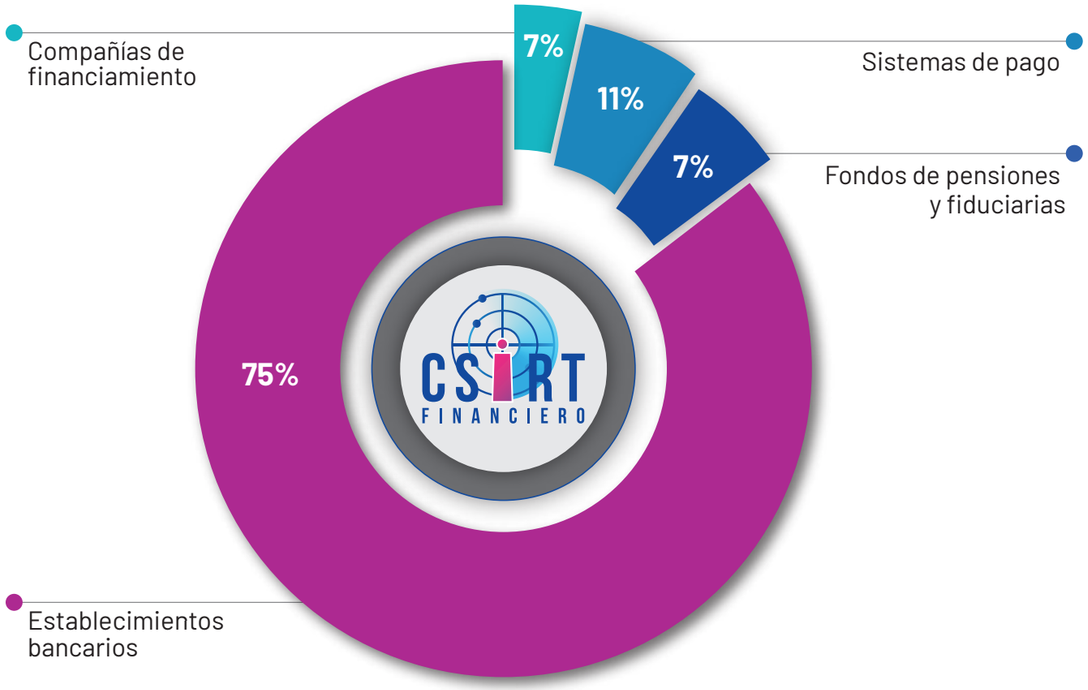
CSIRT FINANCIERO

2021

MEMORIA anual

Aso Ban Caria

En la actualidad consumen e intercambian información 28 entidades financieras como miembros del CSIRT, representando el mayor porcentaje los establecimientos bancarios.



La colaboración se ha profundizado en la investigación conjunta de inteligencia de amenazas sectoriales a través de

1. El uso de herramientas tecnológicas de forma conjunta entre las entidades y el CSIRT.
2. Reporte de más de 200 muestras de código malicioso para análisis de familias y su evolución.
3. Análisis y ejecución de ransomware en laboratorios y espacios controlados.

En 2021 consolidamos la confianza a través de un mayor nivel de intercambio y reporte de información de eventos cibernéticos locales, reflejándose en las actividades lideradas por el equipo de respuesta a incidentes de ciberseguridad.

- Apoyo a la gestión y la resolución de cerca de 400 eventos de seguridad de las entidades miembro.
- Elaboración de recomendaciones operativas para la detección, contención, erradicación y recuperación para el sector.
- Despliegue de más de 250 reglas de seguridad, permitiendo la integración en SIEM de cada entidad, generando un marco de ciberdefensa colectiva.

El Csirt Financiero trabajó intensamente en la identificación de todas aquellas amenazas cibernéticas que rodearon el sector financiero colombiano y que, de forma directa o transversal, buscaron afectar o atacar a las entidades; todo esto en un panorama de constante cambio y adaptación, que permitió entender el comportamiento de estas.

A continuación, se pueden apreciar los trabajos realizados por el Csirt Financiero con la intención de comprender y prevenir las diversas ciberamenzas identificadas:

1.099

DOCUMENTOS GENERADOS

Correspondientes a boletines mensuales, informes monográficos de amenazas, alertas y Casos de uso.

