TECNO

Quiénes están detrás del hackeo a Migraciones y cómo funciona Netwalker, el software malicioso utilizado

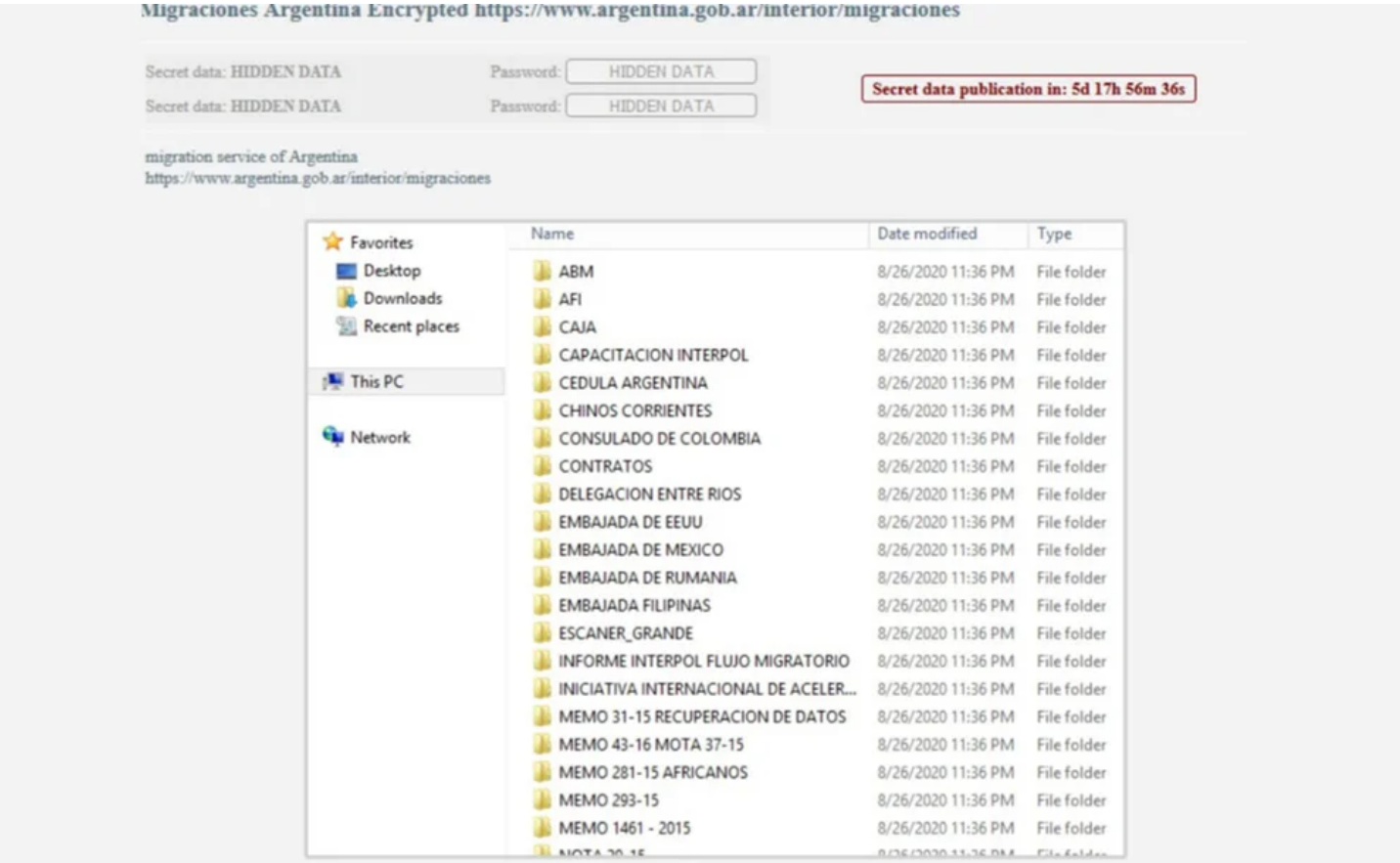
Secuestro de datos, extorsiones millonarias e indicios que conducen a Rusia. Cómo se lleva a cabo uno de los ciberdelitos más frecuentes

Por **Julieta Schulkin**
5 de Septiembre de 2020

El jueves 27 de agosto, un **ransomware** (un software malicioso) denominado **Netwalker** vulneró los datos de la Dirección Nacional de Migraciones. Un mensaje extorsivo señalaba que, si no se pagaba por recuperar la información secuestrada, harían públicos los datos. Están en juego **22 carpetas** con información de **embajadas** (incluida la de Estados Unidos), informes de **Interpol** y de la **AFI** (Agencia Federal de Inteligencia), entre otros.

