El grupo de piratas informáticos detrás de los ataques de ransomware BitPaymer e iEncript, explota una vulnerabilidad de día cero que afecta a un componente poco conocido que viene incluido con el software iTunes e iCloud de Apple para Windows.

El componente vulnerable es el actualizador Bonjour, una implementación de configuración cero del producto de comunicación de red que funciona silenciosamente en segundo plano y automatiza distintas tareas de red de bajo nivel, incluida la descarga automática de futuras actualizaciones para el software de Apple.

Debido a que el actualizador Bonjour se instala como un prorgama separado en el sistema, la desinstalación de iTunes e iCloud no elimina Bonjour, por lo que finalmente se queda instalado en muchas computadoras con Windows, sin actualizar y ejecutándose silenciosamente en segundo plano.

Investigadores de seguridad cibernética de Morphisec Labs, descubrieron la explotación de la vulnerabilidad Zero Day de Bonjour en agosto, cuando los hackers atacaron una empresa no identificada en la industria automotriz con el ransomware BitPaymer.

El componente Bonjour se consideró vulnerable a la falla de ruta de servicio no citada, una vulnerabilidad de software común que ocurre cuando la ruta de un ejecutable contiene espacios en el nombre del archivo y no está encerrada entre comillas.

La vulnerabilidad de ruta de servicio no citada puede explotarse plantando un archivo ejecutable malicioso en la ruta principal, engañando a aplicaciones legítimas y confiables para que ejecuten programas maliciosos para mantener la persistencia y evadir la detección.

> *«En este escenario, Bonjour estaba tratando de ejecutarse desde la carpeta Archivos de programa, pero debido a la ruta sin comillas, en su lugar ejecutó el ransomware BitPaymer ya que se llamó Program. Como muchas soluciones de detección se basan en la supervisión del comportamiento, la cadena de ejecución del proceso juega un papel importante en la fidelidad de la alerta. Sin un proceso*

> *legítimo firmado por un proveedor conocido ejecuta un nuevo proceso hijo malicioso, una alerta asociada tendrá un puntaje de confianza más bajo que si el padre no estuviera firmado por un proveedor conocido. Dado que Bonjour está firmado y es conocido, el adversario usa esto para su ventaja»*, dicen los investigadores.

Además de escapar de la detección, en algunos casos, la vulnerabilidad de ruta de servicio no citada también puede ser abusada para escalar privilegios cuando el programa vulnerable tiene los derechos para ejecutarse con privilegios más altos.

Sin embargo, en este caso, el día cero de Bonjour no permitió que el ransomware BitPaymer obtuviera derechos de SISTEMA en las computadoras infectadas. Pero si permitió que el malware evadiera soluciones de detección comunes que se basan en la supervisión del comportamiento porque el componente Bonjour parece un proceso legítimo.

Inmediatamente después de descubrir el ataque, los investigadores de Morphisec Labs compartieron responsablemente los detalles del ataque con Apple, quien ayer lanzó iCloud 10.7 para Windows, iCloud para Windows 7.14 y iTunes 12.10.1 para Windows.

Los usuarios de Windows que utilicen estas herramientas de Apple deberían actualizar inmediatamente para evitar problemas. Si ya has desinstalado las aplicaciones de Apple, deberías revisar que no tengas Bonjour instalado en el sistema.