CSIRT FINANCIERO

MEMORIA ANUAL 2020

MAYO DE 2021

ASOBANCARIA

Construyendo la **Confianza** y **Solidez** del sector financiero

Indice

Apertura del CSIRT

Mónica María Gómez Villafañe
Vicepresidenta Administrativa y Financiera de Asobancaria

Responsable del Programa gremial de cooperación para la ciberseguridad del sector financiero - CSIRT Financiero -

CSIRT Financiero: Construyendo la confianza para el intercambio de información de amenazas cibernéticas

En su primer año de operación, el CSIRT Financiero de Asobancaria sigue creciendo y consolidando su trabajo para prevención de riesgos cibernéticos de forma colaborativa y sectorial. A la fecha participan en la comunidad, entidades financieras e infraestructuras críticas de la industria cuyos activos representan el 80% del sector. Nuestros miembros no solo representan a las entidades bancarias sino al ecosistema financiero de forma integral, unidos en una gran alianza para fortalecer las capacidades de respuesta frente a las crecientes amenazas cibernéticas derivadas de una operación bancaria cada vez más digital.

El CSIRT (Equipo de Respuesta a Incidentes Cibernéticos del Sector Financiero) es una herramienta idónea de trabajo gremial para reaccionar oportuna y eficazmente a los incidentes digitales de forma altamente técnica, centralizada y especializada. El Centro de Operaciones cuenta con tecnología de vanguardia, desarrollos propios para el procesamiento de datos y fuentes de información globales para realizar un seguimiento de manera unificada a las principales tipologías de riesgo cibernético en el sector. Estas capacidades permiten desarrollar actividades reales de interacción con los diferentes fabricantes, organismos internacionales, agencias de investigación y autoridades; y entregar un acompañamiento continuo y proactivo a las entidades asociadas en el acelerado proceso de transformación digital.

Durante el 2020, el equipo técnico de CSIRT Financiero, tras continuas actividades de investigación y monitoreo digital, entregó a las entidades financieras más de 180 alertas sobre riesgos tecnológicos a nivel global y local, relacionados con tipologías asociadas a la pandemia de COVID 19, al trabajo remoto y a la generalizada operación virtual en el mundo. El

monitoreo constante del equipo técnico CSIRT realizado en 7x24, detecta actividades maliciosas antes de que puedan causar un daño a la entidades y alerta oportunamente para tomar las medidas de prevención necesarias.

Para la entrega oportuna de esta información a los asociados, se automatizó el intercambio de información bajo los más altos estándares internacionales, a través de la Plataforma Global de Inteligencia de Amenazas MISP (Malware Information Sharing Platform), que incluye mecanismos de correlación de información y la constitución de un nodo o segmento de información propio del sector financiero colombiano. Compartir es clave para la detección rápida y eficaz de amenazas, no podemos olvidar que a menudo, organizaciones similares son el objetivo del mismo actor. Este proceso garantiza a los equipos de respuesta de las entidades asociadas la detección oportuna de las nuevas vulnerabilidades reportadas por la comunidad para llevar a cabo acciones de inteligencia, promoviendo así la estabilidad del sistema y por ende la seguridad de los usuarios.

En el 2020, CSIRT Financiero fue certificado por la Comunidad global FIRST (Global Forum of Incident Response and Security Teams) con el sello de calidad de liga global de equipos de respuesta a incidentes de mayor relevancia a nivel internacional, conformada por centros de investigación de referencia para la prevención de amenazas y reacción rápida a incidentes cibernéticos en 96 países, con lo cual garantizamos la continua excelencia operacional y técnica del equipo.

En 2021 continuaremos el trabajo gremial para el despliegue de las capacidades del CSIRT 2.0 y la generación de información, alertas y recomendaciones para la gestión del riesgo cibernético. Se extenderán y profundizarán las actividades con entidades financieras internacionales para la adopción de mejores prácticas, así como los foros de discusión con expertos para la prevención de riesgos del ecosistema, el manejo de riesgos de terceros críticos, y la divulgación de aquellas iniciativas de los miembros que busquen las capacidades en ciberseguridad para soportar operaciones bancarias seguras e innovadoras.

Desde Asobancaria, agradecemos a los responsables estratégicos y técnicos de ciberseguridad de las entidades financieras como líderes de este programa, a las autoridades nacionales, a los organismos multilaterales y a los demás aliados que hacen parte de esta comunidad, por el apoyo continuo y su voluntad de colaboración para la consolidación del CSIRT como Centro sectorial para la prevención del riesgo cibernéticos del ecosistema financiero.

Estamos convencidos que entre más rápido se comparte una amenaza o vulnerabilidad, más posibilidades tienen otras entidades de poner en marcha las defensas para mitigarla. Compartiendo información de forma oportuna, generamos un marco de ciberdefensa colectiva para proteger a los clientes, la infraestructura y el ecosistema digital. Es de vital importancia que recordemos que en materia de seguridad no somos competencia, por el contrario, somos aliados.

Introducción CSIRT Financiero

Carlos Javier Beltrán Camacho
Coordinador Operacional CSIRT Financiero

Es conocido que el mundo cambia de forma vertiginosa, razón por la cual el CSIRT Financiero no puede ser la excepción, y por ello está implementando nuevas estrategias que nos permitan estar a la vanguardia de la ciberseguridad, lo que nos va a dar la oportunidad de compartir con todos ustedes información de prospectiva y de analítica, con el fin de anticiparnos a las múltiples amenazas cibernéticas que van evolucionando con el paso del tiempo.

Cabe recordar las palabras del criptógrafo, experto en seguridad informática, y escritor, Bruce Schneier:

"El hardware es fácil de proteger: encerrarlo en una habitación, encadenarlo a un escritorio o comprar uno de repuesto. La información plantea más un problema. Puede existir en más de un lugar; ser transportado a la mitad del planeta en segundos; y ser robado sin su conocimiento".

El señor Schneier refleja la necesidad real de pensar en los peligros que se desafían al momento de preservar la seguridad de la información. Es aquí, en este punto fundamental, en el que a diario los ciberdelincuentes están mejorando sus técnicas y tácticas para robar nuestra información y afectar nuestro bienestar, valiéndose de herramientas bien estructuradas que les permiten dar golpes certeros que afectan directamente a la economía.

Por consiguiente, nos vemos inmersos en un mundo donde la amenaza es latente y se encuentra al acecho en todos lados, en busca de potenciales víctimas, que con el simple hecho de dar clic o seguir un hipervínculo enviado dentro de un mensaje de correo electrónico, está siendo el blanco perfecto de los ciberdelincuentes, con el fin de implantar malware, que más adelante podría convertirse en un secuestro de información, donde solicitan grandes sumas de dinero para devolver la información afectada.

De acuerdo a lo anterior, se avecina para este 2021, una serie de ataques cibernéticos, aún más fuertes y sofisticados que los anteriores, pues a raíz de esta pandemia que estamos viviendo por cuenta de la COVID-19, los ciberdelincuentes han utilizado su tiempo para mejorar sus técnicas de ataque. Veremos un contexto de ataques dirigidos y sofisticados sin precedentes, toda vez que estos grupos, van a seguir

aprovechando la coyuntura en que nos encontramos para centrar sus ataques a infraestructuras críticas y causar el mayor daño posible, tal y como lo vimos a finales de 2020 con este gran ciberataque a la cadena de suministro SolarWinds Orion, por medio de la cual y a través de un trabajo minucioso y estructurado, lograron impactar a miles de empresas a nivel mundial.

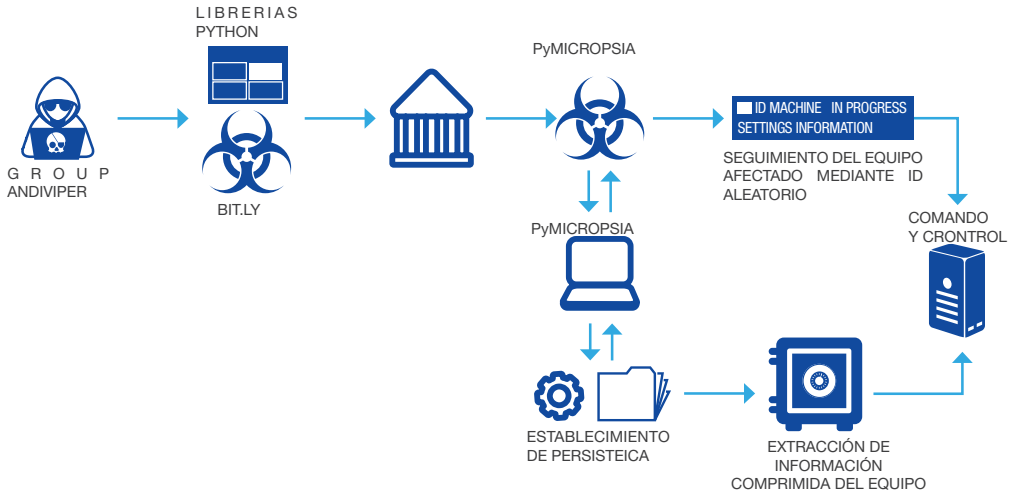
Estos nuevos escenarios conllevan a que generemos esfuerzos conjuntos y de cooperación, que nos permitan anticipar y mitigar este tipo de ataques en nuestras infraestructuras tecnológicas, pero esto sólo se logra con una adecuada articulación, lo que permitirá generar estrategias sólidas y contundentes frente a este tipo de riesgos, que día a día, vienen creciendo de forma acelerada y que buscan causar el mayor daño posible.

Se observa un ecosistema de ciberamenazas que evoluciona constantemente, este es el caso del malware bancario, el cual para finales de 2020, tuvo una representación del 59%, dentro de los que se destacan troyanos como PyMicropsia, diseñado para ejecutarse en ambientes Windows. El malware tiene la capacidad de infectar y exfiltrar información confidencial de los usuarios, como contraseñas de cuenta y datos para acceso a cuentas bancarias online, ejecuta diversas funciones que demandan elevado consumo de recursos del sistema y recopila cookies de los navegadores web.

Además de esas acciones, este troyano establece conexión con servidores comando y control C2 a quienes envía los datos recopilados. Desde esta conexión, se permite descargar e instalar otras familias de amenazas cibernéticas para causar mayor impacto en los equipos vulnerados, información que puede ser consultada a través del apartado de modelado del evento de nuestros informes sobre amenazas.

Modelado del evento

En la imagen se observa el proceso de infección ejecutado por PyMICROPSIA y cómo transmite la información sensible al servidor C2.



Las nuevas amenazas adaptadas son, hoy y en el futuro, el foco de atención por parte del CSIRT, especialmente aquellas que han evolucionado y se han acomodado a las circunstancias del sector y de sus clientes. Mediante las investigaciones se ha demostrado que el rumbo de los actores y originadores de este tipo de acciones, pasan por la fabricación y desarrollo localizado en Colombia.

Cada vez con más mayor periodicidad se muestran nuevos escenarios en los que, el malware financiero, viene ampliando su accionar delictivo. Estos nuevos escenarios van acompañados de diferentes técnicas, tácticas y procedimientos (TTP) que son investigadas por el CSIRT Financiero, para poder desarrollar nuevos mecanismos de análisis y descubrimiento de esquemas locales de información asociados a este tipo de amenazas.

Por otra parte, es para nosotros muy importante contar con su apoyo y aporte en esta dinámica de atención de incidentes, puesto que tanto ustedes como nosotros, debemos estar alineados a las diferentes estrategias, que nos permitan mitigar todos aquellos escenarios de riesgo, que puedan llegar a comprometer tanto la infraestructura tecnológica como la seguridad de la información. Por consiguiente, los invito a fortalecer nuestros lazos de amistad de forma efectiva, lo que nos va a permitir, sin lugar a dudas, obtener resultados óptimos y acertados para afrontar los retos de cara a un mundo que se transforma digitalmente cada día.

Por último, estimados asociados, desde la Coordinación del CSIRT Financiero, estamos a su entera disposición, con el fin de atender, asesorar y ayudar a resolver las inquietudes que se generen de cara a todos los entregables que día a día son analizados, investigados y diseñados para ser enviados a ustedes, quienes son nuestra razón fundamental de todo el ejercicio que desarrollamos con nuestro equipo de trabajo. Por lo anterior, los invito a que participemos activamente en la construcción de un equipo interinstitucional que nos permita afrontar todos los retos que la ciberseguridad nos pone sobre el camino y que se presentan en el panorama del CSIRT Financiero.

Resumen Ejecutivo

A lo largo de 2020 el CSIRT Financiero ha trabajado constantemente para identificar todas aquellas ciberamenazas que han rodeado al sector financiero y que han puesto en riesgo la integridad de las entidades; todo esto en un panorama de constante cambio y adaptación.

Desde los tres pilares fundamentales del CSIRT Financiero, el Observatorio de Ciberamenazas, la Inteligencia de Amenazas y el Apoyo a Incidentes, el equipo de analistas ha podido analizar pormenorizadamente las ciberamenazas con el objetivo de ofrecer una comprensión de las mismas así como una férrea defensa que pueda llegar a evitar diversas categorías de incidentes de seguridad en entidades del sector financiero.

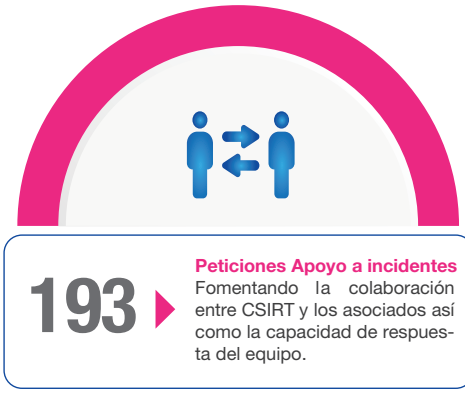
De esta manera, a lo largo de 2020 el CSIRT Financiero ha realizado los siguientes trabajos a disposición de los asociados:

510 **Documentos generados**
Lo que corresponde a Boletines Mensuales, nformes Monográficos de Amenazas, Alertas, Playbooks y Case Study.

510 **Alertas realizadas**
Las 510 alertas se enmarcan dentro del pilar del Observatorio de Ciberseguridad.

5.884 **IOCS Suministrados**
Los IOCs suministrados corresponden en su mayoría a troyanos y grupos APT que afectan al sector financiero.

48 **Alertas inteligencia de amenazas**
Con la función de prevenir ciberamenazas respecto al sector financiero.



193 **Peticiones Apoyo a incidentes**
Fomentando la colaboración entre CSIRT y los asociados así como la capacidad de respuesta del equipo.

61 **Reglas**
Repartidas entre 1 8 reglas YARA y 43 reglas Sigma.

6 **Playbooks y Case Study**
Divididos en 5 Playbooks y 1 Case Study disponibles para los asociados.

Existen muchas ciberamenazas que han tenido lugar en este 2020, 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 en alertas, boletines, informes o monográfico y se recogen a continuación:

- Sofisticación e incremento de campañas relacionadas con troyanos bancarios brasileños cuyo método de distribución ha sido correos electrónicos de phishing con un archivo adjunto .pdf o .zip.
- Incremento de los incidentes de ransomware relacionados con un nuevo modus operandi entre los cibercriminales donde realizan una doble extorsión contra las víctimas. Por consiguiente, la exfiltración de información confidencial ha sido una de las consecuencias más identificadas a lo largo del 2020.
- Campañas que emplearon el RAT AsyncRAT que, tras el análisis por parte del equipo de analistas del CSIRT Financiero, se pudo atribuir con cierta solidez a una campaña llevada a cabo por la APT-C-36, un grupo de cibercriminales identificados entre 2018 y 2019 actuando en Colombia,

entre otros sectores, dentro del sector financiero.

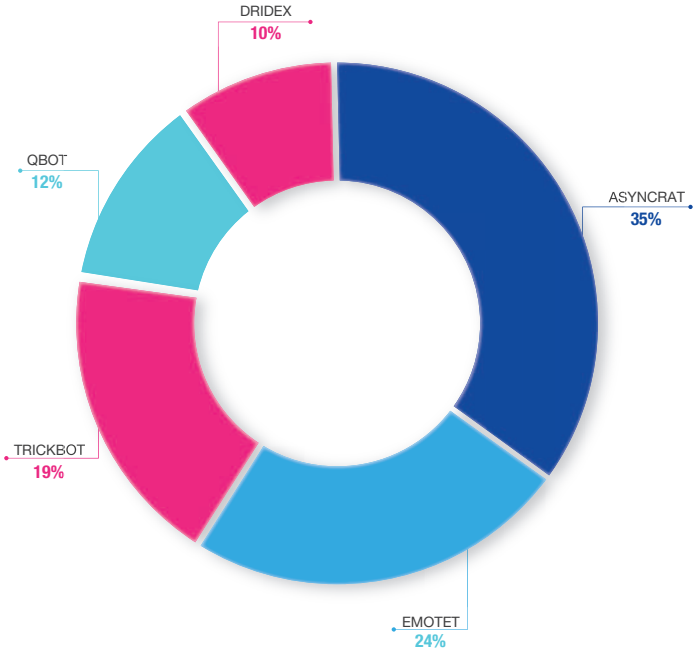
- Incremento en el desarrollo de malware contra dispositivos móviles, especialmente aquellos destinados a la captación de datos confidenciales como credenciales bancarias. Este hecho viene ligado al incremento a nivel mundial del uso de aplicaciones bancarias en dispositivos móviles y el incremento del e-commerce producido por la situación de confinamiento de la Covid-19.

- Las APT (Advanced Persistent Threat) con motivación financiera han seguido muy presentes sobre las entidades del sector financiero, pudiéndose destacar campañas de APTs ya conocidas y tratadas en el CSIRT Financiero como Lazarus, FIN7 o Silence, así como campañas de grupos nuevos enmarcados en el Crime-as-a-Service (CaaS) como DeathStalker.

- Los niveles de fraude se han visto incrementados debido a la constante proliferación de campañas de phishing, estafas y desarrollo del CaaS que los cibercriminales han llevado a cabo a lo largo de 2020 como un nuevo modelo de negocio. Se han podido identificar una multitud de productos vendidos en markets de la Deep Web y Darknet que pueden afectar directa o indirectamente a entidades del sector financiero como venta de logs, accesos RDP, venta de credenciales, venta de ransomware dirigido, kits de phishing, troyanos bancarios y un largo etc.

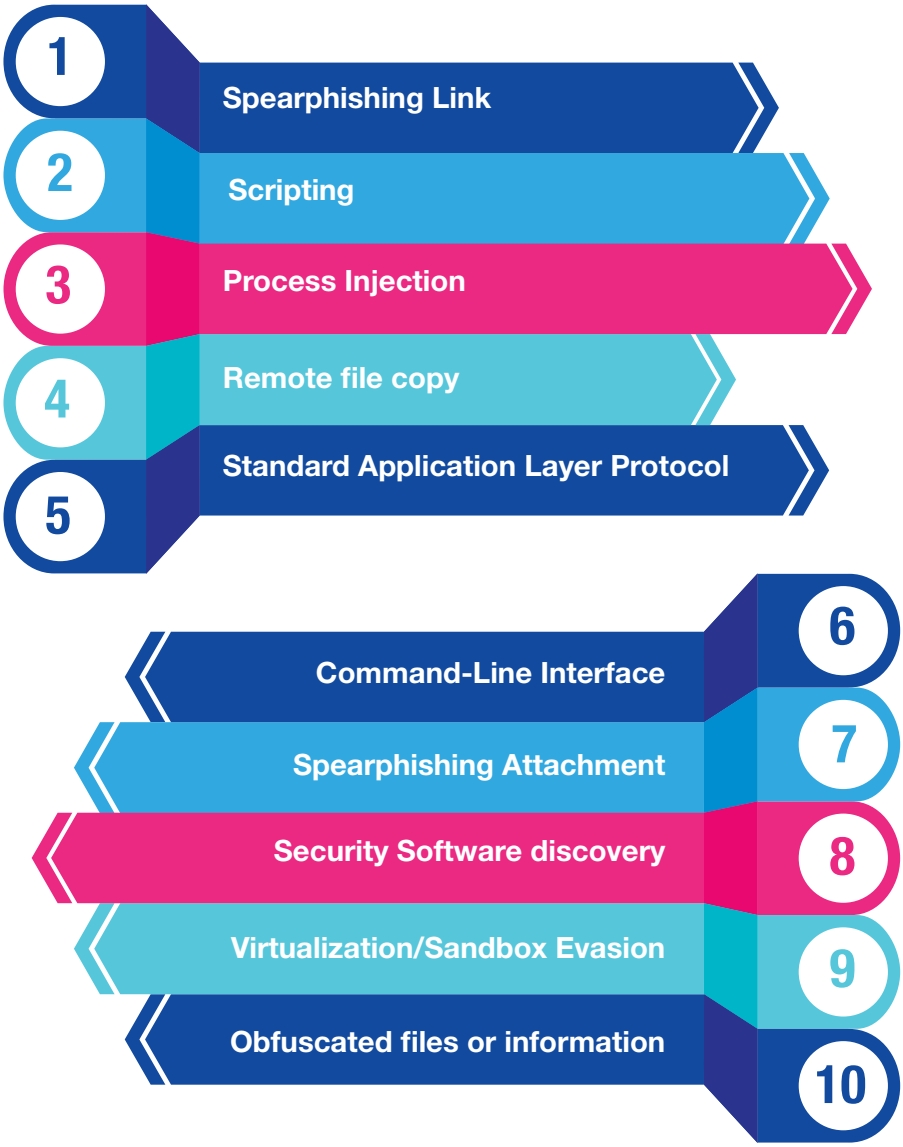
- En este sentido, las principales familias de malware que el equipo de analistas del CSIRT Financiero ha analizado son las siguientes:

Principales familias analizadas



Por último, el siguiente gráfico presenta las 10 TTP (Técnicas, Tácticas y Procedimientos) más relevantes para el sector financiero basados en la matriz MITRE | ATT&CK de acuerdo con el análisis realizado por el equipo del CSIRT financiero desde los inicios del CSIRT en 2020. 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 técnicas MITRE 2020:



CSIRT Financiero en 2020

Top Amenazas por Mes

ENERO
- Malware bancario 47%
- Ransomware 19%
- Spyware 19%
- APT 9%
- Downloader 6%

FEBRERO
- Malware bancario 53,4%
- Phishing 22,41%
- RAT 15,52%
- APT 5,17%
- Ransomware 3,45%

MARZO
- Malware bancario 38,6%
- Phishing 22,7%
- Ransomware 15,9%
- APT 13,6%
- RAT 9,09%

ABRIL
- Malware bancario 31%
- Phishing 31%
- Vulnerabilidades 19%
- Malware móvil 12%
- APT 8%

MAYO
- Phishing 41%
- Malware 37%
- Vulnerabilidades 12%
- APT 6%
- Malware Android 4%

JUNIO
- Malware 61%
- Incidentes 16%
- Phishing 16%
- Malware Android 4%
- APT 3%

JULIO

- Malware 60%
- Phishing 21%
- APT 11%
- Malware Android 6%
- ATM 2%

AGOSTO

- Malware 37%
- APT 20%
- Phishing 20%
- Vulnerabilidad 15%

SEPTIEMBRE

- Malware 50%
- Vulnerabilidad 15%
- APT 13%
- Malware Android 11%
- Phishing 11%

OCTUBRE

- Malware 52%
- Vulnerabilidad 23%
- APT 13%
- Malware Android 8%
- Phishing 4%

NOVIEMBRE

- Malware 43%
- Vulnerabilidad 37%
- Incidente 6%
- APT 6%
- ATM 5%

DICIEMBRE

- Malware 54%
- Vulnerabilidad 16%
- Incidente 11%
- APT 7%
- Malware Android 7%
- Phishing 5%

El 2020 ha sido un año marcado por situaciones nuevas y desconcertantes que se han dado en todos los sentidos, incluido en el mundo cibernético. El mundo se paró durante unos meses, pero este parón puso en marcha un avance tecnológico a una velocidad inimaginable.

