businessinsider.es

Ryuk, el ransomware detrás del ataque al SEPE: qué ha fallado

Alberto R. Aguiar

11-15 minutos

Ni citas, ni web, ni sistemas: los profesionales del Servicio Público de Empleo ya saben lo que es **trabajar en una organización bajo ciberataque.** El SEPE sufrió ayer un incidente con *ransomware* que les ha obligado a suspender y a retrasar citas con los usuarios, y a atender con papel y boli a muchos demandantes de empleo.

La noticia la adelantó *Vozpópuli* a mediodía, después de que se detectara que tanto la web como la plataforma del SEPE estaban caídas.

El propio organismo público reconoció incidencias en su perfil de Twitter. Fuentes del Ministerio de Trabajo **han confirmado** a *Business Insider España* que el incidente es por **un ataque con Ryuk**, una de las familias de *ransomware* más prevalentes de los últimos años.

El código fuente de la web del SEPE dispara las dudas sobre la capacidad del organismo público de recuperarse del ciberataque

Uno de los más prevalentes gracias a que sus operadores

lo saben utilizar bien. En la 'industria' de los ciberdelincuentes hay desarrolladores que crean código malicioso y lo venden al mejor postor. Y siempre hay quienes los mejoran **para hacerlos más indetectables** o incluso para ser capaces de propagarse más rápido: hace apenas unos días *BleepingComputer* advertía que una nueva variante de este *ransomware* era capaz de moverse lateralmente entre dispositivos conectados por una LAN con Windows.

Precisamente el director general del SEPE confirmaba en *Cadena Ser* que el ataque solo había afectado **a los datos compartidos de Windows**, y no a todo el sistema informático ni el sistema de gestión de nóminas. Por lo que podría tratarse de esta nueva 'cepa' del *ransomware*.

Frente a esos movimientos laterales ya existen 'vacunas' desarrolladas por compañías españolas y por el propio Centro Criptológico Nacional, como Microclaudia, que hace creer a los *ransomware* que cuando han infectado un ordenador ya han infectado a todo el sistema para que dejen de propagarse.

Cómo ha atacado Ryuk al SEPE

Ryuk se ha convertido así en una de las mayores amenazas para las empresas de todo el mundo. Solo en España ha golpeado en varias ocasiones y lo ha hecho fuerte: estuvo detrás de un ataque al Ayuntamiento de Jerez o de otro a Prosegur a finales de 2019, cuando **se solía distribuir a través de Emotet**, un troyano bancario

que se ha convertido en todo un distribuidor de código malicioso.

Este *ransomware*, que ha golpeado en el SEPE provocando el primer gran incidente informático en España —que trasciende— en lo que va de 2021, **también se distribuía mediante una *botnet*** —un enjambre de bots, dispositivos y ordenadores vulnerables que se han convertido en parte de una especie de ejército de 'zombies'— llamada Trickbot, que ha sido recientemente desmantelada.

"Está **en el podio de los *ransomware* más utilizados**", explica Eusebio Nieva, director técnico de **Check Point** para España y Portugal. En declaraciones a *Business Insider España*, José Rosell, socio director de **S2 Grupo**, confirma que detrás de Ryuk puede haber grupos muy organizados.

"En determinados sitios **se pueden comprar paquetes para lanzar campañas de *ransomware*** y entre los clientes de ese *ransomware-as-a-service* puede haber colectivos de delincuentes bien organizados o muy chapuceros", concluye.

Ryuk, que se identificó por primera vez en agosto de 2018 según recuerda Daniel Creus, analista del Equipo de Investigación y Análisis de Kaspersky, no siempre responde a un ataque dirigido. En otras palabras: el ataque al SEPE puede haber sido fortuito. O no. Basta con que algún empleado haya pinchado donde no debía en un correo malicioso, y que los sistemas no estuviesen

debidamente protegidos. **Así surgen las tormentas perfectas.**

Siempre pide un rescate económico

Gerardo Gutiérrez, el director general del SEPE, avanzó este martes en la *Cadena Ser* que no se había pedido ningún rescate y **que no se había comprometido ningún dato.** "Los datos de confidencialidad están totalmente asegurados". "La prestación por desempleo se está pagando y se seguirá abonando", enfatizó.

