Ucrânia sofreu maior ciberataque desde o início da guerra

publico.pt/2023/12/17/mundo/noticia/ucrania-sofreu-maior-ciberataque-desde-inicio-guerra-2074022

Carolina Amado

Guerra na Ucrânia

Hackers pró-Kremlin reivindicaram ataque que deixou mais de metade da população na Ucrânia sem telecomunicações e deixaram aviso às "empresas que ajudam as Forças Armadas".

Na última semana, 24 milhões de pessoas — mais de metade da população na Ucrânia — ficaram sem acesso à rede telefónica. Um grupo de *hackers* pró-Kremlin reivindicou o ataque à maior operadora do país, a Kyivstar.

"A guerra também acontece no ciberespaço. Infelizmente, fomos atingidos", afirmou o director executivo da operadora de telecomunicações, Oleksandr Komarov, à televisão ucraniana. Apesar de Komarov ter garantido que os dados dos consumidores não ficaram em risco, especialistas em cibersegurança chegaram a conclusões diferentes.

"Não só deixaram em baixo serviços de comunicações como roubaram informação: moradas, dados de contabilidade, facturação, dados pessoais, entre outros", afirma Bruno Castro, líder da empresa portuguesa de cibersegurança VisionWare, em declarações ao PÚBLICO.

Entre as consequências deste ataque, lançado na última terça-feira, uma das mais importantes foi a desactivação do sistema de alertas para ataques aéreos das forças russas, incluindo na capital, Kiev, que estava sob a responsabilidade da Kyivstar.

O ataque foi reivindicado na última quarta-feira pelo grupo russo Solntsepyok. A agência de segurança ucraniana (SBU) acredita que os *hackers* estão ligados, ainda que de forma não oficial, aos serviços secretos militares do Kremlin (GRU), em particular, à unidade de guerra cibernética do GRU, a Sandworm.

"Atacámos a Kyivstar porque a empresa presta serviços de comunicações às Forças Armadas da Ucrânia, assim como às agências governamentais e de segurança", escreveram no Telegram, deixando um aviso. "Às restantes empresas que ajudam as Forças Armadas: preparam-se."

O grupo alegou ter "destruído" dez mil computadores, mais de 4000 servidores e serviços de armazenamento na *cloud*, mas a operadora rejeitou as afirmações. "A estratégia do inimigo é semear o pânico", justificou a Kyivstar, em comunicado.

Ao contrário de grupos mais conhecidos como o Killnet e o NoName057(16), o Solntsepyok só foi considerado um grupo hostil pela VisionWare no segundo trimestre de 2023. Ainda que só tenham começado a agir enquanto *hackers* este ano, e que nenhum dos anteriores ataques tenha assumido proporções comparáveis ao da última semana, não é a primeira vez que têm a Ucrânia na mira.

Desde 2022 que divulgam, através do Telegram, dados pessoais de ucranianos que consideram "criminosos de guerra": jornalistas, activistas, militares. Em 2023 já reivindicaram ataques aos sistemas informáticos do Ministério das Infra-estruturas ucraniano e de vários órgãos de comunicação social.

A Kyivstar previa retomar os seus principais serviços — Internet móvel, chamadas telefónicas e SMS — até ao final desta semana, mas assume que a recuperação de todas as infra-estruturas tecnológicas e dos serviços adicionais pode levar várias semanas. Na última sexta-feira já tinham sido restabelecidos os serviços de *roaming* e de Internet móvel.

Segundo o director executivo da Kyivstar, os *hackers* terão acedido à empresa através da conta comprometida de um dos seus funcionários, mas a forma como entraram nessa conta continua sob investigação.

Na análise da VisionWare, o ataque teve motivações financeiras, já que toda a informação roubada pode ser vendida, além de políticas e militares, no contexto da invasão da Ucrânia pela Rússia.

"Isto vem demonstrar, mais uma vez, que a guerra cibernética assume um papel fundamental no conflito", diz o director da empresa portuguesa. "E não só por questões de espionagem, como sempre existiu, mas pelo impacto social, para causar alarmismo", pondo em causa a credibilidade de serviços e instituições estatais.

No mesmo dia em que o ataque foi lançado, 12 de Dezembro, o Presidente ucraniano, Volodymyr Zelensky estava nos Estados Unidos para se dirigir aos congressistas norte-americanos e apelar à continuação da ajuda militar e financeira a Kiev. Bruno Castro não acredita que os acontecimentos estejam relacionados.

"Ao contrário do que acontece na guerra convencional, bélica, em que é definida uma estratégia militar consoante certos objectivos, no cibercrime não há planeamento, há oportunidades. É muito mais selvagem", considera o especialista em cibersegurança. "A ciberguerra será o quarto ramo das Forças Armadas. Já é."