RESUMEN EJECUTIVO MEMORIA ANUAL 2022

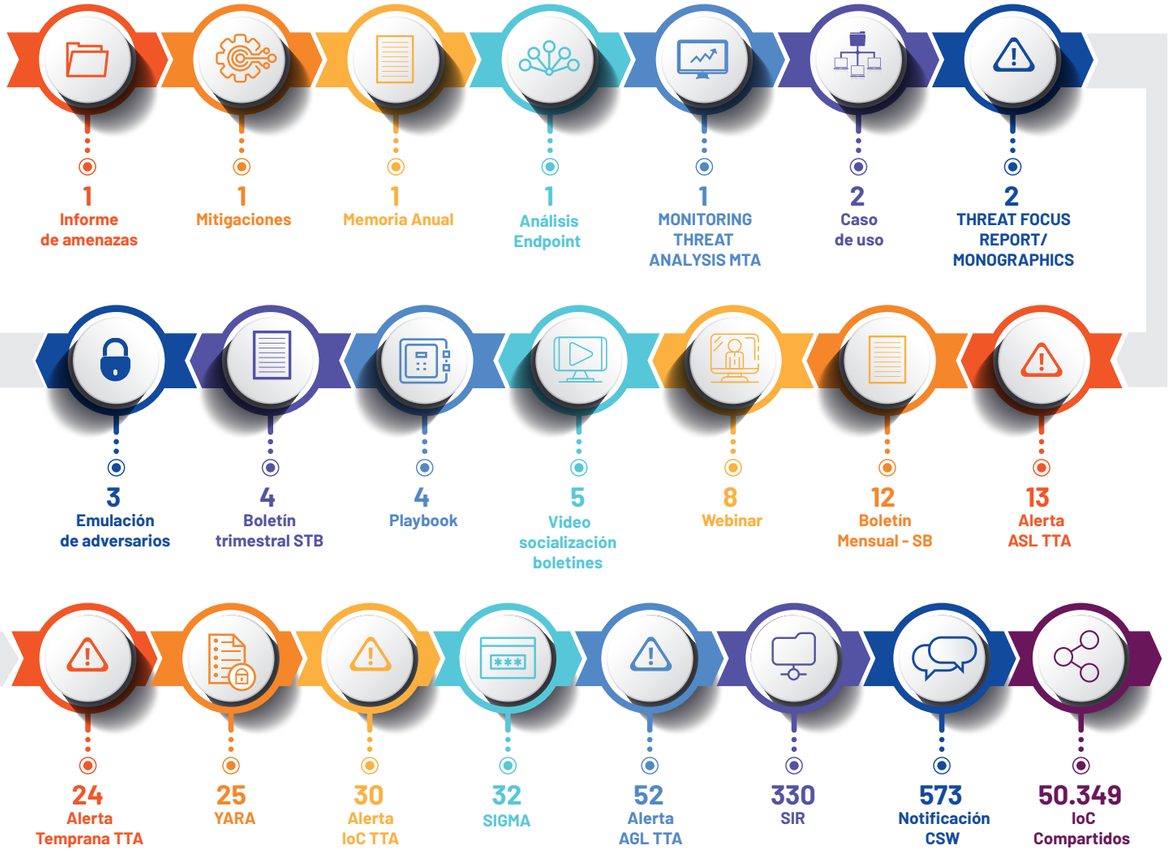
Aso Ban Caria

A lo largo de 2022, el Csirt Financiero trabajó con especial intensidad en la identificación de todas aquellas amenazas cibernéticas que rodearon el sector financiero colombiano y que, de forma directa o transversal, pusieron en riesgo la integridad de las entidades; todo esto en un panorama de constante cambio y adaptación, que permitió entender el comportamiento de estas.

Es significativo indicar que desde las tres capacidades fundamentales del Csirt Financiero; el Observatorio de Ciberseguridad, la Inteligencia de Amenazas y el Análisis y Apoyo de Incidentes, el equipo de analistas logró realizar, de forma pormenorizada, el análisis de las diferentes ciberamenazas que impactaron al sector financiero, con el objetivo de brindar una comprensión detallada de éstas, así como una fuerte defensa que permitió evitar diversas categorías de incidentes de seguridad en las entidades del sector financiero.

