MEMORIA ANUAL

CSIRT FINANCIERO ASOBANCARIA

2019

CSIRT FINANCIERO

ASOBANCARIA

Santiago Castro Gómez
Presidente
Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA

Mónica Gómez Villafañe
Vicepresidente de Admón.
Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA

Angela María Vaca Bernal
Directora Nuevos Negocios
Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA

Equipo Técnico
Alba Valdés
Emanuel Ortiz
Eva Moya
José Libardo López
Leticia Lanuza
Miguel Ángel Martín

Preparado y publicado por el Programa de ciberseguridad del sector - CSIRT Financiero - de Asobancaria (www.asobancaria.com – www.csirtasobancaria.com)

Los contenidos expresados en este documento se presentan exclusivamente para fines informativos. Publicación: abril del 2020.

ÍNDICE

CSIRT Financiero y Ciberamenazas en 2019

1

Tendencias en ciberamenazas para 2020

2

Tendencias tecnológicas para el sector

3

IMÁGENES Y GRÁFICAS

IMÁGENES

GRÁFICAS

APERTURA DEL CSIRT

PRÓLOGO

Seguridad y Transformación Digital de la Banca
de cara al 2020

Por **Mónica Maria Gómez Villafañe**,
Vicepresidente Asobancaria, responsable del Programa de cooperación para la ciberseguridad
CSIRT Financiero

La década que cerramos en 2019 se consolidó como el periodo de mayor innovación para distintas industrias gracias al proceso de incorporación de tecnologías en sus servicios y procesos. La industria bancaria en Colombia no ha sido ajena a la tendencia de digitalización y ha sabido aprovechar los beneficios que brinda una mayor conectividad. Hoy, los usuarios del sector bancario en nuestro país realizan el 63% de sus transacciones a través de canales digitales y realizan anualmente 292 millones de visitas a los portales bancarios.

Este acelerado proceso de digitalización de los servicios financieros no estaría completo si no tuviera la seguridad como uno de sus pilares fundamentales. Las entidades bancarias, catalogadas como infraestructuras críticas, han realizado importantes esfuerzos en el fortalecimiento de sus capacidades para la detección y mitigación de amenazas en el ciberespacio protegiendo así su operación y al consumidor financiero.

Una de las estrategias de mayor relevancia e impacto a nivel de adopción de estándares internacionales y cooperación para la prevención de riesgos, es la puesta en marcha del Centro de Investigación e intercambio de información cibernética del sector financiero colombiano -CSIRT FINANCIERO- de Asobancaria, en el cual se concentran y se monitorean en tiempo real las ciber amenazas para las entidades financieras, a través de herramientas de última tecnología, un equipo altamente especializado y fuentes de información globales.

El CSIRT Financiero se sustenta en relaciones de cooperación local entre sus miembros e internacional con agencias de investigación y una continua articulación con autoridades; a través de una plataforma en línea las entidades financieras, autoridades, y centros de investigación a nivel global, regional y local comparten información frente a amenazas cibernéticas.

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. No debemos olvidar el efecto sistémico que podría significar un incidente cibernético en cualquier entidad del sector. En materia de seguridad no somos competencia, por el contrario, somos aliados.

Con las operaciones que adelanta CSIRT hoy, entre ellas, el registro de incidentes del sector, la generación de alertas tempranas, indicadores de amenazas, análisis y entrega informes de inteligencia tácticos, operativos y estratégicos, ayudamos a las entidades financieras a afrontar los riesgos digitales que se les presentan y a proteger a sus usuarios.

Desde su puesta en operación en junio de 2019, CSIRT Financiero ha analizado en tiempo real 285.435 Indicadores de Compromiso (IoC), ha entregado 406 alertas sobre riesgos cibernéticos para el sector; y ha desarrollado diferentes actividades de sensibilización sobre los riesgos digitales a nivel directivo y operacional de las entidades financieras.

Durante 2019, bajo los acuerdos de cooperación de CSIRT se realizó la misión de seguridad digital a Estados Unidos con la OEA en el cual participaron vicepresidentes de entidades financieras y se realizó el primer foro especializado en inteligencia de amenazas cibernéticas en América Latina en alianza el Centro de Análisis e Intercambio de Información de Servicios Financieros -FS ISAC-, entidad que busca reducir el riesgo cibernético en el sistema financiero global.

El CSIRT sectorial también participó activamente de la iniciativa de ColCERT para implementar la plataforma MISP (Malware Information Sharing Platform) herramienta que permite el intercambio de información de amenazas cibernéticas en forma multidireccional y estandarizada entre los diferentes equipos de respuesta a incidentes de los países de la región e inclusive a nivel mundial. Hoy el CSIRT Financiero cuenta con conexión propia a MISP administrada por personal técnico especializado, mediante el cual recopila la información del sector financiero y de fuentes de información internacionales, para procesarla, correlacionarla y analizarla.

Asimismo, hemos creado una red de relacionamiento y alianzas de colaboración e intercambio de información con entidades líderes en el ámbito nacional, y con organismos internacionales, entre los cuales están Organización de Estados Americanos (OEA), Policía Nacional, la Cámara Colombiana de la Informática y Telecomunicaciones -CCIT- y Microsoft, y contamos con planes de trabajo con empresas líderes en tecnología, innovación y seguridad tales como INCIBE y Amazon, entre otras.

Hoy el CSIRT sectorial es el escenario natural para que la entidades bancarias, autoridades y otros CSIRT puedan colaborar a través del intercambio de información en línea, y generar actividades de entrenamiento que permitan a las entidades financieras, no solo responder y reaccionar de forma oportuna frente a cualquier amenaza cibernética, sino anticiparlas. Sin duda, la colaboración y la cooperación en seguridad cibernética no es una opción; es una necesidad.

Como sector financiero tenemos un gran reto y también una gran responsabilidad de generar confianza en nuestros servicios, y por ello estamos más preparados, más unidos y contamos con relaciones más sólidas para hacer nuestra industria financiera y la economía más segura y resiliente.

PRÓLOGO

El Centro de Excelencia, factor fundamental
Ciberseguridad del Sector Financiero de cara al 2020

Por **Emanuel Ortiz Ruiz**,
Director
CSIRT Financiero

Estamos en un mundo digitalmente modificado donde los flujos de información transforman continuamente nuestra sociedad 4.0.

La cuarta revolución industrial está impulsando rápidamente la disrupción transformadora en todos los sectores de la economía.

En concordancia con las estrategias del Gobierno y su plan nacional de desarrollo específicamente en el "Pacto por la transformación digital, desde la Dirección de operaciones tenemos el reto de mantenernos en constante alerta. Resultado de ello son los análisis, investigaciones y estudios permanentes publicados sobre las amenazas globales en materia de ciberseguridad contra las Entidades Financieras.

Cabe recordar las palabras del Comandante en Jefe de la OTAN, el señor Patrick Shanahan:

« The thing that kept me awake at was cybersecurity. Cybersecurity proceeds from the highest levels of our national interest ... through our medical, our educational, to our personal finance (systems). »

"Lo que me mantuvo despierto por la noche fue la Ciberseguridad. La Ciberseguridad procede del más alto nivel de nuestro interés nacional... a través de nuestros sistemas médicos, educativos y financieros".

El señor Shanahan refleja la necesidad real de todos los países en contrarrestar y mitigar el riesgo cibernético que afecta a todos los sectores de la economía mundial.

Es el momento de revisar y ajustar si nos encontramos preparados (personas y organizaciones) para avanzar en este panorama global para poder afrontar y anticipar inteligentemente los riesgos y amenazas que emanan de la Red. Este pensamiento requiere de una participación activa de todos los sectores y organizaciones, que aprovechando la cuarta revolución industrial, deben generar y consolidar estrategias

alineadas que permitan implementar el fortalecimiento de las medidas y retos anticipativos que se requieren en materia de ciberseguridad para individuos, organizaciones y sociedad en general.

La transformación digital ha generado interesantes avances para distintos sectores productivos, pero sobre todo para el sector financiero, que a través de sus proyectos innovadores ha dejado de ser una banca tradicional para convertirse en una banca digital. Esto le permite diversificar y estar más cerca de sus consumidores, para contar con mejores formas de consumo, hábitos, optimización de recursos y eficiencia de forma transversa en la integridad de sus procesos.

Esta transformación, sin embargo, conlleva realizar un cambio en la implementación de nuevas tecnologías, plataformas más seguras, soluciones para proteger la información, políticas más robustas y aplicadas al entorno actual y equipos humanos preparados y entrenados para responder oportunamente frente a los riesgo y amenazas cibernéticas que implican este desafío.

Estos nuevos retos se vislumbran dentro de las áreas de Seguridad de la Información y Ciberseguridad de las entidades financieras son cada vez menos presenciales. Las entidades, se encuentran mas conectadas que nunca a través del incremento en el uso de plataformas digitales, lo que habilita mayor visibilidad respecto a los riesgos y amenazas cibernéticas.

Este nuevo escenario conlleva nuevos riesgos, vulnerabilidades o brechas de seguridad que se transforman en nuevos retos para las organizaciones, impulsando su transformación para evolucionar e innovar hacia un ecosistema digitalmente conectado y articulado entorno a una visión holística de la ciberseguridad en todos los niveles de la organización. Todo ello, a partir de un desarrollo seguro de las aplicaciones, optimización y eficiencia de las plataformas.

Estas refexiones y experiencias, que hoy marcan la pauta en la industria, son aquellas que, por parte del equipo técnico del CSIRT Financiero, se abordan todos los días. La motivación principal del equipo de expertos y analistas es facilitar una profunda reflexión sobre el comportamiento cibercriminal, así como generar alertas tempranas que les permita a las Entidades asociadas definir e implementar estrategias de prevención, y generar defensas que impidan el aprovechamiento de cualquier vulnerabilidad o brecha de seguridad.

Uno de los horizontes más claros al respecto está referido en la tendencia de Gartner (2019) que señala el futuro en un amplio espectro a través de una serie de conceptos clave como son “hiperautomatizados (hyperautomation), multiexperiencia, democratización de la tecnología, aumento científico humano (human augmentation), transparencia y trazabilidad que afecta la gobernanza de los datos, edad de la computación (edge computing), nube distribuida, las cosas autónomas, Blockchain práctico y la inteligencia artificial aplicada a la Ciberseguridad”.

Estos aspectos permiten determinar cuáles son las argumentaciones iniciales para determinar las preocupaciones en Ciberseguridad.

El CSIRT Financiero no es ajeno a esta problemática. Este futuro es plasmado a través de su operación en sus tres líneas específicas, Observatorio de Ciberseguridad, Inteligencia de Amenazas y Análisis y Apoyo a la Gestión de Incidentes.

El Foro Económico Mundial (Económico, 2017, pág. 10) marca 10 principios para optar por la Ciberresiliencia de las infraestructuras críticamente vulnerables.

10 PRINCIPIOS PARA LA CIBERRESILIENCIA

CYBERRESILIENCE

https://www.weforum.org/docs/IP/2017/Adv_Cyber_Resilence_Principles-Tools.pdf

Esta comprensión permite al CSIRT Financiero definir los aspectos con los cuales trabajar la resiliencia: factor humano, técnico y estandarizado; y así poder fortalecer la economía de la industria financiera.

Se consolida el objetivo de estar a la vanguardia de la disrupción hacia las nuevas tecnologías que presenta actualmente las entidades asociadas, a partir de un sentido holístico y transformador, que permita dar a entender la actuación frente a los estándares internacionales en Ciberseguridad. Se trata de resolver el ejercicio de anticipación no como un fin, si no como un medio para lograr minimizar el riesgo.

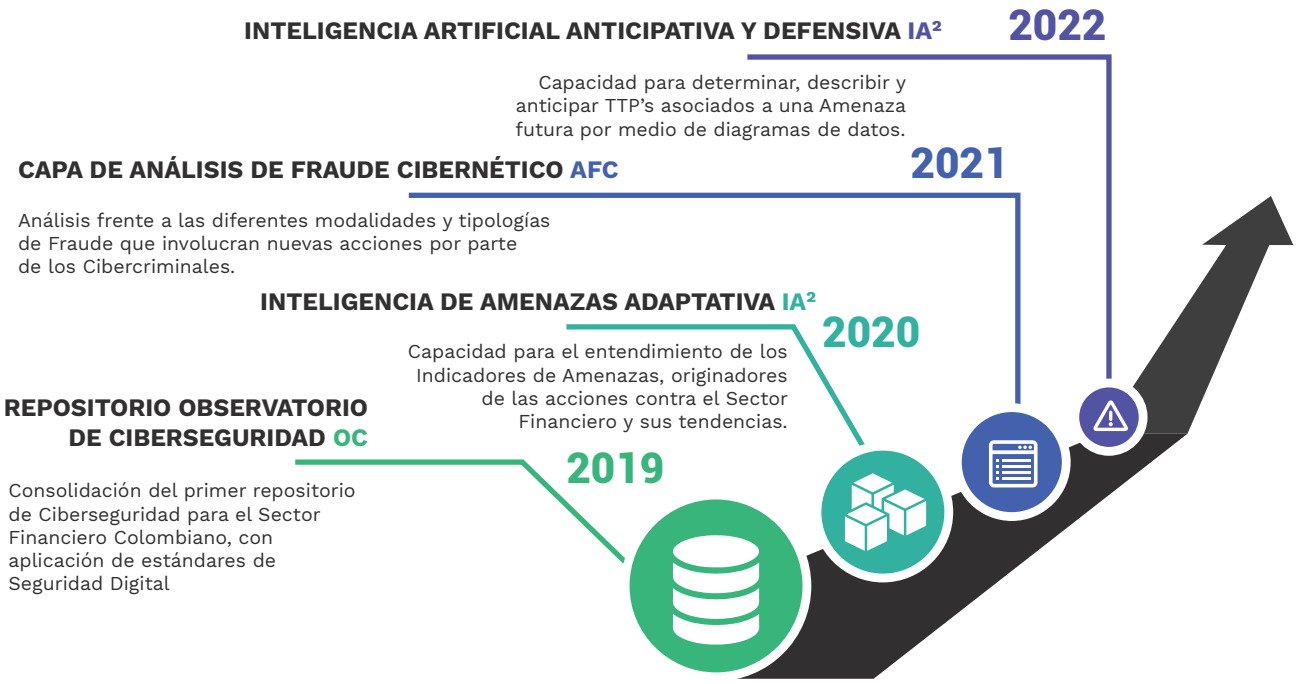
Estos son solo algunos parámetros que hoy tiene en cuenta el Centro de Excelencia en Investigación Cibernética del Sector. A partir de ellos el CSIRT ha integrado la necesidad de brindar a las entidades asociadas, no solamente protección y alertamiento sobre ciber-incidentes; sino de convertirse en una fuente de confianza, para poder compartir información estratégica en ciberseguridad.

Una plataforma de conocimientos con estándares académicos sustentables, información de fuentes con credibilidad certificada, y proyecciones futuras mediante el uso de nuevas tecnologías como partícipe de su gran valor documental en seguridad informática.

El CSRIT Financiero emprendió el camino en 2019 generando contenidos de prevención en ciberseguridad, alertas preventivas, boletines informativos con bases en ciber-investigación, informes de experto y una plataforma que ha venido evolucionando de acuerdo con los diferentes escenarios:

EVOLUCIÓN CSIRT FINANCIERO

ROADMAP Centro de Excelencia en Investigación Cibernética



Fuente de elaboración propia basada en RoadMap CSIRT

- **Consolidación del Observatorio de Ciberseguridad:** este mecanismo de almacenamiento de información ha permitido por parte de las entidades asociadas un valor especial, ya que por medio de este se ha facilitado el conocimiento sobre las principales amenazas que afectan al sector.

- **Inteligencia de Amenazas Adaptativa:** como nueva capacidad, se pretende enfocar y fortalecer la entrega de operables en materia técnica para poder estructurar las acciones dirigidas a asegurar los activos más críticos de las entidades.

Estas dos grandes capacidades son hoy por hoy los argumentos mediante los cuales el CSIRT Financiero se dinamiza aún más, permitiendo elevar su modelo de madurez y que se afiancen los entregables que posee actualmente.

Por otro lado, el camino recorrido ha permitido edificar y estructurar mecanismos estratégicos de confianza para cada una de las entidades asociadas, tal y como se enuncia en el documento Manual de Supervisión de Riesgos Cibernéticos (CICTE, 2017), sobre la necesidad imperante de "observar el panorama de las principales amenazas y tomar acciones conjuntas que permitan identificar, detectar, evaluar, mitigar y responder ante incidentes informáticos".

El CSIRT Financiero propone cinco retos que desea trabajar con sus asociados este año 2020. Para ello requiere consolidar la confianza y las acciones de alto valor para lograr apalancar sus acciones:

Para entender el cibercrimen o crimen financiero (Mckinsey, 2019) el CSIRT ha propuesto y promovido el nuevo ámbito dentro del cual debe dirigir su mirada; y es lo relacionado con el Fraude Cibernético. Un nuevo escenario bajo el que operan las organizaciones que actúan en el mercado oscuro del cibercrimen, y que buscan como realizar más y mejores ataques al sector financiero.

CICLO DEL CRIMEN FINANCIERO

Financial Crime Cycle

FRAUDE Y AMENAZAS INTERNAS

Interno y externo amenazas - Amenazas menores y NO menores - amenazas internas- Abuso de mercado y mala conducta

BRECHAS DE SEGURIDAD

Confidencialidad
Integridad
Disponibilidad de sistemas transaccionales

CRÍMENES FINANCIEROS

Lavado de dinero
Criptomonetización de archivos
Dark Selling

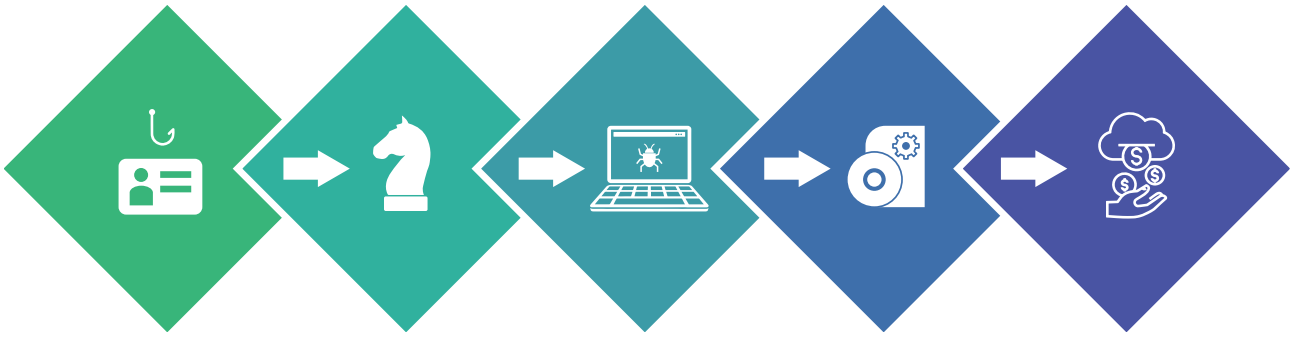
Ilustración Elaboración Propia Crímenes Financieros-Tradicionales

Así pues, es importante para el sector comprender los tipos de ataques que pueden afectar a los métodos tradicionales y no tradicionales de pago, o los ataques a través de SWIFT, o por ejemplo, cómo lograr un acceso rápido a las cuentas de usuarios de banca online; y por supuesto, cómo atacar de forma más eficiente un cajero ATM.

Todas estas amenazas presentes y futuras deben continuar siendo analizadas y transformadas en decisiones y operables que permitan mejorar de forma proactiva las defensas de las entidades asociadas.

