



ALERTA CIBERCRIME

2 de outubro de 2024

Telefonemas Fraudulentos Supostas Contas de Criptoativos

1. Têm sido identificadas e notificadas ao Gabinete Cibercrime um número muitíssimo expressivo de chamadas telefónicas para destinatários em território nacional, com intuitos ilícitos, os quais, todavia, ainda não estão cabalmente identificados. Os destinatários atendem telefonemas de números *nacionais* mas, do outro lado, ninguém responde.

Além deste fenómeno, e em paralelo, foi identificada (esta sim, com clareza) mais uma campanha de burlas telefónicas que passa pela realização de inúmeras chamadas para destinatários em Portugal. Embora os telefonemas fraudulentos visem vítimas portuguesas, a generalidade das conversações é estabelecida em inglês, por vezes de nível rudimentar e com um sotaque comumente utilizado na região do subcontinente indiano.

2. Nos dois diferentes tipos de situações, as chamadas indicam ter origem em números de telefonia móvel de operadores portugueses, mas na verdade, assim não acontece. Tais chamadas telefónicas são efetuadas a partir do estrangeiro, por meio de plataformas informáticas que usam em simultâneo dezenas de cartões telefónicos SIM e recorrem a *software* específico para *mascarar* o verdadeiro número do cartão utilizado. Desta forma conseguem *forjar* aleatoriamente um qualquer número, seja do mesmo operador da vítima ou doutro operador nacional, com o intuito de dar mais autenticidade e credibilidade à chamada telefónica.

Ou seja, tais chamadas utilizam nesta *ofuscação* da origem do telefonema a técnica conhecida por "*spoofing*", por via da qual as chamadas telefónicas aparentam, de forma enganadora, ser efetuadas a partir de um número chamador nacional, que não é realmente aquele no qual têm origem.

CHAMADAS MUDAS

3. O recebimento das chamadas telefónicas *mudas* tem sido muito frequentemente denunciado ao Ministério Público. Quando o destinatário da chamada a atende, não há resposta do outro lado; uns segundos depois a chamada *cai*.

Caso o destinatário da chamada não a atenda e mais tarde a *devolva*, esta última é atendida por uma pessoa em território nacional, cliente de um operador nacional. É pois atendida pelo verdadeiro titular daquele número *forjado* por ação dos agentes criminosos – e que, portanto, não efetuou a chamada em causa nem sabe nada da mesma. Trata-se de uma consequência do "*spoofing*": o verdadeiro titular do número não tem qualquer conhecimento de que o seu número foi utilizado abusivamente para efetuar uma multiplicidade de chamadas.

4. Estas chamadas são efetuadas de forma automatizada, sem intervenção humana imediata. Não se conhecem ainda cabalmente os contornos desta atividade delituosa. Porém, há já suficiente



informação para permitir concluir que este tipo de telefonemas (*mudos*) são exploratórios, destinados a confirmar ou não a validade dos números telefónicos chamados. Portanto, são um procedimento preparatório de outras fraudes telefónicas, das quais já existe vasto conhecimento, seja por via de falsas chamadas policiais ou de mensagens escritas que reclamam a cobrança de quantias. Ou outras.

CHAMADAS ALERTANDO PARA FALSAS CONTAS DE CRIPTOMOEDAS

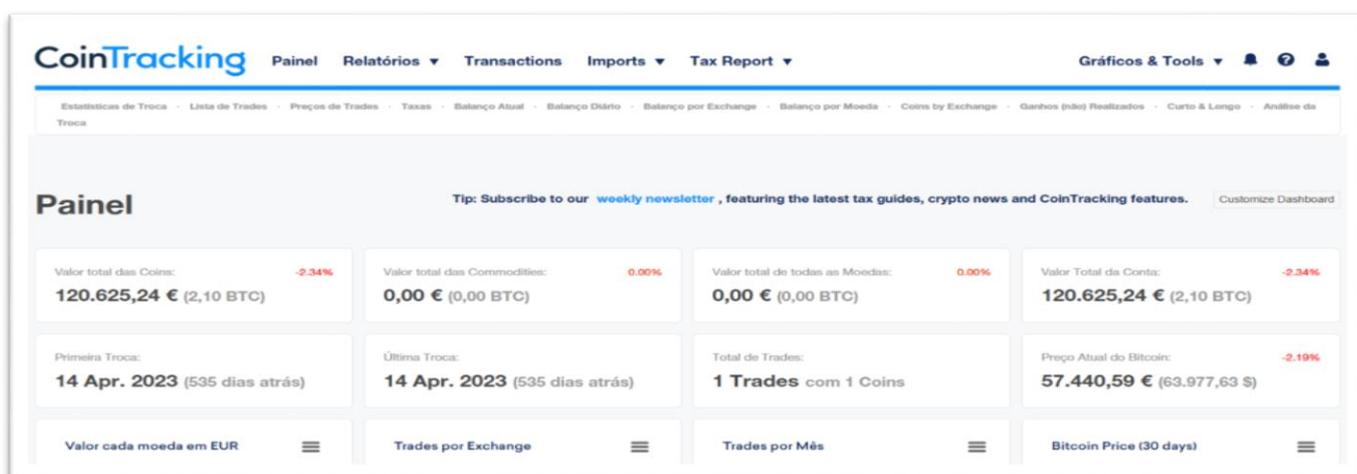
5. Ao contrário do que tem sucedido com outras metodologias de defraudação por via de telefonemas, neste novo processo criminoso não é realizada uma quantidade indiscriminada de chamadas telefónicas para vítimas aleatórias. Ao invés, neste caso, as vítimas são escolhidas porque o seu número de telefone, o seu endereço de *email* e o seu nome constam de listagens em poder dos agentes criminosos (normalmente organizadas a partir do acesso ilegítimo a servidores e a dados pessoais – tais listas são correntemente transacionadas na *Darknet*).

