CSIRT FINANCIERO

2021

MEMORIA anual

JUNIO DE 2022

Aso Ban Caria

ÍNDICE

Índice 2

Prólogo 4

Evolución de Capacidades Técnicas 7

Resumen Ejecutivo 10

Gestión del Csirt Financiero en 2021 23

Observatorio de Ciberseguridad 23

- Troyanos bancarios 25
- RATs 27
- Ransomware 31
- SISTEMAS POS 34
- APTs 36
- ATMs 40
- Malware Móvil 41

Inteligencia de amenazas 46

- Top de vulnerabilidades con mayor implicación en actividades maliciosas Csirt 47
- Top fabricantes con mayores vulnerabilidades relacionadas 48
- Top de fabricantes con mayor número de vulnerabilidades 49

Apoyo a Incidentes 51

- Datos generales 52
- PlayBooks 54
- Informes de Amenazas 56
- Plantillas de remediación 57
- Reglas 59

Tendencias de ciberseguridad para 2022 62

Tendencias tecnológicas para el sector 2022 66

47%
MIN
MAX

PRÓLOGO

Mónica María
Gómez Villafañe

Vicepresidente
Administrativa
y Financiera de
Asobancaria

*"Con la consolidación del **CSIRT Financiero de Asobancaria**, hemos demostrado que juntos podemos hacer más; que la colaboración lleva a que el sector financiero esté mejor equipado para anticipar los crecientes riesgos cibernéticos y que ninguno de nosotros tiene toda la información, pero juntos podemos construir una imagen bastante completa de lo que están haciendo nuestros adversarios."*

1. Consolidación del CSIRT

Es un orgullo para ASOBANCARIA compartir que el Equipo de respuesta a incidentes de ciberseguridad sectorial - CSIRT Financiero- **sigue creciendo y sumando nuevos miembros**. En la actualidad, hacen parte de esta iniciativa 28 entidades financieras, el 75% corresponde a establecimientos bancarios, el 11% a sistemas de pago,7% corresponde a fondos de pensiones y fiduciarias, el restante el 7% a compañías de financiamiento.

En 2021 consolidamos la confianza entre los actores a través de un mayor nivel de intercambio y reporte de información de eventos cibernéticos locales.

En 2021 **consolidamos la confianza** entre los actores a través de un mayor nivel de intercambio y reporte de información de eventos cibernéticos locales. El **equipo de respuesta apoyó la gestión y la resolución de casi 400 eventos de seguridad** de las entidades miembro, con esta información preparó recomendaciones operativas para la detección, contención, erradicación y recuperación para el sector. A partir de dicha información, también se **desplegaron más de 250 reglas de seguridad** que permitieron integrar los eventos de mayor importancia en el sector a los Sistemas de Gestión de Eventos e Información de Seguridad -SIEM- propios de cada entidad, generando un marco de ciberdefensa colectiva.

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

(i) El uso de herramientas tecnológicas de forma conjunta entre las entidades y el CSIRT (MISP, y la integración con las plataformas propias de las entidades).

(ii) El reporte de más de 200 muestras de código malicioso para análisis de familias y su evolución.

(iii) El análisis y ejecución de ransomware, malware en la infraestructura bancaria bajo laboratorios y espacios controlados.

2. Referente internacional en colaboración

El esfuerzo de ASOBANCARIA y de las entidades financieras consolidadas en el CSIRT, nos han posicionado de referencia en la región de Latinoamérica y a nivel mundial. Durante la puesta en marcha de esta iniciativa, hemos compartido nuestra experiencia con asociaciones bancarias, asociaciones gremiales de diversos sectores y CERTs internacionales.

A nivel regional, se han generado sesiones de transferencia de conocimiento con la Federación Latinoamericana de Bancos -FELABAN-, las asociaciones bancarias de Perú, Panamá, Honduras y Bolivia. Recientemente, suscribimos **una alianza pionera** con la **Asociación de Bancos de México (ABM)** mediante la cual compartimos experiencias, iniciativas de mejora, y mejores prácticas entre las partes.

Los procesos de socialización incluyen la presentación de experiencias, el diseño de un modelo de intercambio de información, y el que consideramos uno de los factores de éxito, **lograr un compromiso constante de las entidades miembro.**

Ser parte de estas redes globales de información, permite a las entidades **acceder a las nuevas fuentes de amenazas cibernéticas de mayor cobertura en el mundo**, además de recibir alertas de forma oportuna, llevar a cabo inteligencia de

advertencias accionables y fortalecer la acción de anticipar y mitigar los riesgos de manera integral.

3. Proyección CSIRT: Riesgos Geopolíticos

Dada la confianza y credibilidad que han depositado las entidades financieras y las autoridades nacionales de Colombia en el Equipo de respuesta a incidentes de ciberseguridad, nuestra proyección a corto plazo a nivel Internacional está enfocada en obtener un **mayor conocimiento de las amenazas** que los delincuentes informáticos nos pueden hacer llegar desde cualquier parte del mundo.

Nuestro posicionamiento en el contexto político, nos hace visibles para los adversarios, todo ello, conviviendo con el ecosistema cibercriminal siempre en evolución y siempre dispuesto para monetizar cada una de sus actuaciones.

En el tablero de la geopolítica, nos encontramos a nivel mundial entre los 20 países del mundo más atacados. Una situación que debe hacernos considerar que la polarización ideológica en Latinoamérica, dentro del contexto geoestratégico actual, nos coloca ante un escenario de incertidumbre constante derivada de una realidad dinámica dominada por nuevos actores con nuevos intereses que son **capaces de explotar el ecosistema digital de forma muy intensa y creativa**, mediante técnicas híbridas.

En un escenario de mayor convergencia de los actores de los estados nación y los ciberdelincuentes, se da lugar a ataques transfronterizos más bien financiados y sofisticados donde el sistema financiero y sus proveedores son los principales objetivos. En este contexto, **el intercambio de inteligencia transfronteriza nunca ha sido más crítico para que la industria de servicios financieros se defienda de las amenazas cibernéticas**, protegiendo tanto a las empresas como a sus clientes.

Así, debemos intensificar nuestros conocimientos en las Amenazas Avanzadas Persistentes (APT), además, de mejorar el flujo de las comunicaciones entre los CSIRT para hacernos mucho más anticipativos.

Nuestro posicionamiento en el contexto político, nos hace visibles para los adversarios, todo ello, conviviendo **con el ecosistema cibercriminal siempre en evolución** y siempre dispuesto para monetizar cada una de sus actuaciones.

Desde el CSIRT seguiremos trabajando para entregar una **mirada holística sobre los adversarios**, que integra varios puntos de vista, tanto nacionales como internacionales buscando resolver con éxito las amenazas que se presenten en nuestro sistema financiero.

EVOLUCIÓN DE CAPACIDADES TÉCNICAS

Carlos Javier
Beltrán Camacho

Director Operativo
Csirt Financiero

En un mundo interconectado y operable las 24 horas del día, donde los seres humanos se han visto obligados a **migrar de una era física a una digital** por cuenta de una pandemia que no da tregua, se evidencian una serie de retos para mitigar todas aquellas **amenazas cibernéticas que se ciernen sobre el espacio** y que de una u otra manera afectan la tranquilidad de estos. Los ciberdelincuentes han visto una **ventana de oportunidad para lanzar sus ataques de forma malintencionada** y sin escrúpulos, sin pensar en lo más mínimo en el bienestar de los demás sino en el mismo propio, solo en busca de generar una ganancia criminal que llene sus bolsillos de un forma fácil y desde la comodidad que les ofrece un anonimato y una conexión a internet.

Vale la pena retomar aquellas palabras del profesor estadounidense de informática y destacado experto en seguridad informática, Gene Spafford, "**el único sistema completamente seguro es aquel que está apagado, encerrado en un bloque de cemento y sellado en una habitación rodeada de alambradas y guardias armados**".

De acuerdo con Gene Spafford, **no hay sistemas informáticos seguros que garanticen a los seres humanos que no van a sufrir un ataque informático**, por esto es importante llevar a cabo una verdadera concientización a todos los usuarios, lo que les va a permitir adquirir los conocimientos necesarios para poder contrarrestar las amenazas que a diario buscan romper el eslabón más débil de la cadena.

Al mismo tiempo, se evidencia el uso de diferentes técnicas como la ingeniería social, la cual es utilizada a través de diferentes campañas enviadas por correo electrónico, en las que se busca generar en los usuarios la necesidad de abrir archivos adjuntos o navegar sobre links inmersos dentro de estos, para posteriormente poder acceder a información privilegiada, entre otros.

Cabe destacar, que las amenazas cibernéticas día tras día vienen creciendo de forma exponencial, es por ello que **se observa una gran cantidad de afectaciones a personas y empresas**, en la que mencionada afectación ha causado pérdidas millonarias y reputacionales, que en la gran mayoría de casos ha dejado por varias semanas los servicios indisponibles. **Los ciberdelincuentes han desarrollado un nuevo mercado de ciberextorsión** y han abierto una gran puerta para la comercialización de artefactos que les permiten generar de forma rápida y sencilla ganancias, ya que estos grupos cibercriminales al conocer que el negocio es rentable, están perfilando a sus posibles víctimas, es decir **están realizando verificaciones y un análisis detallado** de cuáles podrían ser aquellas que de acuerdo a su nivel de popularidad y su nivel de ingresos pueden llegar a afectar, de forma tal que consigan exigir un pago por la devolución de la información que han logrado comprometer.

Por otra parte, en la evolución constante de las amenazas cibernéticas, se observa una **creciente predominancia por el uso de ransomware** como herramienta facilitadora para generar caos y desestabilizar una organización. El sólo hecho de cifrar los datos pueden llegar a exigir considerables sumas de dinero por la recuperación de la misma, lo que ha llevado a que cada vez estos **artefactos maliciosos sean más sofisticados y comercializados en el lado oscuro de la red**, en donde grupos cibercriminales se dedican a perfeccionar, automatizar y endurecer su funcionamiento, con el fin de generar mayor impacto en los ataques generados. Cada vez es más difícil su detección, pues se ha evidenciado que esta amenaza en particular viene afectando a muchos sectores no solo de la geografía global sino local, donde se busca generar el mayor daño posible, con **afectación a la disponibilidad de la información y afectación a la disponibilidad de los servicios**, como por ejemplo ataques dirigidos a escuelas, universidades, hospitales, centros de abastecimiento, plantas de tratamiento de agua, entre otros.

"El único sistema completamente seguro es aquel que está apagado, encerrado en un bloque de cemento y sellado en una habitación rodeada de alambradas y guardias armados".

Gene Spafford

Es necesario destacar, que para hacer frente a las amenazas cibernéticas se hace necesario seguir **fortaleciendo la comunidad de confianza**, donde las entidades financieras compartan la información sobre las campañas maliciosas que puedan llegar a afectar sus diferentes plataformas tecnológicas. A través de esta información, desde el Csirt Financiero, se podrá **realizar un análisis detallado y prospectivo**, que permita compartir información operable del comportamiento de una amenaza cibernética y con ello **fortalecer el ecosistema de ciberseguridad del sector financiero**, es por eso que este tipo de iniciativas debe ser constante y cada vez más creciente, con el fin de obtener la mayor información posible que permita generar entregables de valor y así asegurar una verdadera confianza digital del sector.

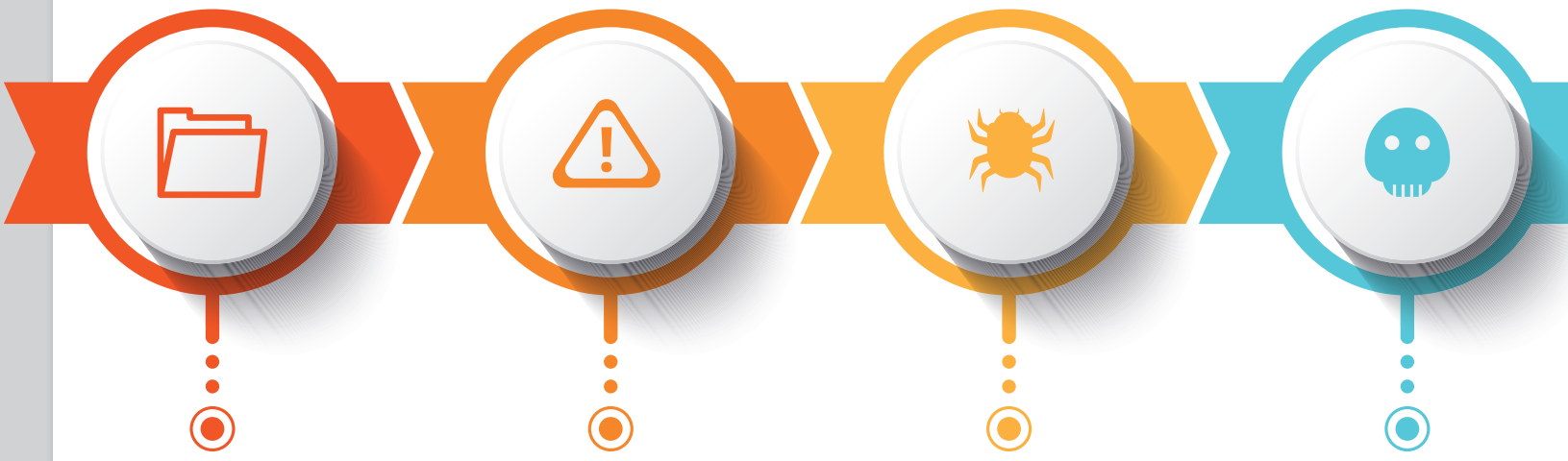
Por último, invitamos a todos nuestros asociados a ver en **el Csirt Financiero un aliado estratégico**, un amigo en el camino, un equipo de trabajo con grandes capacidades que está a su entera disposición para acompañarlos en los **retos que nos plantea a diario la ciberseguridad**, un equipo que crece, evoluciona, se fortalece con sus recomendaciones y está a la vanguardia de las amenazas emergentes y disruptivas que se presentan en el ciberespacio. Amenazas que de **forma directa o indirecta buscan generar el mayor daño posible**, pero que a través de la colaboración mutua y del fortalecimiento de capacidades podemos hacerles frente y con ello mitigar el impacto de forma favorable para todos.

RESUMEN EJECUTIVO

A lo largo de 2021 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.

Es importante 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 dirigidas al sector financiero global, con el objetivo de brindar una comprensión detallada de estas, así como una férrea defensa que permitiera evitar diversas categorías de incidentes de seguridad en las entidades del sector financiero.

De esta forma, a lo largo del año 2021 el Csirt Financiero realizó las siguientes actividades, las cuales puso a disposición de los asociados, así:



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

Distribuidas entre 4 Playbooks y 10 planillas de remediación.

Existen muchas ciberamenazas que tuvieron lugar en el año 2021, si bien es cierto que algunas de ellas son destacables y han podido ser analizadas por el Csirt Financiero como una ciberamenaza recurrente contra el sector financiero de Colombia. Estas ciberamenazas han sido tratadas e informadas a través de alertas, boletines, informes o monográficos, los cuales se recogen a continuación:

- Sofisticación e incremento de campañas relacionadas con troyanos bancarios, los cuales han desarrollado nuevos módulos que permiten generar un mayor impacto en la víctima.

- Incremento en la distribución de malware de tipo ransomware a través de diferentes campañas, por medio de las cuales buscan persuadir a las víctimas para que descarguen archivos adjuntos, y con ello se genere la infección del equipo de cómputo.

- Aumento en las campañas dirigidas al sector financiero empleando troyanos de acceso remoto como: AsyncRAT, BitRAT y LimeRAT; utilizando como vector de distribución correos electrónicos tipo phishing. Adicionalmente incluyen asuntos llamativos con la intención de generar la necesidad de visualizarlos y de esta forma realizar la descarga de archivos adjuntos.

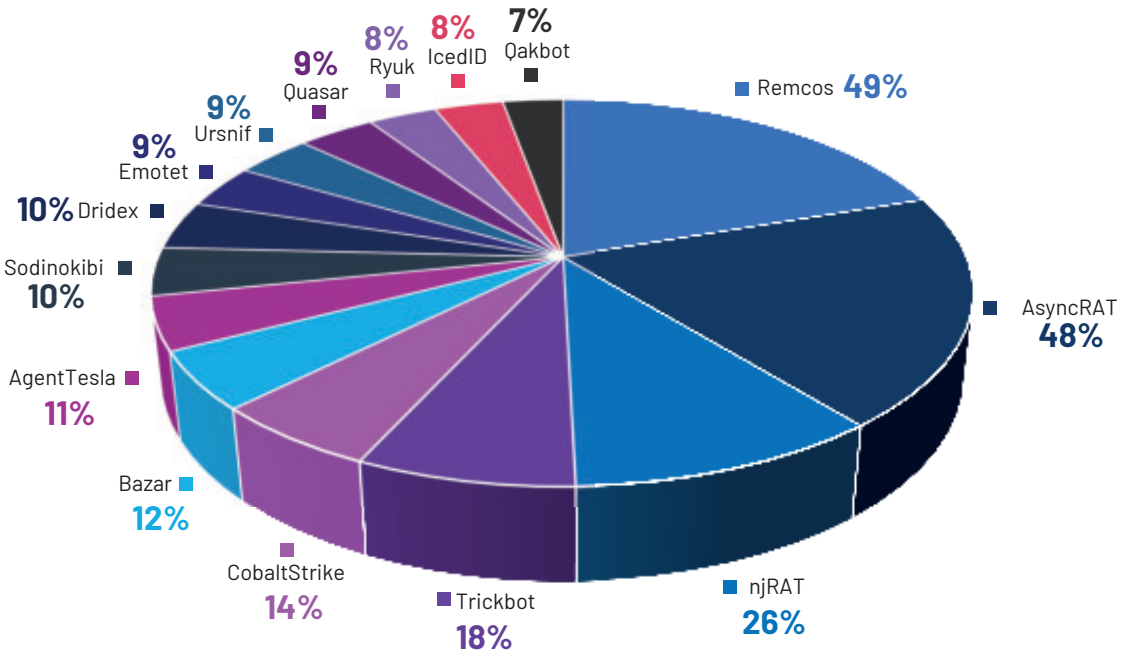
- Incremento en el desarrollo de malware para dispositivos móviles, diseñados para la captura de información bancaria. Estos artefactos maliciosos son capaces de generar superposición de pantallas de aplicaciones financieras, evadir los diferentes controles que ofrece una solución antivirus, exfiltración de información, entre otros.

