secuencias de comandos, por ejemplo, las distribuciones de macOS y Linux incluyen algún tipo de Unix Shell, mientras que las instalaciones de Windows incluyen Windows Command Shell y PowerShell. Los atacantes pueden abusar de estas tecnologías de varias maneras como un medio para ejecutar comandos arbitrarios. Los comandos y scripts se pueden usar como un acceso inicial a las víctimas mediante el envío de documentos atractivos o como llamadas secundarias a un C2 existente. Los adversarios también pueden ejecutar comandos a través de terminales/shells interactivos, así como utilizar varios servicios remotos para lograr la ejecución remota.

Credential access

- T1555.003 – Credentials from Web Browsers: Los atacantes pueden adquirir credenciales de los navegadores web leyendo archivos específicos del navegador objetivo. Los navegadores web suelen guardar las credenciales, como los nombres de usuario y las contraseñas de los sitios web, para no tener que introducirlas manualmente en el futuro. Los navegadores web suelen almacenar las credenciales en un formato cifrado dentro de un almacén de credenciales; sin embargo, existen métodos para extraer credenciales en texto plano de los navegadores web.
- T1003 – OS Credential Dumping: Los adversarios pueden intentar volcar las credenciales del Sistema Operativo para obtener el inicio de sesión de la cuenta y el contenido de la credencial, normalmente en forma de hash o contraseña de texto claro, del sistema operativo y el software. Luego, las credenciales se pueden usar para realizar movimientos laterales y acceder a información restringida.
- T1552-001 – Unsecured Credentials: Credentials In Files: Los adversarios pueden buscar sistemas de archivos locales y recursos compartidos de archivos remotos en busca de ficheros que contengan credenciales almacenadas de forma insegura. Estos pueden ser archivos creados por los usuarios para almacenar sus propias credenciales, almacenes de credenciales compartidas para un grupo de personas, archivos de configuración que contienen contraseñas para un sistema o servicio, o archivos binarios/de código fuente que contienen contraseñas incrustadas.

Discovery

- T1087 – Account Discovery: Los atcantes pueden intentar obtener una lista de cuentas en un sistema o dentro de un entorno. Esta información puede ayudar a los adversarios a determinar qué cuentas existen para ayudar en el comportamiento de seguimiento.
- T1012 – Query Registry: Los atacantes pueden interactuar con el Registro de Windows para recopilar información sobre el sistema, la configuración y el software instalado. El Registro contiene una cantidad importante de información sobre el sistema operativo, la configuración, el software y la seguridad.
- T1057 – Process Discovery: Los atacantes pueden intentar obtener información sobre los procesos en ejecución en un sistema. La información obtenida podría utilizarse para conocer el software y las aplicaciones comunes que se ejecutan en los sistemas de la red. Los atacantes pueden utilizar la información del descubrimiento de procesos durante el descubrimiento automatizado para dar forma a los comportamientos posteriores, incluyendo si el adversario infecta completamente el objetivo y/o intenta acciones específicas.
- T1124 – System Time Discovery: Los atacantes pueden obtener la hora del sistema y/o la zona horaria de un sistema local o remoto. La hora del sistema es establecida y almacenada por el Servicio de Hora de Windows dentro de un dominio para mantener la sincronización de la hora entre los sistemas y servicios en una red empresarial.

Collection

- T1005 – Data from Local System: Los adversarios pueden buscar fuentes del sistema local, como sistemas de archivos y archivos de configuración o bases de datos locales, para encontrar archivos de

interés y datos confidenciales antes de la exfiltración. Los atacantes pueden hacer esto utilizando un intérprete de comandos y secuencias de comandos, como cmd, así como una CLI de dispositivo de red, que tienen la funcionalidad de interactuar con el sistema de archivos para recopilar información. Los adversarios también pueden usar la recopilación automatizada en el sistema local.

- T1113 – Screen Capture: Los atacantes pueden intentar realizar capturas de pantalla del escritorio para recopilar información en el transcurso de la operación. La funcionalidad de captura de pantalla puede incluirse como una característica de una herramienta de acceso remoto utilizada en las operaciones posteriores al compromiso.

Exfiltration

- T1041 - Exfiltration Over C2 Channel: Los atacantes pueden robar datos exfiltrándolos a través de un canal de mando y control existente. Los datos robados se codifican en el canal de comunicaciones normal utilizando el mismo protocolo que las comunicaciones de mando y control.

