"Não são pró-Palestina, são contra o Ocidente". Quem está por detrás da guerra silenciosa contra Israel na dark web?

cnnportugal.iol.pt/guerra/israel/nao-sao-pro-palestina-sao-contra-o-ocidente-quem-esta-por-detras-da-guerra-silenciosa-contra-israel-na-dark-web/20231026/653ab73dd34e65afa2f6e01b

João Guerreiro Rodrigues
Ontem às 20:35

Ainda não tinham sido contabilizadas as vítimas do ataque terrorista do Hamas e um tsunami de ciberataques contra todo o tipo de infraestruturas estatais israelitas estava em curso

Enquanto o confronto entre Israel e o Hamas se intensifica no terreno, uma guerra silenciosa desenvolve-se no submundo da internet que está a elevar o conflito a uma nova dimensão. Dezenas de grupos hackers, de vários países, lançam ciberataques contra infraestruturas e instituições críticas, com o objetivo de dar vantagem a um dos lados.

“Logo no dia 7 de outubro, vimos um conjunto maciço de ciberataques muito bem orientados. Foi um ataque muito bem coordenado e multidisciplinar. Foram ciberataques altamente disruptivos contra instituições do Estado, que deviam demonstrar segurança, estabilidade e solidez, mas foram abaixo”, explica à CNN Portugal Bruno Castro, CEO da empresa de cibersegurança VisionWare.

Nesse mesmo dia, a equipa da Visionware que monitoriza as movimentações destes grupos da *dark web*, detetou as comunicações dos Anonymous Sudan – um grupo com ligações ao Kremlin – que tentavam atingir o sistema Iron Dome, o sistema de defesa antiaéreo israelita, numa altura em que o Hamas lançava um bombardeamento maciço contra o país. Em simultâneo, o grupo tentou atacar várias aplicações de lançamento de alertas para a população civil israelita, com o propósito de causar o pânico.

“Estes ataques servem para criar o medo e o alarmismo”, reforça o especialista em cibersegurança.

O que se seguiu foi um verdadeiro tsunami de ciberataques contra todo o tipo de infraestruturas estatais israelitas. Passwords de membros do governo são divulgadas e os ministérios da Saúde e das Finanças israelitas, os serviços secretos, sites do governo, transportes públicos e meios de comunicação ficaram completamente inoperacionais depois de uma campanha de ataques DDoS (negação de serviço). Este tipo de ataque sobrecarrega a infraestrutura de um site com falsos pedidos de entrada, levando a que estes fiquem temporariamente inoperacionais.

O VisionWare Threat Intelligence Center (VTIC) identificou 20 grupos que declararam apoio a Israel e 77 grupos a mostrar apoio à causa palestiniana. Vários grupos de países muçulmanos com notoriedade na comunidade hacker mundial foram rápidos a juntar-se à causa palestiniana no ciberespaço, mas não só. Grupos do Irão, Paquistão, Bangladesh, Indonésia, Sudão, Marrocos, Malásia, mas também russos, atacaram centenas de alvos em Israel e nos seus aliados nos primeiros dias do conflito.

“Estes grupos não são pró-Hamas ou Palestina, são contra o Ocidente. Há várias geografias a funcionar, desde o Irão à Rússia ou a Liga Árabe, que se juntam para atacar instituições pró-Israel”, explica Bruno Castro.

Não foi preciso esperar muito para ver uma resposta de grupos pró-Israel. No dia seguinte, os hackers da Threatsec atacaram o principal fornecedor de internet palestiniano. Horas mais tarde, o grupo pro-Ucrânia Cyber Anarchy Squad e os Indian Cyber Force anunciaram o início de operações contra infraestruturas palestinianas em solidariedade a Israel. Mas estes ataques foram só um começo.

Mas um dos principais ataques veio de um grupo pró-iraniano conhecido por Haghjoyan. Apanhando a estrutura defensiva israelita despercebida, estes hackers conduziram duas operações separadas, que lhes permitiram infetar mais de duas mil israelitas com software malicioso, roubando mais de dois terabytes de informação sensível, bem como os passaportes de 120 cidadãos israelitas. As autoridades não sabem se o acesso aos dados já tinha sido obtido antes do ataque terrorista de 7 de outubro.

