
Judiciário federal dos EUA reforça segurança após escalada de ataques c

Data: 2025-08-09 03:09:03

Autor: Inteligência Against Invaders

Inteligência Against Invaders

2025-08-08 07:45

O judiciário federal dos EUA anunciou proteções de segurança cibernética mais fortes para documentos judiciais confidenciais após “recentes ataques cibernéticos escalonados” em seu sistema de gerenciamento de casos.

A declaração segue relatos de que o sistema federal de arquivamento de casos foi violado por agentes de ameaças, expondo documentos judiciais confidenciais em vários estados dos EUA.

O Escritório Administrativo dos Tribunais dos Estados Unidos (AOUSC) disse que os ataques recentes são de natureza sofisticada e persistente. Ele observou que a natureza sensível de alguns documentos mantidos neste sistema são alvos de interesse para uma série de agentes de ameaças.

“A grande maioria dos documentos arquivados no sistema eletrônico de gerenciamento de casos do Judiciário não é confidencial e, de fato, está prontamente disponível ao público, o que é fundamental para um sistema judicial aberto e transparente. No entanto, alguns registros contêm informações confidenciais ou proprietárias que são seladas da vista do público”, escreveu o AOUSC em um [soltar](#) datado de 7 de agosto.

O judiciário está trabalhando com os tribunais para mitigar o impacto dos documentos violados nos litigantes afetados.

Além disso, os tribunais de todo o país vêm implementando procedimentos mais rigorosos para restringir o acesso a documentos confidenciais em circunstâncias cuidadosamente controladas e monitoradas, acrescentou o AOUSC.

Documentos judiciais confidenciais supostamente expostos por hack

O anúncio da AOUSC é provavelmente em resposta a um [relatório](#) pelo Politico em 6 de agosto que

o sistema eletrônico de arquivamento de casos usado pelo judiciário federal havia sido violado em uma grande intrusão cibernética.

De acordo com duas pessoas com conhecimento do incidente, teme-se que o ataque tenha comprometido as identidades de informantes confidenciais envolvidos em casos criminais em vários tribunais distritais federais.

As fontes anônimas disseram ao Politico que os atores do estado-nação são amplamente suspeitos de envolvimento no hack.

Acredita-se que o incidente tenha afetado o sistema federal de gerenciamento de casos do judiciário, incluindo um componente usado por profissionais jurídicos para fazer upload e gerenciar arquivos de casos.

Outras informações confidenciais mantidas em documentos judiciais que não estão disponíveis publicamente incluem pessoas cujas identidades são protegidas por ordens judiciais ou legislação, como menores.

Sistema judicial é o principal alvo dos invasores

Os documentos judiciais são um dos principais alvos de uma série de agentes de ameaças, incluindo grupos de estados-nação para fins de espionagem, agentes mal-intencionados que tentam interromper ou influenciar casos individuais e cibercriminosos com motivação financeira que usam dados judiciais confidenciais para extorquir indivíduos e organizações.

Em 2022, um membro do Congresso dos EUA [revelado](#) que um sistema público de gerenciamento de documentos usado pelos tribunais dos EUA foi comprometido por um ataque cibernético em 2020.

Após o incidente, o AOUSC prometeu que documentos judiciais confidenciais agora seriam armazenados em um “sistema de computador autônomo seguro” e não carregados no sistema público de gerenciamento de documentos.

Em setembro de 2024, o presidente do Comitê de Tecnologia da Informação da Conferência Judicial e o juiz do Tribunal de Apelações Michael Y. Scudder [Avisado](#) de crescentes ameaças aos sistemas de TI do judiciário, inclusive por adversários estrangeiros com o objetivo de semear desconfiança no governo dos EUA.

Em junho de 2025, o Tribunal Penal Internacional (TPI) [reportado](#) Ele foi atingido por um incidente de segurança cibernética “sofisticado e direcionado”.

O ICC já havia sofrido um ataque em seus sistemas de TI em setembro de 2023, que mais tarde foi confirmado como [Relacionado à espionagem](#).