La distribución de diferentes familias de malware se ha incrementado debido al uso constante de campañas de phishing y spearphishing que los cibercriminales utilizan para alcanzar sus objetivos. Los cuales buscan afectar a sus víctimas mediante técnicas de ingeniería social, buscando comprometer información.

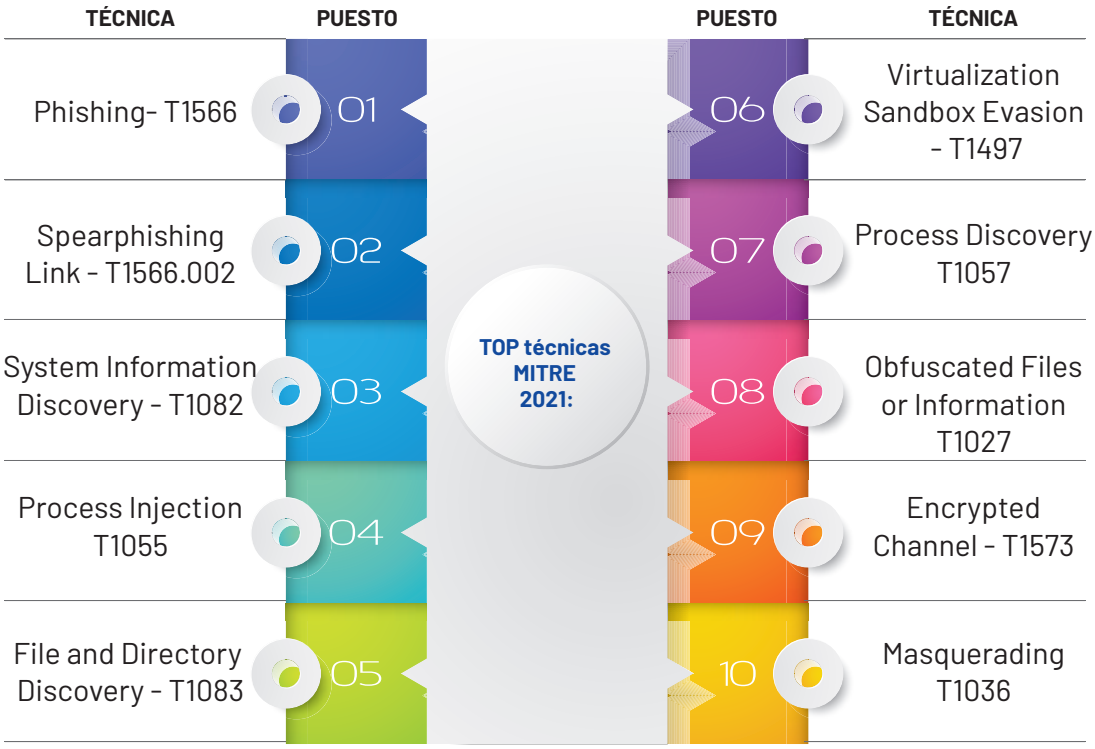
En este sentido las principales familias de malware que el equipo de analistas del Csirt Financiero ha identificado y analizado son las siguientes:

Existen muchas ciberamenazas que tuvieron lugar en el año 2021, si bien es cierto que algunas de ellas son destacables y han podido ser analizadas por el Csirt Financiero como una ciberamenaza recurrente contra el sector financiero de Colombia.

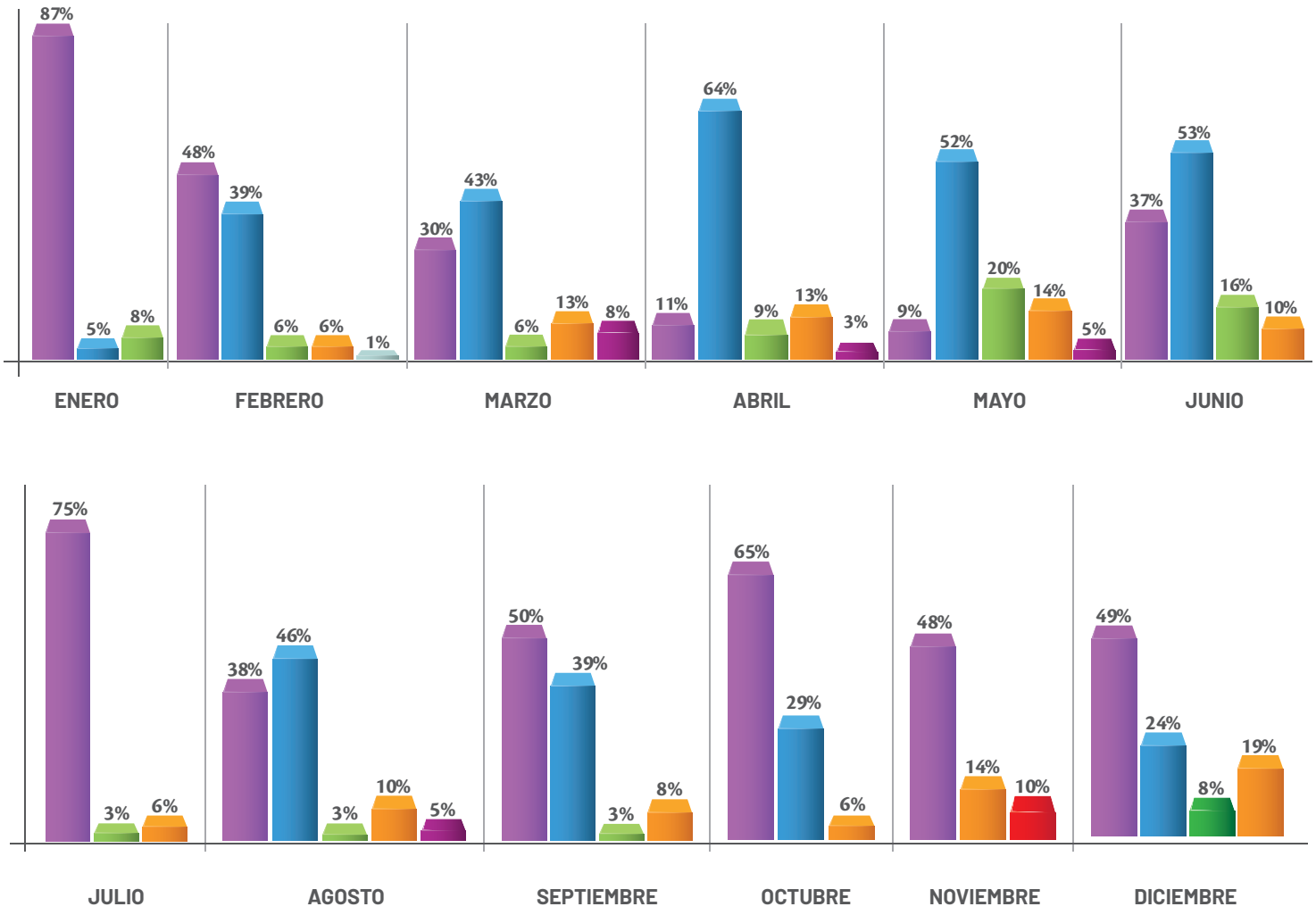
Principales familias de malware analizadas



Por último, el siguiente gráfico presenta las 10 TTP (Técnicas, Tácticas y Procedimientos) más relevantes para el sector financiero basadas en la matriz MITRE ATT&CK, de acuerdo con el análisis realizado por el equipo del Csirt Financiero desde el inicio del año 2021. Tener el conocimiento sobre aquellas técnicas más utilizadas por los grupos cibercriminales en el sector financiero, ayuda a los equipos tácticos y operativos de ciberseguridad a priorizar los mecanismos de detección y mitigación sobre aquellas que resultan más comunes.



Top Amenazas por Mes



Convenciones

- Malware Bancario
- Vulnerabilidades
- Leaks
- Ciberfraude
- Ataques POS
- Suplantación
- Aplicaciones Suplantadas
- Ataque ATM

2021, el año de la reactivación económica

Sin lugar a duda el año 2021 acarreó para el mundo grandes cambios, como lo fue la reactivación económica de los diferentes sectores de la economía global. A su vez trajo consigo grandes desafíos que pusieron en jaque a muchas organizaciones, pues era inevitable pensar cuál sería la mejor opción para regresar a sus sitios de trabajo. Validar el costo beneficio de esto y los grandes retos que traería esta nueva migración a una realidad marcada por aspectos de relacionamiento y acercamiento con compañeros de trabajo y a habituarse nuevamente a jornadas laborales en sus oficinas, transporte público, restaurantes, centros comerciales, entre otros.

Lo anterior hizo pensar en que volver a trabajar desde la oficina traía consigo desafíos importantes para los departamentos de tecnologías de la información, pues se debía contar **con un plan estratégico que permitiera a los empleados volver a entender la importancia de la implementación de controles de seguridad informática y la sensibilización frente a los temas relacionados con la seguridad de la información.**

Los usuarios venían de un ambiente familiar donde poco o nada se había pensado en factores de riesgo que afectaban a la seguridad; por el contrario, era una época netamente basada en la productividad basada en la conectividad remota desde casa.

Volver a los entornos empresariales trajo consigo grandes brechas de seguridad, pues se debía realizar una concientización y un adecuado manejo de la higiene informática, así como empezar a trabajar sobre aquellas conductas o costumbres que se adquirieron durante el confinamiento ocasionado por la pandemia del COVID-19. Las personas habían olvidado cómo se trabajaba con estándares y políticas de seguridad que permitían preservar la integridad, confidencialidad y disponibilidad de la información.

De acuerdo con lo anterior, los grupos de tecnologías de la información de las diferentes empresas tuvieron que retomar todas las medidas de protección de sus infraestructuras y empezar a generar nuevamente cultura de seguridad de la información y la protección de esta, ya que **este regreso representó una verdadera brecha de seguridad que pudo ser explotada utilizando técnicas de phishing y spearphishing** valiéndose de la ingeniería social.

El año 2021 acarreó para el mundo grandes cambios, como lo fue la reactivación económica de los diferentes sectores de la economía global.

Por tal razón, el papel que juega una adecuada concientización en los usuarios es verdaderamente fundamental, pues son ellos quienes están llamados a advertir sobre las diferentes ciberamenazas que viajan constantemente a través del ciberespacio.

Por otra parte, es importante indicar que a través del proceso de reactivación económica vivido en Colombia se incrementó el uso de plataformas de pago online, que permitieron a los usuarios hacer sus transacciones de una forma más ágil y sin realizar largas filas. Así mismo, este fue un espacio aprovechado por los ciberdelincuentes para explotar las brechas de seguridad asociadas a estas tecnologías; razón por la cual en Colombia se observó un incremento radical en las conductas delictivas derivadas de la suplantación de portales transaccionales, a los cuales accedían a diario miles de usuarios de la banca.

Por último, desde el Csirt Financiero, a través del monitoreo diario a las diferentes fuentes de información, se evidenció el comportamiento que han tenido las amenazas cibernéticas, las cuales fueron desarrolladas y ajustadas para afectar directamente a la banca y en especial la banca online.

La banca online enfrenta diferentes tipos de amenazas cibernéticas y en especial los troyanos bancarios, los cuales vienen en constante evolución y perfeccionamiento de sus técnicas, tácticas y procedimientos, además de ser comercializados en el lado oscuro de internet, donde son ofrecidos por una cantidad de dinero y a través del cual ofrecen todo un arsenal con sus respectivas instrucciones de uso.

TIPOS DE ATAQUES (BEC) DURANTE LA REACTIVACIÓN ECONÓMICA 2021

Phishing y Spearphishing

El phishing es sin duda la forma más común de utilizar la ingeniería social y está extendida entre los cibercriminales. Mediante la redacción y envío de mensajes de correo electrónico, destinado a una o varias personas o potenciales víctimas, generalmente realizando una suplantación de identidad y por su parte el spearphishing es un tipo de phishing dirigido, específicamente, a una persona u organización.

Spoofing

La suplantación realizada por parte de los ciberdelincuentes se basa en una serie de técnicas y actividades con las cuales se busca asumir la identidad tanto de personas como de recursos tecnológicos de alguna entidad en pro de lograr un objetivo específico.

Baiting

También llamado cebo, soportado en la mínima interacción con la víctima, el cual aprovecha el sentimiento de curiosidad. Su característica principal es el uso de dispositivos como: USBs, CDs o MP3s expuestos en lugares con bastante actividad o puntos de reunión.

Business Email Compromise o Fraude al CEO

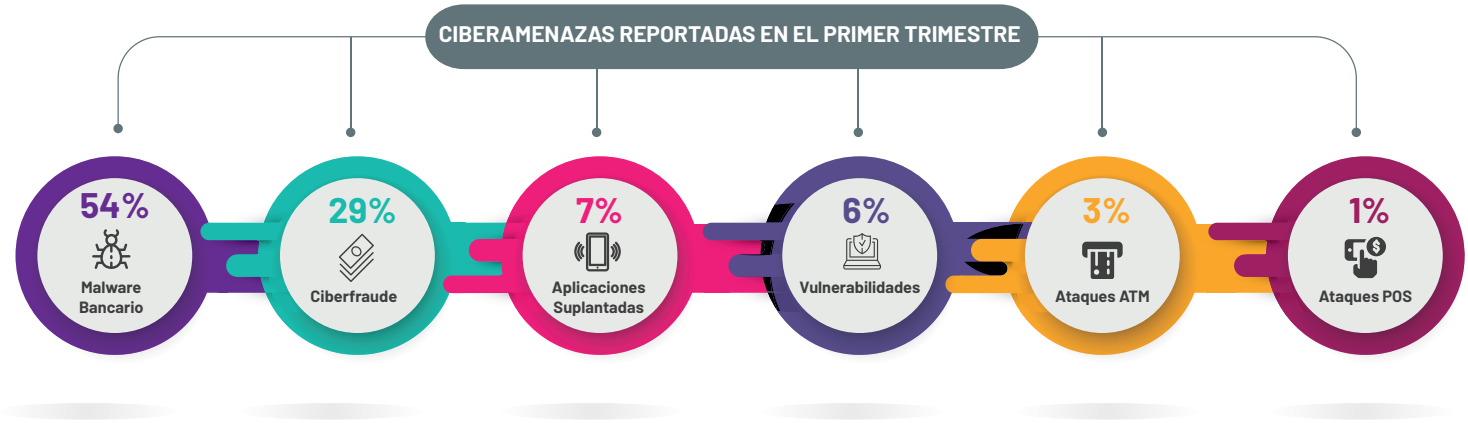
Es un tipo de phishing basado en la ingeniería social que tiene por objetivo empleados con capacidad de decisión dentro de la empresa y que, por lo general, tienen potestad para realizar transacciones financieras y transferencias bancarias.

Smishing

Comunicados a través de mensajes de texto SMS. Es un tipo de phishing que busca aprovechar el uso de dispositivos como tabletas, móviles o relojes inteligentes. Ayudándose de la ingeniería social, se incluye en el mensaje un enlace que redirecciona a la víctima al sitio donde el cibercriminal necesite para alcanzar su objetivo.

Vishing

Este vector de ataque, al igual que el smishing, es una forma de phishing, pero en esta oportunidad la vía de propagación son las llamadas telefónicas. El engaño requiere ser preparado con antelación, ya que el cibercriminal tiene contacto directo con la víctima y su coartada debe ser convincente para no ser descubierto.



En el primer trimestre de 2021 el Csirt Financiero observó que el malware bancario y el ciberfraude siguen siendo las dos principales ciberamenazas más utilizadas por los grupos cibercriminales para tratar de afectar al sector financiero. Esta tendencia es dada por el nivel de maduración que ha tenido el malware como servicio MaaS (Malware-as-a-Service), ya que los operadores mejoran constantemente el código malicioso y su propia infraestructura de comando y control (C2) para obtener mejores ganancias; por ejemplo, el ransomware con su modalidad de exfiltración de información para luego extorsionar a la víctima si no accede a realizar el pago.

El ciberfraude se ve representado en la obtención de credenciales de portales financieros y de información asociada a tarjetas de crédito. Lo anterior a través de troyanos bancarios diseñados para afectar a sistemas operativos Linux y Android y de skimmer dirigidos a portales transaccionales.

En el segundo trimestre de 2021 el Csirt Financiero observó que el fraude cibernético y el malware bancario continuaron siendo las dos principales ciberamenazas con eventos o repercusión negativa sobre el sector. Esta tendencia está marcada principalmente por el CaaS (Crime-as-a-Service), cuyo modelo de operación y monetización incentiva a cibercriminales a desarrollar y ofertar diversos recursos tecnológicos para que se cometa fraude financiero u otro tipo de afectación en contra de la confidencialidad, integridad o disponibilidad de la información.

Debido a esto, es inminente que se formulen estrategias de prevención asociadas a la vigilancia del entorno digital para identificar y gestionar los riesgos de exposición en el ecosistema cibernético de forma anticipada.

