Dark web: qué productos y servicios ofrecen los cibercriminales

Servicios de hacking, alquiler de botnets, lavado de criptodivisas, así como venta de exploits, servidores e información, ESET Latinoamérica analiza los productos y servicios que ofrecen los cibercriminales en la dark web.

Buenos Aires, 21 de abril de 2020 – Las estructuras cibercriminales son cada vez más complejas y la industria del cibercrimen es una de las que más rápido está creciendo. ESET Latinoamérica, compañía líder en la detección proactiva de amenazas, realizó un análisis sobre precios y productos en la dark web con información actualizada y nuevos servicios, como servicios de hacking, venta de exploits o lavado de criptodivisas, para comprender cómo funciona el negocio del cibercrimen y cuáles son las cifras que manejan.

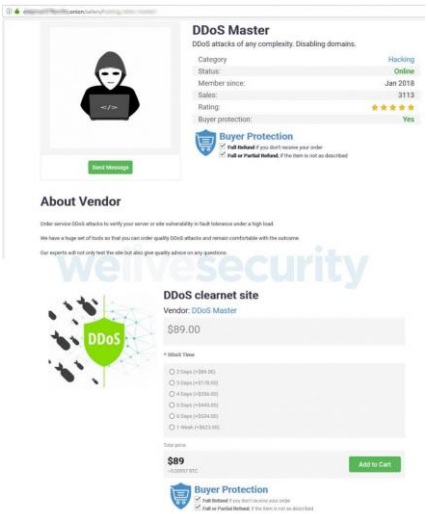
Un grupo cibercriminal está conformado por al menos 10 personas, cada una de ellas con diferentes roles y tareas. Están los desarrolladores de malware, que se encargan de programar los códigos maliciosos, empaquetarlos y aplicar diferentes técnicas para lograr evadir la detección de los antivirus, los spammers, que se ocupan de la cadena de distribución, el equipo de infraestructura, que brindan soporte para que los servidores y las redes que utiliza el grupo permanezcan anónimas y operativas. Por otro lado, el equipo financiero que cobra el dinero por los servicios y productos ofrecidos, y las mulas, que permiten que el dinero recaudado llegue finalmente a los delincuentes. Según una investigación del FBI, en muchos casos las mulas son reclutadas mediante falsos avisos con promesas de trabajo online, puestos como agentes de pagos y transferencias, avisos que prometen ganar dinero navegando en Internet o cualquier otro anuncio que implique mover dinero y ganar una comisión. "**En este sentido, es sumamente importante estar alerta y no creer en estos falsos anuncios ni aceptar transferencias de dinero de personas desconocidas**.", resalta Camilo Gutiérrez, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

Las mayores ganancias de estos grupos organizados provienen de la venta de productos y servicios en la dark web, como son:

Servicios de Hacking: Los atacantes se promocionan destacando sus habilidades técnicas y conocimientos en diferentes lenguajes de programación. Ostentan tener acceso a exploits zero-day y todo tipo de técnicas para cometer un ataque informático. El acceso ilegal a sitios web o una organización, el precio varía dependiendo la arquitectura del sitio y de la organización. También, los cibercriminales ofrecen cambiar las notas de un alumno o el acceso a un teléfono móvil que es un poco más económico, así como el acceso al correo electrónico y redes sociales. La mayoría de los atacantes ofrecen trabajos personalizados, cuyo valor dependerá de la complejidad, alrededor de 250 euros la hora. De hecho, si el problema a resolver es urgente, se ofrece un servicio Premium que garantiza una respuesta en 30 minutos.

Alquiler de Botnets y ataques DDoS: Se identificaron ofertas de ataques de denegación de servicios llevados a cabo mediante grandes botnets distribuidas. Por ejemplo, el vendedor "DDoS Master" ofrece dejar sin servicio un sitio web desde 89 dólares por 2 días y hasta 1 semana por $623. Además, en el sitio se pueden ver comentarios y la reputación de este vendedor, aunque teniendo en cuenta que se trata de negocios ilegales, esta reputación es dudosa. Por otro lado, se puede adquirir un paquete para el armado

de una botnet propia, que incluye el panel de control, el builder y los plugins para control remoto. Además, el servicio incluye manual de instrucciones, soporte y actualizaciones.



