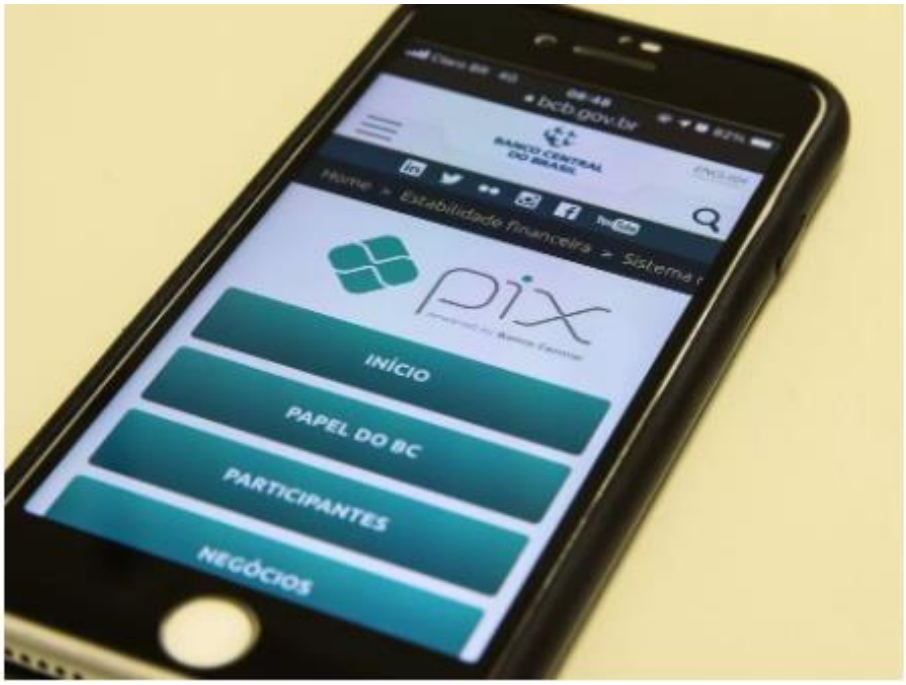
Vazamento afeta 395 mil chaves do Pix

Caso ocorreu no Banese e é a maior falha até agora no sistema de transações instantâneas

Por Álvaro Campos, Mariana Ribeiro e Estevão Taiar, Valor — São Paulo
01/10/2021 07h57 Atualizado há 41 minutos



Marcello Casal Jr/ / Agência Brasil

Poucos dias após atingir 100 milhões de usuários, o Pix enfrenta seu maior teste. Hackers usaram duas contas no Banco do Estado do Sergipe (Banese) e acessaram os dados do Diretório de Identificadores de Contas Transacionais (Dict), obtendo informações de 395.009 chaves de usuários do sistema de pagamentos instantâneos que não são de clientes do banco.

O problema foi revelado pelo Banco Central (BC) e confirmado pelo Banese em comunicado ao mercado na noite de ontem. O BC atribuiu o vazamento a “falhas pontuais” em sistemas da instituição financeira. Segundo a autoridade monetária, não foram expostos dados sensíveis, como senhas, informações de movimentações ou saldos financeiros em contas transacionais, ou outras informações sob sigilo bancário. “As informações obtidas são de natureza cadastral, que não permitem movimentação de recursos, nem acesso às contas ou a outras informações financeiras”, disse o BC em nota.

Em resposta a questionamentos do Valor, o BC reforçou que não foi explorada nenhuma vulnerabilidade em qualquer sistema seu. “O hacker acessou as informações utilizando a infraestrutura tecnológica do sistema do Banese, explorando falhas graves de segurança no aplicativo da instituição. Em suma, quem acessou o Dict foi o próprio participante Banese. O desconhecido não autorizado jamais teve acesso direto aos sistemas do BC.”

Ainda assim, uma leitura preliminar no mercado é a de que, de posse das chaves, o hacker tem informações que facilitam a aplicação de golpes — ligando para uma pessoa e se passando pelo banco dela, por exemplo.