6. Ou seja, quando o agente criminoso realiza uma determinada chamada telefónica, está já munido de alguma (embora pouca) informação sobre o titular do respetivo número telefónico: normalmente, sabe o seu nome (ou parte dele), o seu número de telefone e o seu endereço de *email*.

Quando uma vítima atende uma chamada deste tipo, o agente criminoso identifica-o de imediato pelo seu nome (com isto pretendendo dar credibilidade ao contacto). Por outro lado, igualmente para dar autenticidade ao telefonema, embora os agentes criminosos estejam fora de Portugal, procedem de forma a que, por via de métodos de “*spoofing*”, o número telefónico chamador que a vítima visualiza é sempre um número de um operador português, usando a técnica acima descrita.

7. No decurso da chamada, o agente criminoso refere ser funcionário de uma entidade gestora de carteiras de criptoativos e informa a vítima de que o seu endereço de *email* está associado a uma carteira digital de criptoativos muito antiga, onde está depositado um muito considerável valor financeiro. Ainda diz que esta carteira está inativa há demasiado tempo e, por isso, irá ser encerrada. Adianta por último que este encerramento pode ser evitado, se o seu dono (a vítima) abrir uma conta numa outra entidade, para onde possam ser transferidos os valores que tem na carteira.

Foram identificados casos em que o agente criminoso facultou à vítima instruções e credenciais para acesso a uma plataforma *online* onde poderia ser consultado o saldo da alegada carteira digital.





8. Porém, na verdade, aquela carteira digital em nome da vítima não existe nem existiu nunca. O autor da chamada não trabalha para nenhum operador, intermediário financeiro ou outra entidade gestora de criptoativos. A suposta plataforma financeira que possa ser indicada à vítima é também fraudulenta: o respetivo conteúdo é forjado pelos agentes criminosos e não corresponde a qualquer autêntica plataforma de gestão ou negociação de ativos.

9. Caso, no decurso da chamada, a vítima se disponibilizar para abrir a tal nova conta ou carteira, como lhe é proposto pelo agente criminoso, este informa-a de que tal abertura supõe o depósito imediato, nessa nova conta, de uma quantia – embora os valores referenciados sejam variáveis, em geral são solicitadas quantias na ordem das centenas de euros. Para o efeito, o agente criminoso dá à vítima instruções precisas quanto à forma de proceder à transferência de valores para essa suposta nova carteira de criptomoedas. Trata-se, naturalmente, de uma carteira controlada pelos agentes criminosos.

Caso a vítima proceda efetivamente à transferência de valores, o agente criminoso *desaparece*, deixando de ser possível contactá-lo. E a vítima perde a quantia transferida.

10. Estas chamadas telefónicas são fraudulentas. São efetuadas por agentes criminosos que integram grupos de criminalidade organizada internacional. O objetivo único das chamadas é o de persuadir as vítimas a transferirem quantias monetárias para a carteira de criptoativos que lhes indicam. Caso a vítima (destinatário da chamada) se aperceber do intuito fraudulento e desligar a mesma, ou a ignorar, a ação criminosa não vai mais longe e fica por aí. Isto é, se a vítima não acreditar naquilo que lhe é dito ou confrontar o agente criminoso com este procedimento ardiloso, nada mais acontece: o agente criminoso desligará (e irá efetuar novas chamadas, para outros números...).

11. Todo este procedimento é criminoso. O propósito único dos autores destas chamadas telefónicas é burlar vítimas menos atentas, provocando convencê-las enganadoramente a praticar atos que lhes vão provocar prejuízo patrimonial.

É recomendável encarar cautelosamente chamadas telefónicas como as descritas, vindas de números desconhecidos, efetuadas por pessoas desconhecidas, no estrangeiro. Uma vez identificado o seu teor, não deve responder-se às mesmas, desligando e reportando o facto ao Ministério Público ou aos órgãos de polícia criminal.