687

ALERTAS REALIZADAS

Enmarcadas en el observatorio de ciberseguridad.

72.446

IoC CARGADOS

IoC cargados en la plataforma de intercambio de inteligencia de amenazas MISP.

49

ALERTAS DE INTELIGENCIA DE AMENAZAS

Buscando prevenir ciberamenzas en el sector financiero.

389

PETICIONES DE APOYO A INCIDENTES

Fortaleciendo la colaboración entre CSIRT y los asociados, así como la capacidad de respuesta de los equipos.

253

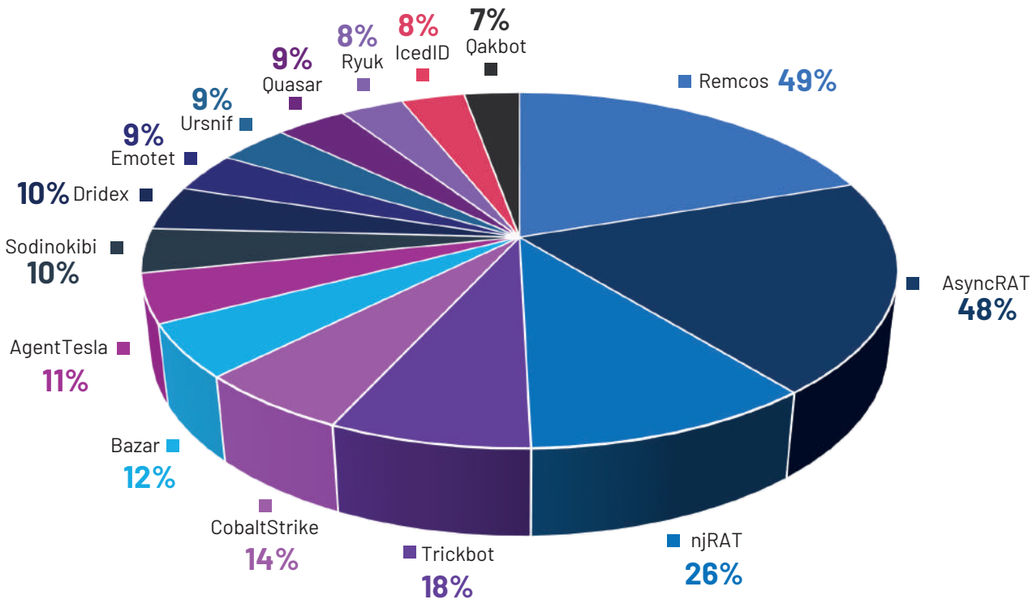
REGLAS

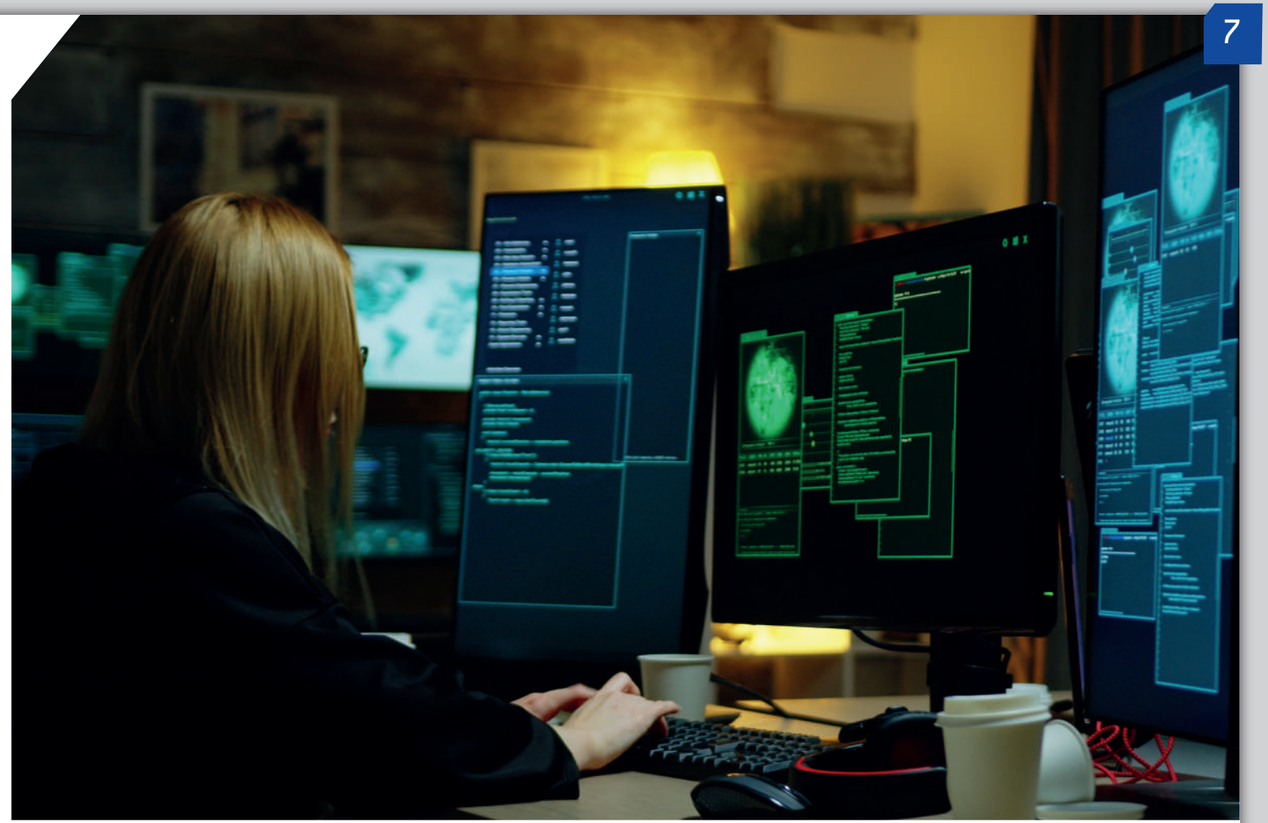