A autoridade monetária informou que as pessoas que tiveram seus dados cadastrais obtidos a partir do incidente serão notificadas exclusivamente por meio do aplicativo de sua instituição de relacionamento. “Nem o BC nem as instituições participantes usarão quaisquer outros meios de comunicação aos usuários afetados, tais como aplicativos de mensagem, chamadas telefônicas, SMS ou e-mail”, frisou.

O BC afirmou ainda que adotou “as ações necessárias para a apuração detalhada do caso” e que aplicará as medidas sancionadoras previstas na regulação. “Mesmo não sendo exigido pela legislação vigente, por conta do baixo impacto potencial para os usuários, o BC decidiu comunicar o evento à sociedade, à vista do compromisso com a transparência que rege sua atuação”, explicou.

Já o Banese afirmou que as chaves vazadas são exclusivamente do tipo telefone, e que o acesso às contas dos banco provavelmente foi obtido mediante engenharia social (phishing ou similar). A instituição afirmou que o evento não afetou a confidencialidade de senhas, histórico de transações ou demais informações financeiras de seus clientes. “Tais consultas foram realizadas no Diretório de Identificadores de Contas Transacionais (Dict), administrado pelo Banco Central do Brasil e de acesso restrito às instituições que iniciam o procedimento para realização de uma transação por Pix”.

Segundo o Banese, o diretório contém informações de natureza cadastral, como nome, CPF, banco em que a chave está registrada, agência, conta e outros dados técnicos utilizados para fins de controle antifraude, tais como a data de abertura da conta e data de registro da chave. “Nos termos das legislações aplicáveis, o Banese comunicou o ocorrido à Autoridade Nacional de Proteção de Dados (ANPD) e, em conjunto com o Banco Central, tem trabalhado na apuração e comunicação dos fatos. De forma tempestiva foram adotadas ações de contenção e medidas técnicas, como a revogação do acesso às duas contas utilizadas e a implementação de mecanismos de segurança visando evitar que casos semelhantes voltem a ocorrer”.

Apesar de ainda não haver detalhes sobre o incidente, um especialista em segurança da informação disse que, a priori, não parece haver uma fragilidade séria no Pix. Ainda assim, aponta, que, com posse de diversos dados dos usuários, os criminosos podem armar outros tipos de golpes usando engenharia social. “É difícil avaliar sem ter muitos detalhes, mas parece que não é uma falha do Pix. A maior parte dos bancos criou estruturas separadas nos seus data centers para o Pix, tanto pelo volume de transações como por questões de segurança”, afirmou a fonte, que não quis ser identificada.

Já Rafael Zanatta, diretor da Associação Data Privacy Brasil de Pesquisa, tem uma visão mais crítica. Para ele, o BC tem responsabilidade regulatória, porque foi quem estabeleceu todas as políticas institucionais do Pix, os critérios de segurança da informação dos sistemas das instituições autorizadas a participar da plataforma. “O BC tem falhado em construir uma metodologia mais pró-ativa de inspeção. Tem sido muito passivo. Só estabelece os critérios e depois verifica o que acontecer após o dano. O caso do Banese parece ser bem sério e coloca em discussão a necessidade de uma cooperação técnica mais robusta entre o BC e a ANPD”.

Nesta semana, o Valor mostrou que a empresa de cibersegurança israelense Check Point, ao realizar uma varredura global, descobriu um aplicativo malicioso (malware) batizado de PixStealer. Voltado para o sistema operacional Android, o PixStealer estava sendo distribuído na Google Play Store como um falso nome de “PagBank Cashback”. Ao instalá-lo, quando o usuário abria seu aplicativo de banco para acessar o Pix, o malware mostrava à vítima uma janela de sobreposição, fazendo com que o usuário não pudesse ver os movimentos do criminoso. Assim, o golpista identificava a quantidade de dinheiro disponível e o transferia, usando o Pix, para outra conta.