Autoridades dos EUA e do Reino Unido acusam dois hackers suspeitos de

Data: 2025-09-18 17:16:02

Autor: Inteligência Against Invaders

Autoridades dos EUA e do Reino Unido acusaram dois supostos membros do infame grupo de crimes cibernéticos Scatter Spider de crimes relacionados a vários ataques cibernéticos de alto perfil.

A dupla foi associada a ataques a tribunais dos EUA, a uma empresa de infraestrutura crítica dos EUA e à Transport for London (TfL) do Reino Unido.

Os dois indivíduos baseados no Reino Unido, Thalha Jubair, 19, do leste de Londres, e Owen Flowers, 18, de Walsall, foram presos em seus endereços residenciais na terça-feira, 16 de setembro.

O Distrito de Nova Jersey [Sem lacre](#) acusações contra Jubair em 18 de setembro, com conspirações para cometer fraude informática, fraude eletrônica e lavagem de dinheiro.

De acordo com as acusações, Jubair, também conhecido como “EarthtoStar”, “Brad”, “Austin” e “@autistic”, conspirou com outras pessoas para usar técnicas de engenharia social para obter acesso não autorizado às redes de computadores das empresas vítimas.

Jubair é acusado de participação em pelo menos 120 invasões e extorsões em redes de computadores envolvendo 47 entidades americanas. Acredita-se que as vítimas pagaram pelo menos US\$ 115 milhões em pagamentos de resgate a Jubair e seus associados.

Partes dos pagamentos de resgate de pelo menos cinco vítimas foram enviadas para carteiras em um servidor controlado por Jubair.

Em julho de 2024, Jubair foi observado transferindo uma parte da criptomoeda originada de uma das vítimas, no valor de aproximadamente US\$ 8,4 milhões na época, para outra carteira, enquanto a polícia estava em processo de apreensão do servidor.

Jubair e associados são acusados de envolvimento em ataques desde maio de 2022 até setembro de 2025.

A agente especial do FBI encarregada Stefanie Roddy disse: “A prisão de Thalha Jubair ressalta uma verdade inegável: não importa o quão evasivos ou destrutivos sejam esses sindicatos de cibercriminosos, continuaremos a perseguir aqueles que supostamente extorquem nossos negócios e garantir que eles sejam responsabilizados. “

Adolescentes acusados de envolvimento com hack da TfL

Os dois adolescentes também foram acusados por [Autoridades do Reino Unido](#) com ofensas relacionadas ao ataque cibernético de agosto de 2024 à Transport for London (TfL).

Eles foram acusados de conspirar para cometer atos não autorizados contra a TfL sob a Lei de Uso Indevido de Computadores e compareceram ao Tribunal de Magistrados de Westminster em 18 de setembro.

Flowers foi [inicialmente preso](#) por suspeita de envolvimento no hack da TfL em 6 de setembro de 2024, aos 17 anos, momento em que os investigadores da NCA identificaram mais evidências potenciais de crimes contra empresas de saúde dos EUA.

Como resultado, ele também foi acusado em 18 de setembro de 2025 de conspirar com outras pessoas para se infiltrar e danificar as redes da SSM Health Care Corporation e tentar fazer o mesmo com as redes da Sutter Health, ambas sediadas nos EUA.

Jubair também foi acusado de acordo com a Lei de Regulamentação de Poderes de Investigação (RIPA) do Reino Unido por não divulgar o PIN ou as senhas dos dispositivos apreendidos com ele.

O hack da TfL afetou dados pessoais confidenciais de cerca de 5000 clientes. Essas informações incluíam dados de reembolso do Oyster, abrangendo números de contas bancárias e códigos de classificação.

Isso teria custado ao operador de transporte cerca de £ 30 milhões (US \$ 40,6 milhões), incluindo £ 5 milhões (US \$ 6,7 milhões) em apoio externo para se recuperar do incidente.

Novo golpe na Aranha Dispersa

As acusações contra Flowers e Jubair seguem o [Prisões](#) de quatro outros membros suspeitos do Scatter Spider pelas autoridades do Reino Unido em julho de 2025.

Os quatro indivíduos, três dos quais eram adolescentes no momento da prisão, são suspeitos de envolvimento nos ataques de abril de 2025 à Marks & Spencer, à Co-op e à Harrods.

O vice-diretor Paul Foster, chefe da Unidade Nacional de Crimes Cibernéticos da Agência Nacional de Crimes (NCA), descreveu as acusações como um “passo fundamental” em uma “investigação longa e complexa”.

“Este ataque causou interrupções significativas e milhões em perdas para a TfL, parte da infraestrutura nacional crítica do Reino Unido”, disse ele, “No início deste ano, a NCA alertou sobre um aumento na ameaça de cibercriminosos baseados no Reino Unido e em outros países de língua inglesa, dos quais o Scattered Spider é um exemplo claro. “

Comentando as acusações contra Jubair e Flowers, Jake Moore, consultor global de segurança cibernética da ESET e ex-policia do Reino Unido, destacou o crescente sucesso da aplicação da lei na identificação e coleta de evidências para processar os cibercriminosos.

HoweVer, ele alertou que ainda pode haver desafios significativos neste processo.

“Coletar evidências sólidas suficientes para produzir no tribunal e processar é o aspecto mais difícil em qualquer investigação de crimes cibernéticos, por isso será vital que essas agências trabalhem minuciosamente para localizar provas definitivas de seu envolvimento”, observou ele.

“É altamente provável que esses membros da gangue tenham reduzido suas evidências e trilhas de comunicação ao mínimo, se é que o farão, o que causará frustrações na investigação”, acrescentou Moore.

No início de setembro, foi [reportado](#) que o Scattered Spider, juntamente com outros 14 grupos de ransomware, anunciou sua “aposentadoria”. No entanto, esses anúncios foram recebidos com ceticismo por especialistas em segurança.

As prisões e acusações contra Jubair e Flowers seguiram uma investigação colaborativa entre agências de aplicação da lei no Reino Unido, EUA, Holanda, Romênia, Canadá e Austrália.