CORREIO BRAZILIENSE

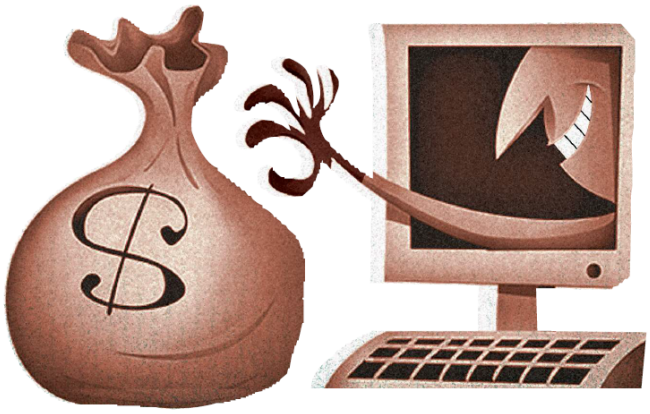
Publicado em 23/04/2024 - 05:56

Sistema de pagamentos do governo é alvo de ataques

Ofensiva ao sistema de pagamento do governo

Polícia Federal e Abin apuram acesso indevido ao software usado pelo Tesouro Nacional, com suspeita de desvio de recursos

» RENATO SOUZA



Criminosos que atuam na internet conseguiram acessar o Sistema Integrado de Administração Financeira (Siafi), usado pelo Tesouro Nacional para fazer todo o processamento patrimonial, contábil e execução financeira do governo federal. O programa é usado também por Legislativo e Judiciário. A suspeita é de que tenham ocorrido desvios de recursos para contas particulares, por meio de ordens de pagamento. A Polícia Federal abriu um inquérito para investigar o caso. Já a Agência Brasileira de Inteligência (Abin) informou, em nota, que acompanha o caso "em colaboração com as autoridades competentes".

Após o acesso indevido, que ocorreu neste mês, o Tesouro Nacional aplicou regras adicionais de segurança, a fim de estabelecer camadas para dificultar qualquer acesso indevido. As primeiras diligências apontam que os criminosos usaram certificados de gestores do sistema para dar os comandos.

O ministro da Fazenda, Fernando Haddad, afirmou que o sistema não foi comprometido, mas sustentou não saber detalhes do caso. "A informação que eu tenho é parcial, de que o problema não é do Siafi, não é do sistema. Provavelmente, foi de autenticação de acesso. Isso está sendo apurado, como alguém teve acesso tendo sido autenticado. Não foi a ação de um hacker que quebrou a segurança. É isso que a PF está apurando e está rastreando para chegar aos responsáveis", destacou, em conversa com jornalistas.

Haddad afirmou não ter sido informado sobre eventuais valores que podem ter sido desviados e frisou que conversaria com o presidente Luiz Inácio Lula da Silva a respeito do assunto. "Eu não tenho essa informação, pois isso está sendo mantido em sigilo, inclusive, dos ministros. Estava entre o Tesouro e a PF. Eu fiquei sabendo no mesmo momento que vocês (jornalistas). Inclusive, vou agora informar ao presidente", completou.

Em nota, o Tesouro Nacional negou que se trate de uma invasão, mesmo reconhecendo o acesso indevido ao sistema. "O episódio não configura uma invasão, mas, sim, uma utilização indevida de credenciais obtidas de modo irregular. As tentativas de realizar operações na plataforma foram identificadas e não causaram prejuízos à integridade do sistema", ressaltou o órgão. "Todas as medidas necessárias vêm sendo tomadas pela STN em resposta ao caso, incluindo a implementação de ações adicionais para reforçar a segurança do sistema."

O Tesouro declarou estar colaborando com as investigações, e também não informou se recursos foram desviados. "O Tesouro Nacional trabalha em colaboração com as autoridades competentes para a condução das investigações; e reitera seu compromisso com a transparência, a segurança dos sistemas governamentais e a preservação do adequado zelo das informações, até o término das apurações", enfatizou o texto.

Em comunicado, o Ministério da Gestão e da Inovação em Serviços Públicos seguiu a mesma linha. Disse que "o episódio não configura uma falha de segurança no gov.br, mas, sim, uma utilização indevida de credenciais obtidas de modo irregular, que já está sendo investigada pelos órgãos competentes".

"O ministério recomenda a todos os usuários que utilizem as ferramentas de segurança disponíveis no gov.br, como a validação em duas etapas e a gestão de dispositivos, que protegem a conta gov.br. Caso seja necessário, os usuários podem utilizar os canais oficiais da pasta para sanar dúvidas sobre a sua conta, como o gov.br/atendimento", acrescentou.

Modus operandi

Os crackers (termo usado para se referir a quem usa conhecimentos de informática para causar danos e prejuízos) tiveram acesso a contas do gov.br de gestores do Siafi, assim como às senhas, acessaram os serviços e liberaram pagamentos.

A informação foi confirmada pelo **Correio** com fontes na Polícia Federal. As credenciais teriam sido realizadas por meio de ataques de "fishing", palavra em inglês que significa "pescaria". Nesse tipo de cibercrime, pessoas mal-intencionadas enviam iscas, como links de páginas falsas, para coletar os dados dos alvos. Acreditando estar em uma página oficial do governo ou de bancos, por exemplo, a vítima insere informações que são usadas em golpes e fraudes.

Uma das hipóteses é que páginas falsas, que imitam o layout (aparência) dos sites oficiais do governo, foram usadas para enganar os servidores públicos. As informações teriam sido coletadas durante meses, silenciosamente, até que fossem reunidas credenciais suficientes para realizar um ataque em larga escala.

Em uma das tentativas, o cracker teria tentado fazer uma transferência via Pix, ou seja, instantânea. Mas o sistema detectou que o CPF, chave Pix utilizada, era o mesmo entre quem enviou o pagamento e quem receberia, o que é vedado pelas regras do governo. Após isso, o Tesouro Nacional teria passado a exigir o uso de certificado digital.

Porém, mesmo com a medida, foram identificadas tentativas de invadir o sistema usando certificado digital emitido por empresas privadas. Por conta disso, a regra passou a obrigar o uso de certificados emitidos pelo Serviço Nacional de Processamento de Dados (Serpro).

Veículo: Impresso -> Jornal -> Jornal Correio Braziliense - Brasília/DF

Seção: Política **Pagina:** 2