Investigadores de seguridad descubrieron el código fuente completo del malware Carbanak. A veces denominado FIN7, Anunak o Cobalto, es uno de los programas maliciosos más peligrosas y con todas las funciones que pertenecen a un grupo de delincuentes cibernéticos de estilo APT que participa en distintos ataques contra bancos, instituciones financieras, hospitales y restaurantes.

En julio del año pasado, se corrió el rumor de que el código fuente de Carbanak fue filtrado al público, pero los investigadores de Kaspersky Lab confirmaron más tarde que el código filtrado no era del troyano Carbanak.

Ahora, los investigadores de seguridad cibernética de FireEye revelaron que encontraron el código fuente de Carbanak, los creadores y algunos complementos nunca antes vistos en dos archivos RAR, que se cargaron en el motor de escaneo de malware VirusTotal, hace dos años desde una dirección IP rusa.

> *«El código fuente de CARBANAK era de 20 MB y comprendía 755 archivos, con 39 binarios y 100,000 líneas de código. Nuestro objetivo era encontrar la inteligencia sobre amenazas que habíamos perdido en nuestros análisis anteriores»*, dijeron los investigadores.

Los investigadores tienen planes de lanzar una serie de artículos de 4 partes que detallan las características y el análisis de CARBANAK según su código fuente e ingeniería inversa.

Descubierto por primera vez en 2014 por Kaspersky Lab, Carbanak es uno de los ataques de malware más exitosos del mundo, lanzado por un grupo muy organizado que evolucionó constantemente en sus tácticas para llevar a cabo la ciberdelincuencia al tiempo que evita la detección por parte de posibles objetivos y las autoridades.

El grupo de hackers comenzó sus actividades hace casi seis años lanzando una serie de ataques de malware utilizando Anunak y Carbanak para comprometer a los bancos y las redes de cajeros automáticos del mundo, y así poder robar miles de millones de euros a más

de 100 bancos en todo el mundo.

Para comprometer a los bancos, los piratas informáticos enviaron correos electrónicos maliciosos de phishing a cientos de empleados en diferentes bancos, los cuales infectaron las computadoras con el malware Carbanak si se abrían, lo que permite a los atacantes transferir dinero de los bancos afectados a cuentas falsas o cajeros automáticos monitoreados por ellos.

Según las autoridades europeas, el grupo criminal más tarde desarrolló un sofisticado troyano bancario listo para el robo, llamado Cobalt, basado en el software de pruebas de penetración Cobalt-Strike, que estuvo en uso hasta 2016.

El grupo fue expuesto por primera vez en 2015 como delincuentes cibernéticos por motivos económicos, y tres sospechosos, Dmytro Fedorov, de 44 años, Fedir Hladyr, de 33 años y Andrii Kopakov, de 30 años, todos de Ucrania, fueron arrestados el año pasado en Europa entre enero y junio.

Los tres sospechosos, de los cuales se cree que Kopakov era el líder, fueron acusados por un total de 26 cargos de delitos graves en agosto de 2018.