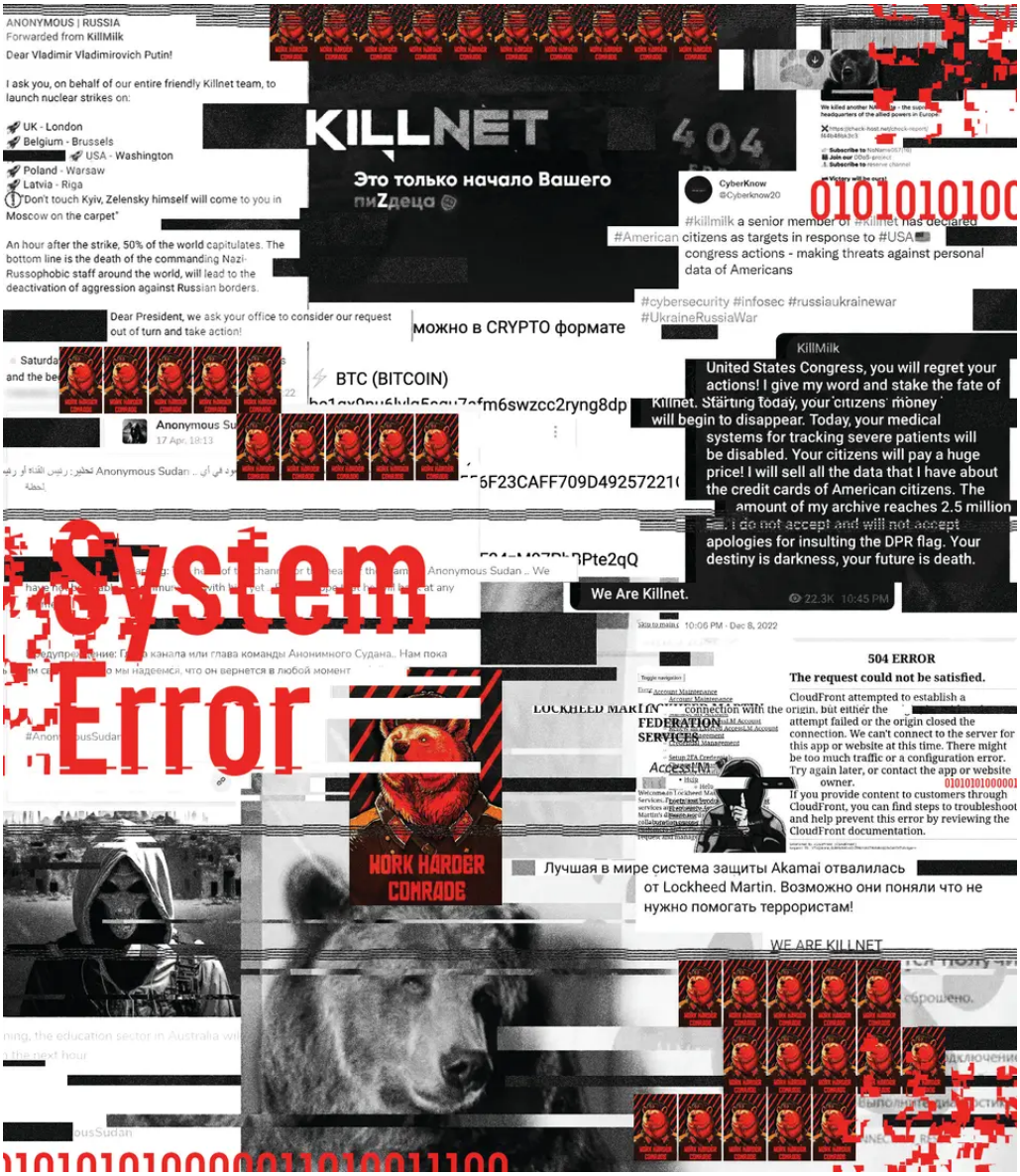
Hackers pró-Rússia criam “caos” a oeste

leitor.expresso.pt/semanario/semanario2634/html/primeiro-caderno/internacional/hackers-pro-russia-criam-caos-a-oeste

CIBERGUERRA

Hackers pró-Rússia criam “caos” a oeste



Grupos lançam milhares de ataques contra entidades ocidentais. Serviços públicos estão entre os alvos

Textos Tiago Soares

Harv Xavier considera-se um “hacktivista”, um neologismo que junta hacker e ativista. Fala com o Expresso a partir de Kiev, onde está a participar numa ciberguerra que é tão antiga quanto a invasão da Ucrânia pela Rússia. “Voluntariei-me para o IT Army há um

ano para ajudar a proteger infraestruturas críticas dos ataques russos, e para conduzir missões de espionagem contra a ciberguerra russa", explica Xavier, também conhecido online como Von Harvix.