De esta forma, a lo largo del año 2022 el Csirt Financiero realizó las siguientes actividades, las cuales puso a disposición de los asociados, así:

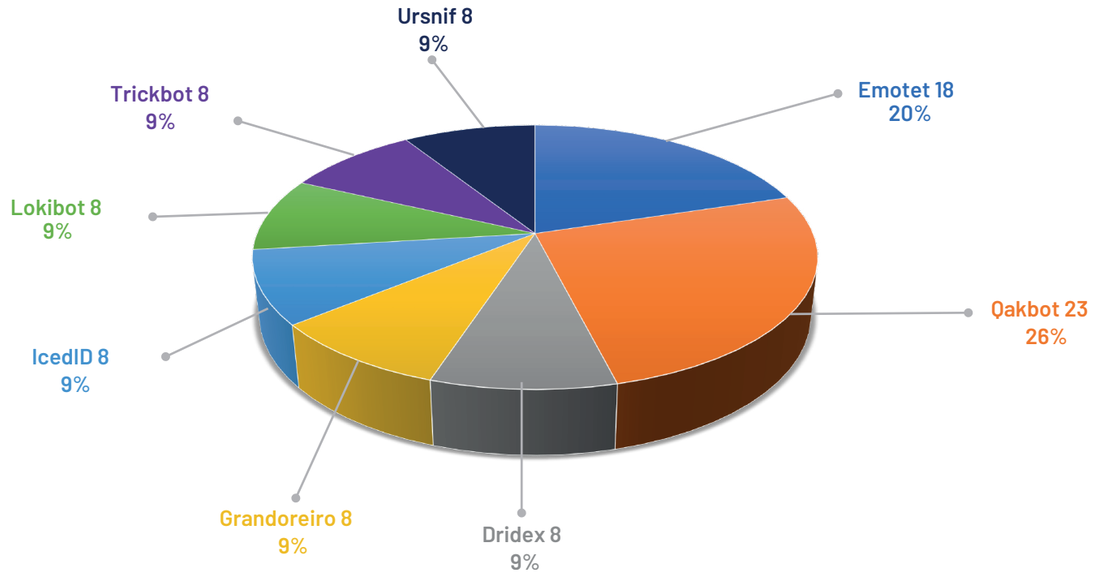
Gráfico 1. Productos compartidos por el Csirt Financiero en el 2022



Fuente: Csirt Financiero 2022

Desde las tres capacidades del Csirt Financiero - Observatorio de Ciberseguridad, Inteligencia de Amenazas y Análisis y Apoyo de Incidentes- el equipo de analistas logró realizar de forma pormenorizada el análisis de la diferentes ciberamenazas dirigidas al sector financiero.

Gráfico 2. Top troyanos reportados 2022

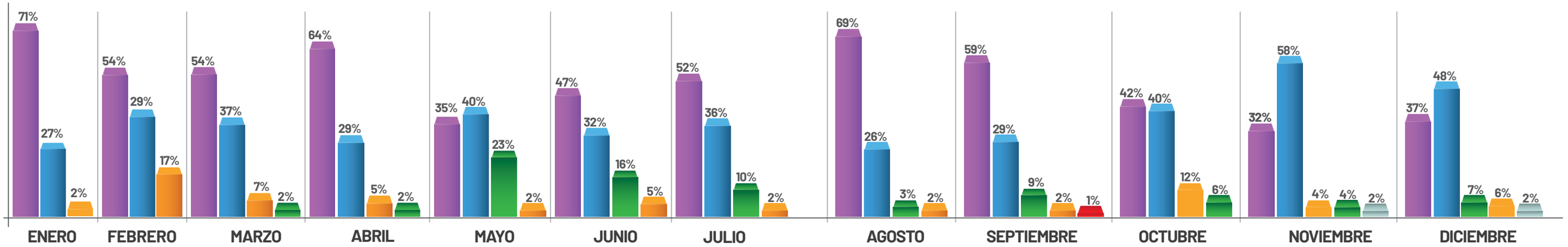


Fuente: Csirt Financiero 2022 – Observatorio de Ciberseguridad

Top amenazas por mes

Los avances por parte de los ciberdelincuentes en la nueva etapa postpandemia han dado como resultado un incremento de amenazas contra el sector financiero. En términos generales, se pudo confirmar que los malware bancarios y el ciberfraude siguen siendo las ciberamenazas de mayor impacto contra el sector.

