Cuando la economía criminal capitaliza el crimen como servicio

Las herramientas de ataque cibernético se venden a diario en la Dark Web. Éstos son algunos de esos servicios comunes que se pueden obtener fácilmente por unos pocos cientos de dólares. Las empresas deben ser conscientes de esto. Desde los albores de los tiempos, ciudadanos, empresas y gobiernos han aprovechado los avances tecnológicos para desarrollarse y prosperar. Y siempre, los criminales han hecho lo mismo.

En los últimos años, los proyectos de transformación digital han abierto nuevas oportunidades para los delincuentes que buscan crecer y prosperar en la actividad ilegal de su elección. Estos delincuentes a menudo pueden aprovechar las capacidades avanzadas con mayor facilidad y velocidad que las empresas legítimas porque no operan dentro de los mismos límites y restricciones. No están regulados ni gobernados, pero a menudo están bien financiados y coordinados porque, aunque sus métodos son modernos, no operan en una economía criminal nueva o aislada.

Mientras las empresas honestas lidian con una crisis de habilidades, uno se pregunta cómo los grupos criminales establecidos han podido llegar a ser tan exitosos tecnológicamente. La respuesta corta es que no lo hicieron.

CaaS Crimen como servicio

La transformación digital de nuestra sociedad ha presentado nuevas formas de realizar actividades delictivas ancestrales

(como el blanqueo de capitales),dinero y robo), y la escasez de habilidades necesarias para hacerlo ha dado lugar a Crime-as-a-Service (CaaS). CaaS es un modelo en el que los ciberdelincuentes experimentados y capacitados construyen y desarrollan herramientas, plataformas y dispositivos sofisticados, y luego los venden o alquilan a otros delincuentes que carecen del conocimiento técnico para crearlos ellos mismos.

CaaS proporciona a los operadores capacitados fondos de delincuentes establecidos y, a cambio, los grupos criminales pueden desarrollar sus habilidades de forma rápida y sencilla. CaaS está impulsando el volumen y la sofisticación de los ataques en el panorama de amenazas actual, y la barrera de entrada al ciberdelito y la economía ilegal está disminuyendo.

La mayoría de nosotros no pasamos mucho tiempo en la Dark Web, y puede parecer increíble hablar de las herramientas de un ciberataque que se venden a los delincuentes a diario. Sin embargo, eso es exactamente lo que está sucediendo. Estos son algunos de los servicios comunes que se pueden obtener fácilmente como CaaS.

Plataformas / kits de phishing

El [phishing es uno de los principales vectores de ataque para comprometer las empresas, por lo que no es sorprendente que estas técnicas se hayan convertido en herramientas estándar.] Los kits y plataformas de phishing están disponibles en la Dark Web por tan solo $ 2-10 para facilitar el ataque a una empresa. Estos kits y plataformas se pueden personalizar con pocos conocimientos o habilidades y cuentan con diferentes niveles de automatización, lo que los hace muy atractivos para los delincuentes.

Kits de explotación

Estos kits incluyen el desarrollo de código de explotación y herramientas para explotar vulnerabilidades conocidas. Uno de los kits más populares, RIG, cuyo uso cuesta solo $ 150 por semana, propaga ransomware, troyanos y otras formas de malware. Tiene una extensa red de distribuidores cuya compleja estructura empresarial la hace accesible y asequible para los delincuentes. Afortunadamente, debido al aumento de las actualizaciones automáticas del navegador y la reducción en el

uso de Flash, los kits de explotación se han vuelto menos comunes desde 2016.

Servicios DDoS

Un grupo delictivo ya no necesita crear una botnet para lanzar un ataque a un objetivo. Hoy, pueden contratar estos servicios bajo demanda. El tiempo necesario para lanzar un ataque es mínimo y la infraestructura se puede configurar y desmontar de forma rápida y eficaz, lo que dificulta la supervisión y la prevención. Los servicios DDoS también son económicos y accesibles, y muchos proveedores ofrecen planes de suscripción en la Dark Web.

Los ejemplos incluyen una lista de fórmulas, la más barata de las cuales es de 4 euros al mes con un ataque simultáneo a un intervalo de 300 segundos, hasta la fórmula más grande y cara, a 50 euros al mes, con un ataque simultáneo en un intervalo. de 10,800 segundos. Otros proveedores participan en ataques de denegación de servicio (DDoS) en servidores o sitios web que usan protección, cobrando alrededor de $ 330 por día, algunos incluso proponen ataques contra objetivos gubernamentales. Todo esto hace que los servicios DDoS sean particularmente peligrosos debido a la facilidad con la que se pueden realizar y las ganancias que pueden generar para los delincuentes, y algunas estimaciones suponen márgenes del 95% por ataque.

Ransomware como servicio

Al igual que con los servicios DDoS, los ciberdelincuentes pueden utilizar servicios de ransomware diseñados específicamente para atacar a una víctima, lo que elimina la necesidad de una gran cantidad de conocimientos técnicos. Estos servicios no solo brindan la profundidad y las habilidades técnicas, sino también toda la información necesaria para completar con éxito un ataque. En algunos casos, también proporcionarán un panel e informarán sobre su

estado.

Ransomware as a Service ofrece una cantidad variable de precios y modelos de pago, algunos de los cuales se basan en suscripción, plan o participación en las ganancias. Las cantidades pueden ser tan bajas como 33 euros y pueden llegar a miles de euros para grandes objetivos. Investigación como servicio Esto implica la recopilación legal o ilegal de información sobre las víctimas objetivo, así como la reventa de datos personales robados, como credenciales comprometidas (Tendencias globales en seguridad cibernética, 2019). También puede incluir la venta de información sobre posibles abusos dentro del software o los sistemas.

Examinar este catálogo malicioso es una experiencia reveladora. Para aquellos de nosotros que pasamos nuestros días construyendo y protegiendo redes de ataques, es casi un insulto ver que el veneno de nuestras vidas se vende tan barato. Y, por supuesto, los mecanismos de compra también son muy sencillos. La industria del crimen como servicio tiene un sistema de pago perfecto e imposible de rastrear gracias a las criptomonedas: fácil de usar, anónimo y no vinculado a fronteras o restricciones internacionales. En 2015, un informe de Europol indicó que bitcoin se utilizó en más del 40% de las transacciones ilícitas en la Unión Europea, una cifra que podría decirse que ha aumentado desde entonces.

Si bien todo esto puede resultar incómodo de interpretar, también es esclarecedor y fascinante. Los profesionales de la seguridad y las redes deben centrarse en comprender el modelo operativo de sus adversarios. Así como los ciberdelincuentes comparten información, coordinan y desarrollan sus capacidades, comprenden sus objetivos e implementan rápidamente técnicas de vanguardia, nosotros también debemos hacerlo. Si el ataque se ha vuelto tan asequible para los delincuentes, no podemos permitirnos el lujo de no defendernos adecuadamente.

Leer también: Informática forense, qué es, definición, significado; 7 Formas Para Aumentar La Productividad De Gran Manera; Ventajas de IaaS, Infraestructura como servicio