O "IT Army da Ucrânia" não faz parte das Forças Armadas ucranianas, mas tem sido essencial para contrariar a avalanche de ataques informáticos de grupos pró-russos contra Kiev, e que têm sido capazes de roubar informação e "atrasar a entrega de comida, medicamentos e assistência humanitária", diz Harv. Pelas suas contas, os grupos de hackers pró-Kremlin aumentaram os seus ataques contra a Ucrânia em 250% desde 2020 — e triplicaram contra países da NATO.

Enquanto este texto estava a ser escrito, durante esta semana, foi atacado o site da Federação de Futebol dos Países Baixos; a rede do multibanco Eurocontrol; e os sistemas do Raiffeisen Bank na Polónia. Em todos os casos, os hackers congratularam-se pelos ataques nas suas redes sociais.

O grupo pró-russo mais ativo chama-se NoName057 e foi anunciado pelos seus membros no Telegram poucos dias antes do início da guerra. Só nos primeiros três meses do ano, foi responsável por mais de 900 ataques informáticos contra entidades públicas e privadas ocidentais, segundo dados partilhados com o Expresso pela empresa portuguesa de cibersegurança VisionWare, que tem uma equipa de informações estratégicas dedicada a monitorizar grupos de hackers na dark web.

Além dos NoName057, duas outras 'equipas' têm-se destacado pela sua atividade criminosa a favor do Kremlin: o grupo Killnet, responsável por atacar bancos dinamarqueses, portais oficiais de Governos europeus ou o site do Festival Eurovisão da Canção; e os Anonymous Sudan, que têm bloqueado vários serviços do Estado sueco, aproveitando o processo de adesão à NATO.

No total, estes três grupos já lançaram mais de 2 mil ataques desde o início do ano — e esta é uma estimativa "muito conservadora", diz ao Expresso Diogo Carapinha, subcoordenador do VisionWare Threat Intelligence Center, apontando para um número real bastante superior. Todos se consideram "hacktivistas" — não cometem ataques por razões financeiras — e especula-se que trabalhem regularmente em coordenação com as autoridades russas.

Desde o início do ano, três grupos de hackers pró-Putin lançaram mais de 2000 ataques contra o Ocidente

"Antes da guerra havia uma grande prevalência de ataques de ciberespionagem com o objetivo de roubar informação, agora sente-se uma manifesta intenção de criar o caos nas entidades ocidentais", diz Luís Lobo e Silva, diretor da Focus2Comply, uma empresa portuguesa que trabalha com outras empresas para estabelecer práticas capazes de prevenir e contrariar ataques. "Estão a travar uma guerra para fazer parar a nossa economia", acrescenta, fazendo o paralelo com as sanções ocidentais contra Moscovo.

O Kremlin está a investir ainda mais na ciberguerra, diz Harv, e estes grupos profissionalizaram-se. A 13 de março, o líder dos Killnet anunciou no Telegram a criação de um exército virtual: "Vou criar uma nova estrutura de 'hacktivistas' para a comunidade russa. Não vai ser apenas um movimento com ideias próprias. Será uma máquina organizacional com as suas próprias leis e objetivos, com disciplina e ordem. 24 divisões 100% sincronizadas. Uma única unidade com uma linha 24/7 para receber pedidos e ordens. Vai chamar-se Organização Militar Privada de Hackers Black Skills, ou Black Skills", escreveu o líder do grupo, conhecido por Blackside e que terá assumido o lugar em junho do ano passado.