Distribuidas entre 147 reglas SIGMA y 106 reglas YARA. El beneficio que trae consigo la incorporación de reglas SIGMA y YARA en las plataformas tecnológicas se traduce en la mitigación del riesgo e impacto que causan las diferentes amenazas cibernéticas.

14

PLAYBOOKS Y PLANTILLAS DE REMEDIACIÓN

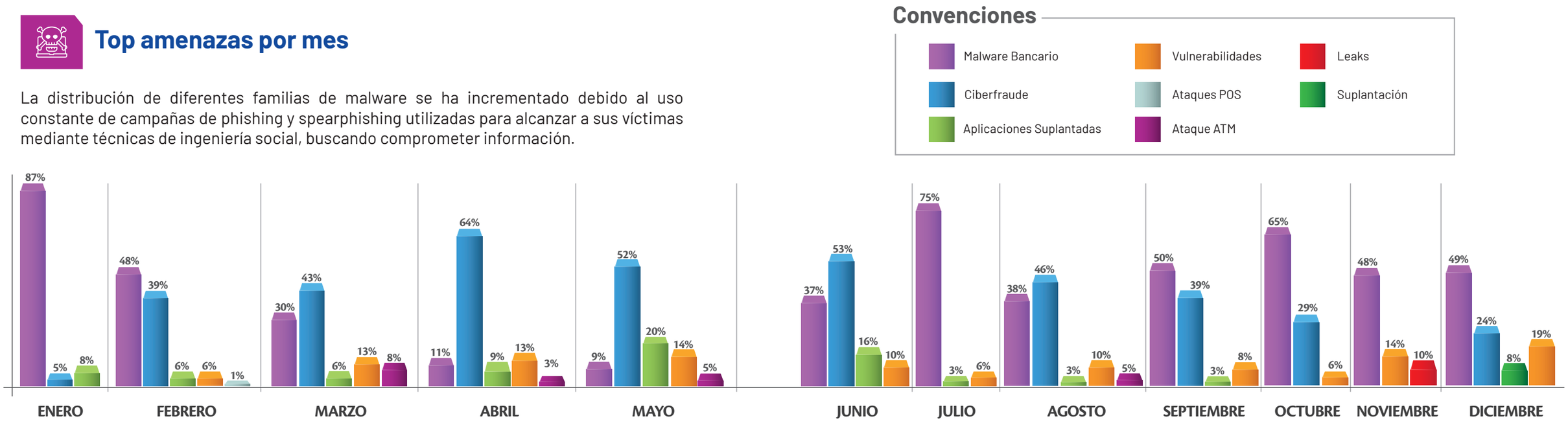
Desde las tres capacidades del Csirt Financiero - Observatorio de Ciberseguridad, Inteligencia de Amenazas y Análisis y Apoyo de Incidentes- el equipo de analistas logró realizar de forma pormenorizada el análisis de la diferentes ciberamenazas dirigidas al sector financiero global.





