MEDIO: EXCELSIOR
SECCION: DINERO
PÁGINA: 1/7
FECHA: 07/MARZO/2022

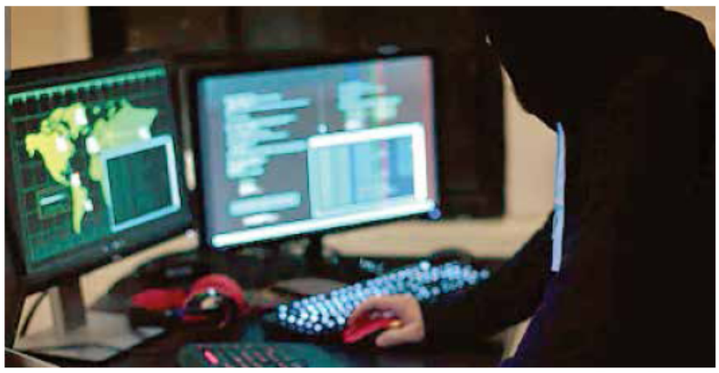


Foto: Freepik

ALERTA FITCH RATINGS

Ataques en la red, más latentes

Fitch Ratings alertó que el conflicto bélico entre Rusia y Ucrania aumenta el riego de ataques cibernéticos indirectos, es decir, que afecten a gobiernos o entidades que tengan negocios en ambos países, que impongan sanciones o que interfieran. Expresó que el ataque conocido como NotPetya, ocurrido en 2017, es un ejemplo de los riesgos que existen hoy. > 7

LÍNEA DE TIEMPO DEL CONFLICTO EN EL CIBERESPACIO:

13 y 14 de enero
Se desfiguraron varios sitios web del gobierno ucraniano y los sistemas se infectaron con malware disfrazado de ataque de ransomware, que era un wiper sofisticado.

15 de febrero
Hubo una serie de ataques de denegación distribuida de servicio (DDos) contra sitios web del gobierno y militares de Ucrania, y contra tres bancos grandes de ese país.

23 de febrero
Se desató otra ola de ataques DDoS contra los ministerios de Relaciones Exteriores, de Defensa, del Interior, el Gabinete de Ministros y la Seguridad de Ucrania.

24 de febrero
Los sitios web del Gabinete de Ministros de Ucrania y los de los Ministerios de Relaciones Exteriores, Infraestructura, Educación y otros no estaban accesibles.

POR AURA HERNÁNDEZ
aura.hernandez@gimm.com.mx

Rusia no sólo sobresalió por su fortaleza en la industria energética en las últimas décadas, también logró ubicarse como uno de los principales jugadores y amenazas en el ciberespacio gracias a que cuenta con especialistas dentro de sus agencias y es el país de origen de varios grupos de cibercriminales.

El país dirigido por Vladímir Putin incluso fue clasificado, junto con China y Corea del Norte, como una de las principales amenazas para la ciberseguridad de Japón, al considerar que dichas naciones emprenden actividades hostiles en el ciberespacio.

De acuerdo con la propuesta de la Estrategia Nacional de Seguridad Cibernética de Japón, que fue publicada a mediados de 2021, Rusia es sospechoso de emprender operaciones cibernéticas hostiles con fines políticos o militares.

Esto se debe a varios incidentes que han ocurrido en los últimos años con grupos cibercriminales que tienen origen ruso y que, por su estructura, posiblemente son financiados por un estado para realizar sus ataques.

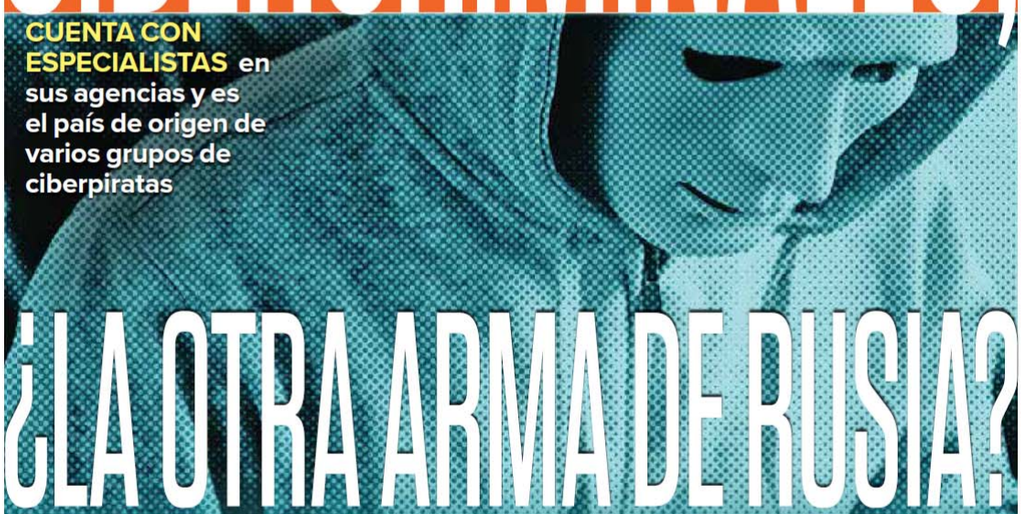
Si bien agencias internacionales como el Buró Federal de Investigaciones de EU han identificado a algunas de las personas que forman parte de los grupos cibercriminales, éstos suelen vivir sin preocupaciones en Rusia.