Microsoft sufre un ciberataque que ya investiga la Casa Blanca: más de 20.000 compañías se han visto afectadas por un 'hackeo' al software del servidor de correo

Aunque el SEPE desmiente cualquier solicitud de rescate, la naturaleza de este tipo de incidentes suele ser siempre la misma: el código malicioso infecta un ordenador del sistema que se ha convertido en el objetivo de los ciberdelincuentes. Una vez se propaga, el código se activa y comienza a encriptar todos los archivos del sistema**, para hacer los equipos inutilizables.** Después, se exige un rescate económico, generalmente en criptomonedas, para que la víctima pague si quiere recobrar la normalidad.

Proofpoint, otra firma de ciberseguridad que también trabaja en España, ha asegurado que el 41% de las empresas españolas que sufrieron ciberataques el año

pasado se negaron a pagar un rescate, lo que supone superar holgadamente la media global de este tipo de incidentes. En el mundo, cuando una firma sufre un incidente de estas características, solo el 31% accede a pagar el rescate que exigen las mafias digitales.

"Es fundamental **evaluar el riesgo frente a la recompensa** en estas situaciones, aparte de considerar otras alternativas", defiende el director general de Proofpoint en España, Fernando Anaya.

Un posible ataque dirigido

Precisamente por cómo navegan en la red los *ransomware*, estos pueden distribuirse mediante *botnets* o troyanos bancarios que tratan de engañar a usuarios para que **pinchen en un enlace fraudulento.** Todo el mundo recibe correos en su bandeja de entrada que en realidad son parte de campañas masivas de *phishing* con enlaces maliciosos.

Pero que exista esa posibilidad no excluye que el ataque haya podido ser dirigido, recuerda Eusebio Nieva, de Check Point. "En muchas ocasiones los ataques de Ryuk pueden iniciarse con un *phishing* muy dirigido a una persona en concreto", incide el experto. **Una persona a la que habrán "estudiado" para conocer sus aficiones, sus relaciones personales, su rutina laboral.** Todo para llegar un correo lo más creíble posible.

Rosell, de S2 Grupo, precisa que los estudios de sus

investigadores destacan cómo en muchos casos los ataques con Ryuk se inician "un viernes a final de mes". En ocasiones, el *ransomware* puede estar latente, *durmiendo* en un sistema informático esperando para ser activado. Y el viernes a final de mes es una fecha clave "porque **es cuando una empresa tiene que pagar nóminas** o hacer facturas".

Este tipo de códigos maliciosos tratan de hacer el mayor daño posible precisamente para encontrarse con una víctima desesperada a la que no le queda otra que acceder a pagar el rescate que pidan.

Nieva continúa: "Ryuk es uno de los ataques con *ransomware* más prevalentes, más utilizados, y en general, aunque no se puede generalizar, suele ser indicativo de que **ha sido un ataque premeditado".**

Demandantes, empresas: qué datos están en peligro

Gerardo Gutiérrez, director general del SEPE, insiste en que no se ha visto comprometido ningún dato confidencial o personal ni de demandantes de empleo ni de empresas.

Pero como recuerda Nieva, "a día de hoy es tendencia que los ataques con *ransomware* hagan lo que se conoce como doble extorsión". La primera extorsión es pedir un rescate si la víctima quiere recobrar el control y la normalidad en sus sistemas informáticos. La segunda

extorsión es exigir el rescate porque, de lo contrario, **los ciberdelincuentes filtrarán todos los datos que hayan robado** en el ataque.

Los chantajes con datos robados durante ciberataques de *ransomware* es una tendencia que se vaticinó en 2019 y se acabó confirmando en 2020. Así, Adif vio cómo se volcaron más de 100 gigas en datos de la compañía en las redes. Varios expertos y analistas de seguridad especializados en vigilar a *ransomware* han visto cómo en la *dark web* muchos de estos operadores publicitan sus *hazañas* e incluso comparten pruebas de los datos que han conseguido usurpar.

De Adif a Mapfre: los ataques con 'ransomware' cuestan al menos 100 millones de euros al año a las empresas españolas

Brett Callow, analista en Emsisoft, explica a *Business Insider España* que detrás de Ryuk suele haber dos colectivos operándolo. Ninguno tiene una página web en la *dark net*. "El grupo principal, el originario, no roba información. **El grupo secundario sí ha robado datos en alguna ocasión** pero no los filtran en su propia página, los cuelgan en foros de ciberdelincuentes aleatoriamente".

