## a.- INTRODUCCIÓN

### a.1. Génesis:

De 10 años a esta parte, el trabajo artesanal de los ciberdelincuentes que se dedicaron, no sólo desde la faz técnica (black hat hacking), sino también los que mediante ingeniería social desarrollaron métodos para obtener fondos ilícitos, ha ido mutando, ganando en músculo, atomizándose y generando nichos de actividades que antes sólo eran un paso más de la estructura del delito, desde su inicio o creación del método, hasta la obtención final de la ganancia.-

Como todos sabemos, el ejemplo más claro, el del phishing, era una actividad restringida a personas que con un conocimiento medio-alto en programación, desarrollaban un set o combo de phishing (sitios web clonados, SMS, mail, entre otros), luego ejecutaban el siguiente paso que consistía en canalizar, mediante "hosteo" -alojamiento- del sitio apócrifo -y su publicidad-, o envíos sistematizados de ataques dirigidos o masivos, logrando obtener credenciales (usuarios y contraseñas, 2fa, mfa).-

Más adelante, veremos que a esta actividad en forma acotada se la denomina "scammers" o montadores de "scams".-

A veces, ellos mismos o personas vinculadas a éstas eran las encargadas de prestar asistencia para actividades conexas, como por ejemplo, prestando su voz para los "vishing" (voice phishing), pero siempre manteniendo un entorno de acción unificado.-

Con ello, era el mismo autor el encargado de vaciar la cuenta obtenida.-

Esta actividad, se valía especialmente del desconocimiento absoluto de la población en general, de las fuerzas de seguridad y de la

justicia, sobre la existencia de estos métodos, quienes ante el resultado no salían de su perplejidad y por ende difícilmente podían identificar a los autores, a sus métodos, y mucho menos recuperar los fondos sustraídos.

Rápidamente, esta realidad fue mutando, resultando necesario desde el punto de vista de la actividad criminal generar reaseguros para evitar ser identificados y detenidos, y con ello perder, no sólo la libertad, sino también el botín obtenido.-

El primer escollo que advirtieron fue el de canalizar los fondos mediante una cuenta propia o de terceros vinculados, lo que permitía de forma muy sencilla realizar la trazabilidad del dinero, y así identificar a las personas que estaban detrás de la maniobra.-

De allí, nacen las "mulas".

La evolución de esta especie marcó rápidamente la necesidad de segmentar la actividad en mulas de primer nivel, y mulas de segundo o tercer nivel.

Las primeras de ellas, las más expuestas al riesgo, fueron reclutadas en el segmento de la población más vulnerable, como adolescentes, ancianos, y personas de bajos recursos, incluso hemos visto en sus inicios que el desconocimiento de la población en general de la existencia de estas maniobras, circunstancia que a la fecha no ocurre, servía para captar voluntades mediante engaños, siendo las "mulas" personas que desconocían los fines espurios de la maniobra asociada a su identidad.

Más adelante en el tiempo, la segmentación de la actividad demandó la necesidad de utilizar canales alternativos a los bancos tradicionales, cuya rigurosidad en las identificaciones de identidad operaban como un obstáculo, para obtener más rápidos y libres de riesgo los fondos mal

habidos.

Ello decantó en el empleo de las incipientes billeteras y bancos digitales, cuyos parámetros de validación de identidad en su inicio resultaban débiles, y por ende un terreno propicio para navegar en el anonimato.

Como sabemos, esas falencias fueron emparchadas por los operadores de dichos sistemas, requiriendo cada vez más parámetros de validación biométrica, generando de este modo un nuevo obstáculo que los ciberdelincuentes debían sortear. Y como era de esperar, lo hicieron.

Para ello se sumergieron en el mundo de las transacciones "cripto", aprovechando la falta de regulación, la especial cualidad de navegar transfronterizamente y la anonimización de las cuentas, y la inicial falta de herramientas de traceo.

Nuevamente jugaron, y lo hacen en la actualidad, con la falta de preparación de las fuerzas del orden y la justicia para lograr métodos efectivos de rastreo de estas transacciones.

Lo cierto es que tibiamente, y con la aparición de nuevas herramientas para lograr desandar este camino, el uso de criptomonedas se está transformando en una actividad no tan libre riesgo, y esperemos que así continúe siéndolo.