Gráfico 3. Top de amenazas por mes



Convenciones

- Malware Bancario
- Ciberfraude
- Vulnerabilidades
- Ataques POS
- Suplantación

Fuente: Csirt Financiero 2022 – Observatorio de Ciberseguridad

Observatorio de ciberseguridad

El Csirt Financiero se encarga de recopilar y analizar información relacionada con las distintas ciberamenazas que pueden afectar al sector financiero, brindando diferentes medidas para identificar y prevenir posibles ataques informáticos a las infraestructuras propias de las entidades, mitigando los riesgos asociados.

Troyanos

Este tipo de malware continúa siendo de los más intensos en relación con los ataques a las infraestructuras y a la seguridad de la información. El comportamiento analizado por el equipo de analistas durante el 2022 se resume de la siguiente manera:

Gráfico 4. Tipos de troyanos identificados en 2022

Fuente: Csirt Financiero 2022 – Observatorio de Ciberseguridad

Troyanos bancarios

Con 188 reportes relacionados a troyanos bancarios, el Csirt Financiero consolidó en el 2022 este tipo de amenaza como una de las más relevantes, tanto por su amplia distribución como por su afectación directa al sector.

En el análisis, el Csirt Financiero observó que algunos troyanos muy conocidos sufrieron modificaciones para mejorar sus capacidades de evasión frente a soluciones antimalware o mejoras para generar persistencia en los equipos comprometidos. Algunos también actualizaron las técnicas para realizar los movimientos laterales dentro de las infraestructuras informáticas afectadas.

Las 24 familias analizadas por el equipo del Csirt Financiero fueron las siguientes:

Gráfico 5. Familias analizadas

Fuente: Csirt Financiero 2022 – Observatorio de Ciberseguridad

Ransomware

Definitivamente, 2022 fue un año importante en la constante evolución de múltiples familias de ransomware. El Csirt Financiero evidenció nuevas cepas y actualizaciones que han impactado negativamente a todos los sectores, incluyendo el financiero. La mayoría de estas familias son ofrecidas en foros clandestinos de la deep y dark web mediante la modalidad de Ransomware- as-a-Service (RaaS) para que los ciberdelincuentes puedan obtener un servicio personalizado hacia distintos objetivos.

Gráfico 6. Evolución del ransomware en 2022

1. Ha sido una de las ciberamenazas que más impacto ha generado a nivel global a empresas de diferentes ámbitos. Al ser una amenaza que puede afectar a diversos sectores (incluyendo al financiero) de manera transversal.

2. El Ransomware como Servicio (RaaS) ha sido mejorado y ha adaptado sus infraestructuras con el fin de captar una mayor cantidad de afiliados que les permitan generar mayores beneficios económicos incrementando progresivamente el valor del rescate exigido a sus víctimas.

3. Los ciberataques basados en ransomware han encontrado en la cadena de suministros un eslabón débil que aprovechan en beneficio propio, logrando llegar a afectar a más de una empresa de manera simultánea y en diferentes partes del mundo, maximizando el compromiso inicial.

4. Dentro de las ciberamenazas observadas se destacan familias de ransomware como Hive, BlackCat, RansomHouse, BlackByte y LockBit 3.0, entre otros. La cadena de infección que utilizan los ciberdelincuentes para la distribución de estas familias varía en función de sus objetivos.

5. Entre los principales vectores de infección utilizados por el ransomware se encuentran:
   - El uso de correos electrónicos tipo Phishing.
   - Aprovechamiento de vulnerabilidades.
   - Ciberataques al protocolo de acceso remoto (RDP).

6. Los grandes grupos cibercriminales siguen incluyendo dentro de su arsenal extorsivo la exigencia a sus víctimas del pago por no hacer pública la información obtenida previamente al cifrado de la misma dentro de sus infraestructuras informáticas.

