Una vulnerabilidad crítica recientemente revelada en el utilizado Oracle WebLogic Server, se ha visto ampliamente explotada para la distribución de una variante de ransomware nunca antes vista, que los investigadores denominaron como *«Sodinokibi»*.

La semana pasada publicamos un artículo referente a una vulnerabilidad de ejecución remota de código de deserialización crítica en Oracle WebLogic Server que podría permitir a los atacantes ejecutar de forma remota comandos arbitrarios en los servidores afectados simplemente enviando una solicitud HTTP especialmente diseñada, sin necesidad de autorización.

Para abordar esta vulnerabilidad (CVE-2019-2725), que afectó a todas las versiones del software Oracle WebLogic y recibió una puntuación de criticidad de 9.8 sobre 10, Oracle lanzó una actualización de seguridad fuera de banda el pasado 26 de abril.

Según los investigadores de seguridad cibernética del equipo de investigación de amenazas de Cisto Talos, un grupo desconocido de hackers ha explotado dicha vulnerabilidad desde al menos el 25 de abril para infectar servidores vulnerables con una nueva pieza de ransomware.

Sodinokibi es una peligrosa variante de ransomware que ha sido diseñada para cifrar archivos en el directorio de un usuario y luego eliminar las copias de seguridad de instantáneas del sistema con el fin de evitar que las víctimas recuperen sus datos sin pagar un rescate.

No se requiere interacción para implementar ransomware

Dado que los atacantes están aprovechando una vulnerabilidad de ejecución remota de código en el servidor WebLogic, a diferencia de los ataques de ransomware típicos, la implementación del ransomware Sodinokibi no requiere la interacción del usuario.

> *«Históricamente, la mayoría de las variedades de ransomware han requerido algún*

> *tipo de interacción con el usuario, como que un usuario abra un archivo adjunto a un mensaje de correo electrónico, haga clic en un enlace malicioso o ejecute un malware en el dispositivo. En este caso, los atacantes simplemente aprovecharon la vulnerabilidad de Oracle WebLogic, lo que provocó que el servidor afectado descargue una copia del ransomware de las direcciones IP controladas por el atacante»,* dijeron los investigadores.

Cuando se descarga, el ransomware Sodinokibi cifra los sistemas de la víctima y muestra una nota de rescate que exige hasta $2,500 dólares en Bitcoin. La cantidad se duplica a $5,000 dólares si el rescate no se paga dentro de un número determinado de días, que puede variar de dos a seis.

Los hackers también están instalando el ransomware GrandCrab

Los investigadores también se dieron cuenta que aproximadamente ocho horas después de implementar Sodinokibi en un sistema, los atacantes explotaron la misma vulnerabilidad de WebLogic Server para instalar otra pieza de ransomware conocida como GrandCrab (v5.2).

> *«Nos parece extraño que los atacantes opten por distribuir ransomware adicional y diferente en el mismo objetivo. Sodinokibi es una nueva variante de ransomware, tal vez los atacantes sintieron que sus intentos anteriores habían sido infructuosos y sigues buscando cobrar al distribuir GrandCrab»,* dicen los investigadores.

Los atacantes han estado explotando la vulnerabilidad de Oracle WebLogic Server desde el 17 de abril aproximadamente, para distribuir mineros de criptomonedas y otros tipos de malware.

WebLogic Server es un popular servidor de aplicaciones empresariales multinivel basado en Java que las empresas utilizan para respaldar aplicaciones empresariales, lo que lo convierte en un objetivo frecuente de los atacantes que intentan realizar operaciones maliciosas, como

ejecutar mineros de criptomonedas e infectar con ransomware.

Las organizaciones que utilizan Oracle WebLogic Server deben asegurarse de actualizar sus instalaciones a la última versión del software tan pronto sea posible.