

CIBERSEGURIDAD III

NOTI 297 – Marzo de 2020

Los criminales compran:

- Datos personales.
- Datos financieros.
- Guías de acceso.
- Software y servicios fraudulentos.
- Evaluación de información.

¿Qué compran los criminales?

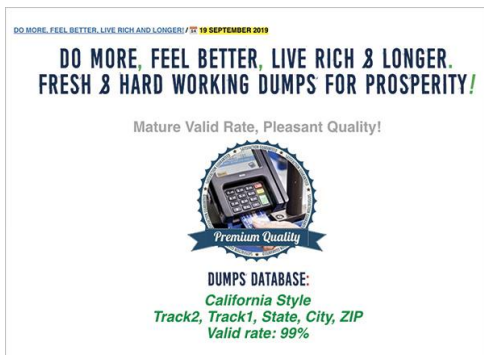
Después de las drogas, la información obtenida de manera fraudulenta es la más popular entre los usuarios de este siniestro negocio. Dicha información se agrupa en cinco categorías:

- **Datos personales:** la economía de la Web Oscura está construida sobre información confidencial expuesta o hurtada, y el flujo constante de brechas de seguridad y hackeos han contribuido a la proliferación de información personal en los mercados del ramo. Los vendedores ofrecen de todo, desde cuentas de plataformas de música, pasando por información crediticia, historiales clínicos hasta paquetes completos de identidad personal e información financiera. Algunos incluso hacen pública

información personal para ser usada "gratis". Listas de usuarios y claves, direcciones de e-mail y otra información de contacto navega libremente en la Web. Los usuarios re empacan y mercadean esta información, generando otro tipo de fraude: vender información confidencial que ya es de dominio público.

- **Datos financieros:** usualmente aparece como información de tarjetas débito/crédito, información bancaria o bonos de combustible o mercado. A diferencia de la información personal, este tipo de información casi nunca se ofrece gratis. La información personal identificable les permite a los defraudadores la ejecución continua de una variedad de fraudes que a veces toman largos períodos de tiempo, mientras que la información financiera abre las puertas para obtener dinero de inmediato. Las cuentas bancarias son casi siempre bloqueadas luego de la primera transacción fraudulenta. Los vendedores retienen el dato del número de tarjeta que están ofreciendo hasta que el cliente paga por la información; si no es que él mismo la utiliza antes de venderla a un incauto comprador.

Uno de los éxitos del cibercrimen es que las personas no son cuidadosas con el manejo de su información.



Ejemplo de aviso de oferta en la Web Oscura de tarjetas de crédito hurtadas.

Los bonos de combustible y similares permiten en cambio a los defraudadores el lavado de dinero o el pago de otras actividades.

- **Guías de acceso:** los mercados de la Web Oscura van mucho más allá de ofrecer simplemente información personal o detalles financieros para la venta. Los comerciantes de esta red también ofrecen manuales y guías para facilitar la comisión de fraudes. Estas guías contienen paquetes de instrucciones detalladas para los defraudadores principiantes, en delitos como Phishing, apoderamiento de cuentas, hackeo de emails corporativos, fraude fiscal y cómo obtener dinero de tarjetas de crédito o débito hurtadas.

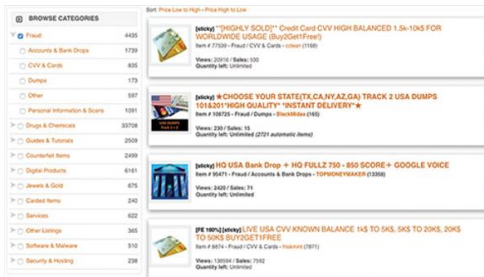
Estas guías se asemejan a recetarios para el uso de la comunidad de defraudadores, ya que ofrecen listas de insumos necesarios, instrucciones y consejos de los autores para lograr los mejores resultados posibles. Si bien algunas de estas guías ofrecen solo información técnica, otras abundan en detalles acerca de cómo utilizar las redes sociales, cómo hablar de manera convincente con representantes de servicio al cliente, gerentes, cajeros de banco y otras personas con quienes será necesario interactuar en el curso de la materialización de un fraude.