Top amenazas por mes

La distribución de diferentes familias de malware se ha incrementado debido al uso constante de campañas de phishing y spearphishing utilizadas para alcanzar a sus víctimas mediante técnicas de ingeniería social, buscando comprometer información.



Observatorio de ciberseguridad

Troyanos

Han generado innumerables afectaciones a la seguridad de la información y ciberseguridad a nivel global ampliando sus capacidades, clasificándose en diferentes tipos.

En el transcurso del 2021 los tipos de troyanos y la cantidad de reportes realizado por el Csirt Financiero fue la siguiente:

Trojan Banker

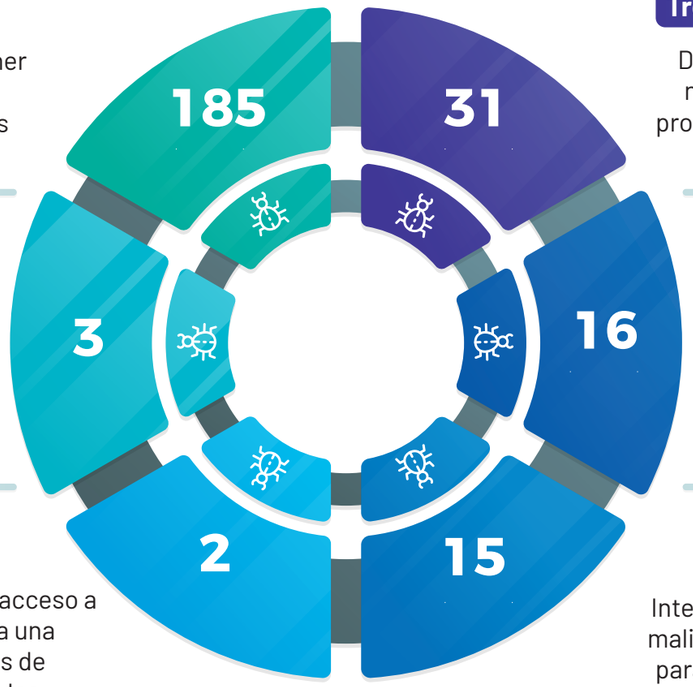
Su objetivo es obtener las credenciales de acceso a las cuentas bancarias.

Trojan Clicker

Diseñados para acceder a los recursos de Internet.

Trojan Proxy

Diseñados para dar acceso a los cibercriminales a una variedad de recursos de Internet, a través de los equipos infectados.



Trojan Downloader

Descargan e instalan nuevas versiones de programas maliciosos.

Trojan Spy

Pueden espiar el uso del equipo de la víctima.

