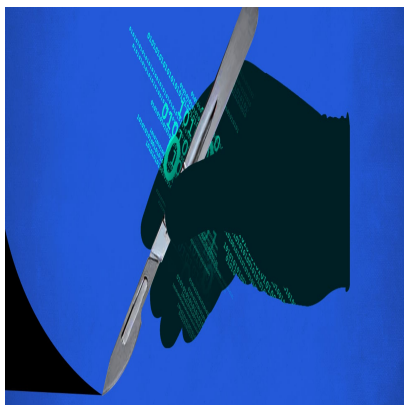




El doctor Zagala y m ster Cracker

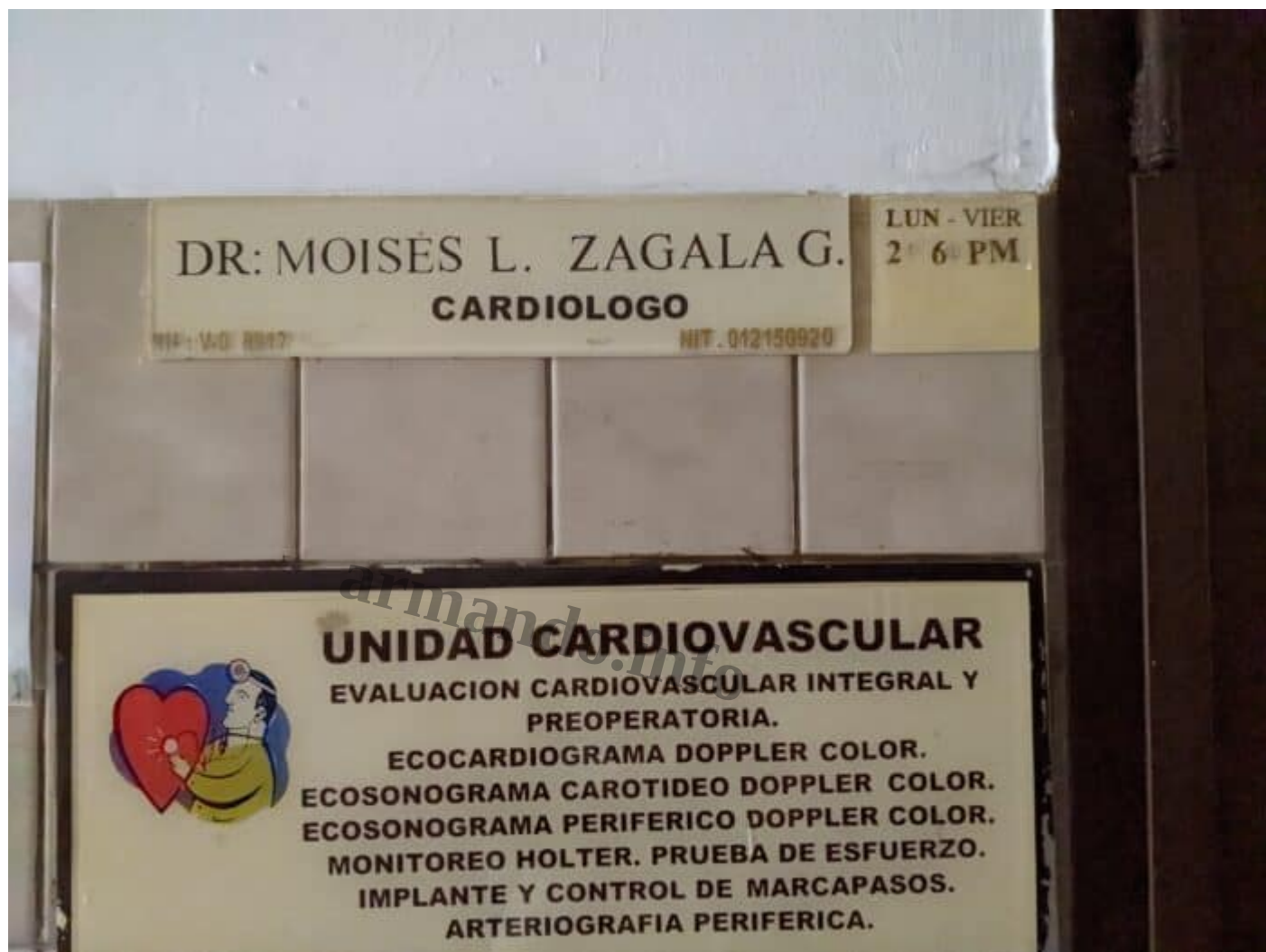
Descripci n

Para seguir los pasos que el presunto pirata cibernetico marca al caminar, hay que atravesar un pasillo sombr o. Las filtraciones corroen el techo y las paredes alrededor de su oficina. Los bombillos del largo corredor se da aron en alg n momento y nadie se acord  de repararlos. Algunas personas esperan en este precario lugar, pero no lo esperan a  l. Ya se sabe que poco aparece desde mayo de este a o, cuando se anunci  que estaba en la mira del Bur  Federal de Investigaciones (FBI, por sus siglas en ingl s) de Estados Unidos.

La descripci n encajar a como locaci n para una pel cula de suspenso, pero en realidad corresponde a la oficina en Ciudad Bol var de Mois s Luis Zagala Gonz lez. All , en la Polic nica Santa Ana, desde hace a os, ejerce la consulta como m dico cardi logo, una pr ctica de servicio p blico que le gan  reputaci n y que contrasta con el deseo de querer pasar inadvertido ahora, cuando tambi n es reconocido como un *cracker*. Traducci n: un experto en vulnerar sistemas inform ticos.



[Moisés Zagala, médico cardiólogo, ejerce su profesión en Ciudad Bolívar, sur de Venezuela. Crédito: Isayen Herrera.](#)



Moisés Zagala, médico cardiólogo, ejerce su profesión en Ciudad Bolívar, sur de Venezuela. Crédito: Isayen Herrera.