Fuente: Csirt Financiero 2022 – Observatorio de Ciberseguridad

Sistema POS y ATM

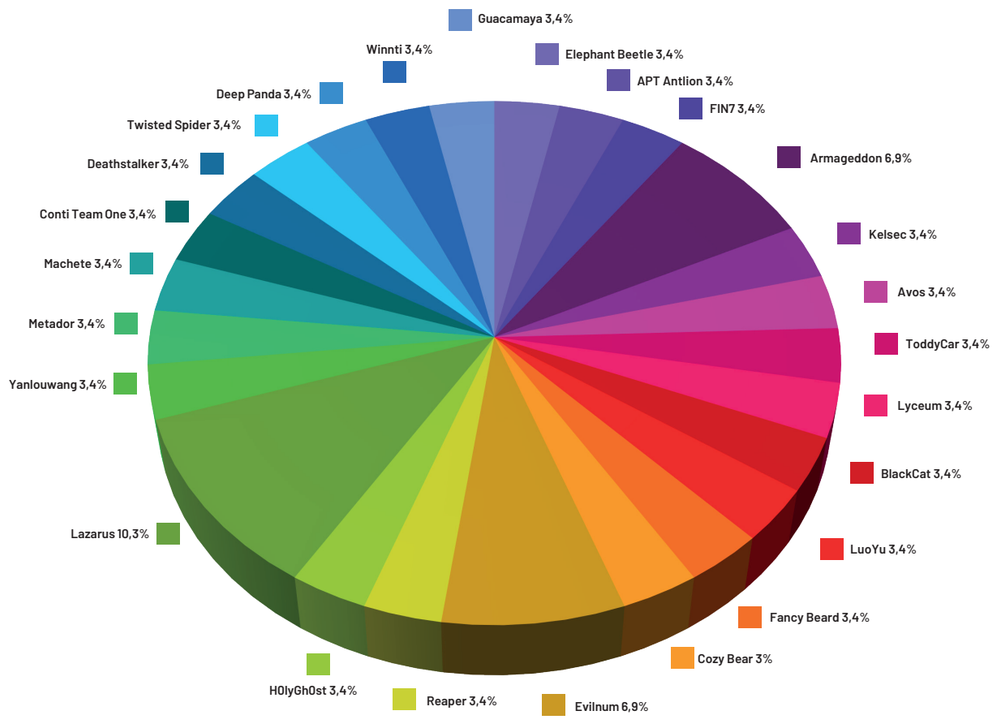
En el año 2022 no hubo gran actividad en cuanto a amenazas contra los sistemas POS (Point of Sale por sus siglas o Punto de Venta en español). Sin embargo, sí se evidenció una evolución considerable frente al malware Prilex, el cual anteriormente realizaba ataques a cajeros automáticos (ATM) para obtener la información de las tarjetas de crédito utilizadas en ellos.

De acuerdo con lo anterior se presentó un aumento en los ataques realizados a los cajeros automáticos (ATM) en comparación con el año anterior, esto se debió en gran parte a que en 2021 las restricciones derivadas de la pandemia producida por el Covid-19 obligó a los ciudadanos a quedarse en casa y realizar las transacciones en línea; sin embargo, a medida que se fue retornando a los hábitos antiguos, los cibercriminales se adaptaron al nuevo contexto.

APTs

Se evidenció un aumento en las campañas de infección generadas tanto por grupos APT nuevos como por grupos ya conocidos. A continuación, se muestra un gráfico donde se encuentra la información de los grupos APT activos durante el año 2022.