Las medidas de seguridad impuestas para frenar el nivel de contagios se han convertido en una forma de vida, nuestro hogar se convirtió en el centro total y absoluto de nuestro día a día, en un aislamiento ficticio, ya que ahora, más que nunca, estamos hiperconectados.

La implementación del teletrabajo a través de sistemas remotos, de manera forzosa y precipitada, por las medidas de confinamiento, ha generado que la superficie de ataque sea mucho mayor y se encuentre menos protegida, situación que aprovechan los ciberdelincuentes para robar datos, generar ganancias y causar interrupciones.

Por otro lado, la pandemia también ha cambiado la forma de consumir, sustituyendo las compras físicas de cualquier producto por la compra online, aumentando considerablemente el número de usuarios y, por lo tanto, el número de posibles víctimas de ciberdelitos.

Ello conlleva también cambios en los medios de pago, incrementándose el uso del e-commerce. En Colombia, según los datos arrojados por el Ministerio de las TIC y de la Cámara Colombiana de Comercio Electrónico (CCCE), en abril, primer mes de la cuarentena, el ***e-commerce*** se incrementó en un 73 por ciento[1].

Pero no sólo ha cambiado la forma en la que consumimos o pagamos, cualquier operación bancaria, gestión o papeleo administrativo se ha implementado en su versión online, por lo que las entidades financieras han iniciado una revolución tecnológica imparable, para poder dar servicio a sus clientes y aumentar las medidas de seguridad frente a los ciberataques.

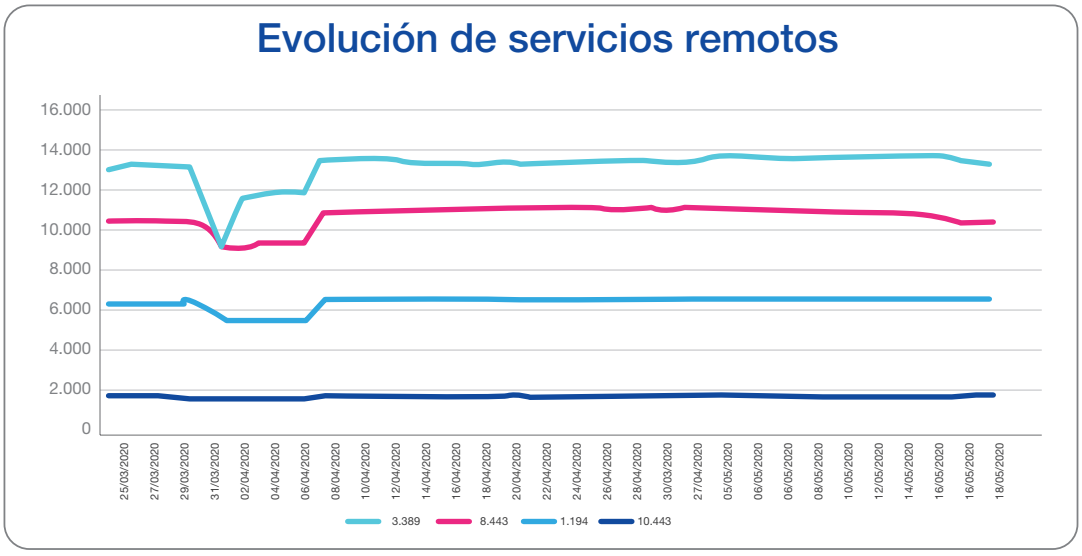
El **CSIRT Financiero** estuvo realizando un **estudio** sobre cómo los **servicios de protocolos remotos**, iban aumentando o disminuyendo durante aproximadamente dos meses de pandemia, teniendo como punto de partida el 25 de marzo y finalizando el 18 de mayo.

Los **puertos** que fueron fruto de la **investigación** son aquellos que, por lo general, tienen **mayor relación con el trabajo remoto**, siendo los siguientes:

Puerto	Servicio	Descripción
3389	RDP	Se trata del protocolo de acceso remoto que incorpora Microsoft Windows en sus sistemas operativos. Este protocolo ha sufrido vulnerabilidades graves.
8443	-	Se trata de un puerto usado para la verificación SSL de conexiones mediante VPN.
10443	-	Se trata de un puerto usado para la verificación SSL de conexiones mediante VPN.
1194	OpenVPN	Es el puerto que usa por defecto OpenVPN por UDP para establecer conexiones.

La evolución durante las semanas que iban transcurriendo del **confinamiento** y que imposibilitaba salir a las personas de sus casas, tuvo por lo general un **incremento** en el uso de estos puertos, ya que las organizaciones iban **habilitando el teletrabajo** de manera creciente.

Existe un pico de bajada de servicios el día 1 de abril en todos los puertos. Este hecho, es probable que esté relacionado con algún tipo de fallo en algún proveedor de Internet de Colombia, ya que durante los siguientes días volvieron los valores normales.



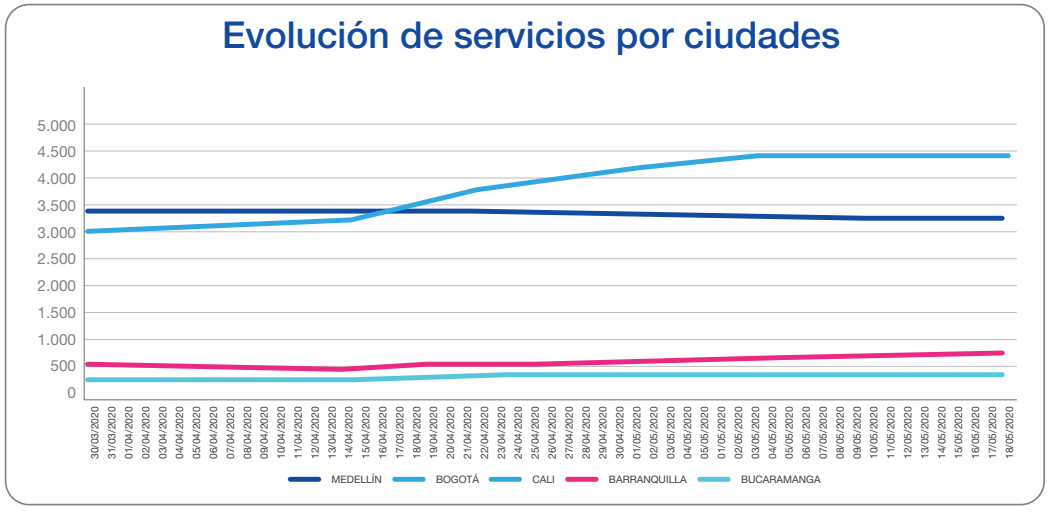
Durante la última semana existen días donde los valores bajaron, y otros subieron. Este hecho puede ser normal, ya que en una primera instancia las organizaciones tuvieron que, de manera rápida, habilitar servicios, en muchos casos, sin implementaciones de seguridad, simplemente por conseguir que sus líneas de negocio no se vieran interrumpidas. Sin embargo, a medida que el tiempo avanzaba, es normal que muchos de estos servicios se fueran deshabilitando por algunos de los siguientes motivos:

- **Adquisición de nueva tecnología para el trabajo desde casa**, permitiendo de esta manera cerrar servicios que potencialmente están más expuestos a la explotación de vulnerabilidades, como es el caso del puerto 3389 relacionado con el protocolo RDP.
- **Estabilización de servicios expuestos** para minimizar la explotación de vulnerabilidades y superficie.
- Implementación de **mecanismos de seguridad**, dando puertos cerrados, en algunos casos, cuando en realidad están abiertos.

Toda esta evolución de protocolos tuvo un **gran impacto** principalmente en **Bogotá**, ya que desde el inicio del estudio hasta el final del mismo, **incrementó sus servicios expuestos** en más de la mitad, un **54,82%**.

Sin embargo, se observa que fue **Medellín donde se inició** esta exposición de servicios públicos, aunque finalmente su registro **fue decreciendo**, teniendo un 3,87% de servicios expuestos que en el inicio.

Medellín es el núcleo industrial y de emprendimiento de Colombia, por lo que probablemente, fueron los primeros en implementar en trabajo desde casa de forma rápida, sin embargo, a medida que transcurrieron los días, y debido a que es una ciudad más avanzada tecnológicamente que Bogotá, reforzaron la seguridad de sus puertos, haciendo que sus registros de exposición fueran decreciendo con el paso del tiempo.



Tipos de ataques producidos durante la crisis sanitaria mundial[2]

Spam y phishing:

Los cibercriminales explotaron la situación de incertidumbre y caos generado por la pandemia para elaborar campañas de phishing suplantando a la entidades gubernamentales, autoridades sanitarias o, simplemente, enviando correos con temática COVID para lograr engañar a las víctimas.

Explotación de vulnerabilidades:

El rápido proceso de implantación del trabajo en remoto, ha generado que las empresas vean diluidas sus fronteras de ciberseguridad, recayendo la responsabilidad de mantener las barreras levantadas, en los empleados. Situación que han aprovechado los actores maliciosos mediante la explotación de vulnerabilidades.

Malware de recolección de datos:

Utilizando información relacionada con COVID-19 como señuelo, los ciberdelincuentes utilizaron troyanos de acceso remoto y troyanos bancarios para el robo de datos y dinero, comprometer redes, o construir botnets con fines maliciosos.

Malware disruptivo (ransomware y DDoS):

Utilizan cada vez más malware contra la infraestructura crítica y las instituciones sanitarias, debido al potencial de alto impacto y beneficio financiero. En las dos primeras semanas de abril de 2020, hubo un aumento en los ataques de ransomware por múltiples grupos de amenazas que habían estado relativamente inactivos durante los últimos meses.

Dominios maliciosos:

Hubo un aumento significativo de nombres de dominio que contienen palabras clave, como “coronavirus” o “COVID”. Estos sitios web fraudulentos sustentan actividades maliciosas que incluyen servidores C2 y distribución de malware y phishing. De febrero a marzo de 2020, se registró un crecimiento del 569% en registros maliciosos.

Tendencias generadas por la covid-19

Cuando los empleados de una planta industrial volvieron al lugar de trabajo tras su cierre durante la pandemia de COVID-19, notaron algunas diferencias. Se utilizaron sensores o etiquetas RFID para determinar si los empleados se lavaban las manos con regularidad. La visión por ordenador permitía detectar si los empleados cumplían el protocolo de las mascarillas y se utilizaban altavoces para advertir de las infracciones del protocolo[3].

La recopilación y el uso de estos datos se denomina **Internet del Comportamiento** (IoB) y su finalidad principal es la de **utilizar los datos recopilados** para **cambiar comportamientos.** Una tendencia que seguirá presente en nuestras vidas mientras continúe la pandemia y que, probablemente, creará un precedente de aplicación futura.

La COVID-19 también justificó la creación de aplicaciones móviles de rastreo de contactos, impulsadas por los gobiernos de cada país. Son aplicaciones que, a través del móvil, registran las personas que se cruzan para determinar si existe riesgo de contagio, al detectar el móvil que el usuario estuvo cerca de alguien que más tarde ha confirmado estar infectado.

A través de la vulneración de este tipo de aplicaciones, los cibercriminales podrían acceder a ellas, robar datos, crear falsas alarmas de brotes falsos y acosar o chantajear a los usuarios.

¿Qué nos depara el 2021 en relación a la COVID-19 y la cibercriminalidad?

Las plataformas de videocomunicación seguirán siendo objetivo de ciberataques debido a la continuación del teletrabajo. 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.

Las estafas online y las campañas de phishing aumentarán, utilizando palabras clave relacionadas con el coronavirus y las vacunas.

Las farmacéuticas y empresas implicadas en el diseño y distribución de la vacuna contra la COVID-19 se convertirán en objetivo de ataques, para robar las patentes, información confidencial o cualquier otro tipo de dato que genere un retorno económico a los ciberdelincuentes.

El Bitcoin obtuvo una espectacular revalorización a principios del 2020, cuando comenzó a confirmarse el brote de coronavirus, convirtiéndose en uno de los activos más atractivos para invertir. Por ello, el robo de Bitcoin, será más atractivo a medida que muchos países caigan en la pobreza como resultado de la pandemia. Igualmente, el desplome de algunas economías, llevará a más personas a involucrarse en el cibercrimen como forma de obtener ingresos económicos.

[1] https://www.portafolio.co/opinion/editorial/covid-19-y-el-e-commerce-editorial-francisco-miranda-542396

[2] https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[3] https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/

Observatorio de Ciberseguridad

Troyanos bancarios

A lo largo de 2020, los ciberataques que han involucrado el uso de malware categorizado como troyanos bancarios, se han incrementado, tanto aquellos diseñados para afectar a ordenadores como los dirigidos contra dispositivos móviles.

Este hecho se ha visto impulsado, principalmente, por la situación de pandemia generada por la Covid-19, que ha acentuado la motivación económica de los cibercriminales, quienes de manera más o menos sofisticada, han buscado la manera de atacar a las entidades financieras en busca de un retorno económico.

Un aspecto para destacar en un año tan marcado por el incremento de ciberataques, ha sido la aparición de múltiples troyanos bancarios de origen brasileño, que han afectado a entidades financieras tanto en Latinoamérica como a nivel internacional.

Los troyanos bancarios brasileños han estado siempre presentes en el panorama cibercriminal, sin embargo, a lo largo de este año, se ha identificado una notable incremento en su uso y una sofisticación en el desarrollo de estos malware, así como su manera de distribuirse y permanecer ocultos en los sistemas de las víctimas sin ser detectados.

Se ha podido evidenciar en el **"Informe de Amenazas: Troyanos brasileños"** cómo estos malware han sido desarrollados con mejores técnicas de ofuscación, anti-depuración, nuevos algoritmos de cifrado y comunicaciones más seguras, además de contar con una entrega en varias etapas. Dicho Informe de Amenazas se encuentra disponible para su consulta para todos los Asociados.

La mayor parte de las campañas identificadas compartían el método de **distribución**, siendo este un correo electrónico de **phishing** que generalmente tiene adjunto un archivo como pdf o zip. Después es común la existencia de descargadores que tienen una URL acortada, que redirige a un servicio de alojamiento, una tendencia al alza que se ha dado a lo largo de 2020.

El objetivo de los cibercriminales que emplean los troyanos bancarios brasileños es la misma que cualquier cibercriminal que lleve a cabo ciberataques contra entidades financieras a través de troyanos, a saber:

1. Robo de información interna de clientes y empleados
2. Robo de información bancaria
3. Robo de bases de datos

Además, tras varios análisis realizados a diversas muestras de esta tipología de malware, el equipo de analistas del CSIRT Financiero, ha podido comprobar cómo estos troyanos han adquirido un carácter reactivo, valorando previamente el entorno en el que se encuentran, esperando las circunstancias idóneas para comenzar sus tareas dentro del sistema comprometido.

En este aspecto, es necesario destacar troyanos brasileños como **Mekotio**, **Casbaneiro, Amavaldo, Grandoreiro, Guilma, Javalí, Lampion, Mispadu** y **Bizarro** entre otros, de los que se han reportado diversos incidentes de ciberseguridad a lo largo del año 2020.

La siguiente matriz de **MITRE ATT&CK** Enterprise muestra las técnicas que más han sido usadas por los diferentes eventos que se han desarrollado con alguna de las muestras de malware analizadas.

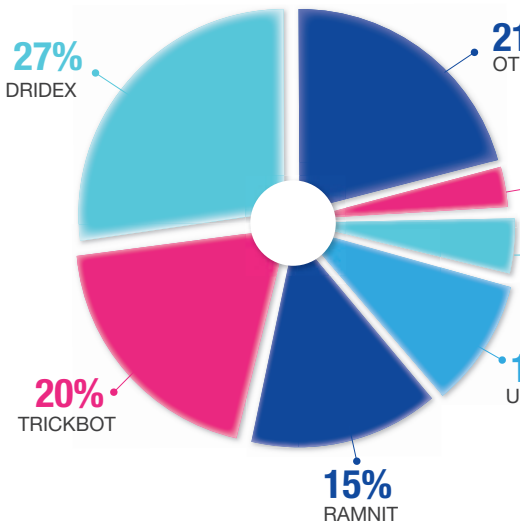
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Spearphishing Link	Scripting	Registry Run Keys / Startup Folder	Scheduled Task	Scripting	Input Prompt	Process Discovery	Remote File Copy	Input Capture	Standard Application Layer Protocol	Exfiltration Over Command and Control Channel	Account Access Removal
Spearphishing Attachment	User Execution	Browser Extensions	Access Token Manipulation	Deobfuscate/ decode files or information	Input Capture	System Information Discovery	Remote Service	Man in the Browser	Web Service	Data compressed	Data Destruction
Drive-by Compromise	Scheduled Task	Scheduled Task	Accessibility Features	Obfuscated Files or Information	Credentials from Web Browsers	Virtualization / Sandbox Evasion	AppleScript	Clipboard Data	Remote File Copy	Data Encryption	Data Encrypted for Impact
Exploit Public-Facing Application	Apple Script	bash_profile and bashrc	AppCert DLLs	Web Service	Account Manipulation	Security Software Discovery	Application Deployment Software	Screen Capture	Uncommonly Used Port	Automated Exfiltration	Defacement
External Remote Services	CMSTP	Accessibility Features	Appinit_DLLs	DLL Side-Loading	Bash History	Browser Bookmark Discovery	Component Object Model and Distributed COM	Video Capture	Custom Cryptographic Protocol	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Command-Line Interface	Account Manipulation	Application Shimming	Virtualization / Sandbox Evasion	Brute Force	Account Discovery	Exploitation of Remote Services	Audio Capture	Multi-Stage Channels	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	Bypass User Account Control	Masquerading	Credential Dumping	Application Windows Discovery	Internal Spearphishing	Automated Collection	Commonly Used Port	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Component Object Model and Distributed COM	Appinit_DLLs	DLL Search Order Hijacking	Access Token Manipulation	Credentials in Files	Domain Trust Discovery	Logon Scripts	Data from Information Repositories	Communication Through Removable Media	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Control Panel Items	Application Shimming	Dylib Hijacking	Binary Padding	Credentials in Registry	File and Directory Discovery	Pass the Hash	Data from Local System	Connection Proxy	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Dynamic Data Exchange	Authentication Package	Elevated Execution with Prompt	BITS Jobs	Exploitation for Credential Access	Network Service Scanning	Pass the Ticket	Data from Network Shared Drive	Custom Command and Control Protocol		Network Denial of Service
Valid Accounts	Execution through API	BITS Jobs	Emond	Bypass User Account Control	Forced Authentication	Network Share Discovery	Remote Desktop Protocol	Data from removable Media	Data Encoding		Resource Hijacking
	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Clear Command History	Hooking	Network Sniffing	Replication Through Removable Media	Data Staged	Data Obfuscation		Runtime Data Manipulation
	Exploitation for Client Execution	Change Default File Association	Extra Window Memory Injection	CMSTP	Kerberoasting	Password Policy Discovery	Shared Webroot	Email Collection	Domain Fronting		Service Stop
	Graphical User Interface	Component Firmware	File System Permissions Weakness	Code Signing	Keychain	Peripheral Device Discovery	SSH Hijacking		Domain Generation Algorithms		Stored Data Manipulation
	InstallUtil	Component Object Model Hijacking	Hooking	Compile After Delivery	LLMNR/NS Poisoning and Relay	Permission Groups Discovery	Thrid-party Software		Multi-hop Proxy		Transmitted Data Manipulation
	Launchctl	Create Account	Image File Execution Options Injection	Compiled HTML File	Network Sniffing	Query Registry	Taint Shared Content		Fallback Channels		System Shutdown / Reboot

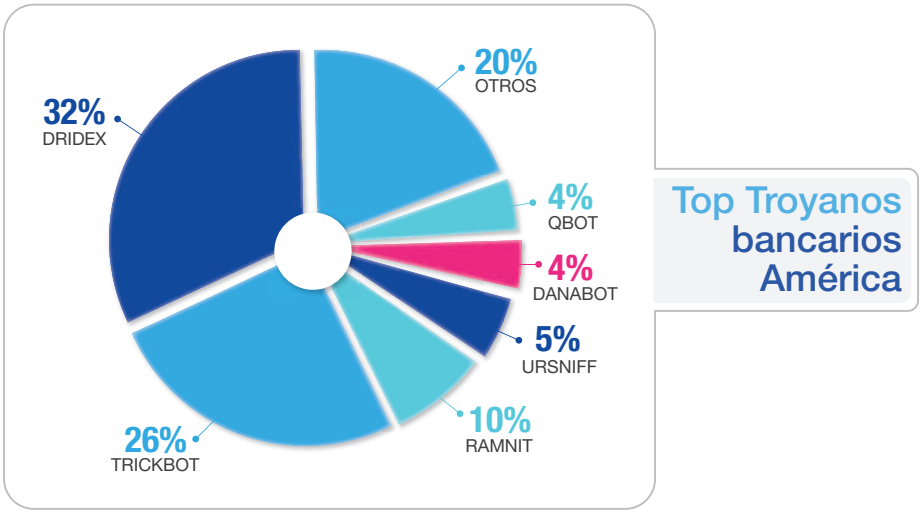
Es bastante probable que, por cuestiones tanto administrativas como de capacidad, **Brasil** albergue dentro de sus fronteras una serie de **grupos cibercriminales** que se encuentran **compartiendo conocimiento entre ellos**, desde diversos malware hasta nuevos vectores de infección y accesos a entidades ya comprometidas. Éstos a su vez, se comunican en foros de la Deep Web y Darknet con grupos cibercriminales de otras regiones como **Rusia**, de donde venden y adquieren nuevos conocimientos y capacidades.

Debido al impacto que han tenido las campañas que han involucrado el uso de troyanos bancarios brasileños, es plausible que a lo **largo de 2021** se sigan identificando **nuevos malware** que compartan **TTPs** con los anteriormente **mencionados**, y que, por tanto, su origen sea el mismo y todos destinados a **entidades financieras**.

Sin embargo, estos no son los únicos troyanos que han destacado a lo largo del año. Es necesario resaltar la permanencia de troyanos bancarios modulares como **Emotet** o **Trickbot**, que han continuado con una notable actividad, teniendo un importante impacto a nivel internacional tanto en entidades financieras como en otros sectores.

Top Troyanos bancarios Global





Por su parte, **Emotet** ha seguido desarrollándose como un **malware** polimórfico, dejando atrás su etapa de troyano bancario, abarcando entonces capacidades de descargar otros programas maliciosos tanto en el equipo comprometido como en la red donde se encuentra.

Actualmente este malware es uno de los mayores ejemplos de **Malware-as-a-Services** (MaaS) y **cooperación cibercriminal**, además de robar datos bancarios y confidenciales, **alquila los hosts infectados** a otros ciberdelincuentes como otro modelo de negocio[5].

El desarrollo del troyano bancario modular Trickbot ya le permitía, en 2019, operar como un malware modular en cooperación con otros malware como Emotet o el ransomware Ryuk. Su evolución le ha conferido la capacidad de ser más eficiente y adaptativo a todo tipo de entornos, pudiendo categorizar, en la actualidad, más como una botnet que como lo que fue en su origen, un malware bancario.