Ha ayudado en este aspecto, el particular interés demostrado por algunos operadores del sistema, públicos y privados, entre ellos, algunas "exchange", operadores judiciales y policiales, que a paso lento, pero firme, proponen desasnar este universo plagado de incógnitas.

Otro ejemplo claro, del crecimiento sobredimensionado de estas estructuras delictivas, y por ende la segmentación y atomización de actividades, se vio claramente en el primer tramo de la cadena de valor de la

actividad ilícita.

Es así que se fueron escindiendo actividades que previamente eran propias del autor y ejecutor de la maniobra de “ingeniería social”, reclamando que sean otros los operadores que converjan en ayuda para desarrollar diversas actividades, o que bien resultaban riesgosas, o que escapaban a los conocimientos técnicos del criminal.

Este es el caso, como veremos, de los “scammers” o “montadores de scams”, cuya actividad es la creación de páginas clonadas, quienes inicialmente eran los mismos que luego de obtenidas las “credenciales” operaban sobre las cuentas intrusadas y obtenían los fondos.

Este segundo segmento de la actividad, ahora, es propio de los denominados “Logueros”, quienes más adelante serán identificados en forma concreta.

Como dijimos, la creación de un set de ingeniería social, por ejemplo uno de “phishing”, mediante la clonación de una página web, hoy por hoy es una actividad absolutamente independiente de toda la maniobra delictiva.

La creación de este set tiene un valor en sí mismo, y se negocia “per se” en el mercado negro de datos por parte de los “montadores de scams”.

Estas “credenciales” son adquiridas por otro grupo dentro de la cadena de valor, los denominados “Logueros”, los cuales justamente aportan su plusvalía mediante alguna actividad, como por ejemplo el “saldeo” de cuenta -actividad que también se comercia por separado-, o la obtención de información personal necesaria para lograr el fin (tokeneros=tokens, poseedores de “login's” para acceder a bases de datos personales públicas o

privadas), o inclusive quienes conocen los mecanismos propios de cada uno de los medios de pago páginas de retails, e-commerce en general, pagos de servicios públicos y privados, etc., a quienes ya veremos se le ha abierto un negocio independiente al que ellos denominan "metodistas".

Una de las importantes consecuencias de este crecimiento desmedido en la actividad criminal y de las estructuras a ellas dedicadas, es el fenómeno de la "segmentación", que es la resultante de la convergencia de variables socio-económicas que se dieron, fundamentalmente, con el avance tecnológico y los distintos aspectos que se dieron en la pandemia del COVID-19.

Las variables referidas son: la digitalización de los medios de pago, el boom del e-commerce, el escaso conocimiento de los usuarios en este nuevo escenario digital, la alta rentabilidad que ofrece la actividad criminal 4.0 y la falta de preparación en las fuerzas del orden en la comprensión y luego persecución de estos delitos; todo ello es un escenario propicio e ideal para este crecimiento.

Como se dijo, lo que antes sucedía en manos de un sólo actor/criminal o de un grupo muy reducido, demandó la aparición de sectores especializados, tendiendo a la especificidad de cada segmento del "iter criminis" como principio rector y directriz de esta especial actividad delictiva.

Es claro que quienes inicialmente dominaron este universo, son quienes hoy en la actualidad y en función de la variable "costo-beneficio" eligen tercerizar el aspecto más riesgoso del proceso delictivo.

Otra variable determinante y de mucho interés a analizar es la ecuación económica.

La incidencia de la misma ha determinado que quien más se aleja

del riesgo, menos recompensa tiene.

Pero claro está, que quienes tienen el conocimiento invierten a su favor este baremo.

¿Cómo lo hacen? tomando para sí y dentro de su estructura, actividades de sumo riesgo (vgr.: los "vaciadores de cuenta", de los que ya hablaremos más adelante), estructurando su unidad de negocio en forma piramidal, segmentaria, escindida y enclaustrada, en donde quienes operan una actividad no conocen la identidad de quien está por encima la estructura, sino sólo de quien los sigue en forma inmediata.

Esto opera de manera de cortafuegos en caso de que algún miembro de esta estructura sea objeto de una investigación penal.

