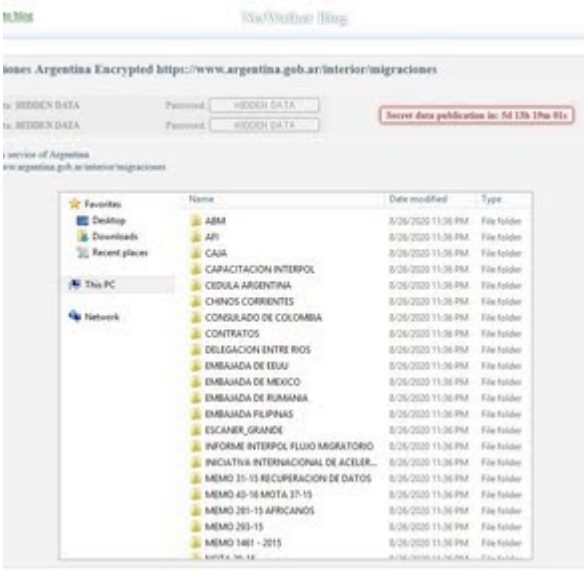
Un grupo internacional de ciberdelincuentes afirma haber robado información de Migraciones y pide un rescate multimillonario

06/09/2020

Un ataque de ransomware conocido como **NetWalker secuestró información de la Dirección Nacional de Migraciones (DNM)** y amenaza con publicar esos datos de la dependencia del Ministerio del Interior si no se efectúa un pago millonario. **Se habla de 76 millones de dólares.** El plazo vence el miércoles que viene.

"Al igual que otros ransomware, NetWalker publica extractos de los datos robados en un llamado **'sitio de filtración'.** Si la víctima no paga, se publica la totalidad de los datos robados. En este caso, sucederá en **un lapso de 5-6 días**", explicó a **Clarín** Brett Callow, analista de amenazas de la compañía de ciberseguridad **Emsisoft**, que confirmó el ataque.

Los datos que se publicaron en este caso se difundieron a través de **una captura de pantalla** donde se ven carpetas que hacen referencia a la **Agencia Federal de Inteligencia (AFI)**, consulados, embajadas e informes de flujos migratorios. Allí también se ve el lapso de tiempo en el que la información será publicada.



La lista de carpetas que difundió NetWalker de la Dirección Nacional de Migraciones. Foto NetWalker Blog

Fuentes del Ministerio del Interior, a cargo de **Eduardo «Wado» de Pedro**, confirmaron a **Clarín** el incidente informático y aseguraron que ya presentaron una denuncia penal al respecto que quedó en manos del juez Sebastián Casanello.

La denuncia, a la que tuvo acceso este medio, reproduce el mensaje amenazante de los hackers:

«No traten de recuperar sus archivos sin un programa desencriptador, podrían dañarlos y dejarlos en condición de irrecuperables. Para nosotros esto son negocios y para probarles nuestra seriedad, les desencriptaremos un archivo sin costo. Abran nuestro sitio, suban el archivo encriptado y tendrán el archivo desencriptado gratis. Además, su información podría haber sido robada y si no cooperan con nosotros, se convertirá públicamente disponible en nuestro blog»

Según explicaron, **un virus entró a Migraciones** y por cuestiones de seguridad se desconectó el sistema para preservar la base de datos, lo que generó que durante tres horas los cinco puestos fronterizos terrestres, el aeropuerto de Ezeiza y la terminal de Buquebus estuvieran sin sistema y cerrados durante ese lapso. Es decir: nadie pudo entrar ni

salir del país en esas horas.

La alarma se encendió cuando a las 7 de la mañana de 27 de agosto el área de Sistemas de Migraciones recibió numerosos llamados de diversos puestos de control solicitando soportes técnico. La cantidad de reportes, de diferentes puntos del país, dio cuenta de que no se trataba de una situación normal, sino de **una maniobra de ciberdelincuentes.**

Tras el ataque, se realizó una pericia técnica y se corroboró el funcionamiento chequeando contra la base de datos. A partir de esa operación se documentó qué **computadoras fueron vulneradas** y todo se incluyó en la denuncia penal presentada que ahora investiga Casanello.

