Notários portugueses foram alvo de um ataque informático que terá recorrido a inteligência artificial

cnnportugal.iol.pt/notarios/cibercrime/notarios-portugueses-foram-alvo-de-um-ataque-informatico-que-tera-recorrido-a-inteligencia-artificial/20231029/651d4547d34e371fc0b853fb

Patrícia Pires
Ontem às 17:00

Os e-mails dos notários portugueses foram alvo de milhares de mensagens potencialmente fraudulentas em junho. Bastonário acredita que criminosos já recorrem à "Inteligência Artificial". Os especialistas admitem que os criminosos já podem recorrer à IA, mas dizem que atualmente a maioria dos casos ainda envolve uma falha de segurança primeiro

Os notários portugueses foram alvos de milhares de mensagens potencialmente fraudulentas. O pico “ocorreu na semana de 20 de junho, mas o sistema de segurança reconheceu que se tratava de um ataque e ao que julgamos saber intercetou a maioria dos e-mails”, revelou à CNN Portugal Jorge Batista da Silva, bastonário da Ordem dos Notários. E este acredita que já houve recurso a "Inteligência Artificial". Os especialistas dizem ser possível, mas garantem que na maioria dos casos envolve, inicialmente, uma conta hackeada.

O fenómeno foi tão percetível que foi pedida, pela Ordem dos Notários, uma avaliação aos e-mails recebidos. E, no futuro, será dada formação nesta área.

Uma conclusão desta avaliação prende-se com a evolução dos e-mails e a sua enorme credibilidade. E é por isso que Jorge Batista da Silva acredita que este ataque “já foi suportado recorrendo a inteligência artificial (IA)”. Ou seja, “o teor do e-mail e os dados utilizados correspondem a textos muito similares a situações análogas e correspondência eletrónica entre notários, entre notários e clientes, entre notários e bancos”.

O ataque de junho foi travado, mas é “impossível ter 100% certeza nesta área”, assume o bastonário, acrescentando, no entanto, que não há “nenhuma indicação de que alguém tenha recebido um e-mail com este teor e tenha sido induzido em erro”.

“Os e-mails já são construídos de acordo com a expectativa do notário que os vai receber e com informações que parecem exatamente adequadas àquilo que o notário está habituado a receber para fazer, por exemplo, um pagamento”, acrescenta Jorge Batista da Silva.

De uma coisa o bastonário tem certeza, os ataques desta natureza não vão acabar e a única forma que temos de nos protegermos é estarmos atentos. “Não existem ferramentas informáticas infalíveis para proteger os utilizadores destes ataques pois muitos deles baseiam-se na ‘engenharia social’. Ou seja, os criminosos tentam induzir os utilizadores a enviar dados ou a fazer download de software malicioso ou a aceder a sites maliciosos”.

Tanto os cidadãos, como as empresas ou as organizações precisam "conhecer aquilo que são as ‘red flags’ no mundo digital e tomar algumas cautelas”. Como, por exemplo, “verificar se o link corresponde ao endereço da entidade que pretendem visitar; não fazer download de ficheiros sem primeiro confirmarem que o email do emissor é de confiança; não introduzir dados sem verificar primeiro se estão no endereço do site da entidade correta, mesmo que graficamente lhes pareça que tudo está bem”.

Ataque partiu de "servidores externos" alojados fora de Portugal

Os números encontrados pela avaliação não surpreendem. Em 30 dias, foram analisados mais de 248 mil e-mails e, destes, 17.490 eram potencialmente fraudulentos. 136 tinham endereços eletrónicos maliciosos; 15 tinham anexos com vírus; em 75 situações, o “pirata” fingia ser uma entidade idónea (impersonation attack) e foram, ainda, detetadas oito entidades que tentaram enviar e-mails, mas eram ilegítimos.

Olhando para estes e-mails os mais frequentes foram o impersonation attack (fingir que são outra entidade), o phishing (conseguir acesso a informações confidenciais, como palavras-passe ou números de cartões de crédito) e o smishing (contacto através de SMS).

Por fim, foi também possível concluir que o ataque partiu de "servidores externos", ou seja, alojados fora de Portugal.