Trojan Dropper

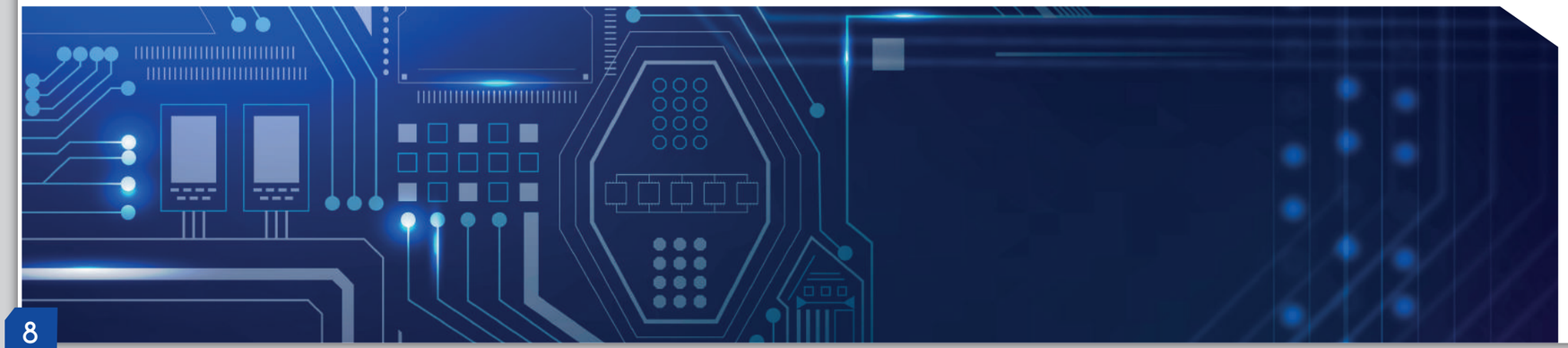
Integran otros recursos maliciosos en su código para luego instalarlos o ejecutarlos en el equipo.

Un aspecto para resaltar ha sido el alza en el uso de troyanos de acceso remoto -RAT- que fueron comunes al momento de realizar actividades malintencionadas por parte de actores maliciosos.

Un aspecto para resaltar ha sido el alza en el uso de troyanos de acceso remoto -RAT- que fueron comunes al momento de realizar actividades malintencionadas por parte de actores maliciosos.

El Csirt Financiero reportó 25 familias de RATs en el año 2021, algunas de ellas implicadas en campañas directamente dirigidas a los asociados, destacándose: **RemcosRAT**, **AsyncRAT**, **njRAT** y **BitRAT**, este último se conoció en noviembre de 2020 pero expandió su actividad maliciosa rápidamente, posicionándose en el top 10.

Como vectores a destacar para difundir los troyanos de tipo RAT principalmente se encuentran **Phishing** y **Spearphishing**.



Ransomware

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.

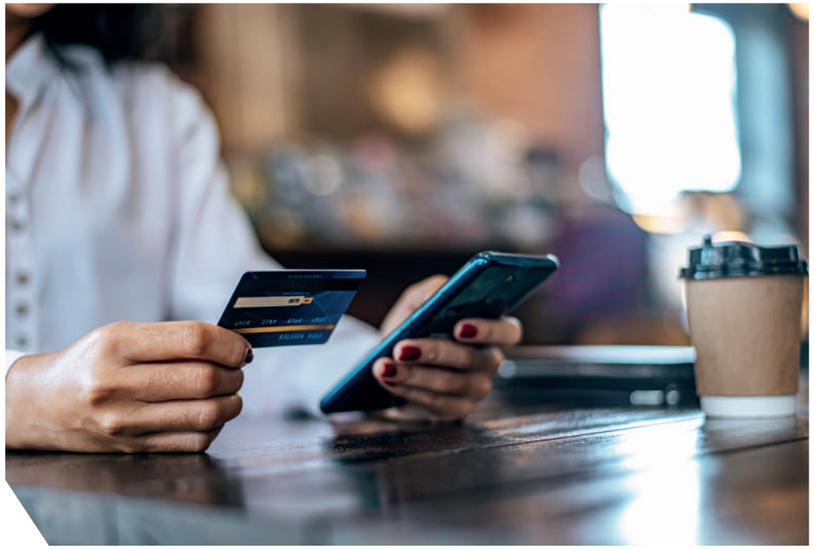
4. Dentro de las ciberamenazas observadas se destacan familias de ransomware como Avaddon, REvil, Ryuk, Pysa, Hive y LockBit 2.0, entre otros. La cadena de infección que utilizan los ciberdelincuentes para la distribución de estas familias varía en función de sus objetivos.

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.

Sistema POS

Pese a que se mantuvo reducción en el uso de sistemas de pago en puntos de ventas físicos en comparación con el año 2020; las afectaciones cibernéticas a los sistemas POS sí fueron bastante relevantes por su implicación en la seguridad de la información, a pesar de no haber recibido numerosos reportes de los asociados al respecto.



En el 2021 se conservó la tendencia a la baja de los ataques realizados por los ciberdelincuentes a los cajeros automáticos (ATM),

ATMs

En el 2021 se conservó la tendencia a la baja de los ataques realizados por los ciberdelincuentes a los cajeros automáticos (ATM), esto debido en gran parte a la actual pandemia ocasionada por el Covid-19.

