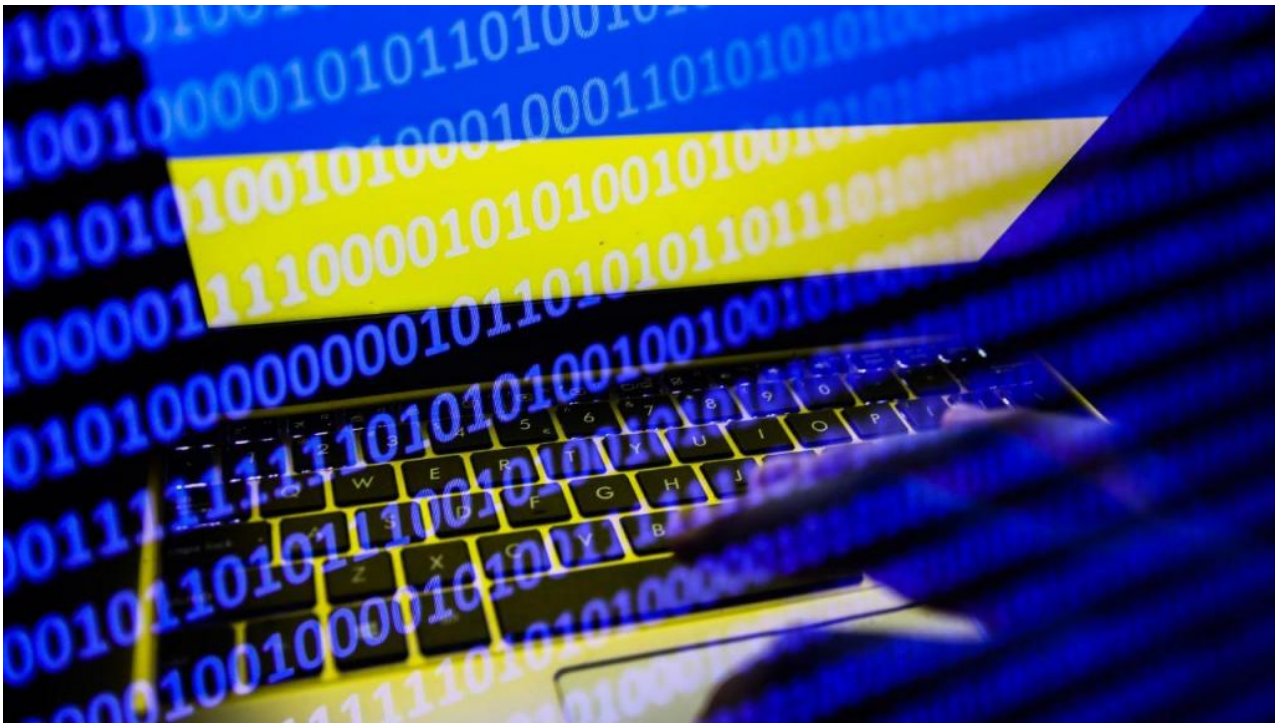
# "Atacamos tudo menos hospitais e serviços essenciais". Por dentro do grupo de hackers portugueses que luta contra a guerra da Rússia

cnnportugal.iol.pt/ciberataque/ciberseguranca/atacamos-tudo-menos-hospitais-e-servicos-essenciais-por-dentro-do-grupo-de-hackers-portugueses-que-luta-contra-a-guerra-da-russia/20230223/63f67feb0cf2c84d7fc94ad2

João Guerreiro Rodrigues
23 fev, 07:00



## Decidiram responder ao chamamento da Ucrânia, no momento em que esta mais necessitava. Dizem-se "hackers éticos" e estão há quase um ano a lançar ciberataques contra infraestruturas digitais russas para tentar travar a guerra lançada por Vladimir Putin

