Guerra no ciberespaço tem cada vez mais meios para complementar a batalha campal, e conflito Israel-Hamas não é exceção

expresso.pt/internacional/medio-oriente/guerra-israel-hamas/2023-10-16-Guerra-no-ciberespaco-tem-cada-vez-mais-meios-para-complementar-a-batalha-campal-e-conflito-Israel-Hamas-nao-e-excecao-3b2d1185

Exclusivo
Guerra Israel-Hamas

Há cada vez mais meios para causar disrupção e comprometer o funcionamento das sociedades, como demonstram a guerra na Ucrânia e, mais recentemente, a guerra Israel-Hamas. A cibersegurança é a outra face dos ciberataques e do ciberterrorismo. O seu papel no controlo e prevenção das ações no universo cibernético é fundamental para manter alguma previsibilidade no mundo tal como o conhecemos

11:00

Cristina Peres

Jornalista de Internacional

Quem tentasse entrar no site da **Universidade Al-Aqsa de Gaza** esta sexta-feira não conseguiria. **"Está em baixo"** e é difícil prever quando é que a ligação vai ser restabelecida, desde que o site foi atacado, logo de manhã, feira pelo grupo Silent One.

Ao mesmo tempo, **aumenta o número de ameaças de cibersegurança em Israel no contexto da guerra Israel-Hamas**, ainda que não sejam inéditas. Quinta-feira, um dos atos disruptores teve grande visibilidade quando dois grandes cartazes eletrónicos em Telavive foram "raptados" e aproveitados para, durante uns minutos, exibirem, em vez da sequência de filmes publicitários, conteúdos anti-Israel e pró-Hamas, como bandeiras israelitas a arder e imagens de Gaza.

Quem forneceu pormenores desta informação à CNBC foi a empresa Check Point Software Technologies, firma de cibersegurança com sede em Telavive. Uma homóloga portuguesa, a **VisionWare, confirmou ao Expresso a atividade fervilhante que está a ser desenvolvida** nestes dias: "O conflito entre Israel e Palestina tem sido acompanhado de

uma **emergência considerável de grupos *hacktivistas*** [neologismo nascido das palavras *hacker* e ativista], havendo ciberataques dirigidos a alvos em ambos os lados do conflito", disse o seu CEO e fundador Bruno Castro.

"São **pequenos exércitos por procuração, pertencentes ou não a Estados e, neste caso atual, têm forte componente religiosa**", identifica Diogo Alexandre Carapinha, consultor da VisinWare e sub-coordenador da VisionWare Threat Intelligence Center.

Todos os dias são criados novos grupos e "não existe qualquer período de aprendizagem e adaptação, explica. Estes grupos de *hacktivistas* estão imediatamente prontos a agir logo que são criados, lançando ataques em nome das causas que defendem e mantendo-se disponíveis a fazê-lo recorrendo a quaisquer meios. Uma coisa é certa: **há cada vez mais meios para causar disrupção**.

Métodos e alvos

O relatório da informação recolhida junto das suas fontes e parceiros pela VisionWare, como fazem outros especialistas em cibersegurança de todo o mundo, faz lembrar um guião. "O Ministério da Saúde de Israel está em baixo depois de ter sofrido um ataque DDoS da Boom Security; Surgiu um novo grupo chamado Libyan Ghosts, que tem como alvos sites mais pequenos em Israel; Ghosts of Palestine está a atacar portais israelitas; Os Anonymous Sudan continuam a atacar o site do 'Jerusalem Post'; A KEP Team afirma ter visado o site do partido político Otzma Yehudit em Israel…".

Este **excerto do relatório elaborado pela VisionWare relativo a dia 9 de outubro** resulta da vigilância levada a cabo e serve de base para avaliar o grau de intensidade e importância dos ataques.