Moisés Luis Zagala González es el ciudadano venezolano-francés buscado en Estados Unidos para que comparezca en un juicio que deberá determinar si es culpable o no de varios ciberdelitos del más puro estilo *matrix*, solo que esta vez llevados a cabo lejos de la clásica estampa ultraurbana de Nueva York: en la capital del estado Bolívar, la antigua Angostura, un puerto de aires coloniales a orillas del río Orinoco, en el sur de Venezuela. Ciudad Bolívar, para más señas, se cuenta entre las ciudades del país azotadas por las precarias condiciones de vida que incluyen, sin reparos, problemas de conectividad. Este inhóspito contexto hace que muchos descarten la posibilidad de que algún delito informático de envergadura pueda gestarse allí; aunque, viéndolo bien, tal vez sea eso precisamente lo que lo convierte en el contradictorio y perfecto escenario para ello.

El médico, profesor de Cardiología de los estudiantes de pregrado de Medicina de la Universidad de Oriente, fue acusado por la Fiscalía del Distrito Este de Nueva York y el FBI de dos cargos -intento de intrusiones informáticas y conspiración para cometer intrusiones informáticas- por haber diseñado múltiples herramientas de *ransomware*, un *software* malicioso capaz de infiltrarse en las computadoras y encriptar sus contenidos (secuestrarlos, prácticamente, desde contraseñas hasta

fotos, informaci3n bancaria o acad3mica). Tras el ataque, el *software* s3lo puede ser desactivado por sus creadores con una clave que le dan a sus v3ctimas tras pagar el rescate -m3is bien, la extorsi3n- que se les exige.

Un delito en ascenso

La acusaci3n contra Zagala Gonz3lez se public3 tras una investigaci3n con agente encubierto del FBI entre abril de 2019 y marzo de 2021, que devel3 no solo los seud3nimos con los que pretend3a ocultarse, sino tambi3n su *modus operandi*.