Dentro de sus servicios de MaaS, los cibercriminales tras Trickbot, ofrecen la posibilidad de realizar cryptojacking, ciberataques con diversos ransomware pasando por el clásico robo de datos, tanto bancarios como personales.

Si bien, es necesario destacar que, en la actualidad, tanto Emotet como Trickbot son empleados, principalmente, para proporcionar acceso a los cibercriminales y mantener la persistencia en las redes de las víctimas, más que como malware bancario[6].

La expansividad de esta botnet a través del Malware-as-a-Service le ha permitido tener una gran actividad a lo largo de 2020, especialmente en los meses de octubre y noviembre, habiéndose alcanzado un pico de 40.000 infecciones en un mismo día.

RATs

RAT hace referencia a herramientas que se pueden utilizar para **controlar y administrar de manera remota** (Remote Access Tool) algún sistema o dispositivo. Es decir, es software legítimo. Sin embargo, los **RAT utilizados de forma maliciosa** pueden representar un problema importante para la seguridad. Son troyanos que abren una puerta trasera en el equipo y pueden controlarlo, son los **llamados troyanos de acceso remoto.**

El software legítimo facilita en gran medida el trabajo de los cibercriminales. En primer lugar, porque algunas de estas **herramientas** son de **libre acceso**, lo que permite a los cibercriminales invertir en otras fases del ciberataque o recibir un mayor beneficio económico. Dicho esto, es importante entonces saber que los cibercriminales no tienen porqué tener muchos conocimientos de desarrollo.

En segundo lugar, permiten tener un amplio arsenal de herramientas que **dificulta detectar una característica común** en los ciberataques de un mismo grupo. Además, al ser software tan accesible, suele ser ampliamente compartido por diversos grupos, por lo que la **atribución de un ciberataque resultará más complicada.**

Por otra parte, la legitimidad de estas herramientas **dificulta la detección de la intrusión** debido a que los motores de antivirus y antimalware no detectarán que la actividad que se produce es de carácter maliciosa.

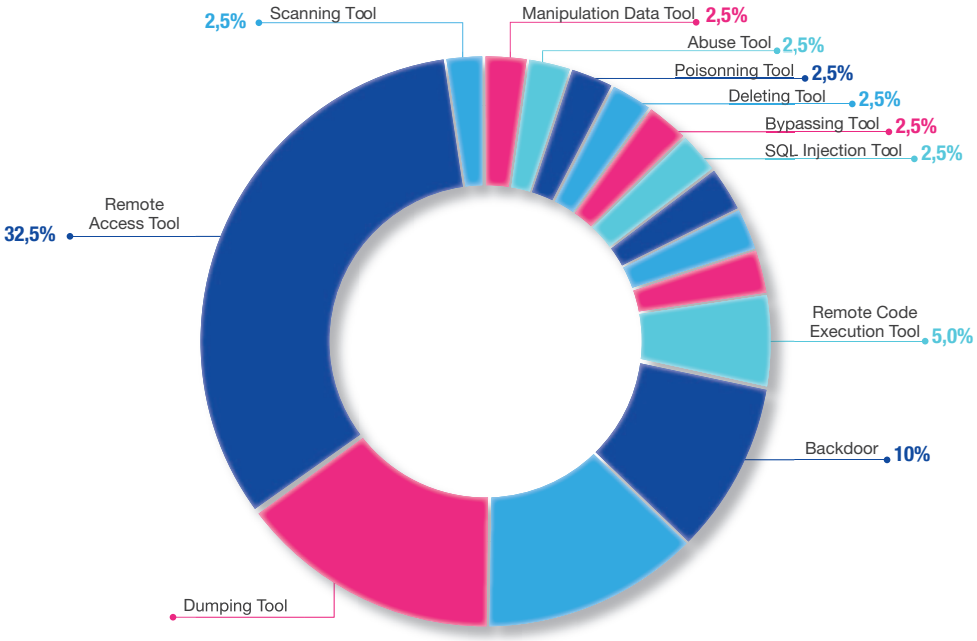
Estas herramientas son usadas por lo general **de dos formas diferentes** durante las intrusiones de los actores:

- **Modifican el código de la herramienta legítima** para incluir payloads maliciosos de cara a que sean ejecutados por el usuario final sin ser conscientes de ello.

- Tras una intrusión completa donde el cibercriminal hace uso de diferentes muestras de malware de distintas etapas, en última instancia, **despliegan la herramienta legítima** que les permite controlar de manera remota el sistema.

En 2020 hubo un aumento de los ataques realizados a través de RAT, debido a que aumentó considerablemente el uso de **herramientas de acceso remoto** por el confinamiento y el teletrabajo.

Como puede observarse en el gráfico a continuación, las herramientas de acceso remoto fueron las más **utilizadas (32,5%)** por los **grupos cibercriminales** en sus ataques durante 2020.



Herramientas más utilizadas por los grupos cibercriminales en 2020

Troyanos de Acceso Remoto en 2020

ASYNCRAT. Colombia en el punto de mira

En 2020, el CSIRT Financiero analizó de primera mano, las intrusiones que estaban teniendo como objetivo principal, el sector financiero de Colombia. Dichas intrusiones tenían muchas relaciones entre sí, ya sea por el modus operandi como por el arsenal desplegado.

Estas intrusiones, finalmente se tuvo constancia tras muchos meses de trabajo de análisis que estaban orquestadas por el conocido grupo APT-C-36, el cual, en el pasado había desplegado RATs como RemcosRAT, LimeRAT y en esta ocasión era el turno de AsyncRAT.

AsyncRAT fue concebida como una **herramienta open source de acceso remoto**, lo que le confiere la capacidad de administrar y controlar un dispositivo de forma remota. Es un software diseñado para Windows C# de acceso gratuito publicado en la conocida plataforma de Github.

Este tipo de herramientas son muy comunes en entornos educativos y laborales. En el caso de AsyncRAT, ofrece una conexión cifrada segura entre los dispositivos que participan de la conexión remota.

Dentro de las capacidades de AsyncRAT como RAT (Remote Access Tool) se encuentran:

- Grabar la pantalla del usuario
- Deshabilitar la solución anti-malware
- Cliente SFTP
- Keylogger
- Recepción de actualizaciones controladas por servidor
- Ofuscador de servidor

Como muchos otros software legítimos, existen diversas finalidades por las que se utilizan los RAT, desde solucionar problemas en el ordenador a distancia hasta la planificación y desarrollo de ciberataques, tal y como ha sucedido durante 2020, en la que AsyncRAT, como herramienta de acceso remoto, ha tomado relevancia en el sector financiero, principalmente, por afectación a los usuarios de diversas entidades bancarias en Colombia.

NjRAT.
Los hackers que atacan a otros hackers

Durante 2020, se detectaron dos campañas orientadas a distribuir malware entre el sector informático.

En marzo, fueron los **propios cibercriminales** los que **fueron víctimas** del troyano de acceso remoto **NjRAT**, que secuestra el dispositivo de la víctima, permitiendo a los atacantes llevar a cabo acciones como el robo de datos o efectuar ataques de denegación de servicio (DoS).

Dentro de las capacidades de NjRAT se encuentran:

- Escritorio Remoto y Ventana activa
- Obtener información de configuración de la máquina víctima
- Ejecución remota de archivos
- Manipulación de archivos
- Ejecutar shell de manera remota
- Ejecutar administrador de procesos
- Modificar el registro de Windows
- Activar la cámara y el micrófono de la máquina
- Registro de teclas (keylogger)
- Robo de contraseñas almacenadas en los navegadores u otras aplicaciones

Los autores del ataque aprovecharon vulnerabilidades en páginas de Wordpress para publicar paquetes infectados con el troyano en varios sitios web y foros donde los cibercriminales descargan habitualmente las herramientas para desarrollar sus campañas de malware. Además, los autores de los ataques desarrollaban, de forma diaria, variantes del troyano, llegando a detectarse más de mil versiones distintas de NjRAT, distribuidas a través de diferentes servidores. Oriente Medio fue el área geográfica más afectada, especialmente Turquía[7].

Más tarde, ese mismo año, en diciembre, se detectó otra campaña de distribución del malware centrada en los desarrolladores.

En este caso, el malware se localizó en dos paquetes subidos al repositorio npm, destinados a ayudar a los desarrolladores a trabajar con archivos JSON generados por aplicaciones

de bases de datos. Los paquetes fueron descargados más de 100 veces antes de que se pudiera detectar el comportamiento malicioso[8].

Aunque se desconoce la finalidad de estos ataques, es muy probable que el objetivo sea robar las credenciales de proyectos, código fuente de los mismos, etc, bien sea para espionaje industrial o para extorsionar.

Remcos RAT y coronavirus.

Como se ha mencionado anteriormente, la crisis del coronavirus ha dado nuevas temáticas a los cibercriminales para la explotación de la ingeniería social.

Así ocurrió en marzo de 2020, cuando los gobiernos comenzaron a imponer sus medidas de contención de la COVID-19. La sociedad estaba tan pendiente de contar con información actualizada sobre esta enfermedad, que las noticias y mensajes relacionados con el coronavirus comenzaron a circular masivamente por todos los medios, mail, mensajería móvil, etc.

Esta circunstancia fue utilizada por los actores maliciosos, que comenzaron a distribuir malware de forma masiva.

RemcosRAT, al igual que hemos visto con NjRAT y AsyncRAT tuvo un impacto importante en Colombia ya que se consiguieron identificar varias campañas activas.

En este caso, esta herramienta de acceso remoto y las campañas en las que se desplegaba esta tecnología tenían ciertas particularidades, sobre todo en el último semestre de 2020, ya que durante la cadena de infección se hacía uso de la esteganografía para evadir defensas y poder desplegar en última instancia RemcosRAT.

Este RAT como cualquier otro tiene la posibilidad de realizar prácticamente cualquier actividad en el sistema comprometido, brindando una puerta trasera de gran tamaño al cibercriminal y que así pueda conseguir sus objetivos.

Dentro de las capacidades de RemcosRAT se encuentran:

- Obtener información de configuración de la máquina víctima
- Ejecución remota de archivos
- Ejecutar shell de manera remota
- Subir y descargar archivos en la máquina infectada
- Modificar el registro de Windows para conseguir persistencia
- Conexión mediante el protocolo TCP a la IP y puerto seleccionados mediante una contraseña para cifrar la información
- Registro de teclas (keylogger)

Como se ha podido ver, el uso de RATs es muy común en las campañas que está sufriendo la región de Colombia, sin embargo, no se trata del malware de primera etapa ni segunda.

Por lo general, las intrusiones analizadas por el CSIRT donde se involucra el despliegue de un RAT, se realizan, en primera instancia, mediante un phishing o spearphishing a un usuario. Tras la descarga de un malware de primera etapa por parte del usuario y ejecución, empieza la cadena de infección, descargándose otra muestra de segunda etapa, en muchos casos, incluso tercera, cuarta y quinta etapa, dejando en último lugar la descarga del RAT.

El objetivo del RAT es, **únicamente**, proporcionar un canal de comunicación entre sistema infectado y actor, donde se incluyen por lo general técnicas muy comunes en RATs, por ejemplo, subida de archivos al sistema, captación del audio y video, captación de las pulsaciones de teclado y un largo etcétera.

Todo lo que pasa hasta que se despliega el RAT en el sistema, es verdaderamente complejo y sofisticado, donde los actores buscan explotar vulnerabilidades, realizar movimientos laterales y persistir en el sistema garantizando su acceso, entre otras cosas. Y hasta que el RAT es puesto en marcha, se han ejecutado sin que el usuario sea consciente binarios (.exe), instaladores (.msi), librerías (.dll), imágenes con esteganografía (.png, .jpeg, .jpg..).

La tendencia del uso de RATs continuará durante 2021, tal y como indica la última operación detectada, **Spalax**, desde la que el CSIRT notificó a sus asociados. Esta campaña, dirigida a Colombia, utiliza los tres troyanos aquí mencionados, AsyncRAT, NjRAT y Remcos RAT, para sus fines maliciosos.

Ransomware

Una de las ciberamenazas que **más ha cambiado su modus operandi** y que más ha **incrementado su actividad** a lo largo de 2020 ha sido el malware de categoría ransomware. Los cibercriminales y grupos organizados que se encuentran tras las grandes familias de ransomware, han cambiado el panorama de los ciberataques durante el curso del año, siendo ésta una de las ciberamenazas más destacable de 2020.

Una de las primeras cuestiones a tener en cuenta sobre el comportamiento del ransomware durante 2020 son los **objetivos** contra los que se han dirigido. Con anterioridad, los ransomware estaban dirigidos contra cualquier entidad que pudiera reportar un beneficio económico resultante de la paralización de la operación por el cifrado de los equipos de la entidad.

Con la evolución de los ransomware, también han cambiado sus objetivos. A lo largo de 2020 se han dejado atrás los ataques aleatorios y masivos, en términos generales. Los grandes grupos cibercriminales han comenzado a **seleccionar cuidadosamente a sus víctimas**, dando lugar a **ciberataques altamente dirigidos** que exigen un pago mayor.

Las víctimas se seleccionan cuidadosamente en función de varios aspectos:

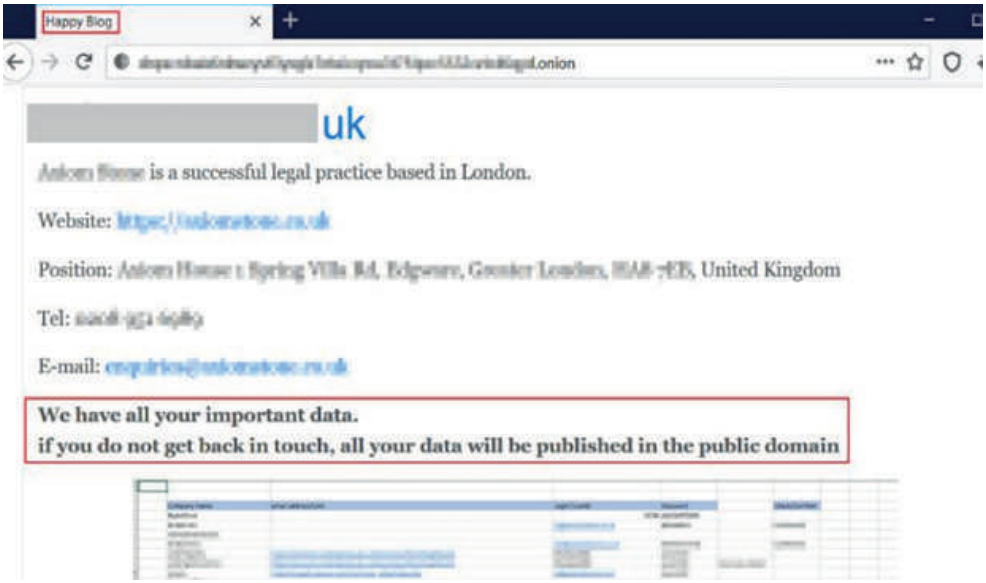
- Según su capacidad de pago
- Su dependencia de los datos cifrados
- Su capacidad de impacto por el bloqueo de la operación

De esta manera, los ransomware se han transformado en un tipo de malware muy adaptativo que, en función de la víctima, emplea un vector de infección u otro para incrementar su efectividad.

Otra cuestión a tener en cuenta es que durante 2020, los ransomware han desarrollado un modus operandi de doble extorsión, en una búsqueda para maximizar los beneficios del ciberataque.

En este sentido, los cibercriminales, previo a cifrar los datos del equipo infectado, exfiltran información que posteriormente será empleada para chantajear a las víctimas. Se realiza una amenaza con publicar la información robada en caso de no recibir el pago del rescate, junto con el tradicional chantaje a través del cifrado de los equipos.

Para llevar a cabo las prácticas de extorsión, muchos cibercriminales han creado sus propias páginas web donde publican información básica de sus víctimas y la información exfiltrada en partes, para dosificar en diferentes fases el chantaje realizado[9].



Blog de REvil chantajeando a una víctima

El grupo de cibercriminales tras el **ransomware Maze**, además, alberga dentro de su propia página web, las filtraciones de datos de grupos más pequeños carentes de infraestructura suficiente para realizar este modus operandi, a saber, Lockbit o RagnarLocker. Es posible que este **alojamiento** sea otro **servicio que da el grupo** para obtener beneficios, ofertando alojamiento de filtraciones de datos en una página web de alto perfil como servicio a terceros[10].

De esta manera, Maze cuenta con toda una **organización de especialistas** entre los que se incluyen personas capacitadas en hospedaje TOR en la nube, almacenamiento y migración de datos en la nube, desarrollo web front-end y facilitación de negociaciones, todos ellos destinados a administrar la organización de forma ordenada y beneficiosa para todos los cibercriminales.

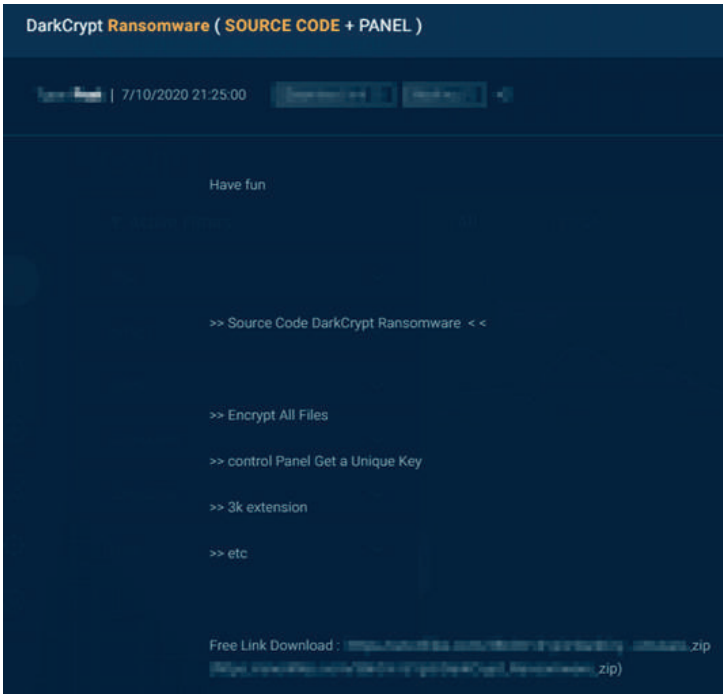
Algunos de los mayores exponentes de esta tendencia han sido los cibercriminales tras los ransomware Maze, Sodinokibi, DoppelPaymer, Nemty, Nefilim y CLOP. Sin embargo, esta tendencia se está identificando también en grupos de cibercriminales operadores de ransomware que no cuentan con tanta sofisticacion como los anteriormente mencionados, por lo que esta tendencia permanecerá proliferando en los próximos años dada la efectividad que está teniendo[11].

Por último, es destacable el predominio del RaaS (**Ransowmare-as-a-Service)** como modelo de negocio entre los cibercriminales, donde no sólo se pone al servicio el uso de los ransomware, sino que también se han creado **programas de afiliación** que **maximizan la colaboración** entre cibercriminales con diferentes objetivos y motivaciones.

Así pues, los **grandes grupos cibercriminales** pueden destinar sus esfuerzos a desarrollar y mantener las capacidades del ransomware, permitiéndoles centrar su energía en planificar y llevar a cabo **ciberataques altamente dirigidos**. Mientras, los cibercriminales de los **grupos más pequeños**, continuarán centrándose en sus labores de **distribución de malware en masa**, por ejemplo, a través de botnets, mientras adquieren los ransomware de terceros.

La existencia de productos en foros de la Deep Web y Darknet como **kits de ransomware** completamente **gratuitos** a los que cualquier cibercriminal puede acceder, también ha sido un detonante para el crecimiento del RaaS en el panorama cibercriminal. Ya no es necesario tener grandes conocimientos técnicos para llevar a cabo un ciberataque con ransomware, y más aún teniendo en cuenta, que algunos de estos kits se facilitan con una guía de uso destinada a todo tipo de usuarios.

Añadido a esto, es necesario tener en cuenta que las **consecuencias económicas** provocadas por la pandemia de la **Covid-19**, ha generado que muchos usuarios se hayan lanzado a adquirir sus propias herramientas para desarrollar ciberataques como una **nueva fuente de ingreso**, lo cual también se encuentra intrínsecamente ligado al incremento del **RaaS** de bajo nivel de sofisticación.



Ransomware gratuito en un foro de la deep web

Es destacable también la identificación de un incremento de aprovechamiento de vulnerabilidades RDP por parte de los ransomware y otros tipos de malware, todo en relación con el aumento del teletrabajo a lo largo de 2020.

De esta manera, existen grupos de cibercriminales dedicados, exclusivamente, a realizar escaneos en busca de puntos finales de RDP para realizar un ataque de fuerza bruta después y extraer las credenciales débiles del sistema atacado. Una vez comprometidas las credenciales, estas se ponen a la venta en markets especializados para ello.

Los principales compradores de este tipo de productos, son otros grupos cibercriminales que pretenden agilizar sus labores de planificación y desarrollo de un ciberataque, identificándose entre los primeros consumidores de este producto los cibercriminales dedicados al ransomware[13].

En el transcurso de 2020, las VPN se elevaron rápidamente como el nuevo vector de ataque entre las bandas de ransomware, siendo las puertas de enlace de red Citrix y los servidores Pulse Secure VPN, los principales objetivos.

Finalmente y más alejado de la tendencia de doble extorsión de los ransomware, no se pueden olvidar otros grandes ransomware que han tenido una importante actividad a lo largo de 2020 y que, probablemente, sigan su continuidad a lo largo de 2021 debido a su constante desarrollo y mejora. En este caso es necesario destacar la actividad **Ryuk**, quien sigue la tendencia de ciberataques altamente dirigidos y de alto impacto.

Ryuk se encuentra diseñado de manera que obliga a los cibercriminales a prestar atención individualizada a las víctimas[14].

Dependiendo de la variante de Ryuk que los cibercriminales estén empleado, este se distribuye por varias vías:

- A través de correos electrónicos de spearphishing diseñados a medida
- Uso de credenciales compradas a terceros para acceder a dispositivos a través de un escritorio remoto
- A través de vulnerabilidades de software como Zerologon (CVE-2020-1472)[15]

Malware POS

A pesar de que durante el año 2020 hubo un aumento considerable del uso del comercio online, debido a las medidas de confinamiento y restricciones a la movilidad por la COVID-19, los **ataques contra los dispositivos en el punto de venta** (Point Of Sale, POS) **persisten**.

Esta persistencia se debe, entre otros factores, a que es un **malware que no** requiere de una **evolución continua** ni de una adaptación según el dispositivo, ya que sus objetivos mantienen las mismas características durante muchos años.

Por lo que el uso de malware contra sistemas POS permanecerá mientras estos sistemas continúen funcionando con **sistemas operativos sin soporte y medidas de seguridad necesarias**. Además, los cibercriminales seguirán aprovechándose de esa fracción de segundo, donde la información no se encuentra cifrada, para seguir extrayendo datos de las tarjetas empleadas.

Por otro lado, cabe mencionar que el **sector financiero no es el objetivo** directo de este tipo de ataques, ya que están más orientados a los usuarios y clientes, sin embargo, sí que se ve afectado de **forma colateral** por este tipo de ataques.

Desde el **CSIRT,** se elaboró un informe orientado a las **principales amenazas para los distintos medios de pago,** disponible para todos los asociados en el portal del Observatorio de Ciberseguridad.

