Killnet: hackers pró-Rússia anunciam venda de serviços de "mercenários cibernéticos" e prometem destruição "pela glória da pátria"

cnnportugal.iol.pt/killnet/ciberataque/killnet-hackers-pro-russia-anunciam-venda-de-servicos-de-mercenarios-ciberneticos-e-prometem-destruicao-pela-gloria-da-patria/20230502/644be9f7d34ed4d514fae04f

João Guerreiro Rodrigues
Ontem às 22:00

São um dos grupos de piratas informáticos pró-russos mais ativos e que têm causado mais estragos. Agora, decidiram colocar os seus serviços à venda e tornar-se "mercenários" digitais, mas mantêm a promessa: vão continuar a levar a cabo ataques "pela glória da pátria"

O grupo de piratas informáticos pró-russo Killnet anunciou na sua página da *darkweb* que vai mudar o seu método de operação e vai tornar-se um grupo de "mercenários cibernéticos" que vai servir entidades estatais e clientes privados interessados em atacar inimigos da Rússia. Especialistas alertam que o grupo de hackers pode estar prestes a tornar-se uma peça chave na contraofensiva russa e, num futuro próximo, poderá vender os seus serviços a países aliados de Moscovo.

"O *hacktivismo* da Killnet chegou a um fim. A partir de agora, nós somos: a companhia privada de hackers russa Killnet. O que é que isto significa? Vamos continuar as nossas atividades destrutivas pela glória da pátria!", escreve o grupo ligado ao Kremlin,

responsável por centenas de ataques contra as mais variadas infraestruturas críticas ocidentais.

Na mensagem, publicada pelo grupo na quarta-feira, os piratas referem que o tempo do "altruísmo" chegou ao fim e que "não é possível viver de doações e de promessas de ajuda dos nossos patrocinadores". Assim, o grupo de hackers decidiu colocar à venda as suas capacidades para que "privados e indivíduos estatais" os utilizem contra qualquer alvo, à exceção de ataques contra a Rússia ou contra países da Comunidade dos Estados Independentes (CEI).

De "hacktivistas" a "mercenários"

Para os especialistas que monitorizam as atividades destes grupos na *darkweb*, este anúncio não é propriamente chocante. Muitas vezes, os cibercriminosos empregam a estratégia de publicar os dados de um ataque que não teve retorno monetário de forma a "criar uma marca" com o seu nome. Os Killnet, devido à forma de operar e aos alvos que escolhiam, mesmo fazendo-o em nome da Rússia, aparentavam ter uma estratégia comercial por detrás das suas operações, mesmo autodenominando-se de "*hacktivistas*".

O conceito de hacktivismo, que nasce da junção das palavras *hack* e ativismo, está ligado à ideia de manipular sistemas informáticos em nome de uma ideologia, que pode ser, por exemplo, política ou de defesa dos direitos humanos.

"Sempre soubemos que eles não eram um grupo *hacktivista*. Quando diziam que eram um grupo de ativistas davam vontade de rir a quem trabalha nesta área. Este grupo criou uma estratégia comercial e agora são uma espécie de grupo Wagner cibernético e é provável que os vejamos a vender serviços a estados próximos de Moscovo", explica Bruno Castro, CEO da VisionWare.

O grupo deverá continuar a ter uma presença muito forte na ciberguerra enquanto Moscovo estiver empenhado em conquistar o território ucraniano, mas é provável que mantenha "uma veia cibercriminosa". Além disso, o grupo pode tornar-se ainda mais ativo na espionagem militar, monitorizando pessoas e organizações.

"Na verdade, eles já eram um grupo muito, muito ativo nesta ciberguerra. Agora, passam a ser um grupo com escritório, com fato e gravata, um kit de boas-vindas, uma estrutura muito mais profissionalizada. Acredito também que venham a fazer espionagem com mais afinco, aliados aos serviços de informações", explica Bruno Castro.

Viktor Zhora, vice-presidente do Serviço Estatal de Comunicações Especiais da Ucrânia admitiu à BBC que o grupo russo, que inicialmente levava a cabo simples ataques de DDoS (negação de serviço após uma invalidação por sobrecarga do mesmo) onde os piratas paralisam os seus alvos, está a recrutar pessoas cada vez mais especializadas. Zhora alega ainda que a Killnet trabalha diretamente em coordenação com consultores militares russos e é capaz de levar a cabo ciberataques sofisticados.

Ciberguerra sem regras

A convenção de Genebra limita as regras da guerra de forma a proibir os militares de atacarem alvos civis. Porém, não existe uma convenção para a guerra cibernética. Os alvos são quase sempre os mesmos: as infraestruturas críticas. Redes de comunicações, energia, saúde, transportes, bancos e tudo o que consiga causar o pânico do outro lado da barricada. Foi isso que aconteceu quando o grupo decidiu pôr à venda milhares de dados sensíveis da NATO por apenas um dólar. Em causa estavam as informações pessoais de milhares de funcionários da aliança.

Entre os dados que estão à venda constam as informações pessoais de 17 mil cadetes, 26 mil utilizadores com acreditação nos portais NATO, bem como informações sobre as armas, equipamentos médicos e o serviço de imprensa. Num vídeo partilhado pelo grupo, é possível ver as informações pessoais de funcionários da organização transatlântica, desde a fotografia à morada, contacto telefónico, dados do passaporte e qual a função que desempenham na instituição.

“Este grupo está a demonstrar três coisas. Primeiro, estão a fragilizar a imagem da NATO e a comprovar a falta de segurança. Segundo, estão a demonstrar que, do ponto de vista operacional, conseguem roubar informações sensíveis. E, por último, promovem-se enquanto mercenários do cibercrime”, explica Bruno Castro.

No passado, o reivindicou uma série de ataques em larga escala contra sites de alguns dos maiores aeroportos nos Estados Unidos, tornando-os inacessíveis. Os ataques em causa sobrecarregaram os servidores que hospedam esses sites, impossibilitando que os viajantes obtenham atualizações sobre os seus voos programados ou reservem serviços no aeroporto. Apesar da inconveniência, não houve a registar, constrangimentos a nível operacional.

A informação foi captada pelo *VisionWare Threat Intelligence Center,* um centro de monitorização de ciberameaças que cria "relatórios geopolíticos relacionados com as ameaças em estudo" e observa o comportamento de actores de risco.

"Eles vão ser uma parte integrante e fundamental da contraofensiva russa na Ucrânia", refere Diogo Carapinha, especialista que monitoriza os principais grupos cibercriminosos para a empresa de cibersegurança portuguesa VisionWare.