Os atos de disrupção no ciberespaço estão normalmente associados a Estados. Porém, **após a pandemia e a guerra na Europa houve uma explosão de *hacktivistas*.** A sua atividade tem um tanto de paralelo com o ciberterrorismo: são pessoas com ideologias e tendências religiosas, apoiam causas e contam com financiamentos, explica Carapinha.

As disrupções apontam para vários objetivos, do ataque a depósitos de água, apagamento de serviços públicos ou exposição de dados pessoais. Segundo disse a Check Point à cadeia CNBC, **o maior ataque ocorrido na última semana afetou o Ono Academic College, perto de Telavive**. Um grupo de *hackers* que afirma ter origem jordana penetrou no sistema privado do colégio e **publicou no Telegram mais de 250 mil fichas com dados de empregados, alunos, ex-alunos e outros**. Em resposta, o colégio desligou o sistema.

No conjunto dos distúrbios há mais ameaças do que ações, porém aquelas contribuem consideravelmente para a perturbação geral. **Parte fundamental destas ações é a mediatização dos atos**. "Os cibercriminosos anunciam a sua grandiosidade para que seja

divulgada a excelência da sua capacidade disruptiva. E, uma vez avaliada, que seja capaz de atrair pessoas recrutando-as para a causa", explica Carapinha.

Os **alvos principais são na maioria organizações governamentais, mas as infraestruturas civis** também têm sido atacadas, apesar de o Comité Internacional da Cruz Vermelha ter publicado um conjunto de diretrizes com regras de atuação para os *hackers* civis que atuam em cenários de conflito. Ao que parece, não teve grande efeito. **Alguns grupos aproveitaram para anunciar a intenção de atacar não só Israel, mas também a Europa e os Estados Unidos, como foi o caso dos Ghosts of Palestine**, resume Bruno Castro.

Um universo em expansão

"Nos mais de 20 anos que tenho de experiência neste domínio, **nunca tinha visto algo deste género**", assegura Castro. Segundo defende, a guerra na Ucrânia veio "abrir um precedente que nunca tinha sido explorado", nos termos do qual **grupos não-estatais passaram a possuir "um poder que antes pertencia apenas aos Estados**".

"Os sites do Governo israelita, agências de comunicação social e sistemas militares, por exemplo, estão entre os alvos mais visados, sendo **o vetor de ataque preferido o DDoS** [o atacante inunda um servidor com tráfico de internet, impedindo os outros utilizadores de terem acesso online aos serviços e sites].

A título de exemplo, "os Anonymous Sudan reivindicaram responsabilidade pela perturbação do sistema de radar de alerta precoce Tzeva Adom de Israel e pelo lançamento de um ataque DDoS ao 'Jerusalem Post', e os Stucx Team afirmaram ter pirateado o site do sistema SCADA israelita", exemplifica o fundador da VisionWare.

Estes **grupos de *hacktivistas* são atores não estáveis que se movimentam na *dark web***. Jogam num "tabuleiro cibernético" e **os seus movimentos e ações deixam um rasto, dispondo, no entanto, de capacidade de disfarce, de ocultar quem são e onde se encontram, sem paralelo no mundo físico**, explica Carapinha. São verdadeiras empresas, diz, com recursos humanos organizadas e gabinetes de comunicação.

Em termos de alinhamentos políticos ou ideológicos, a NATO e as nações ocidentais apoiam frequentemente Israel, enquanto muitos países asiáticos tendem a tomar o partido da causa palestiniana, esclarece o CEO. "Traduzir esta informação para grupos *hacktivistas* é tarefa complicada, uma vez que **estes grupos, embora estejam normalmente alinhados com os objetivos políticos do seu país de origem, podem adotar posições alternativas**".

O secretário-geral das Nações Unidas, António Guterres, referiu que **uma futura grande guerra será iniciada com um gigantesco ciberataque**. Por causa disso, diz Castro, no VisionWare Threat Intelligence Center, acredita-se que a "vigilância, recolha e análise atenta

destes fenómenos no ciberespaço são fundamentais para a consciencialização, estudo e prevenção” desta realidade.