En el tercer trimestre de 2021 el Csirt Financiero observó que el Fraude Cibernético y el Malware Bancario, continuaron siendo las principales ciberamenazas con eventos o repercusión negativa sobre el sector. Esta tendencia se encuentra enmarcada por predominancia de modelos de operación y monetización, como son el CaaS y el MaaS, los cuales incentivan a los cibercriminales a desarrollar y ofertar diversos recursos tecnológicos para que se cometa fraude financiero, estafas u otro tipo de afectación en contra de la seguridad de la información. Por eso se sugirió de manera permanente, la formulación de campañas de prevención relacionadas con el cuidado del entorno digital para la correspondiente gestión oportuna de riesgos, en los cuales se evidencia la exposición de las infraestructuras tecnológicas de los asociados de manera anticipada.

En el cuarto trimestre de 2021 el Csirt Financiero observó que el malware bancario y el fraude cibernético continuaron siendo las dos ciberamenazas que más impactaron de forma negativa al sector.

Esta tendencia se encuentra marcada por el continuo desarrollo del Malware como Servicio MaaS (Malware-as-a-Service) para la venta clandestina de código malicioso, con el objetivo de cometer fraudes, estafas u otras afectaciones en contra de la seguridad de la información respaldado con técnicas de phishing y spearphishing para la distribución de estos malware.

A lo largo del trimestre, también se dieron a conocer varias vulnerabilidades 0 day con niveles de criticidad altos que afectaron a múltiples fabricantes de aplicaciones corporativas, como la vulnerabilidad identificada como CVE 2021 44228 (Log4Shell) que fue utilizada por los ciberdelincuentes para propagar diferentes tipologías de malware como ransomware o troyanos que permitían escalar privilegios.

Igualmente, se observó un incremento en aplicaciones móviles maliciosas que eran distribuidas en tiendas no oficiales y que suplantaron a entidades financieras.

Además, se evidenció que, en diferentes redes sociales, se ofrecían números de tarjetas de crédito de diferentes entidades financieras para ser utilizadas en la compra de servicios de streaming.

Se observó un incremento en aplicaciones móviles maliciosas que eran distribuidas en tiendas no oficiales y que suplantaron a entidades financieras.

¿Qué nos depara el 2022 en relación con la reactivación económica?

1. Las plataformas de videocomunicación seguirán siendo objetivo de ciberataques debido a la continuación del teletrabajo en modo alternancia, mientras se decrete algo diferente frente al manejo de la pandemia del COVID-19. Se seguirán registrando dominios maliciosos que suplanten a plataformas de este tipo, como Zoom o Microsoft Team, para distribuir todo tipo de malware. Lo mismo ocurrirá con la tecnología de acceso remoto, RDP y VPN.

2. Seguiremos viendo la evolución y sofisticación del malware para efectuar ataques sobre diferentes plataformas tecnológicas y así mismo la afectación de los diferentes sistemas operativos, aprovechando las múltiples vulnerabilidades que se presentan en estos. Se evidenciará aún más la comercialización de estos artefactos en la deep y dark web, donde pandillas de cibercriminales realizarán su arribo para comprar estos productos y lanzar nuevos y mejorados ataques cibernéticos contra diferentes sectores de la economía.

3. Los ataques a la cadena de suministros jugarán un papel fundamental en el ecosistema de la ciberseguridad, ya que los grupos cibercriminales, a través de los diferentes ataques que han lanzado, son conscientes de los puntos de entrada para afectar a muchas organizaciones con un solo ataque y con esto poder obtener el mayor provecho posible, tanto a nivel de fama como a nivel monetario.

4. La proliferación y evolución del ransomware va a ser mucho más amplia y detallada, toda vez que los grupos cibercriminales, día tras día, van generando nuevos cambios en sus productos. Han obtenido la experiencia necesaria que les permite generar cambios significativos, que a su vez les brinda la posibilidad de atacar de forma infalible estructuras tecnológicas. Las cuales previamente han sido seleccionadas como objetivo, ya sea por su volumen o por el poco grado de conciencia en temas de seguridad de la información y porque son organizaciones a las cuales pueden exigir grandes sumas de dinero a cambio de devolver la información afectada.

5. En cuanto al phishing y el spearphishing se denotará un volumen de crecimiento exponencial, toda vez que es uno de los vectores de ataque más comúnmente utilizados y de gran efectividad, ya que a través de estos podrán llegar a muchos objetivos buscando romper el eslabón más débil de la cadena de ciberseguridad.

6. La utilización de fake news jugará un papel de suma relevancia en la ciberseguridad de las entidades, ya que grupos cibercriminales inundarán las redes sociales de información falsa valiéndose de acontecimientos de repercusión nacional o internacional, a través de las cuales buscarán generar pánico en los usuarios de los diferentes mercados de la economía.

7. Por último y no menos importante seguiremos viendo como la explotación de vulnerabilidades en las diferentes plataformas tecnológicas de las entidades seguirán siendo blanco de acción de grupos cibercriminales. A través de estas buscarán realizar el aprovechamiento de brechas de seguridad que les permitan generar la entrada y con esto poder llegar a afectar la integridad, confidencialidad y disponibilidad de la información.

GESTIÓN DEL CSIRT FINANCIERO EN 2021

Observatorio de Ciberseguridad

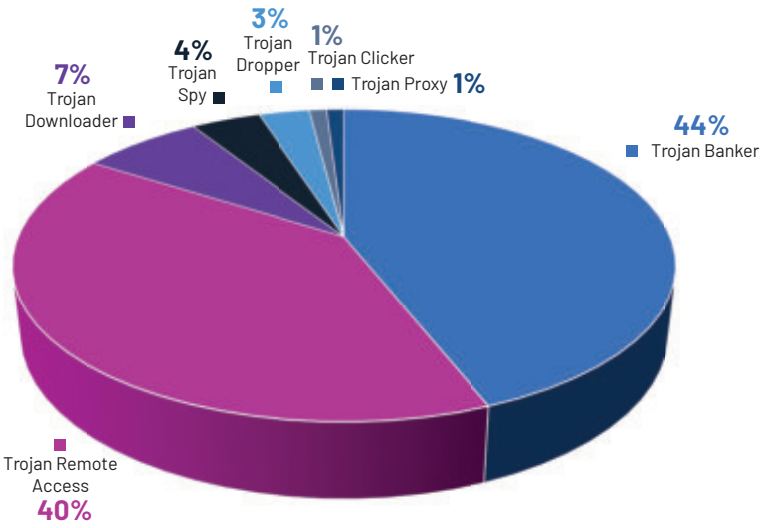
Esta capacidad acoge en gran medida los documentos generados a partir del descubrimiento, seguimiento, monitoreo y análisis a las ciberamenazas que causan afectación, en alguna medida, al sector financiero Colombiano.

En el **2021** se compartieron **711 documentos** bajo la capacidad del **observatorio de ciberseguridad.** En ellos se relaciona información de tipos de **ciberamenazas** como **troyanos** y sus subtipos, **ransomwares, malware móvil, grupos cibercriminales (APT)** y aquellas dirigidas a **ATM.**

Troyanos

Este tipo de malware que ha generado innumerables afectaciones a la seguridad de la información y a la ciberseguridad a nivel global, ha conseguido ampliar sus capacidades y clasificación en diferentes tipos. A continuación, se muestran los tipos de troyanos más utilizados y el porcentaje de reporte realizado por el Csirt Financiero:

TOP TROYANOS BANCARIOS MÁS DIFUNDIDOS



Trojan Remote Access

Controlan un sistema a través de una conexión de red remota.

Trojan Banker

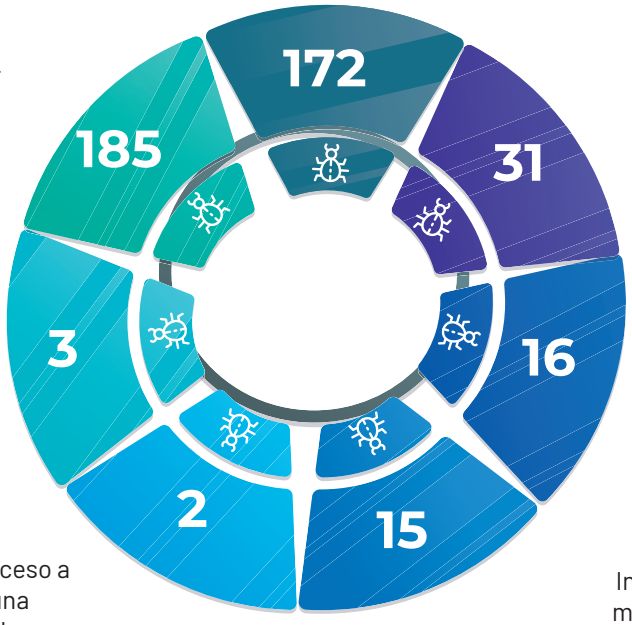
Su objetivo es obtener las credenciales de acceso a las cuentas bancarias.

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.

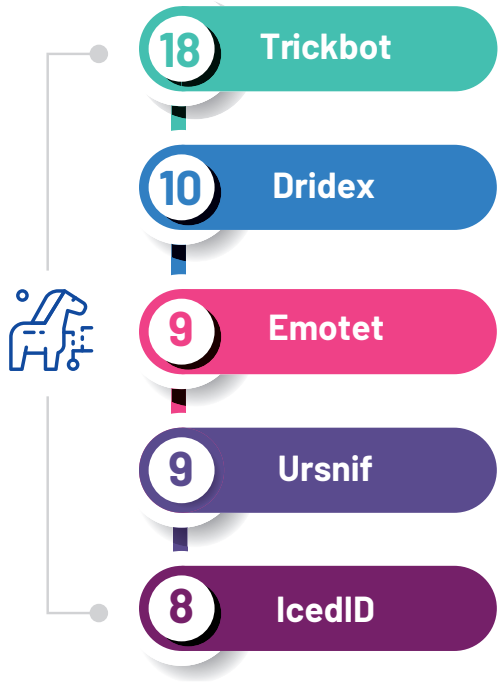
Troyanos bancarios

Con 185 reportes relacionados a troyanos bancarios, el Csirt Financiero consolida en el 2021 este tipo de amenaza como una de las más relevantes, tanto por su amplia distribución, como por su afectación directa al sector.

La amplia difusión de plataformas que corresponden y apoyan la operación de banca en línea se convierte en un foco para los ciberdelincuentes, quienes buscan por medio de diversos métodos adentrarse en los equipos de los usuarios para obtener información que pueda ayudar a generar de alguna manera un beneficio económico.

Los troyanos bancarios que tuvieron lugar en campañas a lo largo de 2021 son conocidos desde hace varios años. Estos han sufrido cambios en sus características y capacidades; sin embargo, han mantenido su estructura y objetivo de funcionamiento. Las 22 familias analizadas por el equipo del Csirt Financiero fueron las siguientes:

De los troyanos bancarios reportados por el Csirt Financiero, los que mayor implicación tuvieron en cibercampañas maliciosas son los siguientes:



El troyano modular Trickbot mantiene su posición siendo el de mayor distribución a nivel global en esta categoría. Entre sus módulos se han implementado técnicas que permiten escaneo de puertos, inyección web, inyección de código, desviar el tráfico, obtener información del controlador de dominio, cookies, logins, contraseñas y otras capacidades destacables que evidencian su amplio uso por importantes grupos APT.

Dridex, conocido en el 2011, ha sido de esos troyanos que han evolucionado a través de múltiples actualizaciones en pro de implementar capacidades que intensifican su actividad maliciosa, entre ellas evadir algunas herramientas de seguridad y funciones adicionales que le permiten agregar los equipos comprometidos a una botnet.

El método de distribución más común de los troyanos bancarios en el 2021 fue por medio de correos malspam (malware en spam), utilizando temas que generan gran interés en los usuarios; por ejemplo, suplantando correos de Netflix asociados a la tendencia vista con la serie del juego del calamar. También es relevante el envío de correos tipo phishing a nombre de sistemas como quickbooks u organizaciones reconocidas en el país como la DIAN, donde se adjunta un archivo que contiene la DLL o carga útil con la ciberamenaza.

El método de distribución más común de los troyanos bancarios en el 2021, fue por medio de correos malspam (malware en spam)

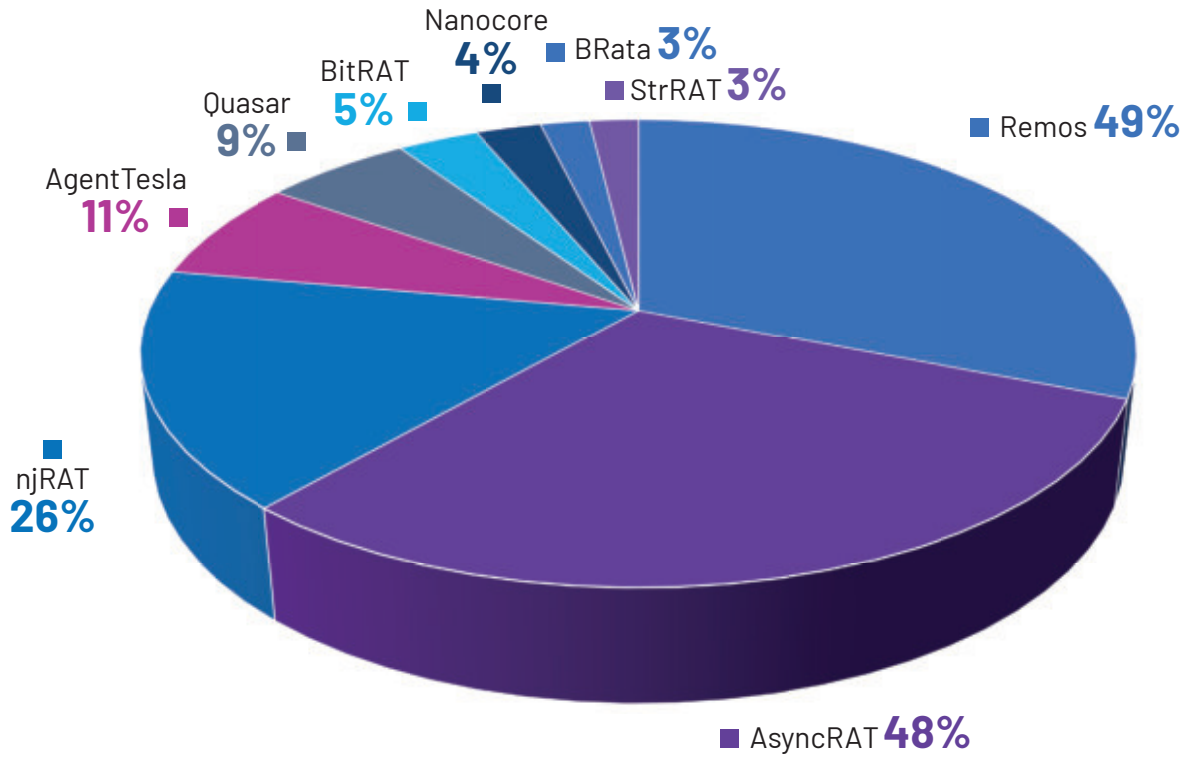
RATs

El tipo de malware que enmarca los troyanos de acceso remoto (RAT) refiere a herramientas utilizadas para controlar de manera remota un equipo o dispositivo. Una gran cantidad de estas herramientas son legítimas; sin embargo, son manipuladas de tal manera que los ciberdelincuentes logran otorgar características malintencionadas que usan para obtener o realizar ataques cibernéticos sofisticados con grandes afectaciones, a continuación, se presentan algunas de estas capacidades:

En la memoria anual del 2020, se planteó una tendencia al alza en el uso de los troyanos de acceso remoto, comprobándose en el transcurso del 2021 que estos fueron comunes a la hora de realizar actividades malintencionadas por parte de los actores maliciosos.

El Csirt Financiero durante el año 2021 reportó 25 familias de RATs, algunas de ellas implicadas en campañas directamente dirigidas a los asociados. A continuación, se muestra el top de las familias de RATs más represantivos:

PRINCIPALES FAMILIAS DE RAT REPORTADAS 2021



RemcosRAT, AsyncRAT y njRAT manteniéndose en el top

En el 2021 la mayor cantidad de campañas de distribución de troyanos de acceso remoto se relacionan a RemcosRAT, AsyncRAT y njRAT. Al igual que el año pasado, encabezan la lista en lo que respecta al conjunto de este tipo de malware.

Desde enero del 2021 se reportó la distribución de estos tres troyanos al mismo tiempo. En algunas ocasiones las campañas fueron amplias y pretendían infectar a varias organizaciones colombianas; una de estas campañas se nombró **Operación Spalax.**

RemcosRAT, AsyncRAT y njRAT como troyanos de acceso remoto han sido constantemente distribuidos en campañas dirigidas al sector financiero, educativo y gubernamental de Colombia. Los ciberdelincuentes que operan estas familias de malware generan actividad dirigida, buscando afectar infraestructuras de entidades reconocidas.

BitRAT con rápida propagación

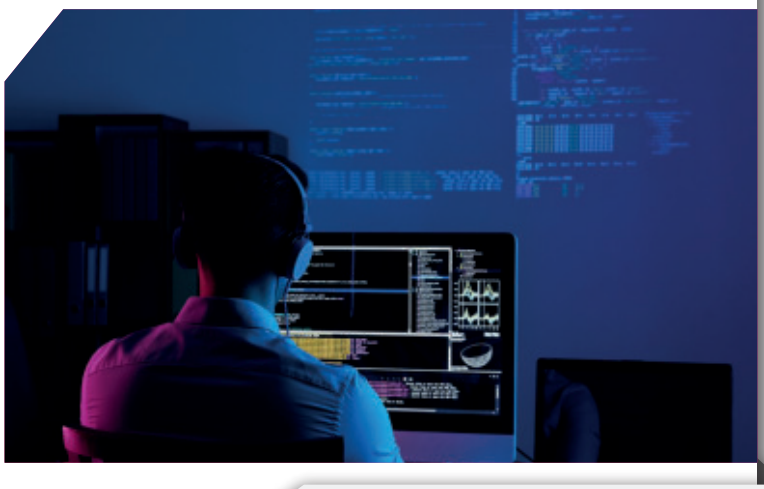
Desde abril del 2021 se analizaron muestras de este troyano y se recibieron reportes de campañas a nivel financiero nacional. Aunque este troyano de acceso remoto se conoció en noviembre del 2020, expandió su actividad maliciosa rápidamente, consolidándose en el top 10 de los RATs presentados por el Csirt Financiero en el 2021.