Los *ransomware* -por *ransom*; "rescate" en ingl3s- aplicados por ciberdelincuentes se ciernen cada vez m3is como una nueva modalidad de delito inform3tico que genera ganancias a trav3s de la extorsi3n. El FBI [emiti3 una alerta](#) a principios de 2021 tras 16 ataques de *ransomware* dirigidos a las redes de atenci3n m3dica y de primeros auxilios de Estados Unidos, apenas una fracci3n de las m3is de 400 organizaciones en todo el mundo que reportaron haber sido v3ctimas de esta modalidad de secuestro y extorsi3n online, de las cuales 290 eran estadounidenses

Entre los ataques m3is pol3micos se cuenta el que ocurri3 el 7 mayo de 2021, cuando Colonial Pipeline, operador de uno de los oleoductos m3is grandes de ese pa3s, anunci3 que hab3a recibido un ataque de *ransomware*. La compa3a cerr3 de manera preventiva su tuber3a, que entrega casi la mitad del combustible para aviones y la gasolina que se usa en la costa atl3ntica, lo que gener3 interrupci3n de viajes a3reos y compras nerviosas de combustible entre el p3blico. Seg3n una investigaci3n del diario *The New York Times*, la empresa termin3 pagando a los chantajistas 75 bitcoin, equivalentes entonces a cinco millones de d3lares.

En junio de ese mismo a3o hubo otro ciberataque que afect3 a los servidores que soportan la plataforma tecnol3gica del proveedor de carne JBS, corporaci3n global de origen brasile3o, en Norteam3rica y Australia. La empresa debi3 pagar 11 millones de d3lares para recuperar su operatividad, pues el ataque afect3 a la cadena de suministro. En ese momento, el gobierno de Washington atribuy3 la responsabilidad a una banda criminal que, se cree, tiene su sede en Rusia o Europa del Este.

En esos casos, que se sepa, no particip3 el m3dico de Ciudad Bol3var. Pero Zagala representa un engranaje que permite descifrar y cauterizar el sistema de este nuevo delito, con dimensiones de industria.

Seg3n la [acusaci3n federal](#), este m3dico cre3, vendi3 y alquil3 su *software* a piratas que lo utilizaron para atacar redes inform3ticas, ense3a a sus clientes c3mo usarlo y, como estrategia de negocio, cre3 un "programa de afiliados", en el que proporcion3 acceso de usuario a uno de los programas a cambio de una parte de las ganancias obtenidas por los ataques. Tambi3n public3, como parte de su mercadeo enlaces en foros para promocionar el historial de los clientes con el *software*.

â??Como se alega, el m3dico multitarea trat3 a los pacientes, cre3 y nombr3 su herramienta cibern3tica (...) se benefici3 de un ecosistema global de *ransomware* en el que vendi3 las herramientas para realizar ataques de *ransomware*, entren3 a los atacantes sobre c3mo extorsionar a las v3ctimas y luego se jact3 sobre ataques exitosos, incluso por parte de actores maliciosos

asociados con el gobierno de Irãjnâ?•, declarã³ el Fiscal Federal Breon Peace.

armando.info

CRH:DKK/AFM
F. #2020R00582

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

MOISES LUIS ZAGALA GONZALEZ,
also known as "Nosophoros,"
"Aesculapius" and
"Nebuchadnezzar,"

Defendant.

----- X

EASTERN DISTRICT OF NEW YORK, SS:

CHRIS CLARKE, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such:

Count One: Attempted Computer Intrusions

In or about and between April 2019 and March 2021, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant MOISES LUIS ZAGALA GONZALEZ, also known as "Nosophoros," "Aesculapius" and "Nebuchadnezzar," did knowingly attempt to cause the transmission of a program, information, code and command and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, resulting in losses in excess of \$5,000 and damage affecting ten or more protected computers during a one-year period; did, with intent to extort from any person any money or other thing of value, attempt to

AMENDED AFFIDAVIT
AND COMPLAINT IN
SUPPORT OF AN
APPLICATION FOR
AN ARREST WARRANT

(T. 18, U.S.C., §§ 1030(a)(5)(A),
1030(a)(7)(C), 1030(b), 1030(c)(3),
1030(c)(4)(B), 371, 2 and 3551 et

No. 21-M-276

El FBI hizo un trabajo de inteligencia en la Dark web entre los años 2019 y 2021 para dar con la identidad de este presunto pirata cibernético. Los detalles están en el expediente del Tribunal de Distrito Este de New York de los Estados Unidos.

