"Recebi uma chamada com o nome e a fotografia do meu irmão". Novas burlas usam Inteligência Artificial e são feitas à medida da vítima

cnnportugal.iol.pt/burla/inteligencia-artificial/recebi-uma-chamada-com-o-nome-e-a-fotografia-do-meu-irmao-novas-burlas-usam-inteligencia-artificial-e-sao-feitas-a-medida-da-vitima/20240909/66d9f60ad34ea1acf26e07d6

Autoridades estão preocupadas com a complexidade e a recorrência dos ataques. Roubam a imagem de familiares e fazem um estudo do perfil para adequar a mensagem à vítima, garantindo o sucesso do crime

São cada vez mais recorrentes e agora são construídas com Inteligência Artificial de forma personalizada com base nos detalhes da vida da própria vítima. As burlas por telemóvel estão a tornar-se um fenómeno cada vez mais comum e as autoridades estão a ter “dificuldades acrescidas” em travar a proliferação destes esquemas, que se estão a tornar cada vez mais complexos. Já há casos em Portugal de ataques com sucesso com utilização de "deepfakes de voz perfeitos". Os especialistas admitem que podemos estar a entrar “numa época de ouro” dos ataques digitais em que é cada vez mais difícil distinguir entre o que é verdadeiro e aquilo que é falso.

“Nós estamos numa época de ouro do cibercrime, porque a tecnologia está a aumentar diariamente. Todos os meses, os criminosos têm uma nova tecnologia e uma nova forma de nos atacar. Isto cria muitas dificuldades, até porque existe uma certa sensação de impunidade por parte de quem ataca”, afirma Nuno Mateus-Coelho, especialista em cibersegurança.

Durante a última semana, a própria Polícia Judiciária (PJ) foi utilizada por cibercriminosos para uma campanha descrita como “intensa e massiva” para burlar milhares de pessoas. Os atacantes utilizam uma técnica chamada *spoofing*, capaz de mascarar uma chamada fraudulenta com um número real de uma entidade, para levá-los a transferir dinheiro para uma conta bancária. O objetivo é sempre o mesmo: ganhar a confiança da vítima para que ela forneça informações sensíveis ou realize transações financeiras. Estes ataques não são novos em Portugal, mas as autoridades admitem estar cada vez mais preocupadas com a sofisticação das campanhas difundidas no nosso país.

José Ribeiro, coordenador de investigação criminal da Unidade Nacional de Combate ao Cibercrime e Criminalidade Tecnológica (UNC3T), explica que os criminosos têm “uma abordagem quase individualizada” no contacto direto com as vítimas. Agora, os burlões fazem uma análise de perfil da vítima, cada vez mais completa e com ajuda a Inteligência Artificial.

"A preocupação com estas técnicas é a forma massiva como as campanhas são difundidas e conseguem ter contacto direto com as vítimas, numa abordagem quase individualizada. Estão a desenvolver padrões individualizados de ataque e de burla, fazem análise de perfil e com recurso a Inteligência Artificial", destaca o coordenador-chefe da PJ.

Os especialistas em cibersegurança referem que antigamente esses ataques eram apenas feitos a vítimas consideradas "VIP", como diretores de grandes empresas ou pessoas que tivessem acesso a grandes quantidades de dinheiro. Nestes casos, os atacantes estudavam o perfil da vítima e enviavam ataques direcionados às preferências e aos hábitos de consumo da mesma. Atualmente, todo este processo passou para uma nova escala, com os grupos criminosos a fazerem a análise de perfil num nível "massivo".

"A Inteligência Artificial veio dar ao cibercrime a capacidade de robotizar aquilo que era um trabalho altamente cirúrgico. Antigamente, um elemento da equipa estudava a vítima e criava o seu perfil. Agora, esta tecnologia varre o histórico de leaks, as redes sociais e cria um ataque personalizado", explica Bruno Castro, CEO da empresa de cibersegurança VisionWare.

O perito em cibersegurança admite que os ataques com *deepfakes* de voz - réplicas quase perfeitas criadas por Inteligência Artificial - já chegaram a Portugal e a evolução destas práticas "vai ser exponencial". Bruno Castro sublinha que uma das principais preocupações é o baixo custo que estes ataques têm para os criminosos. Com pouco mais de 200 euros conseguem fazer um vídeo falso com um som falso e enganar centenas de pessoas, como foi o caso que envolveu o médico português João Ramos, que viu a sua voz e imagem manipuladas para burlar várias pessoas que acreditaram que vendia um medicamento milagroso para a cura da diabetes.

Estes ataques são possíveis graças aos milhões de dados que são colocados a circular na darkweb. Algumas fugas de informação, como foi o caso da TAP, tornam públicas informações pessoais de milhões de clientes, expondo o nome, nacionalidade, género, data de nascimento, morada, e-mail, contacto telefónico, data de registo de cliente, número de passageiro frequente e até o registo de viagens.

Segundo os especialistas, este tipo de violações de dados permite aos criminosos utilizar ferramentas de machine-learning ou de Inteligência Artificial para traçar o perfil da vítima, criando "uma armadilha" feita à medida. Nalguns casos os criminosos chegam a apropriar-se da imagem de um familiar da vítima antes de se fazer passar por ele.