Ejemplo más claro de lo recién explicado, es que un grueso de las investigaciones penales iniciadas contra estas organizaciones criminales, nunca superan el parámetro de cuentas de "nivel 1".

En definitiva, son el "firewall" de las actividades ilícitas.

**b. 2.- Nuevos actores**:


Como se dijo más arriba, la segmentación y especificación de actividades derivó en la necesidad y aparición de nuevos actores, en el universo de la actividad criminal 4.0, especialmente en el mercado negro de datos.

Como vemos, existe una atomización de actividades con un objetivo afín, y que en muchos casos se complementan, conformando de modo aleatorio alianzas transitorias, tendientes a completar el acto ilícito, a los que denominamos una “Comunidad de Negocios” .

Esta unión transitoria, desde el punto de vista técnico no deja de ser una asociación criminal, con el fin de ejecutar un número determinado -o no- de hechos o de actos ilícitos, pero que se necesitan inexorablemente para

lograr la finalidad.

La permanencia en el tiempo que reclama la figura típica está dada por la pertenencia a un “grupo” o “canal” para el cual deben haber pasado previamente por la aceptación de los administradores del mismos, y acatar las normas de convivencia que en general están fijadas por el “staff” (grupo administrador de la comunidad), comprar y vender sus servicios a sabiendas del fin con que serán empleados.

Por su parte, el mercado de venta de datos, reviste un carácter “abierto” para la incorporación de miembros que puedan ofrecer sus servicios por distintos medios, utilizando en especial aquellos que permiten el anonimato, pero que a la vez son de uso extendido y admiten que personas sin conocimientos específicos puedan incorporarse (vgr.: grupos de Telegram).

En este sentido, las particularidades brindadas por esta aplicación, entre otras, es la declamada falta de cooperación con fuerzas del orden a nivel mundial, la posibilidad de “anonimizar” la cuenta mediante el ocultamiento del abonado telefónico vinculado a la cuenta, la posibilidad de apertura de “Canales de difusión”, además de los grupos con que otras apps cuentan, todo lo cual son herramientas que han permitido en el último tiempo desplazar a las plataformas de navegación de la “dark net”, que otrora eran empleadas para el quehacer delictivo, por ésta, cuya interfaz resulta por demás amigable en comparación con la mencionada, que entre otras complejidades, demanda la necesidad de conocimientos básicos de programación para su correcto empleo, lo que minimiza el mercado cuantitativamente.-

Regresando a los operadores del sistema, al poco tiempo, estos nóveles ingresantes ganan en experiencia y conocimientos a pasos agigantados, de manera proporcional a los ingresos que generan, con la

diversidad y precisión de la oferta delictiva que subyace de dichos grupos, y que surge claro de las capturas que se acompañan.

Atendamos este caso, el cual luego será ampliamente analizado:



Veamos:

Como bien se observa en el "mensaje fijado" en este Canal de Telegram, uno de los cuales integra la "Comunidad de Negocios" que venimos describiendo, surge una serie de "rubros de actividades" que ameritan ser descriptas, no siendo éstas las únicas que se identificaron tras esta investigación, por el momento desconocidas, o al menos no identificadas en otras investigaciones penales a nivel nacional según hemos podido recabar en comunidades académicas, judiciales y del mundo TEC.

Entre ellos, tenemos a los:

1.- **Logueros y Montadores de Scams**

2.- **Vaciadores**

3.- **Carderos (carding)**

4.- **Salderos**

5.- **Metodistas**

6.- **Editores (Edit)**

7.- **Tokeros (Tokens)**

8.- **Dropers**

9.- **Rippers**

10.- **Pagos y recargas**

Para conocer este universo, es necesario describir en forma individual cada actividad:

**1.- Los Logueros y Montadores de Scams**:

Son de aquellos actores de los que se demandó originariamente un alto conocimiento técnico de las herramientas de programación, dado que éste es el paso inicial para toda la actividad de "ingeniería social" derivada que se precie de tal.

Eran personas que, entre otras actividades, clonaban códigos fuentes de sitios web para lograr suplantar la identidad de las reales, así como la generación de campañas masivas o dirigidas de mails, SMS, entre otros, para luego, en el caso de las "fake web pages", alojar las mismas, generalmente en servidores fuera del país donde van a ejecutar la maniobra.

