Una nueva cepa de ransomware escrita en Golang denominada «*Agenda*» fue detectada en la naturaleza, dirigida a entidades de salud y educación en Indonesia, Arabia Saudita, Sudáfrica y Tailandia.

> *«Agenda puede reiniciar los sistemas en modo seguro, intenta detener muchos procesos y servicios específicos del servidor y tiene múltiples modos para ejecutarse»,* dijeron los investigadores de Trend Micro.

Qilin, el grupo de hackers que anuncia el ransomware en la deep web, brinda a los afiliados opciones de personalizar las cargas binarias para cada víctima, lo que permite a los operadores decidir la nota de rescate, la extensión de cifrado, así como la lista de procesos y servicios antes de comenzar el proceso de encriptación.

Además, el ransomware incorpora técnicas para evadir la detección aprovechando la función de «*modo seguro*» de un dispositivo para seguir con su rutina de cifrado de archivos sin ser detectado, pero no sin antes cambiar la contraseña predeterminada del usuario y habilitar el inicio de sesión automático.

Después del cifrado exitoso, Agenda cambia el nombre de los archivos con la extensión configurada, suelta la nota de rescate en cada directorio cifrado y reinicia la máquina en modo normal. La cantidad de ransomware solicitada varía de una compañía a otra, oscilando entre 50,000 y 800,000 dólares.

Agenda, además de aprovechar las credenciales de la cuenta local para ejecutar el binario de ransomware, también cuenta con capacidades para infectar una red completa y sus controladores compartidos.

En una de las cadenas de ataque observadas relacionadas con el ransomware, un servidor

Citrix de cara al público sirvió como punto de entrada para implementar el ransomware en menos de dos días.

Trend Micro dijo que observó similitudes en el código fuente entre Agenda y las familias de ransomware Black Basta, Black Matter y REvil.

Se sabe que Black Basta, que surgió por primera vez en abril de 2022, emplea la técnica de doble extorsión de cifrar archivos en los sistemas de organizaciones objetivo y exigir un rescate para hacer posible el descifrado, al mismo tiempo que amenaza con publicar la información confidencial robada si una víctima decide no pagar el rescate.

Hasta la semana pasada, el grupo Black Basta comprometió a más de 75 organizaciones, según Unit42 de Palo Alto Networks, frente a las 50 de junio de 2022.

Agenda es también la cuarta variedad después de BlackCat, Hive y Luna en utilizar el lenguaje de programación Go.

> *«El ransomware continúa evolucionando, desarrollando métodos y técnicas más sofisticados para atrapar a las organizaciones»,* dijeron los investigadores.