Si bien el mismo día del ataque, Migraciones aclaraba que éste "no afectó la infraestructura crítica" del organismo, ni "la información sensible, personal o corporativa", fuentes del Gobierno adelantaron a **Infobae** que **no van a negociar con los hackers.**

Por otra parte, desde la Dirección Nacional de Migraciones señalaron que se "desconoce la identidad de los posibles" autores de la amenaza, que está bajo investigación. La causa está a cargo del **juez Sebastián Casanello** y según pericias realizadas, los ciberdelincuentes no habrían accedido a la base de datos, sin embargo, no está todo dicho. El plazo que han dispuesto los hackers para hacer pública la información sería el próximo miércoles.



Hackeo a Migraciones: las carpetas comprometidas

Por otro lado, saber qué falló y cómo fue posible vulnerar el sistema de Migraciones es una nueva preocupación. En efecto, trascendió que el director del departamento de Seguridad

El malware que pide rescate

Ransomware

Un ransomware es un tipo de ciberdelito que consiste en el **secuestro de datos** por medio de un software malicioso (malware) que cifra archivos **impidiendo que el usuario pueda tener acceso al contenido.** Suele ser llamado virus, pero no es el término apropiado.

Para recuperar el acceso a los datos secuestrados (bloqueados y posiblemente copiados) que son **encriptados y se convierten en inaccesibles para el usuario, el ciberdelincuente le solicita al usuario el pago de un rescate en formato de criptomonedas.**

No es un delito nuevo, existe desde mediados de la década del 90, pero en los últimos años se ha convertido en uno de los ataques más frecuentes. **Existen diferentes tipos de ransomware, el que sufrió Migraciones es NetWalker.** Es una cepa de ransomware que **apareció por primera vez en agosto de 2019**. En su versión inicial, se llamaba **Mailto**, pero luego cambió su nombre a fines del año pasado. Funciona como un **RaaS** (ransomware como servicio) de acceso cerrado.

Expertos de la compañía McAfee señalan que NetWalker ha realizado en el último año
ma o código que se aprovecha de la

software) con credenciales débiles o mediante el personal de *spear-phishing* en empresas importantes.

En este último caso, es una una estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas. Es uno de los engaños más comunes hoy y podría haber sido la puerta de entrada al ataque de Migraciones.

Todos los sistemas operativos podrían ser afectados por un ransomware, aunque, ciertamente, en el caso de NetWalker vulnera poderosamente a Windows. En terminales desactualizadas u obsoletas, el riesgo es aun mayor.

La agrupación detrás, ¿es rusa?

Se cree que los atacantes detrás del ransomware NetWalker han ganado más de USD 25 millones por pagos de rescate desde marzo de este año, según McAfee que ha rastreado pagos que las víctimas hicieron a direcciones de Bitcoin.

NetWalker es el nombre del ransomware, no de una agrupación, sin embargo es posible que exista un grupo organizado detrás. En marzo de este año un usuario de internet que se hace llamar **Bugatti "abría el juego" para que otros ciberdelincuentes se unieran al grupo como parte de un modelo de negocio RaaS, interesado en contratar personas de habla rusa.**

Actualmente, la víctima más destacada de NetWalker es la Universidad Estatal de Michigan, infectada a fines de mayo de 2020, como parte de varios ataques a universidades de los Estados Unidos. Sin embargo, **McAfee señala que NetWalker también representa un riesgo para las empresas de todo el mundo.**

MÁS SOBRE ESTE TEMA:

Qué es el secuestro de SIM y cómo puede afectar la seguridad de tus cuentas

India prohibió 118 aplicaciones chinas, en una nueva escalada de tensión por los conflictos fronterizos