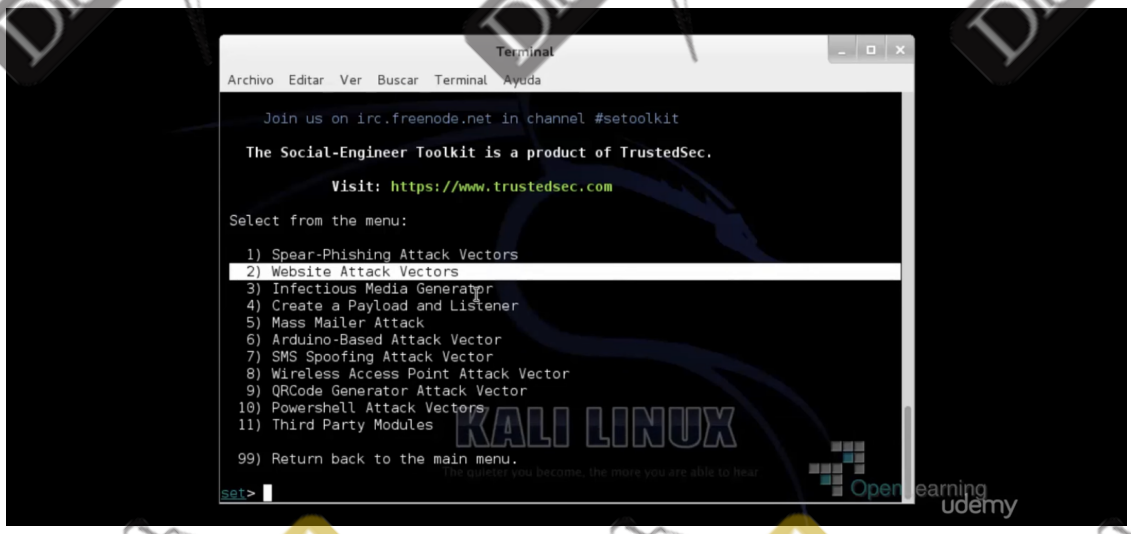
El segundo tramo de acción de estos sujetos es obtener "credenciales" de las personas o empresas a vulnerar.

En la actualidad, esta actividad ha ido mutando, inclusive escindiéndose internamente, generándose nichos, entre los que se identifican

los “montadores de scams” y quienes luego comercializan el mismo, los “Logueros” o vendedores de “Logos”-

La diversidad de herramientas disponibles, por ejemplo en “Kali Linux” (soft de código abierto diseñado para la ciencia forense digital), para ejecutar con relativa sencillez estos “scams” se ponen a mano de personas con relativos conocimientos la posibilidad de armar estos escenario de phishing, mediante herramientas como: Socialphish, Shell Phish; Hidden Eye, King Phisher, Set toolkits, entre otras, dentro de las cuales, inclusive se hallan preseteadas famosos web sites, entre ellos Google, Yahoo, Spotify, Linkedin, ello en el marco de lo que se denomina como “vectores de ataque a sitios web”, usando la opción de “recopilador de credenciales”.


De igual modo, muchas de ellas ofrecen opciones para generar, en el caso de emails, ataques del tipo “massive” (masivos) o “spear” (dirigidos a segmentos socioeconómicos definidos, o ataques más concretos como del tipo “whaling” -por ballena- dirigidos a CEOs o primeras líneas gubernamentales), en definitiva, con básicos conocimientos técnicos, tiempo y paciencia, cualquier persona de puede transformarse en un “scammer” de profesión.




Huelga decir a este respecto que los desarrolladores de estos softs enmarcan su creación en propósitos netamente académicos, forenses, educativos y de corte preventivo para instruir a personas y organizaciones sobre estas vulnerabilidades.

Continuando con lo que veníamos tratando, una vez desarrollado este primer tramo del engaño (scam), existe un segundo segmento que hemos detectado en la práctica que también se encuentra diversificado y comercializado como un valor independiente, que es el de venta de credenciales ya obtenidas (logos).

Ya sea, en forma completa o en forma escindida, esta actividad se ofrece en el mercado negro de datos bajo el nombre de “scams” o “logos”.

