Hackers pró-Rússia reivindicam ciberataques contra websites do governo e família real de Espanha

tek.sapo.pt/noticias/internet/artigos/hackers-pro-russia-reivindicam-ciberataques-contra-websites-do-governo-e-familia-real-de-espanha

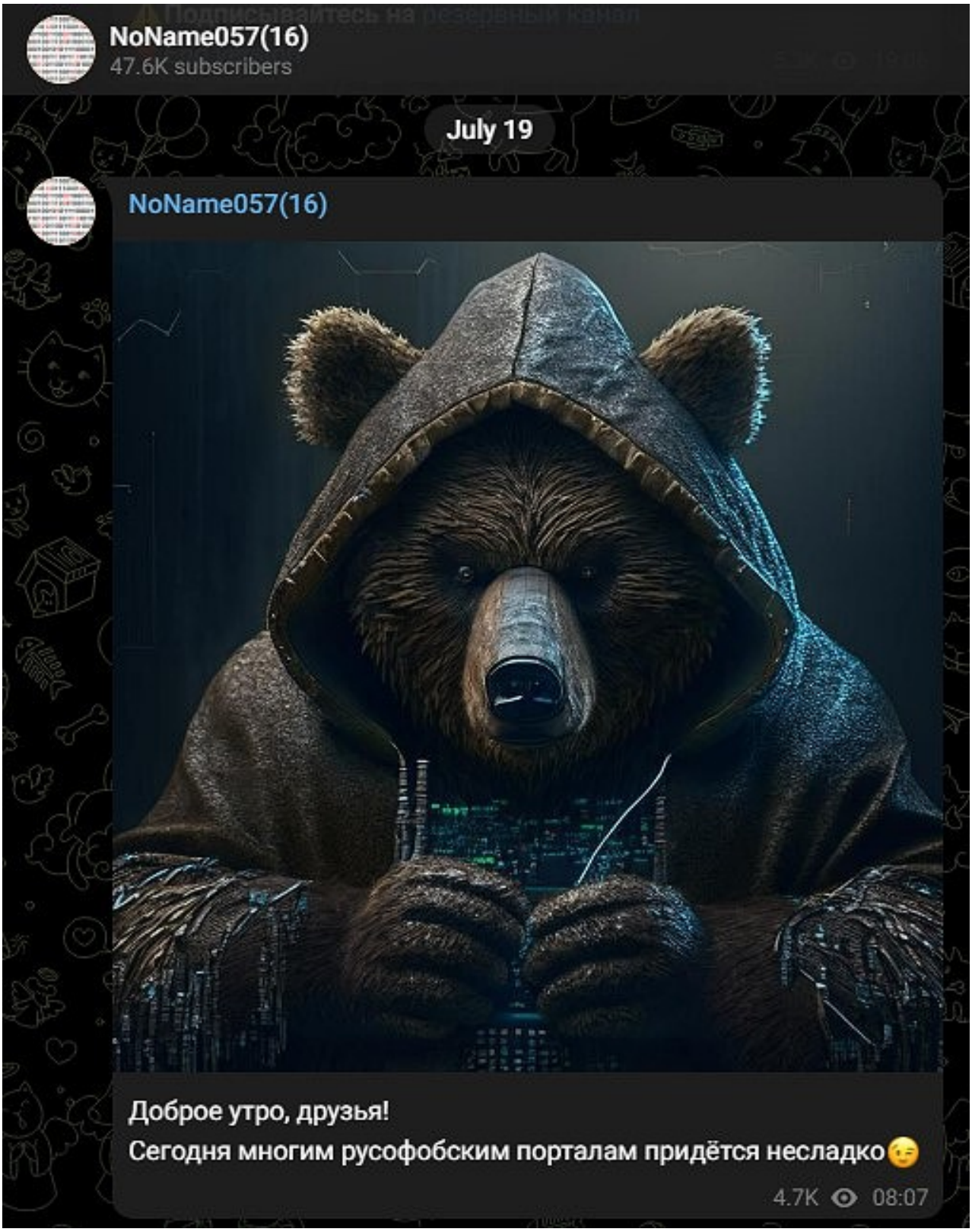
Francisca Andrade 19 de julho de 2023

Os websites do Primeiro-Ministro Espanhol e do Conselho de Ministros, assim como da família real espanhola, entre outras páginas web do país, **foram hoje alvo de ciberataques por parte de um grupo de hackers pró-Rússia, avançam os especialistas da VisionWare**.