- Reto: Nuevas Amenazas dirigidas hacia sistemas transaccionales no presenciales: Carbanak y Silence

Amenazas dirigidas hacia sistemas transaccionales: Carbanak y Silence



SPEARPHISHING

Es enviado un correo por la parte de los Ciberdelincuentes dirigido a pagos transaccionales

EJECUCIÓN TROYANO CARBANAK/SILENCE

Una vez es ejecutado el troyano Carbanak/Silence busca PC's con configuración Admin

INFECCIÓN ADMIN Y EMBEBIDOS

Una vez son identificados intercepta las Comunicaciones y altera los balances

EJECUCIÓN DISPENSADOR PROGRAMADO

Las actividades de dispensación de dinero son programadas a horas específicas

EJECUCIÓN PAGO DELINCUENTE INFORMÁTICO

El efectivo es movido a distintos canales de pago On-Line para ser recibido y transferido

Ilustración elaboración propia

Es un claro ejemplo de este tipo de amenazas que ha tenido como consecuencia la afectación hacia servicios financieros críticos, y que por lo tanto está siendo monitoreada por el CSIRT financiero. Así el equipo de analistas y expertos deberá reforzar la actitud preventiva para ayudar a definir las mejores acciones futuras para la entidad.

- Reto: Amenazas dirigidas con fragmentación y adaptación de tipo local:

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 adaptado a las circunstancias del sector y de sus clientes. Mediante las investigaciones se ha evidenciado que el enfoque de los actores y originadores de este tipo de acciones pasan por la fabricación y desarrollo localizado en Colombia.

Otro de los retos es la importancia en concentrar esfuerzos que involucren a las entidades para poder afianzar la facilitación de esquemas dirigidos al sector. Este nuevo reto exige poder analizar y fortalecer las fuentes de inteligencia que se adapten al contexto colombiano.

- Reto: Aparición del Malware embebido en parámetros de Ingeniería Social Colombiana:

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

- Reto: La Colaboración como base de construcción en Ciberseguridad

La Colaboración y los mecanismos de intercambio de información son unos de los aspectos claves para poder desarrollar y afianzar los escenarios de prevención.

Siempre es necesario contar con esas capacidades para poder fortalecer la confianza entre los actores y posibles afectados; por ello, el CSIRT Financiero propone ambientes orientativos y eficaces para desarrollar estos escenarios en los que se pueda alcanzar niveles de madurez ante nuevos riesgos y esquemas de vulnerabilidad cibernética.

Bienvenidos (as) a su Memoria Anual

"Este es un cercano comienzo ante una realidad extensiva que demanda el mundo de la Ciberseguridad y la Seguridad Digital"

RESÚMEN EJECUTIVO

Desde la creación y puesta en marcha del CSIRT Financiero se han identificado diferentes ciberamenazas contra el sector financiero.

El equipo de analistas ha compartido el resultado de sus ajustes propuestos; así como las recomendaciones de protección a los asociados, a través de los tres pilares fundamentales del servicio: el Observatorio de Ciberseguridad, Inteligencia de Amenazas y Apoyo a Incidentes.

El comportamiento del CSIRT durante sus primeros 7 meses ha resultado en:

Imagen 1. CSIRT en cifras

La distribución de las amenazas reportadas desde el CSIRT Financiero para el sector fue la siguiente.

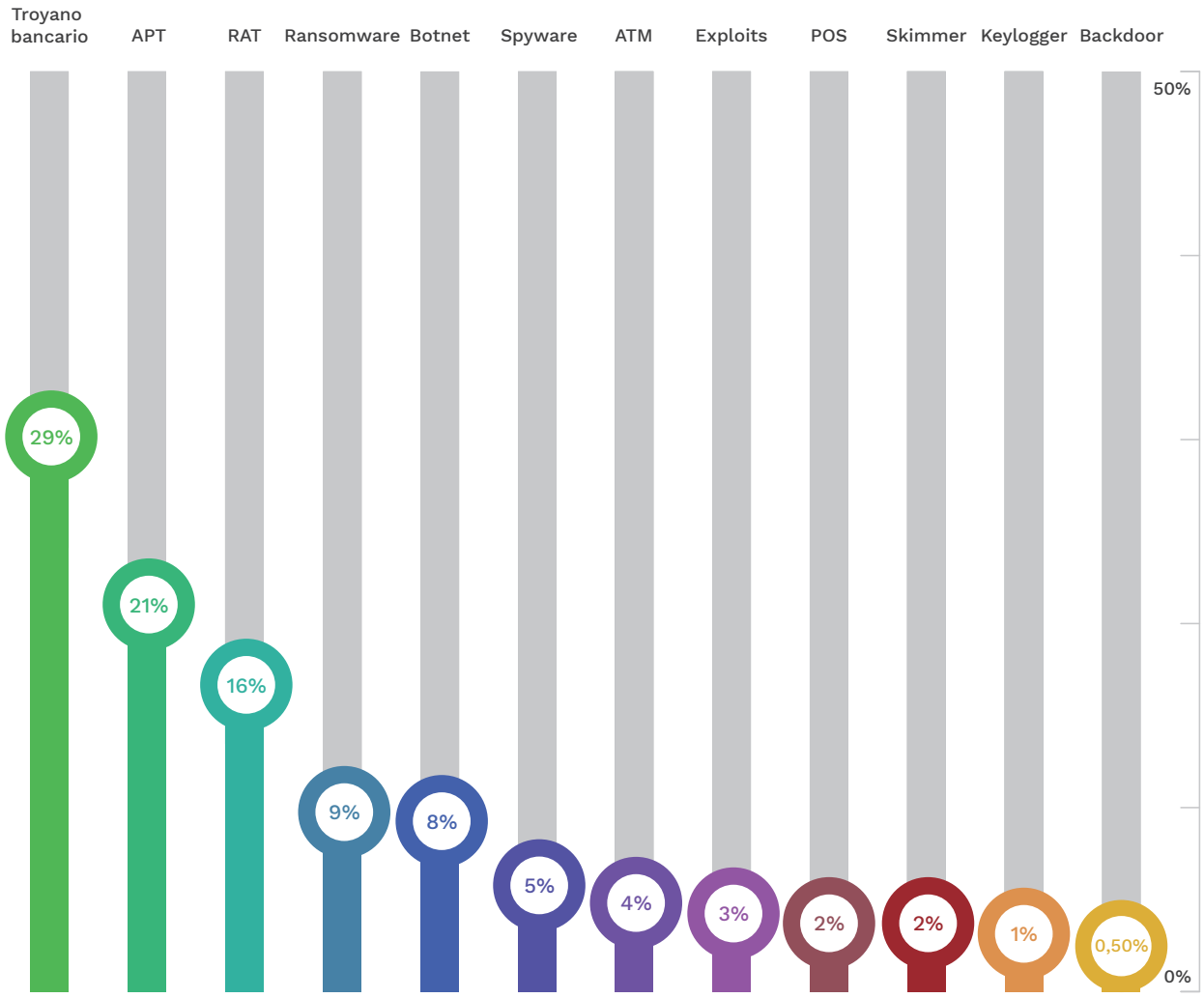


Gráfico 1. Porcentaje de amenazas alertadas

Algunas de las amenazas más relevantes tratadas en las alertas, boletines, informes y monográficos fueron las siguientes.

1. Los troyanos bancarios se convirtieron en la amenaza más reportada por el equipo de analistas. Emotet, Gozi, Ursnif, Trickbot, Dridex y Lokibot, destacaron como el malware bancario de mayor impacto para el sector.

2. Otra de las amenazas relevantes contra el sector fueron los grupos APT (Advanced Persistent Threat) representando el 21% de las amenazas reportadas. TA505, FINF7, FIN8, Cobalt y APT-C-36 fueron las más activas. Ésta última dirigida específicamente contra diferentes entidades de Colombia.

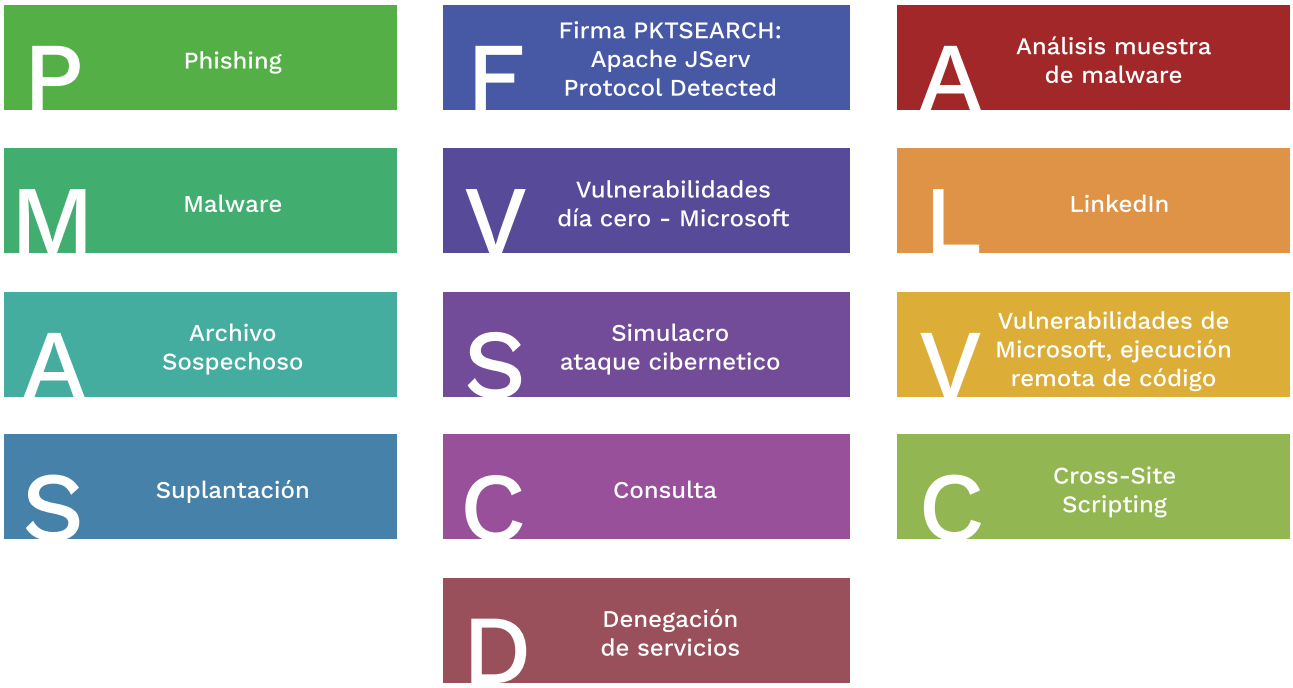
3. En el top 3 de ciberamenazas contra el sector, destacaron los Troyanos de Acceso Remoto (RAT). Nanocore y FlawedAmmyy han sido los más más frecuentes; no sólo para cibercrimen, sino también para ciberespionaje.

Finalmente, y con especial incidencia en los dos últimos trimestres del año, se encuentran los malware del tipo ransomware, siendo los más reportados Ryuk, Megacortex y en menor medida, Bitpaymer.

En relación a Apoyo a Incidentes, desde el arranque en junio de 2019 se recibieron 23 peticiones relacionadas con diferentes tipos de amenazas.

Es destacable que, dentro de estas peticiones, diez corresponden a la categoría "phishing", una amenaza constante en el panorama de la ciberseguridad.

En el siguiente gráfico se muestra la categorización de las diferentes peticiones realizadas a Apoyo a Incidentes por parte de los Asociados:



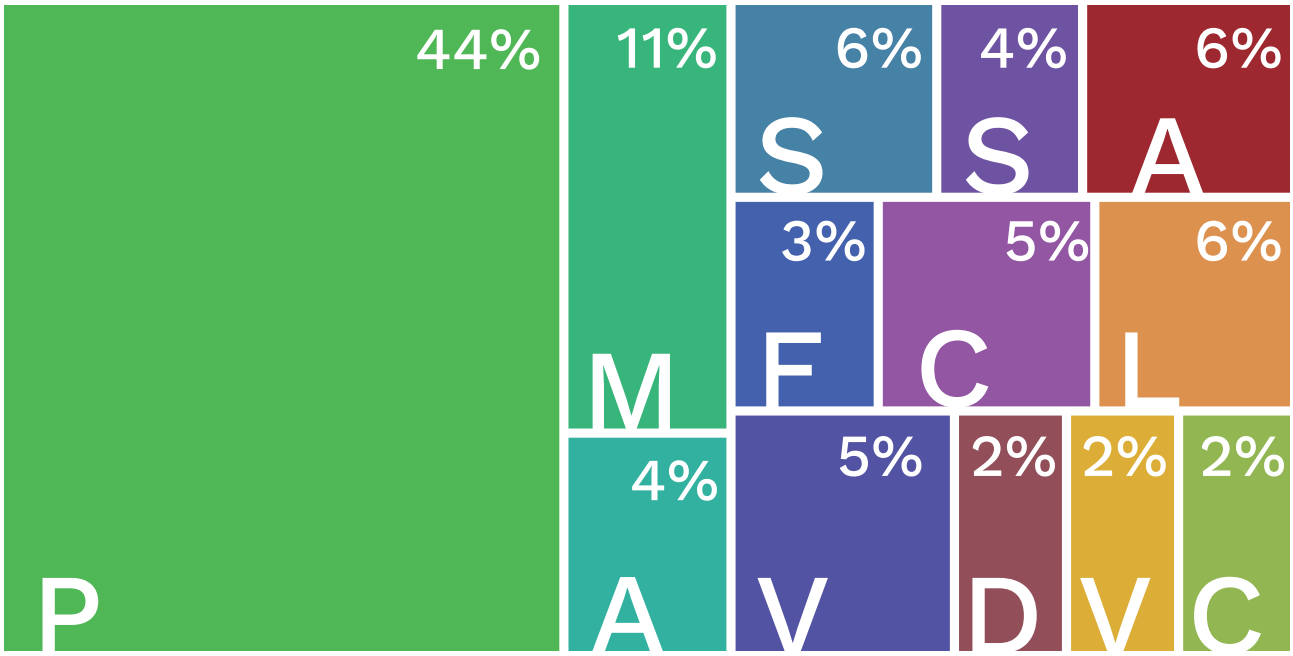


Gráfico 2. Peticiones a la línea de Apoyo a Incidentes

Por último, el siguiente gráfico presenta las 10 tácticas y técnicas más relevantes para el sector financiero, basados en la matriz MITRE | ATT&CK[1], de acuerdo con el análisis realizado por el equipo del CSIRT financiero.

Tener el conocimiento sobre aquellas técnicas más utilizadas por los grupos cibercriminales, ayuda a los equipos tácticos y operativos de ciberseguridad a priorizar los mecanismos de detección y mitigación sobre aquellas que resultan más comunes.

Gráfico 3. Principales TTPs de 2019

[1] https://attack.mitre.org/

CSIRT

FINANCIERO Y CIBERAMENAZAS EN 2019

JUNIO

APT: APT-C-36, TA505
Troyano bancario: Trickbot, lokibot, Danabot, FormBook, Nymeri Goznym, Emotet, Qakbot, Dridex, Refete, Jasperloader
RATs: Netwire, WSH RAT, Nanocore
Ransomware: Megacortex, Loocipher, Dharma
ATM: ATMitch
Móvil: WannaLocker, Riltok
Fraude: Filtración de datos de entidad bancaria rusa, fraude de tarjetas de Chile

JULIO

APT: FIN5, APT15, APT34, APT-C-36, Silence, TA505
Troyano bancario: Dridex, Metamario, Trickbot, Ursnif, Gootkit, Emotet, Trickbooster, Gozi, Astaroth
RATs: FlawedAmmyy
Ransomware: Megacortex, Sodinokibi, Ryuk
ATM: ATM, EMV, XFSADM, JaDI
Móvil: Monokle, Anubis, Anubis 2.5, BianLian
Fraude: Venta de tarjetas en la Deep Web, Phishing de magecart 2.
POS: BadHatch, Mozart POS

AGOSTO

APT: Silence, Machete, Cobalt, FIN6, APT28
Troyano bancario: Cerberus, Gozi, Trickbot, Amavaldo, Guildma, Emotet, Lokibot
RATs: FiawedAmmy, Quasar RAT, Nanocore, Balkan, Adwin, Lookback, Gh0st RAT
Ransomware: Nemty.
Fraude: Filtración de mastercara, Filtración de Movie Pass, Fuga de información financiera

SEPTIEMBRE

APT: Panda, FIN7, FIN5, TA505
Troyano bancario: Emotet, Astaroth, Cerberus, Ursnif, Gozi, Trickbot, Qakbot
RATs: Quasar RAT, Adwin, Orcus, Revenge
Ransomware: Sodinokibi, Kvag, Ryuk, Lilocked
ATM: ATMDtrack
Móvil: BRATA, Joker
Fraude: Magecart, Filtración código fuente de entidad financiera, Fuga de datos de entidad, fraude entidad alemana

OCTUBRE

APT: TA505, Lazarus, Magecart, FIN6, FIN7, Cobalt
Troyano bancario: Nodersok, Banload, Trickbot, IcedID, Ursnif, Dridex, Casbaneiro, Danabot, Emotet, Qakbot, Lokibot, Negatel, Pony, Raccoon
RATs: Ave Maria, Remcos RAT
Ransomware: Bitpaymer
ATM: Cutlet Maker, ATM Boostwrite
Fraude: Phising en pagos online, Fraude financiero dirigido
POS: Framework POS

NOVIEMBRE

APT: Cobalt, FIN7, Magecart, TA2010, TA505, APT38, Andariel
Troyano bancario: Emotet, Trickbot, Mispadu, Ursnif, Dridex, Ginp, Lokibot, IcedID
RATs: Nanocore
Ransomware: Ryuk, Bitpaymer, Megacortex, Buran, Maze
ATM: ATM DispenserXFS
Fraude: Phisihing dirigido

DICIEMBRE

APT: Magecart, FIN5
Troyano bancario: Emotet, Trickbot, Dridex, Lokibot, IcedID, STOR, Gozi, Lampion
Rats: PyXie, Balkan RAT, Dacis
Ransomware: Ryuk, Snatch, Zeppelin, LooCipher
Fraude: Venta de tarjetas en la deep web, phishing dirigido, filtración de correos

Imagen 2. Amenazas relevantes por mes

Desde el CSIRT Financiero se han emitido 420 documentos generados de diferentes amenazas detectadas a lo largo de 2019. También, se han realizado dos informes monográficos de amenazas enmarcados en esas categorías, a saber: Monográfico de Amenaza APT-C-36 y Monográfico de Amenaza de Malware Contra ATM; ambos disponibles para descargar desde el portal del asociado.

En términos generales, durante los últimos siete meses del 2019, se ha evidenciado un constante desarrollo, mejora e implementación de nuevas capacidades en los diferentes tipos de amenaza. Aumenta así, por tanto, el valor de la identificación temprana y prevención ante el incremento de la sofisticación.

Así, por ejemplo, se observó como los cibercriminales fueron capaces de convertir un simple troyano en una herramienta totalmente funcional con múltiples propósitos como la instalación de otros malware, o la incorporación de herramientas de administración del sistema en su arsenal.

Por otro lado, el malware de hoy tiene la capacidad de infiltrarse en el sistema operativo e instalarse como un programa más; evadiendo las medidas de seguridad de los antivirus, antimalware y dispositivos perimetrales. Una vez instalado, realiza la verificación del entorno e inyecta código en algunos procesos del sistema. Además, descarga módulos personalizados por el ciberdelincuente y/o la carga útil del malware. Por otro lado, el usuario dispone de menos medidas de seguridad de la información, que puede ser capturada a través de técnicas de ingeniería social o superposición de imágenes en pantalla.

