Dark web: esto es lo que cobran los ciberdelincuentes por datos privados de empresas

26/08/2022

Una nueva investigación realizada por la empresa de **ciberseguridad** Kaspersky, en la que analizaron más de 200 publicaciones de ciberdelincuentes en la **dark web**, afirma que el costo promedio de los datos de acceso a una gran **empresa** se encuentra entre **1.900 y 3.800 dólares**.

Los cibercriminales responsables de estas publicaciones no solo buscan **información** que permita ingresar a las **bases de datos** de distintas organizaciones sino que también, desean una ganancia económica Al mismo tiempo, estos hechos facilitan otros ataques realizados por más **ciberdelincuentes**.

Sin embargo, son los operadores de **ransomware** **(secuestro de datos)**, los creadores de los virus usados en ataques a compañías quienes reciben las mayores ganancias pues la cifra que Kaspersky estimó como promedio es de **38 millones de dólares** en estos casos.

Los operadores de ransomware, los creadores de los virus usados en ataques a compañías, quienes reciben las mayores ganancias pues la cifra que Kaspersky estimó como promedio es de 38 millones de dólares en estos casos.

Los datos más deseados por ciberdelincuentes

Las publicaciones analizadas para la realización del estudio de Kaspersky indican que el **75 %** de los datos que eran ofrecidos en la dark web eran **accesos RDP** (Protocolos de Escritorio Remoto por su nombre en inglés), que ayuda a los ciberdelincuentes a ingresar de forma remota a los **escritorio de los empleados**.

Los precios de esta información obtenida se establece en

relación con las ganancias de las organizaciones que fueron atacadas, por lo que si una compañía tiene unas ganancias de **450 millones de dólares**, los accesos que se ofrecen pueden llegar a estar a la venta por 50 mil dólares.

