12 personas fueron detenidas como parte de una operación internacional de aplicación de la ley por orquestar ataques de ransomware en infraestructura crítica y organizaciones grandes, que afectaron a más de 1800 víctimas en 71 países desde 2019.

Los arrestos se realizaron a inicios de la semana, el 26 de octubre en Ucrania y Suiza, lo que resultó en la incautación de efectivo por un valor de 52,000 dólares, cinco vehículos de lujo y una serie de dispositivos electrónicos que, según las agencias, están siendo examinados para descubrir nuevas pruebas forenses de sus actividades maliciosas y buscar nuevas pistas de investigación.

Los sospechosos se relacionaron principalmente con el ransomware LockerGoga, MegaCortex y Dharma, además de estar a cargo de lavar los pagos de rescate al canalizar los ingresos de Bitcoin a través de servicios de mezcla y luego cobrarlos.

> *«Los sospechosos seleccionados tenían diferentes roles en estas organizaciones criminales profesionales altamente organizadas. Algunos de estos delincuentes estaban lidiando con el esfuerzo de penetración, utilizando múltiples mecanismos para comprometer las redes de TI, incluidos ataques de fuerza bruta, inyecciones de SQL, credenciales robadas y correos electrónicos de phishing con archivos adjuntos maliciosos»*, dijo la Europol.

Después del exitoso allanamiento, se dice que los sospechosos se han centrado en el movimiento lateral dentro de las redes comprometidas mediante la implementación de malware como TrickBot o marcos, posteriores a la explotación como Cobalt Strike o PowerShell Empire, con el objetivo de permanecer sin ser detectados durante períodos prolongados y obteniendo un acceso arraigado, aprovechando la oportunidad de investigar más debilidades en las redes de TI antes de instalar ransomware.

También se cree que las personas arrestadas llevaron a cabo el ataque de ransomware contra el procesador de aluminio noruego Norsk Hydro en marzo de 2019, según informó el Servicio Nacional de Investigación Criminal del país en un comunicado separado.

El grupo de trabajo conjunto involucró a autoridades de Francia, Alemania, Países Bajos, Noruega, Suiza, Ucrania, el Reino Unido y Estados Unidos, junto con Europol y Eurojust, en el marco de la Plataforma Multidisciplinaria Europea contra las Amenazas Criminales (EMPACT).