Los vectores utilizados para difundir los troyanos de acceso remoto son varios, entre ellos se pueden destacar:

- **Phishing,** con los componentes de ingeniería social para entregar la carga útil electrónicamente. Los ciberdelincuentes realizan el envío masivo de correos intentando que alguno de los usuarios que lo recibió dé un paso inicial para poner en marcha el RAT.

- **Spearphishing,** en sus variaciones de link y attachment, los ciberdelincuentes evalúan sus posibles víctimas y generan plantillas específicas de los correos para que se proceda a la descarga o visita del sitio web.

Muchos de los análisis realizados determinaron que ejecutables de troyanos RAT son desarrollados en el lenguaje de programación .NET y aprovechan entre las características de funcionamiento el uso de **LOLBAS**, un conjunto de binarios y scripts que, aunque son propios del sistema, es decir legítimos, son de común uso en la ejecución de este tipo de malware. Se muestra a continuación el top de binarios identificados en las muestras de troyanos de acceso remoto analizadas en el 2021 por el Csirt Financiero.



Binario	Función	TTP
Regsvcs	AWL bypass - Execute	T1218.009 Regsvcs/Regasm
Rundll32.exe	Execute - Alternate data Streams	T1218.011 Rundll32 T1564.004 NTFS File Attributes
Schtasks.exe	Execute	T1053.005 Scheduled Task
Wmic.exe	Execute - Alternate data Streams	T1564.004 NTFS File Attributes T1218 Signed Binary Proxy Execution
Wscript.exe	Alternate data streams	T1564.004 NTFS File Attributes
Cmd.exe	Alternate data streams	T1564.004 NTFS File Attributes
Installutil.exe	AWL bypass - Execute	T1218.004 InstallUtil
Msbuild.exe	AWL bypass - Execute	T1127.001 MSBuild

LOLBAS, un conjunto de binarios y scripts que, aunque son propios del sistema, es decir legítimos, son de común uso en la ejecución de este tipo de malware.

Ransomware

CANTIDAD DE FAMILIAS
ENERO
3
Avaddon, Babuk Locker, REvil
Egregor, Ryuk, Vovalex, Zeoticus
4
FEBRERO
MARZO
8
AlumniLocker, Avaddon, DearCry, Defray777, Hades, HelloKitty, Pysa, REvil
Avaddon, Cuba, Darkside, Fair/Phobos, REvil, Ryuk
6
ABRIL
MAYO
5
Avaddon, Darkside, GangBang, MountLocker, Zeppelin
Black Kingdom, BlackCocaine, DarkRadiation, Djvu, Epsilonred, FiveHands, Hive, Prometeus, REvil
9
JUNIO
JULIO
7
AvosLocker, Conti, Diavol, HelloKitty, Pysa, REvil, Ryuk
AvosLocker, BlackMatter, Chaos, Conti, DeepBlueMagic, Hive, Karma, LockBit, LockFile, Ragnar Locker, REvil, WannaMad
12
AGOSTO
SEPTIEMBRE
2
Cring, REvil
Atom Silo, BlackBite, Conti, Ryuk, GrandCrab, Karma, Macaw Locker, Ranion, Sayless, Vicesociety, Yanluowang
11
OCTUBRE
NOVIEMBRE
6
Conti, HelloKitty, LockBit 2.0, Memento, Mircop, Zepellin
HelloKitty, Yanluowang, FiveHands, REI, Cuba, Cerber, Diavol, WannaCry, BlackCat, Khonsari, AvosLocker
11
DICIEMBRE

Durante el transcurso del año 2021 el malware de tipo ransomware 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 diferentes sectores (incluyendo al financiero) de manera transversal, los ciberdelincuentes mediante el Ransomware como Servicio (RaaS) han mejorado y adaptado sus infraestructuras con el fin de captar una mayor cantidad de afiliados o suscriptores que les permitan generar mayores beneficios económicos incrementando progresivamente el valor del rescate exigido a sus víctimas.

Al ser una ciberamenaza que puede llegar a afectar a las entidades financieras de manera transversal, el Csirt Financiero no observó ningún compromiso al sector durante el 2021.

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. Por esta razón los actores maliciosos han preferido enfocarse en estos objetivos que les garantiza un mayor alcance ya que en algunos casos sus infraestructuras informáticas no están debidamente aseguradas.

Dentro de las ciberamenazas que el Csirt Financiero observó y compartió con nuestros asociados, 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.

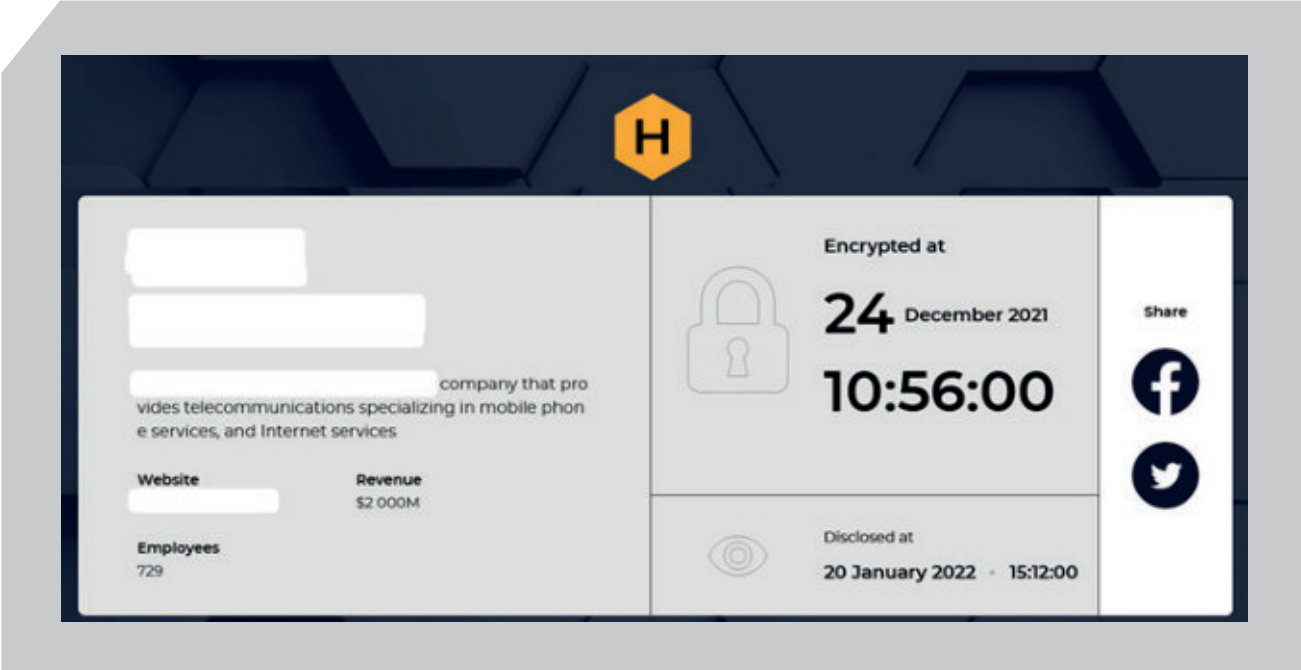
Entre los principales vectores de infección utilizados por el ransomware se encuentran:

- El uso de correos electrónicos tipo Phishing
- Aprovechamiento de vulnerabilidades
- Ciberataques al protocolo de acceso remoto (RDP)

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. Con esto buscan maximizar los ingresos percibidos en los ciberataques realizados. Para ello utilizan páginas web ubicadas en la red TOR (The Onion Routing) con el fin de mantener el anonimato de sus actividades y así publicar la información de las organizaciones afectadas.

Hive

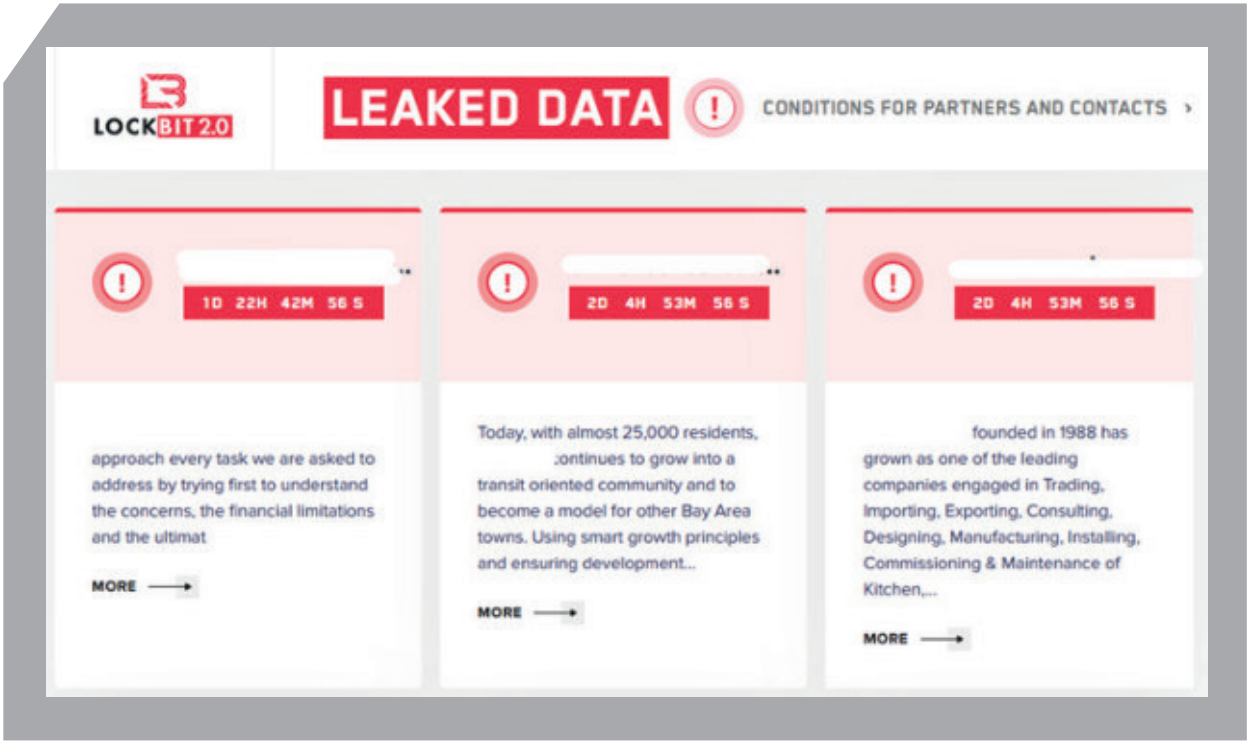
Un ejemplo de lo anterior es Hive. Este cuenta con un portal donde comparte las organizaciones que están comprometidas por el ransomware, mostrando la fecha de afectación y el valor exigido para no publicar la información entre otros datos.



LockBit 2.0

Otro ransomware que cuenta con portal web para publicar los datos exfiltrados de sus víctimas es **LockBit 2.0** quien da un tiempo a las entidades afectadas para realizar el pago exigido mediante una cuenta regresiva. Una vez se cumple este periodo de tiempo, se publica en el mismo portal la información obtenida anteriormente.

Una de las actualizaciones que trajo consigo la versión 2.0 de LockBit es la función que permite exfiltrar la información de las infraestructuras informáticas comprometidas de una manera más rápida conocida como **StealBit**. Adicionalmente, aseguran contar con el software de cifrado más rápido comparado con el de otros actores de amenaza.



SISTEMAS POS

La contingencia vista en el 2021 correspondiente a la pandemia del Covid-19 mantuvo la reducción en el uso de sistemas de pago en puntos de venta físicos comparada con el año 2020; sin embargo, 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. Estos se relacionan a continuación:

VULNERABILIDAD

Omisión de PIN en el protocolo sin contacto EMV.
Su explotación permite a los ciberdelincuentes aprovechar una tarjeta de crédito para realizar compras sin autorización. Se logró evidenciar que este tipo de ataques son posibles sin el conocimiento del PIN de la tarjeta, e incluso pueden engañar al terminal para que acepte transacciones con tarjetas fuera de línea no auténticas.

BACKDOOR

PUNCHBUGGY: captura de pantalla, túneles de proxy, robo de credenciales y ejecución de archivos.

BADHATCH: intenta evadir la supervisión de seguridad haciendo uso del cifrado TLS para ocultar los comandos PowerShell.

MALWARE

PUNCHTRACK: malware no persistente que se carga y ejecuta mediante un lanzador altamente ofuscado y nunca se guarda en el disco. Utilizado para extraer datos de tarjetas de pago y de la memoria de los sistemas punto de venta.

MemPOS: malware distribuido en foro ruso ubicado en la deep web. Intenta evadir la supervisión de seguridad haciendo uso del cifrado TLS para ocultar los comandos PowerShell, buscando volcados de memoria y CW almacenados en la memoria, archivos, teclado, portapapeles o paquetes de red mediante el uso de algoritmos.

APT

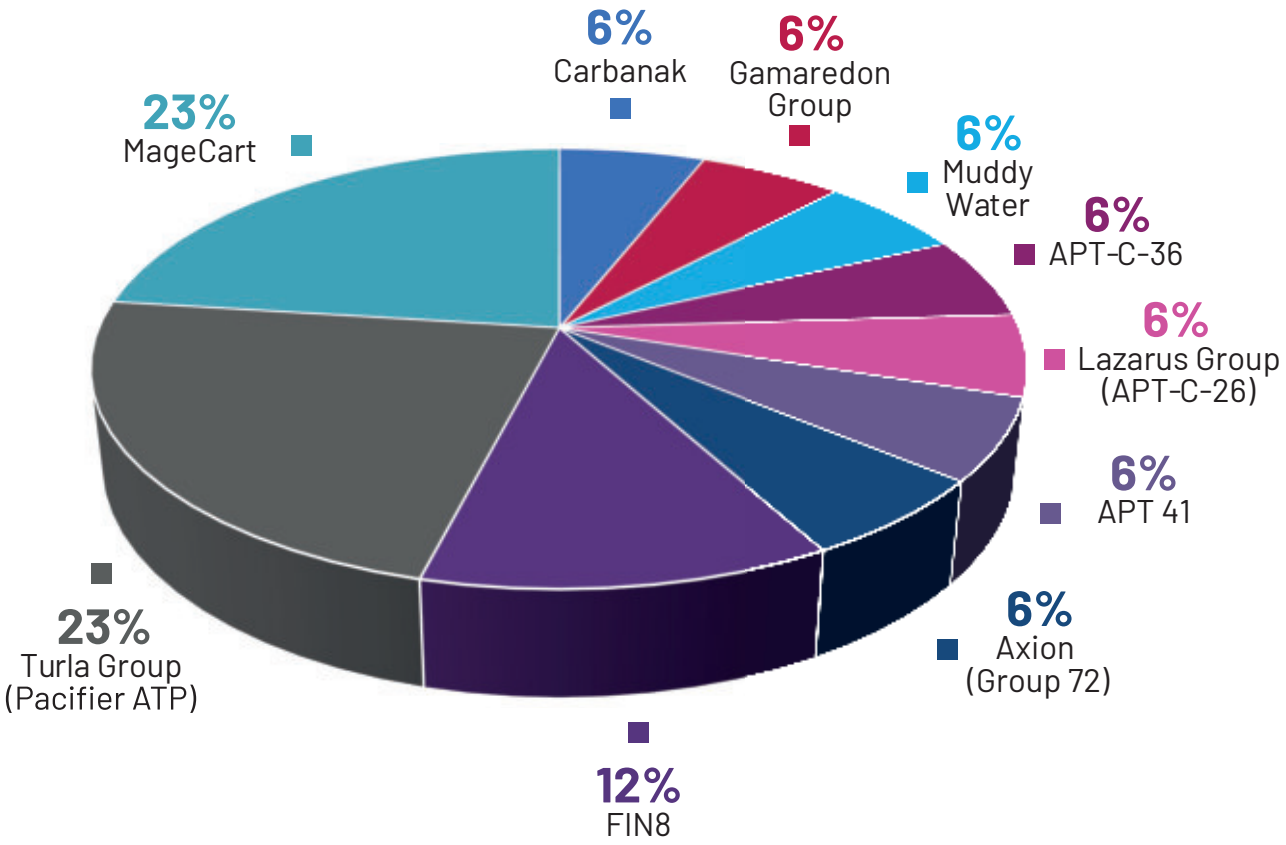
FIN8: este grupo cibercriminal ha enfocado su actividad a la afectación de varios sectores, fortaleciendo constantemente sus capacidades e infraestructura de entrega de malware. Este se considera un actor de amenazas financieras con importantes cualidades, entre su método de operación se identifica que toma largos periodos para refinar herramientas y tácticas para evitar la detección antes de que alcance objetivos viables.

Los movimientos identificados a lo largo de 2021 han sido mayormente asociados a la distribución gratuita de variantes de malware tradicionales y muy conocidos como Ploutus, existiendo muy poca variación o nuevos malware POS en el mercado cibercriminal.

APTs

A lo largo del año 2021, numerosas campañas de malware detectadas utilizaban la temática del Covid-19 como reclamo para atraer la atención de las potenciales víctimas. Además, tal y como sucedió en el año 2020, el aumento del teletrabajo y el uso de soluciones VPN fue clave para la aparición y la mejora de las actividades de diversos grupos de amenazas también categorizadas como APTs. 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, distribuídas a través de campañas de malware con objetivos específicos o generales.