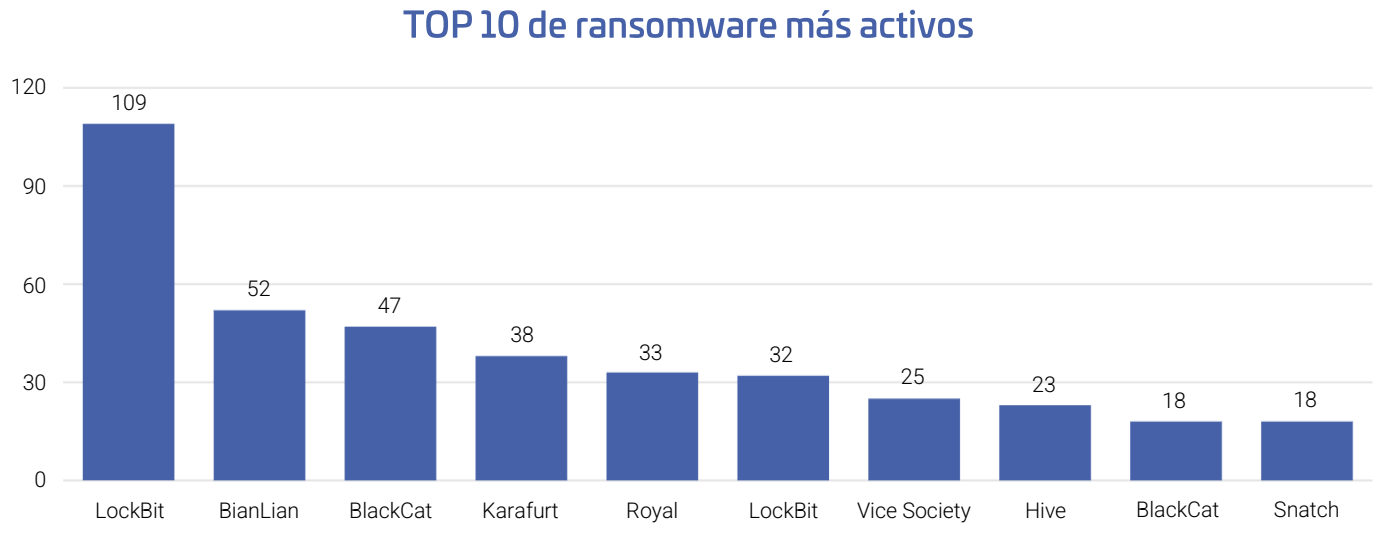
5.2. Ransomware

Durante este trimestre se han contabilizado un total de 390 víctimas de los diferentes grupos de ransomware conocidos.

Como resumen de la actividad de los diferentes actores de Ransomware, durante este trimestre se han contabilizado un total de 390 víctimas de los diferentes grupos de ransomware conocidos. En el siguiente gráfico se puede ver que Lockbit ha sido el grupo más activo con 109 víctimas, lo que implica un decremento del 53% en su actividad respecto al trimestre pasado. Bian Lian y el grupo BlackCat tienen 52 y 47 víctimas respectivamente, siendo el segundo y tercer grupo más activo.

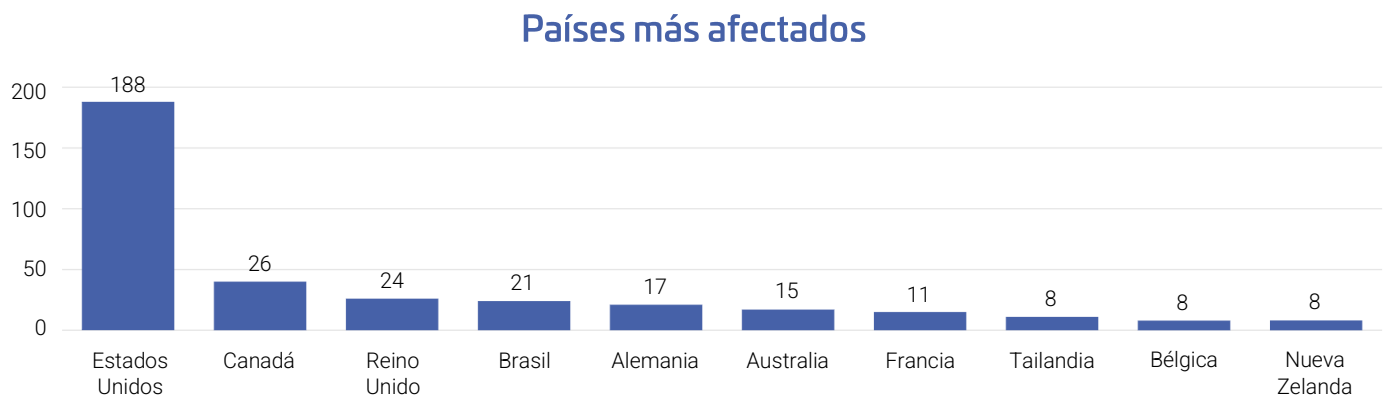
Lockbit ha sido el grupo de ransomware con mayor número de víctimas reconocidas, con un total de 109.