"Esta também é uma guerra nossa", argumenta o grupo de hackers portugueses que, ao longo de um ano, atacou centenas de sites e plataformas russas, mandou abaixo os sites do Partido Comunista Português e da Amnistia Internacional. Prometem não parar enquanto "os crimes de Vladimir Putin" continuarem. Quebram leis ao levar a cabo ataques informáticos, mas veem-se como *hacktivistas* e não como piratas informáticos, porque não querem ganhar dinheiro com o que fazem. Garantem que o que os move "é o respeito pela soberania de um povo e o respeito pela vida humana" e deixam um alerta: "Estamos a planear uma nova onda de ataques cirúrgicos em Portugal."

"Os primeiros meses foram alucinantes", admite à CNN Portugal "Spectre", o líder de um grupo de portugueses que, praticamente desde o início da invasão da Ucrânia, está a conduzir uma vaga de ciberataques contra as mais diversas infraestruturas russas. "Eu

alistei-me após o apelo do ministro da Ucrânia, revi-me na missão e aceitei o desafio", diz. Mas não foi o único. Ao todo são sete os membros do grupo de hackers portugueses que se desdobra em ataques diários contra alvos russos. "Atacamos tudo menos hospitais e serviços essenciais", revela outro membro, conhecido por "Cyborg".

Fazem parte de um grupo conhecido como IT Army of Ukraine, um "ciberexército" criado pelo próprio ministro ucraniano da Transformação Digital, Mykhailo Fedorov, dois dias depois do começo da guerra de Vladimir Putin. À semelhança de Volodymyr Zelensky, que nos primeiros dias da invasão apelou a voluntários com experiência militar de todo o mundo para defenderem a Ucrânia, Federov chamou para si um grupo de especialistas em informática, voluntários com o objetivo de levar a guerra ao ciberespaço russo. No seu auge, o grupo teve quase 300 mil participantes no seu canal de Telegram.

"Chegámos a ser oito, dos quais apenas quatro 'disparavam o gatilho' com acesso aos meios mais pesados", explica Spectre. Quando fala nos meios mais pesados refere-se à rede que utilizam para inundar servidores "inimigos" com entradas falsas. Aos restantes membros cabia a função de deteção de alvos ou, como lhe chamam, "a fase de estudo". Nesse processo, que conta com uma análise de que não haverá danos colaterais, informam o grupo ucraniano e procedem ao ataque.

"Para nós, os alvos legítimos são os que estão dentro das fronteiras russas ou dos seus aliados, como a Bielorrússia ou o Irão. Às vezes, também em países onde existem fortes defensores do regime russo", conta.

## Nova onda de ataques em Portugal

Foi essa mesma motivação que, dizem, os levou a atacar vários alvos em Portugal. Logo em abril, juntamente com um grupo de piratas georgianos, mandaram abaixo o site do Partido Comunista Português, bem como todas as contas associadas à estrutura partidária, como o jornal Avante! ou a Juventude Comunista. Em causa estava a tomada de posição dos comunistas, que se opuseram ao convite do presidente ucraniano, Volodymyr Zelensky, para discursar na Assembleia da República. Seguiram-se ataques contra a Câmara Municipal de Setúbal, após a polémica que envolveu o acolhimento aos refugiados ucranianos - que foram recebidos por simpatizantes russos, e contra a Amnistia Internacional, depois de a ONG ter publicado um relatório que acusa a Ucrânia de colocar em perigo de vida os seus próprios cidadãos.

"Mantemos o PCP debaixo de olho. Estamos a planear uma nova onda de ataques cirúrgicos em Portugal. Estamos a ponderar alargar o critério de alvos contra indivíduos que espalham desinformação", indica "Spectre", o líder do grupo.