Para saber si realmente hay datos en peligro es necesario conocer más detalles del incidente. Nieva calcula que dependiendo de qué infraestructuras informáticas se han visto afectadas, la recuperación del incidente puede demorarse varios días. Lo habitual es que las

organizaciones que se vean atacadas de esta manera recurran, si no pagan el rescate —algo que se desaconseja enérgicamente—, **a copias de seguridad.** Luis Corrons, experto de seguridad de Avast, también habla de "una semana" para recuperar la normalidad.

"Aunque no tenemos la imagen completa, el hecho de que las operaciones de las oficinas se detuvieran y los servicios como el sitio web del SEPE cayeran, hace pensar que los atacantes tuvieron acceso a la mayor parte de su infraestructura", destaca Corrons.

Cuando se produce un ataque a gran escala como este quiere decir que los atacantes "ya llevaban un tiempo dentro de la red, comprometiendo la mayoría de los sistemas de la organización", inciden desde Avast.

Un ataque como este paraliza por completo el proceso de trabajo del SEPE, lo que agravará aún más el estado de colapso que vive la institución debido a la avalancha de archivos que debe gestionar desde el inicio de la pandemia. Cuando se produce un ataque a gran escala como este quiere decir que los atacantes ya llevaban un tiempo dentro de la red, comprometiendo la mayoría de los sistemas de la organización.

Sin embargo Rosell sí advierte de **los efectos "catastróficos"** que puede tener un ataque con *ransomware*. No se han visto en toda su magnitud porque afortunadamente siempre se han evitado los males mayores, pero el socio director de S2 Grupo recuerda

casos muy mediáticos como el WannaCry de Telefónica en 2017 o el NotPetya que afectó a Maersk un año después.

O un hospital. En España ha habido casos de hospitales que no han podido operar con normalidad debido a que sus sistemas informáticos estaban caídos. En Alemania murió una mujer después de que le pospusiesen una operación por este motivo.

Qué ha fallado en la seguridad del SEPE

Hackers y especialistas españoles como Marc Almeida han llamado la atención en redes sociales por lo ilustrativa que puede ser la página web del SEPE.

> #Detalles, es solo un número y es solo en el banner de mantenimiento, pero por ahí se empiezan a dar pistas.#SEPEdown pic.twitter.com/n8RpB9WTzm
>
> — Marc Almeida #sigoEnCasa (@cibernicola_es) March 9, 2021

"Es anecdótico", considera Nieva, de Check Point. El experto cree que, más que no haya habido un mantenimiento adecuado de la seguridad informática, lo que revela el pantallazo que comparte Almeida en Twitter es que el SEPE ha tenido "falta de previsión".

"Al final todo **esto es una cuestión de concienciar a los usuarios**", reivindica Rosell, de S2 Grupo. "A pesar de que desde el punto de vista de la seguridad se haga mucho, evidentemente no deja de existir el riesgo de que

al abrir el anexo de un correo que no se debía haber abierto te entre un *bicho*".

Una de las máximas en la industria de la ciberseguridad es mantener los equipos actualizados siempre. Pero los sistemas de administraciones gigantescas como puede ser el Servicio de Empleo no siempre cuenta con los equipos a la última. El cliché siempre vuelve, y es habitual ver en diversas instituciones a funcionarios trabajando con sistemas operativos que ya no cuentan con soporte, **como Windows XP.**

"Pero eso no pasa únicamente en las administraciones públicas", se detiene Rosell. "Te puedes ir a ver sistemas de control industrial que se utilizan con un programa específico antiguo y con un sistema operativo antiguo". "El personal que se encarga de gestionarlo **tiene miedo de cambiar el programa** porque igual deja de funcionar la maquinaria, porque el fabricante que lo montó hace 15 años ha desaparecido o se ha dejado de tener relación con ellos".

Es "un mal endémico" que va mucho más allá de no actualizar el sistema operativo. "Evidentemente, las organizaciones tenemos que hacer mucho más en materia de seguridad", reconoce. "Pero **el que esté libre de riesgo que levante la mano.** No conozco a ninguno. Todos estamos preocupados". Solo que, "cuanto más inviertes en concienciación y seguridad", "menos riesgo tienes".