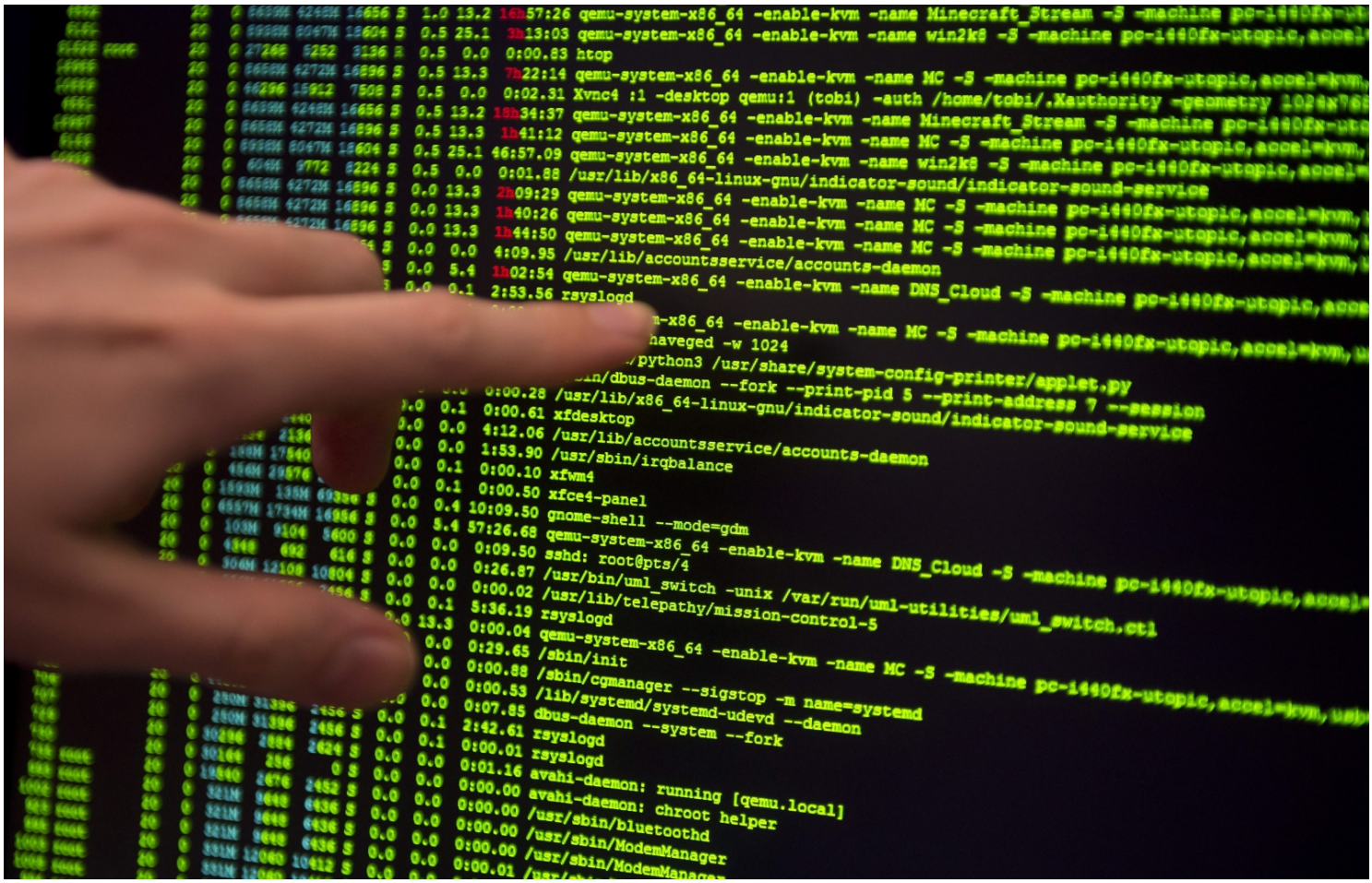
Guerra cibernética tem sofrido mutações visíveis no conflito com Rússia

visao.pt/atualidade/mundo/2024-02-22-guerra-cibernetica-tem-sofrido-mutacoes-visiveis-no-conflito-com-russia/



Lusa

A guerra cibernética tem sofrido mutações nas últimas semanas e os ataques intensos e indiscriminados do início da invasão russa da Ucrânia foram substituídos por uma estratégia focada em setores vitais nas sociedades dos dois países, indica um estudo

O estudo, elaborado pela VisionWare Threat Intellingence Center (VTIC), que a representação portuguesa da instituição disponibilizou à agência Lusa, indica que, apesar de uma redução no número de ataques, “estes são cada vez mais direcionados e disruptivos”.