De hecho, los avances en el desarrollo de las capacidades del malware para dispositivos móviles le permiten:

- Detectar ambientes controlados
- Utilizar sensores de movimiento
- Utilizar la cámara y el micrófono
- Hacer llamadas y enviar mensajes de texto
- Desactivar las medidas de seguridad
- Descargar e instalar aplicaciones maliciosas

Y en definitiva, tomar el control del dispositivo.

La tendencia de los ataques con software malicioso contra equipos de cómputo y dispositivos móviles muestra una mayor automatización, ajustando el malware a través de módulos, según el reconocimiento realizado al equipo víctima y los objetivos del ciberdelincuente. Además, los ataques tienden a un mayor alcance y profundidad, llegando a propagarse a través de la red. Incluso son capaces de encender los equipos para realizar la instalación de la carga útil o enviar mensajes de texto con enlaces que permitan su descarga.

No hay que dejar de lado el malware embebido en archivos y aplicaciones legítimas, código ofuscado y otras técnicas antievasión que le permiten pasar sin ser detectado por los mecanismos de protección del sistema afectado.

Las APT han sido un tipo de amenaza destacada desde el inicio de las operaciones del CSIRT. Al igual que los malware, tienden a la sofisticación en sus ataques, pudiendo llegar a identificar diferentes APT con una variación constante de sus TTPs. En cada avance, disponen de una mayor adaptabilidad hacia la víctima, permitiendo un incremento de la efectividad de los ataques perpetrados.

Además, el incremento de tensiones a nivel internacional entre los países, ha dado lugar a un viraje de los objetivos de estos cibercriminales, incrementándose el número de ataques dirigidos a entidades financieras, sector de la salud y diferentes infraestructuras críticas como empresas petroleras o eléctricas.

En el año 2019, al igual que en años anteriores, se han descubierto numerosas vulnerabilidades relevantes que afectan a productos y fabricantes frecuentes en la gran mayoría de las organizaciones. Sin embargo, y debido a que han sido vulnerabilidades muy explotadas, se destacaron en 2019 la CVE-2019-0708 (BlueKeep) y CVE-2019-19781 de Citrix.

Con respecto a BlueKeep, afecta al protocolo RDP de Microsoft Windows que permite la posibilidad de realizar ejecuciones remotas de código. La vulnerabilidad de Citrix afecta al controlador de entrega de aplicaciones (ADC) y a NetScaler Gateway, lo que permitiría, al igual que BlueKeep, la ejecución remota de código; una de tendencias al alza identificadas a lo largo del año.

Por otra parte, el incremento de la compra en modalidad online y tecnologías como el chip EMV han provocado un importante incremento del fraude Card-Not-Present (CNP) impactando directamente en las entidades financieras.

Cada vez es más amplio el ecosistema en foros especializados de la deep web y darknet donde se venden credenciales, información bancaria, identidades digitales, malware y servicios relacionados como muleros que rematan los ciberataques perpetrados. Así, el Crime-as-a-Service (CaaS) ha sido sin duda uno de los aspectos más destacados de 2019, afectando en general a todo tipo de entidades y sectores.

A. OBSERVATORIO DE CIBERSEGURIDAD

TROYANOS BANCARIOS

Durante el 2019 se observó un crecimiento de ataques realizados a través de los troyanos bancarios. Asimismo, se evidenciaron algunas mejoras en su desempeño y en las capacidades utilizadas para la exfiltración de información de los usuarios y dispositivos comprometidos.[2]

Desde la perspectiva del CSIRT Financiero, estos troyanos son una de las principales ciberamenazas debido al gran impacto que generan sobre el sector.

A lo largo de 2018 y 2019, los troyanos bancarios han tenido un desarrollo muy acelerado como malware; ya no solo en complejidad, sino en el ecosistema al que son destinados. De esta manera, en 2019 se han elevado las cifras, especialmente de los troyanos bancarios para móviles, impulsados por el crecimiento de la banca online y el uso de las apps financieras.[3]

Con respecto a la complejidad de los malware en general, y los troyanos bancarios en particular, se destacan tres tendencias al alza en el desarrollo por parte de los cibercriminales:

- Malware modular. Diseñados para evitar en gran medida su detección, capaces de desarrollar ataques por fases a través de varias cargas útiles. Un ejemplo de esto lo encontramos en el troyano bancario Danabot.

- Malware híbrido. Aquellos malware que combinan características de malware ya existentes. En este sentido, encontramos al troyano bancario. Goznym aprovecha el código del troyando bancario Gozi, a la vez que incorpora parte del malware Nymaim (un dropper sigiloso y persistente que utiliza múltiples técnicas de evasión)

- Diseño de campañas conjuntas de troyanos bancarios con otras categorías para maximizar el impacto del ataque. Esta tendencia ha venido marcada por la utilización de los malware Emotet, Trickbot y Ryuk conjuntamente.

Los troyanos bancarios son la categoría de malware que más participa del Malware-as-a-Service (MaaS), permitiendo que los cibercriminales estén en constante desarrollo de nuevas variantes para su futura venta en mercados de la web oscura.

De hecho, el MaaS ha sido uno de los factores que ha impulsado a los troyanos bancarios a tener un mayor impacto en el sector financiero a través de su ágil distribución en la Darknet.

[2] https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

[3] https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/

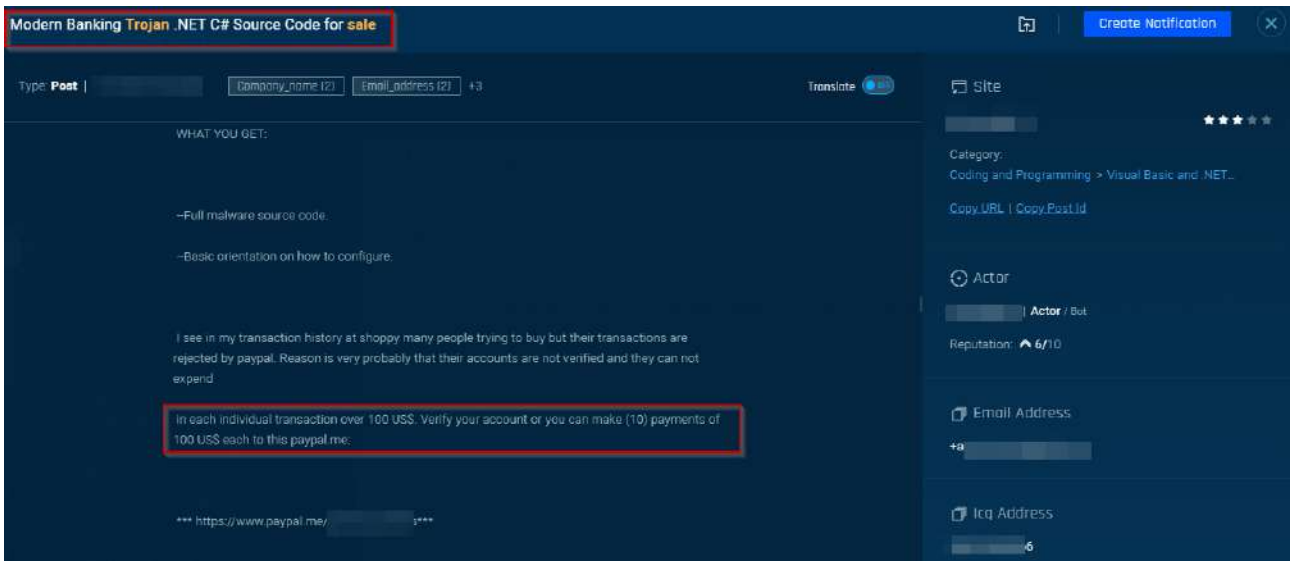


Imagen 3: Venta de troyanos bancarios en darknet

A continuación se recogen los de mayor actividad y/o impacto desde el arranque del CSIRT Financiero y hasta el final del 2019.

A Trickbot

Trickbot ha sido uno de los más destacados, especialmente por su uso conjunto con Ryuk y Emotet[4] de forma coordinada. En este tipo de campañas identificadas en 2019, Trickbot realiza la función de reconocimiento, y una vez que los bots infectan un equipo, crean shells inversas a otros actores permitiendo el uso de Ryuk para cifrar todos los archivos. Así logran la exfiltración de credenciales y acceso a datos y servidores de alto perfil para obtener la mayor cantidad de rescate posible.

Además, Trickbot es destacable por su desarrollo modular y actualizaciones a lo largo de los años. Esto le ha permitido ser eficiente en diferentes entornos. De hecho, desde la integración de un módulo llamado Project Anchor, el troyano participa de las APT. Por otro lado, también renueva las capacidades de recopilación automática de información de red, movimiento lateral y recolección de credenciales automatizada.

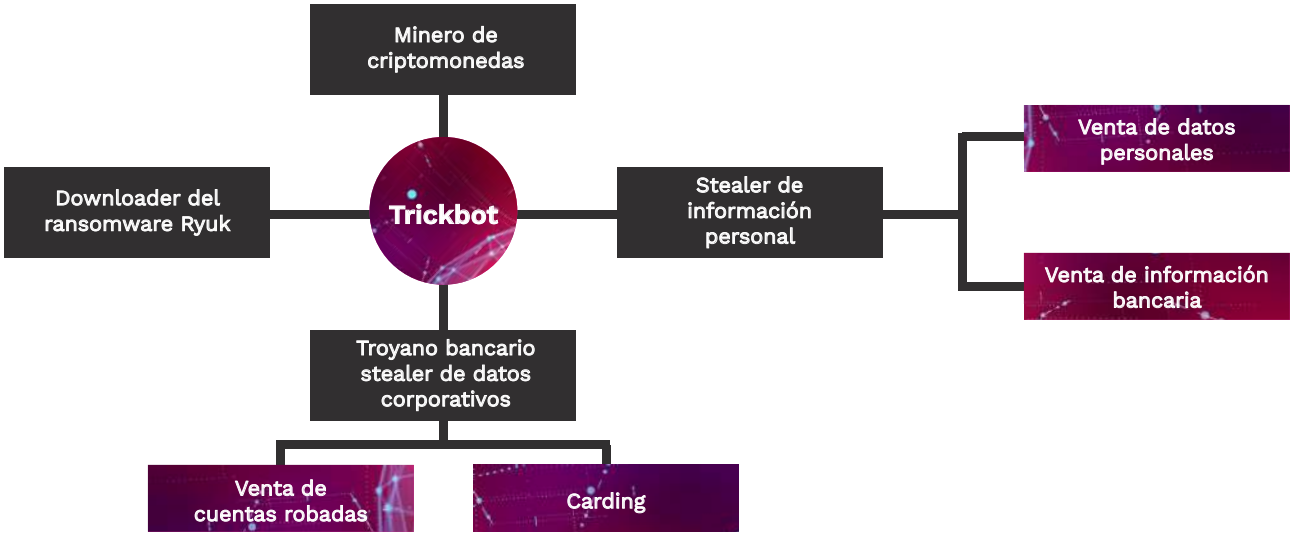


Imagen 4. Capacidades de Trickbot

[4] https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data

B Dridex

Por su parte, Dridex ha sido identificado a lo largo del año con nuevas variantes cuyas capacidades son altamente evasivas. El vector de ataque de este troyano bancario, explotado por los cibercriminales desde 2011, sigue siendo el phishing. Su objetivo es la información financiera, y entre sus capacidades puede:

- Capturar credenciales bancarias.
- Realizar transferencias no autorizadas.
- Abrir cuentas fraudulentas.
- Utilizar las cuentas de las víctimas.

Dridex es un malware que evoluciona con frecuencia. Actualmente tiene la capacidad de utilizar firmas de archivos que no son detectables para un antivirus, evadiendo así la detección. Además, las bibliotecas de vínculos dinámicos (DLL) de 64 bits firmadas, se cargan a través de ejecutables legítimos de MS Windows.

C Emotet

Emotet funciona desde 2014 y es otro de los grandes troyanos bancarios de 2019.

Durante un tiempo parecía que iba a desaparecer, pues mantuvo un periodo de 4 meses de inactividad. De hecho, incluso llegaron a cerrarse los servidores de comando y control (C&C) de la botnet y cesaron las campañas de phishing.

Sin embargo, a mediados de septiembre, el malware se reactivó[5] volviendo a adquirir considerable repercusión mediática. Una vez reiniciaron las campañas de phishing, Emotet incorporó de nuevo a víctimas a la botnet, convirtiéndose de nuevo en una de las ciberamenazas contra el sector financiero más relevantes.

Dentro de sus capacidades, puede extraer contraseñas, distribuirse lateralmente a otras computadoras en la misma red, descargar otros malware, e incluso hurtar hilos de correo electrónico para utilizarlos en campañas de spam para que sean más efectivas.

Para 2020, los troyanos bancarios seguirán siendo una importante amenaza para el sector. Se esperan incluso nuevas variantes que contarán con importantes capacidades evasivas que les permitirán adaptarse y sobreponerse a las soluciones de ciberseguridad.

[5] https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

RATS

Los RAT (Remote Access Trojan) son un tipo de malware común que está dirigido principalmente al ciberespionaje, aunque tienen otras capacidades como:

- Keylogger en la captura de información confidencial.
- Dropper para:
    - Descargar e instalar otro tipo de malware en el dispositivo.
    - Para convertirlo en un bot con capacidad de realizar un ataque DDoS.
    - Para minería de criptomonedas.

Son una amenaza que permanece constante en el panorama de los ciberataques. De hecho, un 14%[6] de las amenazas detectadas en 2019 desde el Observatorio de Ciberseguridad corresponden a RATs.

El vector de ataque más común fue el phishing[7] con archivo malicioso adjunto o un enlace para su descarga.

Un RAT se instala sin el conocimiento del usuario.

Imagen 5. Funcionamiento del phishing

[6] Información obtenida de datos internos

[7] https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf

Dadas sus múltiples capacidades, es comúnmente suministrado como Malware-as-a-Service (MaaS), pudiéndose encontrar a la venta en tiendas especializadas de la Darknet a precios muy bajos o incluso gratis. Este hecho ha incrementado su utilización y distribución.

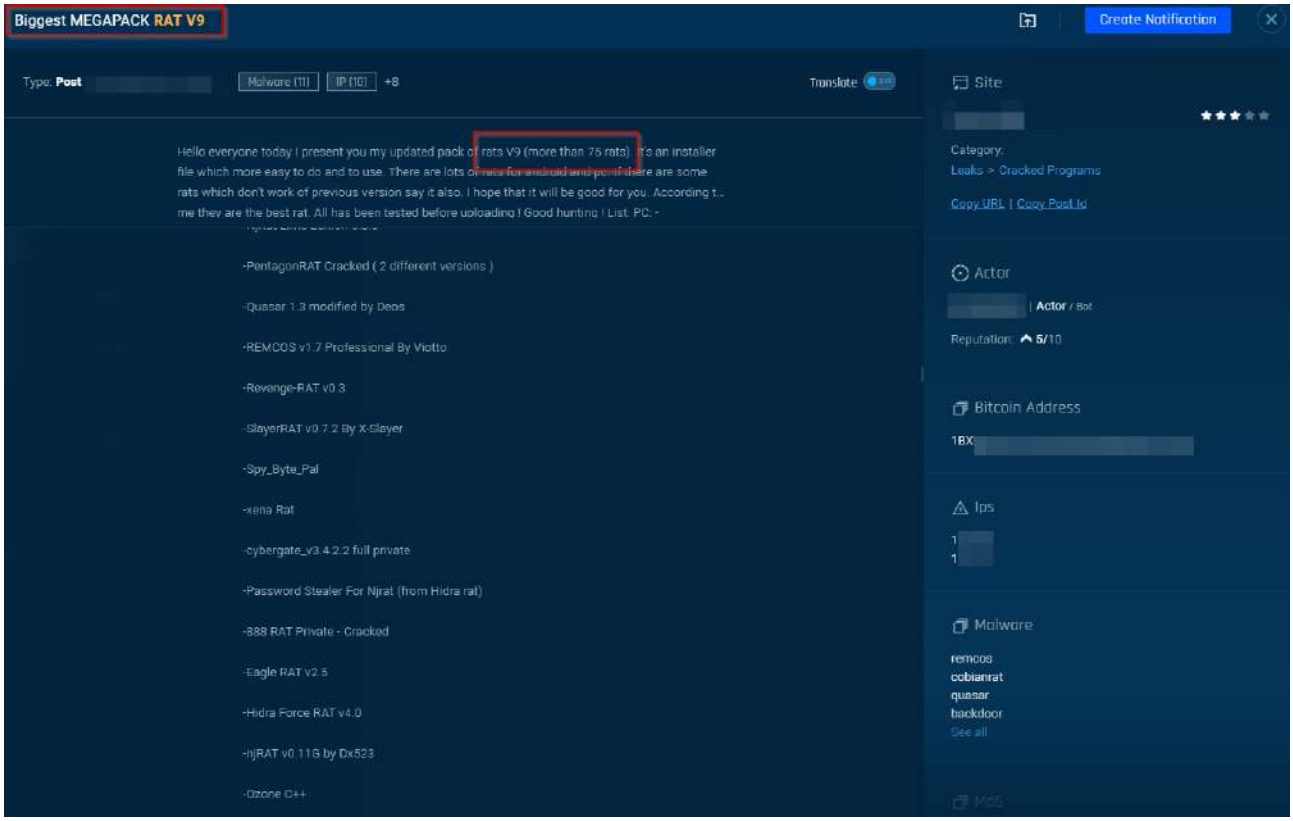


Imagen 6. Disposición para todos los usuarios de forma gratuita de múltiples RATs

Características como la versatilidad o capacidad de sigilo lo han convertido en un tipo de malware muy exitoso. Por otro lado, desarrollan interfaces muy sencillas y fáciles de utilizar por cualquier cibercriminal, facilitando incluso construir un RAT a su medida. Así, sólo sería necesario diseñar una forma específica de distribución para iniciar el ciberataque en cualquier momento.

En 2019 se identificó una gran variedad de RATs actuando en múltiples ataques orquestados, tanto por los cibercriminales como por grupos APT. Los más destacados fueron:

FlawedAmmyy confiere acceso total al equipo de la víctima y puede moverse lateralmente en la red sin ser detectado. Su uso está ligado a una APT muy activa en 2019, TA505.[8] El vector de ataque más común utilizado en 2019 para distribuir este RAT fue el phishing, acompañado de un archivo malicioso en formato .xls. Las regiones más afectadas por esta ciberamenaza fueron Asia y América Latina.

Detectado en 2013, NanoCore es un RAT muy sofisticado, comúnmente utilizado por actores como las APT. Sus diferentes versiones han sido distribuidas en foros de la Darknet de forma gratuita, siendo accesible para cualquier cibercriminal. Además, diferentes complementos de Nanocore también son ofrecidos en los foros para ajustarlo a las necesidades del comprador.

[8] https://thethreatreport.com/a-closer-look-at-ta505s-flawedammyy-rat/

Este es un RAT muy adaptable ya que tiene la capacidad de poder expandir sus funcionalidades, permitiendo una mayor versatilidad para los actores de amenazas que lo utilizan para sus propias campañas. Debido a esto, se ha detectado a Nanocore en múltiples tipos de ataques, desde minería de criptomonedas a campañas ransomware.

Por último, encontramos los RAT Orcus y Revenge. Son programas maliciosos muy populares cuya creación data de 2016. Fueron identificados en 2019 atacando a víctimas del sector financiero entre otros.

Una de sus campañas más reconocidas, fue un ataque a través de phishing mediante el correo electrónico SendGrid. El phishing se acompañaba de un enlace donde se alojaban estos RATs. Una vez descargados en el equipo de las víctimas, imposibilitaban su uso.

RANSOMWARE

Mientras que en 2018 la tendencia en relación con el uso de ransomware por parte de los cibercriminales fue a la baja, en 2019 se ha observado un importante incremento en los ataques a nivel de América Latina.[9] Estos ataques han alcanzado un alto grado de sofisticación, no sólo en el desarrollo a nivel de código; sino también en las técnicas de extorsión para obtener dividendos.

