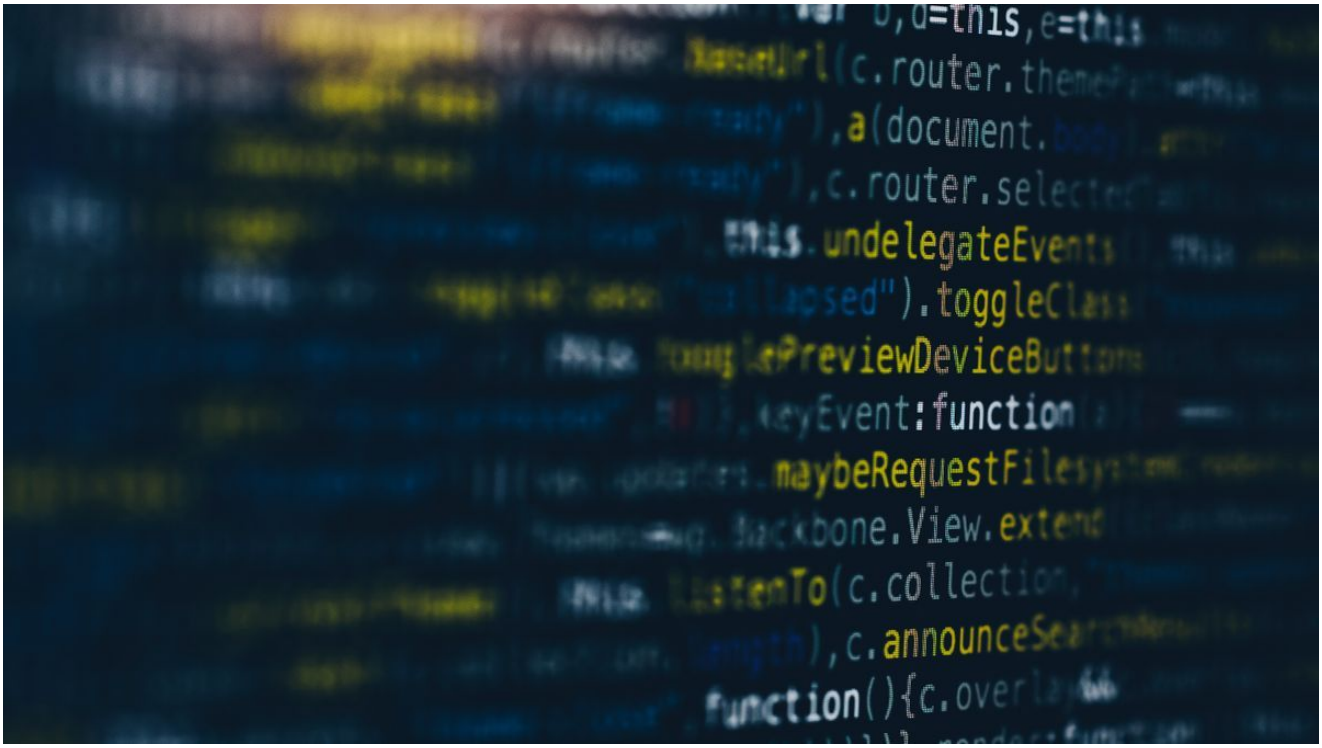
Capos del cibercrimen avisan de que “contratacarán” si se hackea a Rusia

eldiario.es/tecnologia/capos-cibercrimen-avisan-contratacaran-si-hackea-rusia_1_8795458.html

Carlos del Castillo March 2, 2022



Código informático. Markus Spiske | Unsplash

La guerra entre Rusia y Ucrania es una de las primeras que se libra abiertamente por tierra, mar, aire y ciberespacio. Apoyando a los ucranianos hay numerosas *brigadas internacionales digitales* que, con la careta de Anonymous o sin ella, se han lanzado a boicotear objetivos rusos como ferrocarriles o fábricas de armas. Al otro lado se han situado algunos de los más famosos capos del cibercrimen ruso.

El punto débil de Europa ante Rusia que está muy lejos de Ucrania: miles de kilómetros de cables submarinos

Saber más

“Utilizaremos todas nuestras capacidades para tomar medidas de represalia en caso de que los belicistas occidentales intenten atacar infraestructuras críticas en Rusia o en cualquier región de habla rusa del mundo”, ha avisado la mafia de cibercriminales Conti Team. “Usaremos nuestros recursos para contraatacar si el bienestar y la seguridad de los ciudadanos pacíficos están en juego”, añaden en una suerte de comunicado oficial publicado en la *deep web*.

Conti es uno de los grupos más activos y peligrosos de la industria del cibercrimen. Es un operador especializado de *ransomware*, un ataque informático que inutiliza los archivos informáticos del objetivo y le exige un rescate para recuperarlos. Una de sus armas es Ryuk, el virus que tumbó múltiples empresas e instituciones públicas españolas en 2020 y 2021, como el SEPE o el Ministerio de Trabajo.

Antes de que Vladímir Putin invadiera Ucrania, este tipo de posicionamientos era casi inaudito. Sin embargo, desde el comienzo de la guerra los analistas de ciberseguridad ven como declaraciones como estas se suceden, especialmente entre grupos de *ransomware*

como Conti. Todas ellas son organizaciones altamente profesionalizadas que venden estos ataques como un servicio para el que pueda pagarlo y se cree que operan desde territorio ruso.

