SEK Security Ecosystem Knowledge

BOLETIM DE INTELIGÊNCIA

Cibercriminosos aumentam uso de boletos falsos em golpes contra diversos setores

CRÍTICO

TLP: WHITE

BOLETIM DE INTELIGÊNCIA

O QUE É

O Boletim de Inteligência é uma publicação da SEK que esclarece, de maneira breve, acontecimentos ou notícias recentes e relevantes de Cibersegurança. A partir do contexto de cada boletim, trazemos uma análise detalhada com recomendações a serem seguidas na situação reportada ou em casos similares.

INFORMATION SEVERITY FLAG

Para facilitar a identificação do nível de urgência e da gravidade da situação comunicada, segue um sistema intuitivo de classificação a partir de três cores, indicadas na capa de cada Boletim de Inteligência. Cada cor representa a criticidade do que está sendo reportado.

VERMELHO

Material focado em relatar ocorrências e casos urgentes, que merecem ação imediata quanto ao fato comunicado, pois o impacto tende a ser instantâneo e trazer consequências severas.

LARANJA

Material focado em relatar ocorrências e casos críticos ou fora dos padrões, que merecem ação a curto prazo, uma vez que podem trazer impactos graves a diversos setores.

AMARELO

Material focado em relatar ocorrências e casos sérios, porém recorrentes. Esses acontecimentos merecem ação a médio prazo para uma melhora incremental da segurança cibernética na organização.

Nota: A Information Severity Flag da SEK se refere à criticidade da informação e é utilizada de forma complementar ao **Traffic Light Protocol (TLP)**, que trata da classificação da informação.

BOLETIM DE INTELIGÊNCIA

Cibercriminosos aumentam uso de boletos falsos em golpes contra diversos setores

SUMÁRIO

Resumo	04
Entendendo o golpe do boleto falso	04
Outras campanhas similares	10
Conclusão	12
Recomendações	12
Referências	15

01. Resumo

Nesta última década, os boletos bancários têm sido um dos meios de pagamento mais populares entre cidadãos brasileiros. De acordo com a **Federação Brasileira de Bancos** (Febraban), **mais de 4,2 bilhões de documentos foram pagos no país em 2023**. No entanto, junto à popularidade dos boletos, cresceu também a incidência de golpes envolvendo esse meio de pagamento.

A SEK tem notado essa multiplicação em casos envolvendo boletos falsos no Brasil. Consumidores de companhias de diversas áreas, incluindo da infraestrutura crítica, já apontaram terem sido vítimas de ataques que utilizavam os arquivos fraudulentos, ocasionando em perdas consideráveis. Nos últimos meses, a SEK também notificou o CERT.br sobre uma nova campanha de *phishing* que explorava esse método com o objetivo de se passar pelo NIC.br, organização responsável pelo Registro BR.

Com todos esses acontecimentos em vista, este artefato da equipe de *Cyber Threat Intelligence* busca abordar **as principais informações sobre o aumento desses ataques cibernéticos**, considerando investigações da própria equipe de detecção e resposta a incidentes. Além disso, o Boletim de Inteligência fornece recomendações práticas sobre como consumidores e organizações de diversos setores da indústria podem se proteger contra as invasões.

02. Entendendo o golpe do boleto falso

Como apontado neste Boletim, os golpes relacionados aos boletos falsos são mais uma prática criminosa que tem se tornado cada vez mais frequente e sofisticada. Esse tipo de ataque cibernético ocorre a partir do momento em que cibercriminosos emitem boletos com informações alteradas, desde o código de barras até o valor, por exemplo.

Do ponto de vista dos atores de ameaça, a prática é eficaz justamente porque **os boletos podem ser idênticos aos originais, exceto pelos dados bancários modificados**. A semelhança dificulta que clientes identifiquem a fraude antes de efetuarem o pagamento. Dessa forma, os invasores são capazes de **redirecionar os pagamentos para contas bancárias sob seu controle** em vez das contas legítimas usadas pelas companhias prestadoras de serviço ou fornecedoras.

O golpe pode ocorrer no momento de uma compra online, em caso de sites falsificados, ou até mesmo por meio de **e-mails de *phishing*, nos quais os criminosos se passam por instituições legítimas**.

A investigação SEK

De acordo com pesquisas e investigações da SEK, a onda de ataques contra diversas empresas a partir de boletos falsificados teve início ainda em janeiro deste ano.

Desde então, diversas organizações, de áreas críticas da economia ou não, foram exploradas por criminosos que visam atingir seus consumidores.

Os atores de ameaça **fingem ser dos setores financeiros dessas empresas** para enviar, por meio de e-mails, arquivos falsificados aos clientes dessas companhias. Nessa campanha, a justificativa é sempre a mesma.