Relacionada con la presente investigación, los “Logueros” pueden obtener en forma indistinta, “credenciales” de home banking como también de Tarjetas de crédito o débito, dependiendo la página a clonar y la finalidad.-

Vale aclarar que el mote de “logueros” vienen directamente de los “logos”, ello en directa relación a la representación gráfica de la marca de la

empresa a la que clonan su página.

Esta actividad puntual es la de menor riesgo dentro del esquema delictivo 4.0, dado que resulta distante del resultado final de la maniobra.

Sin perjuicio de ello, claramente es una acción punible desde el momento que hay un conocimiento y una voluntad de llevar adelante una maniobra delictiva conocida.

No obstante, aún cuando aparezca poco rentable, frente a otros tramos de actividad, lo cierto es que ello no resulta tan así, dado que el volumen de datos que manejan y el sobredimensionamiento actual del mercado en este momento proponen la generación de sustanciosas ganancias por su venta a granel.

En la actualidad, los precios de los logos guardan estricta relación con el saldo de cuenta de las credenciales obtenidas, siendo que la medida, en términos generales, puede calcularse en un 10% del monto contenido en la cuenta. Es decir, una cuenta con $150.000 se puede vender en $15.000.


**2.- Vaciadores:**

El segmento de los vaciadores de cuentas resulta de aquellos más rentables, pero a la vez más riesgosos.

Se da en general mediante dos metodologías, una, el vaciado de cuentas mediante diversificación de fondos en cuentas “mulas”, o mediante el pago de servicios a terceros (metodología que se explicará por separado más abajo).

Son los encargados de adquirir credenciales ya obtenidas previamente por los “logueros” de cuentas bancarias, para luego vaciar las mismas.-


Como se dijo, en el caso de cuentas de Homebanking, ejecutan la maniobra de extracción de los fondos de la cuenta atacada mediante la diversificación del dinero en cuentas mula en sus diversos niveles (1, 2, 3)

para ocultar su rastro, intercambiando las acreditaciones de diversas estafas de modo “random” con el propósito de generar confusión y evitar la retroversión del pago por parte de entidad bancaria. Ello ocurre en general en su faz más profesionalizada .

También son aquellos que al ingresar a los homebanking pueden obtener los préstamos preacordados y con esos montos girarlos a cuentas de terceros.

Nos ha demostrado la experiencia que el riesgo para sus cabecillas ha sido conminado por éstos mediante la interposición de diversas cuentas alternativas de distintos niveles -como previamente hemos señalado-, mediante las cuales hacen un juego de traspaso de fondos pretendiendo ocultar el origen, enmascarándolo dentro de eventuales movimientos lícitos de terceras personas, que por el principio de “buena fé comercial” -entre otras regulaciones-, impiden a las entidades financiaras “freezar” los mismos o revertir la maniobra.

Para lograr ésto, rara vez los montos transferidos entre cuentas de diversos niveles resulta idéntico, abonando con ello la posibilidad de ocultar de modo más efectivo la maniobra.

De igual manera, en la inteligencia de ocultar los fondos, han utilizado terceros ajenos al conocimiento de la maniobra, como en el caso de “traders” de criptomonedas, a quienes giran directamente a sus cuentas bancarias fondos bajo el engaño de la adquisición de activos digitales, para luego, una vez convertidos, hacerse de ellos.

Esta mecánica es conocida en la jerga como “rulo”, el cual además tienen otras formas más complejas de comisión.

Sucede también muchas veces que estas personas dedicadas al

“arbitraje” de cripto activos lo hacen a conciencia de que se trata de dinero proveniente de una actividad ilícita previa, ingresando de este modo en el esquema delictivo.

Tiempo atrás, la obtención de cuentas bancarias utilizadas como mulas de primer nivel, se producía mediante el engaño a personas que no participaban ni conocían de la ultrafinalidad de la maniobra, proponiéndolas como una actividad comercial alternativa (el alquiler, venta o inclusive préstamo de una cuenta bancaria), pero con la difusión y el alcance que durante la pandemia tuvo esta actividad, pocos pueden ser al día de hoy quienes desconozcan que están participando de estas metodologías, entendiendo que la justificación no es más que aceptar una suerte de “desconocimiento deliberado”, punible por cierto.