En ese marco, apareció esta organización de ciberdelincuentes internacional pidiendo un millonario rescate, y se amplió la presentación judicial con esta nueva información y la capturas de pantalla que ahora circula en redes sociales.

Por esa razón, se sumó **la acusación de extorsión a la acción penal**. "Las pericias nos dicen que no se logró acceder a la base de datos, sino a carpetas de distintas computadoras", explicaron fuentes oficiales. Es el expediente 6853/2020, radicado en la Unidad Fiscal Especializada en Ciberdelincuencia.

Por lo que muestran esos ficheros de la captura, los cibercriminales podrían haber accedido a archivos alojados en esas computadoras sobre inteligencia criminal, fichas de terroristas con ingreso prohibido al país, pero «no información sensible», explican.

En la imagen que colgaron los ciberatacantes se ve una pantalla con 22 carpetas con los siguientes nombres: «ABM», «AFI», «CAJA», «CAPACITACIÓN INTERPOL», «CEDULA ARGENTINA», «CHINOS CORRIENTES», «CONSULADO DE COLOMBIA», «CONTRATOS», «DELEGACIÓN ENTRE RÍOS», «EMBAJADA DE EEUU», «EMBAJADA DE MÉXICO», «EMBAJADA DE RUMANIA», «EMBAJADA DE FILIPINAS»,

«ESCANER_GRANDE», «INFORME INTERPOL FLUJO MIGRATORIO», «INICIATIVA INTERNACIONAL DE ACELER…», «MEMO 31-15 RECUPERACIÓN DE DATOS», «MEMO 43-16 MOTA 37-15», «MEMO 281 – 15 AFRICANOS», «MEMO 293-15», «MEMO 1461 – 2015».

Los nombres de esos archivos podrían dar cuenta de información vinculada a la Agencia Federal de Inteligencia (AFI), información diplomática sobre varias embajadas, y hasta datos de la policial internacional Interpol.

En el Gobierno comparan al ataque con el que sufrió Telecom en julio pasado. El pasado 19 de julio, un ransomware afectó a los sistemas de atención al cliente de la compañía telefónica. Desde **Rusia**, habían pedido una suma que se estimó entre **7.5 y 25 millones de dólares**, pero no lograron tener éxito. Fue similar, a su vez, al inmenso hackeo de cuentas que sufrieron personalidades de alto perfil en Estados Unidos a mediados de julio.

En paralelo, señalaron desde Migraciones, ahora se trabaja con Seguridad Informática para ver **qué falló y cómo los hackers pudieron vulnerar el sistema**. Por lo sucedido, además, fue despedido de su cargo el director de Seguridad Informática a cargo de la dependencia, que estaba en esa posición desde hacía 25 años.

Este ransomware en particular es **una amenaza doblemente peligrosa** porque además de bloquear la información, **la copia**. "Antes los grupos de ransomware solían simplemente encriptar los datos de sus víctimas pero, desde noviembre del año pasado, también los han estado robando.La amenaza de liberar los datos se utiliza luego como **palanca adicional para extorsionar el pago**", detalló el especialista de Emsisoft. Ahora se roban datos en más de 1 de cada 10 incidentes.

El jueves pasado, Migraciones había comunicado de manera pública que había logrado contener un ataque informático. Pero sucede que estos ataques tienen acceso a información desde 56

días previos a **que se active el ataque que encripta los archivos.** "Durante ese período previo, los atacantes ya pueden haber robado información. Para el momento en el que las organizaciones se dan cuenta del incidente, la información ya fue robada", detalla Callow. Y eso sería lo que sucedió en este caso.

A partir de unos links del blog de NetWalker, el especialista en seguridad informática **Javier Smaldone** confirmó a **Clarín** el hackeo: "Se puede ver una lista de sitios y ahí está Migraciones: **fueron víctimas de NetWalker".**

A pesar de que hay algunos ransomware que pueden ser desbloqueados, NetWalker no es uno de ellos. Y por eso ha sido tan exitoso: el grupo de hackers que lo usa logró recaudar 25 millones de dólares desde marzo de 2020.

«Solicitamos se investigue este hecho desde una triple perspectiva, es decir, saber si el ciberataque se realizó como un fin en sí mismo, si fue con el objeto de manipular o dañar informaciñon contenida en nuestra base de datos, o como una herramienta para lograr y/o facilitar la comisión de un delito tradicional», reclamó la Dirección de Migraciones, a través de sus abogados.

