EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Fecha	Sección	Página
08.07.2020	Dinero	1-7

MÁS HACKEOS

Autoridades y expertos en ciberseguridad de Symantec y ESET aseguran que los ataques con ransomware se incrementan.

Alertan de Evil Corp

Los cibercriminales han puesto los ojos en México y aseguran que van a vulnerar a dependencias y empresas en el país. Lo mismo harán en EU.

EVIL CORP

PIDEN MILLONES POR HACKEOS

Se incrementan los ataques de Evil Corp

Los piratas informáticos buscan afectar con ransomware a empresas y gobiernos de Estados Unidos y México

POR PAUL LARA

Paul.lara@gimm.com.mx

Expertos en seguridad cibernética han identificado que el grupo de hackers Evil Corp tiene al menos 31 objetivos en Estados Unidos y México para hackear en los próximos meses, incluidas ocho compañías de la lista Fortune 500.

Un reporte de la división de inteligencia sobre amenazas de la compañía de ciberseguridad Symantec señala que los atacantes son hábiles y experimentados, capaces de penetrar en las corporaciones mejor protegidas, robar contraseñas e identidades y moverse con facilidad a través de sus redes. Para ello utilizan WastedLocker, un ransomware muy peligroso y de fácil propagación.

Sin mencionar nombres, pues algunos son clientes de la firma de ciberseguridad, aseguran que las 31 organizaciones han comenzado a ser atacados, lo que significa que el número total de ataques puede ser mucho mayor. Los criminales cibernéticos, afirman, habían violado las redes de las organizaciones objetivo y estaban en proceso de preparar el terreno para organizar ataques de ransomware rumbo a las elecciones del próximo 3 de noviembre en Estados Unidos.

En México buscan, principalmente, a bancos que trabajan con el gobierno mexicanos en la entrega de beneficios sociales, y aseguran que van por el INE desde ahora, para también vulnerar las elecciones para renovar el Congreso en junio del próximo año, así como por el Banco de México para solicitar rescates con instalación de ransomware. Para ello están usando campañas en redes sociales y servicios de mensajería, tratando de vulnerar los equipos de trabajadores remotos de las dependencias y empresas que, por cuarentena, siguen en casa.

En Symantec aseguran que entre los responsables de los ataques a ambas naciones figuran dos ciudadanos rusos, Igor Olegovich Turashev y Maksim Viktorovich Yakubets, acusados en diciembre pasado en EU por su implicación en Evil Corp, acusada de vulnerar bancos estadunidenses, mexicanos y británicos, y hacerse sólo en 2019 más de 100 millones de

Continúa en siguiente hoja

EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Fecha	Sección	Página
08.07.2020	Dinero	1-7

dólares en robos.

A la fecha hay una recompensa de cinco millones de dólares por parte del gobierno de Estados Unidos a quien ofrezca información que conduzca al arresto del presunto líder de Evil Corp, Maksim Yakubets.

"Yakubets es un verdadero criminal del siglo XXI", señaló el fiscal general adjunto de los Estados Unidos, Brian Benczkowski. "Se ha ganado su lugar en la lista del FBI de los ciberdelincuentes más buscados del mundo".

Desde el año pasado, el gobierno de EU ha puesto el dedo en los vínculos entre los ciberdelincuentes de Evil Corp y el Estado ruso. Funcionarios del Tesoro de EU han señalado que Yakubets trabajó para el Servicio Federal de Seguridad (FSB) de Rusia, su agencia de inteligencia, y robó material clasificado en nombre de Moscú.

EN ALERTA MÁXIMA

Especialistas de la compañía de ciberseguridad ESET aseguran que Evil Corp también está detrás de una familia de software malicioso en evolución conocida como Dridex, la cual ha afectado a bancos y empresas desde 2011.

"El malware funciona al piratear bancos y empresas y realizar transferencias financieras ilegales que eventualmente se canalizan de vuelta a los hackers. Desde entonces, también se ha diversificado el ransomware".

El malware Dridex, según la investigación de ESET, se dirige también a pequeñas empresas y dependencias de gobierno que carecen de las sofisticadas ciberdefensas de las compañías más grandes.

Israel Reyes, director del MIT Analytics, dijo que con la cuarentena por covid-19 se ha puesto mayor presión a empresas y gobiernos para proteger a empleados en sus hogares contra los ciberataques de grupos como Evil Corp.