Pie de imagen: Servicios de DDoS

Venta de Exploits en la dark web: Existen bases de datos con todo tipo de exploits. Algunas pueden descargarse gratis es probable que sean para vulnerabilidades ya corregidas y también se encuentran algunos más críticos entre 0.1 y 0.5 Bitcoins. Se identificaron además exploits para vulnerabilidades zero-day, aunque es necesario realizar un depósito para poder ingresar a esta área restringida. Si bien este dinero queda como crédito, lo cierto es que muchos de los exploits en esta sección probablemente sean aún más caros.

Imagen 2: Zona restringida de venta de 0days

ENJOY SAFER TECHNOLOGY™

Venta de Servidores e información: Los cibercriminales también comercializan servidores comprometidos e información de usuarios que han logrado robar. Se ofrecen servidores de cualquier país del mundo, al cual el comprador puede acceder por escritorio remoto y controlar como prefiera. Estos servidores se venden principalmente para ser utilizados para realizar ataques, guardar información ilegal temporalmente, o simplemente para realizar actividades sin dejar rastro.

Hasta fines del año pasado había en este portal casi 2.500 servidores de Brasil ofrecidos, más de 500 de Argentina, 330 en México y 250 de Colombia. Los precios rondan los 10 a 12 dólares por servidor, aunque pueden llegar a valer 15 dólares cuando el equipo cuenta con más recursos y un sistema operativo más actualizado. La mayoría de los equipos comprometidos tienen Windows Server 2008 y Windows 7, dos sistemas operativos casi obsoletos y con conocidos fallos de seguridad.

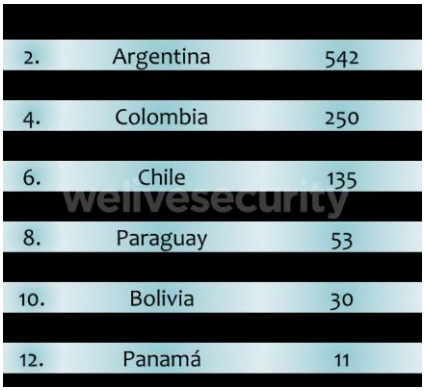


Imagen 3: Servidores en Latinoamérica ofertados en el mercado negro

Además, se vende información de personas físicas, se puede adquirir una nueva identidad que incluye correo electrónico, contraseña, dirección, documento de identidad y hasta números de seguro social o empadronamiento. También se venden cuentas de Amazon, Paypal y otros servicios de pago online por un valor aproximado del 10% del saldo disponible en la cuenta. Asimismo, se comercializan las tarjetas de débito y crédito obtenidas a través de engaños como el Phishing. Por último, además de la información robada también se ofrecen servicios de Ingeniería Social con el fin de obtener, por ejemplo, acceso a cuentas de redes sociales.

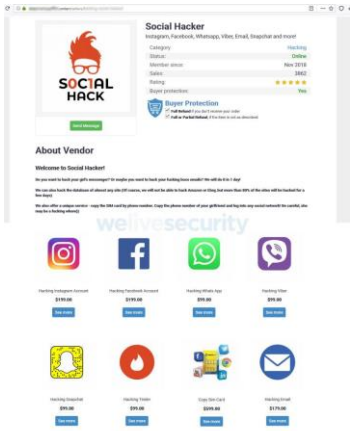


Imagen 4: Servicios de Phishing para obtener cuentas de redes sociales

Servicios Financieros y lavado de criptodivisas: Los servicios de lavado de Bitcoin, también llamados Bitcoin Mixers, son cada vez más populares. El mecanismo es muy sencillo, dado que la cadena de bloques que almacena las transacciones en bitcoins es publica y rastreable, se ofrece realizar numerosas pequeñas transacciones entre el dinero "sucio" y dinero "limpio" de sus reservas. De esta manera se pierde la trazabilidad y continuidad de las transacciones, logrando mayor privacidad y dificultando el rastreo del dinero.