Sobre NetWalker: 25 millones de dólares con extorsiones

NetWalker apareció por primera vez en **agosto de 2019.** Su primer nombre fue "Mailto", pero luego adoptó su nomenclatura actual.

Según explica el sitio ZDNet, autoridad en seguridad informática, NetWalker es una "cepa" particular de este tipo de programas que secuestran información. Distintas bandas de hackers "aplican" para usar este ransomware a través de versiones personalizadas. NetWalker "depura" esas versiones y

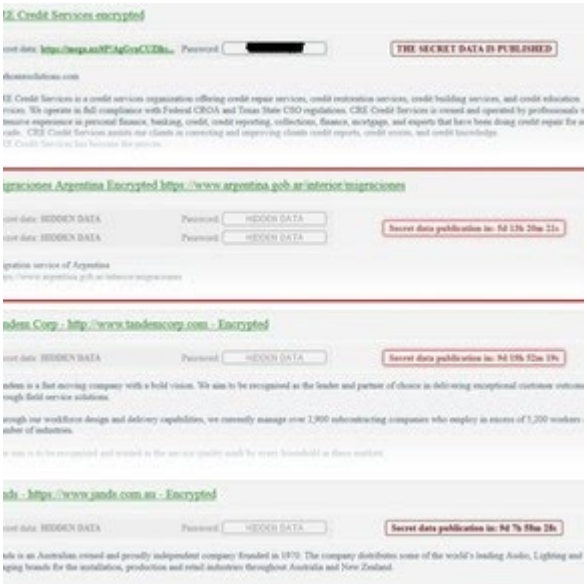
las reparte entre distintos grupos de atacantes para que hagan los “**deploy**” (implementación, publicación) , esto es, que efectivamente ataquen a alguna entidad.

Y sucede que operan incluso antes del “deploy”: “En estos incidentes, los atacantes tienen acceso a las redes durante un promedio de **56 días antes de implementar el ransomware** que encripta los archivos, y este es el punto en el que las organizaciones se dan cuenta de que han sido atacadas”, explica a Clarín Callow.

“Sin embargo, durante esos 56 días anteriores, los atacantes **ya podrían haber realizado varias operaciones**, incluido el robo de datos. En otras palabras, cuando las organizaciones se dan cuenta de que se han visto comprometidas y están bajo ataque, sus datos ya no existen o fueron robados”, completó.

Por esta razón, no está del todo claro el alcance del ataque sobre la Dirección Nacional De Migraciones, que en sus declaraciones a Clarín, reconoció pero relativizó el incidente.

NetWalker tiene un blog al cual sólo se puede acceder a través de navegadores de la Deep Web como Tor: **allí se ven todos los casos activos con sus respectivas cuentas regresivas y los sitios afectados.**



La lista en el sitio de Netwalker, donde aparece Migraciones. Foto: Captura Netwalker Blog

Qué es un Ransomware

WannaCry, un famoso ransomware que hizo estragos en 2017. Foto Bloomberg

Ransomware es un acrónimo de **“programa de rescate de datos”**. Ransom en inglés significa rescate, y ware es un acortamiento de la conocida palabra software: un programa de secuestro de datos. El ransomware es un subtipo del malware, acrónimo de “programa malicioso” **(malicious software).**

Ahora bien, este tipo de virus actúa restringiendo el acceso a partes de nuestra información personal, o la totalidad. Y en general, los hackers explotan esto para pedir algo a cambio: **dinero**. Por eso entre sus blancos predilectos están grandes empresas, gobiernos e instituciones.

Si bien algunos ransomware simples pueden bloquear el sistema de una manera simple, los más avanzados utiliza **una técnica llamada extorsión "criptoviral"**, en la que se encriptan los archivos de la víctima logrando que se vuelvan completamente inaccesibles.

Solo durante los primeros seis meses de 2020 se detectaron casi 400.000 muestras de ransomware más que en el mismo periodo del año pasado, según se extrae del informe Threat Landscape Report. Lo cual significa que su alcance es muy amplio.

Y, durante la cuarentena, fue sin dudas el ciberataque estrella que más usaron los hackers.

Fuente: Clarín

PJB