El buen doctor

En los servicios de mensajería de texto compartidos por doctores y allegados al gremio médico de la capital bolivareña, la noticia corrió como pólvora el 16 de mayo de 2022: un colega conocido en la ciudad por ser hijo de un matrimonio honorable de la localidad, excelente estudiante y profesor universitario, era acusado por un delito informático que a la fecha de hoy pocos entienden y muchos, en cambio, subestiman.

Algunos médicos y amigos de la adolescencia lo defendieron sin dudar. Contactados por **Armando.info** comentaron que "era imposible" que un hijo de Moisés Zagala, un ingeniero y profesor de origen francés, y de Rosalva González, conocida por vender artesanías indígenas, pudiera ser capaz de hacer algo ilegal.

Presuponen, además de la honorabilidad de su familia, que su sencillez contrasta con el perfil de alguien que pueda estar obteniendo grandes ganancias a partir de un delito informático. Aseguran que el dinero no podrá ocultarse y Zagala González, al menos en Ciudad Bolívar, mantiene un estricto bajo perfil, además de una vida muy frugal. Aún maneja la misma camioneta Jeep Cherokee, que tiene al menos diez años de uso. Su consultorio se encuentra en un edificio terriblemente deteriorado y a la fachada del edificio en donde reside solo le quedan vestigios de que alguna vez estuvo pintado.



Moisés Zagala nació, se crió y estudió en el estado Bolívar, lugar donde aún reside.
Créditos: Isayen Herrera.



Moisés Zagala nació, se crió y estudió en el estado Bolívar, lugar donde aún reside.
Créditos: Isayen Herrera.

Su estilo de vida no es ostentoso, hasta el punto que tanta austeridad llama la atención no solo en contraste con la imagen de un mago de la piratería informática, sino para ser un médico destacado, conocido, pero de pocos amigos. En general, las fuentes consultadas por **Armando.info** lo describen como una persona arrogante y algo egocéntrica. Evita los saludos de sus colegas. Eso sí, nadie titubea al admitir que es un hombre muy inteligente.

De todas las fuentes consultadas, el cardiólogo Reinaldo Brines fue de los pocos que ofreció su testimonio dando la cara, junto a su nombre y apellido. Brines tiene su consultorio también en la Policlínica Santa Ana, frente al de Zagala. Han hecho intervenciones quirúrgicas juntos. Muestra una revista en donde salen uno al lado del otro en una fotografía en quírfano; el título de la nota a la que la foto acompaña destaca la innovación en la cardiología. ¿?¿?l no tiene ni Internet en su casa?•, dice. ¿?¿Lo he llamado y no me puedo ni comunicar y he tenido que ir a buscarlo?•, alega,

aunque seÑ±ala que jamÑ±s ha entrado a su apartamento.

Otros mÑ©dicos, compaÑ±eros de la Facultad de Medicina de la Universidad de Oriente, de donde egresÑ±, recuerdan en cambio que la primera vez que en sus vidas vieron una computadora fue en la casa de Zagala, en la dÑ©cada de los 80. Un antiguo pupilo del mÑ©dico dijo que en cierto momento este recomendÑ± ciertas aplicaciones informÑ±ticas para facilitar algÑ±n trabajo, y otro mÑ©dico deslizÑ± el comentario de que Zagala tenÑ±a â??otras fuentesâ?? de ingresos y que logrÑ± arreglar una computadora de su propiedad. Pero solo hasta aquÑ± llegan las anÑ©cdotas mÑ±s cercanas a la informÑ±tica de las que sus conocidos disponen.

armando.info



El médico Reinaldo Brines asegura que su colega Moisés Zagala es un buen profesional y honesto. Créditos: Isayen Herrera.