Teresa, de 50 anos, foi alvo de uma tentativa de burla mais sofisticada, onde os burlões obtiveram informação detalha sobre o seu irmão, que utilizaram para tentar ganhar a sua confiança. Através do Whatsapp, utilizaram um número real com o nome e a imagem do irmão de Teresa. Ligaram-lhe por Whatsapp, mas desligaram alegando má ligação. De seguida, veio a tentativa.

“De repente, recebi uma chamada com o nome e a fotografia do meu irmão. A chamada caiu e começámos a falar por escrito através do Whatsapp, onde me explicou-me que tinha recebido um email com um pagamento em atraso que tinha de ser feito no dia. Pediu-me 975 euros e deu-me uma entidade e uma referência”, recorda.

Outros casos, como no que aconteceu na semana passada, em que um grupo criminoso utilizou a própria PJ para tentar enganar as suas vítimas a enviar-lhes dinheiro, os cidadãos foram contactados pessoalmente e informados de que a sua conta bancária está em risco e tinha sido acedida indevidamente. As vítimas são depois canalizadas pelo operador a escolher várias opções, entre as quais a de ter a chamada reencaminhada para um suposto inspetor da PJ. Assim que o contacto é estabelecido, o criminoso que se faz passar por inspetor explica à vítima que é necessário transferir o dinheiro para uma conta segura. Só no último fim de semana, a PJ recebeu “mais de uma centena de queixas”.

Nuno Mateus-Coelho, especialista em cibersegurança, alerta que agora os criminosos têm mais e melhores ferramentas, algumas delas bem simples, como o ChatGPT. Os criminosos utilizam essas aplicações para criar “guiões realistas” para ler durante a burla, de forma a tornar todo o processo “o mais realista possível”. E com o aparecimento de novas técnicas a uma grande velocidade, está a tornar-se cada vez mais difícil distinguir “o que é real do que é falso” e isso torna muito mais difícil criar técnicas para identificar a burla.

O esquema que está a ser usado no ataque é conhecido por *spoofing* e preocupa as autoridades. Através deste método, os hackers conseguem fazer uma cópia do número de telefone verdadeiro e usam essa cópia para enviar as chamadas ou SMS. Mas a receita tem vindo a ser cada vez mais aperfeiçoada por parte dos piratas informáticos. A CNN Portugal apurou junto das autoridades que os atacantes já conseguem uma cópia do ID Call tão perfeita que as mensagens falsas já conseguem entrar no histórico das mensagens verdadeiras.

Isto faz com que seja praticamente impossível ao utilizador distinguir uma mensagem falsa de uma verdadeira. Até agora havia muitas situações em que a mensagem aparecia com o número real, mas não chegava a entrar no histórico das mensagens verdadeiras, porque não era exatamente igual. Mas agora há cópias tão perfeitas que é impossível ao sistema detetá-las de forma rápida. A CNN Portugal também apurou junto das autoridades que já começaram a aparecer alguns casos destes ligados a instituições bancárias.

As redes cibercriminosas, que muitas vezes operam diretamente do estrangeiro, estão a utilizar números nacionais para esconder a sua origem, de acordo com José Ribeiro. O facto de os ataques acontecerem vindos do estrangeiro, tornam-nos mais difíceis de rastrear. "O facto de pertencerem a números nacionais não quer dizer que sejam feitas pelos titulares desses números. Queremos alertar a população que pelo facto de aparecer um número nacional não quer dizer que seja rastreável", acrescenta José Ribeiro.

De acordo com um relatório do Global Anti-Scam Alliance, cerca de 67% da população mundial foi alvo de uma tentativa de burla por telefone. Entre 2024 e 2028, são esperadas perdas de 362 mil milhões. Apesar de a tendência ainda ser crescente, vários países já começaram a tomar medidas para tentar travar o aumento deste tipo de burla. No Estados Unidos, a solução adotada passa pela criação de um protocolo batizado de STIR/SHAKEN, que passa pela criação de uma assinatura digital para verificar a identidade de origem da chamada. Assim, sempre que é feita uma chamada, este sistema verifica se o número é, de facto, legítimo.

Noutros países, estão a ser adotadas medidas para obrigar as operadoras de telefone a assegurar a verificação de chamadas provenientes de outros países. Estas medidas permitem evitar que grupos criminosos estrangeiros utilizem serviços de telecomunicações de países terceiros para falsificar número do país alvo. Na Europa, este problema já está a ser discutido no Parlamento Europeu, com a União Europeia a planear exigir às operadoras uma maior colaboração na identificação das chamadas fraudulentas.

Em Portugal, PJ já desenvolveu "algumas técnicas de como identificar ameaças", mas assumiu que "é complicado antecipar comportamentos" nesta matéria, assegurando que estão a "trabalhar em conjunto com as operadoras" para identificar estas técnicas de *spoofing* (falsificação de identidade para obter dados). Para Nuno Mateus-Coelho, a tecnologia que permite os ataques está a evoluir a uma velocidade maior do que a nossa capacidade de criar estratégias defensivas que passem pela informação da população. Atualmente, é necessário criar uma solução técnica que leve a uma diminuição significativa destes problemas.

“Estamos neste momento no ground-zero das burlas. Há uma impunidade grande por parte dos grupos criminosos e, atualmente, somos vítimas perfeitas. Apostar na educação e na informação já não basta. É cada vez mais difícil travar só um ataque. Precisamos urgentemente de uma solução técnica para resolver o problema”, frisa Nuno Mateus-Coelho.