Expresso
13.05.2022
P.08

SEGURANÇA

Portugal na mira dos mais perigosos ciberespiões russos

Invasão da Ucrânia fez aumentar o risco de ciberataques a países da NATO. **Hackers têm o patrocínio não-oficial de Putin**

Texto **HUGO FRANCO**
Ilustração **MÓNICA DAMAS**

À superfície, nada os liga aos principais serviços de informações de Moscovo, mas os mais temíveis e eficazes piratas informáticos russos atuam com o patrocínio não-oficial do FSB (o antigo KGB), GRU (serviços secretos militares3) e SVR (informações externas). E, movidos pelos milhares de dólares que ganham por cada ciberataque, prometeram ataques sem precedentes ao Ocidente em nome de Vladimir Putin, ameaçando aceder a bases de dados de instituições militares e governamentais e também de grandes empresas. Fontes ligadas à investigação do crime informático garantem ao Expresso que Portugal também está no mapa destes ciberespiões.

Logo após o início do conflito na Ucrânia, a 24 de fevereiro, o Gabinete Coordenador de Segurança — que engloba polícias, serviços de segurança e militares — reuniu-se de emergência: a invasão russa implicava cuidados especiais. Um facto confirmado por Paulo Vizeu Pinheiro, secretário-geral do Sistema de Segurança Interna na audição parlamentar desta semana, que sublinhou aos deputados que na "avaliação panorâmica" após o estalar da guerra foram consideradas as "ameaças e possíveis ameaças, incluindo o campo cibernético".

O Expresso sabe que antes do início dos confrontos entre Moscovo e Kiev tinham sido já produzidos relatórios de segurança sobre a ciberameaça proveniente da Rússia. Uma fonte que passou pelo Governo nos últimos anos revela que foram trocadas "bastantes informações" sobre esta pasta delicada e sensível durante os dois anos pandémicos. E o Expresso sabe também que as autoridades portuguesas, em conjunto com as congéneres europeias e norte-americanas, já identificaram os principais ciberespiões russos ou liderados por russos: as partes não descartam a hipótese de estes já terem atuado direta ou indiretamente em ataques recentes a organismos estatais e empresariais em Portugal.

Um dos mais temíveis tem um nome carinhoso: Fancy Bear ('Urso Chique'). São suspeitos de nos últimos anos terem atacado organizações governamentais, militares e de segurança de países da NATO, nunca escondendo a promoção dos interesses políticos do governo russo. O seu maior feito foi piratear *e-mails* do Comité Nacional Democrático para tentar influenciar o resultado das eleições presidenciais de 2016 nos Estados Unidos, que deram a vitória a Donald Trump. Mas também perturbaram as eleições alemãs e francesas, no mesmo período, ou o sistema informático de ministérios dos Países Baixos, tentando obter acesso a documentos governamentais secretos.

Os nomes toscos dos *hackers* russos contrastam com a sua perigosidade e sofisticação, como, por exemplo, os Sandworm ('Minhoca na Areia'), considerados o braço direito da secreta militar russa e que atacam a Ucrânia desde 2016. O último ciberataque aconteceu em abril, já durante o conflito. Há dois anos, a justiça norte-americana descobriu a identidade de seis destes operacionais russos, acusando-os de crimes de conspiração informática, sendo um deles suspeito de ter atacado o sistema informático dos Jogos Olímpicos de Inverno em 2018.

Estes *hackers* pertencem a grupos de criminosos "evoluídos tecnicamente", longe do clichê dos "miúdos de borbulhas" atrás de um computador

Já antes do início da invasão russa tinham sido produzidos em Portugal relatórios de segurança sobre a ciberameaça proveniente da Rússia

Apoio "total" a Putin

Para o especialista de cibersegurança Bruno Castro, CEO da empresa Visionware, os *hackers* russos são grupos de criminosos "evoluídos tecnicamente", muito longe da imagem clichê dos "miúdos de borbulhas" atrás de um computador. "São profissionais na intrusão, na chantagem em troca de dados (o chamado *ransomware*), na lavagem de dinheiro e na espionagem." Neste último capítulo, nem sempre se distinguem os piratas informáticos de Moscovo que atuam "ao abrigo da bandeira" dos que agem "apenas com intuito criminoso". Bruno Castro tem dados que levam a suspeitar que em ambos os casos os promotores dos ciberataques são instituições ligadas ao Kremlin, que, de forma anónima, podem esconder-se atrás dos *hackers*. "Desta forma podem atacar países do Ocidente e evitar retaliações, que poderiam, de outra forma, levar até a uma guerra."

A "The New Yorker" entrevistou recentemente jovens *hackers* russos que revelam a existência de uma regra de ouro entre os vários grupos: a de não trabalharem com o domínio ".ru", o que significa realizar operações ilegais sem deixar rasto na Rússia.