Os supostos responsáveis financeiros das instituições apontam que houve um **erro no software de emissão de Notas Fiscais**, e, por isso, ocorreu uma divergência na base de cálculo de alíquotas como PIS, ICMS e Cofins.

Desse modo, os atacantes justificam que o boleto bancário recebido pelo consumidor por meio do *internet banking* ou de canais oficiais apresenta um valor errado.

Ou seja, apontam que o arquivo autêntico cobra um valor adicional, explorando essa justificativa para fazer com que a vítima pague o boleto assim que possível.

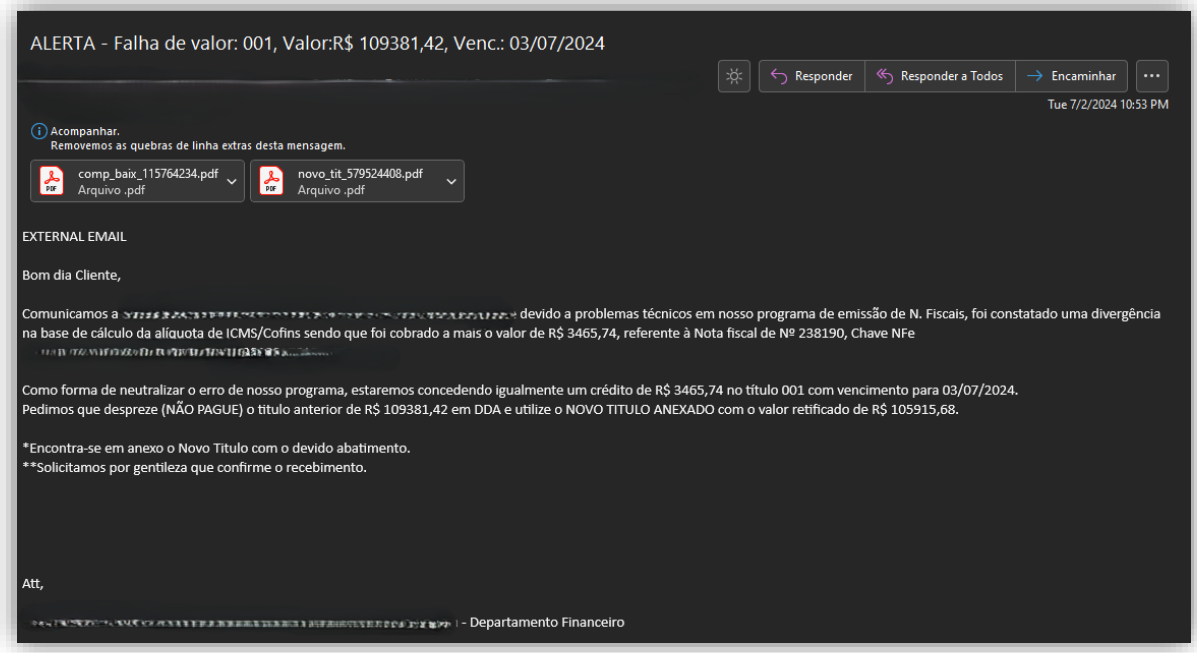


Figura 1 – E-mail falso utilizado para envio de boletos fraudulentos

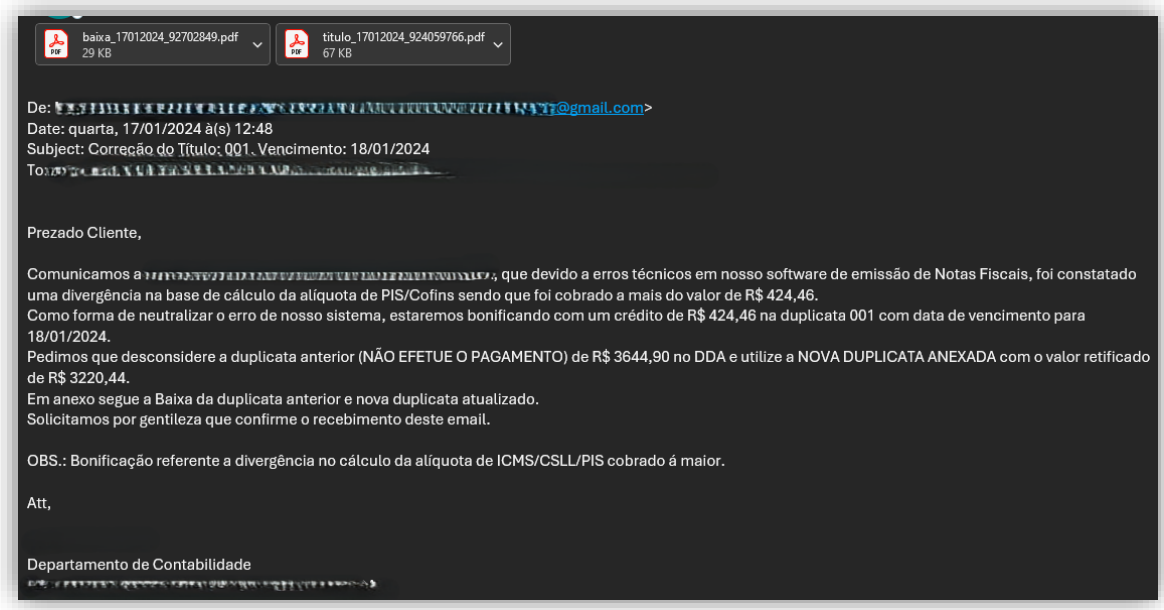


Figura 2 – E-mail falso utilizado para envio de boletos fraudulentos

Assim, os atacantes pedem que o cliente **desconsidere o boleto original e utilize somente o arquivo de boleto em .pdf enviado em anexo**, que conta com um suposto valor corrigido.

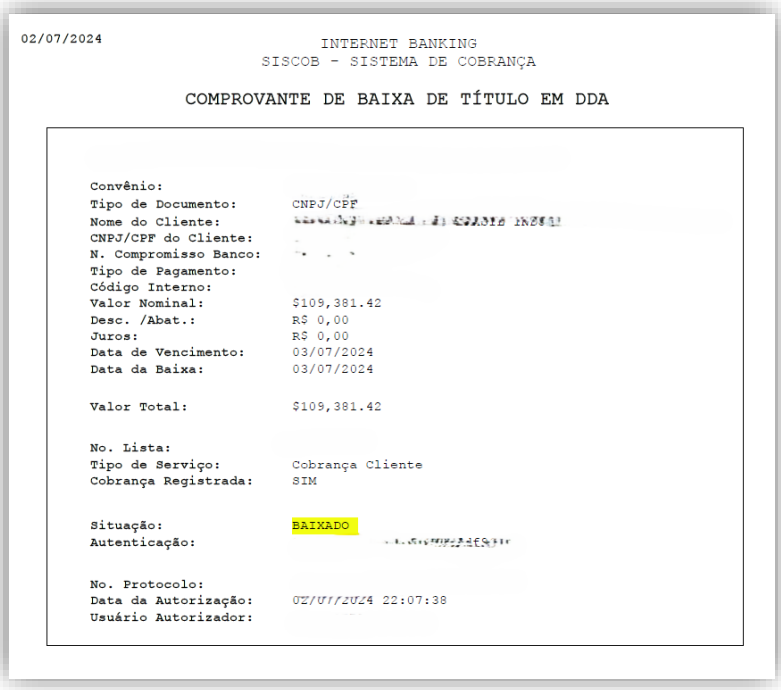
A maioria dos e-mails maliciosos observados pela SEK possui o mesmo padrão de assunto ou título. As comunicações citam a data do vencimento da fatura, bem como o número do título ou até mesmo o valor total desses boletos.

Outro padrão notado pela equipe é a utilização da técnica de *spoofing* de e-mail para a criação desses ataques. À primeira vista, o remetente da comunicação maliciosa parece real para as vítimas, já que **o nome disponibilizado no início da página antes do próprio endereço de e-mail é idêntico ao verdadeiro**. No entanto, a partir do momento em que o consumidor clica para visualizar mais informações sobre o remetente, nota que o endereço de e-mail utilizado é diferente.

Apesar de muito similar a uma comunicação oficial, o endereço é recente, provavelmente criado para a efetivação do golpe. Ele também se encontra **fora do domínio da organização legítima e utiliza serviços gratuitos, como Gmail, Yahoo e Hotmail**.

Além disso, as comunicações enviadas pelos cibercriminosos geralmente contêm dois anexos: um do comprovante de baixa de título e outro do boleto falso.

O comprovante de baixa de título conta com dados como o nome, CNPJ do cliente da companhia, valores idênticos aos originais devidos, códigos de autenticação e números de protocolo.