Estes ataques são levados a cabo com ferramentas de fonte aberta, a que qualquer pessoa pode aceder e modificar, fornecidas pelo exército ucraniano. Algumas destas "armas" são bastante poderosas. "Para alguns, o IT Army of Ukraine é como um curso gratuito de

hacker", admite "Cyborg". Foi precisamente isso que aconteceu a alguns dos membros do grupo, que não tinham qualquer formação tecnológica e foram aprendendo a executar ataques sob a liderança de outros membros.

O tipo de ataque mais utilizado pelo grupo é o chamado DDoS (ataque distribuído de negação de serviço), que, no fundo, inunda um determinado endereço de um site com uma quantidade elevada de requisitos de entrada, bloqueando temporariamente a página. Estes ataques são os mais comuns, a par do "defacing de sites" (danificar a aparência de um site) ou o "web cache poisoning" (explorar vulnerabilidade para desviar o tráfego da internet para servidores falsos).

A capacidade disruptiva desta organização está a ser descrita pelos russos como "um evento sem precedentes". A agência de notícias estatal russa TASS revelou que as estruturas digitais do governo e de algumas das principais empresas privadas estiveram todo o ano a ser vítimas de "um grande esforço técnico" vindo do estrangeiro. Para tentar mitigar estes efeitos, o Kremlin está a ponderar uma bolsa de 14 mil milhões de rublos (aproximadamente 122 milhões de euros) para ajudar as empresas com apoio tecnológico.

Desde que a Rússia fechou a internet ao exterior tem sido mais difícil do ponto de vista técnico para realizar alguns destes ataques, particularmente de endereços registados na Rússia e na Ucrânia. Por isso, a estratégia foi adaptada e no canal de Telegram, onde as autoridades ucranianas dão instruções aos 'piratas informáticos', relembram os passos a dar para contornar a situação. "Não se esqueçam de utilizar uma VPN durante o ataque", insistem constantemente. Ou seja, a solução encontrada passa por utilizar um serviço de VPN (uma rede privada virtual) ou de VPS (um servidor privado virtual) que, na prática, permite "camuflar" a origem do ataque com a utilização de um endereço sediado noutro país.

"Admito que trabalhamos numa zona cinzenta. Compreendo que as nossas ações podem ser vistas como ilegítimas, apesar de promoverem um objetivo legítimo. No fundo, é a guerra necessária para estabelecer a paz. Mas nenhum membro do ciberexército consegue utilizar os meios mais pesados para fins pessoais", frisa "Spectre".

## Hacktivismo está a mudar

Os próprios especialistas em cibersegurança admitem que as características do *hacktivismo* estão a mudar. Segundo um estudo da Check Point Research, o novo modelo é agora mais bem estruturado, organizado e sofisticado. Estes novos grupos, onde assenta o IT Army of Ukraine, destacam-se por terem uma ideologia consistente, processos de recrutamento, uma liderança descentralizada e fornecimento de ferramentas aos membros.

"O 'hacktivismo' é um conceito que está a crescer, particularmente em torno do conflito entre Estados, como é o caso da guerra entre a Rússia e a Ucrânia. Estamos a ver uma espécie de chamada às armas para que se façam ataques com base numa bandeira

estatal", afirma o especialista em cibersegurança Bruno Castro, CEO da Visionware.

Para o especialista, cada vez mais estes grupos cumprem uma função de braços armados de países na tentativa de levar a cabo "uma espionagem não ruidosa", capaz de monitorizar as atividades dentro dos sistemas de outros países, bem como uma "disrupção capaz de colocar em causa a segurança de serviços críticos do Estado". É isso que grupos como o IT Army of Ukraine fazem quando aplicam um ataque de grande escala DDOS. E não existe um antídoto contra estes ciberataques.

"Preventivamente é muito difícil. Um ataque DDOS não tem propriamente grandes vacinas eficazes contra ataques de grande envergadura, capazes de colocar em causa um serviço crítico. Mas diria que a tendência de ataques já não passa tanto por aí. Vamos ver mais espionagem, mais roubo de informação, mais extinção de dados e mais ransomware", aponta Bruno Castro.

