Exclusivo

SEGURANÇA

Guerra no Irão: Portugal é um dos alvos de grupos de hackers do Médio Oriente (mas não está no topo da lista)

Suraxak Suwanmake

Principais grupos de hackers do Médio Oriente que podem atacar sistemas informáticos em toda a Europa como forma de retaliação aos raides aéreos dos EUA e Israel ao Irão estão identificados

HÁ 50 MINUTOS

Hugo Franco
Jornalista

Portugal já foi alvo de ciberataques no passado recente por parte de piratas informáticos iranianos. Não há, no entanto, registo de novas intrusões de hackers de Teerão desde o início dos ataques aéreos dos Estados Unidos e de Israel, a 28 de fevereiro. Portugal é um alvo, por ser um país da NATO e dar apoio à guerra com a Base das Lajes, mas não está no topo das prioridades do Irão, confirmam várias fontes conhecedoras do processo ao Expresso. "Ainda não houve ataques identificados contra Portugal, como represália do que se passa no Médio Oriente, mas podem estar a ser preparados e podem, eventualmente, intensificar-se nas próximas semanas", diz Bruno Castro, CEO da VisionWare, uma das principais empresas portuguesas de cibersegurança.

Os grupos criminosos que acederam de forma ilegítima aos sistemas informáticos nacionais antes do recrudescimento do conflito no Médio Oriente "fizeram-no de forma vertical", não porque Portugal fosse um alvo específico, mas porque se aperceberam de falhas em determinado sector - sobretudo banca, retalho ou hospitais - e atacaram-no em diferentes países simultaneamente, incluindo Portugal.

Existem suspeitas que entre os piratas informáticos que agiram nestes raides em infraestruturas digitais situadas em solo nacional havia alguns a soldo do Irão, mas também da Rússia, China ou Paquistão. "Não é fácil identificarmos especificamente a identidade dos intrusos. Mas suspeitamos que os iranianos agiram em aliança com outros hackers de vários países hostis à NATO, numa espécie de consórcio internacional", adianta Bruno Castro.

Esta quarta-feira, o próprio SIS alertou para a tentativa de intrusão de hackers estrangeiros [neste caso russos] em contas do Whatsapp e do Signal de governantes e diplomatas em toda a Europa para obter informação confidencial.

Bruno Castro a acredita que os grupos de cibercriminosos do passado recente oriundos destes países se transformem agora em 'hacktivistas' [piratas informáticos que atacam a soldo de uma bandeira, causa ou ideologia] como resposta a estas ações militares. O objetivo vai passar a ser a destruição dos sistemas informáticos de infraestruturas críticas dos Estados ocidentais aliados dos EUA. "Vão querer abanar as estruturas de segurança na tentativa de instalar o medo na sociedade." Este clima de insegurança será, para os 'hactivistas', mais importante até do que o roubo de segredos militares. "O ciberespaço permite criar custos, perturbar confiança pública, sondar defesas e preparar ataques mais sérios."

Bruno Castro lembra, no entanto, que irão realizar-se ciberataques em sentido contrário, de países da NATO contra o Irão.

OS PRINCIPAIS PIRATAS INFORMÁTICOS NA GUERRA

OS PRINCIPAIS PIRATAS INFORMÁTICOS NA GUERRA

Entre os principais grupos de piratas informáticos que podem ter um papel ativo durante a guerra no Médio Oriente estão já identificados nomes como os Keymous+ e os DieNet, responsáveis por "cerca de 70% da atividade ilegal observada no ciberespaço", refere o fundador da VisionWare.

Um relatório preliminar desta empresa, a que o Expresso teve acesso, revela que desde a fase inicial da operação militar houve "149 reivindicações" de ataques de Negação de Serviço Distribuído (DDoS) [que inunda um servidor, serviço ou rede com tráfego malicioso, esgotando recursos e tornando-o inacessível a utilizadores legítimos] contra "110 organizações em 16 países", conduzidos por "12 grupos" - com especial peso dos "Keymous+ e DieNet" - que têm "forte concentração geográfica em Kuwait, Israel e Jordânia". Mais de 50% dos alvos "foram entidades governamentais". As atividades ilegais concentraram-se "sobretudo no Médio Oriente, embora a Europa já represente uma parcela relevante do ruído operacional".

O documento refere que, para Portugal, o risco mais realista não é o de ser alvo prioritário de um ataque simbólico de grande visibilidade, mas sim o de ser "atingido por via indireta", destacando as "cadeias de confiança com fornecedores dos EUA, de Israel e do Golfo" e a "exposição de operadores de energia, telecomunicações, portos, aeroportos e cloud". Essa combinação "aumenta o valor estratégico do território português num cenário em que a guerra convencional já se expandiu para o domínio digital e para a infraestrutura tecnológica crítica".

O Keymous+ é um grupo 'hacktivista' que surgiu no final de 2023 e intensificou significativamente as suas operações ao longo de 2025. E é conhecido pelos seus ataques DDoS de alto volume, direcionados aos setores governamental, de telecomunicações e financeiro na Europa, no Médio Oriente e na Ásia. Já o DieNet, reivindicou há um ano um ataque cibernético à Trump Winery, uma produtora vinícola que pertence a Eric Trump, o filho do presidente dos EUA. E é uma das maiores da Virgínia.

Rui Martins, da Iniciativa Cidadãos pela Segurança, destaca um terceiro grupo: o APT33. "A Guarda Revolucionária iraniana está por detrás deste APT33, também conhecido como Holmium, Elfin ou Peach Sandstorm." Segundo o especialista, este grupo de guerra cibernética segue um modelo clássico de intrusão estatal, pouco sofisticado do ponto de vista técnico, mas altamente eficaz na persistência e no volume das suas operações externas.

Rui Martins acredita, tal como Bruno Castro, que os ciberataques vindos do Médio Oriente irão disparar num curto ou médio prazo. E argumenta que eles só não são mais fortes atualmente porque os ataques aéreos sobre Teerão cortaram a eletricidade e a Internet no país, afetando muitas universidades e quartéis da Guarda Revolucionária, onde atuam muitos destes hackers. "Quando estas infraestruturas se restabelecerem, os ciberataques contra o Ocidente podem vir a ser até superiores aos registados antes do início da guerra", vaticina.