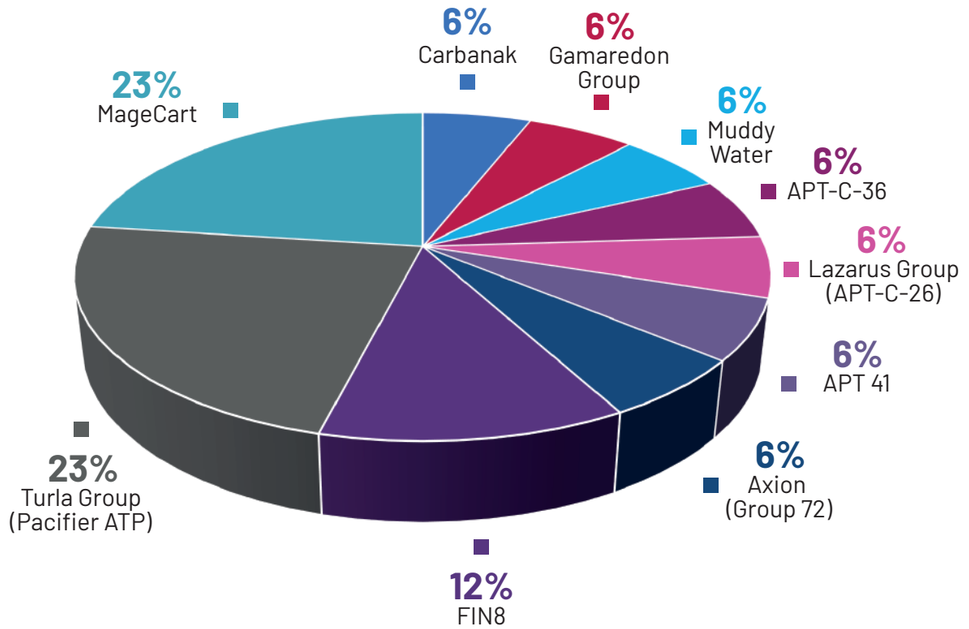
También al impulso que ha tenido la transformación digital y adopción de tecnologías inmersas que han hecho que los usuarios acudan en menor medida a los cajeros automáticos.

APTs

Las APT (Advanced Persistent Threat) siguieron en aumento, tal y como sucedió en 2020, debido al teletrabajo y el uso de soluciones VPN. Muchos de estos grupos aumentaron su actividad e internacionalizaron sus operaciones, teniendo como objetivo numerosos sectores críticos como la sanidad, el financiero, militar, telecomunicaciones, entre otros.

A continuación, se presentan las APT observadas y reportadas a nuestros asociados por el Csirt Financiero en el año 2021.

Las APT (Advanced Persistent Threat) siguieron en aumento, tal y como sucedió en 2020, debido al teletrabajo y el uso de soluciones VPN



Malware móvil

Tuvo gran movimiento generando consecuencias en el pilar de la **confidencialidad** de los usuarios de dispositivos móviles, el sistema operativo más afectado sigue siendo Android debido a que mantiene el mayor porcentaje de instalación a nivel mundial.

El Csirt Financiero comunicó 21 familias bajo la categoría malware móvil, considerando esta una cifra importante por el uso de estos dispositivos en los diferentes sectores sociales, así como el uso ilimitado e indiscriminado de las aplicaciones que soportan transacciones financieras.

