La infraestructura de ataque utilizada para apuntar a Cisco en el incidente de mayo de 2022 también se empleó contra un intento de compromiso de un holding de soluciones de gestión de la fuerza laboral no identificado un mes antes en abril de 2022.

La compañía de seguridad cibernética Sentire, que reveló los hallazgos, planteó la posibilidad de que las intrusiones pudieran ser obra de un actor criminal conocido como mx1r, quien se dice que es miembro del grupo afiliado de Evil Corp denominado UNC2165.

Evil Corp, los creadores del troyano bancario Dridex, refinó su modo de operación a lo largo de los años para ejecutar una serie de operaciones de ransomware para eludir las sanciones impuestas por el Tesoro de Estados Unidos en diciembre de 2019.

El acceso inicial a la red de TI de la empresa fue posible mediante el uso de credenciales de red privada virtual (VPN) robadas, seguidas de herramientas estándar para el movimiento lateral y un acceso más profundo al entorno de la víctima.

> *«Usando Cobalt Strike, los atacantes pudieron obtener un punto de apoyo inicial y las acciones prácticas fueron inmediatas y rápidas desde el momento del acceso inicial hasta que el atacante pudo registrar su propia máquina virtual en la red VPN de la víctima»,* dijo eSentire.

Los vínculos de mx1r con UNC2165 provienen de la superposición de tácticas y técnicas con las de UNC2165, incluyendo la realización de un ataque de Kerberoasting contra el servicio de Active Directory y el uso del acceso de Protocolo de Escritorio Remoto (RDP) para propagarse dentro de la red de la empresa.

A pesar de las conexiones, se dice que la infraestructura «HiveStrike» de Cobalt Strike utilizada para montar el ataque coincide con la de un afiliado de ransomware Conti conocido antes por implementar las cepas Hive y Yanluowang, la última de las cuales publicó archivos robados de la brecha de Cisco a finales de mayo de 2022 a su sitio de fugas de datos.

El fabricante de equipos de red atribuyó el incidente a un agente de acceso inicial (IAB) con enlaces a tres colectivos diferentes: UNC3477, LAPSUS$ y el ransomware Yanluowang.

> *«Parece poco probable, pero no imposible, que Conti preste su infraestructura a Evil Corp. Es más plausible que la filial de Evil Corp/UNC2165 pueda estar trabajando con una de las nuevas subsidiarias de Conti»*, dijo eSentire

> *«También es posible que el acceso inicial haya sido negociado por una filial de Evil Corp, pero finalmente se vendió a los operadores de Hive y sus filiales»,* agregó.