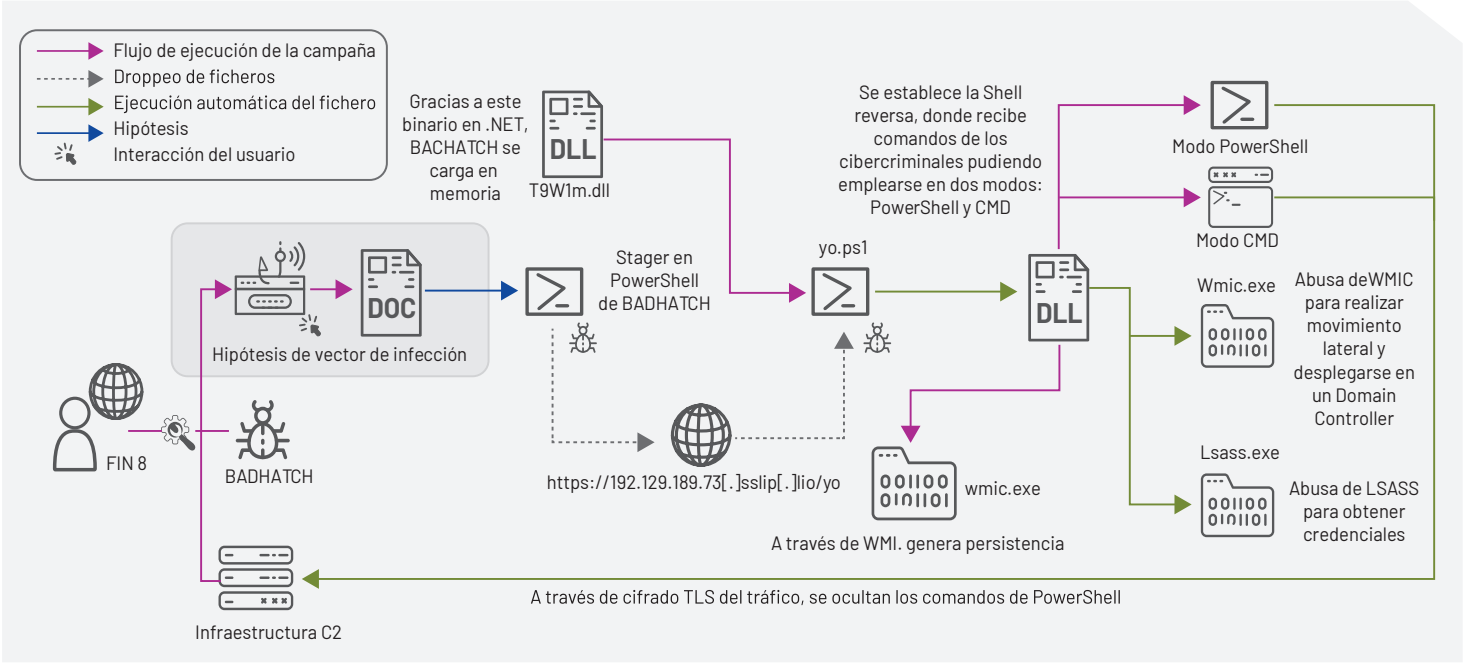
Gráfica con la relación de grupos APT vistos en 2021 por el Csirt Financiero.

Grupo FIN8

FIN8 es un grupo APT del cual se conoce actividad maliciosa desde el año 2016. Conocido por ejecutar diversas campañas contra organizaciones que cuentan con sistemas POS. Entre los sectores objetivo se encuentran el sector retail, restauración y hostelería. También se ha identificado afectación en menor medida a sectores como el de servicios financieros, alta tecnología y telecomunicaciones entre otros.

El vector de distribución utilizado por FIN8 es el Spearphishing, a través del cual comparten correos electrónicos elaborados específicamente para cada víctima por lo que el cuerpo del mensaje varía en función del objetivo. Estos mensajes contienen archivos adjuntos de Microsoft Word con macros maliciosas embebidas, las cuales, mediante ingeniería social, buscan que sus objetivos ejecuten el malware embebido principalmente el backdoor **punchbuggy** y una herramienta de raspado de memoria de nombre **punchtrack**.

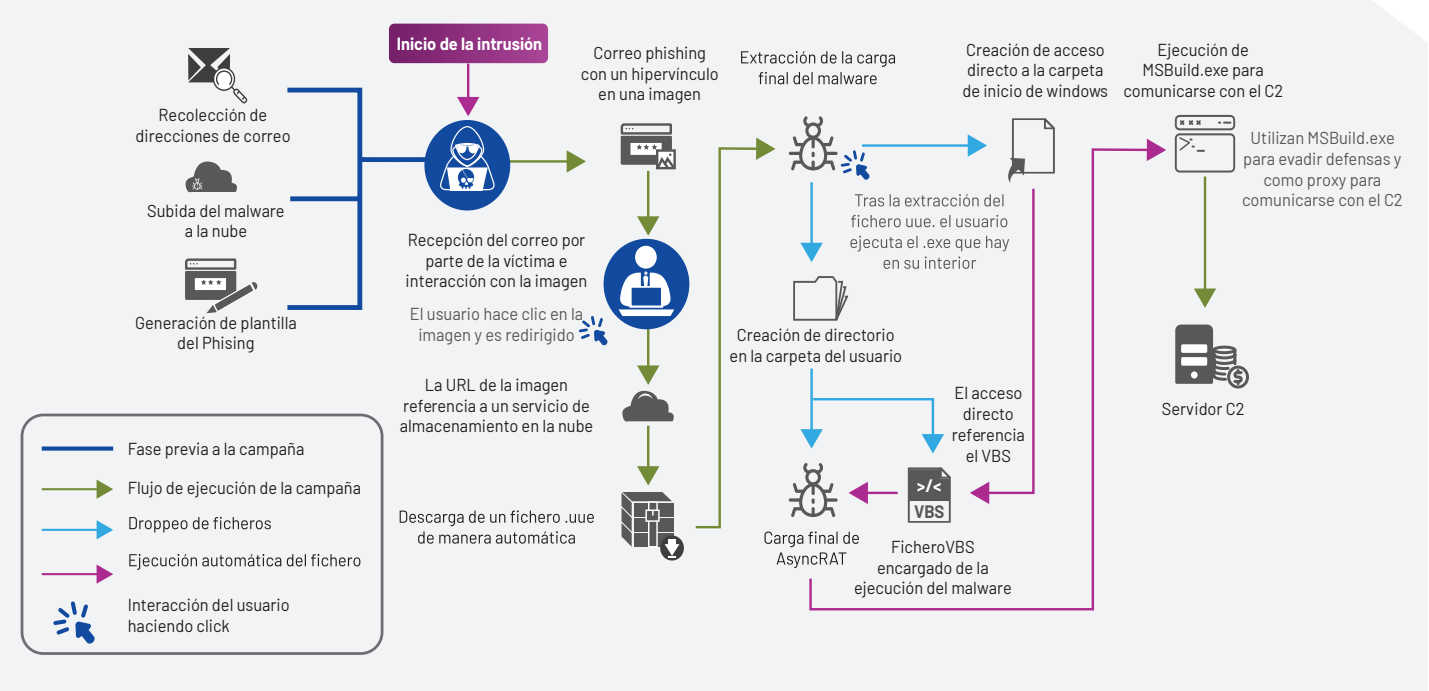
FIN8 una vez consigue comprometer con malware un sistema POS, inicia el proceso de exfiltración de los datos de pago de las tarjetas de crédito y débito para posteriormente venderlos en el mercado negro con fines de lucro. Esto remarca una diferencia con otros grupos de APTs cuyos fines se centran en el robo de información confidencial para ciberespionaje, como es el caso de APT-C-36, el cual ha sido analizado por el Csirt Financiero.



Grupo APT C-36

El grupo APT-C-36 es muy conocido por el uso de troyanos de acceso remoto (RAT) durante sus intrusiones entre las que se encuentran familias como NjRAT, BitRAT, AsyncRAT y RemcosRAT. El objetivo de este grupo es el robo de información estratégica como podría ser documentación de negocios y propiedades intelectuales.

Dentro de las campañas dirigidas a entidades del país, este grupo APT utiliza acortadores de URL como cort.as, acortaurl.com y geotargetly.com; estos son capaces de identificar la ubicación geográfica, por lo que si un usuario de un país no objetivo hace clic en el enlace, será redirigido a un sitio web legítimo.



Turla

La alta sofisticación y el impacto de las campañas desplegadas por este grupo de amenazas, indica que se encuentra respaldado y reforzado por entidades de inteligencia, supuestamente desde el servicio de inteligencia ruso.

Uno de los motivos principales para el aumento de operaciones ejecutadas por grupos APTs, fueron las tensiones geopolíticas relacionadas con conflictos promovidos entre países desarrollados con el ánimo de obtener poder y con ello imponer sus ideologías en el mundo.

El grupo de amenazas categorizado como Turla (también llamado Snake, Turla Team, Pacifier APT) fue clave en el desarrollo de campañas que tuvieron como objetivo el compromiso y robo de información de sistemas informáticos críticos en numerosos sectores y países. Una de las actividades a destacar de este grupo, es el despliegue de un nuevo backdoor llamado TinyTurla, el cual fue utilizado como método de persistencia en intrusiones detectadas en países como Estados Unidos o Alemania.

En estas campañas analizadas, el vector de infección utilizado por este grupo es el envío de correos electrónicos de tipo spearphishing, a través de los cuales se adjuntan archivos ofimáticos maliciosos que contienen la carga del agente del servidor C2 que haya sido configurado por los cibercriminales.

Como temáticas elegidas para las campañas, este grupo criminal utilizaba documentos relacionados con elecciones nacionales, pagos online no realizados, citaciones judiciales, entre muchas otras. El objetivo de estas temáticas, es la de persuadir a las víctimas finales de que los correos electrónicos eran legítimos, para así llegar a más objetivos posibles.

Como grupo, se maneja la teoría de que Turla, despliega este tipo de campañas para que la información que ha sido sustraída de forma ilegítima a las víctimas, sea utilizada en operaciones posteriores de contrainteligencia y ciberespionaje, lo cual define a Turla como una de las amenazas más prolíficas del año 2021.

Magecart

Otra de las amenazas destacadas y relevantes en el sector financiero mundial, es el auge de los grupos englobados bajo la categoría de Magecart. Magecart es el término general que permite la categorización de grupos cibercriminales que realizan la inyección de scripts y código malicioso en los sitios web objetivo. Según las investigaciones realizadas de manera interna y por empresas de seguridad cibernética, los grupos de Magecart tienen dos maneras de conseguir sus objetivos (motivaciones financieras):

- Infección de sitios web de comercio electrónico, mediante skimmers adquiridos de forma ilícita en el mercado negro de la red oscura.

- Venta y comercialización de estos skimmers en tiendas alojadas en la red oscura, normalmente a un precio elevado.

Según datos de la telemetría en los servicios web, más de un millar de tiendas online (alojadas en plataformas de eCommerce) son vulnerables, exponiendo la información confidencial de los consumidores al skimming. Se ha permitido identificar que no solo eran vulnerables al skimming las tiendas online, sino que servicios financieros, mediáticos, de seguridad, farmacéuticos (entre muchos otros) han sido objetivo de esta amenaza, a través de la cual se calcula que se ha podido proceder a la pérdida de millones de dólares. El skimming, dentro de la ciberdelincuencia, es uno de los "negocios" más prósperos y que más beneficios trae a los actores de amenaza.

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.

El Csirt Financiero identificó el uso de algunas muestras de malware desarrollado para ATM, como lo es Ploutus y DispCashBR, esto acompañado del uso de técnicas como caja negra (BlackBox) que permiten interactuar física y lógicamente con el cajero electrónico. Estas afectaciones se presentaron en Latinoamérica y no se observó su uso en Colombia.

Las entidades financieras de Colombia están muy sensibilizadas respecto a las amenazas contra estos activos. Invierten en I+D+I para mejorar las diferentes capas de seguridad con el fin de evitar un posible compromiso y acceso no autorizado.

Uno de los asociados del Csirt Financiero facilitó la infraestructura para realizar la ejecución de diferentes muestras de malware vistas y reportadas a nuestros asociados como Ploutus-D, DispCashBR, Alice, Cutlet Maker y Died, en un entorno real.

Estas pruebas permitieron obtener información relevante y directa de las amenazas asociadas a los cajeros automáticos (ATM).

Malware Móvil

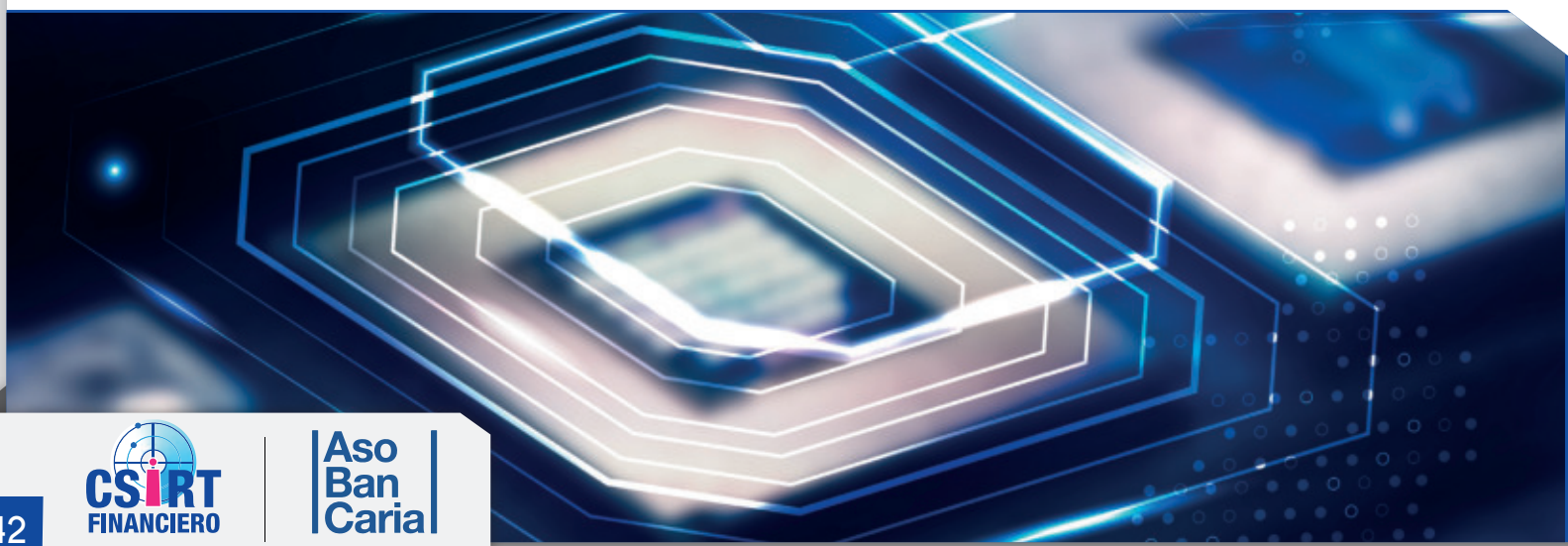
En el año 2021 el malware móvil tuvo gran movimiento generando consecuencias en el pilar de la **confidencialidad** de los usuarios de dispositivos móviles, el sistema operativo más afectado en esta área sigue siendo **Android**, esto debido a que mantiene el mayor porcentaje de instalación a nivel mundial.

El enfoque de los ciberdelincuentes se basa en la amplia difusión del sistema operativo. Es un ítem relevante a la hora de distribuir el malware en el intento de que pueda afectar a gran cantidad de usuarios.

