Debido a que las infecciones de ransomware han evolucionado desde el cifrado puro de datos hasta esquemas como la extorsión doble y triple, es probable que un nuevo vector de ataque prepare el escenario para futuras campañas.

El ransomware para IoT denominado R4IoT por Forescout, es un *«ransomware novedoso de prueba de concepto que explota un dispositivo IoT para obtener acceso y moverse lateralmente en una red de TI e impactar la red OT».*

Este pivote potencial se basa en el rápido crecimiento en la cantidad de dispositivos IoT, así como en la convergencia de las redes TI y OT en las organizaciones.

El objetivo final de R4IoT es aprovechar los dispositivos IoT expuestos y vulnerables, como las cámaras IP, para obtener un punto de apoyo inicial, seguido de la implementación de ransomware en la red de TI, y el aprovechamiento de las malas prácticas de seguridad operativa para mantener como rehenes los procesos de misión crítica.

> *«Al comprometer los activos de IoT, TI y OT, R4IoT ve más allá del cifrado habitual y la exfiltración de datos para causar la interrupción física de las operaciones comerciales»,* dijeron los investigadores.

En otras palabras, R4IoT es un nuevo tipo de malware que reúne un punto de entrada de IoT y el movimiento lateral y el cifrado relacionados con el ransomware en una red de TI, lo que provoca un impacto extendido tanto en las redes de TI como en las redes de OT.

Es un escenario hipotético, esto podría implicar comprometer una máquina en la red corporativa no solo para eliminar ransomware, sino también para recuperar cargas útiles adicionales de un servidor remoto para implementar mineros de criptomonedas y lanzar ataques de denegación de servicio (DoS) contra activos de OT.

Para mitigar tanto la probabilidad como el impacto de posibles incidentes de R4IoT, se recomienda a las organizaciones que identifiquen y apliquen parches a los dispositivos vulnerables, hagan cumplir la segmentación de la red, implementen políticas de contraseñas seguras y supervisen las conexiones HTTPS, las sesiones FTP y el tráfico de la red.

> *«El ransomware ha sido la amenaza más frecuente de los últimos años, y hasta ahora, ha aprovechado principalmente las vulnerabilidades en los equipos de TI tradicionales para paralizar a las organizaciones»*, agregaron los investigadores.

> *«Pero las nuevas tendencias de conectividad agregaron una cantidad y una diversidad de dispositivos OT e IoT que han aumentado el riesgo en casi todos los negocios».*