Los actores de amenazas comenzaron a utilizar el servicio de mensajería instantánea P2P de Tox como un método de comando y control, marcando un cambio de su papel anterior como un método de contacto para las negociaciones de ransomware.

Los hallazgos de Uptycs analizaron un artefacto de formateo ejecutable y enlazable (ELF) «72client«, que funciona como un bot y puede ejecutar scripts en el host comprometido utilizando el protocolo Tox.

Tox es un protocolo sin servidor para comunicaciones en línea que ofrece protecciones de cifrado de extremo a extremo (E2EE) mediante el uso de la biblioteca de redes y criptografía (NaCL) para el cifrado y la autenticación.

> *«El binario que se encuentra en la naturaleza es un ejecutable simplificado pero dinámico, lo que facilita la descompilación. Todo el binario parece estar escrito en C y solo se ha vinculado estáticamente a la biblioteca c-toxcore»,* dijeron los investigadores Siddhart Sharma y Nischay Hedge.

Cabe mencionar que c-toxcore es una implementación de referencia del protocolo Tox.

La ingeniería inversa realizada por Uptycs muestra que el archivo ELF está diseñado para escribir un script de shell en la ubicación *«/var/tmp/»*, un directorio utilizado para la creación de archivos temporales en Linux, permitiendo ejecutar comandos para eliminar procesos relacionados con cripto mineros.

También se ejecuta una segunda rutina que le permite ejecutar una serie de comandos específicos (por ejemplo, nproc, whoami, machine-id, etc.) en el sistema, cuyos resultados se envían posteriormente por medio de UDP a un destinatario de Tox.

Además, el binario cuenta con capacidades para recibir distintos comandos por medio de Tox, según los cuales el escript de shell se actualiza o se ejecuta de forma ad-hoc. Un comando de *«salir»* emitido cierra la conexión Tox.

Históricamente, los atacantes de ransomware utilizan Tox como un mecanismo de comunicación, pero el último desarrollo marca la primera vez que el protocolo se utiliza para ejecutar scripts arbitrarios en una máquina infectada.

> *«Aunque la muestra discutida no hace nada explícitamente malicioso, creemos que podría ser un componente de una campaña de minería de monedas. Por lo tanto, se vuelve importante monitorear los componentes de la red involucrados en las cadenas de ataque»,* dijeron los investigadores.

La divulgación llega en medio de informes de que la solución de sistema de archivos descentralizado conocida como IPFS se utiliza cada vez más para alojar sitios de phishing en un esfuerzo por dificultar los derribos.