Os hackers, do grupo pró-Rússia NoName057(16), reivindicaram os ataques DDoS através do seu canal no Telegram. De acordo com informação avançada pela empresa de cibersegurança portuguesa ao SAPO TEK, importa relembrar os acontecimentos que antecederam o ataque, **em particular a intenção declarada de Espanha em apoiar a Ucrânia no combate à Rússia**.

Clique nas imagens para ver com mais detalhe

Nas mensagens deixadas no seu canal de língua russa no Telegram, **os hackers começam por alertar que, hoje, vários portais online, que descrevem como "russofóbicos", teriam dificuldades**. Os piratas informáticos manifestam a sua oposição às mais recentes decisões do Governo espanhol de apoio à Ucrânia no contexto da guerra contra a Rússia, listando todos os websites espanhóis que afetaram.



Tradução: "Bom dia, amigos! Hoje, muitos portais russofóbicos terão dificuldades"

Entre os websites afetados pelos ataques incluem-se também o website da ISDEF, uma empresa espanhola de consultadoria e engenharia que pertence ao Ministério da Defesa espanhol, **o Ministério da Justiça do país e o seu Tribunal Constitucional**.

Ao SAPO TEK, **Bruno Castro, Fundador e CEO da VisionWare e especialista em cibersegurança e análise forense**, afirma que é possível **"perceber que este ataque não foi por acaso e o timing corresponde a várias situações a ter em conta"**.

Como detalha, o recente envio de quatro tanques Leopard pela Espanha à Ucrânia é uma dessas situações. Além disso, a "Espanha, na sua atual presidência da UE desde o primeiro dia deste mês, coloca como prioridade a candidatura da Ucrânia à UE" e "foi anunciado, também no ínicio desde mês, por Pedro Sanchéz, um novo pacote de ajuda à Ucrânia de 55 milhões de euros".

> "Ora, assim, conseguimos entender que o ataque, para causar disrupção e com uma forte comunicação simbólica e ideológica, pretende não só visar as instituições espanholas pelo apoio à Ucrânia na guerra, mas também aproveitar a fragilidade política que o país vive, prestes a ter eleições legislativas", afirma Bruno Castro.

"Aproveitando este fator, podemos partir de uma análise mais complexa", indica o fundador e CEO da VisionWare. "**Este grupo tenta não só visar um país inimigo, como, de certo modo, passar o testemunho para a opinião pública que ninguém está salvo, muito menos este governo** (e suas ações - que foram os 'causadores' deste ataque)", realça, acrescentando que "num prisma mais conceptual, podemos afirmar que este ataque também visa a democracia espanhola".

Hackers pró-Rússia bloqueiam páginas digitais de portos nos Países Baixos

Ver artigo

Recorde-se que, ainda em junho, os hackers do grupo NoName057(16) reivindicaram ataques contra **os websites dos portos de Groningen, Amesterdão, Den Helder e Roterdão, nos Países Baixos,** que os deixaram incessíveis durante horas ou até mesmo dias.

A Guerra na Ucrânia deu origem a uma nova geração de hacktivistas, como realçado recentemente por um boletim do Observatório de Cibersegurança do CNCS. Estes grupos posicionam-se de um dos lados do conflito, no entanto, **existe alguma ambiguidade no que respeita ao tipo de organização e ao apoio que têm.**

Do lado dos hacktivistas pró-Rússia incluem-se grupos como **NoName057(16), Kilnet, XakNet Team, Anonymous Russia e Cyber Army of Russia**, de acordo com dados do CERT-EU. **O grupo Kilnet é considerado como um dos mais ativos**, tendo afetado entidades dos setores público e privado, incluindo organizações de saúde, como laboratórios farmacêuticos, hospitais e clínicas, através de ataques DDoS.

Nota de redação: A notícia foi atualizada com mais informação (Última atualização: 21h27)