Microsoft reveló el viernes una posible conexión entre el gusano basado en USB, Raspberry Robin, y un grupo ruso de hackers rastreado como Evil Corp.

La compañía dijo que observó que el malware FakeUpdates (también conocido como SocGholish) se entregaba por medio de infecciones existentes de Raspberry Robin el 26 de julio de 2022.

Se sabe que Raspberry Robin, también llamado QNAP Worm, se propaga desde un sistema comprometido por medio de dispositivos USB infectados que contienen archivos .LNK maliciosos a otros dispositivos en la red de destino.

La campaña, que fue detectada por primera vez Red Canary en septiembre de 2021, ha sido esquiva en el sentido de que no se ha documentado ninguna actividad posterior ni ha habido ningún vínculo concreto que la vincule a un actor o grupo de amenazas conocido.

La divulgación, por lo tanto, marca la primera evidencia de acciones posteriores a la explotación llevadas a cabo por el actor de amenazas al aprovechar el malware para obtener acceso inicial a una máquina con Windows.

> *«Desde entonces, la actividad FakeUpdates asociada con DEV-0206 en los sistemas afectados ha llevado a acciones de seguimiento que se asemejan al comportamiento previo del ransomware DEV-0243»,* dijo Microsoft.

DEV-0206 es el apodo de Redmond para un corredor de acceso inicial que implementa un marco de JavaScript malicioso llamado FakeUpdate al atraer a los objetivos para que descarguen actualizaciones de navegador falsas en forma de archivos ZIP.

El malware, en esencia, actúa como un conducto para otras campañas que hacen uso de este acceso comprado a DEV-0206 para distribuir otras cargas útiles, principalmente cargadores Cobalt Strike atribuidos a DEV-0243, que también se conoce como Evil Corp.

Conocido como Gold Drake e Indrik Spider, el grupo de hackers motivado financieramente ha motivado históricamente el malware Dridex y desde entonces cambió a la implementación en una serie de familias de ransomware a lo largo de los años, incluyendo la más reciente, LockBit.

> *«El uso de una carga útil RaaS por parte del grupo de actividad 'Evil Corp' es probablemente un intento de DEV-0243 de evitar la atribución a su grupo, lo que podría desalentar el pago debido a su estado sancionado»,* dijo Microsoft.

No está claro qué conexiones exactas pueden tener Evil Corp, DEV-0206 y DEV-0243 entre sí.

Katie Nickels, directora de inteligencia de Red Canary, dijo en un comunicado compartido con Masterhacks que los hallazgos, en caso de demostrar que son correctos, llenan un *«gran vacío»* con el modus operandi de Raspberry Robin.

> *«Seguimos viendo actividad de Raspberry Robin, pero no hemos podido asociarla con ninguna persona, empresa, entidad o país específico»,* dijo Nickels.

> *«En última instancia, es demasiado pronto para decir si Evil Corp es responsable o está asociada con Raspberry Robin. El ecosistema de Ransomware-as-a-Service (RaaS) es complejo, donde distintos grupos criminales se asocian entre sí para lograr una variedad de objetivos. Como resultado, puede ser difícil desenredar las relaciones entre las familias de malware y la actividad observada».*