Conor Brian Fitzpatrick, de 20 años de edad, fundador y administrador de BreachForums, ahora desaparecido, fue acusado formalmente en Estados Unidos de conspiración para cometer fraude con dispositivos de acceso.

De comprobarse su culpabilidad, Fitzpatrick, conocido en línea como «*pompompurin*«, enfrentaría una pena máxima de hasta cinco años de prisión. Fue arrestado el 15 de marzo de 2023.

> *«El delito cibernético victimiza y roba información financiera y personal de millones de personas inocentes. Este arresto envía un mensaje directo a los ciberdelincuentes: se descubrirá su conducta ilegal y explotadora, y será llevado ante la justicia»,* dijo la fiscal federal, Jessica D. Aber, para el Distrito Este de Virginia.

El desarrollo se produce días después de que Baphomet, la persona que se había hecho cargo de las responsabilidades de BreachForums, cerrara el sitio web citando preocupaciones de que las fuerzas del orden público pudieran haber obtenido acceso a su backend. Desde entonces, el Departamento de Justicia (DoJ) confirmó que llevó a cabo una operación de interrupción que provocó que la plataforma criminal ilícita se desconectara.

BreachForums, según Fitzpatrick, se creó en marzo de 2022 para llenar el vacío dejado por RaidForums, que se eliminó un mes antes como parte de una operación policial internacional.

Sirvió como un mercado para intercambiar datos hackeados o robados, incluyendo información de cuentas bancarias, números de seguro social, herramientas de hacking y bases de datos que contienen información de identificación personal (PII).

En nuevos documentos judiciales publicados el 24 de marzo de 2023, salió a la luz que agentes encubiertos que trabajaban para la Oficina Federal de Investigaciones (FBI) de Estados Unidos compraron cinco conjuntos de datos ofrecidos a la venta, con Fitzpatrick actuando como un intermediario para completar las transacciones.

Los enlaces de Fitzpatrick a pompompurin provenían de nueve direcciones IP asociadas con el proveedor de servicios Verizon que Pompompurin usó para acceder a la cuenta de pompompurin en RaidForums y una vulnerabilidad importante de OPSEC por parte del acusado.

> *«Los registros de RaidForums también contenían comunicación entre pompompurin y omnipotent [administrador de RaidForums] alrededor del 28 de noviembre de 2020, en la que pompompurin menciona específicamente a omnipotent que había buscado la dirección de correo electrónico conorfitzpatrick02@gmail.com y nombre 'conorfitzpatrick' dentro de una base de datos violados de 'ai.type'»,* según la declaración jurada.

Cabe mencionar que la aplicación de teclado de Android Ai.type sufrió una violación de datos en diciembre de 2017, lo que provocó la filtración accidental de correos electrónicos, números de teléfono y ubicaciones asociadas con 31 millones de usuarios.

Otros datos obtenidos de Google revelan que Fitzpatrick registró una nueva cuenta de Google con la dirección de correo electrónico conorfitzpatrick2002@gmail.com en mayo de 2019 para reemplazar a conorfitzpatrick02@gmail.com, que se cerró alrededor de abril de 2020.

Además, la dirección de correo electrónico *«antigua»* conorfitzpatrick02@gmail.com está presente en el sitio de notificación de violación de datos legítimos de la base de datos Ai.type violada Have I Been Pwned.

> *«La dirección de correo electrónico para conorfitzpatrick2002@gmail.com era funmc59tm@gmail.com. Los registros de suscriptores de esta cuenta revelan que la cuenta se registró con el nombre de 'aa' y se creó alrededor del 28 de diciembre de 2018 a partir de la dirección IP 74.101.151.4»,* dice la declaración jurada.

> *«Los registros recibidos de Verizon, a su vez, revelaron que la dirección IP 74.101.151.4 estaba registrada para un cliente con el apellido Fitzpatrick en [una residencia ubicada en Union Avenue en Peekskill, Nueva York]».*

La investigación también arrojó evidencia de que Fitzpatrick inició sesión en varios proveedores de redes privales virtuales (VPN) desde septiembre de 2021 hasta mayo de 2022 para ocultar su verdadera ubicación y conectarse a diferentes cuentas, incluyendo la cuenta de Google vinculada a conorfitzpatrick2002@gmail.com.

Una de esas direcciones IP enmascaradas se utilizó además para iniciar sesión en una cuenta de Zoom con el nombre de «pompompurin» con una dirección de correo electrónico de pompompurin@riseup.net, según revelan los registros obtenidos por el FBI de Zoom. De forma curiosa, se dice que Fitzpatrick usó la dirección de correo electrónico pompompurin@riseup.net para registrarse en RaidForums.

La agencia también descubrió una cuenta de criptomonedas Purse.io que se registró co la dirección de correo electrónico conorfitzpatrick2002@gmail.com y *«fue financiada exclusivamente por una dirección de Bitcoin que pompompurin había discutido en publicaciones en RaidForums».* Los registros de Purse.io mostraron que la cuenta se usó para comprar *«varios artículos»* y enviarlos a su dirección en Peekskill.

Aparte de eso, el FBI obtuvo una orden para obtener la ubicación GPS de su teléfono celular en tiempo real, de Verizon, lo que permitió a las autoridades determinar que había iniciado sesión en BreachForums mientras que la ubicación física de su teléfono mostraba que estaba en su casa.

Pero es no es todo. En otro error de OPSEC, Fitzpatrick cometió el error de iniciar sesión en BreachForums el 27 de junio de 2022 sin usar un servicio VPN o el navegador TOR, exponiendo así la dirección IP real (69.115.201.194).

Según los datos recibidos de Apple, se usó la misma dirección IP para acceder a la cuenta de

iCloud unas 97 veces entre el 19 de mayo de 2022 y el 2 de junio de 2022.

> *«Fitzpatrick ha usado las mismas VPN y direcciones IP para iniciar sesión en la cuenta de correo electrónico conorfitzpatrick2002@gmail.com, la cuenta Conor Fitzpatrick Purse.io, la cuenta pompompurin en RaidForums y la cuenta pompompurin en BreachForums, entre otras cuentas»,* dijo John Longmire, del FBI.

Después de la publicación de la declaración jurada, Baphomet dijo que *«no debe confiar en nadie para manejar su propio OPSEC»,* y agregó que *«Nunca hice esta suposición como administrador, y nadie más debería hacerlo».*