En 2020, VISA alertó de dos incidentes de seguridad[16], ocurridos entre mayo y junio, relacionados con TPVs. Ambos casos se detectaron en Estados Unidos, siendo la víctima una cadena hotelera.

En uno de ellos, los atacantes utilizaron una combinación de varios malware, concretamente de **RtPOS, MMON** (también conocido como Kaptoxa) y **PwnPOS**. En este caso, no se pudo determinar el vector de intrusión, aunque sí que lograron reunir evidencias que apuntan a que el atacante usó **herramientas de acceso remoto** y **dumpers de credenciales** para el acceso inicial, el movimiento lateral y la implementación de malware.

El malware RtPOS utiliza un algoritmo especializado para **verificar los datos de la tarjeta de pago**, antes de agrupar la información en un archivo, que los estafadores extraen a través de un servidor de Command and Control.

El malware **MMon**, por otro lado, implementa una técnica de raspado de memoria de línea de comandos que **recopila datos de tarjetas de pago de la memoria de un dispositivo POS**. Este código malicioso, en uso desde 2010, se personaliza con frecuencia. Por último, **PwnPOS** crea **persistencia** dentro de los dispositivos POS e intenta extraer los datos de la tarjeta de pago de la memoria.

En el otro ataque detectado, se utilizó la variante de **malware TinyPOS**. El ataque se inició con una **campaña de phishing** dirigida a los **empleados** de la cadena hotelera que fue víctima del mismo. Los atacantes lograron **comprometer las cuentas de los usuarios**, incluida una cuenta de **administrador**, y utilizaron herramientas administrativas legítimas para acceder al entorno de datos del titular de la tarjeta (CDE) dentro de la red. Tras ello, procedieron a implementar su skimmer. Para agilizar su despliegue, emplearon un script que automatizó la distribución del malware por toda la red corporativa. TinyPOS intenta recopilar **nombres de titulares** de tarjetas, **números de cuenta**, fechas de **vencimiento** y otra información.

APTs

La Covid-19, al igual que con el resto de ciberamenazas y malware hablados anteriormente, también ha tenido la capacidad de modificar algunos comportamientos de las **Advanced Persistent Threats**, incrementando en cierta manera, su **actividad** a nivel **internacional** y demostrando el alto grado de **adaptabilidad** de este tipo de ciberamenazas.

Es común entre los cibercriminales de cualquier tipo de sofisticación, que se aprovechen de las circunstancias para mejorar la efectividad de sus ciberataques sobre las víctimas

seleccionadas. A lo largo de 2020, se han podido identificar a **grupos APT** o Advanced Persistent Threat como Kimsuky (Corea del Norte), APT27 (China), Lazarus[17] (Corea del Norte) o ViciousPanda (China) empleando la **temática de la Covid-19** para aportar una mayor **credibilidad a sus engaños.**

Añadido a esto, la situación de **confinamiento** provocada por la Covid-19 ha **imposibilitado**, en cierta manera, las **operaciones de los servicios de inteligencia y gobiernos en territorios extranjeros**. Este hecho ha traído como consecuencia que estas operaciones se hayan **desplazado**, a lo largo de 2020, al **panorama cibernético**, identificándose una mayor actividad por parte de los estados nación[18].

Aunque el enfoque ha sido preferentemente sobre objetivos del sector salud, como hospitales y farmacéuticas, durante el año, en el sector financiero también se ha identificado un incremento del número de ciberataques con sus respectivas tendencias, en este caso, relacionados con APTs y una fuerte motivación financiera.

Es destacable que las **tensiones geopolíticas** acaecidas en 2020 han generado una **respuesta** en el ámbito cibernético, especialmente de **actores** provenientes de países como **Irán** (MuddyWater[19]), **Corea del Norte** (Lazarus[20]), **Estados Unidos** (Digital Revolution[21]) o **Rusia** (Fancy Bear[22]). Así mismo, a lo largo de 2020 también se han podido identificar diversas campañas clasificadas como ciberespionaje llevadas a cabo por actores, principalmente de China, sin excluir a actores de las anteriores nacionalidades mencionadas.

Grandes actores conocidos como Lazarus o Roaming Mantis, al igual que muchos otros, han permanecido en el panorama cibercriminal sobre **entidades financieras**, lo que demuestra que el interés económico sigue siendo uno de los pilares fundamentales dentro de la motivación de los grupos APT.

Sobre la cuestión de **Lazarus**, es destacable cómo el grupo ha ido evolucionando sus TTPs (Técnicas, Tácticas y Procedimientos) así como su arsenal de herramientas, para adaptarse a todo tipo de **entidades financieras** en función de su objetivo. Así pues, el subgrupo de Lazarus dedicado a ciberataques con motivación económica, **BlueNoroff**, fue identificado en una **campaña activa** desde al menos 2017, tomando por objetivos entidades de criptomonedas y tecnología financiera.

Para esta **campaña**, el grupo empleó como **vector de infección** correos de **spear-phishing** con un archivo de acceso directo de Windows. Los **nombres de los archivos** se camuflaron como archivos relacionados con la **seguridad o las criptomonedas** para engañar a los usuarios a ejecutarlos.

La cadena de infección era un complejo procedimiento de varias etapas, utilizando dos scripts de VBS y tres de PowerShell para recopilar información del sistema. La carga útil fue una backdoor que también utiliza un procedimiento de infección de varias etapas y su funcionalidad fue la de cargar un malware adicional para el robo de pulsaciones de teclado y capturar la pantalla de la máquina infectada [23].

Por otra parte y por primera vez, también se ha identificado al grupo **Lazarus vinculado con el uso de un ransomware**. A lo largo del año se identificaron diversos incidentes donde se involucró el uso del **ransomware VHD**, caracterizado por su método de autorreplicación compilado con credenciales específicas de la víctima. Esta técnica, junto con la identificación de herramientas conocidas de Lazarus, hizo posible la atribución de estas campañas a dicho grupo, siendo ésta, la primera campaña conocida donde Lazarus ha recurrido a ataques de ransomware dirigidos para obtener ganancias financieras.

Además de los actores de Corea del Norte, otras tradicionales APT han continuado con su actividad sobre el sector financiero con una relevante motivación económica tras de sí. En 2020 se han identificado diversas campañas de grupos como **FIN7**[24] a través del malware **Griffon**[25], **Silence** a través de ataques **DDoS**[26], y **Magecart**, que ha visto incrementada su actividad gracias al aumento del comercio electrónico generado por la cuarentena llevada a cabo como medida contra la Covid-19[27].

Sin embargo, la motivación financiera no es la única que ha podido destacar a lo largo de este 2020 y es que, las campañas de **ciberespionaje y robo de información** confidencial, también han estado muy presentes en estos meses entre las entidades financieras.

Con el auge del **Crime-as-a-Service (CaaS)** también ha crecido otra tendencia denominada **Hacker-as-a-Service (HaaS)** donde han proliferado grupos de cibercriminales que bajo contrato, dedican sus conocimientos a realizar ciberataques a terceros. Este ha sido el caso de **DeathStalker.**

Este grupo de cibercriminales dedica sus servicios a la obtención de información comercial confidencial sobre el sector financiero, sin embargo, no es un grupo APT patrocinado por un Estado Nación como es habitual, sino que es un grupo organizado que ofrece servicios de piratería informática en los círculos financieros.

El grupo emplea un implante basado en PowerShell llamado Powersing, y aunque no cuenta con ninguna herramienta innovadora, sí que tienen una amplia comprensión de los fundamentos de una cadena de infección moderna, por lo que es posible que con el paso de los meses, DeathStalker continúe desarrollándose y mejorando su implante adquiriendo una mayor sofisticacion en sus ciberataques.

Otro aspecto destacable de este grupo es que siguen una interesante tendencia entre grupos APT de realizar **banderas** falsas para desviar la atención sobre sus propias acciones. En este sentido, el grupo incorporó metadatos de certificados del grupo Sofacy en su infraestructura. Este hecho está destinado a dificultar las labores de atribución de los investigadores en ciberseguridad.

Otras tendencias identificadas en 2020 con respecto a las APT y que es necesario tener en cuenta son las siguientes:

1. Continuada explotación de vulnerabilidades del software
2. Aumento de malware dirigido a dispositivos móviles[29]
3. Uso de servicios legítimos en la nube como parte de la infraestructura de ataque (Youtube, Google Docs, Dropbox, Firebase entre otros)
4. Uso de la inteligencia artificial para adquirir mayor credibilidad frente a las víctimas[30]

Finalmente, se hace necesario destacar la actividad de **APT-C-36** sobre la región de Latinoamérica, analizada en el Informe de Amenazas: AsyncRAT disponible para los asociados para su consulta.

En la campaña analizada por el equipo de analistas del CSIRT Financiero se identificó que los cibercriminales emplearon, a lo largo de varios incidentes, un vector de infección similar, **técnicas de ingeniería social** a través de correos electrónicos **phishing** para **distribuir el malware**.

En los correos se **adjuntaba** un fichero cuya miniatura se hacía pasar por un documento de texto con la estructura de una **factura**. Sin embargo el archivo se trataba de una imagen con un hipervínculo.

Imagen con hipervínculo de distribución de AsyncRAT

La imagen **redirigía** a la víctima a un **servicio de almacenamiento en la nube**, como Dropbox o Google Drive, ambos identificados en los diferentes incidentes analizados. Una vez descargado el fichero, se iniciaba la conexión con **el Command & Control** (C2), quedando el **dispositivo comprometido** y en manos de los cibercriminales.

Los cibercriminales **utilizan estos servicios legítimos** para alojar el **malware evitando que sea detectado**, ya que los diferentes sistemas de seguridad perimetral no bloquean las conexiones a los mismos.

Aunque no se puede dar una atribución con absoluta certeza, se identificaron grandes similitudes con niveles de comportamientos y objetivos del conocido grupo cibercriminal APT-C-36, quienes centran su objetivo en instituciones financieras de Colombia.

La imagen a continuación tiene como objetivo agrupar aquellas características que tienen en común las campañas de APT-C-36 y la detectada por el CSIRT Financiero de AsyncRAT.

Grupo de actividad APT-C-36
y campaña AsynCRAT

ATMs

La actividad de campañas contra sistemas ATM y el uso de malware desarrollado específicamente para estos dispositivos, se ha visto en **descenso durante este año 2020.**

Familias como **DispCash y WinPot** han sido de las pocas que han tenido algo de actividad y, únicamente en los cinco primeros meses del año 2020, febrero en el caso de WinPot y mayo por parte de DispCash. Varios **factores** pueden ser el motivo de que el uso de malware para ATM haya **disminuido**.

1. La **facilidad** con la que se pueden conseguir tarjetas bancarias mediante **otro tipo de malware**, como troyanos, puede hacer que los desarrolladores de malware para ATM replantéen en qué herramientas invertir más dinero y tiempo de desarrollo

2. La **pandemia** ha podido influir también a los desarrolladores de malware para ATM, principalmente para aquellas familias que permitían la técnica de jackpotting, ya que con el confinamiento provocado por la Covid-19, no era posible tener acceso a cajeros para vaciarlos.

3. Por último, y no menos importante, es la **complejidad** que tiene el **desarrollo** de malware para ATM. A pesar de estar en sistemas operativos de Microsoft Windows principalmente, hace falta **tener amplios conocimientos** sobre la arquitectura XFS y todas las funciones de la API para sacar el máximo provecho al malware. Por otro lado, también requiere conocer las funciones que permiten los Service Providers (SPI).

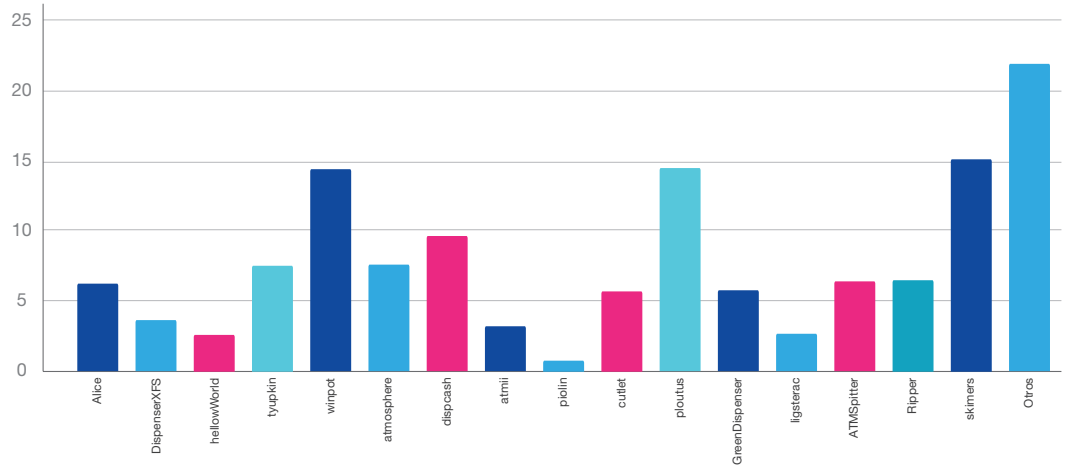
Arquitectura XFS

El hecho de que haya habido poca actividad relacionada con malware de ATM no ha sido un bloqueante para el **CSIRT Financiero**, que a falta de campañas, ha llevado a cabo la obtención y el **análisis** de más de **130 muestras de malware dirigidas a ATMs** con los siguientes objetivos:

1. Identificar **patrones de similitud** entre familias en su código.

2. Identificar las **familias** que **más impacto** tienen contra el **sector financiero** y así poder **priorizar esfuerzos** de seguridad en defensa de sus comportamientos.

ATM Malware - Principales familias analizadas por el CSIRT financiero



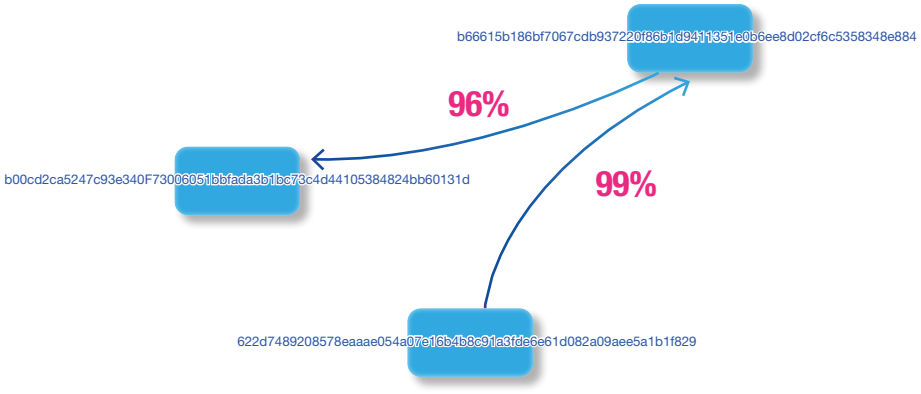
Todas estas muestras de malware obtenidas y analizadas por el equipo de analistas del CSIRT Financiero, han sido correladas entre ellas, originándose así, diferentes clusters basados en relaciones de bloques de código, es decir, **existen muestras en las mismas familias**, la gran mayoría de ellas, que **comparten ciertas partes del código**.

Para un entendimiento mucho más sencillo de lo comentado anteriormente, se expone el siguiente ejemplo a continuación:

- Partiendo de tres muestras diferentes pertenecientes a la familia de malware ATM Dispcash (las cuales llamaremos muestra 1, muestra 2 y muestra 3), se han detectado las siguientes correlaciones:

- **Muestra 1:** Comparte un 96% de código con la muestra 2.
- **Muestra 2:** Comparte un 96% de código con la muestra 1 y un 99% de código con la muestra 3.
- **Muestra 3:** Comparte un 99% de código con la muestra 2.

Este ejemplo sencillo expuesto, de manera visual queda representado de la siguiente forma.

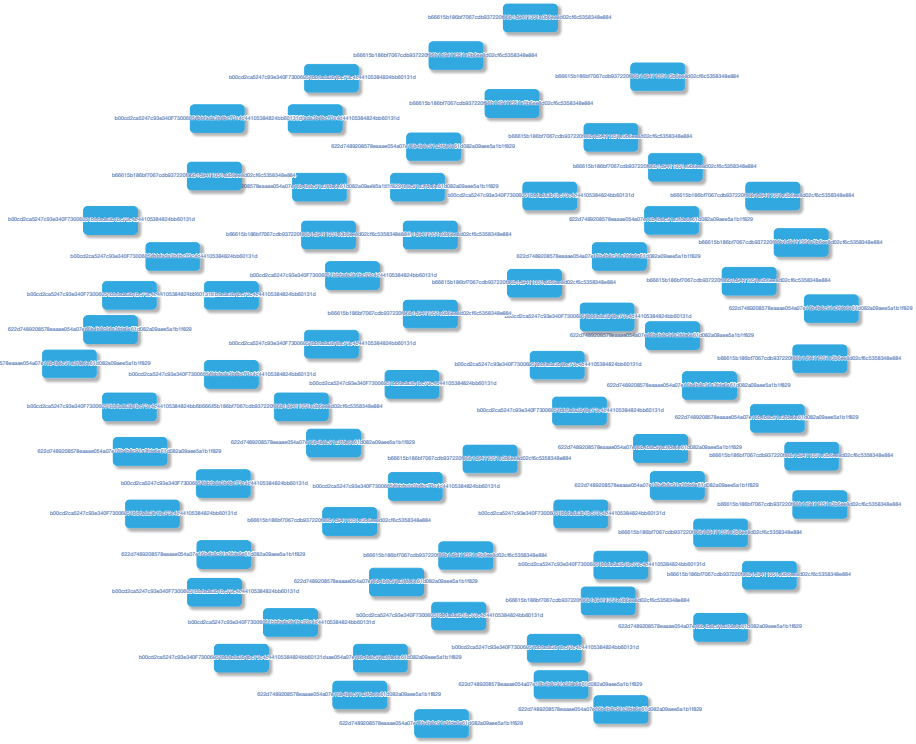


Siguiendo con todas las correlaciones de las muestras de malware ATM obtenidas en 2020, la siguiente imagen es una representación visual de todas las correlaciones que han sido identificadas, de las cuales se exponen las siguientes **conclusiones**:

1. La gran mayor parte de muestras de ATM, **comparten código entre variantes de la misma familia**.

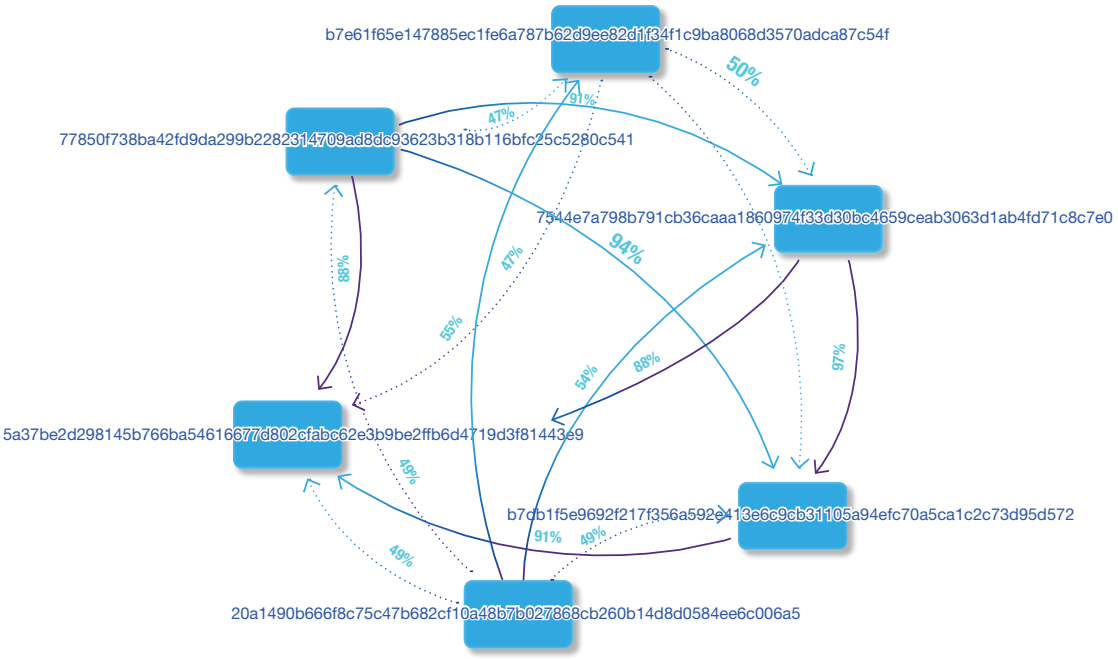
2. El hecho de que sólo las variantes de la misma familia comparta código, puede ser un **indicio** de que los **desarrolladores de malware ATM sean independientes** y no se comparta información entre diferentes actores.

3. A diferencia del malware para endpoint (por ejemplo Microsoft Windows), existen **muchas menos variantes**. Probablemente, las pocas posibilidades que existen en el éxito de estas campañas y la complejidad de desarrollar malware para ATM, sean algunos de los motivos por los que haya pocas variantes.



Haciendo zoom en algunas de las familias que tienen variantes que están relacionadas por compartir bloques de código, nos encontramos por ejemplo con **GreenDispenser**.

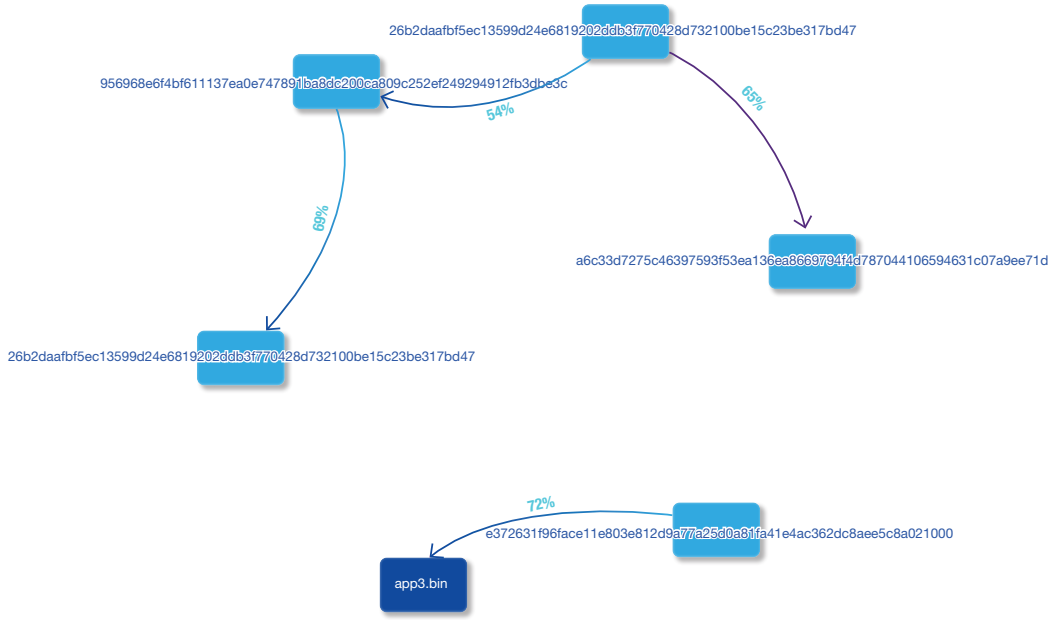
El 100% de las muestras que el CSIRT Financiero dispone de esta familia tiene algún tipo de relación de código superior al 47%, teniendo prácticamente la **mitad del código relacionado entre todas las muestras**.



