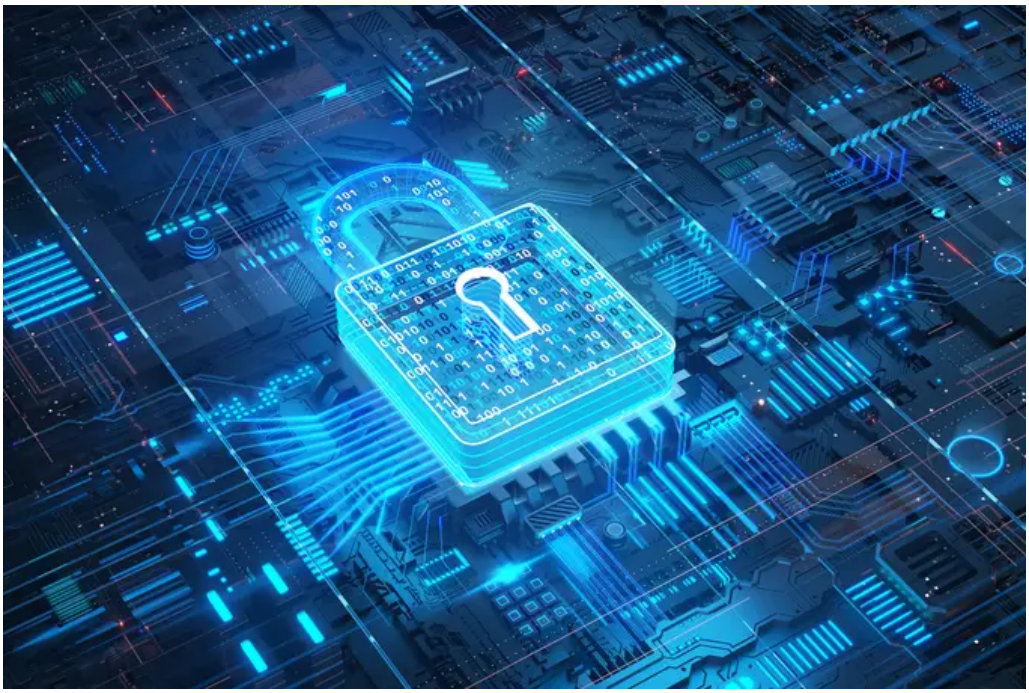
Grupo cibercriminoso pró-Kremlin 'Killnet' elege Portugal como um dos alvos

expresso.pt/economia/economia_tecnologia/2023-02-01-Grupo-cibercriminoso-pro-Kremlin-Killnet-elege-Portugal-como-um-dos-alvos-52e313aa

Tecnologia

1 fevereiro 2023 17:54

Lusa



yuichiro chino/getty images

Bruno Castro, presidente executivo da Visionware, afirma que se trata da segunda vez em menos de uma semana que a 'Killnet' lança idêntico apelo, depois de o último, na quinta e sexta-feira passada, ter afetado instituições ligadas à área da Saúde em vários países, incluindo Portugal

Um grupo cibercriminoso "muito próximo" do Kremlin, Killnet, que tem visado nos seus ataques países pró-Ucrânia como Portugal, lançou esta quarta-feira um apelo ao recrutamento de novos membros ["call to arms"], indicou à agência Lusa o presidente da

empresa Visionware.

Bruno Castro, Chief Executive Officer (CEO) da Visionware, salientou que se trata da segunda vez em menos de uma semana que a 'Killnet' lança idêntico apelo, depois de o último, na quinta e sexta-feira passada, ter afetado instituições ligadas à área da Saúde em vários países, incluindo Portugal, tendo sido atingidos os portais da Direção Geral de Saúde (DGS) e da Faculdade de Farmácia.

Segundo o CEO da empresa credenciada pela NATO em soluções de segurança da informação e cibersegurança, o grupo de ciberativistas russos tem lançado várias campanhas de recrutamento para ciberataques a vários países ocidentais, além dos Estados Unidos, alegadamente em resposta ao alinhamento pró-Ucrânia, em que Portugal está incluído.

"A relação que a Killnet tem com o Estado russo, ou muito próxima do Kremlin, passa pela ideia de que ou é subcontratada como mercenária ou é mesmo por afiliação política. Estão a fazer ações ultraviolentas direcionadas a tudo o que são infraestruturas críticas e de forma contínua. Houve aqui uma onda de ataques que teve bastante sucesso", sublinhou.

Esse sucesso, prosseguiu, e tendo por base os ataques da semana passada, teve mediatismo e visou, tal como noutras incursões, criar uma marca do grupo 'Killnet'. "[O sucesso] serve para [a própria 'killnet'] se autopromover como autor ou origem dos ataques e para poder recrutar mais soldados para aumentar a sua força, por um lado, e, ao mesmo tempo, aumentar também a capacidade de destruição e de ataque para as novas ondas que virão a seguir", sublinhou o CEO da Visionware.

"A guerra cibernética já existe há muito tempo. O que tem vindo a acontecer é o automatizar e profissionalizar destes grupos cibercriminosos para poderem fazer este tipo de ações em prol de um Estado. Será o próximo passo e, tipicamente numa analogia muito de pirata convencional, dependente de qual é o livro de História que lemos, tanto posso ser visto como um pirata malicioso, criminoso ou ladrão como posso ser visto, do outro lado da História, como um herói militar", sustentou.

Segundo Bruno Castro, neste contexto, há também uma abordagem mais abrangente fora dos Estados Unidos "com a ideia de que tudo o que são Estados pró-Ucrânia também serão alvo, depois, de ataques devastadores".

"Este [ataque] foi claramente mediático e fizeram questão que assim fosse. Já houve aqui outro 'call to arms' de outros grupos cibercriminosos ou de 'lone wolves' [lobos solitários] que queriam também apoiar a 'causa' e isto será um processo contínuo, que irá continuar, em que Portugal se encaixa neste contexto porque é declaradamente pró-Ucrânia e fará parte, em teoria, dos próximos alvos do Killnet ou de outros grupos cibercriminosos apoiantes da Rússia", acrescentou.

Em Portugal, prosseguiu, o que a Visionware tem feito não é mais do que tem feito em todo o mundo. "Trabalhamos muito a componente preventiva, a de 'awareness', sermos capazes de analisar e monitorizar em constante o que se passa neste submundo criminoso e, em paralelo, estarmos, continuamente, a 'stressar' as infraestruturas de segurança dos nossos clientes, bem como a dar atenção aos mecanismos internos para reagir e recuperar de ataques cibernéticos", explicou.

"Ataques desta natureza e muito direcionados para infraestruturas críticas (...) é claramente o conceito de guerra cibernética: atacar com violência, interrompendo os serviços básicos de uma sociedade e colocando em causa o Estado de direito", sustentou.

"A partir daí, [a intenção é] criar instabilidade imediatamente na população, através do pânico e de incutir o sentido de terror e de insegurança na população através da interrupção dos serviços básicos, como a energia, comunicações, água, transportes, banca. É isto que sustenta os pilares básicos de uma sociedade que, quando interrompidos numa lógica de guerra digital, tem impacto e, às vezes, é mais violento do que uma guerra convencional, bélica", sintetizou.