Los ataques de ransomware realizados durante 2019 parecen haber sido dirigidos a objetivos específicos, entidades del gobierno, grandes corporaciones y entidades con información de las operaciones tiene un alto impacto en la sociedad.

Este tipo de ciberataques están diseñados para tomar como objetivos aquellos cuya pérdida de información tienen un alto impacto, lo suficiente como para secuestrar información y procesos tan relevantes que las víctimas paguen por el rescate, en contra de las recomendaciones de ciberseguridad.

La característica principal del ransomware es la de cifrar los archivos de usuario de los equipos infectados; sin embargo, durante el 2019 se pudo observar un aumento de las extorsiones fingiendo la publicación de datos sensibles y/o confidenciales hurtados.

De nuevo, el principal vector de ataque fue la ingeniería social y el miedo psicológico. Y, aunque las víctimas pagasen el rescate, en la mayoría de los casos no se recuperó la información, existiendo además, la posibilidad de volver a ser atacados.[10]

Es bastante probable que quienes estén detrás de estos ataques de ransomware más sofisticados sean:

- Cibercriminales solitarios con acceso a la Darknet que participan del Ransomware-as-a-Service (RaaS). Esta es una tendencia al alza con todo un amplio mercado en expansión. Creados en función de las necesidades de los demandantes, disponen de una interfaz sencilla de utilizar por cualquier cibercriminal siguiendo unas pequeñas directrices.

- Grupos de cibercriminales organizados que buscan a través de la extorsión un beneficio económico, reputacional o provocar daño en la entidad atacada.

A pesar de que tradicionalmente los ransomware se han utilizado para realizar ataques genéricos, a lo largo de 2019 se ha asistido a un incremento del uso de este tipo de malware en ataques dirigidos y campañas diseñadas a medida. Por ejemplo, modelos de ataques recientemente detectados como Ryuk, Megacortex o Bitpaymer.

[9] https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/
[10] https://unaaldia.hispasec.com/2019/11/el-gobierno-de-luisiana-es-victima-de-un-ataque-ransomware.html

Por otro lado, se ha identificado el RaaS como una tendencia al alza en los foros de la darknet, facilitando el acceso a esta categoría de malware a todos los tipos de cibercriminales.[11]

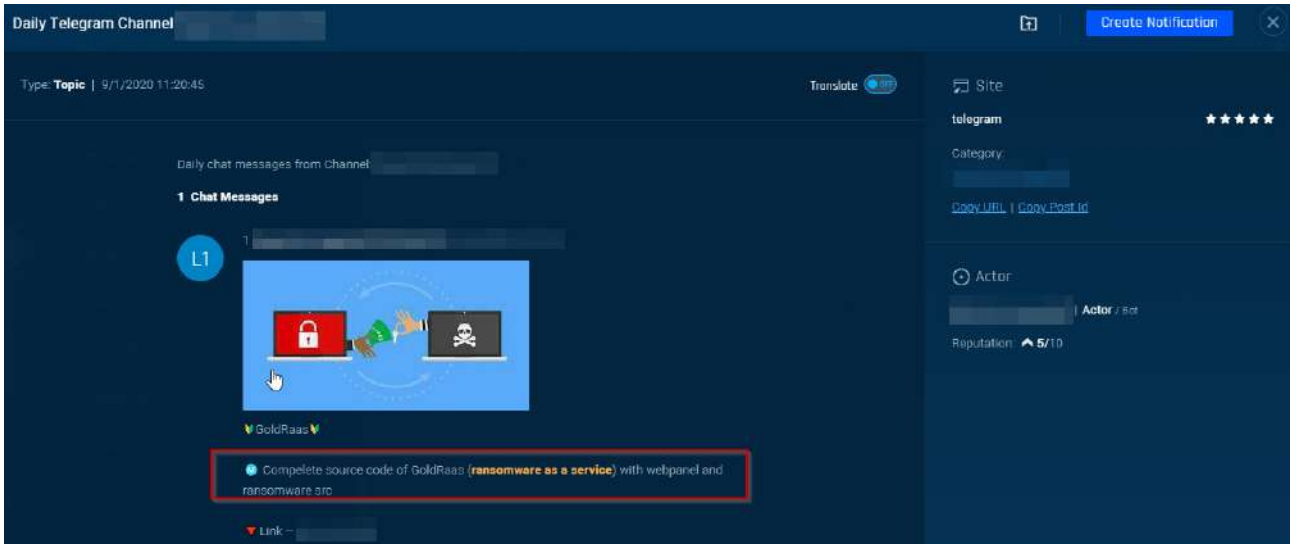


Imagen 7. Petición de colaboración para la realización de Ransomware-as-a-Service (RaaS)

Los principales ransomware identificados en este periodo se resumen a continuación.

Ryuk registra su primera aparición en agosto de 2018, y es la máxima representación de ataques dirigidos. Tiende a atacar a grandes organizaciones con activos críticos. Exige una mayor implicación de los cibercriminales en el ataque, ya que tienen que diseñar toda una campaña personalizada y adaptada al objetivo; a cambio, incrementan la efectividad.

Es necesario destacar en 2019 la actuación de Ryuk en campañas conjuntas con los malware Emotet y Trickbot, lo que genera una gran amenaza en años venideros.

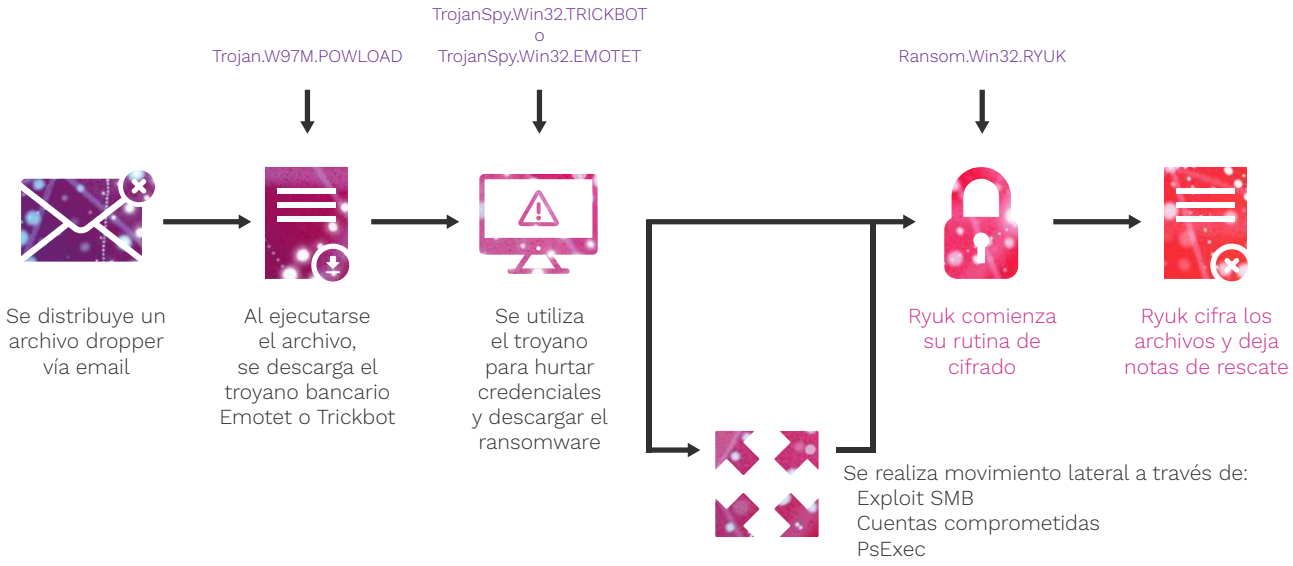


Imagen 8. Funcionamiento general del ransomware Ryuk

[11] https://nakedsecurity.sophos.com/2017/12/13/5-ransomware-as-a-service-raas-kits-sophoslabs-investigates/

Bitpaymer por su parte, parte, fue distribuido a través de phishing. Por otro lado, se le identificó utilizando otros malware como Azorult, Chthonic o Dridex para tener acceso remoto a la red de la víctima.

Los cibercriminales tras este ransomware desarrollaron variantes horas antes de la explotación en la red de las víctimas. Una vez en la red, esperaban el momento idóneo para generar el mayor impacto posible.

Bitpaymer también es capaz de evadir entornos de sandbox y tiene capacidades de ofuscación[12] que incrementan la dificultad en su detección.

Continuando con Megacortex, este ransomware se identificó por primera vez en 2019 y en las últimas campañas detectadas, además de cumplir con la función de cifrado de la información, cambia la contraseña del usuario y amenaza con publicar los archivos de la víctima si no paga el rescate.

Megacortex llega a los equipos a través del acceso a la red proporcionado por troyanos como Emotet. Una vez que tiene acceso, utiliza kits de post-explotación.

A lo largo de 2019 rediseñaron el ransomware dándole la capacidad de autoejecutarse y automatizar una cadena de eliminación, lo que le confiere la capacidad de distribuirse y actuar de manera más amplia.

Finalmente, se encuentra Sodinokibi. Este es un malware cuya aparición también se produjo en 2019. Se le conoce por la utilización de la vulnerabilidad de Oracle WebLogic (CVE-2019-2725) y kits de explotación y correo no deseado para obtener acceso al equipo.

Posteriormente trata de ejecutarse con privilegios para acceder a todos los archivos. Utiliza algoritmos AES y Salsa20 para cifrar los archivos. Investigadores sitúan como autores del ransomware a los cibercriminales detrás del ransomware GandGrab[13], el cual, hasta su descifrado, llegó a ser el responsable del 40% de todas las infecciones de ransomware a nivel mundial.

La capacidad de extorsionar, no solo a través del cifrado, sino a través de la ingeniería social se complementa con capacidades que dificultan el análisis y la detección de los nuevos ransomware desarrollados. Esto provocó que los ataques dirigidos tuvieran un mayor impacto y se produjera un incremento del número de pagos a lo largo de 2019.[14]

[12] Capacidad de permanecer oculto sin cifrado, lo que dificulta identificar la amenaza.

[13] https://www.mcafee.com/enterprise/es-es/threat-center/threat-landscape-dashboard/ransomware-details.gandcrab-5-ransomware.html

[14] https://www.bleepingcomputer.com/news/security/ryuk-sodinokibi-ransomware-responsible-for-higher-average-ransoms/

MALWARE POS

Los cibercriminales han desarrollado malware específico para atacar y exfiltrar la información de los sistemas de punto de venta llamados POS, que, por lo general almacenan los datos de pago del cliente sin cifrar.

La información adquirida a través de la captura con malware POS proporciona un beneficio económico, bien sea por el uso directo por parte de los cibercriminales o bien por la venta en tiendas especializadas de la información bancaria obtenida.

La víctima de este tipo de malware tiene una afectación económica directa a través del card-not-present (CNP) o a través de la clonación de tarjetas.

Con este tipo de malware, los cibercriminales y usuarios de tiendas especializadas de la Darknet, tuvieron mucho éxito. Sin conocimientos técnicos, y apoyados en guías de uso, obtuvieron un beneficio económico inmediato.

El 2019 fue un año donde la amenaza de malware POS tuvo mayor relevancia respecto a años anteriores. Destacaron las vulnerabilidades ya conocidas de estos sistemas, como la falta de cifrado de la información o los sistemas operativos desactualizados. Asimismo, apareció un nuevo riesgo asociado a la finalización del soporte de Windows Embedded POSReady2009 el 9 de abril.[15]

Los sectores más afectados fueron los que tradicionalmente utilizan de forma más intensiva el POS[16] como el sector retail, restauración y cadenas de hostelería. Sin embargo, indirectamente a través del fraude, afectó ampliamente al sector financiero.

Una de las regiones más afectadas fue Estados Unidos, donde el pago con tarjetas de banda magnética sigue siendo común comparado con los pagos de pin o contactless[17].

Es necesario destacar que el malware POS tiene un estrecho vínculo con algunas APT de motivación financiera. Estos sistemas han sido objetivo por lo vulnerables que son y por la rentabilidad que genera a la hora de vender los datos hurtados. Las APT que han recurrido a este tipo de malware han sido FIN6,[18] FIN7 y especialmente FIN8.

En 2019 se observó un comportamiento común en los cibercriminales: la utilización de RAT acompañando a la explotación del malware POS. Esto se debe a que el RAT le permite mayor movilidad dentro del sistema.

[15] https://support.microsoft.com/es-es/help/4489209/end-of-support-for-windows-embedded-2009

[16] https://securityboulevard.com/2019/11/catch-says-pos-malware-incident-might-have-exposed-customers-data/

[17] https://www.visa.com.co/la-diferencia-visa/tecnologia-innovacion/tecnologia-contactless-pagos-latinoamerica.html

[18] https://labs.sentinelone.com/fin6-frameworkpos-point-of-sale-malware-analysis-internals-2/

A lo largo de 2019 se identificaron varios ataques relevantes:

- La APT FIN8 implementó entre marzo y mayo de 2019 un malware de shell inverso denominado Badhatch que fue dirigido especialmente contra el sector hostelero en Estados Unidos. El vector de ataque fue un spearphishing que contiene archivos adjuntos de Microsoft Word [19].

- DMSniff, detectado tras 4 años de actividad, estaba dirigido a pequeñas y medianas empresas de entretenimiento y restaurantes. Los cibercriminales infectaban los dispositivos mediante ataques de fuerza bruta a conexiones SSH o explotando diversas vulnerabilidades [20].

- GlitchPOS, descubierto en 2019, apareció en tiendas especializadas de la Darknet y con una interfaz fácil de usar; lo que facilitaba que cibercriminales de cualquier nivel pudieran utilizarlo. Se vendía alrededor de los 250$ [21].

Aunque el malware POS tiene un alto impacto por la exfiltración de datos y ha continuado su desarrollo en el 2019; es una amenaza relativamente sencilla de mitigar, siempre y cuando se mantengan los sistemas (POS) actualizados.

[19] https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/fin8-reemerges-with-new-pos-malware-badhatch

[20] https://securityaffairs.co/wordpress/82358/uncategorized/dmsniff-pos-malware.html

[21] https://digitalguardian.com/blog/pos-malware-continues-evolve-infect-restaurants

APT

En 2019 las APT (Advanced Persistent Threat) continuaron su actividad con nuevos desarrollos y adaptaciones realizadas según el ataque y la víctima a quien iba dirigido.

Los actores detrás de estos grandes grupos de amenaza siguen siendo provenientes de los países tradicionalmente activos en relación con los ciberataques, como Rusia, Irán, China y Corea del Norte. Sin ser los únicos actores a tener en cuenta.

La necesidad de participación en el panorama internacional como un actor relevante a través de relaciones políticas y económicas está dando lugar a que otros países, como Vietnam[22], participen y orquesten ataques a través de las APT.

Mediante ataques de ciberespionaje el país asegura una línea de financiación y adquisición de conocimiento que le permite a las empresas competir a nivel internacional.

La motivación de los grandes grupos cibercriminales radica en tres factores:

1. Motivación geopolítica.
2. Ciberespionaje, ya sea para la adquisición de conocimiento y patentes, o para el monitoreo de objetivos clave.
3. Motivación económica, mediante la cual se autofinancian, y financian al estado que los patrocina.

Se identificaron varias regiones objetivo. La principal es el Sudeste Asiático[23], debido a que la mayor parte de las APT proceden de esta zona geográfica y es un territorio con tensiones y conflictos regionales.

Seguida por los Estados Unidos[24], América Latina y la Unión Europea, con especial incidencia en el sector financiero y la captura de propiedad intelectual.

Las tensiones a nivel internacional entre los diferentes estados, la constante variación de los TTPs (Técnicas, Tácticas y Procedimientos) de las APT y su complejidad, están dando lugar a un incremento de los ataques orquestados por los Estados Nación, siendo probable que aumenten en el 2020.

[22] https://www.infosecurity-magazine.com/news/vietnamese-hackers-compromised-bmw/

[23] https://www.zdnet.com/article/middle-east-cyber-espionage-is-heating-up-with-a-new-group-joining-the-fold/

[24] https://threatpost.com/oil-and-gas-specialist-apt-pivots-to-u-s-power-plants/151699/

Durante el 2019, las infraestructuras críticas y el sector financiero fueron el objetivo de las APT . Un ataque a la economía y al funcionamiento del Estado pueden tener un alto impacto con graves consecuencias para un país.

El actor más relevante, por cantidad de APT[25] activas en 2019, fue Rusia; siendo las más activas Cobalt, Silence, MoneyTaker y FIN8.

Cobalt Group, cuyos ataques principales fueron en el sector financiero, tuvieron como objetivo principal los bancos y servicios de cajeros automáticos en Europa del Este y Asia.

- En 2019 realizaron una serie de ataques contra instituciones financieras de Kazajistán. Alojaron un documento malicioso en la página web de Kassa Nova Bank que al descargarlo solicitaba permisos para activar las macros que desplegaban la carga útil “Cobalt Strike”.[26]

Imagen 9. Funcionamiento de un documento con macros

[25] https://securelist.com/apt-trends-report-q2-2019/91897/

[26] https://gbhackers.com/cobalt-now-attack/

Silence APT, dirigida al sector financiero, ha realizado ataques a más de 25 países. Acostumbran a iniciar sus ataques por medio de un spear phishing con archivos adjuntos con macros, archivos CHM o LNK.

- En 2019 llevaron a cabo un ataque contra los cajeros automáticos de Dutch-Bangla Bank, hurtando unos 3 millones de dólares a través del uso del malware Silence.Downloader, Silence.MainModule y Silence.ProxyBot. Obtuvieron acceso a la infraestructura del banco y presumiblemente utilizaron el malware Atmosphere para llevar a cabo la captura[27].

MoneyTaker toma como víctimas a instituciones financieras y firmas legales, centrado principalmente en los sistemas de procesamiento de tarjetas como AWS CBR y SWIFT. Dado el amplio uso de STAR en América Latina, estas entidades podrían tener una exposición particular ante un posible interés del grupo. Comúnmente utilizan la vulnerabilidad CVE-2016-7255 para penetrar en la red.

- Entre 2018 y 2019 han perpetrado ataques exitosos contra diversas entidades, de todos ellos, tres ataques contra bancos rusos y uno en Reino Unido.

Proveniente de Corea del Norte, se ha seguido identificando al grupo Lazarus y sus subgrupos Bluenoroff y Andariel como una importante amenaza para el sector financiero. El grupo Lazarus, siendo una amenaza multifacética, ha impactado en entidades financieras a través de campañas y el malware ATMDtrack.

Bluenoroff y Andariel son subgrupos de Lazarus destinados a la financiación tanto del grupo como del régimen de norcoreano. Sus campañas se dirigen contra los ATM, las criptomonedas, SWIFT y entidades bancarias.

- Una muestra de su actividad a lo largo de 2019 es el despliegue por parte de Lazarus del malware ATMDtrack, variante del RAT Dtrack, diseñado para leer y almacenar los datos de las tarjetas de crédito introducidas en los ATM.

[27] http://www.itcandino.com/2019/07/05/grupo-ruso-de-hackers-silence-se-globaliza/

Por último, es necesario hablar sobre otros grupos APT cuya procedencia no está clara, pero actúan sobre el sector financiero. Estas han sido FIN8, APT-C-36 y TA505.

FIN8 lleva a cabo campañas con una motivación económica a través de malware especializado en POS. De esta manera capturan los datos de pago de las tarjetas de crédito y débito para posteriormente venderlos en foros de piratería con fines de lucro.

- En 2019 se destacan tres ataques contra gasolineras, a través de las cuales obtuvieron los datos de pago de los clientes. En uno de ellos, infectaron los sistemas a través de un phishing e instalaron un RAT que le dio el acceso al sistema POS. En otro, se utilizó un backdoor de código shell y sus funciones estaban basadas en el conocido troyano bancario Ursnif o Gozi.