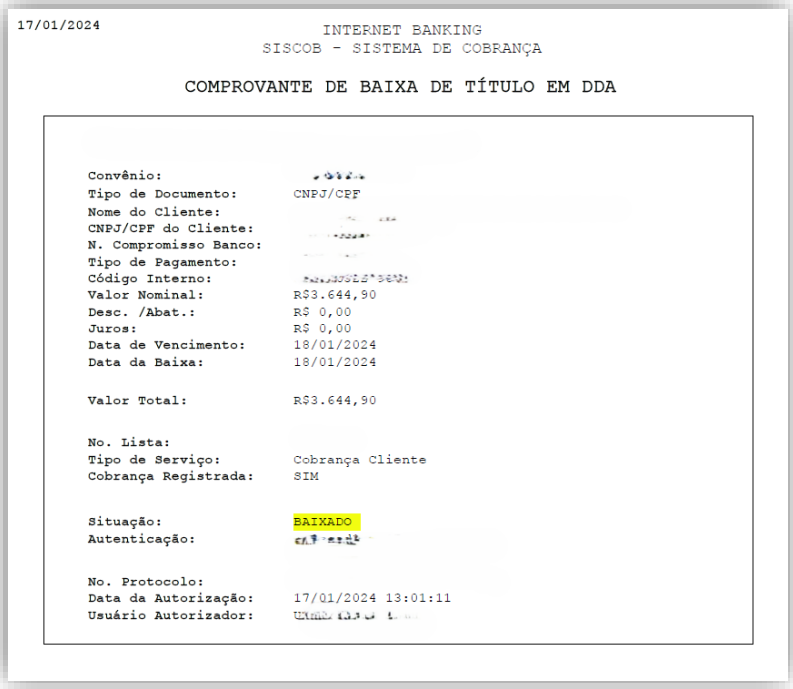
02/07/2024

INTERNET BANKING
SISCOB - SISTEMA DE COBRANÇA

COMPROVANTE DE BAIXA DE TÍTULO EM DDA

Convênio:	
Tipo de Documento:	CNPJ/CPF
Nome do Cliente:	[redacted]
CNPJ/CPF do Cliente:	
N. Compromisso Banco:	
Tipo de Pagamento:	
Código Interno:	
Valor Nominal:	$109,381.42
Desc. /Abat.:	R$ 0,00
Juros:	R$ 0,00
Data de Vencimento:	03/07/2024
Data da Baixa:	03/07/2024
Valor Total:	$109,381.42
No. Lista:	
Tipo de Serviço:	Cobrança Cliente
Cobrança Registrada:	SIM
Situação:	BAIXADO
Autenticação:	[redacted]
No. Protocolo:	
Data da Autorização:	02/07/2024 22:07:38
Usuário Autorizador:	

Figura 3 – Exemplo real de comprovante de baixa enviado por atacantes



17/01/2024

INTERNET BANKING
SISCOB - SISTEMA DE COBRANÇA

COMPROVANTE DE BAIXA DE TÍTULO EM DDA

Convênio:	[redacted]
Tipo de Documento:	CNPJ/CPF
Nome do Cliente:	
CNPJ/CPF do Cliente:	[redacted]
N. Compromisso Banco:	
Tipo de Pagamento:	
Código Interno:	[redacted]
Valor Nominal:	R$3.644,90
Desc. /Abat.:	R$ 0,00
Juros:	R$ 0,00
Data de Vencimento:	18/01/2024
Data da Baixa:	18/01/2024
Valor Total:	R$3.644,90
No. Lista:	
Tipo de Serviço:	Cobrança Cliente
Cobrança Registrada:	SIM
Situação:	BAIXADO
Autenticação:	[redacted]
No. Protocolo:	
Data da Autorização:	17/01/2024 13:01:11
Usuário Autorizador:	[redacted]

Figura 4 – Exemplo real de comprovante de baixa enviado por atacantes

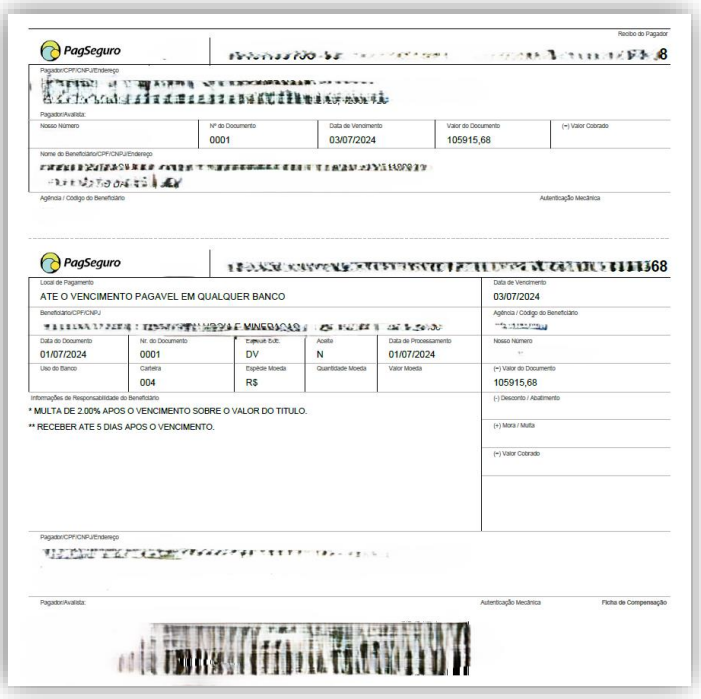
Enquanto isso, o boleto falso enviado pelos atores maliciosos, com um suposto valor corrigido, pode utilizar bancos diferentes dos usados pelas empresas verdadeiras.