Nadie de su entorno se atreve a decir si este médico brillante tiene una doble vida, pero una anecdota de su juventud activa una ligera duda. Hace 30 años, cuando las computadoras caseras se usaban casi solo para escribir -con los llamados "procesadores de palabras"- y las letras en las pantallas eran de color verde, Zagala, junto a tres amigos más, crearon un programa para calcular la probabilidad de ganar carreras de caballos. Diseñaron el programa para obtener las estadísticas de quién era mejor jinete, mejor entrenador y qué caballo hacía los mejores tiempos. Lo usaron. Una vez *pegaron* cinco carreras del juego dominical del 5y6 solo porque desconfiaron de su propio programa y no apostaron al ejemplar que arrojaba su desarrollo como posible vencedor de la sexta válida, cuentan dos personas cercanas a su círculo de cuando eran jóvenes.

Ojos que no ven

Aunque el Tribunal Federal de Primera Instancia del Distrito Este de Nueva York en Brooklyn, Nueva York, emitió una orden federal para arrestarlo y el alerta del FBI insta a dar información sobre el paradero de Zagala o contactar a la embajada más cercana, ninguna autoridad venezolana se ha acercado a su sitio de trabajo para indagar sobre él, según afirma Margot Gutiérrez, la directora del centro de salud público donde el controvertido médico labora.

Por lo demás, la funcionaria alega que no se mete en la vida personal de los médicos. Otro tanto argumentaron los vigilantes de la Policlínica Santa Ana, que a su manera fungieron como voceros o intermediarios de la directiva del recinto, cuyos miembros no quisieron hablar con **Armando.info**. ¿Acá los médicos son autónomos?, expresó un vigilante después de notificar que nadie daría declaraciones sobre el tema por orden de la administración de la clínica.



[El cardi logo contin a trabajando en la Policl nica Santa Ana y en el Hospital Dr H ctor Nouel Joubert, ambos en Ciudad Bol var. Cr ditos: Isayen Herrera.](#)



Es así, amparado por la escasa comprensión colectiva de la magnitud de lo sucedido y por una fÃ©rrea defensa de su privacidad, que Zagala se sigue moviendo por Ciudad BolÃ­var. Va menos a su consulta privada, pero atiende llamados de los pacientes y continÃºa caminando por los pasillos del Hospital Dr HÃ©ctor Nouel Joubert, adscrito al Seguro Social, donde tambiÃ©n presta sus servicios.

Zagala ha sido muy puntual con sus explicaciones. Su colega, el doctor Brines, asegura que Ã©l llegÃ³ a excusarse con su cÃ­rculo Ã­ntimo asegurando que, en algÃºn momento, su correo electrÃ³nico fue intervenido y que no tiene dinero para pagar una defensa en Estados Unidos que le permita enfrentar el proceso judicial que le espera. Su colega, luego de escucharlo, tiene como hipÃ³tesis que hubo una usurpaciÃ³n de su identidad.

A otros amigos les dijo que temÃ­a por su seguridad, que solo querÃ­a que el tema se olvidara y estaba resignado a no salir mÃ¡s del paÃ­s. Al ser contactado por **Armando.info** para este reportaje, Zagala mantuvo un largo silencio que fue por fin interrumpido con una solicitud de no buscarle mÃ¡s a Ã©l, a su familia o amigos, y que no darÃ­a entrevistas por sugerencia de sus abogados.

Ciberpirata y tutor helenista

El trabajo encubierto del FBI entre abril de 2019 y marzo de 2021 detectó que Zagala tenía dos productos estrellas. Uno era un *ransomware* llamado Jigsaw v.2, que tenía, en la descripción de Zagala, un contador que registra cuántas veces el usuario había intentado eliminar el *software* malicioso de su computadora. Con esta herramienta, él aconsejaba a sus clientes que lo usaran como castigo y para determinar cuánto tanto podrían conseguir de la víctima: "Si el usuario elimina el *ransomware* demasiadas veces, está claro que no pagará, así que es mejor que borre todo el disco duro", explicaba el mecanismo de represalia, como parte de sus tutoriales que fueron citados en el expediente judicial.