Su salida en defensa del Kremlin tiene poco que ver con el patriotismo. De hecho, Conti ha expresado que no apoya la guerra. Pero como cualquier mafia, intentará defender el ecosistema donde gana dinero. “Muchísimos grupos de cibercriminales han tenido el beneplácito para operar desde Rusia, que siempre ha hecho la vista gorda”, explica a elDiario.es José Lancharro, director de BlackArrow, la división de servicios ofensivos y defensivos de la firma española de ciberseguridad Tarlogic.

A cambio de que el Kremlin mire para otro lado, estas mafias no atacan objetivos en territorio ruso o en su zona de influencia. “Muchos grupos muy conocidos han operado a sus anchas desde Rusia gracias a una especie de pacto de no agresión. Los *malware* que utilizan están programados para detectar si la máquina comprometida utiliza un lenguaje de la antigua Unión Soviética y, si es así, no la atacan”, revela este experto.

Rusia solo actúa contra estos grupos en casos extremos como el que se dio el pasado verano, cuando Joe Biden llamó directamente a Putin para exigirle que parara los pies a uno de ellos si no quería que interviniera él. Esta situación ha creado una relación de intereses comunes entre el Kremlin y muchas mafias del cibercrimen, aunque “no están bajo control del Gobierno ruso, que tiene otros equipos de ciberataque que sí financia y dirige directamente”, destaca Lancharro.

¿Creíble?

Desde BlackArrow han identificado otros cuatro conocidos grupos de ciberdelincuentes que han anunciado que defenderán los intereses del Kremlin. Sus nombres son Cooming Project, SandWorm, CyberGhost y Free Civilian. Teniendo en cuenta que vienen de mafias, que se producen en medio de una guerra abierta y con el juego de sombras y contrainteligencia que caracteriza a la *deep web*, ¿son creíbles estos posicionamientos?

Todos los especialistas consultados por este medio aseguran que hay que tomárselos muy en serio. “Hay que estar atentos porque lo pueden hacer. No es una amenaza vacía”, expone Igor Unanue, jefe de Tecnología de la española S21Sec. “Tiene muchos visos de veracidad. Por el sitio donde lo han publicado (el foro donde los cibercriminales comunican sus acciones) y porque no es un caso aislado sino varios grupos”, coincide Eusebio Nieva, director técnico de Check Point.

“Estamos en un contexto de guerra y vemos muchas campañas orientadas a desinformar, por lo que siempre hay que cogerlo con pinzas. Pero nosotros le damos veracidad a que se están movilizando porque ya existen datos concretos sobre acciones en las que estos grupos están en el ajo”, añade Lancharro, de BlackArrow.

Otro de los motivos que apoyan la tesis de que algunas mafias se están posicionando para defender a Rusia es que hacerlo les convierte en un objetivo del bando enemigo. Es decir, no tolerarían que alguien lo hiciera en su nombre sin desmentirlo. A Conti su declaración de apoyo a Moscú le ha salido cara, puesto que poco después de hacerla ha sufrido una filtración interna como venganza. Sus intentos de extorsión a sus víctimas de los dos últimos años han sido publicados en la *deep web*, con todas las conversaciones y detalles de sus delitos. Los analistas creen que puede haber sido un miembro descontento con el posicionamiento de su banda, o bien de hackers contrarios a la invasión rusa de Ucrania.

Batalla desigual

Si bien capos tan importantes como los de Conti se han posicionado a favor del Gobierno ruso, están en minoría frente a los grupos de hackers que están operando a favor de los intereses de Ucrania. En cualquier caso, las listas de adhesiones son difusas. Los expertos apuntan que sería lógico que la mayoría de grupos estén actuando en secreto o mediante la identidad colectiva Anonymous, lo que les permite no convertirse en un objetivo a atacar como le ha pasado a Conti.

En el ciberespacio los rusos están en minoría, pero eso no iguala la contienda. Desde BlackArrow destacan que las bandas del cibercrimen ruso están muy bien organizadas en comparación con los grupos descentralizados que se colocan la máscara de Anonymous. Además tienen acceso a malware muy avanzado gracias a su negocio. El último, un virus altamente destructivo que se ha detectado por primera vez en sistemas informáticos ucranianos tras la invasión, y que básicamente destruye todo lo que contengan sin posibilidad de recuperarlos, con rescate o sin él.

> Leaked document from Russian troops showing war against Ukraine was approved on 18th January, and initial plan to seize Ukraine starting 20th Feb to 06th March pic.twitter.com/4zsZD9i0R4
>
> — Anonymous (@YourAnonNews) 2 de marzo de 2022

Según Check Point, los ciberataques contra Ucrania han aumentado un 196% desde el inicio de la guerra, por solo un 4% aquellos que sufre Rusia. Eso no significa que estos últimos sean de fogueo. En los últimos días objetivos como el principal fabricante de armas bielorruso, el sistema de ferrocarriles ruso o múltiples instituciones públicas del Kremlin han caído víctimas de ciberataques. También se han producido filtraciones de información confidencial del ejército ruso.

El último blanco de los hackers que actúan a favor de Ucrania ha sido Roscosmos, la Agencia Espacial Rusa. El entorno de Anonymous ha reivindicado una ofensiva exitosa contra su centro de control este miércoles, lo que habría paralizado sus satélites. El director

de Roscosmos lo ha negado, avisando de que si se detectan vínculos entre un ciberataque contra esta infraestructura y un gobierno extranjero, lo considerarán una declaración de guerra.

Etiquetas

- /
- Tecnología
- /
- Crisis Ucrania
- /
- Ciberataques
- /
- Ciberguerra
- /
- Rusia