Esta familia de malware, cuando introducía una muestra en un dispositivo ATM, mostraban un mensaje indicando que el ATM estaba fuera de servicio.

Es entonces cuando uno de los actores que llevaban a cabo esta infección, introduce un PIN en el keypad que le permitía sacar dinero de dicho ATM. Este **PIN** mencionado sólo era conocido por los cibercriminales.

Otra familia que también guarda mucha similitud entre sus variantes identificadas es **Atmosphere**. Esta muestra de malware, muy conocida también y que tuvo gran actividad durante el 2018, tiene como mínimo un 54% de similitud en código en un total de seis variantes que el CSIRT Financiero dispone. Al igual que en el anterior caso, hasta la **mitad del código** es **reaprovechado para generar una nueva variante** y cambiar ciertas funcionalidades para no ser detectado.



Malware Móvil

El malware para dispositivos móviles sigue siendo una **amenaza muy relevante para el sector**, ya que tiene **alto impacto** en los **clientes de las entidades financieras**, pero pasa desapercibido en muchos casos.

Durante 2020 se llegó a duplicar el volumen de transacciones fraudulentas originadas desde aplicaciones móviles en lugar de navegadores web, que denota un importante viraje de los movimientos de dinero a aplicaciones específicas para ello. Si bien, este hecho puede redirigir las ciberamenazas, precisamente, contra esas aplicaciones. En el primer trimestre de 2020, el fraude relacionado con aplicaciones móviles se disparó al 26%[31].

Entre los malware destinados contra móviles, se encuentra **Cerberus**, que sigue siendo la familia de malware que **más actividad** tiene, y más sabiendo que otras familias que están naciendo, tienen un grado de similitud (pequeño) en cuanto a comportamiento con la mencionada.

La **superposición** sigue siendo uno de los objetivos principales del **malware enfocado al sector financiero** en dispositivos móviles, tanto es así, que durante este pasado año 2020, hemos podido ver cómo el malware de sistemas operativos de escritorio también ha adoptado dicho comportamiento, superponiendo imágenes que suplantan las entidades financieras al acceder por el navegador.

A continuación, se mencionan algunas de las muestras de malware que el CSIRT Financiero ha analizado a lo largo del año.

Cerberus

Cerberus es un troyano bancario dirigido a dispositivos móviles con sistema operativo **Android** que fue detectado por primera vez en Junio de 2019. Desde sus orígenes, este troyano ha sido ofrecido como **MaaS** (Malware-as-a-Service), por lo que son **muchos los cibercriminales** han tenido **acceso** al mismo, utilizándolo no sólo para llevar a cabo sus campañas, sino para utilizarlo como base de desarrollo para otros troyanos. Es por esto que Cerberus es considerado el **padre de muchas otras familias de troyanos bancarios** dirigidos a estos dispositivos.

El equipo del **CSIRT Financiero**, gracias a su constante labor de monitorización e investigación de diferentes fuentes públicas, **logró acceso interno a un panel de administración** utilizado por algún **cibercriminal** que desplegó el panel con el fin de operar el malware.

Gracias a este hallazgo, se pudo **conocer en profundidad** el funcionamiento que tienen, tanto el malware como el modus operandi de los cibercriminales suscritos al servicio de Cerberus.

Desde el **panel de control**, el cibercriminal puede agregar las **plantillas** que crea conveniente para **suplantar las aplicaciones** de las principales **entidades bancarias**, para ello simplemente debe de especificar el nombre de la aplicación que va a suplantar, el fichero HTML que suplanta al Login y un fichero de imagen para servir de icono. De esta manera se consigue aumentar el número de objetivos muy fácilmente.

Resumiendo **todas las funcionalidades del panel de control**, encargadas del funcionamiento remoto del malware, son:

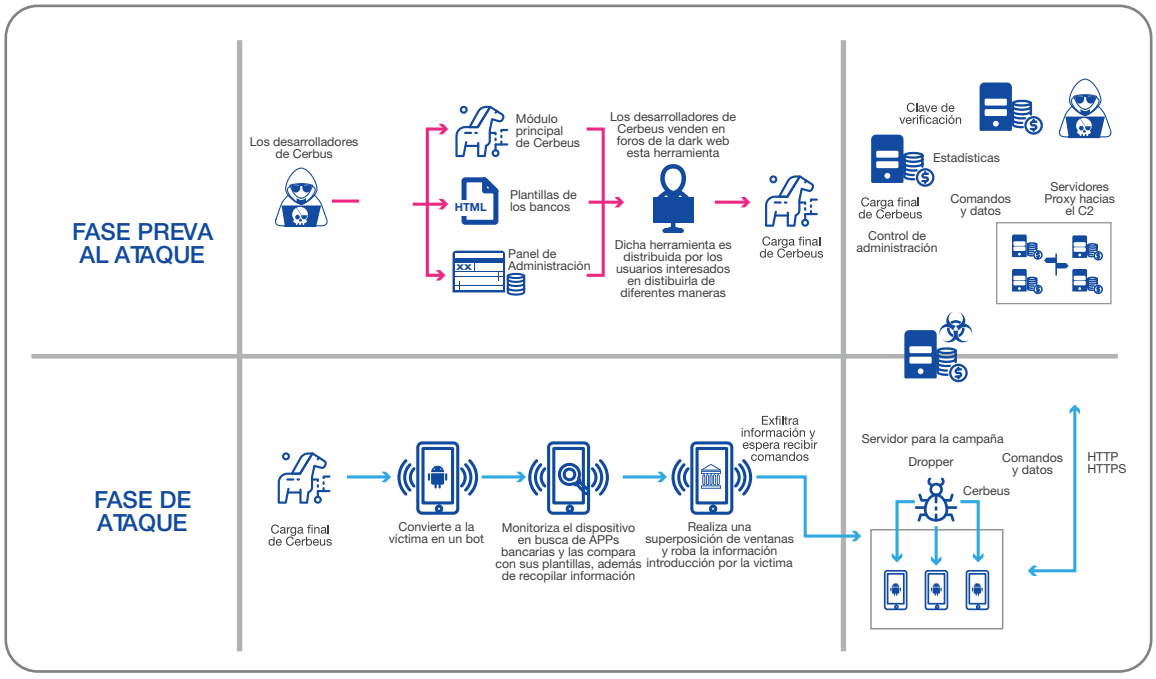
- Enviar SMS a todos los dispositivos infectados o a uno en concreto.
- Enviar dinero a dispositivos seleccionados.
- Reenviar llamadas al número especificado.

- Abrir plantillas.
- Arrancar aplicaciones.
- Enviar notificaciones push.
- Abrir URLs.
- Obtener listado de aplicaciones instaladas.
- Obtener lista de contactos.
- Obtener bandeja de SMS.
- Eliminar aplicaciones.
- Actualizar módulo del malware o plantillas.
- Obtener datos de Google Authenticator.
- Enviar otros comandos a los dispositivos infectados.

Una **característica novedosa** que implementó este malware es su **método de evasión de entornos virtualizados**, ya que utilizaba el podómetro del dispositivo para detectar si se producen movimientos reales de un usuario. Esta técnica fue implementada posteriormente en otros malware, siendo Cerberus el pionero de la misma.

El alcance de este malware, desde su origen, ha sido global, ya que al ofrecerse como MaaS, cibercriminales de cualquier parte del mundo han tenido acceso al mismo para operar geográficamente en diferentes puntos.

En agosto de 2020, el **grupo encargado del desarrollo** de Cerberus anunció que su **proyecto había muerto** tras la última **actualización de seguridad** lanzada por **Google Play Protect**, la cual escaneaba los recursos de todos los ficheros APKs.



Recon. / Weaporization	Delivery	Exploitation / Installation	C2 / Action en Objectives
• Se desconoce la fase de reconocimiento realizada por los usuarios de Cerbeus antes de desplegar este malware. • Los desarrolladores de Cerbus armaron un panel de administradores ubicado en TOR para gestionar bots desplegados por este troyano bancario para Android. • También crearon plantillas HTML inyectores de código CSS y JS con las fuentes e imégenes de las aplicaciones objetivo, una de las observadas ees BBVA.	• Dada su categoría de MaaS (Malware -as -a -Service), cada ususaro de Cerbeus puede utilizar distintos métodos de distribución de este troyani bancario. • Se conoce de un método de distibuición, realizado a través de un ataque a unos servidores MDM.	• Tras la infección del dispositivo, por el principal módulo de Cerbeus, este despliega un bot que realiza las acciones sobre el dispositivo infectado. • Este bot adquiere permisos de acceso, abusando de las funciones de accesabilidad del dispositivo para darse más permisos y ejecutar comandos recibidos por la infraestructura C2. • Está diseñado con técnicas anti-sandbox que le permite determinar dónde se encuentra, al monitorizar la actividad del usuario del dispositivo.	• Desde los dispositivos infectados se envían y reciben comandos a través de HTTP/HTTPS o incluso a través de Teamviewer. • Desde el panel de administración de Cerbus, su usuario puede enviar comandos para controlar el dispositivp donde se haya desplegado el bot. • Las distintas acciones que puede realizar el bot desplegado de Cerbeus en la víctima pueden ser la obtención de la mayor cantidad de permisos abusando de la accesabilidad del dispositivo, enviar SMS, hacer reenvío de llamadas, robo de información, robo de datos bancarios, cifrado del dispositivo.

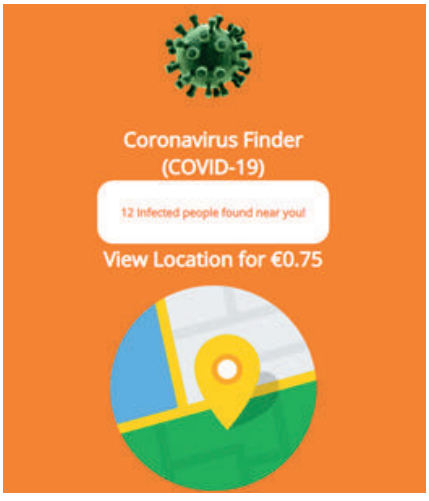
GINP

Ginp es un troyano bancario que, en sus orígenes, tuvo como objetivo a **usuarios clientes de entidades financieras españolas**, exfiltrando los datos de las tarjetas utilizadas en transacciones bancarias.

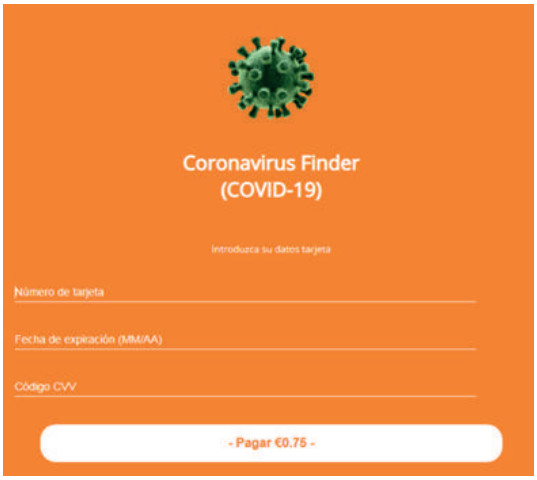
La crisis sanitaria provocada por la COVID-19, facilitó que los cibercriminales que operaban el malware aprovechasen esta temática para su distribución. Esta fue la campaña de mayor impacto llevada a cabo por este malware, ya que su alcance fue global.

En esta campaña se **distribuyó el malware** bajo el **nombre de una aplicación** que hacía entender a la víctima que se trataba de un radar que localizaba **personas contagiadas** por el **coronavirus**. El nombre de esta aplicación era **Coronavirus Finder**, la cual era distribuida a través de markets de aplicaciones no oficiales.

El funcionamiento de este malware es bastante simple, ya que se mantiene a la escucha de su servidor C2 a la espera de recibir una instrucción que ejecute la aplicación. Cuando esta se ejecuta, se le muestra un aviso a la víctima advirtiendo que existen personas infectadas a su alrededor.



Hasta este momento, la aplicación no parece mostrar actividad maliciosa. Para la **exfiltración de credenciales financieras**, se le muestra a la víctima un **mensaje** ofreciéndole mostrar la **ubicación** de las **personas infectadas** a cambio de un **importe**, normalmente inferior a un euro. Si la **víctima accede** a este mensaje, se muestra un **formulario** en el que se solicita **información de la tarjeta**.



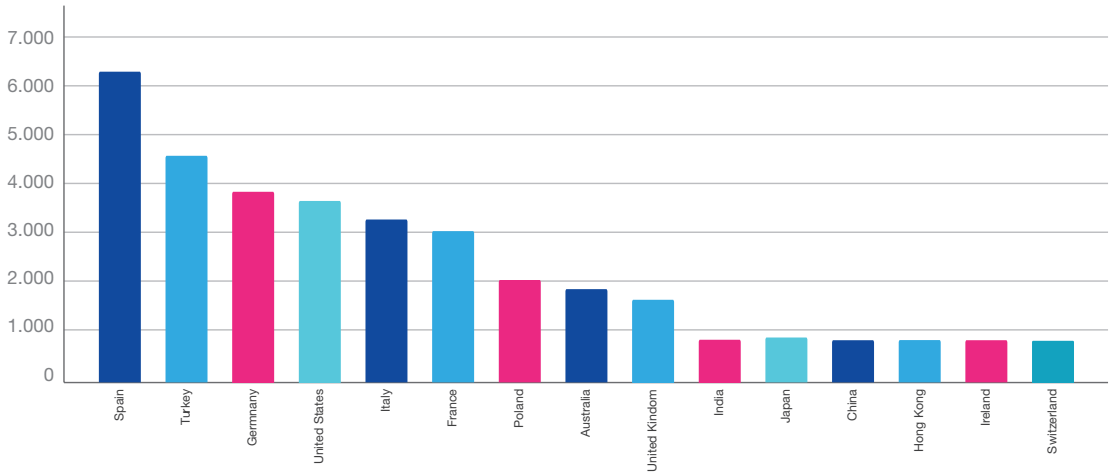
ALIEN

En su **distribución** se adaptó a la alarma sanitaria, suplantando la identidad de sitios web legítimos que contenían los **contactos de usuarios que son positivo de COVID-19**.

Este troyano es un heredero de Cerberus, donde existe una gran cantidad de funcionalidades que son implementadas del mencionado. Desplegaba sus funcionalidades de RAT para obtener las credenciales de acceso para diferentes aplicaciones, entre las que se encontraban una gran cantidad de bancos.

Técnicas de superposición, lectura de SMS, obtener información del dispositivo, keylogging, son algunas de las implementadas por esta familia. Lo que llamó realmente la atención de este malware son las **técnicas avanzadas** que usaba para **obtener códigos de doble factor de autenticación** (2FA) de las aplicaciones bancarias. Esto lo conseguía mediante el permiso "BIND_NOTIFICATION_LISTENER_SERVICE" que le permitía obtener el contenido de notificaciones en la barra de estado del dispositivo, consiguiendo así, que cuando hubiese una notificación de generación de un código 2FA, lo pudiese obtener y utilizar el actor.

A pesar de que Colombia no se encuentra en el TOP de países afectados por este malware, sí que pusieron foco en algunas entidades financieras del país, produciéndose alguna infección en clientes.


7.000
6.000
5.000
4.000
3.000
2.000
1.000
0
Spain
Turkey
Germany
United States
Italy
France
Poland
Australia
United Kindom
India
Japan
China
Hong Kong
Ireland
Switzerland

Fraude y Deep Web

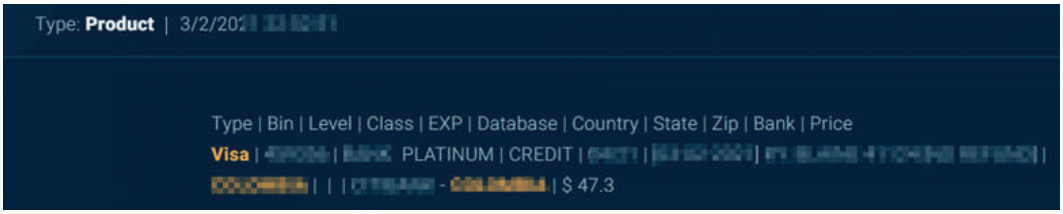
A lo largo de 2020 se han podido identificar diversos comportamientos con respecto a las ciberamenazas que han derivado en situaciones de fraude financiero. Algunos comportamientos han seguido las tendencias ya marcadas de años anteriores, y otras se han adaptado a la nueva realidad generada por la Covid-19. El **CSIRT Financiero** realiza una **monitorización** de fuentes localizadas en la **Deep Web y Darknet** para identificar estas ciberamenazas de manera temprana.

Una de las primeras cuestiones a destacar, es la estabilidad dentro del mercado cibercriminal de los precios de la información acerca de tarjetas bancarias robadas, es decir, **CVVs y Dumps**. En este sentido, es notable la **reducción de los precios de estos productos** en periodos **vacacionales,** intrínsecamente **ligado** a un **incremento en el robo de información bancaria** debido a un aumento del uso de las tarjetas por parte de los usuarios en estas épocas.

El precio medio de un CVV a lo largo de 2020 ha sido de 11,766 €

El precio medio de un dump en 2020 ha sido de 44,618 €

Los detalles de la tarjeta de crédito, generalmente, tienen el formato de un código simple que incluye el número de la tarjeta, las fechas asociadas y el CVV, junto con los datos de los titulares de la cuenta, como la dirección, el código postal, la dirección de correo electrónico y el número de teléfono.



Información básica de venta de tarjetas bancarias robadas

Otro tipo de productos ofrecidos que es necesario destacar es la **venta de credenciales y logs**, cuya actividad se ha visto **incrementada** en los markets especializados de la Deep Web y Darknet derivado en parte a la implementación de la **modalidad de teletrabajo**.

Las credenciales bancarias generalmente incluyen información de inicio de sesión, así como el nombre y la dirección del titular de la cuenta y detalles específicos sobre cómo acceder a la cuenta sin ser detectado. Los inicios de sesión en la banca en línea cuestan un promedio de 35$[32].

Por otra parte, las **credenciales corporativas** son otro tipo de productos bastante demandados en los foros especializados, dado que agilizan los trabajos de planificación y desarrollo de ciberataques. De esta manera, un cibercriminal que adquiera este tipo de credenciales tiene la capacidad de **suplantar a la empresa comprometida** para enviar **correos electrónicos** con archivos adjuntos maliciosos entre otras acciones.

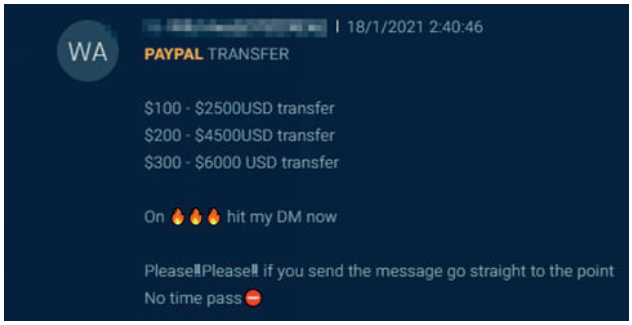
Las principales vías de robo de credenciales expuestas en foros de la Deep Web y Darknet han sido las que se muestran a continuación[33]:

1. Robo directo a bases de datos de servicios en línea y tiendas electrónicas
2. Correos de phishing con formularios de autenticación falsos
3. Infección por malware destinado a robar credenciales
4. Ataques de fuerza bruta

Entre otras cuestiones, la Covid-19 ha traído consigo un importante incremento de ciberataques a diferentes plataformas de pago online, cuyo uso se extendió durante la cuarentena y meses posteriores. Esto ha derivado en unos elevados niveles de fraude a usuarios y entidades relacionadas con estas plataformas, a saber Cash App y PayPal aunque no son las únicas a tener en cuenta.

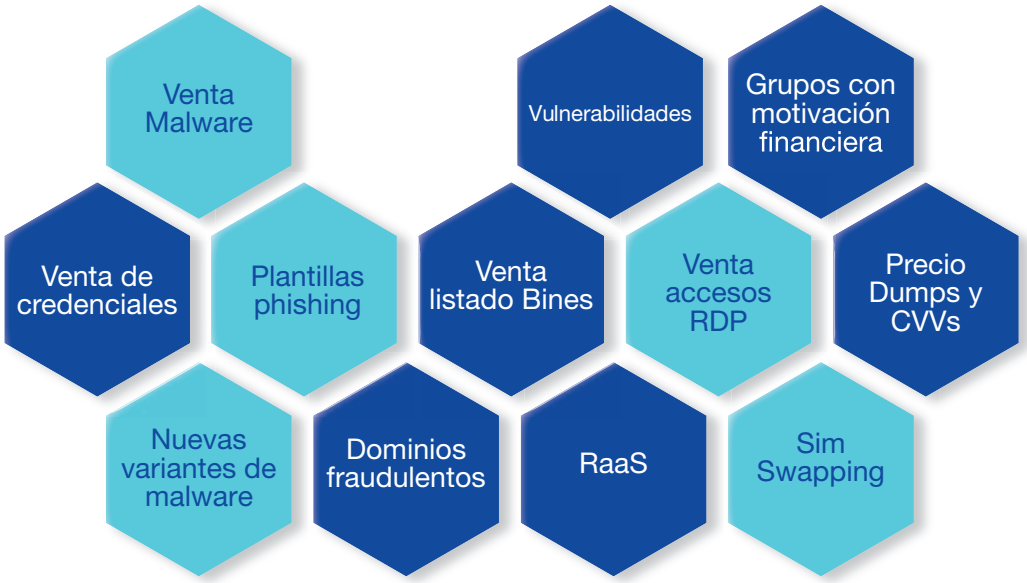
Las plataformas de pago pueden ser empleadas por parte de los cibercriminales principalmente para dos fines. En primer lugar, para acceder a través de las credenciales a la cuenta y transferir todo el dinero que esta contenga. Si bien, como implican un alto nivel de exposición y es una actividad rastreable, en muchos casos los cibercriminales prefieren vender las credenciales antes que extraer el propio dinero que contengan[34].

En segundo lugar, las cuentas en plataformas de pago comprometidas también pueden ser empleadas para **blanquear dinero obtenido de actividades ilícitas**. Es necesario tener en cuenta que para realizar este tipo de movimientos de forma efectiva, los cibercriminales tienen que tener conocimientos acerca de los mecanismos antifraude, así como de las técnicas para evadirlos, por lo que este tipo de servicios pueden llegar a costar hasta un tercio del monto transferido.



Por último, ha sido relevante el incremento de la demanda de accesos a redes internas de entidades financieras entre los cibercriminales en los foros de la Deep Web y Darknet. Este tipo de productos no son ofrecidos de forma continua y pertenecen a un conjunto de publicaciones maliciosas poco frecuentes y de alto impacto.

A lo largo de 2020, el **CSIRT Financiero** ha realizado alertas de **diferentes temáticas** relativas al **negocio cibercriminal y fraude** que, directa o indirectamente, han generado ciberamenazas que podrían impactar sobre las entidades financieras colombianas. A continuación se evidencia las temáticas identificadas a lo largo del año.