Para abril de 2019, según las investigaciones, el pirata cibernético vendía su producto con el valor agregado de evadir los antivirus y configurarse para pedir cuentas de bitcoin diferentes a cada víctima, además de la capacidad de robar las contraseñas y datos de la tarjeta de crédito de la persona atacada. Esta herramienta la fue perfeccionando con el tiempo. Zagala vendía su producto en foros de Internet por 500 dólares y el código fuente por 3.000 dólares.

A finales de 2019, anunció otro producto que llamó Thanos, una referencia simultánea al villano ficticio de la serie *Avengers* y a Thanatos, la muerte de la mitología griega. En otro foro dijo que los interesados en usar su herramienta debían compartir con él una parte de las ganancias obtenidas como producto de los ataques cibernéticos. Un funcionario infiltrado del FBI le compró esta licencia en septiembre de 2020.

Aunque los agentes no saben cuántas licencias de Thanos se vendieron, sí confirmaron algunas transacciones. El servidor de control de Thanos contenía un archivo que enumeraba el estado de las licencias de 38 clientes, lo que indica que al menos 38 copias se han vendido del programa *ransomware*, detalla el expediente. Y agrega que su uso de un programa de afiliados le permite beneficiarse directamente de tales intrusiones.

El FBI acota en su expediente que la afición de Zagala por la informática empezó desde su juventud. Lo describen como un "pirata informático" autodidacta que comenzó su clandestinidad al menos en el año 1997, a través de participaciones en línea en la High Craking University (HCU), una comunidad en línea selecta de piratas informáticos de elite e ingenieros. El expediente agrega al caso la comprobación de que Zagala usaba seudónimos también de origen griego: *Esculapio*, en referencia al antiguo dios de la medicina, o *Nosophoros*, palabra que significa "portador de enfermedades", también en griego. El FBI encontró que una persona identificada como *Aesculapius* tenía tutoriales en línea publicados por la HCU sobre cómo descifrar programas *shareware* y desafíos de codificación que sirvieron como prueba de admisión para la universidad elite.

Los rastros del ego

"Es imposible que esto sea cierto. Trata solo de hacer un pago mágico y verás", dijo uno de sus amigos y colegas para defenderlo, echando mano a los problemas de conectividad que hay en Ciudad Bolívar. Luego se detiene a pensar en medio de la conversación. "Aunque Moisés será capaz de querer un *feedback* para que le dijeran que es el mejor, tal cual como lo describe el FBI. Él es ególatra. ¿Será que sí es cierto? Pero los errores existen", dice, al contradecirse a la vez.

Zagala, cuando hac a los foros de entrenamientos para usar su programa que cifraba datos de sus v ctimas, solo ten a una solicitud: "Si tiene tiempo y no es demasiado problema para usted, describa su experiencia conmigo ", ped a en l nea. Y as  se abr a la ventana de los elogios.

  Eres el mejor desarrollador de todos los tiempos , le dijo un cliente citado en el expediente. Y   I respondi : "Gracias, es bueno escucharlo. Estoy muy halagado y orgulloso".

Zagala, aunque se escudaba bajo tres seud nimos, no logr  hacerse tan invisible en la llamada *Dark web*. De hecho, en medio de tanta enjundia cibern tica, cometi  errores de novato que dej  pistas clamorosas para los investigadores. Por ejemplo: el m dico ped  pagos en criptomonedas o transferencias de Paypal. Esta empresa, que ofrece un servicio de monedero digital, suministr  informaci n al FBI y asegur  que el correo electr nico afiliado de quien recib a los pagos era moiseszagala@gmail.com, y el nombre que la persona report  era Mois s Zagala. Este mismo email lo report  el m dico en Estados Unidos en sus datos migratorios. Adem s, Google aport  informaci n del n mero telef nico que este usuario registr  para abrir su correo electr nico y dio acceso a la informaci n que conten a, por el proceso judicial en curso.