Gráfico 7. Grupos APT activos durante 2022



Fuente: Csirt Financiero 2022 – Observatorio de Ciberseguridad

Malware móvil

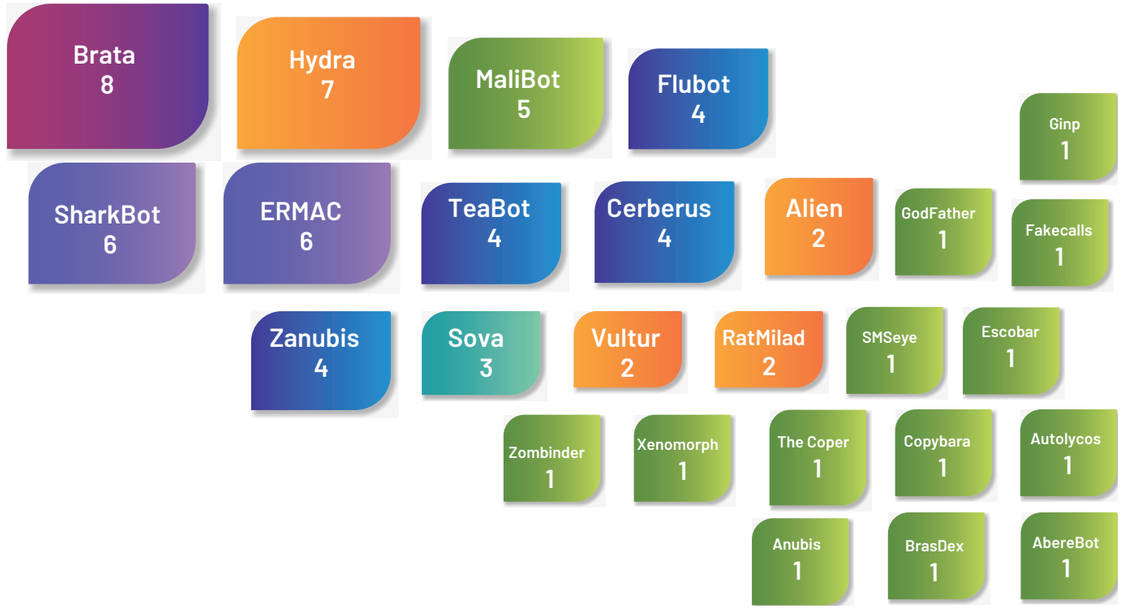
Una de las amenazas que impactó de manera significativa al sector financiero y a sus usuarios fueron los troyanos bancarios, sobre todo aquellos dirigidos a los dispositivos con sistema operativo Android, el cual es el sistema más utilizado en los dispositivos móviles.

El Csirt Financiero comunicó a los asociados cerca de 26 familias de malware que fueron desarrolladas para dirigir sus actividades maliciosas a los dispositivos Android; una cifra mayor en comparación con el año 2021 debido a dos elementos clave:

- La constante actualización de las tácticas, técnicas y procedimientos (TTP) de las amenazas ya existentes.
- El surgimiento de nuevas familias de malware.

En este sentido, las familias de malware analizadas y comunicadas por el Csirt Financiero son las siguientes:

Gráfico 8. Número de familias de malware móvil analizadas



Fuente: Csirt Financiero 2022 – Observatorio de Ciberseguridad

Capacidades de malware móvil

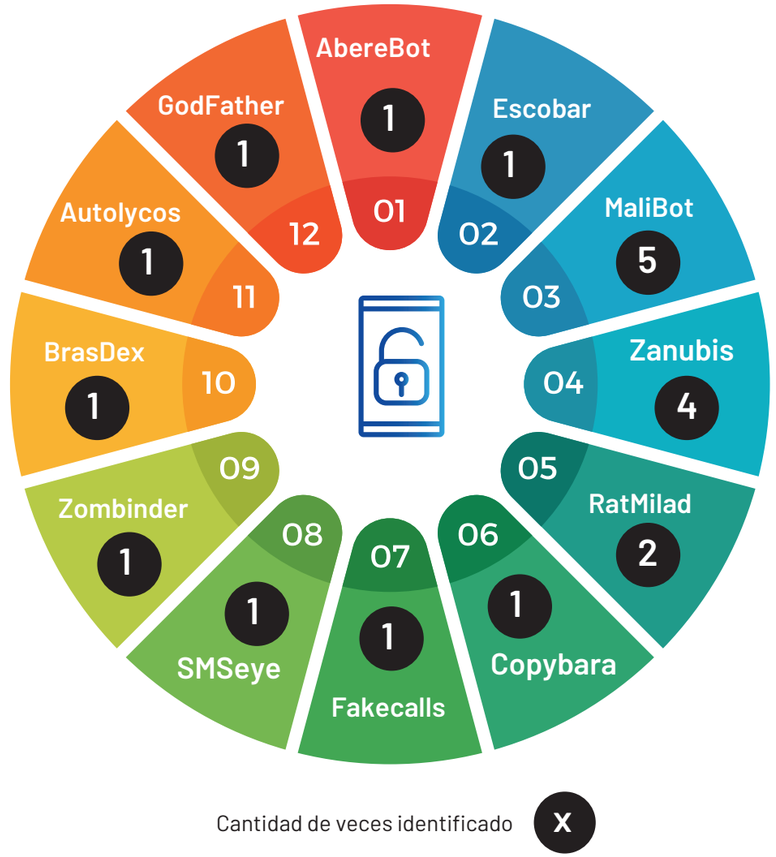
Entre las familias de malware analizadas se destacaron las siguientes funcionalidades, orientadas a generar mayor afectación en los dispositivos comprometidos:

Gráfico 9. Capacidades del malware móvil

Fuente: Csirt Financiero 2022 – Observatorio de Ciberseguridad

Dentro de estas familias de malware reportadas por el Csirt Financiero, se identificó que 12 de ellas surgieron en el año 2022, así:

Gráfico 10. Familias de Malware Móvil que surgieron en 2022



Fuente: Csirt Financiero 2022 – Observatorio de Ciberseguridad

Inteligencia de amenazas

A través de esta capacidad se evidenció un aumento en los ciberataques debido a la detección de numerosas fallas de seguridad en productos ampliamente utilizados por las empresas en todo el mundo. Para hacer frente a este problema crítico, el Csirt Financiero ha recopilado información y conocimiento en inteligencia de amenazas relacionadas con las vulnerabilidades de los sistemas informáticos en el sector financiero.

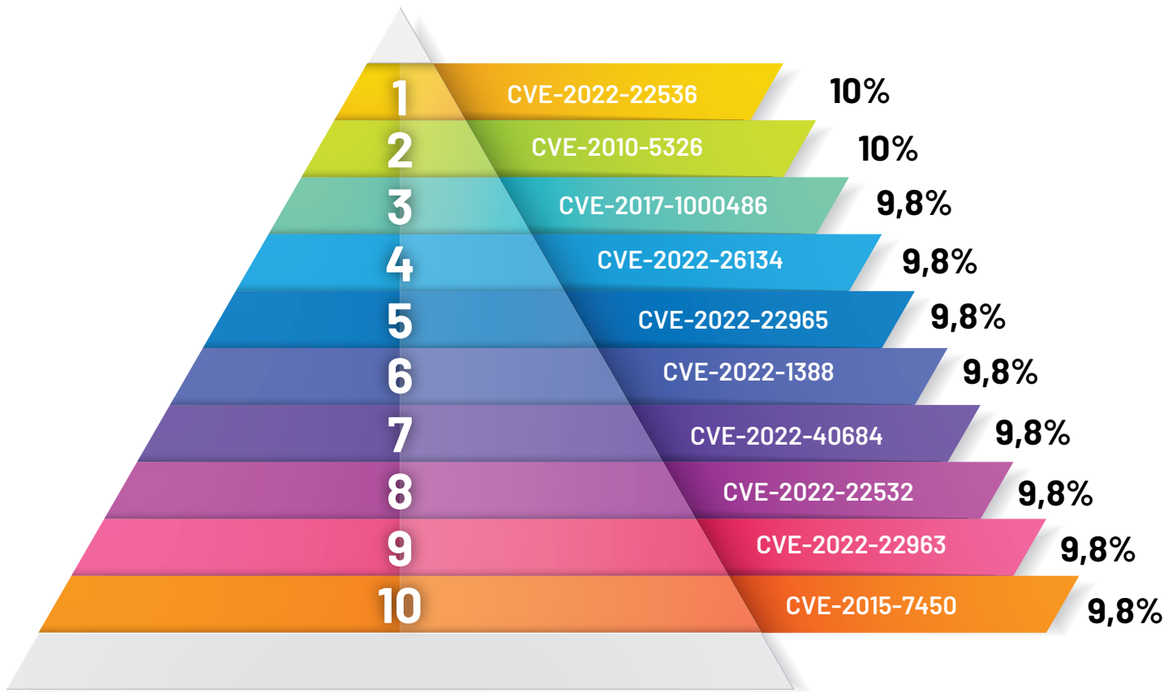
Adicionalmente, se han clasificado estas vulnerabilidades según su gravedad e impacto potencial en las organizaciones que utilizan estos servicios.

