El grupo de hacking denominado UNC2165, que comparte numerosas superposiciones con un grupo de ciberdelincuencia con sede en Rusia conocido como Evil Corp, se ha relacionado con múltiples intrusiones de ransomware LockBit en un intento de eludir las sanciones impuestas por el Tesoro de Estados Unidos en diciembre de 2019.

> *«Estos actores han dejado de utilizar variantes exclusivas de ransomware para LockBit, un conocido ransomware como servicio (RaaS), en sus operaciones, lo que probablemente obstaculice los esfuerzos de atribución para evadir sanciones»,* dijo la compañía de inteligencia de amenazas Mandiant.

Activo desde 2019, se sabe que Unc2165 obtiene acceso inicial a las redes de las víctimas por medio de credenciales robadas y un malware de descarga basado en JavaScript llamado fakeUpdates (también conocido como SocGholish), aprovechándolo para implementar previamente el ransomware Hades.

Hades es el trabajo de un grupo de hacking con motivación financiera llamado Evil Corp, que también recibe los apodos de Gold Drake e Indrik Spider, y se ha atribuido al troyano Dridex (también conocido como Bugat), así como a otras cepas de ransomware como BitPaymer, DoppelPaymer, WastedLocker, Phoenix, PayloadBIN, Grief y Macaw en los últimos cinco años.

El giro de UNC2165 de Hades a LockBit como táctica para eludir sanciones parece haber comenzado a principios de 2021.

FakeUpdates también sirvió, en el pasado, como vector de infección inicial para distribuir Dridex, que después se usó como un conducto para colocar BitPaymer y DoppelPaymer en sistemas comprometidos.

Mandiant dijo que notó más similitudes entre UNC2165 y una actividad de ciberespionaje conectada con EvilCorp rastreada por la compañía suiza de seguridad cibernética PRODAFT bajo el nombre de SilverFish, dirigida a entidades gubernamentales y compañías Fortune 500 en la UE y Estados Unidos.

A un compromiso inicial exitoso le sigue una serie de acciones como parte del ciclo de vida de lataque, que incluyen la escalada de privilegios, el reconocimiento interno, el movimiento lateral y el mantenimiento del acceso remoto a largo plazo, antes de entregar las cargas de ransomware.

Debido a que las sanciones se utilizan cada vez más como un medio para frenar los ataques de ransomware, lo que a su vez impide que las víctimas negocien con los actores de amenaza, agregar un grupo de ransomware a una lista de sanciones, sin nombrar a las personas detrás de él, también se ha complicado por el hecho de que los sindicatos de hackers por lo general tienden a cerrar, reagruparse y renombrarse con un nombre distinto para eludir la aplicación de la ley.

> *«La adopción de un ransomware existente es una evolución natural para que UNC2165 intente ocultar su afiliación con EvilCorp. Las sanciones no son un factor limitante para recibir pagos de las víctimas»,* dijo Mandiant.

> *«El uso de este RaaS permite que UNC2165 se mezcle con otros afiliados. Es plausible que los actores detrás de las operaciones de UNC2165 sigan tomando medidas adicionales para distanciarse del nombre Evil Corp»,* dijo la compañía.

Los hallazgos de Mandiant, que está en proceso de ser adquirido por Google, son particularmente significativos ya que el grupo de ransomware LockBit alegó desde entonces que había violado la red de la compañía y robado datos confidenciales.

El grupo, más allá de amenazar con publicar *«todos los datos disponibles»* en su portal de fuga de datos, no especificó la naturaleza exacta del contenido de esos archivos. Sin embargo, Mandiant dijo que no hay evidencia para respaldar el reclamo.

> *«Mandiant revisó los datos revelados en el lanzamiento inicial de LockBit. Según los datos que se publicaron, no hay indicios de que se haya divulgado los datos de Mandiant, sino que el actor parece estar tratando de refutar la investigación de Mandiant del 2 de junio de 2022 sobre UNC2165 y LockBit»,* dijo la compañía.