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 y el uso ilimitado e indiscriminado de las aplicaciones que soportan transacciones financieras. Los malware móviles identificados se conocen bajo los nombres:

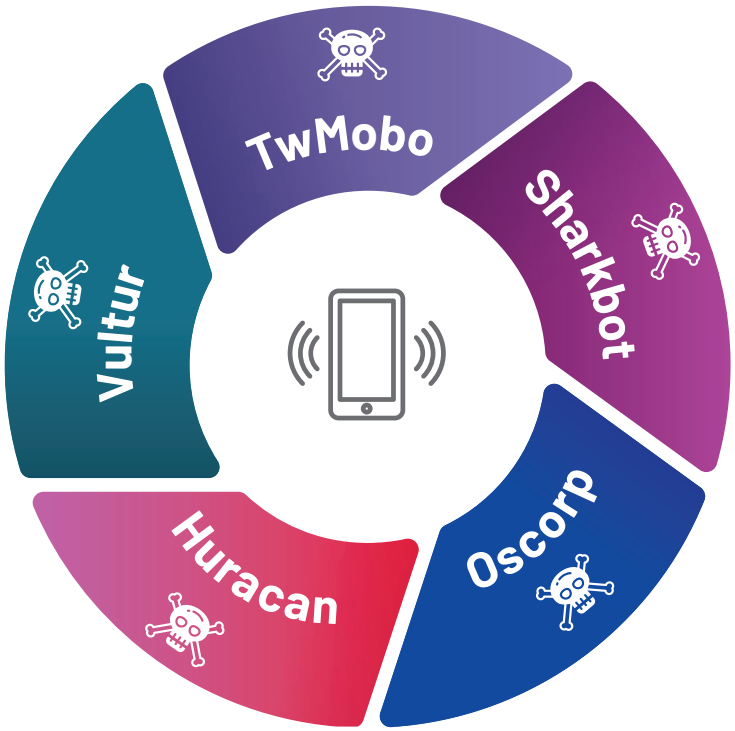
MALWARE MÓVIL 2021

Alien
BasBanke
BrazKing
Ermac
EventBot
Flubot
Huracan
Joker
MalRhino
Oscorp
MobileInter
PixStealer
Wroba
SharkBot
Sova
SpyNote
TangleBot
TeaBot
TwMobo
Ubel
Vultur



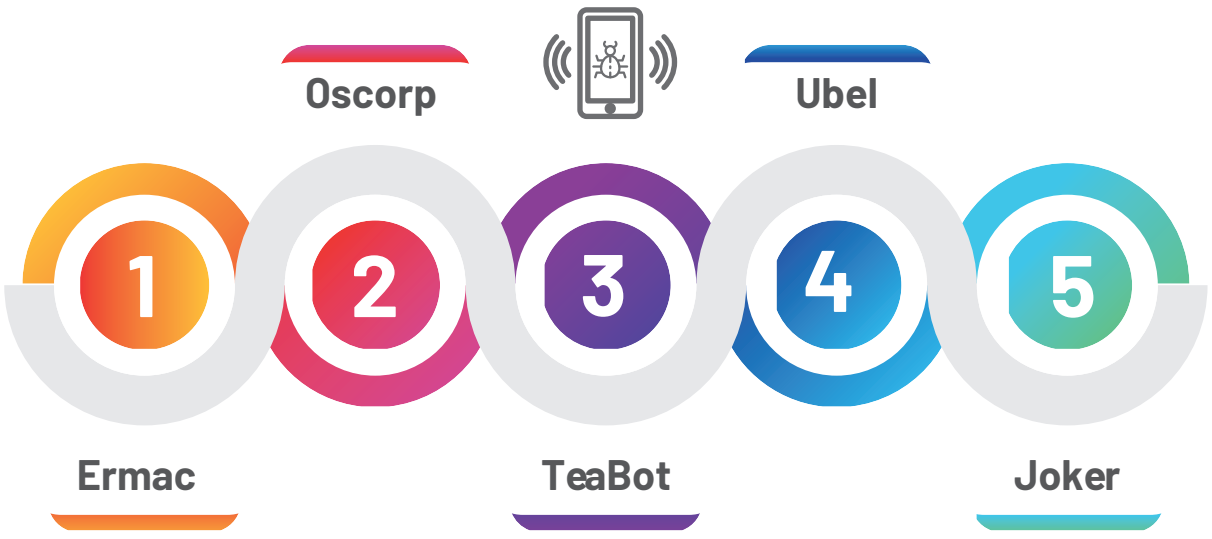
El 2021 fue un año en el que surgieron nuevas familias de esta categoría, entre ellas se destacan:

NUEVAS FAMILIAS DE MALWARE MÓVIL EN 2021



A continuación se presentan las familias de malware móvil más difundidas en el 2021:

TOP 5 MALWARE MÓVIL EN 2021



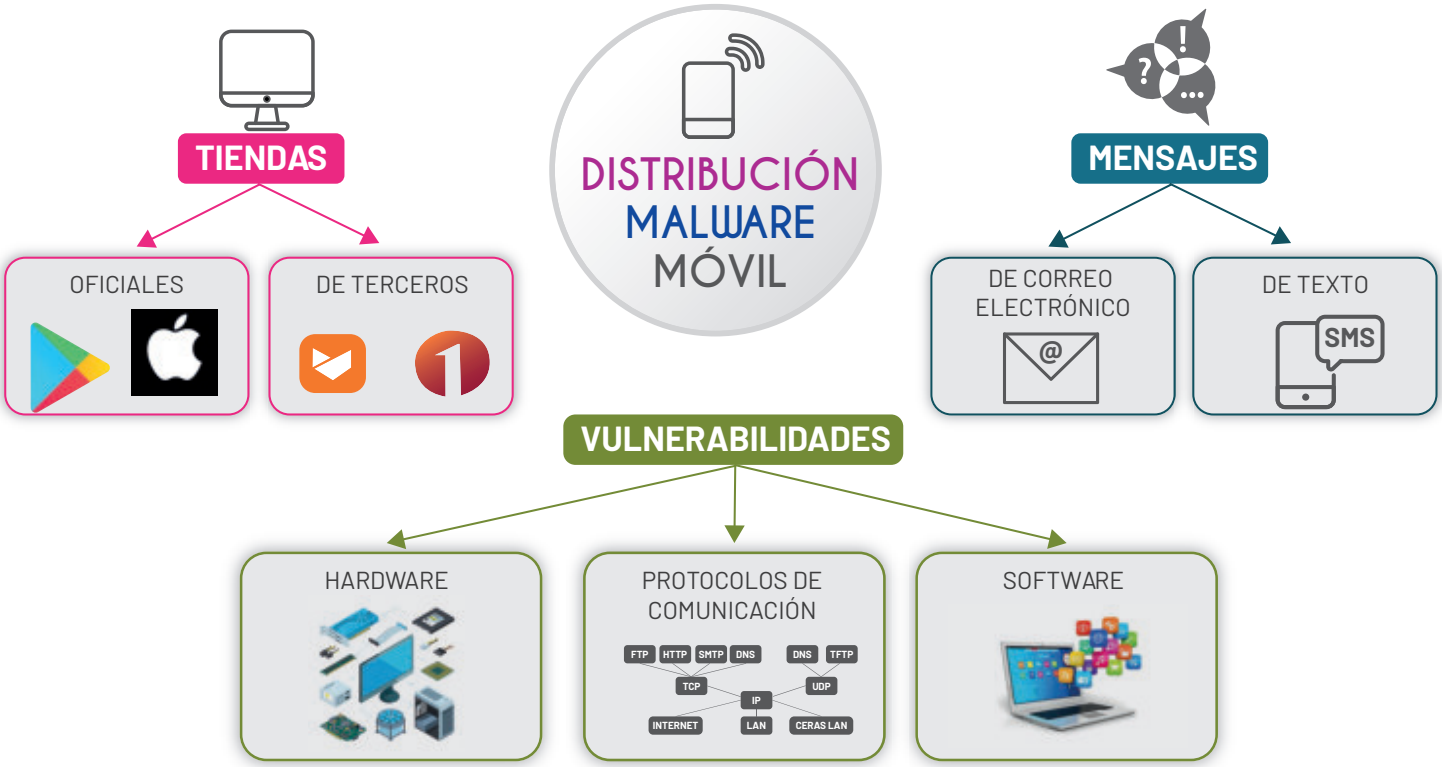
Capacidades de malware móvil

Se evidencia en el 2021 que muchas de las familias que componen este tipo de malware suman funcionalidades para afectar con un impacto mayor a cada dispositivo, entre ellas están:

- 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

Distribución de malware móvil

La forma en la que los ciberdelincuentes despliegan el malware móvil es diversa, intentan aprovechar diferentes recursos para camuflar las cargas maliciosas. Las más utilizadas en el 2021 fueron:



Tiendas

Suplantando aplicaciones:

- Oficiales como Google Play Store y AppStore
- De terceros como Aptoide y 1Mobile

Mensajes

Relacionando un enlace que al desplegar se dirige a la descarga de malware:

- De texto (SMS)
- De correo electrónico

Vulnerabilidades

Explotación de brechas de seguridad a nivel:

- Hardware
- Software
- Protocolos de comunicación

INTELIGENCIA DE AMENAZAS

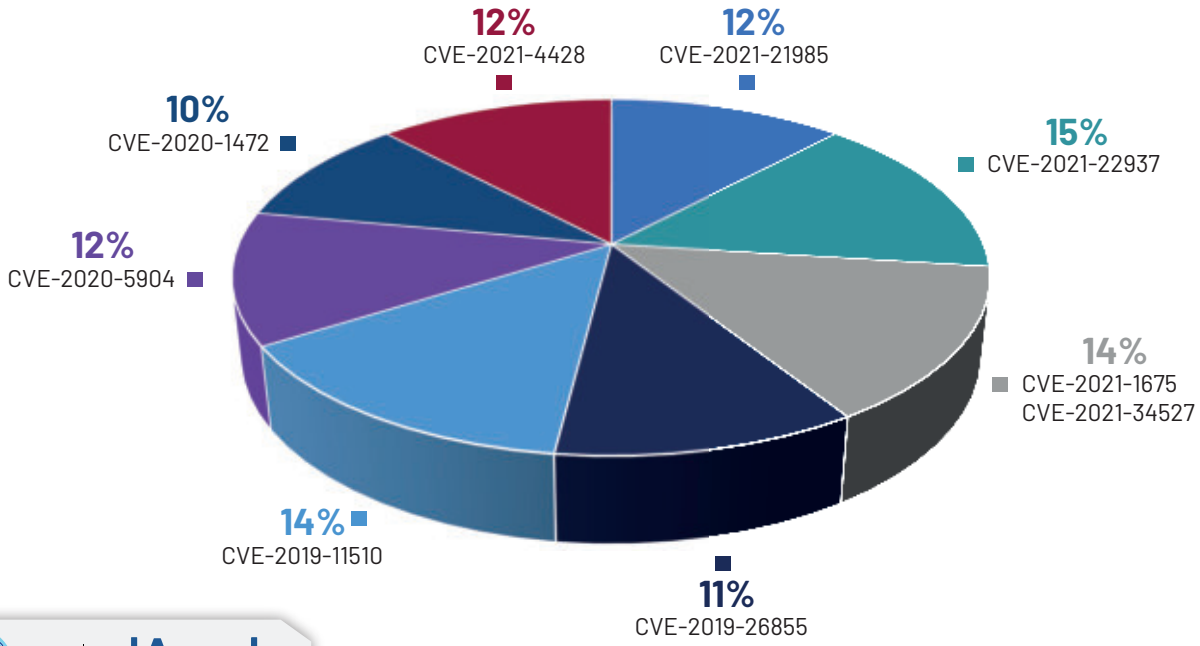
La base de conocimiento e información del sector financiero respecto a las vulnerabilidades de los sistemas informáticos, se encuentra recogida en la capacidad de Inteligencia de Amenazas por el Csirt Financiero.

A lo largo del año 2021, se detectaron numerosas fallas de seguridad en productos ampliamente usados por las corporaciones a nivel mundial, lo cual produjo un aumento en los ciberataques y en los incidentes detectados. Para brindar inteligencia e información relevante en este tema tan crítico, se procede a incluir la clasificación de las vulnerabilidades, incluyendo las más críticas y las que mayor impacto ocasionarían en las organizaciones que implementen sus servicios. Los análisis y la documentación reportada por el equipo del Csirt Financiero, permitió la identificación y la remediación de las vulnerabilidades compartidas.

Los análisis y la documentación reportada por el equipo del Csirt Financiero, permitió la identificación y la remediación de las vulnerabilidades compartidas.

A continuación, se procederá a exponer un mayor contexto relacionado con las vulnerabilidades más críticas detectadas y reportadas en el año 2021.

TOP DE VULNERABILIDADES CON MAYOR IMPLICACIÓN EN ACTIVIDADES MALICIOSAS CSIRT



Vulnerabilidad	Descripción	Productos Afectados	CVSS
CVE-2021-21985	Permite la ejecución de código remoto debido a un fallo de sanitización en la entrada del plugin Virtual SAN Health Check.	VMware Vcenter	9.8
CVE-2021-22937	Permite a un administrador autenticado el sobreescribir un archivo arbitrario para ganar una ejecución de código remoto.	Pulse Connect Secure	9.1
CVE-2021-1675/CVE-2021-34527	Permite la ejecución de código remoto en servicios vulnerables de la cola de impresión de Windows.	Windows Server 2008, 2012, 2016, 2019	8.8
CVE-2021-26855	Permite la ejecución remota de código en servidores Microsoft Exchange Server.	Microsoft Exchange Server	9.1
CVE-2019-11510	Permite que un atacante sin autenticación envíe una petición modificada suministrando una URI diseñada para leer archivos del sistema de forma arbitraria.	Pulse Connect Secure	10
CVE-2020-5902	Permite que un atacante sin autenticación que pueda acceder a la plataforma TMUI ejecute código remoto.	F5 BIG-IP	9.8
CVE-2020-1472	Permite la escalada de privilegios si un atacante establece una comunicación Netlogon hacia un controlador de dominio.	Windows Server 2008, 2012, 2016, 2019	10
CVE-2021-44228	Permite el envío de consultas a través de JNDI para ejecutar código de forma remota.	Apache Log4j y demás productos que requieran de esta librería	10

Top fabricantes con mayores vulnerabilidades relacionadas

El equipo de analistas del Csirt Financiero, ha identificado los cinco fabricantes de productos con mayores vulnerabilidades en equipos de usuario como en una infraestructura corporativa. A continuación, se procede a dar más contexto acerca de estas vulnerabilidades y del impacto que pueden ocasionar en los productos afectados.

Al contrario que en los años 2019 y 2020, **Google** se ha impuesto como el fabricante con el mayor volumen de vulnerabilidades en sus productos, debido a la amplia gama de servicios y al uso común que se les da a estos.

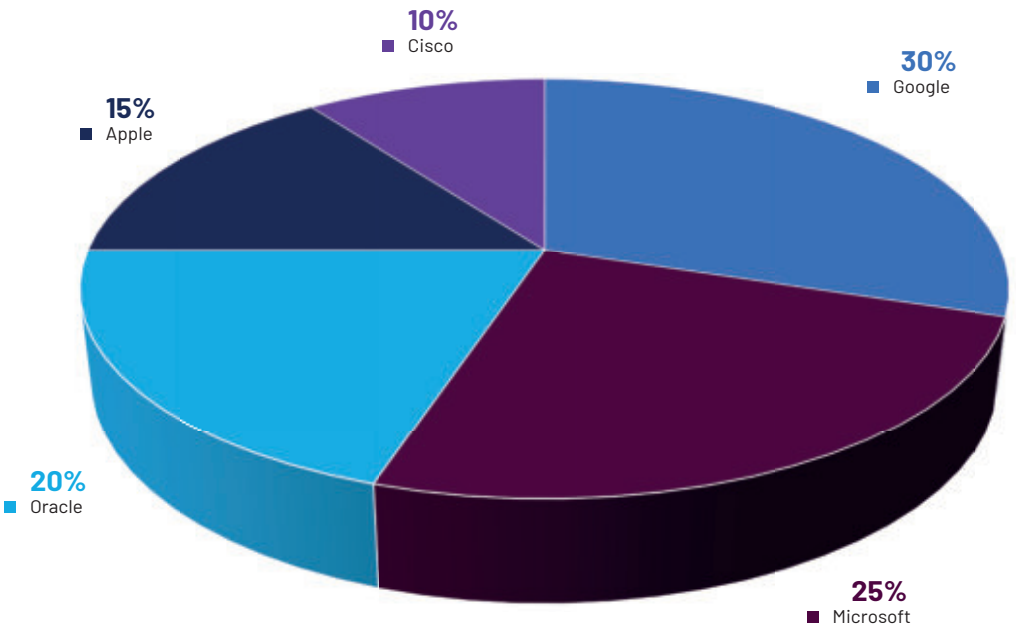
El siguiente fabricante con mayores vulnerabilidades, es **Microsoft**. Este fabricante continúa en el top de mayor número de reportes de vulnerabilidades, dado que es el sistema operativo más utilizado en el mundo, tanto a nivel usuario como de manera corporativa. Durante todo el año 2021, se han observado numerosas vulnerabilidades de ejecución remota de comandos y escalada de privilegio en sistemas de escritorio como en servidores, lo cual ha desembocado en uno de los años con mayores intrusiones detectadas hasta la fecha.

El tercer fabricante con el mayor número de reportes de vulnerabilidades públicas en el año 2021 fue **Oracle**, siendo este situado en el mismo puesto que el año anterior.

Apple se sitúa en cuarto puesto, siendo uno de los fabricantes con mayor presencia a nivel mundial debido a los productos desarrollados a nivel usuario que pueden ser utilizados en un entorno corporativo.

Por último, **Cisco** fue afectado por numerosas vulnerabilidades que son ampliamente explotadas en intrusiones reales realizadas por diversos grupos de amenazas a nivel mundial, en productos expuestos a Internet que puedan permitir una ejecución remota de comandos.

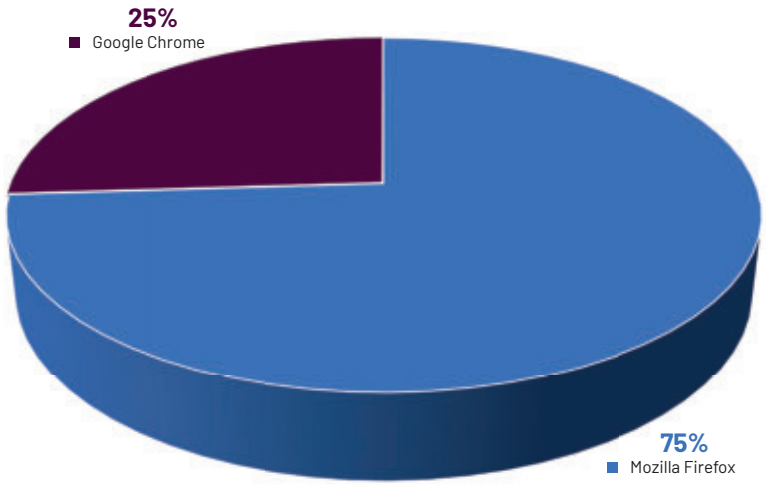
TOP DE FABRICANTES CON MAYORES VULNERABILIDADES



Navegadores con más vulnerabilidades conocidas

Con el objetivo de generar información más explícita, el equipo del Csirt Financiero presenta la categoría de vulnerabilidades en navegadores web vistas en 2021.

NAVEGADORES CON MÁS VULNERABILIDADES RECONOCIDAS



Google Chrome:

Tal y como ha sido tendencia en los últimos años, el navegador Chrome, uno de los productos estrella de Google, ha sido víctima de numerosas vulnerabilidades que afectan a millones de usuarios que utilizan este software a diario. En el año 2021 se detectaron un total de 309 vulnerabilidades asociadas a este producto, siendo el navegador con mayores brechas de seguridad.

