Los responsables detrás del ya desaparecido Inferno Drainer crearon más de 16,000 dominios maliciosos únicos durante un período de un año, comprendido entre 2022 y 2023.

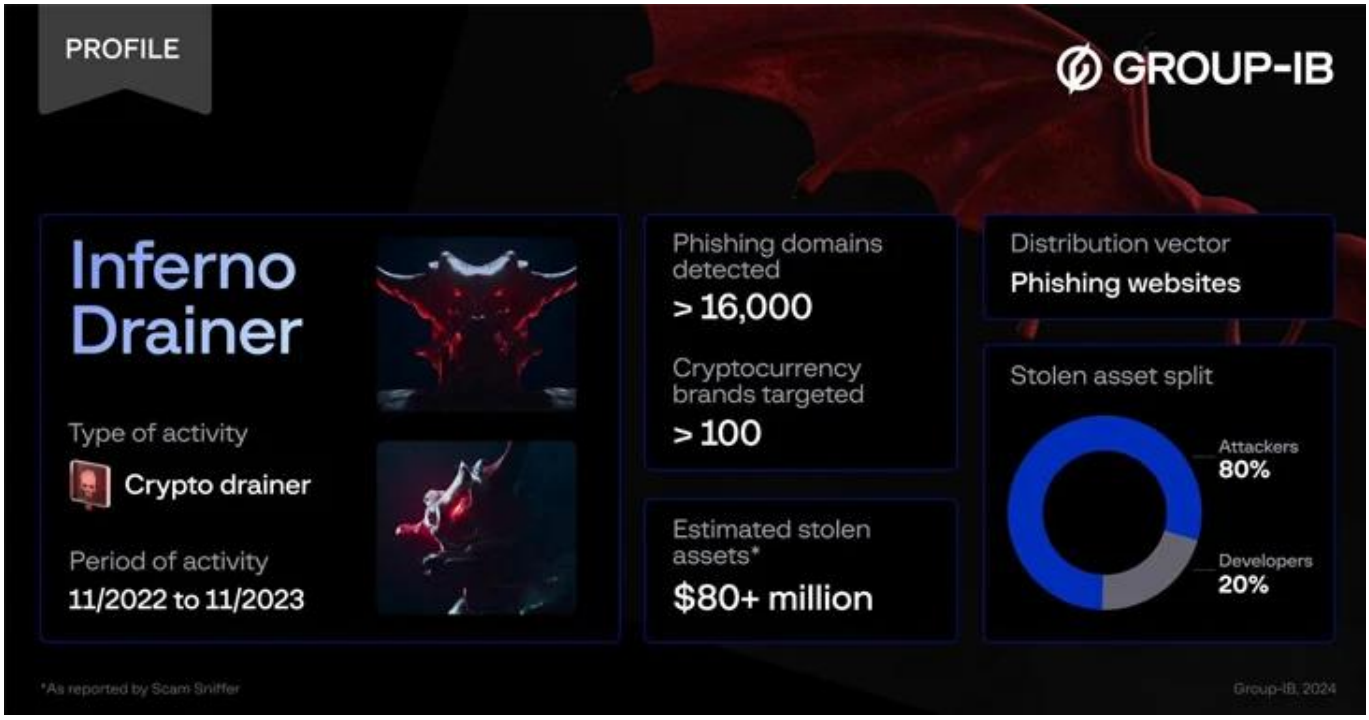
> *«La estrategia se valió de páginas de phishing de alta calidad para atraer a usuarios desprevenidos y llevarlos a conectar sus billeteras de criptomonedas con la infraestructura de los atacantes, que falsificaba los protocolos Web3 para engañar a las víctimas y autorizar transacciones»*, informó la firma con sede en Singapur, Group-IB, en un informe.

Inferno Drainer, activo desde noviembre de 2022 hasta noviembre de 2023, se estima que generó más de $87 millones en ganancias ilícitas al estafar a más de 137,000 víctimas.

El malware es parte de un conjunto más amplio de ofertas similares disponibles para afiliados bajo el modelo de estafa como servicio (o drainer como servicio), a cambio de un 20% de sus ganancias.

Además, los usuarios de Inferno Drainer tenían la opción de cargar el malware en sus propios sitios de phishing o utilizar el servicio del desarrollador para crear y alojar sitios de phishing, ya sea sin costo adicional o cobrando el 30% de los activos robados en algunos casos.

Según Group-IB, la actividad falsificó más de 100 marcas de criptomonedas mediante páginas especialmente diseñadas alojadas en más de 16,000 dominios únicos.



Un análisis adicional de 500 de estos dominios reveló que el drainer basado en JavaScript se alojaba inicialmente en un repositorio de GitHub (kuzdaz.github[.]io/seaport/seaport.js) antes de ser incorporado directamente en los sitios web. Cabe mencionar que el usuario «kuzdaz» actualmente no existe.

De manera similar, otro grupo de 350 sitios incluía un archivo JavaScript, «coinbase-wallet-sdk.js,» en un repositorio de GitHub diferente, «kasrlorcian.github[.]io.»

Estos sitios se propagaron en plataformas como Discord y X (anteriormente Twitter), atrayendo a posibles víctimas para hacer clic en ellos bajo el pretexto de ofrecer tokens gratuitos (también conocidos como airdrops) y conectar sus billeteras, momento en el cual sus activos se agotaban una vez aprobadas las transacciones.

Al utilizar nombres como seaport.js, coinbase.js y wallet-connect.js, la intención era hacerse pasar por populares protocolos Web3 como Seaport, WalletConnect y Coinbase para completar transacciones no autorizadas. El sitio web más antiguo que contiene uno de estos

scripts data del 15 de mayo de 2023.

> *«Otra característica común de los sitios web de phishing asociados a Inferno Drainer fue que los usuarios no podían acceder al código fuente del sitio mediante combinaciones de teclas o haciendo clic derecho con el mouse. Esto indica que los criminales intentaron ocultar sus scripts y actividades ilegales a sus víctimas»,* señaló Viacheslav Shevchenko, analista de Group-IB.

Es importante destacar que la cuenta X de Mandiant, propiedad de Google, fue comprometida a principios de este mes para distribuir enlaces a una página de phishing que alojaba un drainer de criptomonedas identificado como CLINKSINK.

> *«Creemos que el modelo 'X como servicio' continuará prosperando, en parte porque brinda más oportunidades a personas menos técnicamente competentes para probar suerte como ciberdelincuentes, y para los desarrolladores, es una forma altamente rentable de aumentar sus ingresos»,* comunicó la empresa.
>
> *«También anticipamos un aumento en los intentos de hackeo de cuentas oficiales, ya que las publicaciones supuestamente escritas por una voz autoritaria probablemente generarán confianza en los espectadores y harán que las posibles víctimas sean más propensas a seguir enlaces y conectar sus cuentas».*

Además, Group-IB afirmó que el éxito de Inferno Drainer podría impulsar el desarrollo de nuevos draines y provocar un aumento en los sitios web que contienen scripts maliciosos que falsifican protocolos Web3, señalando que 2024 podría convertirse en el *«año del drainer»*.

> *«Inferno Drainer puede haber detenido su actividad, pero su prominencia a lo largo de 2023 resalta los graves riesgos para los poseedores de criptomonedas a medida*

> *que los draines continúan desarrollándose»,* declaró Andrey Kolmakov, jefe del Departamento de Investigación de Delitos de Alta Tecnología de Group-IB.