28/06/24

Detenidas dos personas por un centenar de ciberataques a organismos de la Administración Pública y entidades privadas

Resumen

Mediante el análisis de trazabilidad de los datos se relacionó con multitud de ciberataques a un actor conocido como “GUARDIACIVILX”, comprobando a lo largo de la investigación que estaba conformado por dos personas diferentes

Debido al grado de sofisticación de estos ciberataques, han llegado a verse comprometidos más de 100 organismos y entidades del sector público y privado, tanto a nivel nacional como internacional

Este actor comenzó sus operaciones al menos en octubre de 2022, quedando acreditada su responsabilidad en ataques a instituciones públicas y privadas como ITVASA, Ayuntamientos de León y Salamanca, Universidad Autónoma de Madrid, Diputaciones de Jaén y Málaga, Servicio Cántabro de Salud, Ministerio de Salud de Perú y Ministerio de Cultura de Argentina, entre muchas otras

Contenido

La Guardia Civil, en la denominada operación “Oceansx”, ha detenido a dos personas como responsables de la obtención de accesos no autorizados a redes informáticas y credenciales de accesos corporativos, tanto públicos como privados, ofreciendo la venta de los mismos, y de bases de datos y conjuntos de datos comprometidos en mercados del cibercrimen.

La investigación se inició tras relacionar una serie de ciberataques con la información obtenida de los análisis realizados en determinados materiales intervenidos en investigaciones anteriores, localizando un canal de Telegram donde se mostraban accesos fraudulentos a varias administraciones públicas de relevancia.

Especializados en ataques contra el sector público en España

Analizado el contenido de dicho canal mediante técnicas de investigación tecnológica avanzadas y búsquedas en fuentes abiertas, los agentes atribuyeron esos ataques a un “actor nacional” del ámbito de la ciberdelincuencia, que actuaba bajo el seudónimo “GUARDIACIVILX”, utilizando además otras 14 identidades como “9bands”, “banz9”, “TheLich”, “Crystal_MSF”, “OUJA”, “unlawz” o “teamfs0ciety”.

A partir de ese momento, la investigación se centró en obtener la identidad de las personas que estaban actuando bajo ese seudónimo, así como el número y puntos de ataques realizados.

El actor nacional "GUARDIACIVILX" se publicitaba como un vendedor de credenciales de acceso a servicios remotos y correos electrónicos corporativos, ofreciendo la venta privada de credenciales de acceso sobre un portal de consultas de vehículos de la Dirección General de Tráfico (DGT) e ITVASA. Para ello, solicitó inicialmente un pago de 13.000 dólares, siendo detenido en el momento de proceder a la citada venta. Además, se ha podido comprobar como trató de vender una base de datos con información de más de 200.000 personas.
Paralelamente se pudieron analizar diferentes cuentas de criptodivisas vinculadas a este “actor nacional”, corroborando que gran parte de ellas se dirigían o provenían de distintos exchangers (casa de cambio de criptomonedas), desde donde se habrían materializado los pagos de la venta de varios paquetes con estas credenciales de acceso obtenidas ilegalmente.

“GUARDIACIVILX”; investigado por ataques a intereses en Latinoamérica

Mediante labores de cibervigilancia en la red se localizó a este “actor” en distintos foros utilizados por cibercriminales, donde éste desarrollaba su actividad, identificándose así nuevas cuentas e identidades utilizadas por el mismo.

Comprobados e identificados así varios indicadores atribuidos al supuesto autor, la Guardia Civil colaboró con otras agencias policiales como el FBI, dejando ya patente el alcance trasnacional de las acciones llevadas a cabo por “GUARDIACIVILX”, muchas de ellas sobre instituciones del continente americano, especialmente de países de habla hispana.

Detenidos en Sevilla y Asturias

Esta investigación permitió detener a dos individuos el pasado otoño, uno en Sevilla y el otro en Asturias, ambos como responsables directos de los hechos investigados.

Del material intervenido en estas detenciones, tanto informático como documental, los investigadores han logrado las evidencias necesarias para vincular otros ciberataques a entidades tanto públicas como privadas, como es el caso de ITVASA, Ayuntamientos de León, Salamanca, Vitoria, Bermeo y Basauri entre otros, así como a la Universidad Autónoma de Madrid, Diputaciones de Jaén y Málaga, Servicio Cántabro de Salud, Banco Atlántida, Ministerio de Cultura de Argentina, Ministerio de Salud de Perú, Poder Judicial del Estado de Txascala en México, entre muchas otras, destacando también su interés por el robo de información de redes de farmacias.

Tras los resultados obtenidos de los análisis de los dispositivos, se ha podido conocer el alto grado de sofisticación alcanzado para perpetrar los mismos, evidenciándose que ambos detenidos ejecutaban las acciones delictivas de manera coordinada. El hecho de desplegar esta actividad de forma conjunta conllevaba que los ciberataques fueran de una gravedad y complejidad creciente, llegando a verse afectados más de 100 organismos y entidades del sector público y privado tanto a nivel nacional como internacional.

Hay que resaltar la relevancia de esta investigación, destacando la estrecha colaboración entre la Autoridad Judicial, la Fiscalía de Criminalidad Informática y el Centro Criptológico Nacional (CCN-CNI) con los investigadores, así como con otras agencias internacionales, permitiendo todo ello dar una respuesta adecuada al incremento de los delitos en el ámbito del ciber espacio.

Esta operación ha sido dirigida por el Juzgado de Primera Instancia e Instrucción nº 2 de Grado (Asturias) y llevada a cabo por el Departamento Contra el Cibercrimen de la Unidad Central Operativa de la Guardia Civil.

Imágenes


GUARDIA CIVIL
Mº INTERIOR


GUARDIA CIVIL
Mº INTERIOR
UCO


GUARDIA CIVIL
Mº INTERIOR
GUARDIA CIVIL
UCO


GUARDIA CIVIL
Mº INTERIOR
GUARDIA CIVIL
UCO