Nos exemplos a seguir, o Banco Safra, apesar de renomado, não é o oficial da organização; mesma situação do boleto do banco virtual PagSeguro, que não é utilizado pela companhia real. No entanto, este não é o padrão absoluto. Diversos são os casos de boletos falsos que também contêm os mesmos bancos emissores das empresas autênticas.

Na maioria das ocorrências, os bancos online, como PagSeguro e Mercado Pago, são os mais utilizados na criação desses boletos fraudulentos. Ao longo dos últimos anos, vários processos entendem que a flexibilização nas exigências para cadastro acaba por dificultar o rastreamento do beneficiário, já que ele acaba sendo o CNPJ do próprio banco emissor.

Além disso, nos exemplos deste Boletim, o nome do beneficiário, isto é, aquele que recebe o dinheiro, também é idêntico ao legítimo. Apesar de todas as semelhanças, o pagamento do boleto bancário é direcionado para uma conta utilizada pelos invasores.

Investigações levantam a hipótese de que essa onda de ataques use contas de laranjas, ou seja, pessoas que emprestam suas contas bancárias para recebimento dessas quantias. Essa ação, muito comum no mundo do cibercrime, facilita o desvio desses valores e, em consequência, complica a recuperação do dinheiro pelas vítimas e autoridades. Em muitos casos, porém, essas contas também podem ser abertas em nome de terceiros que não têm conhecimento do golpe.


PagSeguro

Recibo do Pagador

Pagador/CPF/CNPJ/Endereço

Pagador/Avalista:

Nosso Número	Nº do Documento	Data de Vencimento	Valor do Documento	(=) Valor Cobrado
	0001	03/07/2024	105915,68	

Nome do Beneficiário/CPF/CNPJ/Endereço

Agência / Código do Beneficiário

Autenticação Mecânica

PagSeguro

Local de Pagamento

ATE O VENCIMENTO PAGAVEL EM QUALQUER BANCO

Data de Vencimento

03/07/2024

Beneficiário/CPF/CNPJ

Agência / Código do Beneficiário

Data do Documento	Nr. do Documento	Espécie Doc.	Aceite	Data do Processamento
01/07/2024	0001	DV	N	01/07/2024

Uso do Banco	Carteira	Espécie Moeda	Quantidade Moeda	Valor Moeda
	004	R$		

Nosso Número

(=) Valor do Documento

105915,68

Informações de Responsabilidade do Beneficiário

* MULTA DE 2.00% APOS O VENCIMENTO SOBRE O VALOR DO TITULO.

** RECEBER ATE 5 DIAS APOS O VENCIMENTO.

(-) Desconto / Abatimento

(+) Mora / Multa

(=) Valor Cobrado

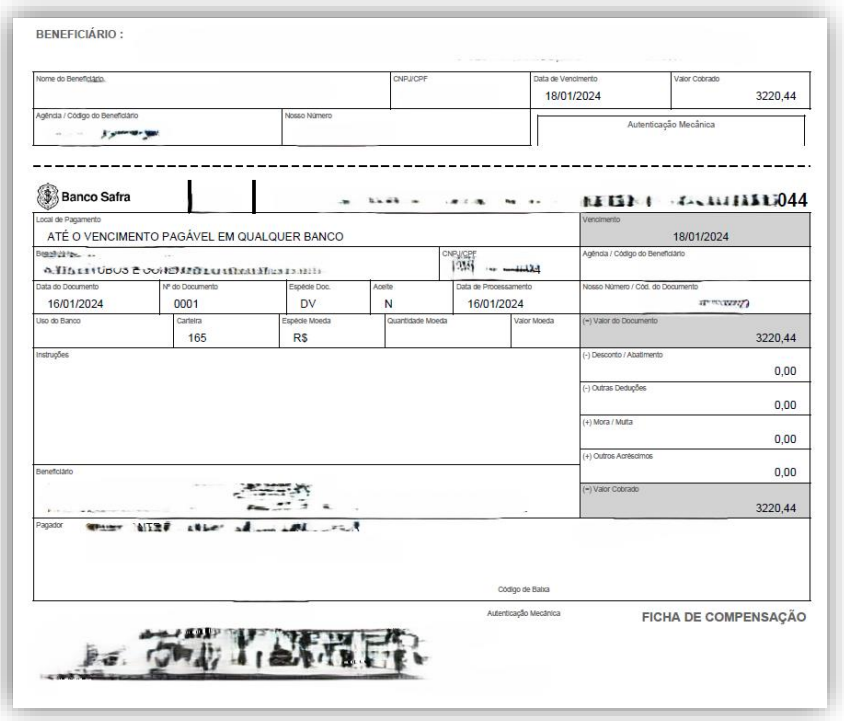
Pagador/CPF/CNPJ/Endereço

Pagador/Avalista:

Autenticação Mecânica

Ficha de Compensação

Figura 5 – Boleto falso estudado pela SEK com PagSeguro como banco emissor



BENEFICIÁRIO :

Nome do Beneficiário	CNPJ/CPF	Data de Vencimento	Valor Cobrado
		18/01/2024	3220,44
Agência / Código do Beneficiário	Nosso Número	Autenticação Mecânica	

Banco Safra

Local de Pagamento	Vencimento
ATÉ O VENCIMENTO PAGÁVEL EM QUALQUER BANCO	18/01/2024
Beneficiário	CNPJ/CPF / Agência / Código do Beneficiário

Data do Documento	Nº do Documento	Espécie Doc.	Aceite	Data de Processamento	Nosso Número / Cod. do Documento
16/01/2024	0001	DV	N	16/01/2024	

Uso do Banco	Carteira	Espécie Moeda	Quantidade Moeda	Valor Moeda	(=) Valor do Documento
	165	R$			3220,44

Instruções	
	(-) Desconto / Abatimento: 0,00
	(-) Outras Deduções: 0,00
	(+) Mora / Multa: 0,00
	(+) Outros Acréscimos: 0,00
Beneficiário	(=) Valor Cobrado: 3220,44
Pagador	

Código de Baixa

Autenticação Mecânica

FICHA DE COMPENSAÇÃO

Figura 6 – Boleto falso estudado pela SEK com Banco Safra como banco emissor

É importante apontar que outro ponto crítico dessa campanha é **a qualidade das informações** incluídas nos e-mails fraudulentos, desde os valores até os anexos. **Os criminosos obtiveram acesso a dados reais das organizações e de seus clientes**, como números de notas ficais eletrônicas, bancos usados para geração dos boletos, valores devidos pelos consumidores e os destinatários finais dos e-mails.

O uso desses dados exatos nos golpes tem como consequência e-mails e anexos extremamente convincentes, aumentando a taxa de sucesso desses ataques. A SEK ressalta que as companhias utilizadas pelos criminosos como pretexto para os ataques não possuem nenhuma ligação entre si, ou seja, são de setores diferentes e utilizam sistemas distintos. Segundo conclusões dos especialistas, a suspeita é de que esses atores maliciosos tenham **interceptado as notas fiscais, com dados sigilosos, no meio do trajeto** que fazem para se tornarem disponíveis.

03. Outras campanhas similares

Até o momento de elaboração deste Boletim de Inteligência, a onda de ataques apresentada anteriormente não tinha sido divulgada na mídia. Porém diversos casos similares de golpes com boletos falsos são noticiados constantemente, causando prejuízos em diversos níveis, tanto para pessoas físicas quanto jurídicas.

As consequências desses ataques são diversas e vão além das perdas financeiras imediatas. Empresas e consumidores afetados enfrentam dificuldades para recuperar os valores pagos e, muitas vezes, **têm que lidar com processos legais complicados para buscar ressarcimento**. No caso das empresas, há também o risco de danos à reputação, que podem **afetar a confiança dos clientes e parceiros comerciais**.

Além das táticas já apontadas aqui, os cibercriminosos têm passado a explorar outros métodos de ataque. **Um dos golpes mais recentes aproveita uma nova versão da ferramenta "Reboleto"**, usada para revalidar boletos vencidos. Para aplicar a fraude, **golpistas trocam o código de barras no arquivo**. Assim, quando a vítima fizer o pagamento, toda essa quantia vai para a conta do atacante. A alteração desses dados é feita somente no arquivo em PDF enviado para o usuário, sem qualquer mudança no valor. Dessa forma, a vítima raramente suspeita do golpe.

Esse tipo de fraude dos boletos tem ganhado **destaque no cenário judicial brasileiro**. Diversas ações judiciais têm sido movidas por vítimas que buscam ressarcimento pelos valores pagos indevidamente. Em decisões, juízes abordam que intermediadoras precisam responder pela reparação dos danos. "Espera-se que um meio eletrônico de mediação de pagamentos ofereça minimamente a segurança quanto à real identidade dos agentes que nele atuam", afirmou o juiz de Direito **Cassio Pereira Brisola**.

Em outro caso, o **Tribunal de Justiça de São Paulo** (TJSP) decidiu que uma intermediadora financeira **deveria ressarcir um banco em R$ 8,4 mil** pelos prejuízos causados por um golpe de boleto falso. O banco alegou que a companhia não teria feito a verificação completa dos perfis de clientes que utilizassem seus serviços para aplicar golpes. Para a Corte, a empresa intermediadora facilitou o cadastro de indivíduos, permitindo que usuários mal-intencionados criassem contas e dificultassem a sua identificação.