Durante el 2019 se descubrió un ataque persistente de la APT-C-36 contra grandes corporaciones y administraciones públicas de Colombia cuya motivación era el ciberespionaje de información confidencial y estratégica del país

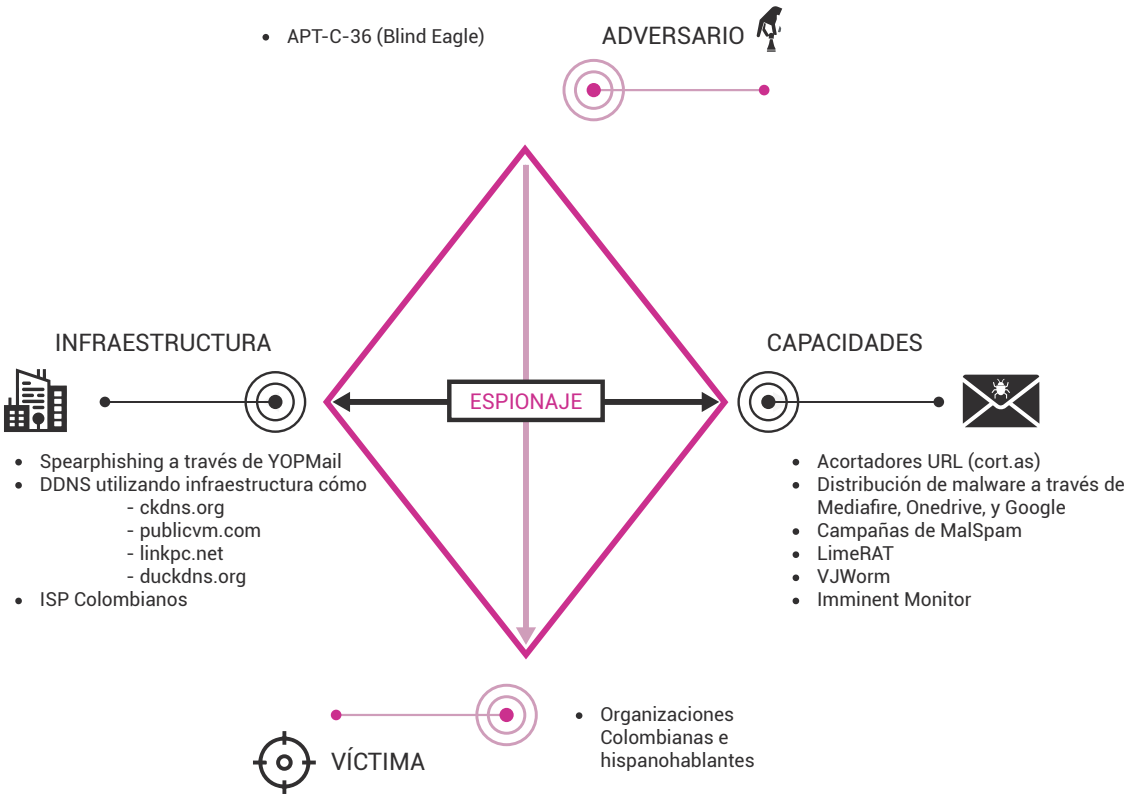


Imagen 10. . Modelo Diamante de APT-C-36

- Esta APT realizó intrusiones en compañías estratégicas del sector financiero mediante las cuales se podría obtener información relevante de las operaciones financieras del país.[28]

[28] Consultar monográfico APT-C-36 en el portal del asociado.

Por último, TA505 representa una parte importante del panorama de amenazas de correo electrónico y es responsable de una de las campañas de spam maliciosas más grandes observadas. Dentro de sus características, posee un alto grado de adaptabilidad y con frecuencia cambia sus herramientas y técnicas, operando a gran escala. Distribuye el troyano bancario Dridex, los ransomware Locky y Jaff y el troyano bancario Trickbot entre otros.

- Durante 2019 ha realizado diferentes campañas con variados TTPs tomando como víctimas diferentes entidades del sector financiero, entre otras .[29]

[29] https://www.cyberscoop.com/ta505-cybercrime-singapore-uae-us-proofpoint/

ATM

Los cajeros ATM son uno de los activos financieros más interesantes para los cibercriminales debido al beneficio económico inmediato que pueden llegar a obtener de ellos.

Para optimizar los ataques, los cibercriminales han ido desarrollando nuevos métodos, tanto desde la perspectiva lógica como la física.

Al ser el ATM un elemento físico, presenta diferentes vulnerabilidades fácilmente explotables como son los periféricos y la caja fuerte, los cuales han sido objetivos tradicionales para realizar ataques físicos.

Además, es necesario destacar que algunos manuales de los ATM y sus componentes están en la deep web, al acceso de cualquier usuario. Esto permite aprender su funcionamiento para poder planificar mejor un ataque.

Por otra parte, cabe señalar el equipo del ATM como el objetivo principal de los ataques lógicos.

Los ataques de tipo lógico han tenido especial relevancia en 2019 gracias al aumento de las capacidades de los cibercriminales y a la facilidad en el intercambio de herramientas maliciosas entre ellos.

Los ataques a la red del cajero se realizan principalmente a través de insiders[30] y phishing,[31] dos importantes amenazas para los ATM y el sector financiero. Especialmente los insiders son una amenaza que va en aumento, con un alto impacto para la entidad. Por medio de la coacción, por la voluntad propia de un empleado o técnicas de ingeniería social, los cibercriminales se infiltran en la red del banco e instalan un malware destinado a la captura de dinero.

Otro elemento que destacar y, que marcará un incremento de ataques en 2020, es relativo al sistema operativo de los cajeros automáticos. El 14 de enero, el sistema operativo de Windows 7 dejó de tener soporte,[32] por lo que un relativo alto porcentaje de cajeros automáticos quedan vulnerables ante futuros ataques perpetrados por cibercriminales.[33]

[30] https://www.techrepublic.com/article/60-of-companies-experienced-insider-attacks-in-the-last-year/

[31] https://www.computerweekly.com/news/252467639/Financial-services-top-cyber-attack-target

[32] https://www.zdnet.com/article/the-end-of-windows-7-is-the-real-end-of-the-pc-era/

[33] https://www.digitaltransactions.net/how-ready-are-deployers-for-the-next-big-operating-system-conversion-for-atms/

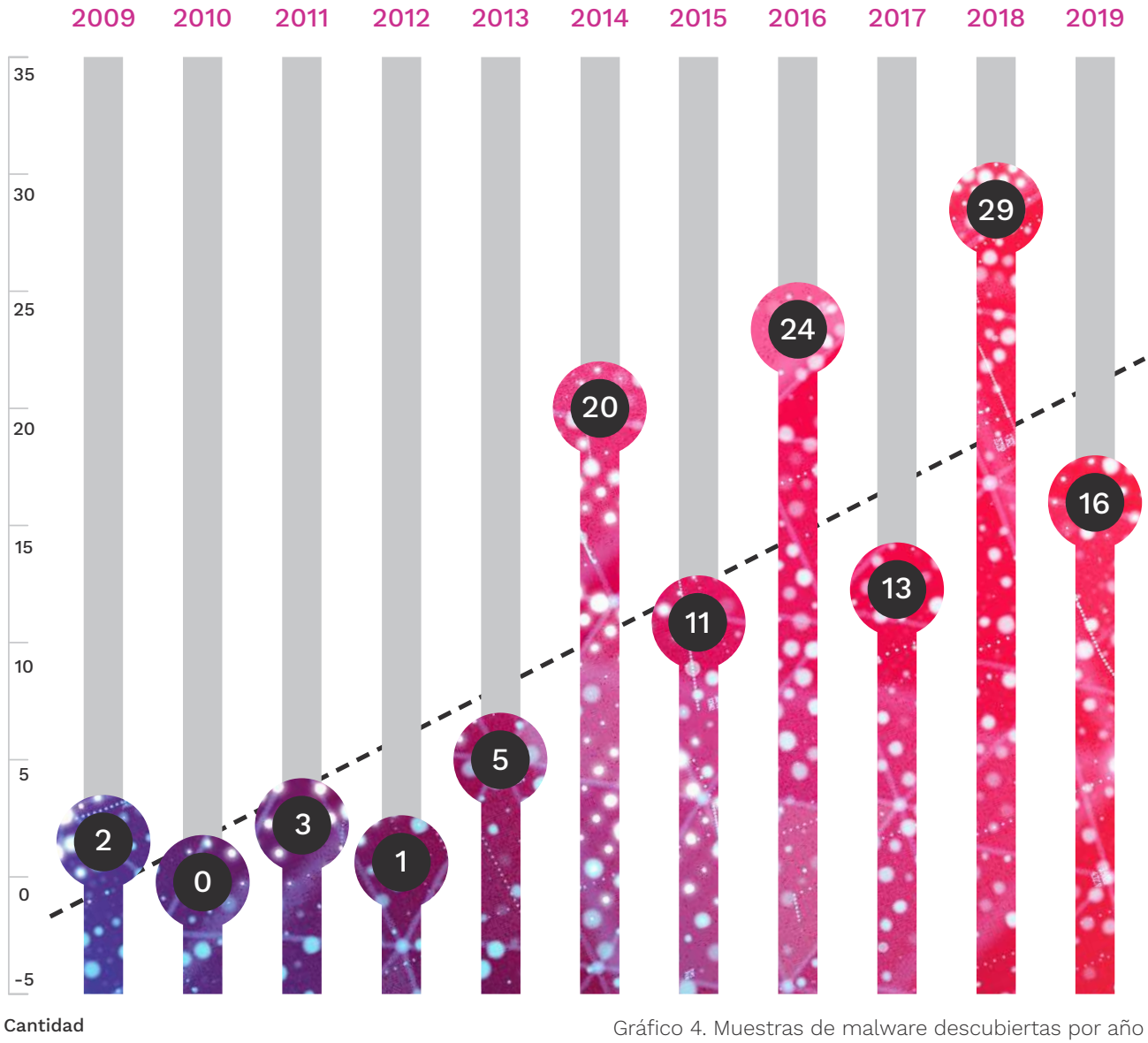


Gráfico 4. Muestras de malware descubiertas por año

Los ataques lógicos comenzaron en 2009 con el desarrollo del primer malware contra los ATM. Tras su aparición, se han ido desarrollando multitud de familias con características y funcionalidades adaptadas a diferentes objetivos. Así pues, los ataques lógicos contra ATM se han situado como una de las principales amenazas a lo largo de 2019.

Al igual que el malware para equipos, el destinado a ATM también sigue la tendencia en el desarrollo de códigos y técnicas más complejas con la intención de permanecer más tiempo en el sistema y poder hurtar un mayor monto de dinero.

En este sentido, los ataques denominados jackpotting[34] y blackboxing[35] tienen una especial mención por su impacto a lo largo de 2018 y 2019. Son técnicas que utilizan un malware que toma el control del ATM. Estos malware responden a comandos introducidos por los cibercriminales de manera remota. No requiere del uso de tarjetas y permiten la captura de elevadas cantidades de dinero en efectivo.

[34] https://www.cpomagazine.com/cyber-security/atm-malware-and-jackpotting-attacks-could-be-making-a-return/

[35] https://www.bankinfosecurity.com/no-card-required-black-box-atm-attacks-move-into-europe-a-10820

Los malware contra ATM que han evolucionado más rápido, tanto en complejidad como en uso son los siguientes:

- **ATMDispCash:** es capaz de interactuar con la unidad de dispensador de efectivo del cajero automático y tiene funciones relacionadas con instrucciones de control remoto del cajero. El uso de este malware requiere de un cibercriminal o mulero que esté presente, para presionar un código y retirar el dinero.

- **WinPot:** reemplaza la pantalla estándar del cajero automático con una interfaz que simula una máquina tragamonedas con cuatro botones con la etiqueta "SPIN". Adicionalmente se muestra un botón SPIN para sacar el dinero, un botón SCAN para volver a escanear el cajero y actualizar la información y, por último, un botón STOP para finalizar la extracción en curso.

A lo largo de 2019 se han hecho notar los malware CutletMaker, XFSCashNCR y ATMJaDi, siendo los que más impacto han tenido tanto en la región de América Latina como a nivel internacional.

- **CutletMaker:** está diseñado para ejecutarse desde una memoria USB y se basa en la DLL Diebold Nixdorf para enviar comandos a la unidad dispensadora del cajero automático. El troyano está ofuscado con VMProtect y recibe información sobre la moneda, el valor y el número de billetes de cada bandeja. El software se descifró y actualmente se distribuye de forma gratuita.

- **XFSCashNCR:** utiliza funciones de la API del XFS Manager (msxfs.dll) para conseguir dispensar, a través de los SPI, todo el dinero que sea ordenado.

- **ATMJaDi:** utiliza el software del cajero automático del banco, por lo que solo funciona en un pequeño subconjunto de cajeros. Se considera que pueda ser un malware específico que se desplegó gracias a un insider de la entidad afectada. Busca el proceso que controla el cajero automático y se inyecta en él, dándole el control del proceso legítimo.

Imagen 11. Venta del malware CutletMaker en un foro de la Darknet

Hasta el momento, sin embargo, las familias de malware que más han destacado a lo largo de la historia son Ploutus y Skimmer, ya que por su permanencia en el tiempo se han convertido en los malware tradicionales para la captura en cajeros automáticos.

Si bien es cierto que, en los últimos años, no han tenido especial actividad, continúan siendo el malware más vendido en modo servicio (MaaS).

Es probable que la actividad más reciente de Ploutus y Skimmer, provenga de ciberdelincuentes independientes que hayan comprado el malware; y no de grandes grupos cibercriminales, los cuales dirigen más su actividad a desarrollar nuevos malware complejos para campañas específicas o venta en la deep web para la autofinanciación.

MÓVILES

El desarrollo de malware contra dispositivos móviles es una tendencia al alza desde 2018, trayendo consigo un incremento de ataques contra estos dispositivos y todo un abanico de nuevos malware con un importante impacto a lo largo de 2019.[36]

Esta tendencia viene marcada por la evolución que han sufrido los teléfonos móviles , hasta convertirse en dispositivos inteligentes cuyas capacidades aprovechan todo el potencial de internet para convertirse en verdaderos equipos de bolsillo.

Este potencial es aprovechado por los cibercriminales, los cuales han identificado los dispositivos móviles como valiosos objetivos de ataque de donde extraer información confidencial y así poder obtener beneficios económicos.

La predisposición de las empresas a facilitar el trabajo desde los teléfonos móviles y el hábito de almacenar información sensible en estos dispositivos a través, por ejemplo del BYOD[37], han facilitado la proliferación de cibercriminales interesados en malware contra móviles.

Las nuevas prácticas de la banca online o el e-commerce están incentivando el repunte de ataques a los dispositivos en busca de información personal o financiera, como las credenciales bancarias.

Existen factores de riesgo que predisponen a los dispositivos móviles a ser víctimas de los cibercriminales. Vulnerabilidades como la CVE-2017-0781 de Bluetooth referente a BlueBorne[38] o la CVE-2019-2114 sobre la tecnología NFC[39] de los móviles, recuerdan que no existe un software 100% seguro, y que las actualizaciones son vitales para seguir protegidos.

El sistema operativo que utilice el dispositivo es otro factor relevante para determinar si un dispositivo es vulnerable o no. Es destacable que los sistemas operativos Android e IOS son los más atacados debido a que son los sistemas más extendidos en uso.[40]

Especialmente Android, es la mayor víctima de los cibercriminales. Su naturaleza de plataforma abierta da la capacidad a los cibercriminales para desarrollar nuevas muestras con facilidad.

Por otra parte, la falta de antivirus, de verificación de correos electrónicos, SMS y URL y, en general, la falta de precaución a la hora de utilizar un dispositivo móvil con la información y capacidades de las que este dispone, facilitan la generación de vectores de ataque para los cibercriminales.

36 https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/

37 https://www.incibe.es/protege-tu-empresa/blog/bondades-y-riesgos-del-byod

38 https://www.armis.com/blueborne/

39 https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2019-2114

40 https://www.macworld.co.uk/feature/iphone/iphone-vs-android-market-share-3691861/

En este sentido se detecta el phishing, en conjunto con la ingeniería social, como el principal vector de ataque contra los dispositivos móviles en 2019.

Otro vector de ataque muy común en este 2019 ha sido la descarga de aplicaciones para móvil, especialmente aquellas que provienen de fuentes de terceros, ya que estos no cuentan con el control de los distribuidores oficiales como Apple Store o Google Play.

Así mismo, desde junio de 2019 se ha identificado el Malware-as-a-Service (MaaS) como una importante vía de distribución de malware, incluyendo en este ecosistema cibercriminal a los malware para dispositivos móviles. Se puede llegar a considerar estas tiendas como una vía de distribución que ofrece pistas sobre el comportamiento final del mismo, y adelanta la elaboración de escenarios y tendencias futuras.

El CSIRT Financiero monitorea el mercado cibercriminal en la deep web, pudiendo determinar de esta manera que el tipo de malware contra dispositivos móviles más vendido es el troyano bancario.

A lo largo de 2019, los malware para móviles han tenido un desarrollo muy similar al de los malware para equipos.[41] Han ido adquiriendo capacidades de ocultación de software, siendo además más persistentes y eficaces. De esta manera se puede esperar para 2020 que los códigos sean más complejos y difíciles de detectar.

Cabe destacar, por su alto impacto en 2019, los siguientes malware:

- **Xhelper.** Dispone de la capacidad especial de persistir, incluso cuando el dispositivo móvil se devuelve a estado de fábrica. Es un malware que se encuentra en constantes modificaciones y mantenimiento, por lo que se observa mucha actividad. Dado que es reciente, seguirá teniendo una gran repercusión a nivel global.

- **Anubis.** Su relevancia procede de la filtración de su código fuente en tiendas de la Darknet. Diferentes grupos cibercriminales han tenido acceso a este malware modificándolo en función de sus necesidades, lo que ha dado lugar a que, con el tiempo, se le haya dotado con mayores capacidades con respecto a la original.

- **Cerberus.** Troyano bancario generalmente distribuido por medio de aplicaciones descargadas de sitios de terceros. El malware es comercializado en distintos foros de la darkweb, aunque los desarrolladores tienen una cuenta y foro “oficial” para ofrecer “demos”. Este troyano está diseñado netamente para dispositivos móviles con sistema operativo Android. Tiene la capacidad de obtener datos financieros de distintas aplicaciones bancarias, entre ellas PayPal, lo que supone un riesgo de suplantación de identidades para realizar compras electrónicas.

[41] Consultar monográfico sobre malware en dispositivos móviles en el portal del asociado.

FRAUDE

Desde el CSIRT Financiero se realiza un monitoreo constante del ecosistema cibercriminal para poder detectar tendencias que pudieran resultar en un incremento del fraude.

De esta manera, a lo largo de 2019 se han identificado varias tendencias al alza que están desembocando en un importante incremento de diferentes tipos de fraude, exigiendo nuevas medidas de seguridad al sector financiero como una víctima más.

Card Not Present

En primer lugar, se ha identificado una tendencia al alza del fraude "Card-Not-Present" (CNP) gracias a la facilidad en la captura de los datos de tarjetas mediante técnicas de ingeniería social a través de Internet, especialmente phishing y sus variantes.

Al no necesitar la tarjeta física y no poderse comprobar la identidad del propietario, es visto como el eslabón débil dentro de los procesos de compra a través de internet. Además, es utilizado como punto de entrada del fraude.

La implantación del chip EMV y, el incremento de seguridad en las tarjetas en general, han sido factores determinantes para el aumento del fraude CNP.[42]

Para poder proceder a la explotación de las tarjetas, los ciberdelincuentes necesitan obtener el nombre del titular, el número de cuenta, el código de seguridad CVV y la fecha de vencimiento de la tarjeta.