El impacto de estas ciberamenazas es muy amplio, si se tiene en cuenta que pueden ser extrapolables a cualquier sector y tipo de entidad. Si bien es cierto, sobre **entidades financieras** tienen un impacto relativamente acotado que involucra diferentes escenarios de fraude:

1. **Carding**
2. Incremento de **phishing** para obtención de datos financieros
3. Descarga de otros **malware financieros**
4. Robo y venta de los **datos exfiltrados** en foros de internet
5. **Suplantación de identidad**
6. **Acceso no autorizado** a cuentas bancarias, billeteras de criptomonedas o cuentas de plataformas online de pago
7. **Transacciones fraudulentas**
8. Nuevas **campañas contra entidades** financieras a través de malware bancario
9. Casos de **extorsión**

---

[4] https://www.checkpoint.com/downloads/resources/cyber-attack-trends-report-mid-year-2020.pdf?mkt_tok=eyJpIjoiTldNM05UWTJOelEwTnpZeCIsInQiOiJTSVY0QTBcL0d1UnpKcXM1UzZRRnRRV1RBV1djcnArM3BWK0VrUlQyb2JFVkJka05EWFhGOFpSSVJOZGszcnlpVFNVNVBwSjZDRXNxZGdkTGRKQzJJem4yYWlBQXJERUdkNDNrZEJDWGxNVUZ3WWt5K25vc2trRnNPNFZaY3JzOE8ifQ%3D%3D

[5] https://thehackernews.com/2020/11/anyrun-emotet-malware-analysis.html

[6] https://www.infosecurity-magazine.com/news/emotet-and-trickbot-top-malware/

[7] https://www.europapress.es/portaltic/ciberseguridad/noticia-descubren-campana-troyanos-utilizada-atacar-otros-hackers-20200310143020.html

[8] https://unaaldia.hispasec.com/2020/12/detectado-njrat-distribuido-a-traves-de-paquetes-npm.html

[9] https://blog.emsisoft.com/en/36303/ransomware-statistics-for-2020-q1-report/

[10] https://www.databreachtoday.com/7-ransomware-trends-gangs-join-forces-decryptors-improve-a-14401

[11] https://securelist.com/apt-predictions-for-2021/99387/

[12] https://securityboulevard.com/2020/08/ransomware-attacks-fracture-between-enterprise-and-ransomware-as-a-service-in-q2-as-demands-increase/

[13] https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme/#ftag=RSSbaffb68

[14] https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2020-q2/

[15] https://www.varonis.com/blog/october-2020-malware-trends-report/

[16] https://usa.visa.com/dam/VCOM/global/support-legal/documents/new-pos-malware-samples.pdf

[17] https://www.europapress.es/portaltic/ciberseguridad/noticia-atribuyen-grupo-lazarus-dos-incidentes-apt-relacionados-investigacion-vacuna-covid-19-20210111121646.html

[18] https://www.checkpoint.com/downloads/resources/cyber-attack-trends-report-mid-year-2020.pdf?mkt_tok=eyJpIjoiTldNM05UWTJOelEwTnpZeCIsInQiOiJTSVY0QTBcL0d1UnpKcXM1UzZRRnRRV1RBV1djcnArM3BWK0VrUlQyb2JFVkJka05EWFhGOFpSSVJOZGszcnlpVFNVNVBwSjZDRXNxZGdkTGRKQzJJem4yYWlBQXJERUdkNDNrZEJDWGxNVUZ3WWt5K25vc2trRnNPNFZaY3JzOE8ifQ%3D%3D

[19] https://www.cyberscoop.com/muddywater-iran-symantec-middle-east/

[20] https://securityaffairs.co/wordpress/112621/apt/lazarus-apt-targets-covid-19.html

[21] https://www.zdnet.com/article/hackers-breach-fsb-contractor-and-leak-details-about-iot-hacking-project/

[22] https://www.wired.com/story/russias-fancy-bear-hackers-are-hitting-us-campaign-targets-again/

[23] https://securelist.com/apt-predictions-for-2021/99387/

[24] https://www.cyberscoop.com/fin7-usps-fireeye-trustwave/

[25] https://attack.mitre.org/software/S0417/

[26] https://www.itnews.com.au/news/australias-banks-targeted-by-dos-for-ransom-threat-538563

[27] https://www.computerweekly.com/news/252481069/Coronavirus-Magecart-attacks-on-online-retailers-jump-20

[28] https://securityaffairs.co/wordpress/107532/cyber-warfare-2/deathstalker-hacking-group.html

[29] https://www.4hou.com/posts/Np9L

[30] https://securelist.com/apt-predictions-for-2021/99387/

[31] https://www.darkreading.com/attacks-breaches/mobile-app-fraud-jumped-in-q1-as-attackers-pivot-from-browsers/d/d-id/1338336?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple

[32] https://www.helpnetsecurity.com/2020/06/19/dark-web-prices/

[33] https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2020-q2/

[34] https://blog.cybersixgill.com/rising-fraud-on-payment-platforms-amid-the-coronavirus-pandemic?utm_campaign=THREAT%20REPORT%3A%20Corona%20Cash%20-% -%20Payment%20Apps&utm_content=140094477&utm_medium=social&utm_source=twitter&hss_channel=tw-3662748197

Inteligencia de amenazas

La base de conocimiento colectiva del sector financiero, en el entorno de debilidades de ciberseguridad, está incorporada por el CSIRT en la capacidad Inteligencia de Amenazas.

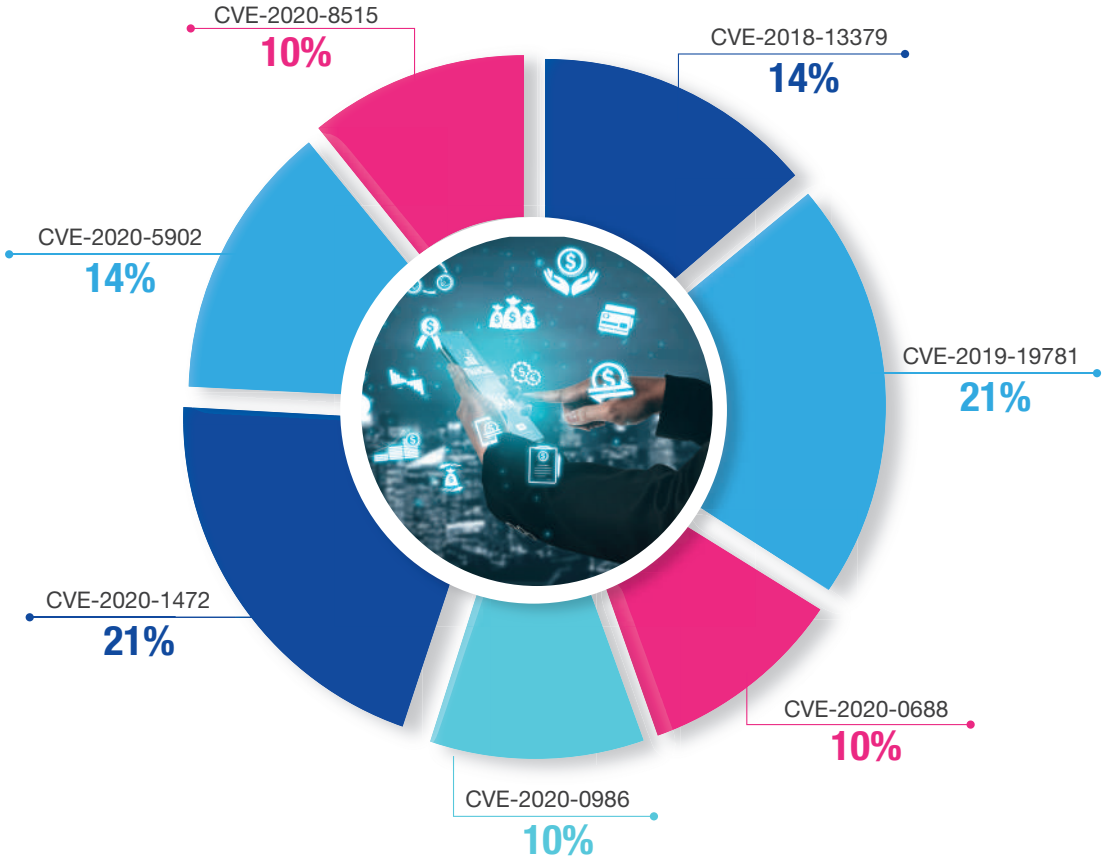
En el transcurso del 2020, se consolidaron **nuevas colaboraciones** que se convierten en fuentes relevantes de datos para el sector, a partir de estos y la investigación puesta en práctica, se procede a generar la lectura, clasificación y análisis de **vulnerabilidades**, considerándose las que podrían generar un **mayor impacto en las organizaciones asociadas** y que se comparten con el objetivo de entregar información sobre patrones, técnicas y brechas utilizadas por ciberdelincuentes para adentrarse en las organizaciones y generar una alteración en la seguridad.

Cifras reportadas (01/01/2020-31/12/2020)

Es innegable que la Inteligencia de Amenazas se ha consolidado en un elemento imprescindible para las organizaciones, ahora mismo esta labor es una parte fundamental de cualquier ecosistema de ciberseguridad y el **CSIRT Financiero** correspondiendo a ello, notificó y alertó **197 vulnerabilidades**, referidas en 12 alertas tempranas y 49 notificaciones.

Cada análisis realizado en el transcurso del 2020 representa información de vulnerabilidades que fueron utilizadas por los ciberdelincuentes para afectar directa o transversalmente instituciones financieras a nivel mundial, además, el equipo del CSIRT Financiero, consolidó la información reportada, obteniendo así los **CVE más observados en actividades maliciosas**, los cuales se muestran a continuación.

Top de vulnerabilidades con mayor implicación en actividades maliciosas CSIRT



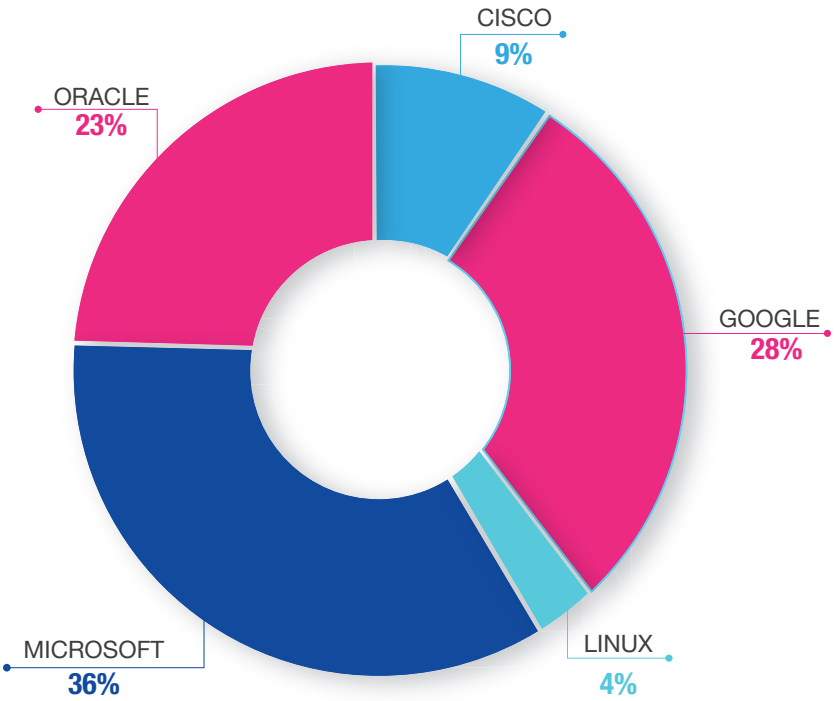
En la siguiente tabla, se detallan las principales características de las vulnerabilidades presentadas en la imagen anterior:

Vulnerabilidad	Detalle	Productos Afectados	CVSS
CVE 2020-1472	Permite elevar privilegios cuando un atacante establece una conexión de canal seguro Netlogon vulnerable hacia un controlador de dominio	Microsoft Active Directory	10.0
CVE 2020-19781	Permite ejecución de acceso remoto, un cibercriminal podría tomar el control de una manera muy sencilla del sistema vulnerado	Citrix Application Delivery Controller Citrix Gateaway	9.8
CVE 2020-5902	Permite ejecución remota de código en páginas no reveladas	BIG IP versiones: 15.0.0 hasta 15.1.0.3 14.1.0 hasta 14.1.2.5 13.1.0 hasta 13.1.3.3 12.1.0 hasta 12.1.5.1 11.6.1 hasta 11.6.5.1 Traffic Management User Interface (TMUI)	9.8
CVE 2018-13379	Permite acceso no autentificado a un cibercriminal para descargar archivos de sistema a través de solicitudes de recursos HTTP especialmente diseñados	Fortigate SSL VPN	9.8
CVE 2020-0688	Permite ejecución remota de código en el software Microsoft Exchange cuando el software no puede manejar correctamente los objetos en la memoria, conocida como Vulnerabilidad de corrupción de memoria de Microsoft Exchange	Microsoft Exchange	8.8
CVE 2020-0986	Permite elevación de privilegios cuando el kernel de Windows presenta un fallo al manejar apropiadamente objetos en la memoria	Windows 8.1 Windows 10 Windows Server 2012 Windows Server 2016 Windows Server 2019	7.8
CVE 2020-8515	Permite la ejecución remota de código como root (sin autenticación) a través de metacaracteres de shell	Draytek en sus versiones: vigor 3900_firmware: 1.4.4 beta vigor 300b_firmware: 1.3.3 beta vigor 2960_firmware: 1.3.1 beta vigor 3900 vigor 300b	

Principales CVEs sobre fabricantes y productos

Por su lado, entre los fabricantes que se evidenciaron con un alto compromiso y que por su común uso son relevantes tanto a nivel usuario como infraestructura de organizaciones, el CSIRT Financiero relaciona los siguientes:

Top fabricantes con mayores vulnerabilidades relacionadas



Al igual que en 2019, **Microsoft** sigue siendo el fabricante con el mayor número de reportes de vulnerabilidades, debido a su amplia gama de productos y el común uso que, estadísticamente, es elevado alrededor del mundo. **Google** toma relevancia en debilidades, especialmente por su alto reporte de vulnerabilidades principalmente asociadas al **navegador Chrome**.

Cisco fue afectado, principalmente, por vulnerabilidades explotadas en algunas versiones de sus dispositivos Cisco Security Manager y Cisco IOS XR.

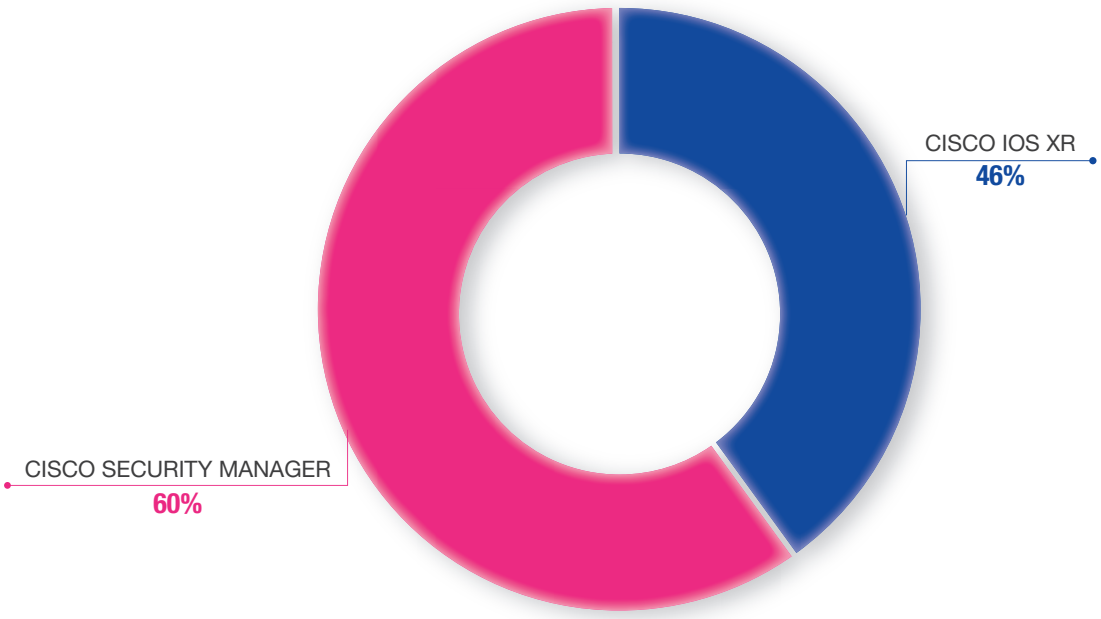
Teniendo en cuenta lo transmitido en el año anterior, en el cual las vulnerabilidades asociadas para **Oracle** fueron del 9% y para **Linux** del 13%; el CSIRT Financiero evidenció un cambio

representativo, situando a **Oracle** en el tercer lugar durante el año 2020 con un 23% resultado de las más de 700 vulnerabilidades identificadas que llegaron a comprometer productos o servicios, mientras que **Linux,** con un reporte del 4% que corresponde a 117 vulnerabilidades, se ubica entre los fabricantes con menos detecciones de debilidades en sus productos.

Se considera que las cifras anteriores se deben al aviso de **Oracle** sobre el aumento de sus ingresos tras el impacto del coronavirus, que conllevó a la captación de clientes, especialmente en su división cloud, tanto para utilizar su infraestructura como sus aplicaciones, entre los que se destaca Oracle Database Server. **Linux,** que sigue aumentando su cuota de clientes debido a la diversidad de distribuciones que amplían su portafolio, para el año 2020 también tuvo una expansión importante destacando MX Linux, Manjaro y Mint.

Con el objetivo de generar información más explícita, el CSIRT financiero presenta algunas categorías para la explicación de sus vulnerabilidades:

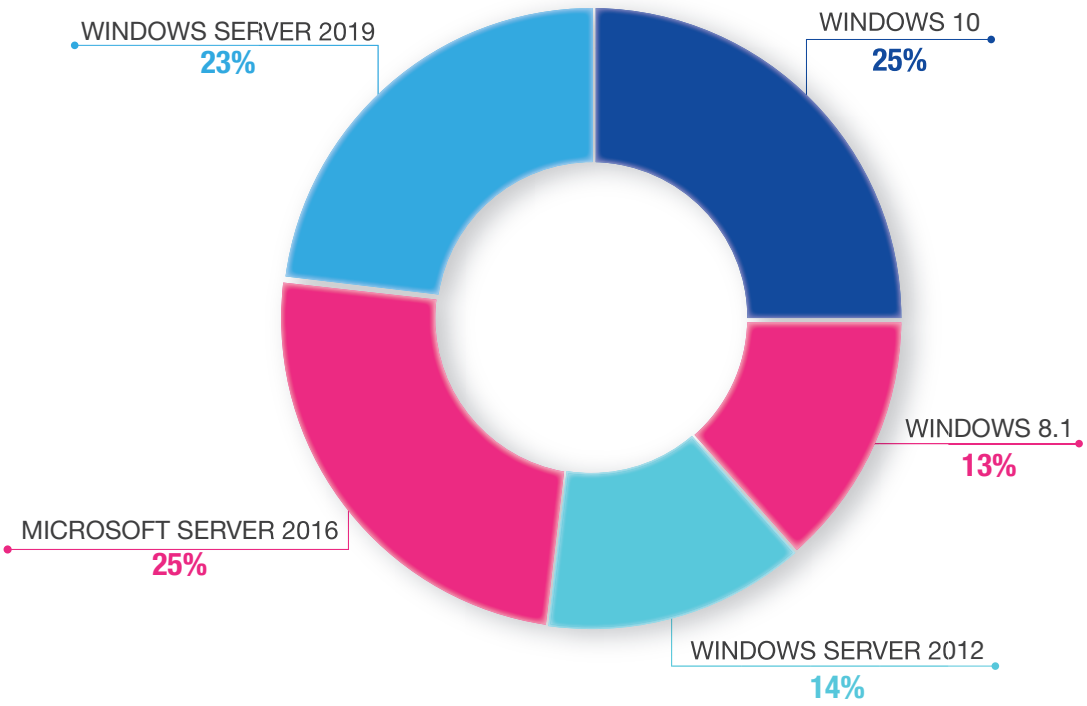
Productos CISCO con más vulnerabilidades relacionadas



Los productos **Cisco IOS XR** se vieron afectados por vulnerabilidades como CVE-2020-3566, que permite a un ciberdelincuente no autenticado **agotar la memoria de proceso** del dispositivo comprometido y CVE-2020-3118, que se debe a una validación incorrecta de algunas cadenas de entrada y podría causar **desbordamiento de pila** y/o **ejecutar** código arbitrario con **privilegios de administrador**, este último afectó directamente las versiones 5.2.5, 6.5.2, 6.5.3, 6.6.25, 7.0.1.

Las versiones 4.21 y anteriores de **Cisco Security Manager** se vieron afectadas por las vulnerabilidades, CVE-2020-27125, CVE-2020-27130 y CVE-2020-27131 las cuales permiten **acceso no autenticado** para la obtención de información, descarga de archivos y ejecución de comandos arbitrarios con privilegios.

Productos MICROSOFT con más vulnerabilidades relacionadas



En el 2020 se registraron 1187 vulnerabilidades para Microsoft, convirtiéndose en el fabricante con mayor número de vulnerabilidades asociadas; el CSIRT Financiero reportó 48 debilidades de este fabricante y, acogiendo la equivalencia de métricas de evaluación, 33 de estas con severidad importante, 9 críticas, 5 con valoración media y 1 con valor bajo.

Por su criticidad y valor de cvss correspondiente a 10.0 se destacan las siguientes:

- **CVE-2020- 1350**, se trata de una vulnerabilidad que permite ejecución de código remoto en los servidores del Sistema de nombres de dominio de Windows cuando no pueden manejar adecuadamente las solicitudes.

- **CVE-2020-0796**, vulnerabilidad que permite ejecución de código remoto en la forma en que el protocolo Microsoft Server Message Block 3.1.1 (SMBv3) maneja ciertas solicitudes.

Otras vulnerabilidades destacadas de este fabricante son los Zero-Day:

- **CVE-2020-1380**, vulnerabilidad que permite ejecución de código remoto en la manera en que el motor de scripting maneja objetos en memoria en Internet Explorer.

- **CVE-2020-1464**, vulnerabilidad de suplantación de identidad cuando Windows valida incorrectamente las firmas de archivos.

- **CVE-2020-17087**, vulnerabilidad de desbordamiento de búfer "basada en grupos" en el controlador de criptografía del kernel de Windows.

Entre las vulnerabilidades comunicadas por el CSIRT, se evidenció que muchas apuntaron a versiones de Windows 10, Windows Server 2016 y 2019, la explotación de estas permitiría realizar acciones como:

- Ejecutar código malicioso.

- Escalar en permisos hasta conseguir la mayor cantidad de privilegios.

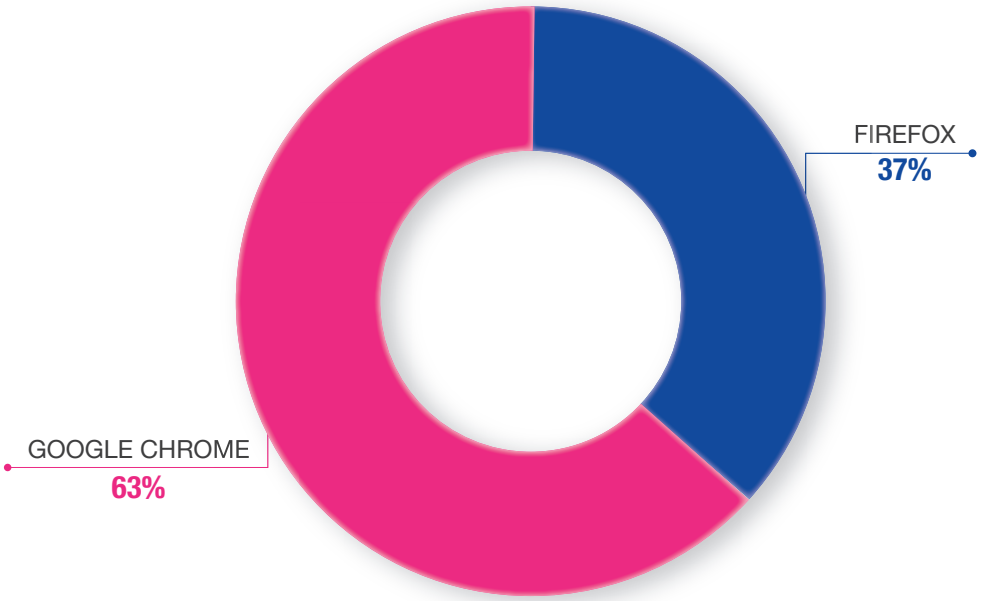
- Tomar control total del sistema afectado para instalar programas.