Outro grupo, os Lockbit, têm semelhanças com os Black Skills: responsáveis por pelo menos 796 ataques informáticos só em 2022, também têm uma estrutura desenhada ao pormenor. "É como se fossem uma empresa. Têm um departamento de comunicação e um processo de recrutamento rigoroso", aponta Diogo Carapinha. Conseguiram bloquear sistemas de hospitais no Canadá na altura do Natal, e no início do ano entraram dentro do sistema da Royal Mail, a empresa de correios britânica, exigindo um resgate na ordem dos €80 milhões.

A NATO tem reforçado as suas defesas — ainda esta semana levou a cabo exercícios de segurança a partir de Tallinn, na Estónia — mas isso não impediu um ataque ao site da sua sede operacional (SHAPE) no final de março, noticiado pelo Expresso, nem o ataque desta semana levado a cabo pelos Killnet: informações sensíveis sobre as operações da Aliança Ocidental foram roubadas e postas à venda na dark web por um euro.

"O ataque desta semana foi muito mais grave. Houve intrusão nos servidores e roubo de informação sensível que pode vir a ser usada para fins militares e políticos. É uma forma de criar pânico e mostrar a fragilidade do lado ocidental", considera Bruno Castro, fundador da Vision Ware.

Ameaças contra Portugal são "muitas e diárias"

Portugal não tem escapado a esta ameaça. As tentativas de ataques informáticos a entidades públicas e privadas nacionais são "muitas e diárias", revela ao Expresso o secretário de Estado da Digitalização e da Modernização Administrativa, Mário Campolargo. Sectores críticos como a saúde e a educação são alvos preferenciais. Só em fevereiro, o Killnet atacou o sistema do Hospital Amadora-Sintra e mandou abaixo os sites da Direção-Geral de Saúde e da Faculdade de Farmácia da Universidade de Lisboa. A Câmara Municipal de Odemira viu os seus servidores "atingidos" no final de março, o que "afetou os serviços municipais" durante vários dias. E há duas semanas, foi a vez do site do Ministério da Economia.

Segundo dados do Centro Nacional de Cibersegurança (CNCS), foram registados 2023 ataques informáticos no ano passado, uma subida de 14% em relação a 2021. "Há um forte crescimento no ransomware e nos ataques de negação de serviço (DDoS)", diz fonte oficial do Governo.

“O efeito da guerra na Ucrânia não representa, instantaneamente, um maior número de incidentes, mas antes uma alteração no quadro de ameaças, motivações e modus operandi dos seus agentes. Destaca-se o surgimento de dezenas de grupos, de ambas das partes do conflito, a realizar estes ataques”, acrescenta a Secretaria de Estado da Digitalização, que tem a tutela da cibersegurança nacional.

Alguns alvos dos hackers pró-russos este ano

9, 10 e 11 de janeiro

Grupo Killnet ataca os sistemas de três bancos da Dinamarca e o site do Ministério das Finanças.

12 de janeiro

Os NoName057 lançam um ataque em massa contra vários portais do Governo da Chéquia, incluindo o do Ministério dos Negócios Estrangeiros.

23 de janeiro

Os NoName057 bloqueiam os serviços da Avast, uma empresa de antivírus sediada na Chéquia.

28 de janeiro a 2 de fevereiro

O grupo Killnet publica uma lista de instituições médicas na Europa e nos EUA que planeia atacar e mobiliza os seus apoiantes para o efeito. Vários dos ataques são bem-sucedidos, incluindo contra a Direção-Geral da Saúde.

8 de fevereiro

As plataformas de vários aeroportos da Suécia são atacadas pelo grupo AnonymousSudan. Dois dias depois são bloqueados vários hospitais e clínicas.

12 de fevereiro

Coordenado entre vários grupos, é lançado um ataque DDoS (bloqueio do serviço) ao site da Sede de Operações Especiais da NATO. Poucas semanas depois, o feito é repetido contra o quartel-general da Aliança Atlântica.

21 a 26 de fevereiro

Em poucos dias, os NoName057 imobilizam várias plataformas oficiais dos governos de Itália e Espanha.

15 a 22 de março

Os AnonymousSudan bloqueiam aeroportos e hospitais franceses, ao mesmo tempo que os NoName057 travam a ADIF, a entidade governamental responsável por operar a rede de comboios em Espanha.