A continuación, se muestra el top de vulnerabilidades con mayor implicación en actividades maliciosas reportado por el Csirt Financiero:

24 Alertas reportadas a lo largo del 2022

60 CVE y/o vulnerabilidades reportadas en 2022

Gráfico 11. Top 10 vulnerabilidades más críticas reportadas



Fuente: Csirt Financiero 2022 – Inteligencia de amenazas

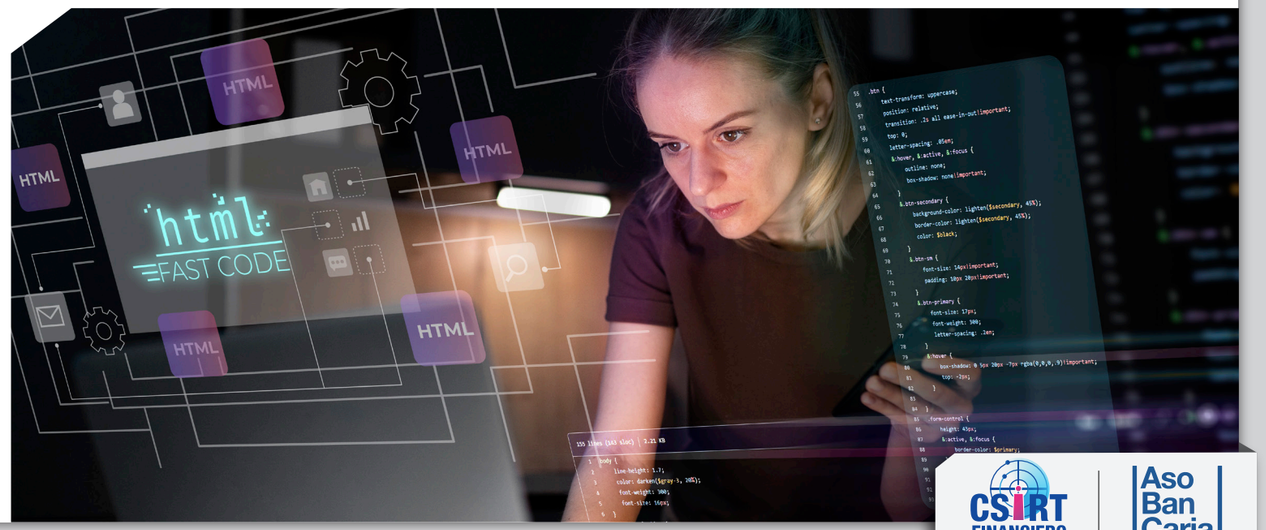
Gráfico 12. Eventos reportados por los asociados en el 2022

Fuente: Csirt Financiero 2022 – Support Incident Response

Apoyo a incidentes

El análisis y apoyo de incidentes se ha convertido en el eje central del Csirt Financiero durante el 2022. Esta capacidad se centra en la identificación, modelación, detección y mitigación de amenazas que afectan de manera directa al sector bancario. De acuerdo con lo identificado durante el año 2022, se logró observar diversas familias de troyanos de acceso remoto, así como variantes de amenazas potenciales que se dirigían al sector, dentro de las que se destacan AsyncRAT, RemcosRAT y BitRAT.

Así mismo, se observó el incremento de campañas que tenían como finalidad realizar la suplantación de identidad de la banca virtual de las entidades financieras, a través de formularios de tipo phishing que capturan datos de los funcionarios y clientes, con el objetivo de realizar fraude financiero o capturar la cuenta de correo electrónico.



Tendencias en ciberseguridad 2023

1. Contra el sector financiero

Se prevé que para 2023 continue aumentando el robo de identidad y uso fraudulento de datos dentro del sector financiero. Los cibercriminales usarán herramientas sofisticadas, como ingeniería social mejorada a través de los deep fake o mediante los chat inteligentes como ChatGPT, para obtener información confidencial e intentar robar fondos de cuentas bancarias personales o corporativas sin ser detectados por los sistemas existentes.

2. Ataques relacionados con la IA

Los avances actuales en Inteligencia Artificial están demostrando cómo pueden ser utilizadas las redes neuronales y algoritmos para ser explotados por el cibercrimen. Uno de los elementos más reveladores es la existencia de bots de IA, que permiten evolucionar el discurso según se propone y aprende.

3. Ataques contra plataformas cloud

El aumento de la adopción de la nube en el sector financiero es una magnífica oportunidad para optimizar los procesos de negocio y hacer más eficiente la operación, sin embargo, también genera nuevos riesgos digitales que deben ser tenidos en cuenta. De hecho, todas las estadísticas demuestran que, en 2022, se dispararon los intentos de ataque, centrados en la explotación de vulnerabilidades en la infraestructura y las configuraciones.

