Português (Original) Inglês


(/profiles/publishers/ec919192-b113-4ac6-971f-32a343edcd44)

AVE 13 389 € • OTS 111 575

Guerra cibernética. A guerra silenciosa que a televisão não pode mostrar, mas que já preocupa os EUA (https://observador.pt/especiais/guerra-cibernetica-a-guerra-silenciosa-que-a-televisao-nao-pode-mostrar-mas-que-ja-preocupa-os-eua/)

(HTTPS://IMAPP.INVISIBLEMEANING.COM/VIEW/ARTICLES/24DF76E6-8A2D-48D3-8E61-43681DD1A536?CROWID=C057ABDA-4E5A-4047-8E33-8AD77555EC36&LANG=1) •
OBSERVADOR (/PROFILES/PUBLISHERS/EC919192-B113-4AC6-971F-32A343EDCD44) •
ONLINE (HTTPS://OBSERVADOR.PT/ESPECIAIS/GUERRA-CIBERNETICA-A-GUERRA-SILENCIOSA-QUE-A-TELEVISAO-NAO-PODE-MOSTRAR-MAS-QUE-JA-PREOCUPA-OS-EUA/) •
SÓNIA SIMÕES • 25/02/2022 23:55 • 7 MIN

Guerra cibernética. A guerra silenciosa que a televisão não pode mostrar, mas que já preocupa os EUA

Sónia Simões

O Departamento de Segurança Nacional norte-americano avisou todas as estruturas do Governo para reforçarem os seus sistemas virtuais, temendo ataques cibernéticos por parte da Rússia após as sanções.

Enquanto as tropas russas avançam em terreno ucraniano com artilharia pesada, há uma guerra invisível em várias frentes que ninguém vê e que usa outro tipo de armas: as cibernéticas. Uma guerra que se arrasta há anos por um território bem mais amplo e que agora está a preocupar os países que aplicaram sanções à Rússia, sobretudo os Estados Unidos — que já lançaram um alerta no país.

O Departamento de Segurança Nacional (DS) norte-americano avisou todos os departamentos do Governo, dos maiores aos mais pequenos, para terem especial atenção às vulnerabilidade dos seus sistemas e melhorarem a sua resistência física e digital. Melindrados com um passado não muito longínquo de ataques que os serviços secretos atribuíram aos russos, os Estados Unidos admitem que, “embora não existam ameaças neste momento”, o DSN está a tomar “medidas apropriadas para garantir que os esforços federais sejam coordenados, se necessário”,

lê-se num comunicado citado pelo El Mundo

As autoridades advertem mesmo para possíveis ataques informáticos por parte dos russos contra empresas ou infraestruturas do país, embora o Presidente Joe Biden já tenha garantido que Washington está preparada para responder a possíveis ataques digitais, — depois de esta quinta-feira ter respondido à invasão da Ucrânia com sanções contra cinco entidades financeiras russas, entre elas dos maiores bancos do país, o Sberbank e o VTB, assim como contra oligarcas próximos do Kremlin, como Ígor Sechin, o presidente da Rosneft, a maior petrolífera do país. Biden anunciou também restrições às exportações de alta tecnologia para debilitar os setores estratégicos e militares russos.

Um ataque a uma empresa que atingiu 18 mil clientes

Alguns dos maiores ataques contra estruturas norte-americanas nos últimos dois anos têm, segundo os norte-americanos, as mãos de hackers russos. Na lista está o ataque à SolarWinds, como recorda a Business Insider , que levou ao encerramento de um dos maiores oleodutos de combustível americanos por vários dias. Houve ainda um ataque a um dos maiores produtores de carne do mundo, a multinacional JBS.

Quem atacou o sistema atingiu os 18 mil clientes que usavam o software daquela empresa de tecnologia, uma rede chamada Orion — foi atacada ao longo de nove meses de 2020, até ser detetado. Entre os clientes afetados estão empresas como a Microsoft e a Malwarebytes, órgãos do governo dos EUA, como o Departamento de Justiça, o Departamento de Energia, a National Nuclear Security Administration (NNSA) — responsável pelo arsenal de armas nucleares dos EUA –, a Federal Energy Regulatory Commission (FERC), os laboratórios nacionais de Sandia e Los Alamos no Novo México e em Washington, o Office of Secure Transportation na NNSA e o Richland Field Office do DoE.

Já antes a Rússia tinha sido acusada de perpetrar campanhas de desinformação online contra os Estados Unidos, interferindo mesmo nas eleições norte-americanas. E não foi apenas através da alegada criação de algoritmos e perfis no Facebook que evidenciavam opiniões pró-Donald Trump. A própria candidata às presidenciais de 2016, Hillary Clinton, afirmou ter perdido as eleições por causa dos russos. Dois anos depois o Departamento de Justiça dos Estados Unidos acusava 12 funcionários do serviço de inteligência russo por terem invadido os computadores do Partido Democrata e do comité de campanha da candidata do partido e terem roubado documentos e informações que divulgaram na internet.