El TOP 10 de grupos de ransomware más activos se muestran en el siguiente gráfico:



TOP 10 DE GRUPOS DE RANSOMWARE MÁS ACTIVOS. FUENTE: BCSC

En la distribución de países más afectados por cada tipo de ransomware, Estados Unidos es el más atacado de todos, para todos los tipos de ransomware diferentes. Se puede apreciar en el siguiente gráfico el TOP 10 de países más afectados por estos actores de ransomware:



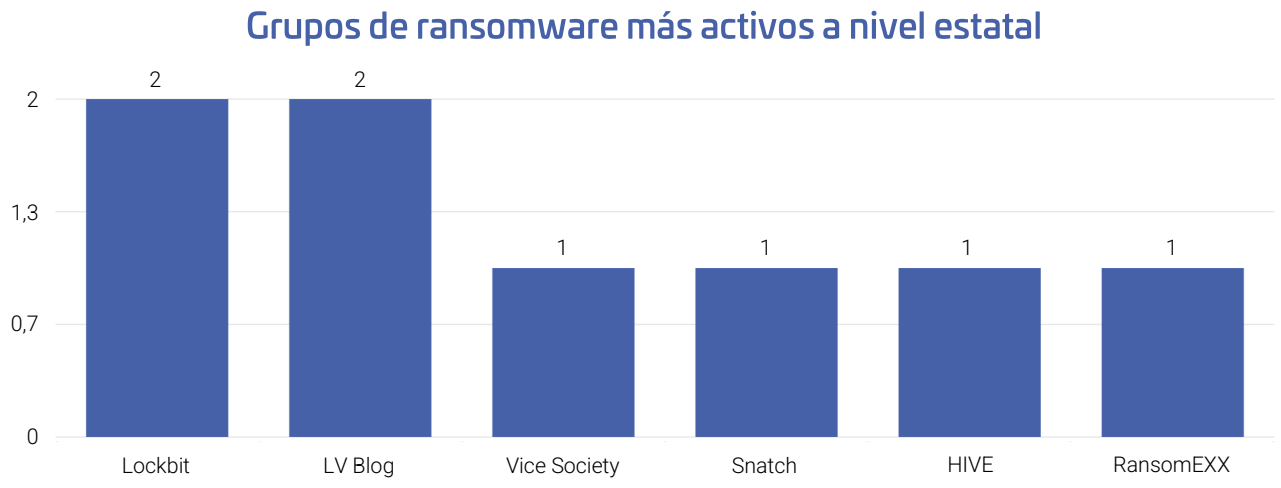
PAÍSES MÁS AFECTADOS POR RANSOMWARE. FUENTE: BCSC

Si se analizan los sectores más atacados por ransomware, se puede ver que el más afectado, a nivel internacional, es la educación, seguido de empresas de construcción. A continuación, se presenta la lista de sectores más atacados por ransomware:

SECTORES MÁS ATACADOS POR RANSOMWARE. FUENTE: BCSC

Por lo general, no se diferencia un patrón de un actor que ataque más a algún tipo de sector. Se han podido ver campañas puntuales, pero los ataques suelen ser indiscriminados.

A nivel estatal, en el cuarto trimestre del año se han hecho públicos 8 ataques de ransomware, lo que supone un aumento del 170% respecto a los 10 reportados en el trimestre anterior, distribuidos entre los diferentes grupos de la siguiente manera:



GRUPOS DE RANSOMWARE CON MAYOR IMPACTO ESTATAL. FUENTE: BCSC

Es importante tener en cuenta que estos datos se basan en aquellos ataques que los propios grupos han hecho públicos, por lo que es posible que hayan sido más, existiendo ciertas evidencias de que la atribución de algún ataque se ha realizado a alguno de estos grupos, pero este no lo ha reconocido en su web.

Al igual que la tendencia revisada a nivel internacional, Lockbit es el ransomware de mayor incidencia con 2 víctimas, junto con LV Blog.