Imagen 5: Servicio de lavado de Bitcoins

En estas últimas semanas, la preocupación mundial que provocó el nuevo coronavirus fue aprovechada por todo tipo de cibercriminales, quienes comenzaron a realizar campañas de todo distinta naturaleza intentando aprovechar esta situación para su beneficio. "*Si bien los operadores detrás del ransomware Maze comunicaban que durante la pandemia no atacarían a instituciones de la salud, otros tipos de ransomware, como Ryuk, continuaron apuntando a hospitales. Esta visión dividida también se puede ver en los foros de la dark web, donde algunos usuarios ofrecen datos y documentos relacionados al COVID-19 y consultan cómo aprovecharse de esta situación para ganar dinero; mientras que otros, a diferencia de lo que uno podría imaginarse en este tipo de sitios, proponen donar un porcentaje de sus ganancias para ayudar a quienes más lo necesitan*.", comenta Gutiérrez.

Algunos usuarios ofrecen supuesta información robada y confidencial respecto al virus y la pandemia.

Imagen 6. usuarios ofrecen supuesta información confidencial y documentos relacionadas al COVID-19

"El cibercrimen es hoy una industria millonaria en expansión y es algo que tanto empresas como usuarios finales deben tener en cuenta. Hoy en día la información de cualquier individuo tiene valor y es comercializada en el mercado negro, así como también la de grandes empresas. Conocer la industria del cibercrimen y el modo en que se manejan estos grupos criminales permite ser más conscientes del accionar malicioso y así mejorar las herramientas de protección. Hoy en día cualquiera puede ser víctima de un ataque informático o una infección de malware, por lo que contar con las medidas de seguridad básicas como un antivirus, doble factor de autenticación y los dispositivos actualizados es imprescindible.", concluye el Jefe del Laboratorio de Investigación de ESET Latinoamérica.

En el contexto de aislamiento por el COVID-19, ESET comparte #MejorQuedateEnTuCasa, donde acerca protección para los dispositivos y contenidos que ayudan a aprovechar los días en casa y garantizar la seguridad de los más chicos mientras se divierten online. El mismo incluye: **90 días gratis de ESET INTERNET SECURITY** para asegurar todos los dispositivos del hogar, una **Guía de Teletrabajo**, con buenas prácticas para trabajar desde el hogar sin riesgos, **Academia ESET**, para acceder a cursos online que ayudan a sacar el mayor provecho de la tecnología y **Digipadres**, para leer consejos sobre cómo acompañar y proteger a los niños en la Web.

De manera de conocer más sobre seguridad informática ingrese al portal de noticias de ESET: https://www.welivesecurity.com/la-es/2020/04/17/dark-web-productos-servicios-ofrecen-cibercriminales/

Visítanos en: @ESETLA /company/eset-latinoamerica

Acerca de ESET

Desde 1987, ESET® desarrolla soluciones de seguridad que ayudan a más de 100 millones de usuarios a disfrutar la tecnología de forma segura. Su portfolio de soluciones ofrece a las empresas y consumidores de todo el mundo un equilibrio perfecto entre rendimiento y protección proactiva. La empresa cuenta con una red global de ventas que abarca 180 países y tiene oficinas en Bratislava, San Diego, Singapur, Buenos Aires, México DF y San Pablo. Para obtener más información, visite www.eset-la.com o síganos en LinkedIn, Facebook y Twitter.

Datos de Contacto de Comunicación y Prensa

Para más información se puede poner en contacto a través de prensa@eset-la.com o al +54 11 2150-3700. Además, puede visitar "Somos ESET" nuestro Blog de Comunicación de ESET con las últimas novedades, disponible en: https://www.somoseset.com/

Copyright © 1992 – 2020. Todos los derechos reservados. ESET y NOD32 son marcas registradas de ESET. Otros nombres y marcas son marcas registradas de sus respectivas empresas.

ENJOY SAFER TECHNOLOGY™