- **Software y servicios fraudulentos:** este software ofrecido no tiene que ser necesariamente ilegal, pero que puede ser utilizado para efectos ilícitos, como el Adobe Photoshop para la adulteración de documentos legales.

Los delincuentes que usan el método de Phishing (extracción de información mediante engaño) compran páginas web previamente elaboradas para convencer a sus víctimas de que están visitando páginas legítimas. Dichas páginas falsas vienen cargadas con la tecnología que se usa para capturar información de los incautos que las visitan.

Incluso, algunos de estos vendedores ofrecen este tipo de servicios como una "cortesía" a los compradores de sus bases de datos obtenidas de forma ilegal. Ello con el propósito de ganar confianza entre sus clientes.

Otros ofrecen servicios no relacionados, pero igualmente fraudulentos, como copias de documentos debidamente impresos en máquinas de alta calidad.



Un ejemplo de oferta de productos y servicios fraudulentos en la Web oscura

Por: Alejandro Morales, Gerente General, ASR S.A.S.

Carrera 43B N° 16-41
Medellín, Colombia
+57 4 266 33 42
asr@asr.com.co
<http://www.asr.com.co/>

• **Evaluación de información:** todos los bienes y servicios transados en estas plataformas delictivas refuerzan el crecimiento y estabilidad de la economía de la Web Oscura. La mayoría de los movimientos se fundamenta y nutre de la existencia de información personal vulnerada y apropiada de forma ilegal, constituyéndose en la materia prima más importante para el delito. Este hecho modifica la forma como los defraudadores ven y valoran la información sensible que cae en sus manos. Esta valoración puede ser por su valor intrínseco de monetización (como las tarjetas débito y crédito), o por su poder para abrir puertas en varias plataformas (como los números de cédula, password o códigos de acceso) lo que permite a los defraudadores intentar sus acciones criminales en una variada gama de situaciones a partir de este simple dato.

Las organizaciones se preocupan más por proteger su información financiera, secretos industriales, o actividades de compra o fusión con otras empresas. En cambio, los

defraudadores buscan con mayor interés datos aparentemente masivos e inocuos, como datos de los empleados, de los clientes, perfiles de sus ejecutivos y números de cuentas bancarias y otros productos financieros.

El futuro del fraude

Los defraudadores siempre han hecho uso de los desarrollos tecnológicos como un medio de desarrollar formas rápidas y eficientes de fraude. La Web Oscura no tiene porqué ser diferente, ya que es solo otro componente de Internet, que es una herramienta que creó un acceso más amplio a la información de todo tipo. No todos comprendemos que la información es el activo más valioso que existe en las economías comerciales, y que esa misma información que utilizamos para realizar las transacciones legítimas está siendo utilizada paralelamente, a gran escala, en los círculos del crimen cibernético.

Mientras que estos mercados oscuros resultan poco familiares para la mayoría de las personas, sus resultados de pesadilla aparecen de vez en cuando: los defraudadores siguen accediendo fácilmente a cuentas y servicios, suplantando nuestra identidad para su propio beneficio. Estas personas cuentan con una amplia gama de recursos técnicos y de acceso a información, lo que les permite operar a gran escala, sin herir físicamente a nadie y con muy escasas probabilidades de ser detectados, menos de ir a juicio o a la cárcel por sus acciones delictivas. Lo que más preocupa es que sus métodos cambian poco en esencia o en ejecución, siendo tan solo actualizaciones de las primeras versiones de los mismos. La razón de su éxito es simple: las personas no son cuidadosas con el manejo de su información; y en muchos casos

la codicia o la estupidez las lleva a dejarse tentar por ofertas imposibles de beneficios que no se han ganado, tratamientos preferenciales sin justificación o el deseo de obtener utilidades relámpago por negocios sin ningún sustento en la realidad.

asr@asr.com.co