“Os danos causados não afetam apenas o ciberespaço, mas causam também problemas em outros serviços. Os setores mais visados têm sido os da energia, das telecomunicações e as instituições financeiras”, disse à Lusa Bruno Castro, CEO da VisionWare e responsável pela área Strategic Intelligence.

“Além dos graves danos causados, os ataques visam frequentemente desferir golpes, afetando a confiança nestas instituições, e recolher informações pessoais e de localização”, acrescentou.

O relatório, dedicado à temática sobre “A Evolução da Ciberguerra no Conflito Rússia/Ucrânia”, sublinhou Bruno Castro, pretende dar a conhecer que a guerra cibernética tem vindo a sofrer “mutações visíveis nas últimas semanas”.

“Os ataques são cada vez mais disruptivos e demonstram a existência de um maior planeamento e estratégia por parte de ‘hackers’ [piratas informáticos] altamente profissionalizados e ultrapassam a negação de serviço a ‘websites’, havendo disrupção total de infraestruturas e afetando a credibilidade das instituições visadas”, frisou.

Bruno Castro adiantou que se verifica “tendencialmente” uma maior capacidade de resposta da Ucrânia na sua contraofensiva, em que os ataques de Kiev “têm um envolvimento direto das organizações de ‘Intelligence’ estatais”.

“O mesmo não se pode afirmar sobre os ataques russos. Apesar de não haver uma ligação clara entre os piratas informáticos e os serviços secretos russos, é visível um alinhamento ideológico dos principais grupos atuantes com os objetivos estratégicos de Moscovo. A dimensão dos danos causados à Rússia é de difícil análise, uma vez que a informação divulgada é fortemente censurada”, sublinhou.

Entre dezembro de 2023 até ao final de janeiro passado, referiu Bruno Castro, a Kyivstar, gigante das telecomunicações ucraniana, foi uma das empresas atacadas, tendo sido apagados “milhares de servidores virtuais e computadores”, deixando milhões de clientes sem acesso à internet e à rede telefónica, aparentemente “destruindo completamente” o núcleo do operador de telecomunicações.

A VTIC suspeita que o ataque tenha sido levado a cabo pela Sandworm, uma unidade de ciberguerra dos serviços secretos militares russos.

Em resposta, ‘hackers’ do grupo Blackjack, associados à Agência de Espionagem Ucraniana (SBU), “atacaram os sistemas informáticos de um fornecedor de internet russo, a M9 Telecom, que, na sequência do ataque, levou a que alguns residentes de Moscovo perdessem o acesso à internet”.

“Já este ano, a empresa energética ucraniana Naftogaz sofreu um ciberataque a uma das suas bases de dados. O ‘website’ da empresa e o seu ‘call center’ ficaram inoperativos. Adicionalmente, a agência de transporte responsável pela segurança nas travessias na fronteira ucraniana Ukrtransbezpeka, viu o seu ‘data center’ comprometido”, acrescenta-se no documento.

Segundo a VTIC, as instituições financeiras também têm sido fortemente visadas. A 19 de janeiro, o banco ‘online’ ucraniano Monobank sofreu um dos seus maiores ataques ‘DDoS’ de sempre, nas palavras do CEO, com 580 milhões de ‘services requests’ durante três dias, “deixando inativos alguns dos seus serviços”. O banco é frequentemente usado na recolha de donativos para o exército ucraniano nas redes sociais.

Além das empresas ligadas às telecomunicações, energia, banca, transportes e armazenamento de dados, realçou Bruno Castro, foram afetados pelos ataques cibernéticos vários serviços governamentais, públicos e postais, centros de investigação e as próprias forças armadas ucranianas.

Os ataques a instituições ucranianas, segundo o relatório da VTIC, foram perpetrados por uma coligação de diferentes grupos de ‘hackers’ russos, como o 22C, Skillnet, CyberDragon, Federal Legion, Peoples Cyber Army, Phoenix e NoName, bem como pelo Russian Cyber Army, havendo ainda outros cuja autoria é inconclusiva.

No sentido inverso, a contraofensiva ucraniana foi protagonizada por sobretudo pela diretoria principal da Inteligência ucraniana e por um grupo de ‘hackers’, como o Blackjack, que visaram serviços governamentais e públicos, telecomunicações, centros de investigação e ainda o exército russo.

JSD //