VisionWare detetou 961 ataques cibernéticos de 'piratas' pró-russos

noticiasaominuto.com/tech/2404311/visionware-detetou-961-ataques-ciberneticos-de-piratas-pro-russos

Lusa September 21, 2023

O VisionWare Threat Intelligence Centre (VTIC) detetou 961 ataques cibernéticos cometidos por piratas informáticos pró-russos a países e organizações ocidentais entre outubro de 2022 e março de 2023, indica hoje um relatório oficial enviado à agência Lusa.

21/09/23 12:26 · Há 53 mins por Lusa

Tech Hackers

Partilhar

Intitulado 'A Ação dos Grupos Cibernéticos Pró-Rússia Contra os Estados-Membros da NATO', o relatório é elaborado pela VTIC, um centro de operações e análise de ameaças cibernéticas que alerta as instituições públicas e privadas, a nível global, sobre os perigos da cibercriminalidade e da desinformação.

> O centro produz relatórios geopolíticos relacionados com as ameaças em estudo, monitoriza atores de risco, notifica em tempo real, sempre que dados das instituições ficarem comprometidos, elabora relatórios de análise e estudo perante as principais ameaças e atores, divididos por tempo e setor de risco.

A análise do relatório incide na atividade cibercriminosa levada a cabo pelos grupos 'KillNet' e 'NoName057(16)', tendo sido verificada pela VisionWare, uma empresa 100% portuguesa, fundada em 2005, especializada em segurança de informação, cibersegurança, tecnologias de informação e investigação forense, 'compliance', privacidade, formação e 'intelligence'.

Em declarações à Lusa, Bruno Castro, fundador e CEO da VisionWare, admitiu não haver confirmações de que o 'hacktivismo" pró-russo seja patrocinado pelo Estado, pelo que uma eventual participação do Kremlin "é pouco clara".

"Não há material que permita concluir que os grupos têm filiação ao Kremlin (ou ao GRU e FSB). No entanto, há uma estratégia ofensiva muito bem coordenada, de acordo com os interesses do governo russo", frisou.

Segundo o relatório, foram analisadas, no total, 8.347 mensagens na rede social Telegram: 6.805 referentes aos 'Killnet' e 1.542 referentes aos 'NoName057(16)'.

Durante o período analisado, o setor mais atacado pelos grupos em questão foram os ligados aos "Organismos Estatais, Banca e Defesa", com um total de 371 ataques. Janeiro de 2023 foi o mês com maior frequência de ataques, 333, o equivalente a aproximadamente 35% do total.

Portugal foi vítima de dois ataques providenciados pelos 'KillNet', que atingiram os portais da Direção Geral de Saúde (DGS) e da Faculdade de Farmácia.

Nos dois trimestres analisados, 41% dos ataques 'Killnet' foram nos Estados Unidos. Entre os países que mais foram alvo de ataques por parte dos 'NoName057(16)', destacam-se a Estónia, a Letónia e a Lituânia -- que sofreram 33,9% dos ataques efetuados por este grupo -- e a Polónia.

No período de tempo analisado, entre os dois grupos de 'hacktivistas', a Polónia, em particular, sofreu um total de 123 ataques e a União Europeia (UE) e a Organização do Tratado do Atlântico Norte (NATO) foram alvo de 17.

Questionado sobre o que se avizinha para os grupos de "hacktivismo" pró-russos, Bruno Castro disse prever que continuarão a reagir aos assuntos da atualidade, observando as relações da Rússia com países terceiros.

"Este estudo, baseado na análise pormenorizada dos fenómenos diários que monitorizamos destes grupos, sugere que os alvos irão para além da Ucrânia. Por exemplo, os 'KillNet' reivindicaram a responsabilidade por ataques DDoS em grande escala contra os principais aeroportos dos Estados Unidos em outubro de 2022. Estes ataques não afetaram os voos, mas perturbaram ou atrasaram os serviços aeroportuários", sustentou,

"Todos estes ataques DDoS dão prejuízos reputacionais e/ou financeiros, muitos deles, mais elevados do que calculamos. O relatório que apresentamos elucida para o desenvolvimento das capacidades, recursos e poder disruptivo destes grupos para atacar Estados e contribuir para a destabilização de sociedades", alertou Bruno Castro.

Sob o mote 'Challenging an Unsafe World', a VisionWare, credenciada pela NATO, visa contribuir para o sucesso dos seus clientes, em estreita relação de parceria, "num mundo que é marcado pelas constantes inovações tecnológicas", refere a VisionWare.

Os resultados do relatório, segundo a VisionWare, "ganham particular importância com o mais recente lançamento da Estratégia Cibernética do Departamento de Defesa de 2023 dos Estados Unidos, que se baseia na guerra entre a Rússia e a Ucrânia, sendo uma das prioridades globais da estratégia cibernética norte-americana.

Nesse sentido, refere a VisionWare, o crescente cenário de guerra cibernética entre atores estatais e não-estatais representa "um dos desafios mais complexos e urgentes enfrentados na era digital".

"Nesta nova forma de conflito, os atores utilizam habilidades cibernéticas para alcançar os seus objetivos políticos, estratégicos e ideológicos.

Os ataques cibernéticos lançados por atores estatais surgem de países com recursos significativos que podem realizar operações cibernéticas altamente sofisticadas, atacando infraestruturas críticas, sistemas de defesa e redes governamentais.

"Estes grupos, como 'hacktivistas', recorrem frequentemente a ataques DDoS, 'defacing' de 'websites', divulgação de informação e sabotagem digital para promover causas políticas e sociais", refere a empresa portuguesa, o mesmo sucedendo com os ataques cibernéticos não estatais.

No entanto, "a natureza descentralizada e muitas vezes anónima" dificulta a atribuição de responsabilidade pelas suas ações.

"A guerra cibernética não se limita a ataques entre países rivais, incluindo também ações de grupos 'hacktivistas', cibercriminosos e extremistas, que operam com diversas motivações e maioritariamente sem vínculos oficiais a governos", termina a VisionWare.