El grupo de hackers detrás del ransomware Ryuk ha ganado más de 150 millones de dólares

Autor: I. Stepanenko

Fecha: Sunday 24th of January 2021 06:50:00 AM

Se estima que los operadores del ransomware Ryuk han ganado más de 150 millones de dólares en bitcoin por pagos de rescate luego de intrusiones en empresas de todo el mundo.

En un informe conjunto del 7 de enero, la compañía de amenazas Advanced Intelligence y la compañía de seguridad cibernética HYAS, dijeron que rastrearon los pagos a 61 direcciones de Bitcoin previamente atribuidas y vinculadas a los ataques de ransomware de Ryuk.

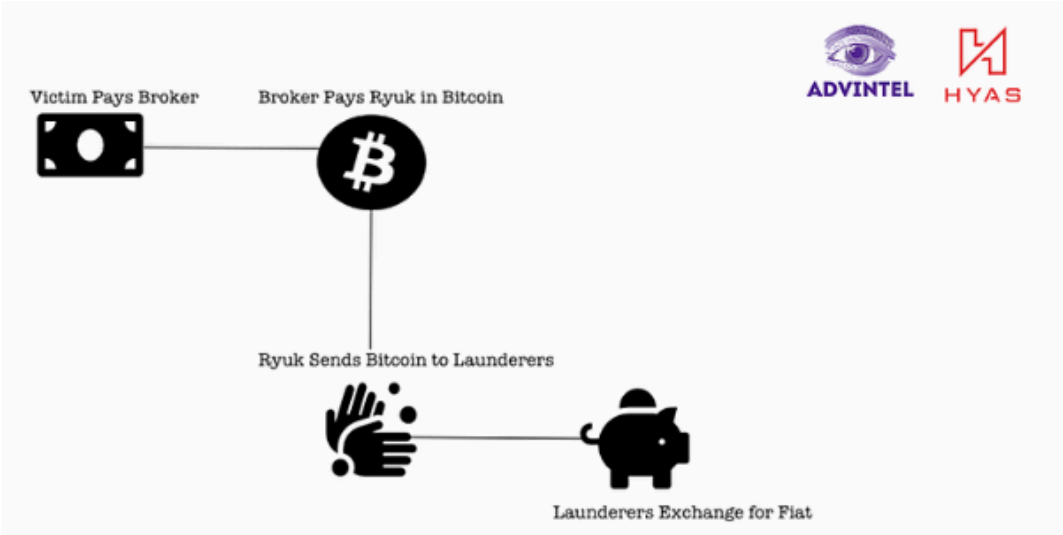
> «Ryuk recibe una cantidad significativa de sus pagos de rescate de un conocido corredor que realiza pagos en nombre de las víctimas del ransomware. Estos pagos a veces ascienden a millones de dólares y normalmente se ejecutan en el rango de cientos de miles», dijeron las dos empresas de seguridad.

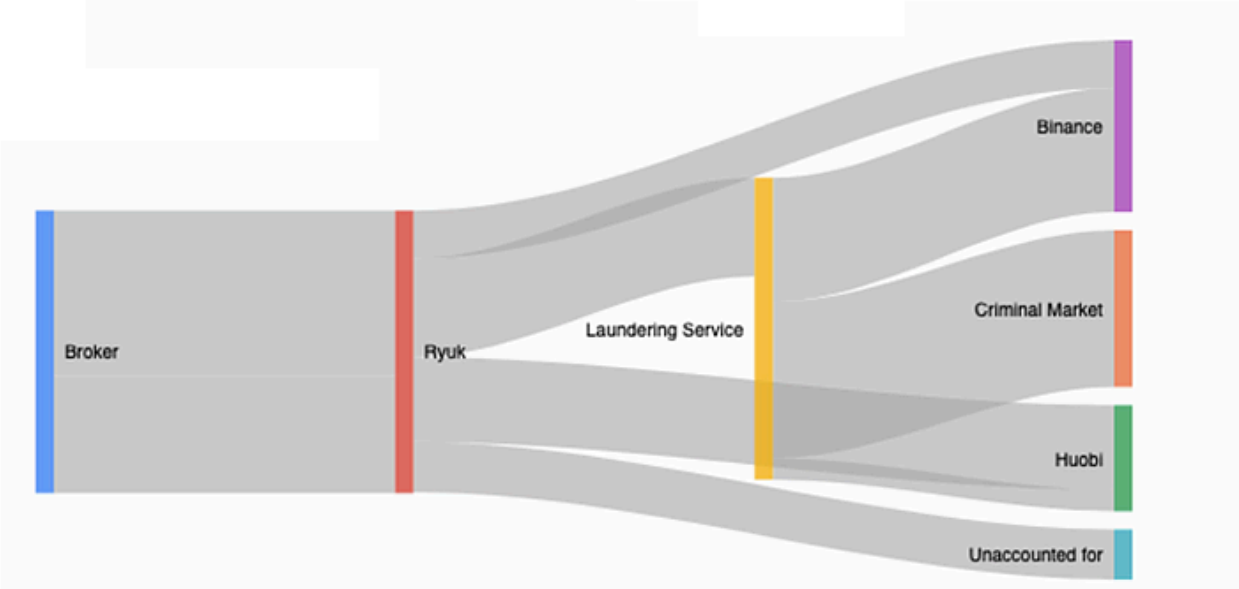
AdvIntel y HYAS aseguran que los fondos extorsionados se recolectan en cuentas de retención, se transfieren a servicios de lavado de dinero y luego se canalizan de regreso al mercado criminal y se utilizan para el pago de otros servicios criminales o se cobran en plataformas de intercambio de criptomonedas reales.

El grupo de hackers detrás del ransomware Ryuk ha ganado más de 150 millones de dólares

Autor: I. Stepanenko

Fecha: Sunday 24th of January 2021 06:50:00 AM





Ambas compañías encontraron algo extraño, pues mientras que otros grupos de ransomware generalmente usaban intercambios menos conocidos para retirar fondos, Ryuk convirtió Bitcoin en moneda fiduciaria real utilizando cuentas en dos portales de cifrado bien establecidos, como Binance y Huobi, probablemente utilizando identidades robadas.

Pero el informe conjunto de AdvIntel y HYAS también proporciona una cifra más actualizada con respecto a las operaciones de Ryuk.

La última cifra que se tenía fue de febrero de 2020, cuando los funcionarios del FBI hablaron en la conferencia de seguridad de RSA. En ese entonces, el FBI dijo que RYUK era el grupo de ransomware más rentable activo en la escena, habiendo ganado más de 61.26 millones de dólares en pagos de rescate entre febrero de 2018 y octubre de 2019, según las denuncias recibidas por el FBI Internet Crime Complaint Centrar.

Con este nuevo informe y la cifra de 150 millones de dólares, sigue claro que Ryuk ha mantenido su lugar hasta ahora.

Durante el año pasado, otros grupos de ransomware, como REvil, Maze y Egregor, también se hicieron populares y han estado muy activos, infectado cientos de empresas.

Sin embargo, no ha existido ningún informe sobre la suma estimada que han ganado esos grupos.