Algo que se mantuvo sin cambios hasta enero de este año, cuando el Servicio de Seguridad Federal de Rusia (FSB), tras un pedido de Estados Unidos, desmanteló a REvil tras arrestar a 14 personas e imputarlos por cometer delitos de circulación ilegal de medios de pago.

"Sirve como una advertencia para otros delincuentes de que operar desde Rusia podría no ser el puerto seguro que pensaban que era", dijo el asesor senior de seguridad de Sophos, John Shier. Sin embargo, esos avances podrían quedar atrás debido a la reciente invasión de Ucrania.

LA GUERRA TAMBIÉN EN EL CIBERESPACIO

CIBERCRIMINALES, ¿LA OTRA ARMA DE RUSIA?



CUENTA CON ESPECIALISTAS en sus agencias y es el país de origen de varios grupos de ciberpiratas

La confrontación

Un día antes de que las tropas rusas invadieran, varios sitios web gubernamentales ucranianos fueron bloqueados a través de ataques de denegación de servicio y también se encontró un nuevo código malicioso, bautizado como HermeticWiper.

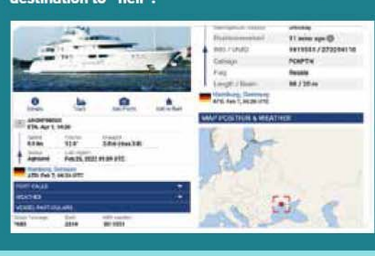
Ucrania responsabilizó de esos ataques a Rusia, algo que confirmó la Casa Blanca al indicar que tiene información técnica que vincula a la Dirección Principal de Inteligencia de Rusia con el ataque de denegación de servicios.

Si bien el Kremlin ha negado cualquier implicación en los ciberataques, el apoyo que ha recibido de grupos cibercriminales es sospechoso.

@Excelsior

Ryan Gallagher
@rj_gallagher

Según los informes, Putin tiene un yate de lujo de $97 millones llamado "Graceful". El sábado, un grupo de piratas informáticos anónimos descubrió una manera de alterar los datos de tráfico marítimo e hizo que pareciera que el yate se hubiera estrellado en la Isla de las Serpientes de Ucrania, y luego cambió su destino al "infierno": changed its destination to "hell":



El peor escenario

Al platicar con Excélsior, Marcus Fowler, vicepresidente senior de Compromisos estratégicos y amenazas de Darktrace, no descartó que los grupos de cibercriminales, probablemente respaldados por Rusia, tengan como objetivo las infraestructuras críticas ucranianas como los sectores de energía, tecnologías de la información y comunicaciones.

"Estos ataques también podrían causar daños colaterales si un ataque se extiende más allá del objetivo previsto", consideró.

Muestra de ello es el ataque NotPetya de 2017, dirigido contra la infraestructura ucraniana y se salió de control, paralizando fábricas.

w

25 de febrero
Se pasa de ciberataques a la guerra terrestre. Una cuenta de Twitter que representa a Anonymous declaró una "guerra cibernética" contra el gobierno ruso.

26 y 27 de febrero
Altos mandos ucranianos pidieron a las personas con habilidades cibernéticas que se unieran al IT Army virtual para ayudar a atacar los activos rusos en represalia.

28 de febrero
Partidarios hacktivistas de Ucrania piratearon las estaciones de carga de automóviles eléctricos en Rusia para mostrar mensajes ofensivos a Putin.

1 de marzo
Filtración de casi todas las comunicaciones internas, código fuente y planes operativos de Conti. El equipo de ransomware ruso TheRedBanditsRU se deslindó.

Foto: Freepik