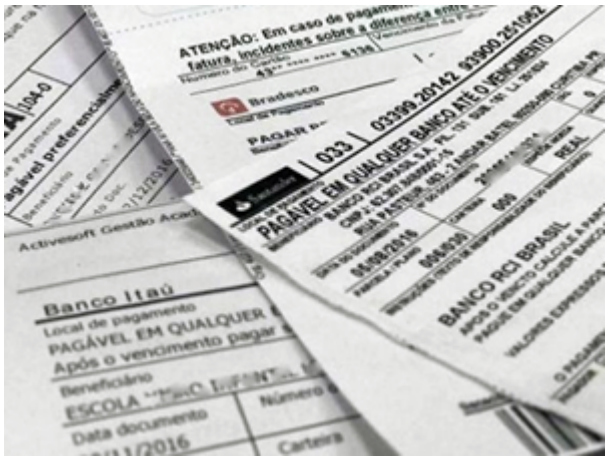
Scaff Jr. e Ferraz: Crescimento alarmante da fraude digital em boletos

29/03/2023

Em uma era digital como a presente, os sistemas tecnológicos estão expostos a inúmeros *malwares* que podem adentrar, sem qualquer autorização, nos dispositivos digitais e realizar uma série de modificações com os mais diversos intuitos, como obtenção de dados, utilização de rede remota, além do cometimento de fraudes.

Divulgação



Reprodução

Nesse último caso, há um golpe cuja incidência vem crescendo de forma alarmante no Brasil. São os denominados *bolwares*, isto é, *malwares* criados especificamente para adulteração de boletos bancários diretamente no computador do usuário, desviando os valores pagos para a conta de criminosos.

A incidência dessa espécie de golpe apresentou crescimento da ordem de 45% durante a pandemia [1], mas não se trata de algo novo, haja vista que a Federação Brasileira de Bancos (Febraban) alerta a população sobre ele desde 2018. Por essa razão, ela lançou uma plataforma de cobrança que permite o registro de todos os boletos, com inserção de informações no documento como CPFs/CNPJs do emissor e do pagador.

Ainda assim, os consumidores não estão completamente protegidos desse tipo de vírus. Isso porque o computador pode ser infectado por esse *malware* de diversas maneiras, como clicando em links e anexos por intermédio de *e-mails* falsos, acessando *links* em *sites* contaminados, realizando *download* de *softwares* piratas ou até mesmo por invasões na rede.

Não bastasse isso, esse tipo de vírus é silencioso e não pode ser facilmente identificado. Após instalado, ele observa furtivamente a atividade do usuário no navegador de internet ou e-mail [2]. Tão logo seja possível detectar que o usuário gerou um boleto, o vírus altera os dados de sua linha digitável e modifica a conta de recebimento original do beneficiário pela conta dos criminosos.

Dessa forma, ainda que o consumidor pague o boleto acreditando ser o documento correto, o valor nunca será creditado ao emitente por ter sido desviado para conta de terceiros.

Infelizmente, esse tipo de *malware* é bastante comum e tem sido alvo de alerta pelas empresas de tecnologia justamente por ser muito difícil de ser identificado [3].

Quando esse tipo de golpe é efetivado com sucesso, a vítima realiza o pagamento do boleto para uma conta que não pertence ao verdadeiro credor. Embora acredite ter cumprido a obrigação, o valor segue em aberto para o verdadeiro beneficiário.

Copyright © 2026 Consultor Jurídico

A partir de então, iniciam-se as cobranças que, sob a ótica do consumidor, são indevidas, o que ocasiona a judicialização desses casos.

Como as adulterações são, na maioria das vezes, difíceis de serem identificadas de imediato, a saída para o fornecedor é demonstrar que o boleto enviado de sua máquina era idôneo e que as modificações ocorreram por *bolware* presente no computador da própria vítima. Tal comprovação é possível, desde que acompanhada por uma equipe de especialistas em detecção de *malwares*, *bolwares* e outros tipos de itens maliciosos em dispositivos eletrônicos.

Nesses casos, é importante demonstrar a adoção de mecanismos de proteção e defesa do sistema do remetente, justamente para evidenciar que a adulteração ocorreu por falha na segurança do dispositivo do próprio consumidor. É interessante ao credor adotar uma ferramenta que realize o envio dos boletos via *Electronic Data Interchange* (*EDI)* [4] — Intercâmbio Eletrônico de Dados.

Esse sistema faz a integração de dados entre beneficiário e pagador. Resumidamente, ele integra o fluxo de comunicação das empresas à gestão das transações comuns, de modo que automaticamente realiza o envio e recebimento de ordens de pagamento, emissão de notas fiscais etc.

Dentre os benefícios do uso dessa tecnologia, consta a segurança concedida na troca dos dados, porque elimina por completo qualquer intervenção humana. Esse tipo de sistema, portanto, impede que sejam realizadas alterações indevidas nos arquivos enviados, por estes não dependerem de encaminhamento manual.

Além disso, os servidores de e-mail possuem uma série de mecanismos de defesa para evitar que *malwares* consigam adentrar o sistema do usuário e adulterar informações. Dentre esses mecanismos, o mais relevante chama-se *Domain-based Message Authentication, Reporting & Conformance* (Dmarc) [5] e, quando configurado, garante a autenticidade de um e-mail.

