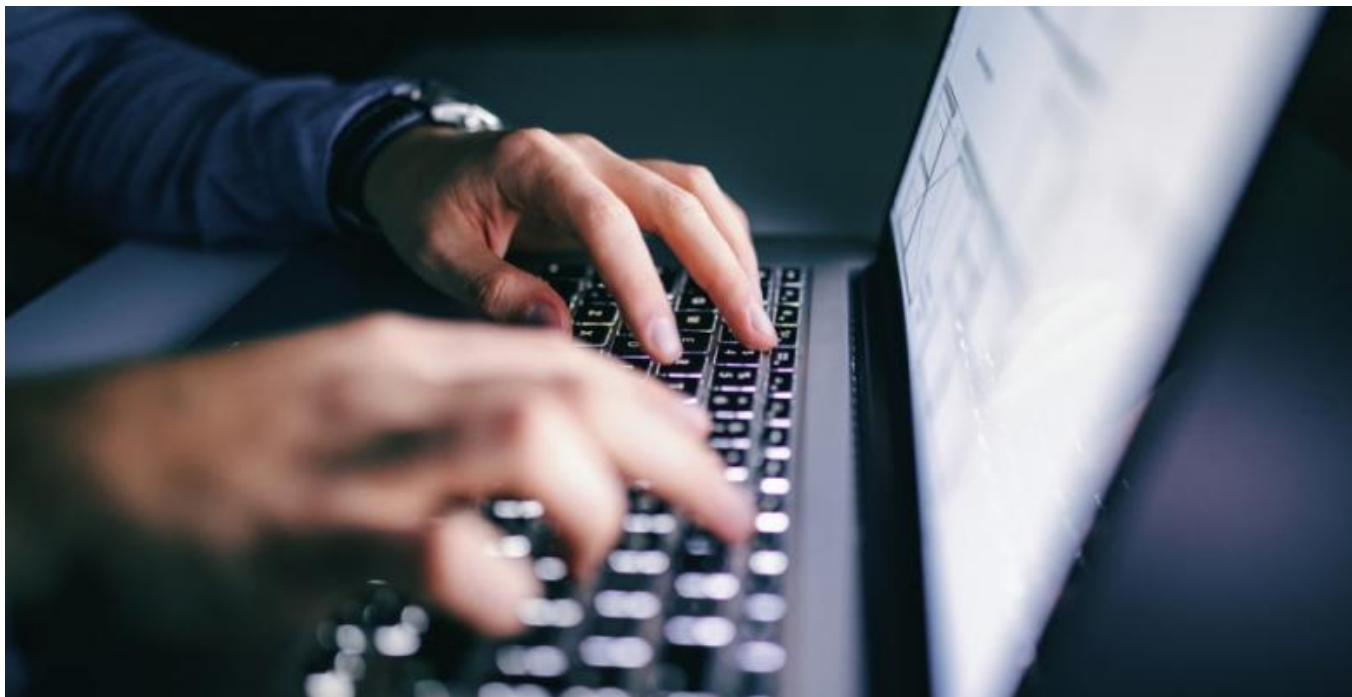

Uno de los dominios más peligrosos del mundo sale a la venta

12/02/2020



Ha salido a la venta uno de los dominios más peligrosos de Internet, que en manos equivocadas podría poner en riesgo los datos de cientos de miles de sistemas de empresas en todo el mundo.

Se trata de corp.com, un dominio que fue adquirido en 1994 por el empresario tecnológico Mike O'Connor junto con otros tan básicos como: bar.com, cafes.com, place.com y television.com. Aunque a lo largo de los años O'Connor vendió muchos de ellos, hasta ahora se había negado a subastar el que, quizás, sea el más sensible de todos, explica el blog Krebs On Security.

Quien maneje el dominio en cuestión tendría acceso a un flujo interminable de contraseñas, correos electrónicos y otros datos personales pertenecientes a grandes corporaciones. Esto, gracias una antigua ruta predeterminada de los sistemas Windows que las empresas han utilizado por décadas.

Se trata de la manera en que el sistema operativo de Microsoft maneja los dominios dentro de una red local. Windows valida los nombres a través de un servicio conocido como Active Directory, cuya ruta predeterminada desde las primeras versiones es denominada 'corp'. Muchas compañías mantuvieron esa configuración sin modificarla.

Por ejemplo, si un empleado intenta acceder a los datos de su compañía, cuyo dominio interno sea "corp", desde un lugar público —un restaurante, un centro comercial, etc.— es posible que su computadora intente extraer los datos desde corp.com en lugar de desde los propios sistemas internos de su empresa. Por tanto, los dominios destinados a ser utilizados exclusivamente en una red interna podrían solaparse con otros de la Internet abierta.

Un vertedero de desechos

Así, quien controle corp.com podría interceptar pasivamente las comunicaciones privadas de cientos de miles de computadoras que terminan siendo llevadas fuera del entorno corporativo que utiliza esta designación de 'corp' para su dominio en Active Directory. Un estudio de tráfico corporativo en 2019 encontró que más de 375.000 computadoras con Windows intentaron enviar información de dominio de corp.com, incluidos intentos de iniciar sesión en redes corporativas internas y de acceder a archivos compartidos en esas redes.

El precio inicial de venta de corp.com es de 1,7 millones de dólares. O'Connor afirmó que espera que Microsoft sea el comprador, ya que esta dirección representa un peligro para sus productos a nivel de seguridad. Sin embargo, teme que el gigante informático rechace hacerlo y el dominio sea finalmente adquirido por ciberdelincuentes.

"Básicamente estoy subastando un vertedero de desechos químicos porque no quiero pasarlo a mis hijos y que carguen con él. Mi frustración aquí es que a los buenos no les importa", confiesa O'Connor.