Por ello es que en la actualidad, quienes lo hacen son sometidos a un proceso penal.

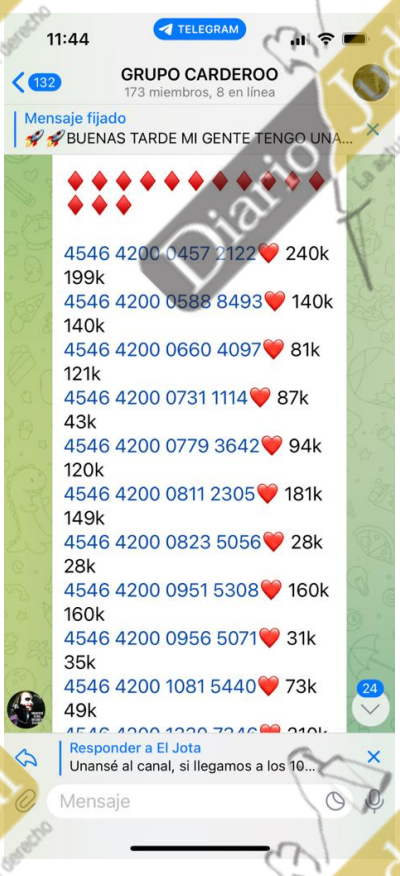
Como se dijo, las mulas tienen distintos niveles y de ahí el sobredimensionamiento de este segmento (vaciadores de cuentas) cuyas cabezas arman una estructura enclaustrada que los protege del conocimiento del eslabón más débil (mulas), incorporando como segmentos intermedios, no solamente mulas de segundo y tercer nivel, sino también otros operadores interpósitos, como los “reclutadores de cuentas” mula, e inclusive en las más sofisticadas que hemos visto la creación de un puesto intermedio que ellos denominan “coordinadores” de estos reclutadores, que son los únicos que conocen la verdadera identidad del jefe de la banda y los vaciadores.

Claro está que en aras de mantener su lejanía con la maniobra riesgosa, los mecanismos de comunicación empleados son del tipo de mensajería instantánea renuentes a colaborar con las fuerzas del orden (entre

ellos Telegram, Signal, Line, etc.), utilizando nicks que ocultan su identidad en los grupos en los que ellos interactúan, ocultando los números de abonado de registro una vez instalada en los dispositivos móviles dichas apps, de modo de dificulta su vinculación a la información de registro.

**3.- Carderos (Carding)**:

Esta actividad está reservada a quienes negocian tarjetas de crédito y débito obtenidas mediante "scams", "generación" o "bases de datos" sustraídas.


En el primer caso, el método empleado es el descripto para los "Logueros", es decir, la creación mediante "clonación" de una página web

copiada de alguna entidad u organismo, en este caso, que demande la necesidad de introducir las credenciales de tarjetas de crédito o débito, y luego esa información reconducida al administrador de esa página "fake" sin que su usuario siquiera perciba lo que acaba de ocurrir.

Estos datos "per se" son de suficiente entidad y cantidad que forman un nicho de negocios diferenciados que permiten ser vendidos a granel y así obtener, sin mayores riesgos, gruesos beneficios patrimoniales.

A diferencia de los logueros, la actividad del "carding" tiene cierta complejidad que demanda de la ayuda de otros nichos de negocios dentro de estas comunidades para hacerlos efectivos, entre ellos, los "Edit", los "salderos" y los "metodistas", sin los cuales la mecánica iría al fracaso en forma inexorable como veremos.

Los "Generadores" son aquellos que crean mediante herramientas dedicadas, tarjetas de crédito virtuales válidas que se emplean en general para activar servicios, pero no sirven para acreditar pagos. También son aquellos que engañan a los estafadores simulando vender tarjetas para realizar compras espurias, pero en realidad, ellas nunca serán operativas porque no se encuentran vinculadas a una cuenta real.