Após o ataque em massa sofrido em junho, a Ordem dos Notários “irá disponibilizar anualmente uma formação aos notários e trabalhadores de cartórios em cibersegurança para melhorar a capacidade da rede notarial perante este tipo de ameaças”, garantiu à CNN Portugal Jorge Batista da Silva. Como se tratou de ataque isolado, mesmo que em massa, a Ordem dos Bastonários optou por não apresentar queixa às autoridades.

Inteligência Artificial? "É possível, tecnicamente é possível"

A CNN Portugal procurou, junto de alguns especialistas, saber se é possível, atualmente, usar a Inteligência Artificial (IA) para cometer este tipo de crimes. Bruno Castro, CEO da empresa de cibersegurança VisionWare não tem dúvidas: "É possível, tecnicamente é possível, sim".

Todavia, em declarações à CNN Portugal, explica na grande maioria das fraudes cometidas por e-mail, os criminosos usam informação "genuína". Ou seja, as conversas "foram, muito provavelmente roubadas de alguém".

"Isto é um crime que temos muitas vezes. Infelizmente, é o método mais usado. De alguma forma conseguem aceder aos e-mails trocados em ambiente verdadeiro e depois utilizam essa cadeia de e-mails, esse histórico para enganar", esclarece. "É o mais comum, 90% dos casos, é feito dessa forma", acrescenta Bruno Castro.

O que não significa que os criminosos não recorram a IA: "Também temos casos em que já começam a aparecer conteúdos, usado em e-mails de phishing, que é gerado, sim, por Inteligência Artificial. Tendo em atenção "o setor e o contexto".

"Ensinou-se um computador a aprender"

Rui Duro, gestor da empresa de cibersegurança Check Point Software também partilha da mesma opinião. Em declarações à CNN Portugal garante que "sim", que é possível ter sido usada Inteligência Artificial. Todavia, lembra que "quando se fala de Inteligência Artificial estamos sempre a falar de uma coisa chamada 'machine learning'. Ou seja, ensinou-se um computador a aprender".

A fórmula usada parece-lhe parecida com o ataque conhecido como o "ataque CFO" - um ataque ao diretor financeiro de uma empresa. "Compromete-se uma conta e depois eles andam a ver exatamente o que lá está e descobrem a maneira de operar, de falar, escrever. E depois, a uma dada altura, mandam um e-mail ou a um cliente ou internamente, exatamente usando a mesma linguagem do diretor e os mesmos processos financeiros para conseguirem o acesso".

E por isso, admite como hipótese que "um cliente ou um notário, basta um só, tenha tido uma conta comprometida". Porque para desenvolver e-mails com conteúdos verosímeis é preciso "ter acesso a um e-mail tipo, a dois ou a três, para depois gerar então e-mails similares, ou com tópicos similares".

"Pode ter sido usado a inteligência artificial, ou neste caso machine learning, mas teve que haver primeiro um acesso a uma conta e a partir daí foram retiradas amostras, que depois uma máquina de machine learning aprendeu, para gerar e-mails parecidos e muito idênticos", acrescenta.

E é por isso que Rui Duro alerta que "na internet, falamos muito no chat de GPT, mas há centenas de ferramentas". E dá um exemplo concreto: "Uma delas é para quando queremos mandar um mail a um cliente e ensina a escrever o e-mail ao cliente com os dados certinhos. Já há estas ferramentas".

A cibercriminalidade é cada vez mais comum e o grau de sofisticação dos ataques é maior. A Polícia Judiciária, responsável pela investigação deste tipo de crimes sabe que, na maior parte dos casos, são organizações que estão na origem dos ataques e, muitas vezes,

atacam de fora para dentro do país. Os prejuízos causados por estes tipos de phishing já atingem "os milhões de euros" e as autoridades alertam que, nestes ataques, as falhas de segurança vêm sempre do lado da vítima.

E, por isso mesmo, lembramos que há três esquemas online que estão a roubar milhões aos portugueses e indicamos como se proteger.

Temas: Notários Cibercrime Emails Ataque Bastonário