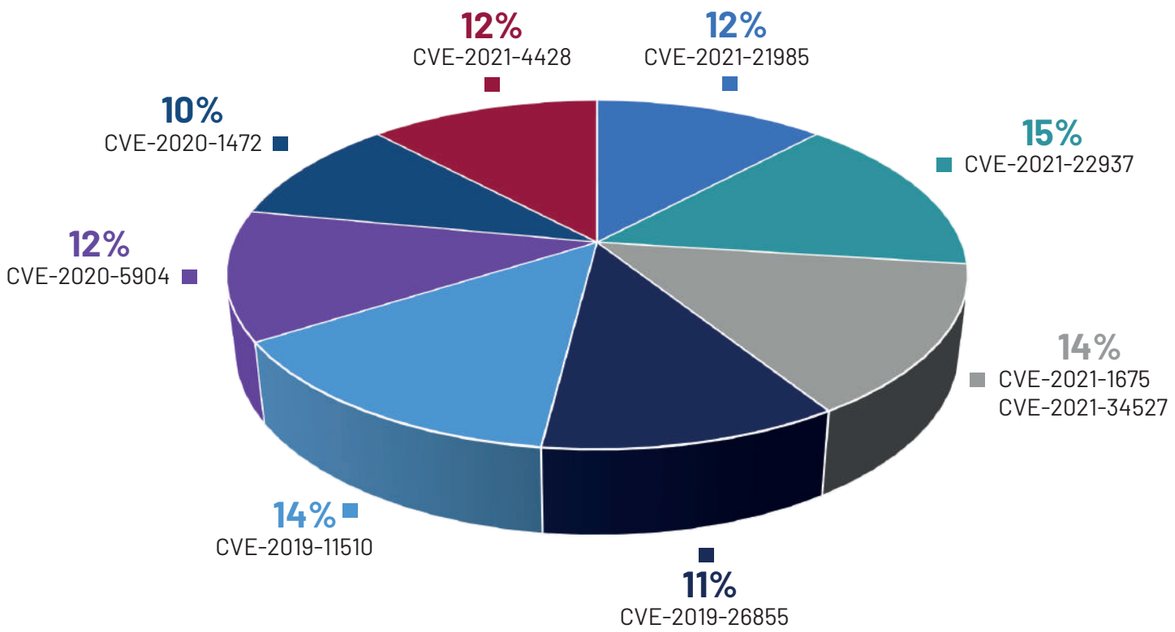
El malware móvil cada vez más suma capacidades con el fin de generar mayor impacto en los dispositivos, entre las que se destacan:

- Superposición de ventanas
- Registrar pulsaciones de teclas
- Desinstalar aplicaciones
- Realizar llamadas
- Enviar mensajes de texto
- Acceder a códigos de autenticación
- Grabar audio, vídeo y pantalla
- Controlar remotamente el dispositivo
- Restablecer el dispositivo a las características de fábrica
- Exfiltrar datos de acceso a aplicaciones bancarias
- Exfiltrar datos correspondientes a tarjetas financieras
- Elevar permisos
- Enviar información al servidor de comando y control
- Evadir detecciones de soluciones antimalware
- Ejecutar código malicioso

Nombre de malware móvil

Los malware móviles identificados se conocen bajo los nombres:

Inteligencia de amenazas



En el año 2021 se detectaron numerosas fallas de seguridad en productos ampliamente usados por las corporaciones a nivel mundial, generando aumento en los ciberataques y en los incidentes detectados.

Apoyo a incidentes

Como resultado de un trabajo colaborativo entre los asociados y el Csirt Financiero, se logró gestionar y brindar apoyo en **389 incidentes** entre los que se encontraba la verificación de campañas. Valiéndose de técnicas de phishing y spearphishing, los ciberdelincuentes **realizaban la distribución de malware para dirigir sus ataques a funcionarios de las diferentes entidades financieras.** Los ataques fueron dirigidos principalmente contra la información corporativa, siendo el principal objetivo la adquisición de bases de datos para elaborar ataques posteriores y/o para filtración con motivación lucrativa.

Es importante indicar que a través de la información compartida por los asociados se lograron identificar las diferentes amenazas cibernéticas que afectaron al sector financiero. Permitiendo así, **ampliar nuestra base de datos de muestras de malware financiero hasta 1608 muestras a día de hoy.**

Esto permitió al Csirt Financiero realizar un análisis minucioso. Gracias a esta información se logró compartir el contexto y las recomendaciones de seguridad para mitigar el riesgo específico que estaba sufriendo cada entidad. **El equipo de apoyo a incidentes acompañó en todo momento a las entidades a través del ciclo de vida del incidente**, contribuyendo así al mejoramiento del ecosistema de ciberseguridad del sector y al fortalecimiento de la comunidad de confianza.

Se logró gestionar y brindar apoyo en 389 incidentes entre los que se encontraba la verificación de campañas.