> Pro-Iranian hacker group, Haghjoyan, claims to have compromised over 2,000 devices, gaining access to 2 TB of data. This data allegedly includes IP addresses, file locations, usernames, zip codes, geographic locations, hardware IDs, screen sizes, time zones, operating systems,… pic.twitter.com/qXNrMgPflj
>
> — FalconFeeds.io (@FalconFeedsio) October 13, 2023

“A espionagem sempre foi utilizada. Ser capaz de roubar dados e informação privilegiada sem ser detetado é algo que ambos os lados estão a fazer”, afirma Bruno Castro.

Devido ao pânico e à incerteza sentida pela população israelita na manhã do dia 7 de outubro, a procura por aplicações de alerta que ofereçam alertas de segurança de forma regular disparou. Mas os piratas informáticos aproveitaram-se disso. O grupo Anonymous Sudane explorou uma vulnerabilidade na aplicação do sistema de alertas israelita, permitindo-os enviar alertas falsos para os seus utilizadores, incluindo a informação de que “uma bomba nuclear vai a caminho”.

“Ninguém estava à espera que houvesse tanta permeabilidade neste ataque direcionado a Israel, que é um país que tem a componente de segurança muito bem vincada. Ninguém esperava este sucesso por parte do Hamas, principalmente para nós que trabalhamos nesta

área da cibersegurança", admite Bruno Castro.

Uma investigação da equipa da Cloudforce One Threat Operations descobriu várias aplicações maliciosas que se tentavam fazer passar por sistemas de alerta legítimos. Estas aplicações permitiam roubar dados sensíveis dos utilizadores, desde a lista de contactos, às mensagens, chamadas e outros ficheiros.

Em 2022, com o estalar da guerra na Ucrânia, vimos uma explosão de grupos hacktivistas afiliados a Estados e essa parece ser uma tendência que veio para ficar. Pelo menos, segundo os especialistas, "a morfologia é a mesma". E a tendência é para aumentar. Segundo um relatório produzido pela empresa de cibersegurança Check Point Software o número de ciberataques semanais aumentou 8% a nível mundial. É o aumento mais significativo dos últimos anos.

"O hacktivismo começou a imitar de perto as batalhas no mundo real, como se viu no conflito russo-ucraniano e na guerra entre o Hamas e Israel.Embora a influência e o impacto dos ciberataques e do hacktivismo sejam menos proeminentes durante o auge do combate, os incidentes aumentaram à medida que os mundos digital e físico colidem", pode ler-se no documento.

Segundo este estudo, a natureza do hacktivismo também está a mudar. Se antigamente estes atos eram feitos por indivíduos ou grupos ideologicamente motivados, agora aparecem cada vez mais organizações coordenadas e, muitas vezes, patrocinadas por Estados. A somar ao aparecimento de tecnologias como a Inteligência Artificial que levaram a uma "democratização da pirataria informática", multiplicando o número de atores.

Muito desse poder é canalizado para a criação "de uma narrativa" que apoie a causa que cada um destes grupos defende. Para isso, estes grupos utilizam plataformas como o X ou o Telegram, para propagar informação, que muitas vezes pode ser falsa, sem qualquer controlo. No entanto, esta é uma prática recorrente em ambos os lados.

Depois do choque inicial, Israel parece ter recuperado alguma da capacidade defensiva e o número de ataques com sucesso aparenta ter diminuído de forma significativa. Para Bruno Castro, isto deve-se às elevadas capacidades israelitas e ao fim do fator surpresa, que incapacitou a reação de Telavive.

"Os ataques existem na mesma, são em escala, muito diversificados, mas a capacidade de reação é superior e o fator surpresa diminui. Vemos o mesmo número de ataques, mas com menos sucesso", refere Bruno Castro.

Temas: Guerra Israel Hamas Palestina Ciberataque