Pessoas físicas também são atingidas por esse tipo de golpe. Neste ano, Osvaldo Gomes, morador de Mauá, recebeu uma conta de energia elétrica falsificada diretamente de um suposto leiturista — o responsável por fazer a medição dos consumos de energia nas residências. A novidade, neste caso, é o fato de que os boletos da concessionária Enel chegam ao destinatário por meio do próprio leiturista, em vez do correio. A vítima notou a fraude a partir do momento que recebeu uma notificação sobre a falta de pagamento da fatura. Ao entrar no site para verificar se havia algo errado, percebeu que o valor do boleto recebido através do falso profissional não estava correto.

A companhia relata que ainda apura o ocorrido. Doroti Gomes Cavalini, diretora do Procon de Santo André, ressalta em reportagem que, nessas fraudes, o consumidor não pode ser penalizado. "No caso de a conta fraudulenta ter sido paga, tem que baixar esse valor da responsabilidade do cliente, ou negociar. Esse prejuízo não pode ficar com o consumidor", afirma em entrevista ao **jornal RD**.

Em **Boituva**, município de São Paulo, uma família foi vítima de um golpe que resultou no pagamento de um convênio médico falso para o filho com paralisia cerebral. As vítimas pesquisaram na internet um meio para conseguir a segunda via do boleto e acessaram um **site falso muito similar ao oficial**. No portal, obtiveram um boleto fraudulento no valor de quase mil reais, que foi pago.

A SEK também chegou a investigar uma **campanha massiva de *phishing* disparada contra várias empresas brasileiras sob o nome do NIC.br**, responsável pela administração dos domínios por meio do Registro BR.

FATURA DE REGISTRO

nic.br registro.br

05.506.560/0001-36 Núcleo de Informação e Coordenação do Ponto BR - NIC.BR Av. das Nações Unidas, 11541, 7º andar - Brooklin Paulista 04578-000 São Paulo - SP

NÚMERO	DATA DE EMISSÃO	VENCIMENTO	CÓDIGO DE VERIFICAÇÃO
14831307	01/04/2024	06/04/2024	qPIOVOqnhmWgLccbgk7gMr58

DISCRIMINAÇÃO DOS SERVIÇOS

Registro do domínio:
Serviços de e-mail
Manutenção de 01/03/2024 a 01/04/2024
ref. 6022432

Tributos: COFINS 7,6%

VALOR TOTAL: R$ 958,00

00190.00009

Figura 7 – Fatura falsa do serviço Registro.BR

De forma muito similar à campanha explicitada anteriormente neste Boletim, **a onda de ataques de *phishing* que exploravam o Registro.BR também usava serviços públicos de e-mail, como Terra e Gmail**. Em comunicado emergencial, a equipe de inteligência da organização apontou que os e-mails simulavam cobranças de fatura e eram acompanhados de um boleto falso em anexo.

As análises sobre esses casos mostram que os golpes têm **evoluído cada vez mais**, adaptando-se às novas tecnologias e explorando informações reais.

04. Conclusão

Embora os golpes com boletos falsos **não sejam uma novidade** no cenário das fraudes financeiras, a **sofisticação e a frequência desses ataques têm aumentado** gradativamente no cenário brasileiro. Os cibercriminosos continuam explorando a confiança dos consumidores nos boletos bancários, aproveitando a percepção de segurança associada a esses pagamentos.

A onda de ataques a partir desses arquivos também chama a atenção de autoridades. **Uma das medidas de prevenção implementada pelos bancos é o DDA** (Débito Direto Autorizado), sistema que permite aos pagadores receberem seus boletos eletronicamente por meio dos canais de atendimento oficiais dos bancos, como *internet banking*. Esse método oferece uma camada adicional de segurança, pois elimina a necessidade de recebimento desses documentos por outros meios, como e-mails. "Como o serviço pega as informações direto da Plataforma Centralizada de Recebíveis, **não há o risco de o documento ser fraudado por um golpista**...", relata a **Febraban**.

Consumidores e empresas precisam estar atentos aos sinais de golpes e adotar boas práticas com base nas melhores recomendações das indústrias. Nessa tendência, **as companhias têm o dever de desempenhar um papel ativo na proteção dos seus clientes**, que são as vítimas diretas desses ataques cibernéticos. Como essas são campanhas ainda em andamento, ressaltamos que **qualquer instituição pode ser utilizada como pretexto para os golpes**.

05. Recomendações

Considerando todos os pontos abordados neste Boletim, **é fundamental que as organizações comuniquem qualquer suspeita de fraude aos seus consumidores**, de pessoas jurídicas a pessoas físicas. A intenção dessa ação é conscientizar esses clientes sobre a possibilidade de que sejam visados por cibercriminosos em golpes do tipo.