Para conseguir todos los datos, además del uso del phishing, los cibercriminales recurren a tácticas de investigación avanzada sobre sus víctimas en Internet y Social Media. También es muy común el uso de skimming, los malwares bancarios y en menor medida, el uso del hacking en bases de datos de comercios.

Tras esto, la información de las tarjetas puede ser vendida o utilizada directamente por parte de los cibercriminales. En el primer caso, suelen ser publicadas en foros especializados de compra de tarjetas de crédito en la deep web y la darknet, oscilando su precio en función de si la tarjeta ha sido verificada por los cibercriminales y el tipo de tarjeta que sea, entre 2$ y 8$.

[42] https://usa.visa.com/visa-everywhere/blog/bdp/2019/05/28/chip-technology-helps-1559068467332.html

Dumps y fraude de tarjeta presente

Durante 2019 se mantuvo al alza la venta de dumps de tarjetas de crédito, implicando con ello un incremento del fraude.

Los dumps de tarjetas consisten en el volcado de la información de la banda magnética de una tarjeta de crédito o débito en una tarjeta falsa. Estas tarjetas se utilizan para realizar lo que se llama “fraude de tarjeta presente”. Este es un tipo de fraude es muy común y de los más lucrativos en el ecosistema criminal.

El precio de los dumps, que generalmente proviene de minoristas, hoteles y restaurantes ha rondado durante 2019 entre los 15$ y 20$ por tarjeta. Sin embargo, el precio de los CVV se ha mantenido entre los 2$ y 8$ por cuenta. Los dumps todavía se mantienen muy por delante en términos del número total de tarjetas comprometidas para la venta.

Sin embargo, desde 2018 se registra una tendencia en la que, debido a que la oferta no alcanza la alta demanda de CVV, su precio se ha incrementado llegando a superar en ocasiones incluso el precio de los dumps.

El valor creciente de los datos de CVV ha hecho que muchos cibercriminales hayan redirigido su actividad hacia el fraude CNP. Esto explica el incremento durante 2018 y 2019 de ataques a sitios web e-commerce para obtener los datos de tarjetas de crédito.

A través de diferentes técnicas, los criminales son capaces de hurtar los datos de las tarjetas de sus víctimas. La técnica más común es el skimming en entornos físicos, como cajeros automáticos o estaciones de servicio.

Generalmente, los skimmers los proporcionan comunidades cerradas de skimmers profesionales que se mueven dentro de foros especializados en la deep o dark web. Estas redes proporcionan logística, herramientas (skimmers, cajeros, decodificadores) e información para ejecutar operaciones correctamente.

Otra técnica existente para realizar dumps es la utilización de malware que infecta sistemas POS. La mayoría de estos malware tienen la capacidad de leer los datos de las tarjetas que se encuentran alojados en la RAM; así, los cibercriminales se conectan mediante acceso remoto y adquieren los datos.

Imagen 12. Pasos de un ataque típico para realizar fraude CNP

Fraud-as-a-Service (FaaS)

El CSIRT Financiero ha podido evidenciar a lo largo de 2019 que el fraude ahora es comercializado en la modalidad de servicio, es decir, la información hurtada por los criminales se dispone para ser vendida en Internet. La compra de este tipo de información se realiza por transferencias bancarias o a través de criptomonedas, ya que son pagos difíciles de rastrear.

El FaaS genera una amenaza constante para el sector financiero. Es una modalidad de cibercrimen que permanecerá mientras siga habiendo usuarios dispuestos a realizar comprar de productos ilícitos.

Tras una investigación del CSIRT Financiero, se pudo determinar algunos factores que hacen propensos a algunos usuarios a ser víctimas de un posible fraude.

En primer lugar, se encuentra la región de procedencia de la tarjeta. Tras un estudio de las tarjetas puestas a la venta en foros de la deep web, se identificó que dos de cada tres tarjetas provienen de Estados Unidos; sin embargo, Rusia refleja el menor número de tarjetas expuestas.

El proveedor de la tarjeta es otro factor relevante a tener en cuenta, ya que se determinó que el 57 % de las tarjetas expuestas eran Visa, el 29% de Mastercard y el 12% pertenecían a American Express.

El tercer elemento relevante es el tipo de tarjeta del usuario, una tarjeta corporativa o tarjetas especiales como las Platinum de American Express son objetivos más beneficiosos para los cibercriminales que una tarjeta de crédito o débito.

Huellas digitales

Por último, el equipo de analistas del CSIRT Financiero ha investigado, desde sus inicios a mediados de año, uno de los mercados que más está creciendo entre los cibercriminales: la venta de huellas digitales.

Estas permiten la realización de actividades maliciosas y fraude con mayor discreción. Por ello, se detecta un aumento de la captura de huellas digitales. Además, facilita la circulación de este producto de un modo “más abierto” a través de la Darknet.

Se ha podido investigar un mercado con más de 60.000 perfiles robados de diferentes sitios, entre los que se incluyen organizaciones pertenecientes a sectores financieros, streaming, almacenamiento, gaming y, en general, sectores con crecientes beneficios.

El tipo de información que se vende suele ser login y password, cookies, fingerprints de navegadores e información de tarjetas de crédito, lo que posiblemente dé lugar a la realización de fraude a través del uso de esa información adquirida.

Esta información está a la venta a un precio que, por lo general, puede variar entre los 5 y 200 dólares por perfil dependiendo del valor de la información robada.

Dentro de los perfiles de la víctima, la información recogida que se encuentra a la venta en los foros de la darknet incluye la resolución de la pantalla, IP e ISP, navegador y plugins, versión del sistema operativo y, en general, información que ayuda a suplantar a la víctima.

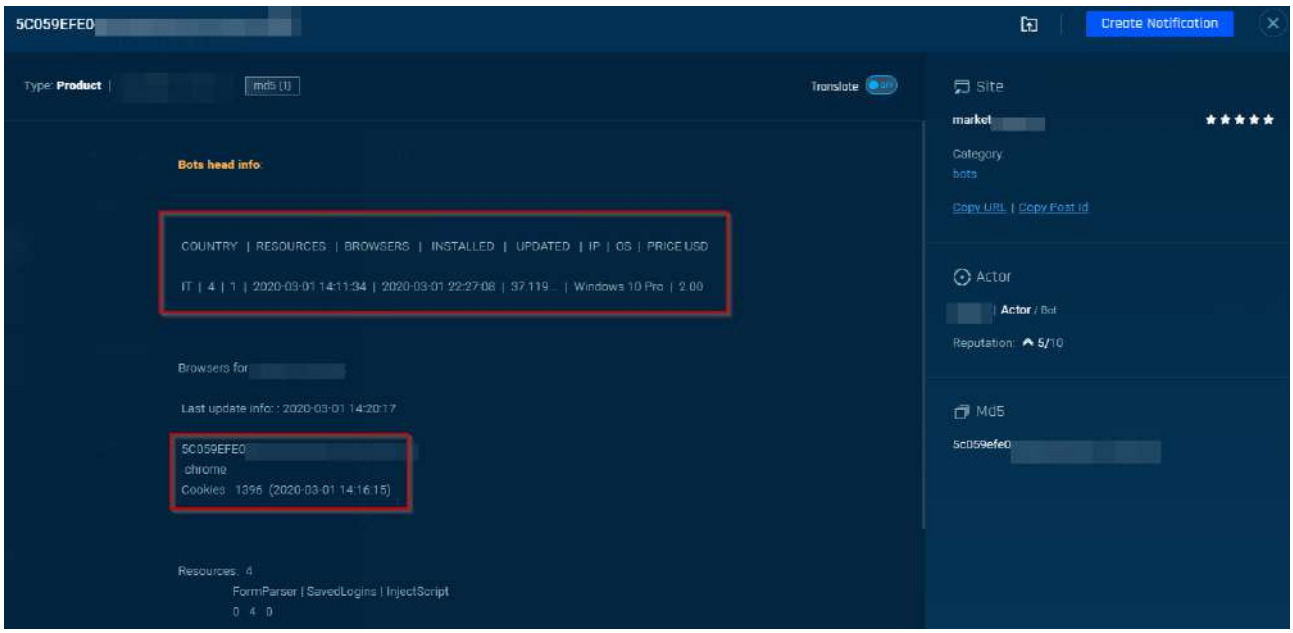


Imagen 13. Captura de una venta de bots en la Darknet

De esta manera, los cibercriminales que adquieran estas identidades pueden evadir las soluciones antifraude que incorporan estos parámetros como parte de la autenticación.

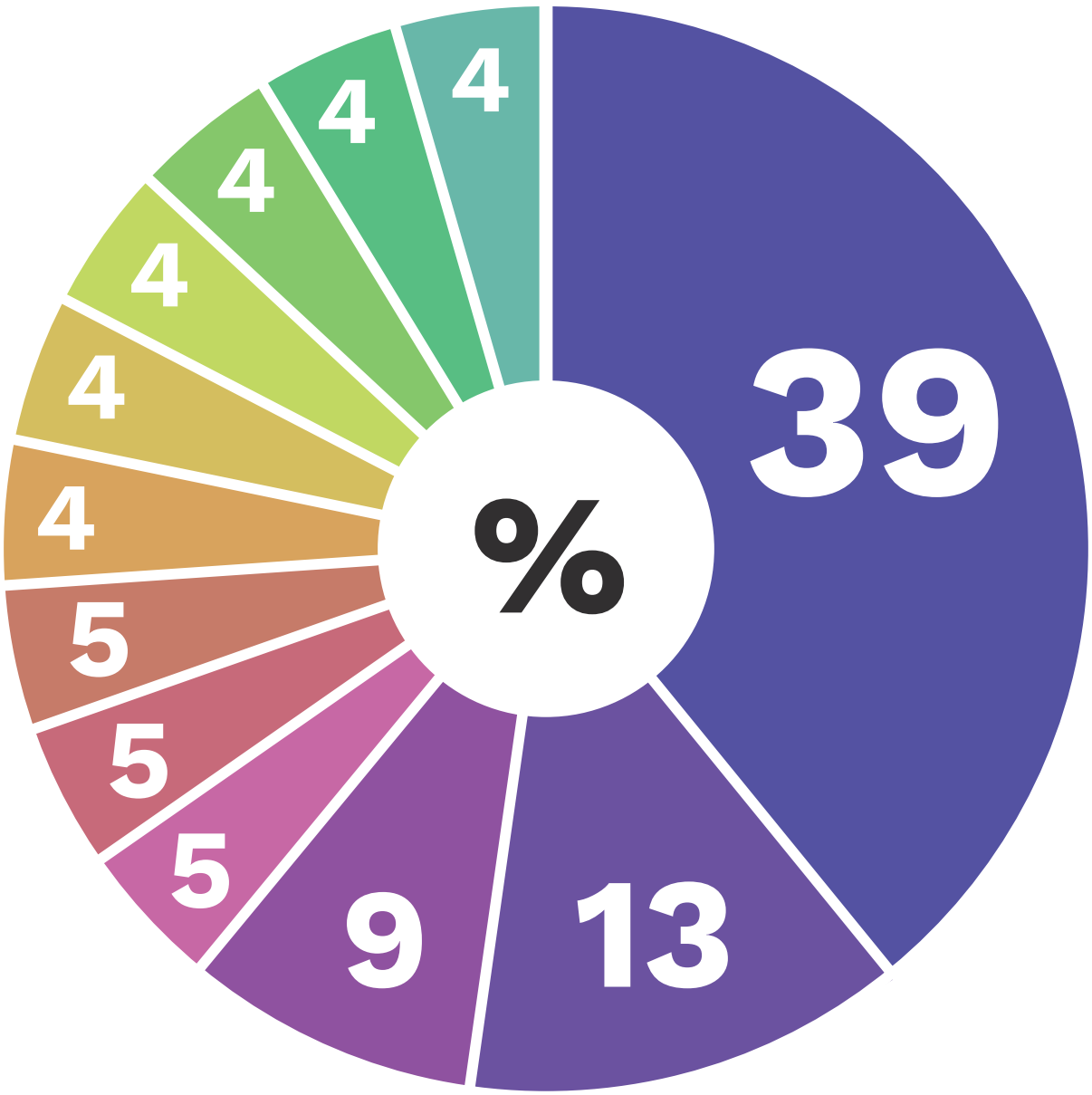
Para su correcto funcionamiento, una vez que el criminal adquiere una huella digital, debe disponer de un entorno preparado para poder explotarlo, que generalmente parte de adquirir un bot “proxy” para poder salir a Internet por una IP que esté geoposicionada en el mismo país del fingerprint adquirido.

B. INTELIGENCIA DE AMENAZAS

Inteligencia de amenazas está enfocada a la investigación, análisis, clasificación y validación de información a través de fuentes internacionales y locales del CSIRT Financiero. Su fin es investigar y analizar vulnerabilidades para prevenir la apertura de brechas de seguridad mediante la generación de alertas tempranas.

Desde junio de 2019 se reportaron un total de 31 alertas tempranas, entre las que se destacaron las vulnerabilidades que afectan a sistemas Microsoft, Linux y Oracle.

A continuación, se resaltan las vulnerabilidades más relevantes ocurridas en el año anterior, que por su criticidad podrían lograr impactar el sector financiero.



39%	Microsoft	13%	Linux	9%	Oracle
5%	Docker	5%	Notepad	5%	Intel
4%	Opteva 4.x	4%	Hardware de Memoria	4%	ProFTPD
4%	VMware	4%	WordPress	4%	SQLite

Gráfico 5. Vulnerabilidades reportadas por inteligencia de amenazas

A. Oracle Flexcube Direct Banking

En primer lugar, se evidenciaron dos nuevas vulnerabilidades dirigidas a la plataforma “Oracle FLEXCUBE Direct Banking”, creada para el soporte y administración a canales de banca por internet, banca móvil y banca por texto.

Estas vulnerabilidades, a las que se les han asignado los CVE-2019-2979 y CVE-2019-2980, forman parte de “Oracle Financial Services Applications”, cuyas versiones compatibles que se ven afectadas son la 12.0.2 y 12.0.3. Las vulnerabilidades, fácilmente explotables, permiten que un cibercriminal, con bajos privilegios y acceso a la red a través de HTTP, comprometa la banca directa de Oracle FLEXCUBE.

Los ataques exitosos de estas vulnerabilidades pueden resultar en un acceso no autorizado a datos críticos, o acceso completo a todos los datos sensibles de la herramienta.

Aunque no se han observado explotaciones de dichas vulnerabilidades en un entorno real, si se llegase a producir alguna explotación en alguna entidad que hiciese uso de dicho software, las consecuencias que tendría serían muy graves a nivel de confidencialidad e integridad de la información recogida en la herramienta.
Un cibercriminal que aprovechara esta vulnerabilidad lograría acceder a información relacionada con credenciales bancarias de los clientes de la organización, pudiendo realizar un volcado de esta información para su posterior venta en diferentes fuentes o incluso la realización de transferencias ilegítimas.

El impacto que tendría a nivel reputacional sería tal, que podría llevar al cierre de la organización por las pérdidas, tanto económicas como de clientes.

B. Sistema operativo Windows

Se identificaron vulnerabilidades que afectan a controladores del sistema operativo Windows. Investigadores descubrieron más de 40 controladores de los que se puede abusar para elevar los privilegios del espacio del usuario a los permisos del kernel. Los proveedores afectados incluyen todos los principales proveedores de BIOS y compañías de negocio de hardware de computadores como lo son: ASUS, Toshiba, Intel, Gigabyte, NVIDIA y Huawei.

Las vulnerabilidades encontradas permiten que el controlador sirva como proxy para realizar acceso con privilegios a los recursos de hardware, como lo son el acceso de lectura y escritura al espacio del procesador y chipset. Además, los cibercriminales podrían sobrepasar el interfaz de firmware y hardware, lo que permite comprometer el host víctima de tal forma que no podría ser detectado por los productos normales para la protección de amenazas que operan a nivel de sistema operativo.

C. Memoria

Otra de las vulnerabilidades destacadas son las amenazas mediante ataques “RAMbleed”, que explotan vulnerabilidades en la memoria RAM de las máquinas para extraer datos y tomar control remoto de máquinas.

Esta vulnerabilidad tiene el CVE-2019-0174 y podría permitir a un cibercriminal sin privilegios leer los datos contenidos en los procesos que se encuentran en ejecución en memorias DDR3 y DDR4. El ataque consiste en la sustitución de bits en las líneas vecinas del módulo de memoria. A través de este tipo de ataque, se podría disponer del acceso a credenciales root de un proceso vecino en ejecución, obteniendo de esta manera el control de todo el sistema.

De Windows aparecieron una serie de vulnerabilidades 0-day[43] que podrían afectar los sistemas mediante escalamiento de privilegios sin permiso de usuario, inyección de código arbitrario por medio del proceso iexplore.exe y ejecución de código malicioso en segundo plano.

D. Protocolo RDP

Además, sobre Windows se han reportado 4 vulnerabilidades críticas en el protocolo RDP que podrían permitir a los ciberdelincuentes ejecutar código remoto en los equipos víctimas.

A estas vulnerabilidades se les han asignado los CVE-2019-1181, CVE-2019-1182, CVE-2019-1222 y CVE-2019-1226. En total, las vulnerabilidades afectan a todos los sistemas Windows a partir de la versión 7 SP1, entre las que se incluyen Windows

[43] Una vulnerabilidad para la cual no se crearon parches o revisiones y que se emplea para llevar a cabo un ataque.

Server 2008 R2 SP1, Windows 8.1, Windows Server 2012, Windows Server 2012 R2 y todas las versiones compatibles de Windows 10, incluidas las versiones de servidor.

Su criticidad tan alta es debida a la facilidad de explotación y propagación que tienen, ya que un criminal solo necesitaría un paquete RDP de pre-autenticación especialmente diseñado para poder ejecutar código no autorizado de manera remota sobre el equipo de la víctima. Además, gracias a las propiedades de gusano que comparten dichas vulnerabilidades, cualquier criminal podría propagarse por la red del equipo infectado.

E. BlueKeep

Estas propiedades son similares a las que tiene la vulnerabilidad CVE-2019-0708, mejor conocida como BlueKeep, la cual fue notificada por Microsoft en su boletín de mayo de 2019 y tuvo gran impacto mediático.

Si un cibercriminal aprovechara alguna de estas vulnerabilidades, y se propagase a través de la red, sería capaz de causar daños de una magnitud considerable, ya que podría instalar otros tipos de malware como podría ser un ransomware o RAT.

El mejor ejemplo lo encontramos en el conocido ataque de WannaCry, un Ransomware que se distribuyó aprovechando la vulnerabilidad EternalBlue de Microsoft. Permitía ejecutar código no autorizado de manera remota y propagarse por la red. Afectó a más de 300.000 equipos alrededor de 151 países, tanto a empresas como a particulares, y causó pérdidas de miles de millones de dólares.

El alcance de estas vulnerabilidades es muy extenso, ya que en la actualidad existen un total de 800 millones de usuarios que utiliza alguno de los sistemas mencionados. Así pues, se trata de vulnerabilidades críticas que pueden afectar a la confidencialidad, integridad y disponibilidad de la información.

Por último, cabe recordar el anuncio de Microsoft en el que se notifica el fin del soporte técnico para Sistema Operativo Windows 7, con fecha de 14 de enero de 2020. Por tal razón, se deberá prever que a partir de esta fecha no habrá ningún tipo de parche a posibles vulnerabilidades.

Más de 40 controladores certificados por Microsoft, de alrededor de 20 proveedores diferentes de hardware, han sido descubiertos como vulnerables por sus fabricantes, pudiendo ser aprovechados por los cibercriminales para obtener privilegios más elevados en los sistemas víctimas.