- Ver, modificar, borrar archivos o crear nuevas cuentas con todos los permisos.

- Evadir mecanismos de seguridad para cargar archivos firmados de manera indebida.

- Ejecutar aplicaciones especialmente diseñadas en un dispositivo de la red al establecer una conexión entre un canal Netlogon vulnerable con un controlador de dominio.

NAVEGADORES con más vulnerabilidades relacionadas



Google Chrome: tal como se ha planteado desde hace algunos años, Google sigue haciendo honor a su apodo de gigante de Internet y el navegador Chrome es una muestra de ello. Por su preferencia en **gran cantidad de usuarios**, también se convierte en un **blanco débil** que aprovechan los actores maliciosos que ven en éste, una puerta para expandir sus ataques. En el 2020 fue el **navegador con el mayor número de vulnerabilidades asociadas**, 227 en total. Entre las comunicadas por el CSIRT Financiero están: CVE-2020-6555, CVE-2020-15963, CVE-2020-15966, CVE-2020-16004, CVE-2020-16005, CVE-2020-16006, CVE-2020-16007, CVE-2020-16008, CVE-2020-16009, CVE-2020-16011, CVE-2020-16013, CVE-2020-16017 y CVE-2020-16010, está última afectando a Chrome en Android.

Mozilla Firefox: aunque el navegador en el 2020 no tuvo la misma cantidad de usuarios que años anteriores, sigue siendo **altamente comprometido**. Se consolidaron 132 vulnerabilidades en el 2020, algunas de las asignaciones para este producto son: CVE-2020-15683, CVE-2020-15684, CVE-2020-15678, CVE-2020-15675, CVE-2020-12426.

La mayoría de las vulnerabilidades reportadas para **estos navegadores** tienen una valoración **mayor a 8.5** y su explotación podría **permitir**:

- Obtener **información altamente confidencial** de la memoria de procesos a través de páginas HTML diseñadas.

- Aprovechar la **corrupción de la pila** (desbordamiento de buffer) a través de paquetes WebRTC especialmente diseñados.

- Escalar en permisos y ejecutar código con **suficientes privilegios**.

- Generar **denegación de servicios**.

- Ejecutar código arbitrario en el navegador y **adentrarse en el equipo**.

Principales amenazas cibernéticas: vulnerabilidades usadas por malware APT

El seguimiento realizado a los APT y diferentes familias de malware que tienen entre sus objetivos el sector financiero ha permitido identificar el uso de vulnerabilidades, destacándose durante el 2020 las siguientes relaciones:

- A lo largo del 2020 se identificaron campañas lanzadas por el grupo cibercriminal **APT-41.** Por un lado, aprovechando el error de Citrix Application Delivery Controller, conocido como **CVE-2019-19781**, para comprometer tecnologías y aplicaciones Cisco, Citrix y Zoho, con la ejecución de código que le permitiera obtener **acceso al dispositivo** afectado, y por otro lado, explotando el **CVE-2020-10189**, que permite la ejecución remota de código en instalaciones afectadas para obtener **privilegios de sistema** y expandir su ataque hasta comprometer más de 75 organizaciones alrededor del mundo.

- La vulnerabilidad con asignación **CVE-2020-1472**, conocida como **Zerologon** y en cadena con el **CVE-2020-25213**, tuvieron un aprovechamiento por parte de grupos maliciosos como **TA505, MuddyWater** y los desarrolladores del **ransomware Ryuk.** Las campañas se evidenciaron en mayor medida en el mes de octubre, entre sus objetivos se destacan: obtener un punto de apoyo inicial para ingresar a la red y comprometer los controladores de dominio de la organización, agregar herramientas como Mimikatz que permiten la instalación de otras cargas maliciosas o exfiltrar información sensible del equipo comprometido.

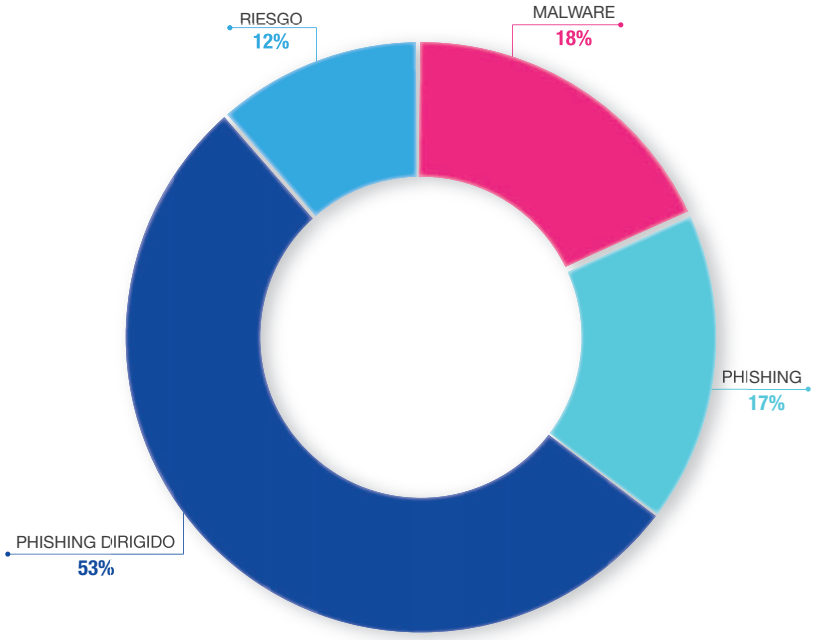
- La botnet conocida como **LemonDuck,** aprovechó diferentes fallas de seguridad, entre las que se destacan las vulnerabilidades BlueKeep **(CVE-2019-0708)** y SMBGshost **(CVE-2020-0796)**.

Apoyo a Incidentes

El procedimiento o capacidad de análisis y apoyo a incidentes que el **CSIRT Financiero** dispone para los asociados, está orientado en la **identificación preventiva de amenazas cibernéticas**, para ponerlo en conocimiento del asociado y **evitar la materialización de dichas amenazas**, así como el potencial impacto o problema que pueda llegar a ocasionar. De igual manera, el equipo técnico de especialistas y analistas, se encargan de realizar actividades enfocadas a la evaluación, investigación y análisis sobre los **posibles eventos o incidentes que reportan los asociados**, con el propósito de brindar información a partir de una investigación, generando valor para los asociados en pro de fortalecer la seguridad de los activos de información.

Durante el año 2020, la situación de pandemia puso a prueba a las entidades en la capacidad de transformar el desarrollo de actividades y prestación de servicios, todo dentro de un entorno de ciberseguridad que permitiera dar continuidad al negocio. Sin embargo, este suceso también fue utilizado por los cibercriminales que aprovecharon la situación de pánico y desinformación para generar campañas de distribución de malware con técnicas de phishing, para captar la atención de usuarios y trabajadores, dando como resultado la **captación de información confidencial** por medio de **falsos sitios web**, que suplantan la identidad de las compañías, o la infección de equipos de cómputo y redes corporativas con **software malicioso**.

Como resultado de un **trabajo colaborativo entre los asociados y el CSIRT Financiero**, durante la vigencia anterior, se logró gestionar y brindar **apoyo en la gestión de 193 incidentes** que tienen relación, principalmente, con la distribución de sitios de phishing, suplantación de sitios web o phishing dirigido, análisis de malware e identificación de vulnerabilidades, tal y como puede observarse en la siguiente imagen.

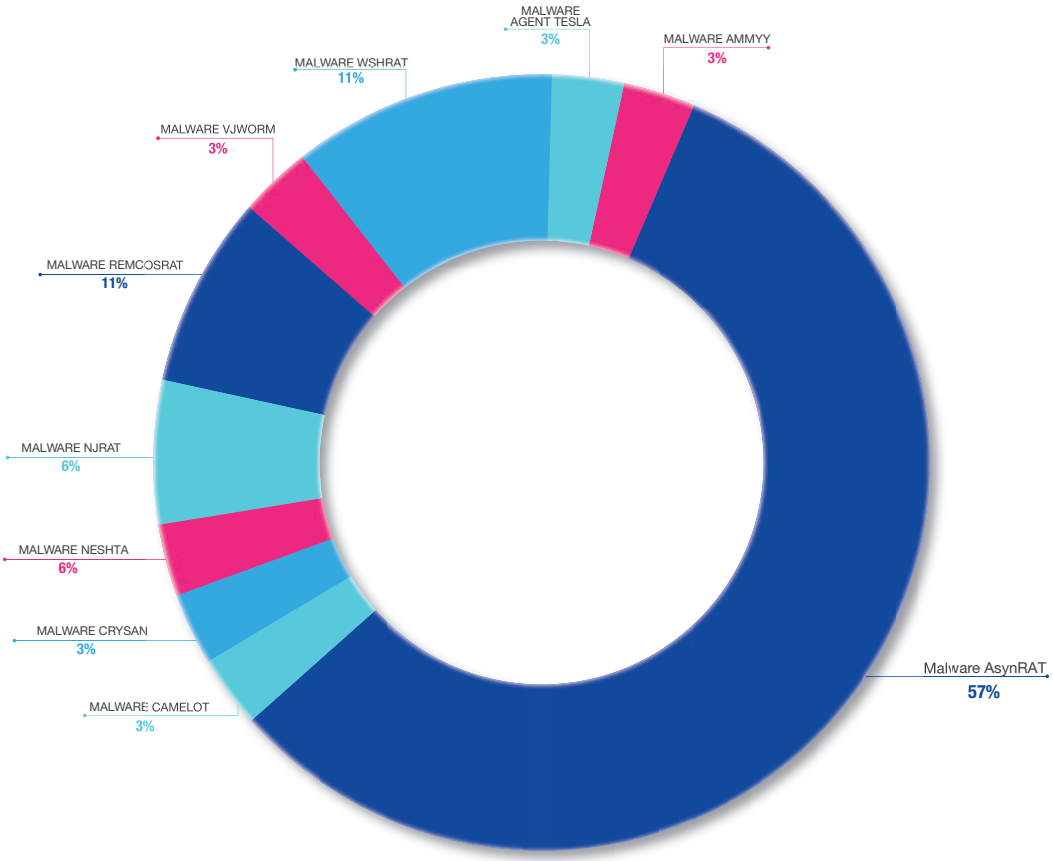


Se observa un **53%** que corresponde al **phishing dirigido**, asociado, principalmente, a la **suplantación de sitios web** que construyen, ponen en producción y distribuyen los ciberdelincuentes a posibles víctimas, con el propósito de recopilar información confidencial para cometer, principalmente, fraude financiero.

El siguiente **18%** corresponde al **malware** identificado desde el CSIRT Financiero, que está siendo **distribuido** a algunos de los **asociados** o que, por su parte, el **asociado identificó y compartió** para realizar el análisis correspondiente.

El **17%** hace alusión a las diferentes **técnicas de phishing** utilizadas para captar la atención de usuarios, haciendo que suministren información sensible en distintos sitios web. Finalmente, el restante **12%**, catalogado como **riesgo**, corresponde, principalmente, a la **exposición de información sensible** identificada en la Clear, Deep y Dark Web a partir de la cual, se pueden materializar incidentes de seguridad digital en contra del asociado que estuvo comprometido.

Por otra parte, sobre la cantidad de muestras de malware reportadas por los asociados e identificados por el CSIRT, al realizar el análisis correspondiente, se logró identificar que el troyano **AsyncRAT**, con un 57%, corresponde al **malware más distribuido** por las campañas ejecutadas por los cibercriminales. Es preciso mencionar que durante la anterior vigencia, el CSIRT Financiero desarrolló un informe de amenazas sobre este troyano de acceso remoto el cual posee el código **CRT-IA-20-003.pdf** y se encuentra disponible en el portal privado para su consulta.



En la imagen anterior, aunque con un porcentaje más bajo de identificación y análisis, aparece actividad ejecutada por parte de los troyanos de acceso remoto **WshRAT** con 11%, **RemcosRAT** con 8% y **NJRAT** con 6%, como las amenazas cibernéticas distribuidas directamente para comprometer las redes e infraestructura tecnológica de los asociados.

Por otra parte, a lo largo del año 2020, el **CSIRT Financiero** desarrolló y puso a disposición de los asociados **insumos de tipo PlayBook, Casos de uso, Monográficos e Informes de amenazas** que contienen información dirigida a fortalecer el entorno del ciberespacio, al comprender recursos humanos, operacionales y tecnológicos.

PlayBook

En la vigencia anterior, como resultado del análisis e investigación sobre amenazas cibernéticas, el equipo técnico desarrolló cinco **PlayBooks**, de los cuales en un primer PlayBook se indicaron las pautas dentro de los escenarios: preparación, detección, contención, mitigación y recuperación, respecto a los posibles incidentes ocasionados por el **ransomware Maze**. De acuerdo con esta información, luego fueron elaborados otros dos PlayBooks correspondientes a un compendio de actividades que aportan lineamientos para gestionar incidentes de seguridad informática causado por ransomware, describiendo allí el comportamiento, forma en que compromete los recursos y otras acciones realizadas por varias familias de este tipo entre los que se encuentran Exorcist, Ryuk y Sodinokibi.

De igual forma, se generó un PlayBook orientado al **análisis de técnicas de mayor concurrencia** que ejecutan los distintos tipos de malware como mecanismos para **generar persistencia** en la infraestructura tecnológica comprometida. En él, se detallan las principales claves de registro y utilización de bibliotecas de enlace dinámico, que en un sistema operativo Windows son comprometidas, como técnicas más comunes para lograr persistencia en los equipos afectados, aún cuando estos sean reiniciados.

Finalmente, se generó un Playbook que brinda a los equipos de respuesta a incidentes de seguridad informática **recomendaciones o pautas** para detectar, analizar y contrarrestar las actividades maliciosas ocasionadas por los troyanos de acceso remoto - **RAT**.

Casos de Uso

El objetivo fundamental de los casos de uso consiste en la **elaboración de un escenario** en el que se plantea un problema relacionado con el comportamiento de una **amenaza cibernética** y en base a ello, plantear una **solución idónea** para contrarrestar dicha amenaza.

El **CSIRT Financiero** estableció una serie de **controles y buenas prácticas** de estándares relacionados con la ciberseguridad, para que los **asociados adopten** dentro de sus compañías, con el propósito de **minimizar la exposición** y posible **impacto** frente a la materialización de un incidente ocasionado por el troyano de acceso remoto **AsyncRAT**, el cual posee una alta actividad delictiva enfocada hacia el sector financiero en Colombia.

Informes de Amenazas

Este tipo de informes se originaron luego de realizar la correspondiente **investigación**, en la cual se contempló un análisis acerca del **comportamiento** de los distintos **tipos de malware dirigidos** específicamente, al **sector financiero** o que por su finalidad o potencial afectación, puede llegar a comprometer los activos de información de nuestros asociados, como es el caso del **ransomware**, que niega el acceso

a la información indistintamente del sector económico, político o social.

En tal sentido, durante el año 2020 se generaron nueve informes de amenazas que describen el comportamiento de las campañas maliciosas logradas por los ciberdelincuentes para distribuir el malware, el reconocimiento de posibles objetivos, preparación del conjunto de técnicas y amenazas cibernéticas, canales o medios de distribución, la explotación que persigue ocasionar la amenaza, la respectiva instalación en el equipo para lograr el objetivo, la comunicación que el malware establece con los ciberdelincuentes por medio de infraestructura maliciosa y por último, las acciones deliberadas que ejerce el malware sobre el objetivo.

De acuerdo con lo anterior, los informes **comprenden el accionar delictivo** que realizan amenazas cibernéticas como lo son los **troyanos bancarios de origen brasileño**, responsables de atentar y generar actividad maliciosa en buena parte de Latinoamérica. En el mes de julio, se generó un informe sobre el troyano de acceso remoto **AsyncRAT** que contiene un histórico acerca de dicha amenaza, la correlación de eventos MISP, el análisis de las campañas ejecutadas, incluyendo el vector de infección y el análisis de las fases del **Cyber Kill Chain** del evento, los componentes o recursos del sistema empleados para la infección, las diferentes tácticas, técnicas y procedimientos (TTP) dispuestos en función de esta amenaza e incluso, las motivaciones detrás de los grupos de ciberdelincuentes principalmente **APT-C-36.**

Del compendio de informes de amenazas generados, el **informe sobre medios de pago** presenta un contexto de la seguridad de los dispositivos POS y menciona los ataques dirigidos contra los sistemas ATM, dispositivos tipo datáfonos y medios de pago en sitios web de comercio electrónico, mencionando los skimmers de tipo físico como lógicos al igual que malware dirigido contra este tipo de medios.

El informe de resumen del **Observatorio de Ciberseguridad y Cibercriminalidad en Colombia**, presenta un contexto de las amenazas dirigidas con afectación a compañías del sector financiero en el ámbito global y nacional respectivamente. Dicho informe de Cibercriminalidad contiene la tipología presente en Colombia, los modelos de tendencias ejecutadas, los presuntos estados y grupos encargados de llevar a cabo dichas labores delictivas así como los diversos esquemas establecidos sobre el comercio de bines, carders, personas catalogadas como “money mules”, que prestan su nombre y cuenta bancaria para recibir transferencias monetarias producto del desarrollo de actividades ilícitas, y los grupos de hacktivistas, que promueven ideologías, pensamientos enfocadas a condiciones sociopolíticas.

Es preciso destacar que a comienzos del mes de septiembre, teniendo en cuenta labores de investigación que incluyeron realizar un proceso sistemático de prospectiva o vigilancia cibercriminal y de reportar de manera oportuna notificaciones y alertas, se generó un informe de amenazas sobre el **ransomware Sodinokibi**, que afectó al

Banco Estado de Chile. En él se detalla la evolución y correspondiente análisis de la amenaza, el estudio técnico incluyendo principales vulnerabilidades explotadas, las herramientas utilizadas durante el procedimiento y las correspondientes acciones de detección previa a la infección.

Siguiendo la misma línea de investigación acerca del potencial impacto que genera el ransomware, se llevó a cabo un **trabajo colaborativo** entre el CSIRT Financiero y el asociado **Bancolombia S.A.**, en cuyo informe se plasmó el estudio técnico logrado sobre dos muestras del ransomware **Exorcist**, detallando el comportamiento, funciones ejecutadas sobre equipos vulnerados con sistema operativo Windows, TTP´s implementadas durante el procedimiento de infección, el modelado o flujo de operación de la infección y correspondientes recomendaciones que se deben tener frente a este tipo de amenazas.

Cabe mencionar que el **trabajo mancomunado aporta valor** para los equipos de respuesta a incidentes de seguridad informática, en el entendimiento y capacidad de hacer frente ante este tipo de amenazas cibernéticas, por lo que se invita a los demás asociados a crear espacios de investigación y co-creación de productos que aporten inteligencia y madurez, para hacer frente a las diferentes amenazas cibernéticas que atentan en contra del sector financiero.

Monográficos

A inicios del año 2020 se puso a disposición de los asociados, un monográfico acerca de las **tendencias del malware contra dispositivos móviles.** En su contenido, producto de una investigación, se describen las principales vulnerabilidades existentes en los aparatos móviles, se analizan y detallan las categorías de malware dirigido, los principales vectores de

ataque que comprometen e intentan vulnerar los equipos móviles y se presentan las tendencias en cuanto a unos posibles escenarios que se pueden presentar debido al aumento de amenazas enfocadas a estos dispositivos, la implementación de TTP´s que causen una mayor afectación y otras técnicas logradas para irrumpir y sortear los controles en la tienda de aplicaciones.

Para el mes de mayo, el equipo técnico del CSIRT Financiero generó un monográfico que describe los **factores relevantes** que logran que, a partir de técnicas de ingeniería social, la **distribución de phishing y spearphishing** se propague e infiltre malware de distinto tipo en las organizaciones. El monográfico contiene los principales vectores de ataque, entre los cuales se describe el comportamiento del **phishing en Colombia** a través de las diversas tácticas, técnicas y procedimientos, al igual que el estudio acerca de los principales tipos de archivos con contenido malicioso que se distribuyen por medio de campañas ejecutadas por cibercriminales.

El último de los monográficos formulado durante el 2020 tuvo un enfoque que detalla el comportamiento de las **ciberamenazas sobre los medios de pago físicos**, al tratarse de los cajeros automáticos o **ATM** y digitales que comprende los portales web transaccionales, aplicaciones bancarias para dispositivos móviles, los terminales de punto de venta **(TPV o POS)**, los monederos de criptomonedas y el sistema de pagos en línea PayPal. A su vez, el monográfico presenta un análisis sobre las principales muestras de malware de tipo POS y skimmer conocidos como **GLITCHPOS y GSTATICAPI**. Además de presentar las principales tendencias las cuales estuvieron soportadas en temas relacionados con el COVID-19, los skimmer y el malware móvil.

Reglas

El CSIRT Financiero compartió con los asociados un total de **68** reglas de distintos fabricantes, que tienen como **finalidad** ser **implementadas en herramientas de seguridad tipo SIEM**, facilitando y describiendo eventos de registros de seguridad informática que sean relevantes en la **detección de comportamientos de amenazas cibernéticas**. A continuación se enumeran las reglas generadas sobre el tipo de amenaza

Regla	Amenaza / Vulnerabilidad	Total
YARA	APT 28 - backdoor Zebrocy	1
SIGMA	APT 29 - FireEye	23
YARA	Gootkit	2
SIGMA	Gootkit	1
YARA	SombRAT	1
YARA	Qbot	2
SIGMA	Qbot	1
YARA	RansomExx	1
YARA	Vizom	1
YARA	Sodinokibi	3
SIGMA	Sodinokibi	11
YARA	Bizonal	1
SURICATA	Ursu	1
YARA	Ursu	1
SNORT	Ursu	1
YARA	CessoATM	1
YARA	RevCode WebMonitor RAT,	1
YARA	Evilnum	1
YARA	Javali	1
SURICATA	Azorult	2
YARA	Azorult	1
SIGMA	Yellow Cockatoo	1
SIGMA	Crutch	1
SIGMA	CVE-2018-13379, CVE-2020-14750, CVE-2020-14882, CVE-2019-2725	4
AZURE SENTINEL	CVE-2020-1472	1
SIGMA	CVE-2020-1472	1
QRADAR	CVE-2020-1472	1
SPLUNK	CVE-2020-1472	1

Tendencias de ciberseguridad para 2021

El 2020 fue un año sin duda de adaptación para muchas organizaciones de todo el mundo debido a la pandemia de la Covid-19. El teletrabajo se convirtió de una opción a una obligación, no llevada a cabo por las áreas tecnológicas, sino más bien por la Covid-19, que pasó de ser un virus a casi una normativa de cumplimiento para el teletrabajo.