De estas 309 vulnerabilidades, 4 de ellas superaron el valor de 9 en la escala del sistema de puntuación de vulnerabilidad común (CVSS), las cuales fueron identificadas de la siguiente forma: CVE-2021-21106, CVE-2020-16039, CVE-2020-16037, y CVE-2020-6572.

Estas cuatro vulnerabilidades fueron explotadas para conseguir los siguientes objetivos:

- Escapar de la sandbox del navegador de manera arbitraria mediante una página HTML previamente diseñada.
- Realizar una corrupción de la pila a través de un exploit embebido en una página HTML desarrollada por los atacantes.
- Realizar una ejecución de código arbitrario a través de una página HTML maliciosa.

Mozilla Firefox:

Según algunos datos de telemetría a nivel mundial, Mozilla Firefox se encuentra en el top de navegadores más utilizados por los usuarios, tanto para uso personal como profesional. Este hecho implica, que sea susceptible a alojar vulnerabilidades en el código de la aplicación, lo cual ha sido detectado gracias a que ha sido el segundo navegador con mayores CVEs asignados durante el año 2021, siendo un total de 106. En concreto, 4 vulnerabilidades han superado la puntuación de 7.5, siendo registradas de la siguiente manera: CVE-2021-38504, CVE-2021-38503, CVE-2021-29971 y CVE-2020-26972.

Estas cuatro vulnerabilidades fueron explotadas para conseguir los siguientes objetivos:

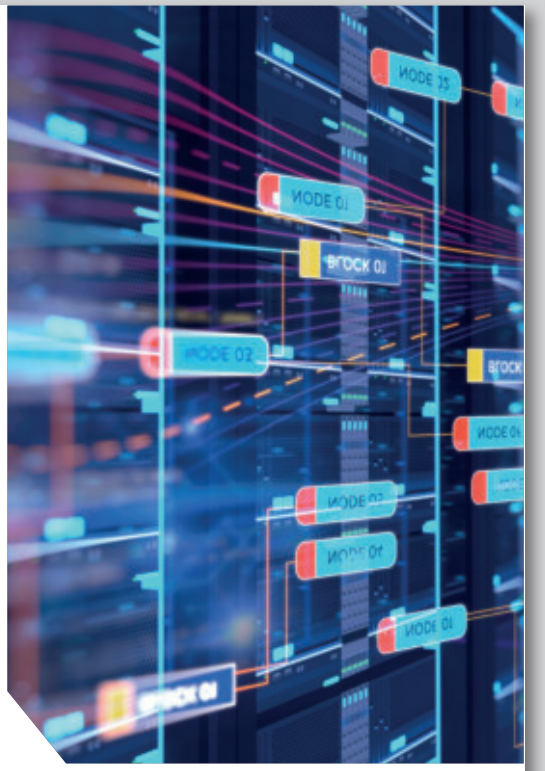
- Realizar una corrupción de memoria, pudiendo explotar de manera arbitraria el proceso fallido ocasionado por la vulnerabilidad de la aplicación.
- Evadir las restricciones en el navegador para conseguir una ejecución de scripts en etiquetas iframe en hojas de estilo XSLT.
- Realizar una corrupción de memoria como resultado de un input malicioso que no haya sido tratado.

Principales amenazas cibernéticas: vulnerabilidades usadas por grupos APT.

A lo largo del año 2021, se identificaron numerosas campañas de malware operadas por el grupo cibercriminal categorizado como APT35. En estas campañas operadas por el grupo de supuesto origen iraní, realizaban una primera explotación de las vulnerabilidades identificadas como ProxyShell (CVE-2021-31207, CVE-2021-34473 y CVE-2021-34523) para acceder a la infraestructura interna de las víctimas, concretamente en los servidores de Microsoft Exchange. Cabe recalcar que estas vulnerabilidades permitían a un atacante remoto la ejecución de código arbitrario con privilegios de SYSTEM (mayores privilegios en sistemas Windows).

Una vez realizada esta primera explotación, se descargaban los agentes de algunos de los servicios C2 y frameworks de post explotación más abusados por los cibercriminales, los cuales permitían el establecimiento de la persistencia y la comunicación con la infraestructura desplegada por los actores de amenazas.

Otra de las vulnerabilidades más explotada a nivel mundial por los grupos de amenazas y cibercriminales, fue identificada bajo el id CVE-2021-40444. Este Zero Day permitía la inclusión de controles ActiveX incrustados en documentos ofimáticos de Microsoft Office, lo cual podría desencadenar en la ejecución de código arbitrario en los sistemas víctima. Esta vulnerabilidad, y algunas otras relacionadas con productos de Microsoft, fueron explotadas por grupos de Ransomware as a Service (RaaS) como Netwalker, Stampado, RaaSberry, Satan, entre muchos otros.



Una vulnerabilidad crítica en dispositivos IoT, conocida como CVE-2021-36260, permitía una inyección de comandos de manera remota en los servidores web de algunos de los productos de Hikvision. Dado a que el input del usuario no se encontraba tratado de manera correcta, un cibercriminal podría inyectar comandos de manera remota para ganar acceso al sistema vulnerable. Este fallo permitió la inclusión de miles de dispositivos a una botnet relacionada con Mirai, llamada Moobot.

APOYO A INCIDENTES

El equipo del Csirt Financiero dispone de la capacidad de Análisis y Apoyo a incidentes la cual es utilizada para realizar análisis, definición de medidas para la contención o mitigación ante incidentes de ciberseguridad y la identificación de amenazas cibernéticas que puedan causar impacto negativo a los asociados.

Durante el año 2021 se realizó constante seguimiento a cada uno de los incidentes y eventos de seguridad reportados, a partir de ellos se generaron y compartieron varios productos de investigación como **Playbooks, Informes de Amenaza, Plantillas de Remediación y Generación de Reglas** con el fin de aportar a la prevención y mitigación de posibles eventos y amenazas cibernéticas que puedan afectar a las entidades financieras nacionales. Todos estos productos están disponibles en el portal corporativo para su consulta.

Datos generales

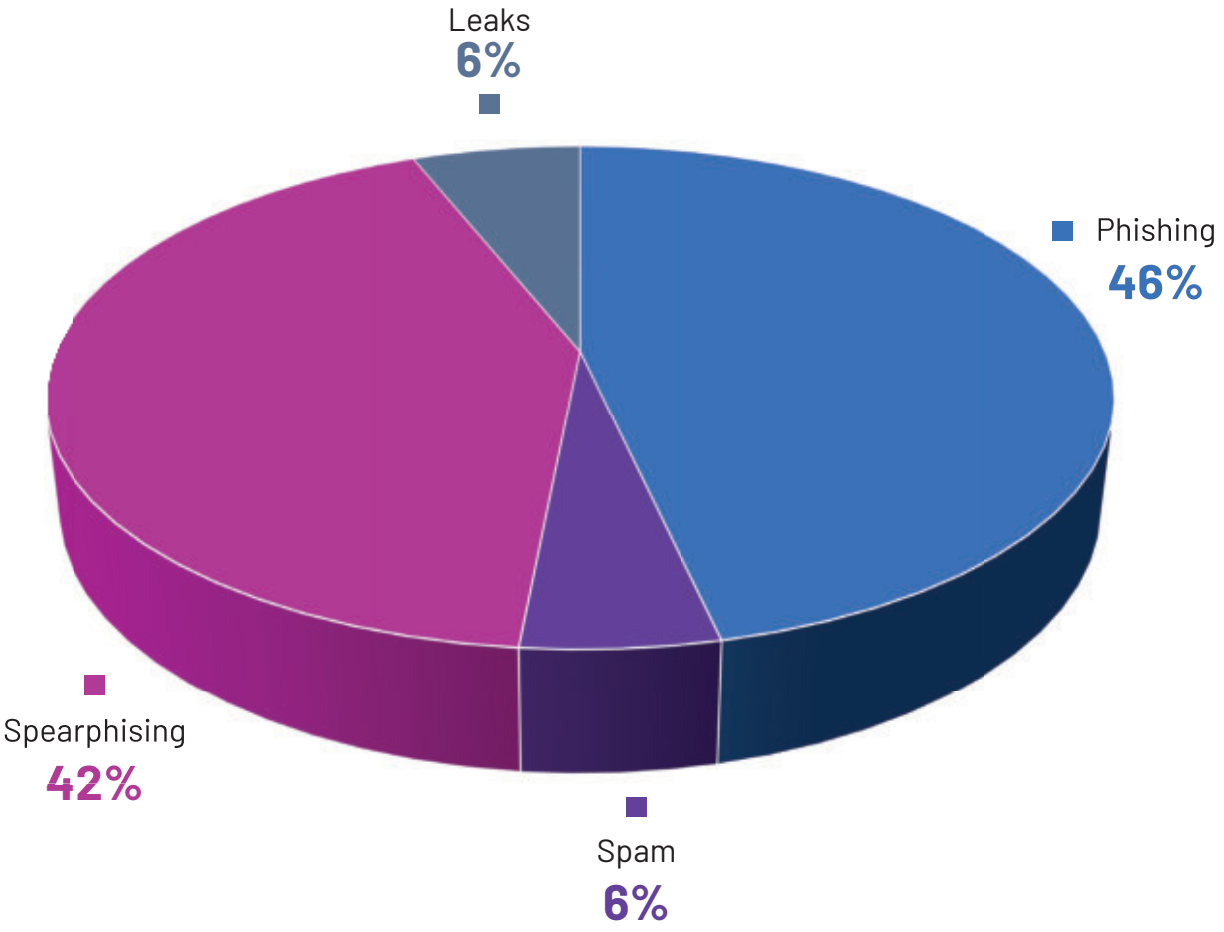
En el año 2021 el Csirt Financiero recibió y gestionó **389 incidentes**, entre los que se encontraban **sitios fraudulentos** que suplantan a organizaciones legítimas, venta de **credenciales bancarias en redes sociales**, información de usuarios de entidades financieras expuesta en **leaks de foros clandestinos** y reporte de números de telefonía celular utilizados para actividades de **smishing** y **vishing**.

Entre los vectores de ataque utilizados por los ciberdelincuentes se pueden observar el **phishing** y el **spearphishing**, los cuales tienen un porcentaje de uso del 46% y el 42% respectivamente, asociados principalmente a la suplantación de organizaciones colombianas con gran reconocimiento nacional, cuyo objetivo es el de engañar a los usuarios para que **descarguen y ejecuten malware** en sus equipos. También se han utilizado estos vectores para el envío de **formularios fraudulentos** de entidades bancarias a sus clientes, para que estos ingresen las credenciales de acceso a sus bancas virtuales y a sus cuentas de correos electrónicos.

Se puede observar al **spam** con un valor del 6%, en donde se encuentran mensajes de correo electrónicos engañosos relacionados a temas como venta de productos o servicios desconocidos, estafas nigerianas y extorsión para no difundir vídeos íntimos de los usuarios objetivos.

También se observó con un porcentaje del 6% el incremento de **información sensible** de usuarios de entidades financieras **expuesta en leaks** tanto en clear, deep y dark web. La información extraída de estas actividades puede ser utilizada para planear y ejecutar posibles ataques en contra de las entidades financieras que se hayan visto expuestas en estos eventos.

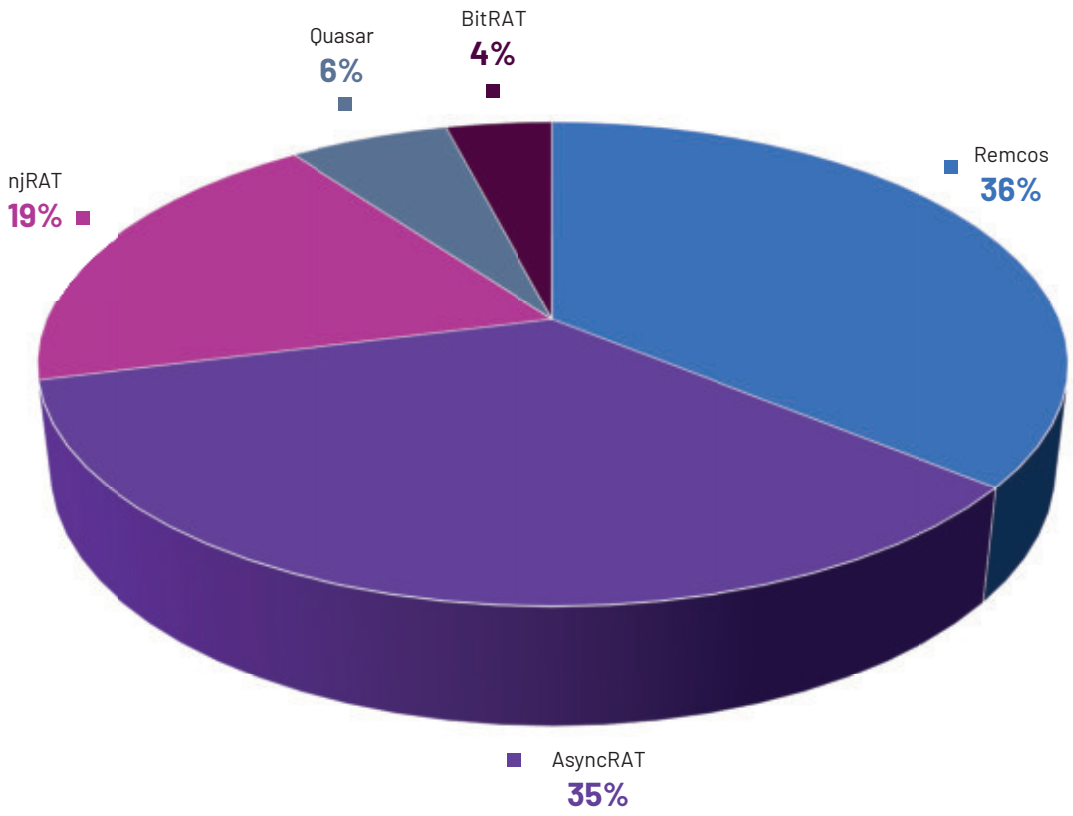
En el año 2021 el Csirt Financiero recibió y gestionó 389 incidentes, entre los que se encontraban sitios fraudulentos que suplantan a organizaciones legítimas.



Sin duda alguna la actividad maliciosa que más se destacó durante todo el 2021 y sigue en gran aumento hasta el día de hoy es la distribución de **Troyanos de Acceso Remoto (RAT)** a través de mensajes de correo electrónico, con el fin de comprometer equipos corporativos de diferentes organizaciones nacionales para acceder a su información confidencial.

Las familias de malware más utilizadas para estas actividades fueron **RemcosRAT** y **AsyncRAT**, sin olvidar a otros como **NjRAT**, **QuasarRAT** y **BitRAT**. Todas estas familias de malware tienen en común que son **herramientas legítimas** que fueron utilizadas por ciberdelincuentes para realizar actividades maliciosas.

RAT MÁS DISTRIBUIDOS EN INCIDENTES



PlayBooks

El equipo técnico del Csirt Financiero desarrolló y publicó cuatro Playbooks con el objetivo de brindar información de manera estructurada a los asociados para que puedan llevar a cabo las acciones necesarias en un corto periodo de tiempo y de manera efectiva.

El primer playbook fue realizado con el objetivo de brindar información sobre las acciones a llevar a cabo frente a los posibles incidentes ocasionados por la **inyección de procesos**, técnica comúnmente utilizada para la ejecución de malware en un sistema.

Con este documento se pretende dar apoyo a los equipos de respuesta ante incidentes con el fin de llevar a cabo acciones que permitan la identificación de mecanismos de persistencia, recomendaciones para la realización de actividades de forense en los equipos comprometidos y la explicación de las subtécnicas asociadas con la **inyección de procesos.**

El siguiente playbook fue una recopilación de información de **Phishing análisis**, con el fin de brindar al asociado características que deben ser analizadas durante el tiempo que se encuentra un phishing activo. Allí se plasman pautas que se deben tener en cuenta cuando se reconoce un sitio web utilizado para la suplantación de identidad de una compañía, otorgando información sobre cómo se puede identificar la infraestructura, direcciones, URL y rutas que se encuentran alojados en un sitio web malicioso

El tercer playbook compartido con los asociados se desarrolló con el fin de brindar el conocimiento de las técnicas y subtécnicas relacionadas a la táctica de **movimiento lateral**, las cuales son utilizadas por grupos cibercriminales y software maliciosos con el fin de obtener el ingreso y control a sistemas remotos en una red comprometida.

El cuarto playbook enviado tiene como fin brindar y dar apoyo a los asociados para detectar posibles **exfiltraciones de información** en un sistema comprometido. Se documentó un marco de trabajo, actividades y recomendaciones para dar apoyo a los equipos de respuesta a incidentes frente a un evento de seguridad relacionado a exfiltración de información y realizar acciones de análisis, contención, erradicación, recuperación y actividades post-incidente para el aprendizaje de los incidentes generados.

También se realizaron actualizaciones a playbooks compartidos en años anteriores, como los de **Actuación ante ransomware, Actuación ante RAT y Mecanismos de persistencia**, los cuales han tenido cambios en sus grafos de actividades al ser implementado bajo el estándar BPMN.

Informes de Amenazas

El equipo técnico del Csirt Financiero desarrolló y publicó **cinco Informes de Amenaza** con el objetivo de presentar diferentes perspectivas y puntos de vista relacionados con la forma de operar, las técnicas, tácticas y procedimientos descubiertos a través de la investigación realizada a las amenazas evidenciadas.

