20minutos.es

Así es Ryuk, el virus que tiene en jaque al Ministerio de Trabajo: este malware ya fue responsable del ciberat

Marta Gascón

4-5 minutos

El Ministerio de Trabajo y Economía Social se ha visto afectado este miércoles por un ataque informático, según ha informado el propio organismo a través de su cuenta de Twitter.

Tras constatar que se trataba de un ciberataque, los técnicos han establecido los cortafuegos correspondientes, con el fin de evitar más daños. Precisamente, esos profesionales están evaluando los daños y el alcance de la amenaza, que **parece que no tendrá graves consecuencias**.

> ⚠ El Ministerio de Trabajo y Economía Social se ha visto afectado por un ataque informático. Los responsables técnicos del Ministerio y del Centro Criptológico Nacional están trabajando de manera conjunta para determinar el origen y restablecer la normalidad lo antes posible.

> — Ministerio Trabajo y Economía Social (@empleogob) June 9, 2021

Según apuntan los expertos, **detrás de este ataque se encuentra Ryuk, un viejo conocido del ministerio**: fue también el responsable del ciberataque al Servicio Público de Empleo Estatal (SEPE) el pasado mes de marzo, que dejó sus sistemas inoperativos durante semanas.

El malware Ryuk realiza ciberataques de ransomware, muy comunes hoy en día, pero la clave está en su sofisticación: es un tipo de virus que funcionan como producto empresarial con el que posteriormente lanzan campañas. La peligrosidad reside en la profundidad del ataque. “Normalmente explotan las vulnerabilidades que tiene bien explotadas y saben que funcionan bien, hasta el punto de no saber qué es lo que van a encontrar”, explica Chema Cuadrado, especialista en ciberseguridad en Hiberus.

Se aloja en la infraestructura de la empresa u organización a la que ataca y se queda ahí “el tiempo necesario” para conseguir “escalar privilegios (paso lateral) y/o **posiblemente robo de información**”, explica Cuadrado.

Una vez el atacante obtiene los permisos para operar a su antojo, **lanza el ataque e infecta y encripta todos los sistemas**, exigiendo el pago de un rescate para restablecer su funcionamiento.

Este virus informático apareció en agosto de 2018 y

detrás de él podría estar **un grupo de cibercriminales rusos llamado Grim Spider** que se dedica a lo que en el sector se conoce como 'Big Game Hunting', es decir, su objetivo -su 'caza'- son administraciones públicas o grandes organizaciones y corporaciones.

En el ataque al SEPE aparecieron ficheros .ryuk, por lo que no hubo dudas sobre su autoría. El Ministerio de Trabajo deberá confirmar si ha ocurrido lo mismo en esta ocasión.

Según el experto, cuando se produce un ciberataque a gran escala como este quiere decir que "**los atacantes ya llevaban un tiempo dentro de la red**", es decir, que podrían haber estado meses recabando información y esperando pacientes a colapsar toda la organización.

No es la primera vez que Ryuk ataca a algún organismo público en España -ni fuera de ella-. En la lista de víctimas se encuentran el Ayuntamiento de Jerez o la Cadena SER en nuestro país. De hecho, en octubre de 2020, el FBI estimaba que las víctimas han pagado más de 61 millones de dólares para recuperar archivos cifrados por este virus. La mayoría de ese dinero ha sido reclamado en Bitcoin "para que rastrear las transacciones sea más difícil", apunta Cuadrado.

Conforme a los criterios de