No mesmo sentido, **as companhias devem oferecer orientações claras sobre como seus clientes podem verificar a autenticidade de e-mails e boletos** supostamente enviados pelas suas equipes financeiras. Essas recomendações podem ser fornecidas em diferentes formatos, como cartilhas, áudios ou newsletters oficiais.

Notar um boleto falso é uma das partes mais importantes na defesa contra esses golpes. No entanto, as alterações realizadas pelos cibercriminosos tendem a ser sutis, passando despercebidas a um olhar desatento.

Dessa forma, em todo boleto recebido, deve ser feita uma checagem detalhada de todas as suas partes. **A primeira recomendação que deve ser repassada aos consumidores é a verificação dos dados do boleto bancário**, comparando-os com as informações já conhecidas, como número do beneficiário e o código do banco. Além disso, **o cliente deve verificar se os números superior e inferior do código de barras são os mesmos**. Outra sugestão é conferir se o **nome do beneficiário e o CNPJ disponibilizados correspondem** aos da empresa verdadeira.

Empresas também precisam ressaltar que seus consumidores **devem dobrar a atenção ao checar os remetentes de e-mails justamente pelo risco de baixar um arquivo malicioso ou falsificado**. Diversas vezes, os atacantes alteram somente um caractere dos remetentes, o que aumenta as chances de que uma vítima não perceba a alteração. Isso também vale para caso surja a necessidade de gerar uma segunda via do boleto e checar o valor cobrado na fatura. Por isso **os usuários devem utilizar sites e canais oficiais da companhia fornecedora do serviço** em vez de fazer o download de arquivos das comunicações.

Adicionalmente**, as organizações devem implementar sistemas de monitoramento de e-mails corporativos** para detectar e bloquear tentativas de *phishing* que utilizam boletos falsos. A integração de campanhas de conscientização em cibersegurança para colaboradores, nesse caso, atinge também os filtros dos próprios serviços de e-mail. Assim, ao saberem como notar as falsas comunicações, os funcionários conseguem denunciar tais remetentes nos próprios aplicativos de e-mail, **melhorando o filtro do serviço** e evitando que esses arquivos façam outras vítimas.

Ao identificar uma possível fraude, **é importante que a vítima registre um boletim de ocorrência (BO) imediatamente**. Isso não só auxilia na investigação e na recuperação dos valores perdidos, mas também contribui para estatísticas que podem direcionar ações de combate a esse tipo de crime. As empresas também devem ter **um canal de atendimento específico para que os clientes possam relatar incidentes de fraude** rapidamente e obter orientações sobre os próximos passos.

Outra recomendação é **realizar auditorias frequentes nos sistemas de emissão de boletos das empresas**. Esses processos verificam não apenas a conformidade dos sistemas com as normas de segurança, mas também a segurança de todos os dados transmitidos pela organização, incluindo informações de seus consumidores.

Como já apontado anteriormente, as empresas **devem adotar uma abordagem proativa em relação à educação de seus colaboradores**, treinando-os para reconhecer tentativas de fraude e responder adequadamente. Promover a cultura da segurança cibernética dentro da organização é essencial para garantir que todos estejam atentos às possíveis ameaças.

Esse tipo de conscientização sobre riscos cibernéticos pode ocorrer por meio de newsletters, e-books, treinamentos, simulações de *phishing*, *vishing* e até mesmo palestras. **Todos esses produtos são oferecidos pela SEK através do PSAP**, serviço de conscientização de funcionários com foco na realidade do mundo de cibersegurança.

Por fim, é importante reforçar nas companhias **o uso de softwares e sistemas atualizados**. Muitas fraudes ocorrem por causa de vulnerabilidades em sistemas desatualizados exploradas por criminosos. Para isso, **serviços de gerenciamento de vulnerabilidades têm um papel fundamental ao escanear redes e sistemas** em busca de falhas exploráveis por criminosos. Assim, as empresas conseguem garantir que todos os *patches* de segurança sejam aplicados assim que possível e que as suas infraestruturas sejam seguras o suficiente para resistir a ataques.

Tais recomendações, alinhadas às melhores práticas do mercado, podem ajudar a preservar dados de colaboradores e clientes, bem como aumentar a confiança dos consumidores nos serviços prestados pelas organizações. **A SEK se compromete a continuar a investigação sobre esta e outras campanhas ativas em território brasileiro, notificando seus parceiros se novos acontecimentos relacionados ocorrerem.**

TLP: WHITE

06. Referências

- Banco Central do Brasil
- Febraban
- Serasa
- TJSP
- Estadão
- G1
- Infomoney
- Migalhas
- Repórter Diário

THINK AHEAD, ACT NOW.