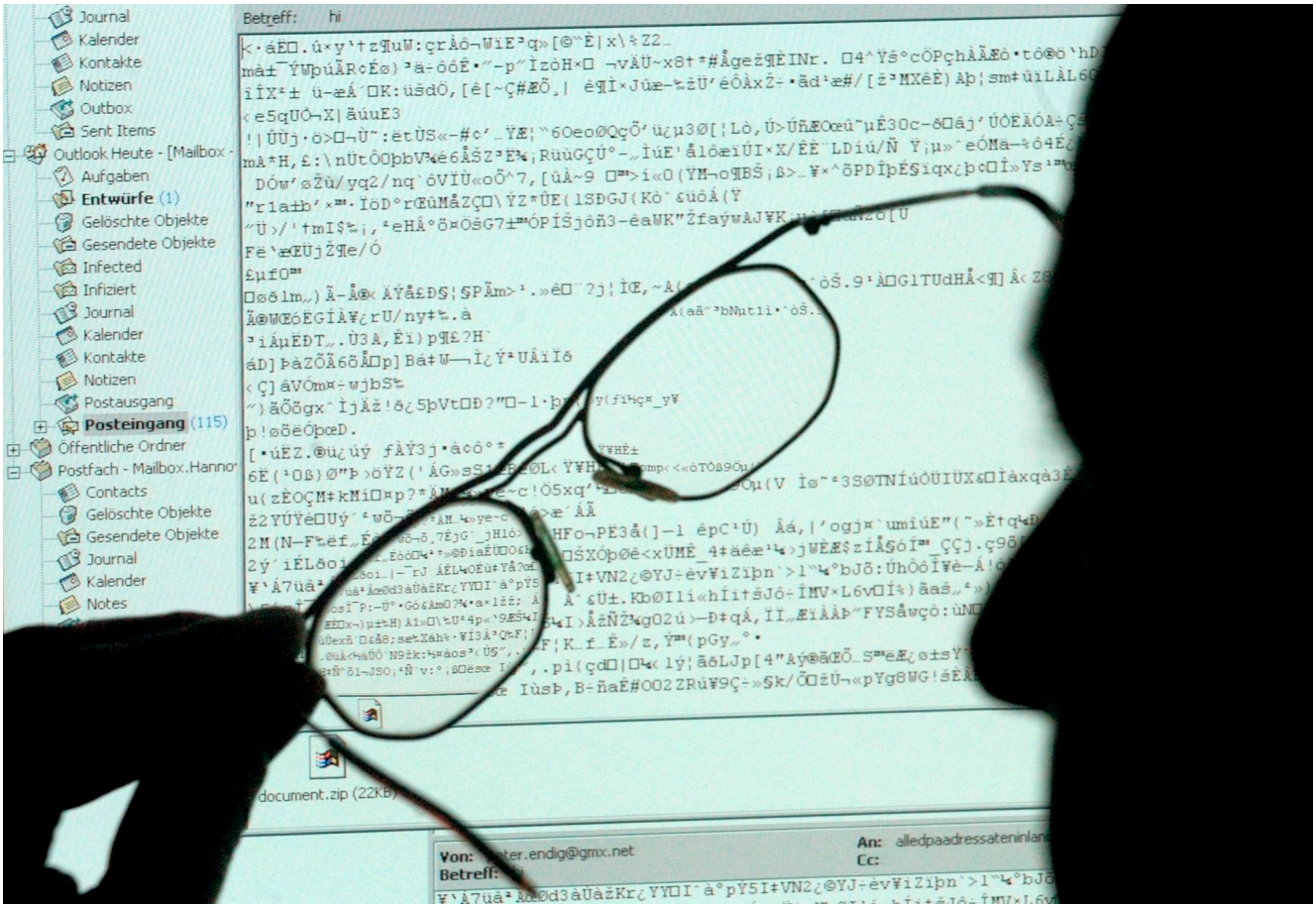
Además, un aspecto no menor al momento de establecer un precio por la información recolectada, es la **posible ganancia** que se puede llegar a obtener luego de realizar un ataque. Es por eso que los ciberdelincuentes están dispuestos a pagar elevadas cantidades de dinero por estos datos.

Los cibercriminales también pueden publicar algunos datos robados como seguro adicional, amenazando con publicar más si la empresa no paga el dinero que exigen dentro de un plazo estipulado. (EFE/Oskar Burgos/Archivo)

Por su parte, los cibercriminales también pueden publicar en sus blogs algunos datos robados, de hecho, usan ese medio como prueba y amenaza a las víctimas para que paguen el rescate dentro del plazo estipulado.

“Obtener visibilidad de las fuentes en la Dark Web es esencial para las empresas que buscan enriquecer su **inteligencia de amenazas**”, indicó Fabio Assolini, director del Equipo de Investigación y Análisis para América Latina en Kaspersky.

Además, afirmó que la información oportuna sobre los ataques planificados, las discusiones sobre vulnerabilidades y las **filtraciones de datos** pueden ayudar a tomar las medidas adecuadas”.



El reporte “Cost of a Data Breach Report” indica en el documento, el tiempo que le toma a una organización de esta región identificar y controlar una situación de filtración de datos es de un periodo de 331.5 días en 2022. (EFE/Archivo)

Filtración de datos en empresas

El reporte Cost of a Data Breach Report (Costo de una filtración de datos) de IBM, que se basa en un análisis de casos reales experimentados por 550 organizaciones a nivel

mundial, entre los que se encuentran 66 empresas de América Latina; tiene datos relevantes sobre el tiempo que tardan las organizaciones en controlar estos ataques.

El tiempo que le toma a una organización de esta región identificar y controlar una situación de filtración de datos es de un periodo de **331.5 días en 2022**, 25 menos que el registrado en el reporte anterior.

Además, se informa que la gran mayoría de las organizaciones que formaron parte del estudio, en total un 83 %, ha experimentado alguna vez un caso de filtración de datos.