Por supuesto, todo tiene su lado bueno, y es que el teletrabajo ha venido para quedarse. Esto en sí, tiene múltiples implicaciones para las organizaciones que deben de tener en cuenta, y los cibercriminales lo saben, aprovechándose de la situación.

El perímetro de seguridad de las empresas se extiende y diluye hacia los hogares de los empleados. Cada empleado se convierte en un punto de acceso a la red corporativa y un potencial punto de ataque, ya que las redes de hogar, son más vulnerables a un ataque informático. Asimismo, la nube también se convierte en una extensión de la red corporativa, mejorando su seguridad, cifrando sus conexiones, etc, aunque durante el 2021, será necesario seguir mejorando y ampliando los sistemas de seguridad, tanto de la nube como de la red de teletrabajo, puesto que en 2021, el teletrabajador será el vector de ataque número 1 para la explotación de los cibercriminales.

Desde el CSIRT Financiero, se ha realizado un estudio minucioso de todas las amenazas investigadas en este 2020 con el objetivo de poder identificar algún tipo de patrón o tendencia que pudiese verse durante el 2021.

1 - Ransomware sin escrúpulos

Si a finales del año 2019 se empezaron a observar un incremento de campañas relacionadas con ransomware, lo que sucedió a lo largo del 2020 fue similar, incrementándose y con una tendencia al alza.

El **concepto de ransomware** que hasta hace poco conocíamos, **ha cambiado** por completo. Atrás quedaron aquellas muestras iniciales de ransomware que eran distribuidas de manera directa, a través de un correo electrónico, y que al cifrar el sistema, pedían un rescate si querías recuperar la información.

Lo que conocemos a día de hoy como **ransomware**, se trata de una **pieza más de malware**, distribuida en una **etapa final** después de que, en primera instancia, hayan sido ejecutadas muestras de 1ª, 2ª y hasta 3ª etapa, para llegar a la carga final donde se encuentra el ransomware.

Todas esas piezas previas y la propia muestra final del ransomware, incorporan técnicas de evasión, mecanismos para infectar otros sistemas de la misma red y otras tantas muy sofisticadas, consiguiendo así **dificultar el trabajo** de muchos **fabricantes de seguridad y analistas de malware**.

Otra característica que, a día de hoy, ha avanzado en el ransomware son las **extorsiones**. Se ha observado en las últimas campañas de ransomware que, antes de comprometer el sistema mediante el cifrado de archivos, los ciberdelincuentes **roban la información que será cifrada**, pidiendo un **rescate**, no sólo para liberar el sistema, si no también para recuperar los datos y **evitar que los hagan públicos**.

Adicionalmente a esto, se ha observado durante el 2020 y que seguirá siendo una tendencia en el 2021, cómo los cibercriminales utilizan markets de la deep web con los siguientes objetivos:

- Anunciar las víctimas que han conseguido comprometer
- Poner a la venta la información que han conseguido exfiltrar (antes de cifrar los datos, exfiltran la información para tener control total)
- Poner a disposición de todo el mundo archivos de pruebas que corroboren el compromiso

Estos nuevos objetivos de los cibercriminales que distribuyen ransomware, ha conseguido que las **organizaciones entren en pánico** y realicen los **pagos de una manera más ágil**, ya que, en una primera instancia, recuperar los datos en algunos casos podía ser "sencillo" en caso de que tuvieran planes de backups, sin embargo, el hecho de que la información sea publicada en Internet si no se paga el rescate, es otro factor que puede salir muy caro a muchas organizaciones.

Por lo general, estos ataques y chantajes entre víctima y actor son escenarios duraderos en el tiempo y que se componen de diferentes etapas, donde en muchas ocasiones, existe hasta un soporte mediante chat para poder tener una comunicación fluida con el cibercriminal y preguntar cualquier duda que existiese, como si de un soporte técnico de la compañía de telefonía se tratase.

Un factor importante en muchas infecciones que han podido identificarse por ransomware durante el año 2020 y que seguirán ocurriendo, se deben a la **explotación de vulnerabilidades** relacionadas con **servicios expuestos** que no deberían de ser visibles para todos. Un claro ejemplo de esto es el **protocolo de conexión remota RDP**. La adaptación al **teletrabajo** ha tenido que realizarse de una manera muy rápida y poco segura, favoreciendo en una balanza la usabilidad en vez de la seguridad.

Pero también han existido casos donde ha bastado con realizar **ataques de**

fuerza bruta de contraseñas para poder entrar en los sistemas, lo que evidencia el **uso de credenciales débiles** en protocolos expuestos de Internet.

Es de vital importancia, que para reducir los posibles objetivos de un cibercriminal contra nuestra organización, en primer lugar sepamos que tenemos expuesto. Las **auditorías de reconocimiento** pueden ayudarnos en estos casos. En este sentido, el famoso término Shadow-IT, que hacía referencia a redes internas indicando "No te puedes defender de lo que no conoces", puede usarse en estos tiempos de manera externa, ya que en muchos casos, existen organizaciones que **no saben qué activos tienen publicados en Internet**.

2 - Acceso inicial: Explotación de vulnerabilidades

Durante el Q4 del pasado año 2020, se experimentó una subida en las explotaciones de vulnerabilidades por los cibercriminales como acceso inicial a las redes y sistemas de sus víctimas.

Tecnología de diferentes fabricantes fueron explotadas a través de vulnerabilidades conocidas y exploits que se aprovechaban de dichos fallos de seguridad. Esto, muy relacionado con la anterior tendencia mencionada, fue aprovechado por los grupos de cibercriminales para introducir ransomware en infraestructuras y poder así cifrar diversos sistemas.

Este incremento, sin duda, fue en alza desde el confinamiento en todos los países, ya que obligaba a las organizaciones a exponer nuevos servicios en Internet para que sus empleados pudieran llevar a cabo su jornada laboral sin ningún tipo de inconveniente.

Para este año 2021 y los próximos se prevé que muchas empresas mantengan el teletrabajo implantado, ya que esto beneficia al empleado que puede trabajar desde cualquier lugar y la organización abarata sus costes, ya que no depende de tener un lugar físico para que sus empleados puedan ir.

Por lo tanto, los cibercriminales aprovecharán esta casuística hasta que las organizaciones consigan fortalecer de una manera correcta y efectiva

sus servicios expuestos en Internet, evitando que puedan explotar algún tipo de vulnerabilidad y poder realizar acciones en las redes internas.

El desarrollo de exploits y su posterior venta en markets de la deep web pueden ser un importante actor para estas situaciones durante los próximos meses.

3 - Deep Fake e Inteligencia Artificial: combinación explosiva para la ingeniería social

Deep Fake hace referencia a **vídeos falsos** en los que se **suplanta la identidad** de alguna celebridad, ya sea por **diversión** o como forma de **atentar contra la intimidad y la reputación** de una persona.

Comienza su andadura en 2017, pero gracias a los avances tecnológicos, cada vez es más **fácil y sencillo realizar este tipo de vídeos.** Incluso existen aplicaciones móviles que, a modo de entretenimiento, permiten realizar este tipo de producto audiovisual.

Pero cómo sucede siempre, cuando avanza la tecnología, los ciberdelincuentes comienzan a idear nuevas maneras de llevar a cabo sus actividades ilícitas y a explotar las nuevas herramientas en su propio beneficio.

En 2019, el uso de unos audios falsos que suplantaban la voz del CEO, se utilizaron para robar millones de dólares en tres empresas. Es la **nueva generación** del conocido "Fraude al CEO".

Para ello sólo se necesita disponer de fuentes de audio y vídeo como charlas o conferencias) y la Inteligencia Artificial y el Deep Learning aprenderán de ellos para imitar a la perfección su voz, sus movimientos y su personalidad.

En 2021 se espera que este tipo de ataques aumenten, orientándose **hacia ataques hiperpersonalizados a usuarios con privilegios**, ya sea por tener **puestos de responsabilidad** dentro de las compañías, como por tener **privilegios de acceso a la red corporativa.**

Es una amenaza todavía muy nueva, pero que está evolucionando a un ritmo tan rápido que, si no se frena pronto, tiene atisbos de convertirse en un problema a nivel mundial, sobre todo, porque es una técnica tan realista, que a simple vista cuesta mucho identificar si se trata de una falsificación, y ni las empresas, ni las entidades financieras, ni los gobiernos, ni las redes sociales ni los medios de comunicación están preparados para hacer frente a este tipo de amenaza. Invertir en **concienciación** será la herramienta fundamental de las entidades para evitar ser víctima de este tipo de fraudes.

4 - Nuevos riesgos en el IoT: el teletrabajo

Desde que nació el llamado **Internet de las Cosas** (IoT), los dispositivos que lo conforman siempre han estado expuestos a v**ulnerabilidades y fallas de seguridad**. Para el año 2021, se espera que los riesgos más preocupantes derivados del IoT provengan de la relación entre los **dispositivos**

domésticos inteligentes y el teletrabajo.

La línea entre los dispositivos personales y profesionales se está difuminando, provocando un aumento significativo en la superficie de ataque general. Los **hogares inteligentes**, en los que Alexa, Siri, Google Home o Amazon Echo nos facilitan la vida, apagando y enciendo luces, poniendo música o encendiendo la tele, pueden convertirse en ***insiders* involuntarios en nuestro puesto de trabajo**. Mientras estos **dispositivos estén conectados, escucharán** y recogerán cualquier información que pueda surgir de las reuniones en streaming, de las llamadas de teléfono entre compañeros, etc.

Esta **información recopilada** será guardada en alguna parte y, por el momento, no está claro que se hace con ella cuando está en la nube, si es procesada, analizada, clasificada, etc.

Por ello, y debido a que el teletrabajo ha venido para quedarse, es importante ser conscientes que si en casa **tenemos asistentes domésticos inteligentes**, es mejor **desconectarlos** durante nuestra **jornada laboral** y, tenerlo muy presente cuando es necesario trabajar fuera de dicho horario.

5. Identidades sintéticas para delitos financieros

El fraude al sector financiero a través de identidades sintéticas está en **auge en Estados Unidos** y se espera que a lo largo de 2021 se abra a **otras geografías,** animado por el auge de las operaciones bancarias online, debido a las medidas de prevención de la COVID-19.

Las identidades sintéticas se crean utilizando una **combinación de información personal identificativa** (IPI) **real y falsa** o **totalmente falsa**, que después se utiliza para **abrir cuentas bancarias ilegítimas**. Suelen utilizar información de personas sin apenas historial de crédito, para que las entidades financieras no tengan expedientes anteriores, lo que hace menos probable que salten las alarmas. Por lo tanto, la **información de los jóvenes es la más buscada** por los fraudsters, porque carecen de historial de crédito, al igual que los niños y los ancianos.

El **crimen organizado** hace uso de este tipo de identidades para **abrir cientos de estos tipos de cuentas** para el blanqueo de capitales, cuentas mula o para elevar las calificaciones de crédito de las cuentas mediante reembolsos inmediatos y ampliar los límites de crédito, antes de desaparecer retirando todos los fondos posibles, sin ninguna intención de devolverlos.

La amenaza reside en que **la mayoría de los sistemas de detección de riesgos no alertan** sobre las identidades sintéticas, porque las identidades falsas parecen de clientes reales con un historial de crédito limitado que solicitan una cuenta.

La **monitorización continua de usuarios**, analizando su forma de interactuar con la entidad y generando un perfil general del *fraudster*, son algunas de las medidas que se pueden adoptar para evitar este tipo de delito.

6 - Ataques más sofisticados y silenciosos

Los APTs cada vez realizan ataques más sofisticados contra sus víctimas, no con exploits que explote vulnerabilidades no conocidas de productos ni con malware novedoso que implemente técnicas muy complejas. Si bien es cierto que los exploits y el malware en ocasiones es complementario, lo que realmente les está haciendo llevar a cabo ataques más silenciosos y complejos es el uso de software legítimo del sistema para obtener conseguir sus objetivos.

Los denominados LOBAS (Living Off The Land Binaries and Scripts and also Libraries) que son aplicaciones, scripts y funcionalidades legítimas que integra el sistema operativo son cada vez más usadas por los APTs en sus intrusiones.

El hecho de que usen este tipo de técnicas tiene varios beneficios:

1. No requiere tener altos conocimientos y existe una gran cantidad de documentación de dichas funcionalidades. Sin ir más lejos, la funcionalidad WMIC de Microsoft Windows (muy usada por los APTs) tiene una gran cantidad de documentación generada en su repositorio de docs.

2. Por lo general, no hace ruido en el sistema donde se emplea la técnica, a menos que existan alertas configuradas para notificar de su ejecución a los usuarios, algo que no es normal. El motivo de esto es sencillo, el uso de una funcionalidad del sistema no es considerado una acción maliciosa, sin embargo, si que se puede usar durante las intrusiones.

3. El tiempo de planificación de una campaña por parte de los APTs es reducido, ya que lo que hacían antes con el desarrollo de un malware que consiguiera X objetivo, a día de hoy es conseguido sencillamente mediante una funcionalidad nativa del sistema operativo.

Para poder paliar estas técnicas, los EDR jugarán un papel muy importante durante los próximos años ya que, serán los principales responsables de ver los comportamientos que tengan lugar en los puestos de trabajo de los empleados.

[35] https://www.welivesecurity.com/la-es/2019/09/11/estafadores-utilizan-inteligencia-artificial-imitar-voz/

[36] https://www.fbi.gov/audio-repository/ftw-podcast-espanol-synthetic-ids-010920.mp3/view

Tendencias tecnológicas para el sector 2021

1. Neobancos y digitalización de procesos

Los **neobancos** son entidades bancarias **sin oficinas físicas**. Las operaciones se realizan a través de la **app móvil**, siendo innecesario entrar en su página web. Como se ha comentado a lo largo del documento, las medidas de distanciamiento social y el detrimento del pago en metálico frente al pago con tarjeta o a través del móvil, **han incrementado el uso y contratación de este tipo de bancos**, como es el caso de Monzo, Revolut o Qonto, tendencia que se mantendrá a lo largo del 2021, debido a la continuidad de la pandemia y a las preferencias de los usuarios.

Por su parte, los **bancos tradicionales**, iniciarán o continuarán llevando a cabo una importante **digitalización de sus procesos** para adaptarse a la nueva situación social y continuar siendo competitivos dentro de su sector.

Es muy posible que en un futuro no muy lejano, los **cajeros y el dinero en efectivo** acabe **desapareciendo**. En España, por ejemplo, desde 2016, los bancos fueron incrementando la implantación de nuevos ATM. Sin embargo, en 2020, esta tendencia se ha roto y el volumen de máquinas ha disminuido en unas 600, bajando el umbral de los 50.000. En el tercer trimestre del año, el **descenso** es del 2,7% interanual, que es superior al 1,6% de los tres meses precedentes.

Por lo tanto, a lo largo de 2021 se irá viendo una d**isminución del malware ATM,** ya que los cibercriminales dirigirán sus ojos a la **creación de nuevos troyanos bancarios** para los dispositivos **móviles**.

La proliferación de los **neobancos y la digitalización de procesos** que estamos viviendo actualmente, prefiguran una posible **disrupción** del **sector de la banca** tradicional.

2. Blockchain everywhere

La tecnología blockchain es una realidad y, a pesar de estar en sus comienzos, promete **revolucionar el modo en que se gestiona la información en el mundo digital**. Cada vez se está implantando más, y no sólo en el tema de criptoactivos, sino a través de otros sectores para proteger datos o crear identidades digitales. Por ejemplo, en el Consumer Electronics Shows de Las Vegas, celebrado en 2020, (CES 2020) **se presentó el primer teléfono inteligente** basado en la **tecnología blockchain.** Así, los **usuarios** tendrán el **control de sus datos**, los cuales ya no estarán sujetos al manejo por parte de aplicaciones, sitios de internet y otros servicios. Como resultado, **terceros no podrán monitorear o bloquear los datos.**

Se espera que en 2021, muchos de los sectores económicos comiencen a

implantar esta tecnología, aportando una **mayor seguridad y claridad a los procesos.** La industria del gas y petróleo podrán aprovechar el potencial de esta tecnología con el fin de asegurar las operaciones de procesos complejos, como lo es el transporte de los suministros donde participan diferentes actores. En el sector alimentario, existen aplicaciones que permiten rastrear la fuente de los ingredientes que se usan para cocinar alimentos, digitalizando las transacciones de las cadenas de suministro y garantizando mayor transparencia y confianza en este proceso.

En el **sector financiero**, la revolución puede llegar a cambiar nuestro modo de relacionarnos en el mundo digital de la banca, favoreciendo, entre otros aspectos, la **inmediatez de la transacción**, su **trazabilidad**, y una mayor **información ligada a cada transacción.** Además, permite una **reducción de la burocracia** necesaria en las operaciones financieras y mejora la **transparencia**.

Son muchas las entidades bancarias las que están realizando carreras contrarreloj para implementar soluciones, procesos y herramientas basadas en esta tecnología, y así seguirá siendo durante el año 2021.

3. Zero Trust

Los modelos Zero Trust Architecture (NIST Special Publication 800-207. Zero Trust Architecture) parten de la **premisa** de que n**o existe confianza para las comunicaciones de aplicaciones, sistemas o usuarios dentro de una misma red.** Es una solución que el NIST y la Cybersecurity & Infrastructure Security Agency del Departamento de Homeland Security de USA plantean de cara a que las organizaciones implementen estas medidas.

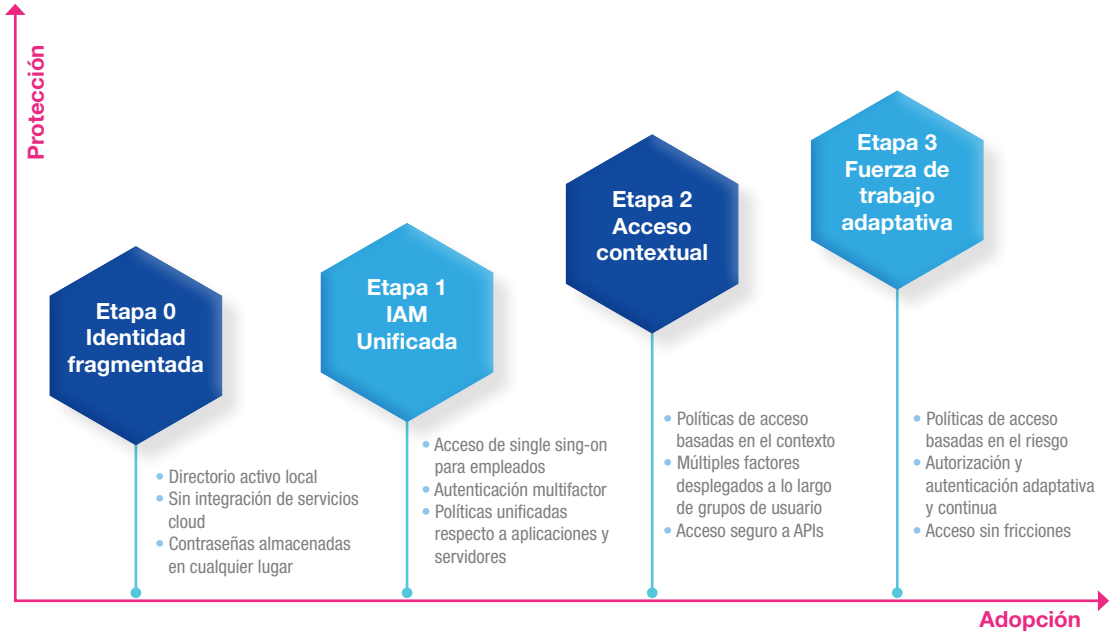
Sin duda es una **apuesta arriesgada** implementar este tipo de arquitecturas en las organizaciones, pero los **resultados** en cuanto a **seguridad** pueden ser **muy buenos,** ya que en caso de que exista un **incidente**, el **impacto** en comparación a como están diseñadas por lo general las redes hoy día, es **bastante menor.**

En un momento donde los usuarios cada vez trabajan más desde sus casas y en muchos casos, incluso con sus propios sistemas que no son controlados por las áreas de IT… ¿Quién puede confiar en ellos?

Implementar esta capacidad **requiere una plataforma de identidad unificada** que consta de **cuatro elementos clave** dentro de un sólo modelo de seguridad.

1. Verificar el usuario
2. Verificar su dispositivo
3. Limitar el acceso y privilegio
4. Aprender y adaptar

Curva de madurez Zero Trust



4. BAS: Breach and Attack Simulation

Las tecnologías BAS están orientadas a evaluar la efectividad de los procedimientos de seguridad, infraestructura, vulnerabilidades y técnicas mediante el uso de simulación de violación y ataques a plataformas.

A través de la simulación de ataques, se pone a prueba el nivel de seguridad y respuesta ante un ataque de **ransomware**, ataques de **phishing** y **whaling**, o hacer clic en banners y enlaces **maliciosos** en sitios web sin afectar a los sistemas de producción.

Las plataformas "Breach and Attack Simulation" **simulan ataques múltiples**, internos o externos, atacando las **vulnerabilidades más recientes**, incluidas las que se encuentran en estado embrionario. De esta forma, las posibles brechas de seguridad que existan, permiten a la organización determinar si la arquitectura de seguridad proporciona la protección adecuada y si las configuraciones se implementaron de forma adecuada.

Por ello, y debido a la creciente expansión de la superficie de seguridad de las entidades, sufrida en 2020 por la implantación urgente del teletrabajo, este tipo de tecnologías experimentarán una evolución importante durante el año 2021.

Desde el **CSIRT Financiero** se están generando **nuevas emulaciones sobre amenazas financieras** (principalmente APTs) para que puedan ser **ejecutadas** en las infraestructuras de los bancos de **manera controlada.** Esto persigue los siguientes objetivos:

1. Identificar si en las entidades financieras existen capacidades de **visibilidad**.

2. En caso de que exista capacidad de **visibilidad**, verificar que también existen mecanismos de **detección**. Es decir, si hay tecnología que permite dar visión de los sucesos, habrá que configurarlos para que detecte los eventos y genere algún tipo de notificación.

3. Mejorar los procesos de **Threat Hunting** internos, permitiendo a través de estas emulaciones realizar detecciones basadas en intrusiones reales de actores.

ASOBANCARIA

Hernando José Gómez
Presidente

Mónica María Gómez Villafañe
Vicepresidente Administrativa y Financiera

Angela María Vaca
Directora Nuevos Negocios

MNEMO

Equipo técnico y de operación del CSIRT

Emanuel Ortiz
Codirector Operativo

Roberto Peña
Codirector Estrategia

Eva Moya
Responsable Implantación Estrategia

Jose Luis Sánchez
Director Técnico

Carlos Javier Beltrán
Coordinador Operación

Carlos Guzmán
Líder Técnico

Leticia Lanuza
Líder Dirección Documental

Carlos Rojas
Líder Gestión

Ximena Galindo
Líder Calidad

Belén Viqueira
Tendencias y Prospectiva

MOUSE GRAPHIC

Adriana Cuéllar González
Diseño y Diagramación


5,000
2.08
75,000
2.08
500
2.08
40,000
2.08
22,000
2.08
4,000
2.08
20,000
5,000
sales

www.csirtasobancaria.com
csirt@asobancaria.com
incidente@csirtasobancaria.com
Tel: (+571) 4391639
018000111505
+57 3174345665

@CsirtFinanciero

ASOBANCARIA
Construyendo
la **Confianza** y **Solidez** del sector financiero