Desmanteladas tres grandes redes de malware y bloqueados 41 millones en criptomonedas

Una operación internacional ha desmantelado infraestructuras vinculadas a los programas maliciosos (malware) SocGholish, Amadey y StealC, utilizados para distribuir programas de secuestro de datos y fraude informático, en una acción que permitió además bloquear criptomonedas de origen criminal valoradas en más de 41 millones de euros.

La operación, denominada Endgame, reunió durante dos semanas a las fuerzas de seguridad de Canadá, Dinamarca, Alemania, Países Bajos, Reino Unido y Estados Unidos, junto a Microsoft y otras empresas, para interrumpir las herramientas que los ciberdelincuentes usan para lanzar ataques contra empresas, administraciones e infraestructuras críticas.

Las autoridades actuaron contra 326 servidores y 142 dominios utilizados para distribuir los malware y recuperaron 27 millones de credenciales de acceso robadas, según informó Europol este miércoles.

Los programas desmantelados formaban parte del modelo conocido como “ciberdelincuencia como servicio”, mediante el cual grupos criminales alquilan o venden herramientas a otros delincuentes para facilitar ataques informáticos.

Entre ellos figuraba SocGholish, que se propagaba a través de falsas actualizaciones de navegadores distribuidas desde páginas comprometidas, muchas de ellas creadas con WordPress, y una vez instalado, permitía a los atacantes acceder al sistema infectado e introducir programas más peligrosos, incluido aquellos destinados a la extorsión digital.

La operación permitió además limpiar 14.971 sitios web infectados, entre ellos páginas de restaurantes, talleres mecánicos y otros pequeños negocios.

Las autoridades vinculan SocGholish al grupo criminal ruso Evil Corp, relacionado anteriormente con los programas Zeus y Dridex, así como con operaciones de ransomware y blanqueo de capitales.

También fueron desmanteladas infraestructuras asociadas a StealC, especializado en el robo de contraseñas, credenciales e identidades digitales para su venta o uso fraudulento, y a

Amadey, una herramienta utilizada para introducir un programa maligno adicional en sistemas ya comprometidos.

Según datos recopilados por Microsoft, ambos programas estuvieron relacionados con más de 140.000 ordenadores infectados en todo el mundo durante las dos primeras semanas de mayo.

La Patilla