Si se aprovecha este fallo de seguridad, un cibercriminal podría tener acceso a la lectura/escritura de la memoria del núcleo, los registros de control (CR), los registros específicos de modelo (MSR), los registros de depuración (DR), la memoria física y la memoria virtual. Pudiendo de esta manera ocultar e instalar malware difícil de detectar por las soluciones de seguridad (dando al cibercriminal persistencia en el sistema, incluso si se reinstala el sistema operativo).

F. Internet Explorer

En la detección de amenazas al sector financiero, se identificaron vulnerabilidades de varias versiones del navegador Internet Explorer y Windows Defender, que al ser explotadas podrían generar ataques de tipo denegación de servicio, ejecución remota de código y/o elevación de privilegios lo que permitiría comprometer la confidencialidad, disponibilidad e integridad de la información.

Un cibercriminal que aproveche esta vulnerabilidad sobre un sistema que tuviese iniciada una sesión con privilegios de administrador, podría tomar los privilegios de este permitiéndole tomar control absoluto del sistema infectado. Entre las tareas que podría realizar se encuentran:

- Modificación y borrado de archivos.
- Creación de nuevas cuentas o modificación de las ya existentes.
- Captura de información.
- Descarga de otros archivos en el sistema.

Todo este problema reside en la librería jscript9.dll, que es el motor de scripting de este navegador en sus versiones 9, 10 y 11. Aunque Microsoft desaconsejó el uso de este navegador y advirtió a los usuarios que migraran a Edge, se tiene constancia de que todavía ocupa un 7% del mercado mundial aproximadamente, es decir, Internet Explorer es el tercer navegador en cuanto a expansión y uso de navegadores web, siendo solo superado por Chrome y Firefox.

Hoy en día existen ya una serie de herramientas potencialmente peligrosas que pueden explotar vulnerabilidades de JScript en Internet Explorer, como por ejemplo jRAT, Koadic y NanHaiShu. Herramientas que son utilizadas activamente por grupos criminales como Leviathan y APT28.

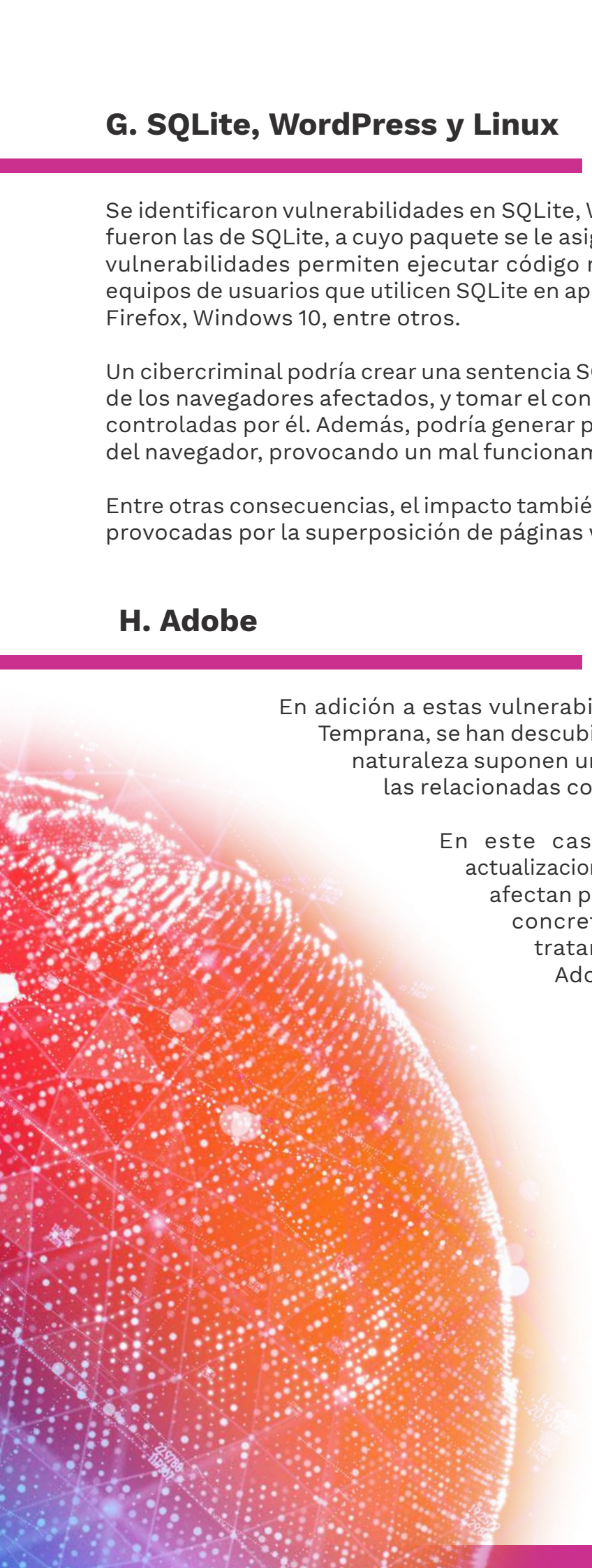
G. SQLite, WordPress y Linux

Se identificaron vulnerabilidades en SQLite, WordPress y Linux. Las más relevantes fueron las de SQLite, a cuyo paquete se le asignó el nombre de “Magellan 2.0”. Estas vulnerabilidades permiten ejecutar código remoto a través de internet sobre los equipos de usuarios que utilicen SQLite en aplicativos como Google Chrome, Mozilla Firefox, Windows 10, entre otros.

Un cibercriminal podría crear una sentencia SQL con código malicioso, dirigida a uno de los navegadores afectados, y tomar el control del sistema abriendo páginas web controladas por él. Además, podría generar problemas en el manejo de la memoria del navegador, provocando un mal funcionamiento.

Entre otras consecuencias, el impacto también puede producir fugas de información provocadas por la superposición de páginas webs legítimas.

H. Adobe



En adición a estas vulnerabilidades reportadas a modo de Alerta Temprana, se han descubierto otras vulnerabilidades que por su naturaleza suponen un riesgo para cualquier entidad, como las relacionadas con Adobe.

En este caso, Adobe publica mensualmente actualizaciones para sus vulnerabilidades, las cuales afectan principalmente a equipos de escritorio, concretamente a software encargados del tratamiento de documentos como lo son Adobe Acrobat y Adobe Acrobat Reader.

Numerosos atacantes se aprovechan de las vulnerabilidades que Adobe hace públicas, debido a su gran expansión, siendo explotadas principalmente para la exfiltración de información confidencial o la distribución de algún tipo de malware. En relación a la distribución de malware, se destaca Sykypot Trihab, un troyano que fue capaz de hurtar las credenciales de las tarjetas inteligentes del Departamento de Defensa de los Estados Unidos (DoD), consiguiendo así acceder a recursos e información altamente restringida.

C. APOYO A INCIDENTES

La línea de apoyo a incidentes que el equipo del CSIRT Financiero tiene como objetivo asesorar a la entidad asociada sobre las acciones en la verificación, análisis y definición de medidas para la contención o mitigación de incidentes de ciberseguridad; proporcionando información relevante y recomendaciones a través del análisis de información sectorial.

Así pues, a lo largo de 2019, además de apoyo a incidentes, se ha trabajado sobre una serie de Case Study y Playbooks con el objetivo de comprender las amenazas tradicionales que se pueden encontrar en el sector financiero a fin de saber actuar en consecuencia y mitigarlas.

En este sentido, se encuentran a disposición de los asociados dos Case Study sobre ciertas amenazas concretas que han sido muy relevantes en 2019: Emotet y WannaCry. Por otra parte, también están disponibles ocho Playbooks, cinco de ellos concernientes a los ataques más comunes de los que el sector financiero es víctima (Ransomware, Malware, Defacement, DDoS y Fuga de información) y dos restantes concernientes a dos amenazas más específicas, WannaCry y Emotet.

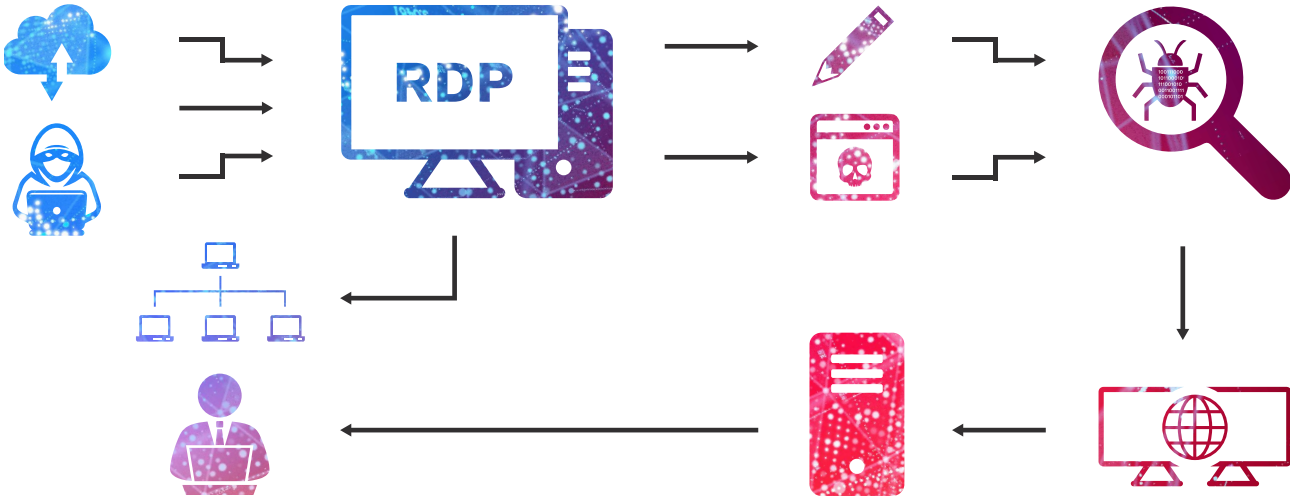
Imágen 14. Portada del PlayBook de la amenaza Ransomware

Tal y como se ha comentado anteriormente, desde junio de 2019 se han lanzado 23 peticiones a la línea de Apoyo a Incidentes del CSIRT Financiero, siendo destacable que, 10 de esas peticiones, estuvieron relacionadas con phishing. A pesar de la constante concienciación, el phishing y la suplantación de identidad siguen siendo los principales vectores de ataque de las ciberamenazas existentes, aprovechándose del factor humano y la ingeniería social para llevar a cabo los ataques.

De los reportes realizados, el más relevante fue un incidente sobre una variante de WannaCrypt. En este caso se creó un caso de incidente de seguridad reportado como sospechoso en un servidor de almacenamiento de la red interna. Tras una investigación realizada por el equipo del CSIRT Financiero se identificaron evidencias de tráfico hacia direcciones IP externas e internas.

Las conexiones se realizaban hacia múltiples direcciones IP de redes internas, por el puerto 445 (SMB), el cual se utiliza para ofrecer acceso compartido a archivos. Se hace necesario destacar que este protocolo trae consigo una serie de vulnerabilidades como la que permitió el cifrado de archivos de equipos a nivel mundial con WannaCry.

Entre otras evidencias descubiertas, se identificó la desactivación del antivirus, conexiones SSH a una de las direcciones IP externas relacionadas con redes Botnet y servidores de Comando y Control (C&C).



Imágen 15. Infografía del incidente

Finalmente se pudo identificar que, a través de una vulnerabilidad no parcheada del equipo en el RDP, un atacante ejecutó un código variante de Wannacrypt con características de gusano. Eso le permitía la propagación a través de la red, alcanzando principalmente al servidor de almacenamiento de la entidad reportadora.

El objetivo logrado por el ransomware fue mantener el acceso (persistencia) al servidor de almacenamiento en caso de ser descubierta la actividad RDP. Posteriormente logró conectar a una red botnet, así como al servidor de comando y control (C&C) para finalmente, deshabilitar el antivirus.

TENDENCIAS

EN CIBERAMENAZAS PARA 2020

Las organizaciones se ven inmersas en los procesos de transformación digital que impulsan las nuevas tendencias en el desarrollo de las estrategias, la gestión y la operación de las compañías; y que facilitan el paso hacia los nuevos modelos de negocio.

Según el informe de Accenture[44] sobre el análisis de la transformación a nivel mundial, más del 50% de las compañías han acelerado la transformación en los últimos tres años. Esto significa un aumento considerable de la velocidad respecto al periodo anterior.

Esta transformación afecta a todas las áreas de las compañías. Desde recursos humanos hasta las áreas de operación y tecnología, presentes en procesos internos, pero también en la relación de las organizaciones con sus stakeholders. Ciertamente, según avanza esta transformación, también se abren nuevas vías de explotación de vulnerabilidades corporativas que pueden materializarse en el impacto de una ciberamenaza.

El equipo de analistas del CSIRT Financiero ha elaborado una lista de aquellas tendencias en ciberamenazas que estarán presentes durante el 2020.

Se han seleccionado en función de dos criterios:

- Las nuevas ciberamenazas que puedan impactar sobre determinados sectores o áreas organizativas.
- Las que, aun estando presentes hoy en día, pueden aumentar en volumen y daño al sector.

[44] https://www.accenture.com/_acnmedia/pdf-94/accenture-techvision-2019-tech-trends-report.pdf

LAS TIC EN LA SOMBRA

Algunas compañías consideran la posibilidad de facilitar a los empleados la instalación de herramientas al margen de las consideradas por la organización. En este sentido, ya se habla de que, probablemente, un tercio de los ataques exitosos sufridos en las empresas son debido a las denominadas TIC en la sombra.

Los cibercriminales dedican mucho esfuerzo y dinero a descubrir puntos débiles que puedan explotar; como son las vulnerabilidades tecnológicas presentes en las herramientas que usan los empleados. Aplicaciones que la mayoría de los casos no son tenidas en cuenta por las corporaciones, que no son controladas ni son actualizadas.

En paralelo, se observará un aumento de los ataques relacionados con la técnica Supply chain attack, dirigida especialmente hacia la suplantación de software legítimo, que induce a las víctimas a instalar aplicaciones aparentemente limpias. Sin embargo, estas aplicaciones realmente contienen información para realizar conexiones a servidores de comando y control (C&C) para la descarga de programas maliciosos que le permitan al ciberdelincuente realizar la captura de la información sensible del usuario y el equipo comprometido.

Desde este punto de vista, se hace cada vez más necesario el control del software instalado en los activos corporativos, así como continuar con la concienciación de todas las personas relacionadas con la organización.

AUMENTO EN LA FILTRACIÓN DE DATOS

La exfiltración de información ya sea para venta o para explotación, se presenta como una de las principales ciberamenazas del 2020.

En este sentido, las técnicas avanzadas de SQL injection y/o el query string manipulation, facilitan la intervención de formularios de datos, cookies e incluso las cabeceras http abriendo la posibilidad a la exfiltración masiva de la información por parte de los cibercriminales.

Por otro lado, el error humano seguirá presente, en las bases de datos mal configuradas o las que no tienen suficientes medidas de seguridad.

El equipo de analistas del CSIRT Financiero, ha evidenciado que la venta de datos en el mercado negro continúa siendo una de las más dinámicas, así como es de lo más rentable para los ciberdelincuentes, llegando a considerarse un “commodity” o necesidad.

MALWARE CON NUEVAS CAPACIDADES

Durante el próximo año presenciaremos ataques cada vez más sofisticados y focalizados en objetivos específicos, con nuevos métodos, técnicas, tácticas (TTP) y un arsenal de programas maliciosos cada vez más precisos y difíciles de identificar. Además de código malicioso eficaz y eficiente.

En este sentido se observan las siguientes tendencias para el 2020.

Malware “sin archivo” (fileless)

Aunque continúa la expansión de malware a través de las macros de Windows, se ha evidenciado la aparición de malware ejecutándose en la memoria. Esta nueva técnica podría llegar a tener un largo recorrido.

En términos generales, el malware “sin archivo” penetra normalmente a través de la memoria RAM, maniobra que le permite evadir la detección de los antivirus y herramientas de seguridad, siendo activado en cualquier momento por malware híbrido que desee pasar desapercibido.

Actualmente este tipo de malware es comercializado en el mercado negro para la exfiltración de información confidencial.

Malware modular

Continúa la evolución y el desarrollo del malware modular que inició su peligroso despliegue en 2018, y que está demostrando ser una de las mayores ciberamenazas. Es un nuevo tipo de malware que se adapta completamente a los sistemas que pretende infectar utilizando novedosas técnicas y tácticas que le permiten acceder al dispositivo sin ser detectado.

Para conseguirlo, actúa en varias fases: primero instala sus componentes esenciales, después analiza a profundidad el sistema y su seguridad, posteriormente, envía la información recolectada al servidor de comando y control (C&C) y por último descarga los módulos más requeridos para lograr su cometido.

En el mercado negro se comercializa cada día más malware de este tipo, por lo que es probable que haya un incremento en su uso.

Algunas de las ventajas del malware modular frente al tradicional son la posibilidad de cambiar la firma (hash) para no ser detectado por los antivirus y herramientas de seguridad perimetral, así como la activación de exploits específicos en función de las vulnerabilidades detectadas en el sistema objetivo.

En términos generales, el malware modular se adapta a cualquier entorno y se integra al sistema objetivo, convirtiéndose en una de las ciberamenazas más peligrosas conocidas.

Ransomware

Se ha observado un descenso en los ataques de ransomware dirigido al ciudadano, aunque no va a desaparecer. Sin embargo, se observará un aumento contra áreas de la sociedad de las que pueda nutrirse más rápido y obtener mayores beneficios. En este sentido, aumentarán los ataques contra las corporaciones y entidades gubernamentales, con la intención de interrumpir el funcionamiento y operación mediante el cifrado de la información e indisponibilidad de los sistemas que la usan.

Por otro lado, se están evidenciando avances en el uso del ransomware contra las distribuciones de Linux. Los cibercriminales son conscientes que muchos sectores, entre ellos el financiero, han optado por este tipo de distribuciones, teniendo en cuenta su Licenciamiento, el supuesto bajo índice de ataques que sufren y que son más seguros que los sistemas comerciales como Windows.

Troyanos de acceso remoto (RAT)

En el último año se ha evidenciado una gran expansión en la venta y uso de los troyanos de acceso remoto por los ciberdelincuentes. Sin duda, hoy se ha constituido en uno de los productos estrella del mercado negro.

El equipo de analistas del CSIRT Financiero ha observado un cierto nivel de competitividad entre los ciberdelincuentes con este tipo de malware, a través de una mayor oferta a precios más asequibles y con una mayor cantidad de funcionalidades.

Una de las grandes ventajas del RAT es que aparenta ser una aplicación legítima, por lo que su detección es muy complicada. Una vez que se ha producido la infección, el cibercriminal puede ver la pantalla, así como todo lo que hace la víctima, de manera que puede realizar sin problema las acciones que más le convengan, incluyendo los desplazamientos laterales.

Por su naturaleza, los RAT son un tipo de troyano muy utilizado para la captura de cuentas bancarias, aunque también son el medio ideal para el ciberespionaje.

Infraestructuras críticas

Cabe resaltar que durante el año 2019 se han visto varios intentos de atacar a diferentes infraestructuras críticas con diversas familias de malware, tendencia creciente en los sistemas industriales que estará presente en 2020.

Project Anchor

El troyano bancario Trickbot es uno de los malware que se han ido desarrollando de forma modular, lo que le permite ajustarse a un mayor número de actores maliciosos.

Project Anchor es un nuevo módulo recientemente añadido que confiere a Trickbot una serie de herramientas, como Meterpreter, PowerShell Empire o CobaltStrike, que otorgan la capacidad al troyano bancario de mantener a los cibercriminales ocultos dentro de la red infectada, dándoles tiempo para hurtar información y mapear la infraestructura TI.