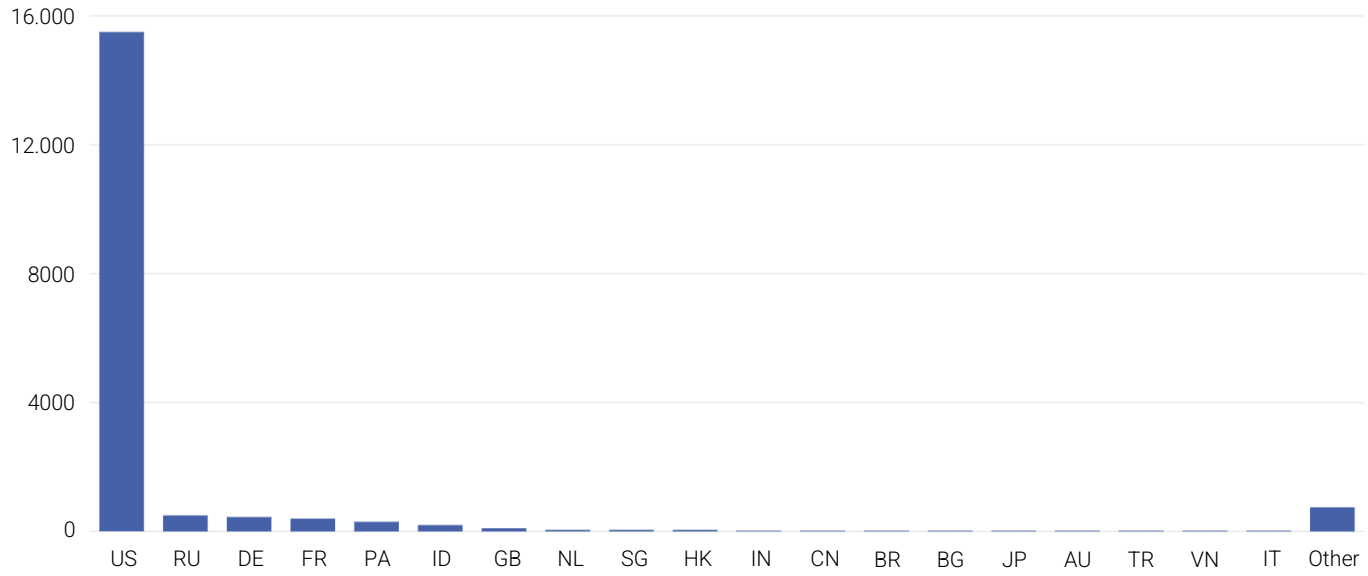
Respecto a los sectores más atacados, siguen la siguiente distribución:

SECTORES MÁS ATACADOS POR RANSOMWARE A NIVEL ESTATAL. FUENTE: BCSC

6. Phishing

Durante el cuarto trimestre hemos identificado un total de 19.262 URLs de phishing activas.

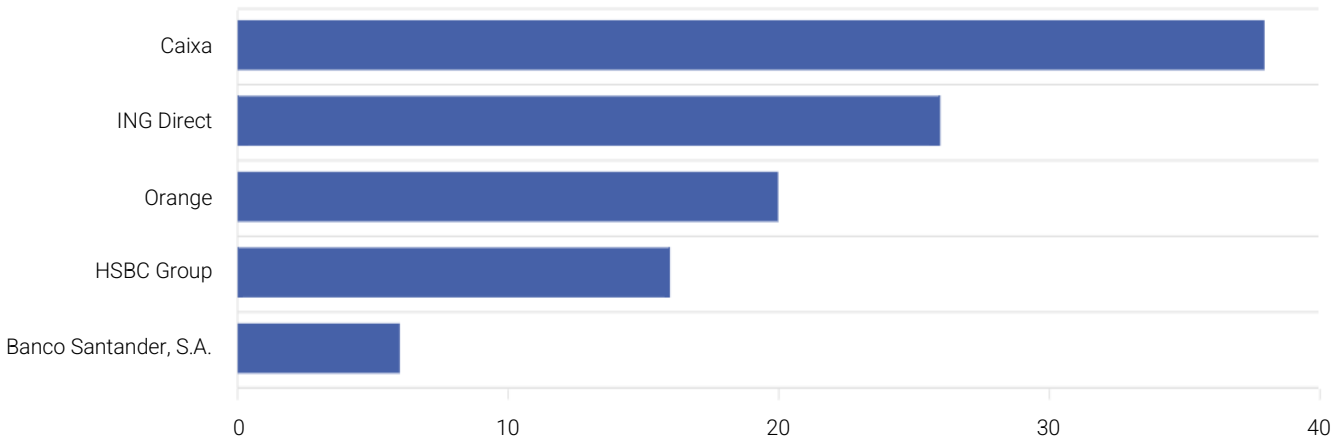
Durante el cuarto trimestre hemos identificado un total de 19.262 URLs de phishing activas. A continuación, se puede observar su distribución en base al país de origen:



DISTRIBUCIÓN DE PHISHING. FUENTE: BCSC

Las 5 entidades estatales (o con alta actividad local) que han sufrido más campañas de phishing durante este trimestre son:

1. Caixa
2. ING Direct
3. Orange
4. HSBC Group
5. Banco Santander S.A.



TOP 5 DE ENTIDADES ESTATALES MÁS AFECTADAS POR PHISHING. FUENTE: BCSC

7. Recomendaciones generales

Tras analizar las amenazas que han afectado a Euskadi en el cuarto trimestre del 2022, es posible identificar las medidas de protección más adecuadas en las que se debería trabajar para poder protegerse de los ataques de las familias de malware que han tenido un mayor impacto.

Revisando la matriz ATT&CK anterior, que recoge las técnicas más habituales utilizados por atacantes en Euskadi, las recomendaciones a tener en cuenta son las siguientes:

- M1049 (Tácticas: Initial Access, Execution, Peristence, Privilege Escalation, Defense Evasion) - Usar un sistema para detectar sofwate malicioso.
- M1015 (Tácticas: Privilege Escalation, Credential Access, Execution, Defense Evasion) - Gestionar la lista de control de acceso para "Replicar cambios de directorio" y otros permisos asociados a la replicación del controlador de dominio. Considere la posibilidad de añadir usuarios al grupo de seguridad de Active Directory "Usuarios protegidos". Esto puede ayudar a limitar el almacenamiento en caché de las credenciales de texto plano de los usuarios.
- M1040 (Tácticas: Execution, Persistence, Persistence, Impact, Defense Evasion, Credential Access, Privilege Escalation, Initial Access) - En Windows 10, active las reglas de reducción de la superficie de ataque (ASR) para asegurar LSASS y evitar el robo de credenciales.
- M1042 (Tácticas: Reconnaissance, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Laeral Movement, Collection, Command and Control, Exfiltration) – Eliminar o deniegue el acceso a software potencialmente peligroso, como son las shells de sistema o los intérpretes de comandos, para que no sean abusados por un atacante.
- M1043 (Tácticas: Persistence, Defense Evasion, Credential Access) - En Windows 10, Microsoft implementó nuevas protecciones llamadas “Credential Guard” para proteger los secretos de LSA que pueden ser utilizados para obtener credenciales a través de formas de volcado de credenciales. No está configurado por defecto y tiene requisitos de sistema de hardware y firmware. Además, no protege contra todas las formas de vertido de credenciales.
- M1041 (Tácticas: Credential Access, Collection, Exfiltration, Impact, Defense Evasion, Credential Sniffing) - Asegurarse que las copias de seguridad del Controlador de Dominio estén debidamente protegidas.
- M1028 (Tácticas: Privilege Escalation, Discovery, Persistence, Command and Control, Exfiltration, Defense Evasion, Impact, Discovery, Lateral Movement, Execution, Credential Access) - Considere desactivar o restringir NTLM. Considere la posibilidad de desactivar la autenticación WDigest.
- M1027 (Tácticas: Credential Access, Persistance, Defense Evasion, Discovery, Lateral Movement, Execution, Exfiltration, initial Access) - Asegurarse de que las cuentas de administrador local tienen contraseñas complejas y únicas en todos los sistemas de la red.
- M1026 (Tácticas: Privilege Escalation, Persistence, Defense Evasion, Execution, Persistence, Initial Access, Lateral Movement, Impact, Credential Access, Privilege Escalation)
    - Windows: no incluir cuentas de usuario o de dominio de administrador en los grupos de administradores locales en todos los sistemas a menos que estén muy controlados, ya que esto suele ser equivalente a tener una cuenta de administrador local con la misma contraseña en todos los sistemas. Seguir las mejores prácticas de diseño y administración de una red empresarial para limitar el uso de cuentas privilegiadas en todos los niveles administrativos.
    - Linux: para extraer las contraseñas de la memoria se necesitan privilegios de root. Seguir las mejores prácticas para restringir el acceso a las cuentas privilegiadas para evitar que los programas hostiles accedan a esas regiones sensibles de la memoria.
- M1021 (Tácticas: Initial Access, Execution, Defense Evasion, Credential Access, Lateral Movement, Command and Control, Exfiltration) - Restringir el uso de ciertos sitios web, bloquee descargas/archivos

adjuntos, bloquee Javascript, restringir las extensiones del navegador, etc. Para código malicioso enviado a través de anuncios, software como bloqueadores de anuncios pueden ayudar a su ejecución en primera instancia.