El **primer informe** esta relacionado con el **Mercado negro de credenciales bancarias**, el cual refleja un trabajo colaborativo entre el Csirt Financiero y un asociado. En este documento se menciona la cadena de negocio y el incremento en la venta de credenciales bancarias pertenecientes a usuarios de entidades bancarias localizadas en la región de LATAM. Se destaca información relevante sobre los troyanos bancarios y los skimmers digitales más utilizados para el robo de este tipo de información. Además se menciona la venta de las credenciales exfiltradas en foros ilegítimos de la Deep Web.

En el **segundo informe** se da a conocer el **Análisis operacional** de los troyanos brasileros **Gêmeos, Mekotio** y **Bizarro**, los cuales siguen siendo una de las principales amenazas que sufren hoy en día las entidades financieras y sus clientes. Este documento da a conocer información de utilidad para que los asociados puedan hacer seguimiento al comportamiento y cadena de infección llevado a cabo por estas familias de malware controladas por actores desconocidos.

Por consecuencia de la recepción de gran cantidad de muestras de "malware" por parte de los asociados relacionadas con la herramienta legítima de acceso remoto **RemcosRAT**, se realizó el **tercer informe de amenazas**. Dicha herramienta fue distribuida a través de campañas de spearphishing con el objetivo de obtener acceso remoto a los sistemas de las entidades financieras y a partir de ahí, poder realizar cualquier acción. En este documento se puede encontrar el análisis realizado a Remcos e información de las campañas que probablemente están manipuladas por un mismo actor de amenazas denominado APT-C-36.

En el **cuarto informe de amenazas** se recogen las conclusiones obtenidas a través del análisis de distintas muestras de malware compartidas por los asociados, dando a conocer un posible **nuevo actor de amenazas denominado Pjoao**, el cual ha desarrollado varias campañas de distribución de RATs en Colombia. El Csirt Financiero logró establecer relaciones entre indicadores de bajo y alto nivel, detectando ciertos patrones de comportamiento en las muestras que fueron reportadas y analizadas en este documento para mostrar las tácticas, técnicas y procedimientos utilizados en la distribución de RATs en Colombia por parte de este actor de amenazas.

El **quinto informe de amenazas** tiene relación con el análisis realizado en la ejecución de diferentes muestras de m**alware para máquinas ATM** en una infraestructura destinada para tal fin, con el objetivo de evidenciar su comportamiento en un entorno real. Entre las muestras de malware ejecutadas se encuentran **Ploutus-D**, **DispCashBR**, **Alice** y **Cutlet Maker**. Esto pudo realizarse gracias a la colaboración total por parte de una de las entidades que puso a nuestra disposición todos los recursos necesarios para simular el entorno real y emitir el informe.

Plantillas de remediación

Con el objetivo de ofrecer métodos de mitigación a diferentes técnicas utilizadas por los ciberdelincuentes, el Csirt Financiero compartió con los asociados **10 plantillas de remediación**. Las mitigaciones analizadas en los documentos compartidos fueron:

Mitigación M1024 - Restrict Registry Permissions

Relacionado a configuraciones de registros de windows afectadas en actividades malintencionadas.

Mitigación M1036 - Account Use Policies

Relacionado a ataques que tienen como objetivo acceder a cuentas de usuario de terceros, principalmente empleando la fuerza bruta.

Mitigación M1015 - Active Directory Configuration

Técnicas utilizadas para comprometer el Directorio Activo, el cual permite almacenar y gestionar información sensible dentro de una red.

Mitigación M1049 - Antivirus/ Antimalware

Relacionada a los software que detecta, bloquea, monitoriza la actividad en tiempo real y elimina amenazas que se encuentren localmente en el sistema. Por ello, los ciberdelincuentes durante sus intrusiones intentan desactivar o anular la ejecución de estos.

Mitigación M1013 - Application Developer Guidance

Relacionada a generar un entrenamiento para los programadores que puedan crear un estilo de código que minimice la superficie de ataque que un cibercriminal pueda aprovechar a su favor para evitar los riesgos y amenazas de seguridad.

Mitigación M1048 - Application isolation and sandboxing

Relacionada con los riesgos asociados a una mala configuración cuando se realiza el aislamiento de aplicaciones y uso de entornos controlados para ejecutar archivos potencialmente maliciosos y que puede generar el compromiso del sistema operativo anfitrión.

Mitigación M1050 - Exploit Protection

Relacionada con los riesgos asociados a las vulnerabilidades sin parchear o fallos tecnológicos sin descubrir que un cibercriminal puede aprovechar.

Mitigación M1051 - Update Software

Relacionada con los posibles impactos derivados de una infraestructura tecnológica obsoleta o que no cuenta con los últimos parches de actualización ofrecidos por los fabricantes.

Mitigación M1020 - SSL/TLS Inspection

Relacionada con las configuraciones de tráfico de red que pueden ser modificadas para actividades malintencionadas.

Mitigación M1038 - Execution Prevention

Relacionada a la protección y prevención de la ejecución de código malicioso.

Reglas

El Csirt Financiero compartió con los asociados un total de **253 reglas** entre **Yara** y **Sigma** que tienen como finalidad ser implementadas en herramientas de seguridad, facilitando y describiendo eventos de registros de seguridad informática que sean relevantes en la detección de comportamientos de amenazas cibernéticas. A continuación se relacionan las reglas generadas por mes:

ENERO

8 Reglas Yara
32 Reglas Sigma

Detección de ataques de fuerza bruta, parámetros típicos en ataques que utilizan PowerShell y detección de explotación de vulnerabilidades. Reglas para la detección de actividades maliciosas relacionadas a las familias de malware Spynote, Bizarro, Basbanke, Babuk, JSSLoader y Raindrop.

FEBRERO

14 Reglas Yara
2 Reglas Sigma

Detección de los troyanos bancarios Osiris, Wroba, RemcosRAT, Troyano Masslogger, Trickbot y actividades del APT Gamaredon.

MARZO

17 Reglas Yara
29 Reglas Sigma

Detección de explotación de la vulnerabilidad CVE-2021-26855 en servidores Exchange, reglas para la detección de actividades maliciosas relacionadas a las familias de malware ObliqueRAT, QakBot, Ploutus, Gootkit RAT, BazarLoader, Badhatsh, Nanocore y eventos relacionados con APT-C-36.

ABRIL

15 Reglas Yara
20 Reglas Sigma

Reglas para la detección de actividades maliciosas relacionadas a las familias de malware Phobos, Darkside, RemcosRAT, NjRAT, QuasarRAT, AsyncRAT, BRata y Dridex.

MAYO

2 Reglas Yara
12 Reglas Sigma

Reglas para la detección de actividades maliciosas relacionadas a las familias de malware Valyria, IcedID, Trickbot y Avaddon.

JUNIO

8 Reglas Yara
15 Reglas Sigma

Reglas para ayudar a la mitigación M1024 de Mitre y detección de las familias de malware GootKit e IcedID.

JULIO

6 Reglas Yara
15 Reglas Sigma

Reglas para ayudar a la mitigación M1038 de Mitre y detección de las familias de malware Ryuk, Ursnif, REvil, Bazar, Trickbot y Hancitor.

AGOSTO

9 Reglas Yara
9 Reglas Sigma

Reglas para la detección de actividades maliciosas relacionadas a las familias de malware MosaicLoader, IISpy, BitRAT, Karma, Blackmatter, Varsovia, Ursnif, Agent Tesla, OrcusRAT, Redline Stealer y Racoon Stealer.

SEPTIEMBRE

11 Reglas Yara
11 Reglas Sigma

Reglas para la detección de actividades maliciosas relacionadas a las familias de malware JsOutProx RAT, Snake Keylogger, Lockbit 2.0, Bazarloader, RemcosRAT, Chaos, Sova, AgentTesla, REvil, Maxtrilha y CobaltStrike.

OCTUBRE

8 Reglas Yara
1 Reglas Sigma

Reglas para la detección de actividades maliciosas relacionadas a las familias de malware Cring, ERMAC, Ranion, Numando, Formbook y MirrorBlast.

NOVIEMBRE

4 Reglas Yara
1 Reglas Sigma

Reglas para la detección de actividades maliciosas relacionadas a las familias de malware BazarLoader, ransomware Hellokitty, RemcosRAT y troyano Emotet.

DICIEMBRE

4 Reglas Yara

Detección de explotación de la vulnerabilidad Log4j (CVE-2021-44228) y ransomware Khonsari.

TENDENCIAS DE CIBERSEGURIDAD PARA 2022

PHISHING

1

Durante el año 2021 el Csirt Financiero analizó un total de 364 incidentes asociados con phishing.

Esta estrategia de ingeniería social puede llegar con más fuerza y renovada en el año 2022, teniendo en cuenta que se vale de diferentes métodos como el vishing (comunicación por voz), el whaling (suplantación de la identidad de un compañero de trabajo), el smishing (contacto a través de SMS), y el baiting (USB infectados con malware y abandonados en lugares públicos).

Técnicas que han crecido con fuerza en los últimos años y que cada vez son más creíbles y confiables.

RANSOMWARE DIRIGIDO

2

Malware en constante evolución que sigue siendo una de las mayores preocupaciones de las empresas. Para el año 2021 se evidenció su uso cada vez más sofisticado y especializado, incorporando técnicas de evasión y distribución en fases.

Debido a los esfuerzos que vienen realizando las empresas para combatir esta amenaza, los cibercriminales han cambiado el enfoque de sus campañas generalizadas a operaciones dirigidas hacia objetivos puntuales.

Para el año 2022 se prevé el aumento de esta amenaza, debido al teletrabajo, el crecimiento de las actividades desarrolladas en línea y en entornos digitales, generando oportunidades de ataque y grandes beneficios económicos para los ciberdelincuentes.

RIESGOS EN LA NUBE

3

La llegada del Covid-19 condujo a que las empresas aprovecharan más el uso de servicios en la nube, situación que también es utilizada por los ciberdelincuentes. El uso de PaaS (Platform as a Service), SaaS (Software as a Service) y soluciones IaaS (Infrastructure as a Service), hace que se incremente el número de objetivos de ataques informáticos a sistemas en la nube, aumentando así la superficie de ataque.

AUMENTO DE TROYANOS EN DISPOSITIVOS MÓVILES

4

En el año 2021 se evidenció una tendencia en el incremento de troyanos bancarios dirigidos a dispositivos Android, orientados a diferentes regiones como Europa, América Latina y Medio Oriente, identificando varias familias como RealRAT, Coper, Bian, SMisor, Ubel, TwMobo, BRata y BasBanke, que apuntaron activamente a usuarios móviles.

Estas campañas generalmente suelen estar acompañadas de actividades de ingeniería social mediante las cuales, a través de llamadas, se amenaza a las víctimas y se envía un mensaje de texto diseñado con un enlace de descarga que contiene un archivo APK malicioso.

Lo anterior, se prevé como tendencia para el 2022, toda vez que la banca móvil ha sido adoptada masivamente en todo el mundo, en parte por la pandemia; siendo un medio muy utilizado para la realización de transacciones en línea por los usuarios y empresas.

5 EL USO DE LA BANCA ABIERTA (OPEN BANKING)

Sistema que brinda a los proveedores de servicios financieros acceso abierto a la banca de consumo, transacciones y otros datos financieros, permitiendo la conexión en red de cuentas y datos entre diferentes instituciones para uso de consumidores, instituciones financieras y proveedores de servicios externos.

La incorporación de este servicio se debe al uso de interfaces de programación de aplicaciones (API), que permite la integración de productos y servicios de manera segura; sin embargo, es importante resaltar que el uso de las API puede convertirse en un vector de ataque de mayor relevancia para los cibercriminales.

Según reporte generado por la empresa **Gartner**, el 90% de las aplicaciones web serán más vulnerables a los ataques a través de API expuestas.

Asi mismo, en un informe publicado por la empresa de seguridad **Salt Labs**, se indica que el tráfico en las API aumentó más del 140% en el primer semestre del año 2021, mientras que el tráfico malicioso de API se incrementó mucho más rápido, llegando casi al 350%.

6 MALWARE EN CAJEROS AUTOMÁTICOS

Los ataques a los cajeros automáticos presentaron una notable disminución debido a las restricciones generadas por la pandemia, toda vez que el aislamiento obligó a las personas a quedarse en sus casas y realizar las compras en línea; sin embargo, a medida que se levantan las restricciones y se retorna a la presencialidad, es posible que se presente incremento de campañas dirigidas a los cajeros automáticos.

ATAQUES DE FUERZA BRUTA A CLIENTES RDP

7

Para el año 2022 se prevé un incremento en los ataques de fuerza bruta, principalmente porque desde la pandemia se han publicado equipos hacia internet, exponiendo servicios como el de escritorio remoto. Para evitar estos ataques es importante que las empresas adopten medidas para proteger los accesos remotos, como por ejemplo utilizar doble factor de autenticación.

TENDENCIAS TECNOLÓGICAS PARA EL SECTOR 2022

Visión de las nuevas tecnologías que pueden llegar a desplegarse en el sector, creando nuevas sensaciones en los clientes; incluso mejorando los servicios bancarios, pero a la vez también, generando nuevos riesgos y amenazas.

1

El Metaverso Financiero

Un mundo digital creado en 3D dónde los clientes pueden interactuar con los agentes bancarios a través de una realidad virtual más próxima, más placentera sin limitaciones físicas para realizar su actividad económica.

El entorno traerá nuevas tecnologías de software y hardware, además, de la creación de avatares en el ciberespacio para realizar nuestra actividad, llevando la identificación digital a otro nivel.

Este nuevo ecosistema se desarrolla gracias a las nuevas tecnologías que llegarán en relación a la computación espacial, la creación de nuevos y más atractivos entornos virtuales y el aumento de la economía virtual.

Sin duda, en los próximos años el sector puede dar un salto muy relevante si todas estas tecnologías terminan de implementarse en los nuevos modos y usos de la sociedad.

Tokens no fungibles

Inspirados en el valor subjetivo derivado de los bienes artísticos, que son irremplazables e indivisibles; aparecen este tipo de tokens que están revolucionando algunos sectores como el del arte, el gaming o incluso ya el inmobiliario, creando ecosistemas económicos alternativos.

Desarrollados con tecnología blockchain siguen en la línea de ser considerados activos digitales. Si bien el último año creció un 300% su uso, está por ver si finalmente penetra en más sectores, como por ejemplo el financiero. Algunos usos que se le podría dar están relacionados con la gestión de la inversión, compra-venta de deuda, etc.

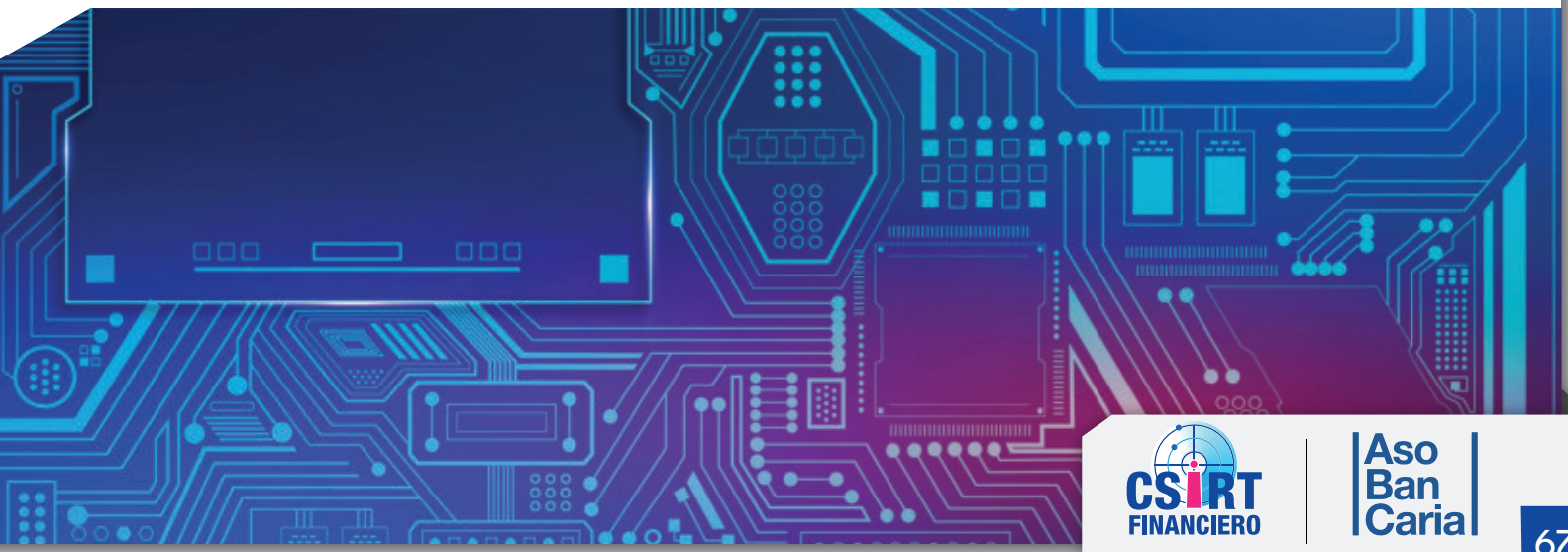
2

3

5G y 6G, un salto en la comunicación digital

En el mundo de las telecomunicaciones hemos vivido las distintas generaciones de conectividad móvil y actualmente se está desplegando ya el famoso 5G, el cual permite una velocidad muy superior de las transacciones de datos 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.

Sin embargo, a pesar de que el 5G todavía no está completamente desplegado y aún está por ver la utilidad que le damos; el 6G ya se está desarrollando actualmente, siendo los primeros países que desean experimentar con ella Corea del Sur y China. De nuevo, un paso más en la reducción de latencia nos llevará a un escenario donde se podrá desarrollar por completo gran parte de las capacidades de la inteligencia artificial, así como, por ejemplo, otras novedades casi de ciencia ficción como la proyección holográfica.



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

Aso Ban Caria