Este nuevo módulo, enmarcado dentro del Crime-as-a-Service (CaaS), permite a actores como las APT tener una mayor facilidad para explotar las redes de las víctimas de alto perfil. Esto da lugar a una nueva forma de cibercrimen donde grupos cibercriminales y Estados Nación colaboran para realizar ataques de alto perfil más enfocados y en menor tiempo, compartiendo información y ganancias.

Probablemente para 2020 se vea un incremento de la detección de campañas de APT con motivación económica y de ciberespionaje en el sector financiero debido a las facilidades que proporciona Project Anchor en el panorama cibercriminal.

EXPANSIÓN DE LA INGENIERÍA SOCIAL

El phishing continúa expandiéndose y utilizando nuevas tácticas. Durante el año que viene seguiremos asistiendo a la utilización de la ingeniería social para cometer todo tipo de estafas, especialmente dirigidas a hurtar la información bancaria de los usuarios.

En este sentido continúan avanzando las técnicas orientadas al perfeccionamiento de la manipulación del usuario, mejorando especialmente el uso multiplataforma del phishing para desconcertar a la víctima a través de canales más cercanos.
Así se verá un incremento en:

- El uso de las redes sociales en dos direcciones: por un lado, como plataformas para investigar en mayor profundidad a las potenciales víctimas y manejar un mejor discurso contra ellas; y por otro, utilizarlas como plataformas para la rápida difusión de phishing.

- La utilización de mensajes de texto SMS (Smishing) que facilitan y aumentan la presión y ansiedad sobre la víctima al recibir directamente los avisos “falsos” en su propio teléfono.

- La proliferación del uso de portales de gaming, tanto para coordinar futuros ataques como para difundir las estafas.

- El uso, cada vez más frecuente, de las llamadas de teléfono (vishing y FakeIP Calling) con la intención de aumentar la presión y aumentar la confusión en los usuarios.

También continúa en auge el fraude al CEO, a través del cual se manipula a las víctimas para realizar una transferencia fraudulenta.

FRAUDE Y CIBERATAQUES AL SECTOR FINANCIERO A NIVEL GLOBAL

TROYANOS BANCARIOS PARA MÓVIL

El universo de los dispositivos móviles no para de crecer gracias a que la sociedad estimula el desarrollo de nuevas funcionalidades y aplicaciones en movilidad.

El avance de estos dispositivos es tal, que hay partes de la sociedad en las que han desplazado completamente a los equipos de cómputo.

Las organizaciones están acelerando el proceso de transformación digital como un valor competitivo más para aumentar su cuota en el mercado de nuevos negocios o nuevas líneas de negocio que incluyen la banca online.

Los cibercriminales continúan aumentando su inversión de tiempo y dinero en la elaboración de nuevos troyanos bancarios más difíciles de detectar y más eficaces en la captura de información bancaria, como números de cuenta, usuarios y contraseñas, perfiles biométricos, etc.

Desde el 2018 se han evidenciado un aumento en los ataques a dispositivos móviles con estos propósitos, sin embargo, su auge se dio en 2019. Es de esperar que la tendencia continúe en aumento y se convierta en una de las ciberamenazas más peligrosas contra el sector financiero.

AVANCE DEL CARD-NOT-PRESENT

Colombia es el cuarto país de la región en volumen de transacciones a través de e-commerce. Y la cifra va a continuar creciendo durante los próximos años.

El aumento del e-commerce[45] es una tendencia mundial impulsada por los cambios en las costumbres de compra de los ciudadanos. La falta de tiempo, la comodidad del transporte actual de mercancías y los precios altamente competitivos en la adquisición de productos globales, convierten a esta modalidad en una verdadera oportunidad para clientes y proveedores.

Sin embargo, la facilidad en los métodos de pago online abre una puerta a que los cibercriminales puedan hurtar la información personal, números de tarjetas y demás información sensible.

El phishing y la captura de bases de datos que contienen información de tarjetas aumentan todavía más el riesgo de ser víctima de un ciberdelito.

En el último año, el Card-Not-Present se ha convertido en una tendencia al alza, ya que para los cibercriminales es más sencillo conseguir los datos, incluyendo el CVV y pasar a explotarlas de forma virtual, dejando la captura y clonado de tarjetas físicas relegado a un nicho en concreto: los cajeros ATM.

EL DOBLE FACTOR DE AUTENTICACIÓN YA NO ES SEGURO

En los últimos años se ha producido un uso intensivo del doble factor de autenticación para identificar a un usuario. Para ello, normalmente se recurre como primer paso al uso de unas credenciales y, como segundo paso, al uso del celular del cliente, al que se le envía un código de verificación (también puede ser enviado a un correo electrónico).

Este es uno de los métodos de autenticación más utilizados por el sector financiero para validar que el usuario es quien dice ser.

Sin embargo, en los últimos meses está proliferando el uso de malware que permite el salto “bypass” del 2FA. Por ejemplo, se ha producido un aumento de malware contra dispositivos móviles capaz de permitir al cibercriminal leer el código de verificación y borrar todo rastro en el celular del usuario. También ha aumentado el uso de Troyanos de acceso remoto (RAT), que facilita la toma de control de la cuenta de correo cuando el usuario está “logueado”.

Este tipo de ciberamenazas han comprometido la capacidad de protección del factor de doble autenticación, lo que ha obligado a introducir nuevas medidas, como por ejemplo la biometría y la biometría gestual pasiva.

[45] https://www.portafolio.co/negocios/colombia-cuarto-en-ventas-a-traves-de-ecommerce-532185

VENTA DE LA HUELLA DIGITAL

El equipo de analistas del CSIRT Financiero lleva tiempo siguiendo la venta de la huella digital en los mercados negros de la Deep Web y la Darknet, o lo que a nivel técnico se denomina fingerprint.

Esta huella contiene datos como la resolución de pantalla, versión del sistema operativo, navegadores utilizados y plugins instalados en los mismos, sistema operativo del dispositivo móvil, etc.

Toda esta información se está comercializando actualmente entre 5 y 200 dólares por perfil y es utilizada para suplantar la identidad digital del usuario.

Este tipo de información puede ser empleada en aquellas aplicaciones que gestionan el acceso en el reconocimiento, no sólo de las credenciales, sino también del perfil tecnológico del usuario.

El equipo de analistas está observando un aumento en la venta de estos perfiles, por lo que considera que es una ciberamenaza a tener en cuenta en los próximos años.

Para poder explotar este tipo de información, los cibercriminales necesitan instalar un plugin en su navegador y comprar bots con las IP que les permitan falsear el geoposicionamiento del usuario suplantado

INSIDERS

A lo largo de 2018 y 2019 se ha identificado a los insiders como una amenaza creciente para todos los sectores, si bien es cierto que, en algunos sectores como el financiero, esta amenaza tiene una mayor incidencia e impacto.

La tendencia a la externalización de la fuerza laboral de las empresas y la existencia de numerosos proveedores externos son factores que pueden incrementar el riesgo de la existencia de un insider, además del riesgo de recibir un ciberataque a la cadena de suministro.

Un insider puede suponer un importante riesgo para la entidad financiera, desde casos de fraude, a sabotaje de sistemas informáticos y captura de propiedad intelectual, generalmente motivado por el interés propio.

A pesar de la existencia de tecnologías como registros de gestión de identidad y acceso (IAM), que permiten un mayor control de la actividad, los insiders suelen ser empleados con accesos privilegiados que les permiten realizar actividades ilícitas con una menor posibilidad de detección.

En 2019 se han detectado varios casos relevantes de insiders que han impactado con un coste económico importante para las organizaciones, sin embargo, cabe destacar el caso del malware ya tratado anteriormente, ATMJaDi.

Este malware utiliza el software del cajero automático del banco víctima, y, por tanto, sólo funciona en un pequeño subconjunto de cajeros automáticos. Es posible que, en este caso, cuya afección se dio en México y Colombia, el vector del ataque haya sido un insider de la entidad bancaria.

Finalmente, a lo largo de 2019 se ha identificado qué elemento ha sido el más vulnerable frente a estos ataques, la información confidencial y estratégica que las entidades manejan, por lo que un riguroso control de los accesos privilegiados ayudará a mitigar esta amenaza.

ATAQUES A LA “NUBE”

En los últimos años se ha evidenciado que la computación en nube resulta ser la base de uno de los modelos de negocio y operación más rentables de los últimos tiempos.

La expansión de la migración de los datos e información propia de la operación al modelo nube “en modo servicio” facilita los nuevos modelos de trabajo, como el teletrabajo, o el trabajo colaborativo; así como ahorra costes fijos a las compañías.

Sin embargo, precisamente bajo la filosofía de “todo conectado” y “disponible en cualquier lugar y en cualquier momento”, toda la información recopilada en la nube se ha convertido en un activo muy interesante para los ciberdelincuentes.

En este sentido, los cibercriminales han dado ya los primeros pasos en dos direcciones:

- Uso de la nube para desplegar los ataques. Por ejemplo, una de las grandes ventajas para los ciberdelincuentes es la posibilidad de desarrollar botnets directamente en la nube para diversos tipos de ataque, como los DoS.

- Ataques contra bases de datos mal configuradas en la nube. Este nuevo ecosistema digital es realmente interesante por contener gran parte de la información y datos sensibles de las compañías que están migrando a ella. No sólo las grandes compañías, sino que las pequeñas también están entrando en esta nueva forma de trabajar. Así pues, cuanta más información se migra, más interesante se vuelve para los cibercriminales.

EXPANSIÓN DE LA GUERRA CIBERNÉTICA

Debido a la inestabilidad política a nivel mundial y al choque de intereses variados, tanto de estados como de grandes corporaciones vinculadas a los mismos, continuará la frecuencia en el uso de diferentes técnicas, tácticas y procedimientos (TTP) orientadas al ciberespionaje con motivaciones políticas, como por ejemplo:

- Conocer los últimos movimientos políticos del enemigo o de los aliados.
- Hurtar propiedad intelectual para obtener ventajas competitivas.
- Adquirir información privilegiada para disponer de ventaja ante posibles negociaciones.
- Mejorar ofertas y/o adelantarse ante concursos de grandes infraestructuras.

En términos generales, se pretende disponer de información sensible para la toma de decisiones a nivel geopolítico y geoeconómico. En este sentido, el uso de APT como recurso para la guerra cibernética continuará siendo tendencia durante el 2020.

Es importante destacar que, en la guerra cibernética, cualquier organización puede ser víctima, pues puede contener una pieza de información interesante, ya sea para la corporación, o para el país en el que opera o del que es originaria.

NUEVAS TECNOLOGÍAS

Las nuevas tecnologías estarán presentes, tanto para mejorar las defensas como para ser explotadas por los cibercriminales. En este sentido se observan movimientos en los desarrollos de inteligencia artificial, tanto en su versión de machine learning, como en su versión de deep learning:

- Por un lado, se ven movimientos para poner a prueba diferentes sistemas que puedan contener desarrollos basados en Inteligencia Artificial.

- Por otro lado, se han observado intentos de ataque utilizando redes neuronales con la intención de desarrollar ataques mucho más rápidos y adaptativos al entorno víctima.

Si bien es cierto que durante el 2020 no se verá una proliferación de estos escenarios, es evidente que están en un estadio inicial que verá su eclosión más tarde o más temprano.

Otro de los recursos tecnológicos más interesantes como nuevo vector de ataque durante el 2020 es el uso de drones para realizar ataques a la red. En este último año se ha visto una proliferación de estos, a la par que se desarrollan nuevos modelos de drones más pequeños, potentes y con baterías de larga duración. Por lo que es de esperar cada vez un mayor uso por parte de cibercriminales especializados en este tipo de ataque.

El ataque con drones suele tener una motivación centrada en el ciberespionaje para la posterior explotación diversa de los datos recopilados.

Finalmente, la implantación de los nuevos modelos tecnológicos basados en IoT y 5G crearán nuevas vulnerabilidades, tecnológicas, procedimentales y humanas que serán explotadas por los cibercriminales.

TENDENCIAS

TECNOLÓGICAS PARA EL SECTOR

La problemática derivada de la transformación digital y el ataque a los procesos de negocio por parte de los cibercriminales lleva consigo el desarrollo de nuevas tecnologías que tienen por objetivo reducir el riesgo y/o su impacto.

En esta memoria anual se pretende dar visibilidad a aquellas tecnologías más relevantes para el sector financiero, y que despegarán o se consolidarán durante el 2020.

GESTIÓN DE IDENTIDADES

La identidad digital se crea cuando un usuario de un sistema o aplicación se conecta a ella. Mientras se produce la conexión, se van generando una serie de atributos que la tecnología o software que la gestiona va a ir utilizando para la conexión y el uso que la organización ha considerado “adecuado”.

En la mayor parte de las ocasiones, mientras se recopilan estos atributos, también se puede proceder a la validación (en caso de que sea necesario validar que sean auténticos) o autorización de los mismos (para determinar si se permite el acceso y/o a qué partes).

Hasta la fecha, la gestión de identidades se ha desarrollado en torno a una serie de procesos y tecnologías basadas en la parametrización de reglas, detección de patrones, etc.

Una de las grandes tendencias tecnológicas para el sector financiero es la sustitución de los procesos y tecnologías tradicionales vinculados a la Gestión de Identidades (IAM) por su transformación en procesos y tecnología que apuntan a la Gestión de la Identidad en modo Servicio (IDaaS) como dominante.

La tecnología asociada al IAM se basa en complejas parametrizaciones, cada vez más difíciles de gestionar debido a la gran cantidad de aplicaciones a las que deben acceder los stakeholders de la organización, desde los clientes hasta los proveedores.

Por otro lado, cada vez es más frecuente que haya que gestionar identidades en aplicaciones “on premise”; a la vez que deben gestionarse los accesos a aplicaciones en nube a las que se puede conectar desde cualquier parte del mundo y desde cualquier dispositivo.

Esta complejidad y dinamismo termina, por ejemplo, empujando a los empleados a utilizar sólo una contraseña para todas las aplicaciones. A los empleados (corporativos) y usuarios (clientes o intermediarios) les resulta complejo recordar diferentes contraseñas y, más aún, si son seguras (incluyendo números, minúsculas y mayúsculas y sin coherencia gramatical).

Por otro lado, la tendencia al Single Sign On (conexión a múltiples aplicaciones y plataformas con un único usuario y contraseña) plantea un riesgo al usuario, que junto a la complejidad y dinamismo de tener que utilizar múltiples plataformas, termina tomando la decisión de utilizar la misma en todas.

BIOMETRÍA

A medida que el 2FA reduce su eficacia contra el cibercrimen aparecen nuevas tecnologías orientadas a la autenticación, como es el caso de la biometría, normalmente acompañada del uso de la huella digital (tipo de dispositivo, IP desde donde se conecta, navegador, sistema operativo, etc.).

Desde hace unos años se ha disparado el uso de la biometría física como un elemento clave para el control de acceso a instalaciones físicas, ya sean públicas o privadas. Incluso se han incorporado a edificios y casas particulares, sustituyendo a la tradicional llave o las tarjetas de acceso.

En el mundo digital, se ha visto potenciado el uso de la biometría física[47], como el registro de la cara o la huella dactilar, gracias a la nueva generación de móviles que permiten utilizar el escaneo y la fotografía como herramientas de control de acceso. Algunos incluso incluyen en el hardware un espacio para situar el dedo.

Tal es el avance hacia este tipo de posibilidades, que los cibercriminales ya están investigando cómo aprovechar las posibles vulnerabilidades que deriven de ellas; como el hecho de que la información recopilada debe guardarse en una base de datos para ser explotada y que, por lo tanto, se puede "asaltar".

Para reforzar la biometría física se está desarrollando en paralelo la biometría basada en el comportamiento del usuario con el interfaz (behavioral biometrics). Este tipo de tecnología utiliza toda la potencia del machine learning para elaborar perfiles muy detallados basados en el uso frecuente que da el usuario a las aplicaciones o plataformas con las que interactúa.

Uno de los sectores más beneficiado por este tipo de tecnología es el financiero, pues con el perfilado de los usuarios, el sector puede asegurar no sólo que el usuario es quien dice ser, sino que además no está siendo manipulado. Si alguien toma el control de una cuenta de la banca online durante la sesión, generará una anomalía en el patrón de comportamiento que será alertada y gestionada según considere la organización.

[47] https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html

CVV DINÁMICO

El CVV o CVC dinámico[48] es una tecnología que apareció ya en 2015 como una prometedora solución contra el fraude en las transacciones realizadas en e-commerce. Con el paso de los años, diferentes bancos la han ido implementando,[49] y aunque aún existen factores de mejora, intenta simular el modelo del chip EMV para evadir la posibilidad de fraude.

A través de un algoritmo, bien a través de la aplicación de banca online o bien a través de una pantalla electrónica que contiene un CVV o CVC en la tarjeta, se facilita un número diferente válido para un periodo corto de tiempo, impidiendo la realización de acciones fraudulentas si los datos de las tarjetas han sido comprometidos.

El tiempo que manejan las tarjetas con esta tecnología para cambiar el CVV va desde 30 minutos hasta 4 horas, por lo que limita en gran medida el margen de actuación de un cibercriminal dentro del fraude CNP, desde que obtiene la información de la tarjeta hasta que la usa o la vende en foros de la darknet.

Si bien es cierto que encontrar una frecuencia ideal para el cambio de CVV puede ser un potencial problema, pudiendo dificultar la agilidad de las transacciones online.

Por otra parte, esta es una tecnología que incrementa el precio de producción de las tarjetas, desde unos 4 dólares hasta los 20 dólares por tarjeta. A pesar de todo, la disminución del fraude CNP que puede proporcionar el CVV dinámico podría llegar a cubrir el incremento.

[48] https://www.gemalto.com/latam/servicios-financieros/tarjertas/tarjeta-dcv

[49] https://www.deutsche-bank.es/pbc/data/es/calma.html

NUEVOS SISTEMAS DE PAGO

Los sistemas de Punto de Venta (POS)[50] y los métodos de pago utilizados sobre estos han tenido una gran evolución en los últimos años. Atrás quedan ya otros sistemas como la caja registradora, las TPV o la banda magnética de las tarjetas bancarias.

Los sistemas POS y los métodos de pago se benefician de las nuevas tecnologías para evolucionar, basándose en factores como la inmediatez, la versatilidad y la movilidad para adaptarse a la necesidad de los consumidores.

De esta manera, con respecto a los sistemas POS y, teniendo en cuenta lo anteriormente mencionado, lo más destacable es la tendencia hacia lo inalámbrico, desarrollándose sistemas de lectores inalámbricos cada vez más pequeños, portables y con capacidad para la lectura de cualquier tipo de código.

Por otra parte, los métodos de pago se adaptan constantemente a las nuevas tecnologías, tendiendo a abandonar las tradicionales tarjetas bancarias y el chip EMV.

De hecho, se está extendiendo el pago a través de contactless con la tecnología NFC[51], bien sea a través de las propias tarjetas bancarias que tengan habilitada esta opción o a través de los dispositivos móviles.

El NFC agiliza los procesos de pago y evita el uso de tarjetas físicas y captura de las mismas. Sin embargo, es necesario tener en cuenta que este tipo de tecnologías pueden traer consigo nuevas ciberamenazas, como nuevas vulnerabilidades.[52]

Con el desarrollo de los dispositivos móviles y las capacidades que estos tienen, la tendencia será a convertirlos en medios de pago capaces de sustituir las tarjetas bancarias convencionales.

[50] https://www.oracle.com/es/industries/food-beverage/what-is-restaurant-pos.html

[51] https://www.techradar.com/news/what-is-nfc

[52] https://latesthackingnews.com/2019/11/05/hackers-may-exploit-android-nfc-beaming-vulnerability-to-deliver-malware/