E é essa a grande tendência do outro lado. Na Rússia, existe um grupo de piratas informáticos que tem conseguido fazer nome na procura de retaliação contra o Ocidente: a Killnet. Desde fevereiro, o coletivo russo atacou dezenas de alvos um pouco por todo o mundo, desde aeroportos internacionais, a páginas dos governos e das polícias de vários países, bem como o portal da DGS e da Faculdade de Farmácia da Universidade de Lisboa.

O grupo é reconhecido internacionalmente por, à semelhança dos mercenários da Wagner, ter ligações ao Kremlin, embora a identidade dos seus líderes seja muito mais obscura, de natureza descentralizada e com pouca informação sobre os seus membros. Antes do conflito, estes piratas informáticos alugavam a sua *botnet* para levar a cabo ciberataques por 1.350 dólares por mês (cerca de 1.270 euros). As *botnets* são exércitos virtuais de computadores infetados que podem ser organizadas para levar a cabo ataques DDOS.

Os ciberataques de origem russa contra países da NATO aumentaram 300% em 2022, segundo um relatório dos investigadores da Mandiant, empresa de investigação ligada à Google.

"A Killnet é o braço armado no ciberespaço de Putin. Vão atacar mais. Olhamos com cuidado e preocupação porque Portugal não está preparado para ataques a sério. Até agora foi tudo a brincar", garante o grupo português.

## "Risco de ser paralisado"

É um dos principais alertas dos piratas informáticos: o Estado português "corre o risco de ser paralisado" com ciberataques. De acordo com vários membros do grupo, existe uma falta de capacidade nos sistemas do Estado e que eles próprios já testaram a resiliência de alguns dos principais domínios. Uma mistura explosiva quando combinada com o facto de o nosso país ser cada vez mais escolhido como alvo de cibercriminosos. No ano passado, Portugal foi um dos países mais afetados por ciberataques na Europa, com bancos e hospitais a verem os seus serviços limitados devido a atores externos.

Ataques desta magnitude não são baratos e os sete membros do grupo português admitem gastar perto de mil euros mensais para poder continuar a atacar a Rússia. São necessários “muitos gigas” e “servidores em centros de dados internacionais” para levar a cabo os ataques de larga escala capazes de saturar os sistemas mais bem preparados. “Fazemos ataques de força bruta e por isso é que a guerra custa muito dinheiro. Uma ciberguerra não se faz só com vontade, é preciso planeamento e muito dinheiro. Controlamos vários servidores espalhados pelo mundo, inclusive na Rússia”, frisa "Cyborg".

Questionados sobre se o que estão a fazer constitui um crime, "Spectre" diz que ele e os restantes portugueses são o que chama de “hackers éticos” e afasta a ideia de que as ações do grupo contra a Rússia possam acabar por fazer com que os cidadãos russos se sintam injustamente atacados. “Nós não somos iguais a Putin”, defende o hacker, acrescentando que “pagar a fatura” do seu líder pode ser a única forma de fazer com que os russos queiram derrubar o regime.

E mesmo que a guerra acabe o grupo tem já uma missão em preparação, e que continua a passar pela Rússia. À CNN Portugal o grupo revelou que começou a trabalhar, em simultâneo com membros de outros países, para encontrar o rasto das centenas de milhares de crianças ucranianas que foram deportadas para a Rússia e que estão a ser adotadas de forma forçada por famílias russas.

“No final da guerra, demore o que demorar, vamos atrás do rasto das milhares de crianças roubadas pelos russos para o mercado de adoções ilegais dentro da Rússia. Há registos. Estamos atrás deles. Nós, portugueses, e alguns estrangeiros já escolhemos essa como a nossa derradeira operação. Queremos colocar a bandeira portuguesa nesse esforço”, garante o grupo.

Temas: Ciberataque Cibersegurança Hackers Ucrânia Guerra