También están los "Carboneros", que son aquellos que se dedican a la venta de tarjetas "quemadas", en la mayoría de los casos, empleada para estafar a recién iniciados en estas comunidades delictivas.-

**4.- Salderos:**

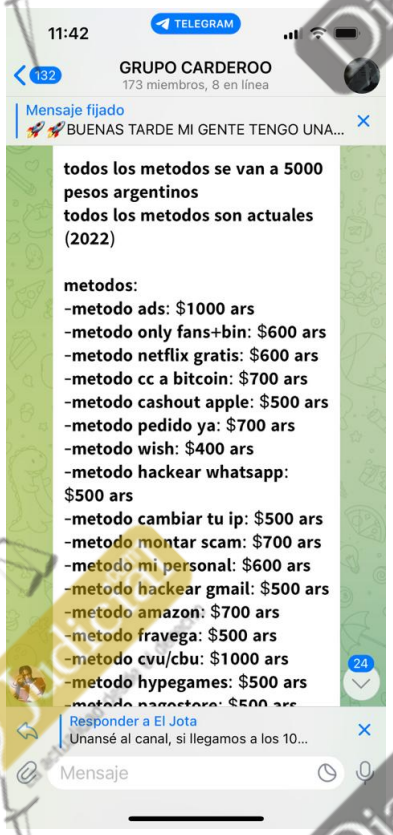
Las actividades y oferta brindada por este segmento se reduce al chequeo de saldos de las tarjetas previa su utilización. Esta actividad es de riesgo medio por la factibilidad de traceo de su operatoria, y resulta de suma

necesidad para completar las compras, atendiendo a los filtros y las alertas de los operadores del sistema ante intentos reiterados de compras fallidas, o los montos que se pretenden ingresar atendiendo a los saldos existentes y en especial al perfil histórico del cliente.-

Como se dijo, son suma importancia para que la compra intentada sea efectiva, existiendo en este sentido un conocimiento necesario para evitar controles automáticos que cada tarjeta tiene preseteada ante compras con determinadas características, en especial por su monto en relación a su límite y saldo.-

**5.- Metodistas:**

El servicio brindado por este segmento de la cadena de valor resulta de sustancial importancia, y radica en la venta de los mecanismos o "know how" para arribar a una compra efectiva y libre de riesgos, o al pago de un servicio.


Efectivamente, esta actividad implica la detección de brechas de seguridad que los organismos públicos/privados y compañías presentan en su oferta pública comercial en redes, en especial, en sus segmentos de verificación de identidad y pagos.

Existe una ecuación comercial que estos ciber traficantes de información aprovechan en su beneficio, que es conocida en la jerga comercial como “fricción cliente”, que no es otra cosa que el índice de aceptación o rechazo del cliente y su consecuente fidelización con la compra o el pago, dependiente de los “obstáculos” que cada organismos o empresas impone para concretarlo, en especial en punto a la verificación de identidad.

Mientras más riguroso, más distante está la concreción de la operación y viceversa.

La actividad de los "Metodistas" es dinámica dado que en forma permanente organismos y empresas detectan estas brechas y las enmiendan, surgiendo nuevas que son vendidas como conocimiento novedoso para sortear estos "firewalls".

En general, se venden en forma de tutoriales y son necesarias (aunque imprescindibles), por ejemplo para comprar con tarjetas sustraídas en retails de todo tipo, en especial de electrodomésticos e indumentaria, pero también para el pago de servicios de streaming e impuestos.

**6.- Editores**:

El segmento de los Editores es de particular importancia para arribar al resultado que los ciberdelincuentes pretenden.

En efecto, su trabajo estriba en "Editar" documentación y tarjetas modificando su contenido en forma parcial o integral para hacerlos pasar por instrumentos de identificación y pagos reales.

¿Para qué se necesitan? Las páginas de pago de servicios y retails de compras digitales, entre los reaseguros que proponen para evitar sustituciones de identidad, introducen la acreditación de estos extremos mediante envío adjunto de fotos o scanneos de estos instrumentos adjuntos a la compra.

Según el monto de compra en general (a más elevado, mayores restricciones), dichas organizaciones requieren en mayor medida que el supuesto cliente acredite su identidad mediante este precario medio, cuya efectividad, como será demostrada más adelante, carece de todo sentido, más que el de la apariencia de seguridad que pretende generar a sus clientes, cuando en rigor de verdad, sólo es un escollo menor para los ciberdelincuentes, quienes echan mano a sus asistentes, los editores, para modificar a su gusto y antojo, con herramientas, en algunos casos sin mayores pretensiones (ej. Photoshop) y crean documentos de apariencia real para sortear esta débil medida de seguridad.