O especialista em cibersegurança e CEO da VisionWare, Bruno Castro, lembra ao Observador que esta guerra cibernética não é só dessa altura. Já na guerra do Iraque foi usada “numa fase prévia aos bombardeamentos para anulação das estruturas do sistema de defesa”. Também em

2014, antes de a Rússia tomar a Crimeia, “houve um ataque cibernético que comprometeu as comunicações e a energia de forma a deixar o pais às cegas”, lembrou ao Observador, por seu turno, o professor da Universidade do Porto, Luís Filipe Antunes, do Centro de Competências em Cibersegurança e Privacidade.

Antes de invadir a Ucrânia, a Rússia terá atacado informaticamente algumas estruturas ucranianas. E depois de entrar no país pelo norte, leste e sul, e de bombardear várias cidades, o próprio Centro Nacional de Coordenação e Resposta a Incidentes de Computador da Rússia alertou para uma retaliação com possíveis ataques informáticos que “podem ter como objetivo interromper o funcionamento de importantes recursos e serviços de informação, causando danos à reputação, inclusive para fins políticos”, como foi noticiado.

“Qualquer falha na operação de objetos [infraestrutura de informação crítica] devido a um motivo que não é estabelecido de forma confiável, em primeiro lugar, deve ser considerado como resultado de um ataque de computador”, advertiu a agência russa. Uma guerra que corre paralelamente à guerra no terreno, com material bélico, e que serve para fragilizar o outro estado. Neste casos, explica Bruno Castro, estamos perante a chamada warfare , por ser uma guerra entre estados. “Numa guerra cibernética, não temos imagens para passar na televisão, mas são guerras ultraviolentas, silenciosas e só visíveis quando há uma disrupção de um serviço” que afeta o cidadão.

E lembra que Rússia não só está bem apetrechada no que toca a material bélico, como “tem também um armamento cibernético muito avançado”. Para Bruno Castro não são só os Estados Unidos que correm riscos, mas também todos os países que estão do lado da Ucrânia, o que significa os estados-membros da NATO e até da União Europeia, que fazem fronteira. Até porque um ataque bélico, com artilharia pesada, tem um custo humano muito elevado. E não só.

“Estes países poderão ser alvos, dado que um movimento bélico convencional iria originar uma terceira Guerra Mundial. Enquanto nesta guerra invisível pode atacar-se a energia de um país, o seu sistema de saúde, de defesa. Mas, no fim do dia, será sempre anónimo, não terá lá uma bandeira ou um tanque russo a assinar o ataque”, explica. “Poderá ser uma das grandes armas da Rússia”, antecipa.

Já Luís Filipe Antunes lembra que a falta de prova de um ataque destes permite criar disrupções noutro país sem com isso ter consequências, caindo-se mesmo “no campo das especulações” de quem fez o quê. O especialista, que prefere chamar aos hackers de peritos em segurança informática, pela conotação negativa dos primeiros, lembra que o ciberespaço tomou uma nova dimensão na guerra. Pelo que já é comum cada Estado apetrechar-se de especialistas, uns com maior apetência em ataques e outros na defesa para protegerem as suas estruturas.

"É quase como um jogo de futebol. É muito mais fácil atacar do que defender. Para atacar a sua casa basta que tenha uma janela aberta, para defender temos que cobrir toda a área potencial do ataque", explica. E já há grandes empresas a fazer o mesmo. "Existem empresas à escala global que identificam os melhores profissionais de cibersegurança em vários pontos geográficos do mundo e reúnem os 20 melhores num hotel por exemplo. O objetivo é, imaginemos, derrubar a Google. Os que conseguem têm uma compensação valiosíssima.

Os grandes gigantes tecnológicos vão por aqui, é o chamado Bug Bounty, em que as empresas pagam a quem lhes reportar vulnerabilidades. O Estado português devia ter um programa de Bug Bounty dentro da Administração Publica", sugere. A ideia é que estes especialistas testem ao limite as vulnerabilidade de cada empresa ou país, como já está a ser feito em muitos Estados. "Se eu tivesse que defender um servidor, o que eu queria fazer era contratar os melhores profissionais do mundo para me atacarem. Se não conseguissem dormia descansado", acrescenta.