Em suma, essa ferramenta protege o servidor contra a falsificação de domínios, de modo que impede o envio e o recebimento de mensagens por domínios falsificados ou não autorizados. Assim, não é possível que um *bolware* acesse o servidor do fornecedor e envie e-mails contendo documentação adulterada.

Além dos mecanismos de prevenção e segurança, na maior parte dos casos são claros os indícios de fraude, ou pelo menos perceptíveis, principalmente no momento da realização da operação pelo consumidor.

Por isso, os consumidores devem sempre se atentar aos indícios de adulteração presentes nos boletos fraudados. Antes de realizarem o pagamento de qualquer boleto, devem se pautar com diligência e atenção, a fim de evitar maiores problemas, sobretudo em se sabendo dos altos índices de fraudes que ocorrem envolvendo essa forma de pagamento.

É importante conferir se as linhas digitáveis do boleto são iguais em todos os fragmentos do documento, pois a adulteração pode ocorrer somente em uma delas, o que basta para o desvio do pagamento.

Outra atitude é a verificação do logotipo do banco, pois esse logotipo, após a adulteração, pode ficar fora de formatação, ou mesmo não coincidir com a instituição originariamente escolhida pelo credor. Além disso, ao conferir o logotipo, é prudente analisar novamente a linha digitável, pois os três primeiros números devem corresponder ao código daquele banco junto ao Banco Central.

Porém, o mais relevante ainda é a conferência dos dados do beneficiário em uma tela prévia à confirmação do pagamento. Eles são indicados pelo banco pagador exatamente por questões de segurança. Esses dados são os mesmos que aparecem no comprovante de pagamento após efetivação da transação. Havendo divergência com os dados constantes no boleto, não deve ser realizado o pagamento ou, caso tenha sido efetivada a transação, o banco deve ser imediatamente contatado para desfazê-la.

A cautela no momento do pagamento tem sido o ponto-chave da jurisprudência para decidir se a dívida é ou não exigível pelo fornecedor. A ausência de observância dos deveres de cuidado e vigilância no ato do pagamento configuram culpa exclusiva da vítima, mesmo em casos analisados sob a incidência do Código de Defesa do Consumidor. Nesse sentido, os Tribunais de Justiça de São Paulo [6], Paraná [7], Mato Grosso do Sul [8] e Rio Grande do Sul [9] entendem não haver responsabilidade do fornecedor pelos danos oriundos do golpe.

Sob essa perspectiva, o valor pode ser novamente cobrado pelo credor, desde que, obviamente, ele prove que adotou os mecanismos de segurança acima mencionados e que o vírus estava no computador do consumidor.

Copyright © 2026 Consultor Jurídico

Por fim, conforme informado no início do artigo, a Febraban disponibilizou uma ferramenta por meio da qual é possível garantir a idoneidade do boleto. Mediante uma simples consulta ao sítio eletrônico www.buscabanco.org.br verifica-se o boleto original emitido pelo credor, o que evita o pagamento de documentos adulterados.

[1] Informações disponíveis em: https://revistapegn.globo.com/Administracao-de-empresas/noticia/2020/05/nova-versao-do-golpe-do-boleto-faz-mais-vitimas.html. Acesso em: 4 maio 2022.

[2] Informações disponíveis em: https://aciapi.com.br/cuidado-com-o-virus-bolware-para-evitar-ser-vitima-do-golpe-do-boleto/. Acesso em: 4 maio 2022.

[3] Informações disponíveis em: https://blog.certisign.com.br/bolware-o-virus-que-e-capaz-de-adulterar-boletos-digitais/. Acesso em: 4 maio 2022. Mais informações disponíveis em: https://servcloud.com.br/bolware-te-ajudamos-a-nao-cair-nesse-golpe/. Acesso em: 4 maio 2022.

[4] Para saber o que é EDI e suas funcionalidades: https://finnet.com.br/o-que-e-edi/. Acesso em: 9 mar. 2023.

[5] Em tradução livre, "Autenticação, relatórios e conformidade de mensagens baseadas em domínio". Para Saber mais, acesse o site da organização: https://dmarc.org/.

[6] TJ-SP – AC: 10032347920198260010 SP 1003234-79.2019.8.26.0010, relator: Costa Netto, data de julgamento: 30 jun. 2021, 6ª Câmara de Direito Privado, data de publicação: 30 jun. 2021.

[7] TJ-PR – APL: 14835651 PR 1483565-1 (Acórdão), relator: Guilherme Freire de Barros Teixeira, data de julgamento: 21 jul. 2016, 10ª Câmara Cível, data de publicação: DJ: 1865 17 ago. 2016.

[8] TJ-MS – AC: 08137713820198120001 MS 0813771-38.2019.8.12.0001, relator: des. Marco André Nogueira Hanson, data de julgamento: 2 ago. 2021, 2ª Câmara Cível, data de publicação: 6 ago. 2021.

[9] TJ-RS – AC: 50009965920208210095 RS, relator: Paulo Sérgio Scarparo, data de julgamento: 26 ago. 2021, 17ª Câmara Cível, data de Ppublicação: 3 set. 2021.

Fonte: https://conjur.jumps.com.br/2023-mar-29/scaff-jr-ferraz-crescimento-alarmante-fraude-digital-boletos2/

Copyright © 2026 Consultor Jurídico