Este servicio a gran escala se comercia por separado dado el tiempo que insume confeccionar instrumentos creíbles.-

**7.- Tokeros (Tokens):**

Dentro de este segmento navegan actores de sustancial importancia para la concesión de la estafas.

Son quienes aportan los datos personales y financieros de las víctimas de los "scams", tanto para concretar un "login" exitoso en una apps, para conformar una C.C. válida, para la edición de documentos, para sortear los reaseguros en la compra en retails o pagos de servicios, entre otros usos. ¿En qué consiste su aporte? Ellos son quienes han obtenido de modo irregular

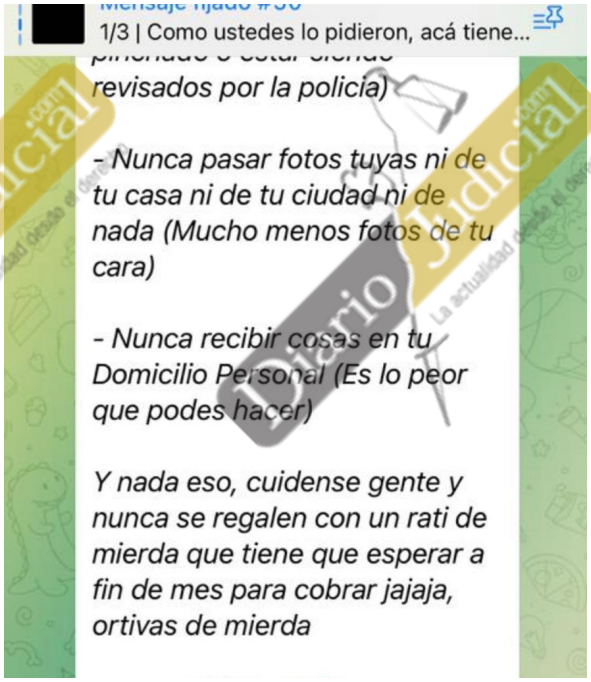
"tokens" de acceso a diversas bases de datos públicas o privadas de información personal sensible.

Estas base pueden ser pagas o no, públicas o privadas, y en casos más extremos, de aquellas con información ultra sensible.

Entre ellas se ofrecen, por ejemplo, accesos a bases policiales, judiciales, de registros personales y de Salud.

**8.- Dropers:**

Este nicho colaborativo, nació a la sombra de la necesidad de completar el tramo final de las compras de bienes físicos con tarjeta de crédito.




Son, al igual que las mulas, el eslabón más expuesto de la cadena de scams, o estafas por medios tecnológicos, puesto que son quienes aportan una dirección postal física donde la compra espuria llega por medio del correo elegido.

Dicha dirección, claro, queda en el registro de la página del retail de modo que es accesible.

No obstante, este servicio es ofrecido en los grupos de venta de

servicio para cometer estafas digitales, siendo de los más buscados, dado que sin ellos, quien opera detrás de la identidad falsa queda expuesto en una investigación penal.

Se ha detectado un grado de profesionalización importante de este nicho, al punto de alquilar viviendas al solo efecto.

**9.- Ripers:**

Este término es empleado en la jerga, para quienes, dentro de un grupo de servicios dedicados a las estafas, operan contra los mismos integrantes del grupo vendiendo servicios apócrifos y comprado otros sin pagar el costo.

**10.- Pagos y recargas:**

Este servicio implica la utilización de tarjetas de crédito o débito adquiridas en forma fraudulenta, que son empleadas para pagar en general servicios públicos y privados, impuestos, Tasas y Contribuciones de todo tipo.-

La mecánica consiste en que el cliente aporta el servicio que quiere pagar, cuya deuda es oblada en forma completa mediante este medio de pago espurio, mientras que el cliente abona al “scammer” sólo el 50% (a veces 40% o 30% dependiente de los movimientos del mercado) de la deuda original.-


Claro, este pago lo puede hacer mediante dos formas previamente explicadas, es decir mediante la compra de “logos” de homebanking, haciendo transferencias desde allí, o mediante el pago con tarjetas de crédito o débito del segmento del “carding” antes descripto.-