Uma guerra com várias frentes. E que não tem só militares no ataque

Numa outra frente desta guerra cibernética estão também os chamados hacktivistas. Esta sexta-feira, pouco mais de 24 horas após a entrada dos russos na Ucrânia, o grupo Anonymous publicou um apelo na rede social Twitter. Pela paz iriam todos tentar atacar as infraestruturas russas de modo a enfraquecer o inimigo que está a desolar a Ucrânia. Horas depois anunicavam que tinham deitado abaixo o site do Kremlim — ainda que vários utilizadores do Twitter afirmassem que estava a funcionar e que conseguiam aceder. Outros sites russos foram depois disso atacados.

"Queremos que o povo russo entenda que sabemos ser difícil para eles falarem contra seu ditador por medo de represálias. Nós, como um coletivo, queremos apenas paz no mundo. Queremos um futuro para toda a humanidade. Então, queremos que entendam que isso é inteiramente direcionado às ações do governo russo e de Putin", anunciou o grupo, segundo o Tecmundo. "É uma guerra muito mais ampla e com atores que não são só os militares. Esta parte do hacktivismo, se conseguir criar disrupção na Rússia, é uma realidade", adverte Luís Filipe Antunes.

Aliás, já no dia anterior, o primeiro do ataque com mísseis sobre o território ucraniano, segundo a Reuters, a Ucrânia tinha lançado um apelo a voluntários hackers que quisessem colaborar com o Governo, não só para protegerem as suas infraestruturas, como para fazerem ações de espionagem. Esta é, segundo Bruno Castro, uma outra componente da guerra cibernética. Segundo a sua explicação, existem duas camadas: a espionagem cibernética e a guerra cibernética usada para a disrupção de serviços, provocando a instabilidade do país no seu

sistema de informação. Também a componente de inteligência, para a qual contribuem as ações de espionagem, é “igualmente importante”. “Este é o patamar de jogo que não tem nada a ver com o cibercrime”, avisa.

Tecnológico PT (/articles/?themeId=1458)

Observador (/profiles/publishers/ec919192-b113-4ac6-971f-32a343edcd44)

Já há bancos russos a cair na União Europeia. Braços do Sberbank em insolvência (/articles/fe1c442a-3ce7-44ee-8ae9-85bf11bc5273)
OBSERVADOR (/PROFILES/PUBLISHERS/EC919192-B113-4AC6-971F-32A343EDCD44) •
ONLINE (HTTPS://OBSERVADOR.PT/2022/02/28/JA-HA-BANCOS-RUSSOS-A-CAIR-NA-UNIAO-EUROPEIA-BRACOS-DO-SBERBANK-EM-INSOLVENCIA/) •
28/02/2022 00:59 • 3 MIN

Financeiro PT (/articles/?themeId=1459)

Rosneft tornou-se a maior petrolífera russa com Putin. Saída da BP é muito mais do que economia (/articles/e9385630-3c71-435c-a0f6-de60da0af9f1)
OBSERVADOR (/PROFILES/PUBLISHERS/EC919192-B113-4AC6-971F-32A343EDCD44) •
ONLINE (HTTPS://OBSERVADOR.PT/ESPECIAIS/ROSNEFT-TORNOU-SE-A-MAIOR-PETROLIFERA-RUSSA-COM-PUTIN-SAIDA-DA-BP-E-MUITO-MAIS-DO-QUE-ECONOMIA/) •
27/02/2022 23:53 • 6 MIN

Energético PT (/articles/?themeId=1463)

Governo prepara medidas para atenuar subida dos preços da luz, gás e combustíveis (/articles/61612596-fdd9-4040-abb1-9079f3c94506)
OBSERVADOR (/PROFILES/PUBLISHERS/EC919192-B113-4AC6-971F-32A343EDCD44) •
ONLINE (HTTPS://OBSERVADOR.PT/2022/02/27/GOVERNO-PREPARA-MEDIDAS-PARA-ATENUAR-SUBIDA-DOS-PRECOS-DA-LUZ-GAS-E-COMBUSTIVEIS/) •
ANA SUSPIRO (/PROFILES/AUTHORS/20E734B8-D3A3-4B2D-B701-4920CFC288F5) • 27/02/2022 22:31 • 3 MIN

Energético PT (/articles/?themeId=1463)

Novo contrato de concessão dos CTT entra em vigor (/articles/9f6f0c0e-645a-4ce5-b44c-e92f92480d14)
OBSERVADOR (/PROFILES/PUBLISHERS/EC919192-B113-4AC6-971F-32A343EDCD44) •
ONLINE (HTTPS://OBSERVADOR.PT/2022/02/27/NOVO-CONTRATO-DE-CONCESSAO-DOS-CTT-ENTRA-EM-VIGOR/) • 27/02/2022 20:04 •
MENOS DE UM MINUTO

Telecomunicações PT (/articles/?themeId=1464)