Embora a maioria se esforce por não mostrar proximidade com as estruturas do Kremlin, há quem não se mostre preocupado em demonstrar que trabalha em prol do regime de Vladimir Putin, como os grupos Conti e Coomingproject. O primeiro deixou uma mensagem de aviso partilhada no Twitter: "A equipa Conti anuncia oficialmente o apoio total ao governo russo. Se alguém decidir organizar um ataque cibernético ou quaisquer atividades de guerra contra a Rússia, vamos utilizar todos os nossos recursos possíveis para atacar as infraestruturas críticas do inimigo." O Departamento de Estado dos EUA anunciou este mês uma recompensa até 15 milhões de dólares por informações sobre este grupo de *hackers* russos. O Coomingproject também aproveitou as redes sociais para marcar uma posição: "Olá a todos. Nós iremos ajudar o governo da Rússia se forem realizados ciberataques contra o nosso país."

Pista russa esfumou-se

Tal como o Expresso revelou em fevereiro, a PJ seguiu o rasto de um *hacker* russo que anunciou num fórum *online*, Exploit.in, de acesso pago e onde piratas informáticos transacionam dados e informações quase sempre ilegais, estar à procura de compradores para o acesso ilegal ao sistema informático de uma companhia de telecomunicações portuguesa com receitas entre um e quatro mil milhões de dólares. Suspeitava-se que fosse a Vodafone Portugal, alvo de um ciberataque sem precedentes em Portugal no mesmo mês. Mas a pista esfumou-se e nunca se conseguiu saber a identidade e provar as transações deste pirata informático, apurou o Expresso junto de fontes judiciais.

Francisco Nina Rente, especialista em segurança informática da empresa Art Resilia, explica que os objetivos dos *hackers* russos diferem entre os que atacam grandes empresas privadas e os que entram nos sistemas informáticos governamentais. "Os primeiros, os chamados cibercriminosos, procuram o lucro. Os segundos andam atrás de informação confidencial de valor com o objetivo de fazerem exfiltração de dados e de criarem disrupção e destruição de sistemas."

O testemunho de um *hacker* russo à revista "Wired" revela a existência de uma cultura de *hacking* naquele país já nos tempos da URSS: "Quando andava na escola, nos anos 80, éramos encorajados a piratear software americano. Por isso dizemos que fomos o primeiro país a ter uma cultura *hacker*."

hfranco@expresso.impresa.pt

Russos tentam infiltrar-se em todo o lado

Polícias, forças militares, academia, laboratórios. Todos são alvo dos espiões russos nos países ocidentais. Portugal não é exceção

As informações são escassas, mas nos últimos anos têm sido produzidos relatórios na área da segurança nacional que dão conta de tentativas de infiltração, "de forma genérica", de espiões russos em áreas tão diferentes como as polícias, forças militares, na academia e em laboratórios. "Admito que isso tenha acontecido, mas os serviços de informações estão atentos", salienta José Manuel Anes, especialista em terrorismo.

Jorge Bacelar Gouveia, presidente do Observatório de Segurança, Criminalidade Organizada e Terrorismo, lembra que a Rússia reconstruiu o império em grande parte porque "recorreu à política de espionagem aos países considerados adversários". Portugal não é exceção, lembra.

No meio académico, a Fundação Russkiy Mir, liderada por um oligarca russo próximo de Putin, e que tinha há dez anos protocolos com a Universidade de Coimbra e do Minho, levantou suspeitas. Em 2016, o Parlamento Europeu acusara aquela fundação de desinformação e propaganda. Mas só esta semana, no meio da polémica com as associações pró-Putin de Setúbal, é que as duas universidades decidiram afastar-se daquela instituição "em função do contexto geopolítico atual", como noticiou a CNN Portugal.

Na última semana, o Expresso revelou que já depois do início do conflito na Ucrânia, dois russos foram detetados junto de instalações militares na área da Grande Lisboa. Em 2014, os serviços de segurança fotografaram russos perto de instalações da NATO, à guarda das Forças Armadas portuguesas, onde existem combustíveis e munições, na margem sul. De acordo com a SIC, nessa altura, os suspeitos terão descoberto que estavam a ser controlados, reagindo com manobras de contravigilância.

A polémica das associações russas pró-Putin em Portugal poderem estar a passar informações sensíveis a Moscovo tem gerado desconfianças mesmo no interior das polícias. Uma funcionária natural de um país de Leste do SEF da área dos passaportes foi recentemente acusada por colegas de ter ido para casa de baixa e levado consigo informações sensíveis. O caso tem estado a causar desconforto, mas fonte oficial daquela força de segurança desmente que a funcionária possa sequer ter acesso à base de dados interna. "Há um clima de caça às bruxas que pode levar inocentes a serem considerados suspeitos", diz uma fonte daquela polícia.

Espiões em Roma

O único caso de espionagem pró-russa que acabou na Justiça portuguesa foi o de Carvalhão Gil, agente do SIS condenado a sete anos e quatro meses de prisão por espionagem e corrupção. O operacional foi preso pelas autoridades italianas após um encontro suspeito em Roma com o espião russo Sergey Pozdnyakov, que viria a desaparecer de circulação. **H.F.**