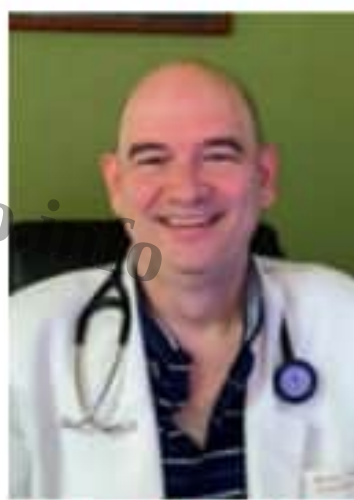
armando.info



BUSCADO POR EL FBI

MOISÉS LUIS ZAGALA GONZÁLEZ

Tentativa de comisión de intrusismo informático; confabulación para cometer intrusismo informático



DESCRIPCIÓN

Alias: Moisés Zagala, "Nosophoros", "Aesculapius", "Nebuchadnezzar"

Fecha(s) de nacimiento usada(s): 7 de febrero de 1967

Lugar de nacimiento: Venezuela

Cabello: calvo

Ojos: color café

Sexo: masculino

Raza: blanca (hispano)

Ocupación: cardiólogo

Nacionalidad: venezolana

Idiomas: inglés, español, francés

ADVERTENCIA

Desde abril de 2019 a marzo de 2021, Moisés Luis Zagala González supuestamente diseñó y ofreció varias herramientas de programas de cibersecuestro de datos. Entre esas herramientas había una programa de cibersecuestro de datos que se llamaba "Jigsaw v. 2" que se empleó para extorsionar instituciones, mediante la codificación de los archivos de las víctimas y la exigencia de un rescate para descifrarlos, al igual que un "programa privado para crear programas de cibersecuestro de datos", como "Thanos", que se concibió con la finalidad de evadir los programas antivirus y que es capaz de acceder a archivos específicos según las extensiones de estos. Zagala González se lucró como consecuencia de sus supuestos actos, incluso al ofrecer licencias para utilizar el programa "Thanos" a personas que pagaban una cuota mensual, y al operar un programa "afiliado" del que recibía parte del pago de la recompensa obtenida de la víctima al ser extorsionada.

El 16 de mayo de 2022, el Tribunal Federal de Primera Instancia del Distrito Este de Nueva York en Nueva York, emitió una orden federal para arrestar a Zagala González después de que lo acusaran de comisión de intrusismo informático y confabulación para cometer intrusismo informático.

Si usted tiene información con respecto a esta persona, póngase en contacto con la oficina local del FBI, o con la embajada o el consulado estadounidense más cercano.

Oficina regional del FBI: Nueva York

El FBI descifr  la identidad del m dico porque us  su correo personal para recibir pagos por Paypal y abrir servidores en Estados Unidos. Cr ditos: Tribunal de Distrito Este de New York de Estados Unidos.

Tambi n el pirata inform tico deriv  pagos a la cuenta Paypal de un pariente, que qued  identificado como un hermano residenciado en Florida y que luego fue interrogado. Seg n el expediente, el familiar confirm  que Zagala reside en Venezuela y revel  que era un autodidacta en programaci n inform tica. El individuo tambi n mostr  a los agentes la informaci n de contacto de Zagala en su tel fono, que coincidi  con el correo electr nico registrado para la infraestructura maliciosa asociada con Thanos.

Sus allegados aseguran que este hermano regres  de Estados Unidos, luego de haber migrado hace cuatro a os, porque se sinti  â??asediadoâ? por el FBI. Regres  de Florida y se atrincher  en la antigua casa de dos pisos de sus padres, ubicada en Ciudad Bol var, de linda fachada, reci n pintada y en la que un trabajador procura que el jard n se mantenga en  ptimas condiciones.

Para este reportaje se contact  a sus hermanos, pero solo uno respondi . Le espet  a la reportera que ning n periodista busc  la verdad, pero, aunque fuera su oportunidad para decir esa verdad, se neg  a dar su versi n. Asegur  que se encontraba en Estados Unidos para el momento en que respondi  a la petici n de entrevista.

Nadie quiso contar su versi n.

Fecha de creaci n

2022/09/11