Tendencias en Ciberseguridad

Tendencias en ciberseguridad

1. Phishing valiéndose de diferentes métodos en busca de crecer con fuerza, siendo cada vez más creíbles y confiables.
2. Ransomware con enfoque orientado a objetivos puntuales, siendo cada vez más sofisticado y especializado.
3. Riesgos en la nube. La llegada del Covid-19 condujo a que las empresas aprovecharan más el uso de servicios en la nube, aumentando así la superficie de ataque.
4. Incremento de troyanos en dispositivos móviles a través de campañas acompañadas de actividades de ingeniería social, situación que va en aumento, toda vez que la banca móvil ha sido adoptada masivamente en todo el mundo, siendo un medio muy utilizado para la realización de transacciones en línea por los usuarios y empresas.
5. Uso de banca abierta - Open Banking-, servicio que hace uso de interfaces de programación de aplicaciones (API); las cuales pueden representar un vector de ataque de mayor relevancia para los cibercriminales.
6. Malware en cajeros automáticos. Con el retorno paulatino a la presencialidad es posible que se presente incremento de campañas dirigidas a los cajeros automáticos.
7. Ataques de fuerza bruta a clientes RDP. Debido a la pandemia se ha generado la publicación de equipos hacia internet, exponiendo servicios como el de escritorio remoto, lo cual es aprovechado por los cibercriminales.

Tendencias tecnológicas

1. **El Metaverso Financiero.** Aparecen nuevos ecosistemas que pueden dar a lugar a nuevos comportamientos sociales que generarán nuevas actividades que pueden ser una oportunidad para el sector Financiero. Por ejemplo, la creación de avatares dentro de este Metaverso puede llevar la identificación digital a otro nivel.
2. **Tokens no fungibles.** Desarrollados con tecnología blockchain y nacidos en el mercado del arte, ya están revolucionando sectores como el gaming o incluso el sector inmobiliario. Los nuevos usos sociales podrían llegar a extenderse a otros sectores como el financiero.
3. **Comunicaciones 5G y 6G.** Un salto en la comunicación digital, brindando una velocidad muy superior de las transacciones de datos, lo que implica la posibilidad de nuevos desarrollos y opciones a explotar para la comunicación y la prestación de los servicios entre el sector financiero y sus clientes.

ASOBANCARIA

Hernando José Gómez

Presidente

Mónica María Gómez Villafañe

Vicepresidente Administrativa y Financiera

Angela María Vaca Bernal

Directora de Programas de Innovación Gremial

Daniela Orjuela Castro

Profesional Master Dirección de Programas de Innovación Gremial

MNEMO

Equipo técnico y de operación del CSIRT

Carlos Beltrán

Director Operativo Csirt Financiero

Eva Moya

Director de Estrategia Csirt Financiero

Carlos Guzmán

Líder Técnico

Belén Viqueira

Líder Dirección Documental

Jorge Chaves

Líder Gestión

Paula Natalia Orjuela

Líder Calidad

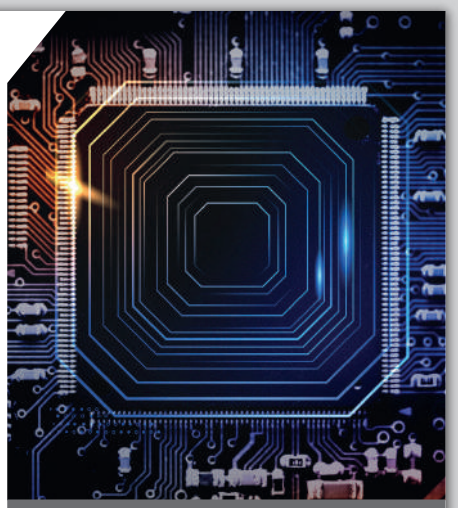
Ximena Galindo

Tendencias y Prospectiva

MOUSE GRAPHIC

Adriana Cuéllar González

Diseño y Diagramación



MEMORIA ANUAL 2021

CSIRT FINANCIERO

www.csirtasobancaria.com
csirt@asobancaria.com
incidente@csirtasobancaria.com
Tel.: +57 601 439 16 39
Cel.: +57 3174345665

@CsirtFinanciero

Aso Ban Caria