- M1025 (Tácticas: Persistence, Credential Access) - En Windows 8.1 y Windows Server 2012 R2, active la luz de proceso protegida para LSA.
- M1017 (Tácticas: Credential Access, Persistence, Collection, Defense Evasion, Initial Access, Reconaissance, Execution, Credential Access) - Limitar el solapamiento de credenciales entre cuentas y sistemas formando a los usuarios y administradores para que no utilicen la misma contraseña para varias cuentas.
- M1057 (Tácticas: Collection, Exfiltration) - La prevención de la pérdida de datos puede detectar y bloquear el envío de datos sensibles a través de protocolos no cifrados.
- M1031 (Tácticas: Credential Access, Command and Control, Collection, Exfiltration, Exfiltration, Lateral Movement, Discovery, Initial Access, Persistence, Defense Evasion, Execution) - Los sistemas de detección y prevención de intrusiones en la red que utilizan firmas de red para identificar el tráfico de un malware específico del adversario pueden utilizarse para mitigar la actividad a nivel de red. Las firmas suelen ser para indicadores únicos dentro de los protocolos y pueden basarse en la técnica de ofuscación específica utilizada por un adversario o una herramienta en particular, y probablemente serán diferentes entre varias familias y versiones de malware. Es probable que los adversarios cambien las firmas de Command and Control de las herramientas con el tiempo o que construyan los protocolos de tal manera que eviten ser detectados por las herramientas defensivas comunes.
- DS0017 (Tácticas: Privilege Escalation, Discovery, Persistence, Discovery, Collection, Exfiltration, Persistence, Discovery, Credential Access, Execution, Impact, Inhibit Response Function, Defense Evasion) - Supervisar los comandos y argumentos ejecutados que pueden interactuar con el Registro de Windows, buscar detalles sobre la configuración y los ajustes de la red, como las direcciones IP y/o MAC, realizar capturas de pantalla o exfiltrar documentos sensibles de los sistemas a los que acceden o mediante el descubrimiento de información de sistemas remotos.

8. Bibliografía

I. https://thehackernews.com/2022/10/fbi-cisa-and-nsa-reveal-how-hackers.html

II. https://therecord.media/cyberattack-disrupts-bulgarian-government-websites-over-betrayal-to-russia/

III. https://www.noticiasdealava.eus/union-europea/2022/11/23/web-parlamento-europeo-sufre-ciberataque-6251329.html

IV. https://www.infosecurity-magazine.com/news/ransomware-australian-defence/

V. https://www.thenews.com.pk/print/1007174-indian-hackers-target-computers-of-pak-politicians-generals-report

VI. https://securityaffairs.co/138127/cyber-crime/cyberattack-blocked-trains-denmark.html

VII. https://www.europapress.es/catalunya/noticia-ciberataque-afecta-tres-hospitales-barcelona-madrugada-viernes-20221007110113.html

VIII. https://www.xataka.com/seguridad/telefonica-ha-sufrido-ciberataque-eres-cliente-movistar-u-o2-asi-puedes-cambiar-contrasena

IX. https://www.interior.gob.es/opencms/eu/detalle/articulo/La-Policia-Nacional-desarticula-una-organizacion-criminal-dedicada-al-fraude-del-CEO-que-operaba-a-nivel-nacional-e-internacional/

X. https://www.noticiasdealava.eus/sociedad/2022/11/19/ciberataque-grupo-noticias-6243829.html

XI. https://www.elcorreo.com/alava/araba/cinco-detenidos-banda-alava-por-estafar-a-clientes-entidades-bancarias-con-envio-sms-falsos-20221021104817-nt.html

Basque CyberSecurity Centre

BASQUE CYBERSECURITY CENTRE:

Zibersegurtasunaren topagunea Euskadin

El punto de encuentro de la ciberseguridad en Euskadi

info@bcsc.eus

Albert Einstein 46, 3ª planta Edificio E7
Arabako Teknologi Parkea
01510 Vitoria-Gasteiz

945 236 636