4. Aumentan las amenazas internas (insider)

Los motivos detrás de las amenazas internas pueden variar, desde el robo de información confidencial para obtener ganancias financieras, hasta la toma de represalias contra la empresa o los compañeros de trabajo. En cualquier caso, estas amenazas internas pueden tener graves consecuencias como la pérdida de datos, la interrupción del negocio y el daño a la reputación.

5. Continúan los ataques a la cadena de suministro

Las instituciones financieras pueden ser atacadas a través de terceros que manejan datos sensibles para ellas, como proveedores de software, plataformas de pagos en línea o empresas de seguridad cibernética. Por supuesto, también proveedores de servicios no digitales.

Tendencias tecnológicas para 2023

1. Tecnología Cuántica

Como toda disciplina vinculada a la tecnología, la ciberseguridad depende también de la capacidad de almacenamiento, velocidad de comunicación de los datos y procesamiento. Desde hace varias décadas, investigadores de todo el mundo trabajan por encontrar la clave para dar un salto significativo a los principios básicos que rigen los desarrollos de hoy día.

La tecnología basada en computación cuántica cada vez está más cerca de conseguir su objetivo. Prueba de ello es el anuncio de NIST realizado en 2022, a través del cual comunicaba a la comunidad científica que estaban trabajando ya en sus propios algoritmos criptográficos cuánticos. Tanto es así, que la comunidad internacional ha bautizado a la nueva era “El mundo Post-Quantum”.

2. Biometría

El uso de la biometría continúa un año más entre nuestras tendencias futuras a pesar de ser ya un hecho totalmente reconocido. Esto se debe a la rápida evolución de las nuevas tecnologías que combinan diferentes vectores biométricos, además de mejorar la definición de estos, interpretando más puntos de la huella biométrica, ya sea dactilar, iris, facial, de escritura o de voz. Precisamente, será en la voz donde se avance especialmente para continuar perfilando cada vez más parámetros. Actualmente es posible identificar más de 100 parámetros que diferencian la voz, no sólo relacionados con los elementos físicos, sino también con relación al comportamiento y múltiples estados que provocan diferentes tonos. Sin duda una evolución frente al avance en los deep fake que pueden ser utilizados para suplantar una identidad mediante la voz.

3. Inteligencia Artificial

Otro de los grandes pilares de la nueva era digital es el desarrollo y capacidad de explotación de la Inteligencia Artificial (IA) y el Aprendizaje Automático (ML).

Al igual que sucede con la tecnología cuántica, la IA lleva décadas en desarrollo, sin embargo, es a raíz de la pandemia, cuando grandes inversiones han permitido una aceleración de su explotación comercial. Y en este sentido, estas tecnologías están demostrando ser de gran valor para la ciberseguridad gracias a su capacidad para detectar rápidamente amenazas, proporcionar una mejor visibilidad de las actividades sospechosas y reducir de forma significativa el tiempo necesario para reaccionar ante incidentes.

Créditos

ASOBANCARIA

Presidente

Jonathan Malagón González

Vicepresidente Administrativa y Financiera

Mónica María Gómez Villafañe

Directora Dirección de Programas de Innovación Gremial

Angela María Vaca Bernal

Profesional Máster Dirección de Programas de Innovación Gremial

Sergio Andrés Silva Perico

Profesional Junior Dirección de Programas de Innovación Gremial

Cristian Camilo Rubiano Bautista

CSIRT FINANCIERO (MNEMO)

Equipo técnico y de operación del CSIRT

Director de Operaciones

Carlos Javier Beltrán

Directora de Estrategia Operativa

Eva Moya

Líder Técnico

Carlos Andrés Guzmán

Líder Edición y Calidad

Belén Viqueira

Líder Gestión

Jorge Andrés Chaves

Analistas Csirt Financiero

Paula Natalia Orjuela

Lady Zolanyi Páez

Brayan Andrés Gómez

Fernando Vargas

Cristian Alexander Moreno

ALCG DISEÑO • PUBLICIDAD

Diseño y Diagramación

Adriana Cuéllar González