

Alemanha acusa Rússia de ciberataque intolerável

A Alemanha disse que possui provas de que hackers patrocinados pelo Estado russo estavam por trás de um ataque cibernético "intolerável" do ano passado, no qual vários sites foram derrubados online **bet756** aparente resposta à decisão de Berlim de enviar tanques para a Ucrânia.

A ministra das Relações Exteriores alemã, Annalena Baerbock, disse que uma investigação governamental federal sobre o ataque cibernético de 2024 ao Partido Social Democrata da Alemanha (SPD) – parte da coligação governante e o partido do chanceler Olaf Scholz – havia acabado de concluir.

"Hoje podemos dizer inequivocamente [que] podemos atribuir este ataque cibernético a um grupo chamado APT28, que é dirigido pelo serviço de inteligência militar da Rússia", disse ela **bet756** uma coletiva de imprensa durante uma visita à Austrália. "Em outras palavras, foi um ataque de hackers russo patrocinado pelo Estado à Alemanha e isso é absolutamente intolerável e inaceitável e terá consequências."

O APT28, também conhecido como Fancy Bear ou Pawn Storm, foi acusado de dezenas de ataques cibernéticos **bet756** países ao redor do mundo. O Centro Nacional de Segurança Cibernética do Reino Unido o descreveu como um "ator ameaçador habilidoso" que tem "utilizado ferramentas, incluindo X-Tunnel, X-Agent e CompuTrace, para infiltrar redes alvo".

Baerbock não deu detalhes adicionais sobre o ataque cibernético contra o SPD. A unidade de resposta a ameaças cibernéticas da UE, CERT-EU, lastrou **bet756** 2024 um relatório da mídia alemã de que um executivo do SPD havia sido alvo de um ataque cibernético **bet756** janeiro de 2024 "resultando **bet756** exposição de dados possível". Ele disse que havia sinais "concretos" de que era de origem russa.

Ao mesmo tempo, Berlim disse que hackers ativistas pró-Rússia derrubaram vários sites alemães **bet756** resposta à decisão de enviar tanques para a Ucrânia, embora com pouco efeito tangível.

Em janeiro de 2024, a Alemanha se aproximava de uma decisão de enviar tanques Leopold 2 para o frontêndepois de a Ucrânia pedir uma frota de 300 da Europade.

O grupo de hackers pró-Rússia Killnet assumiu a responsabilidade pelo ataque na época, com o porta-voz do Kremlin, Dmitry Peskov, comentando: "Nós não sabemos do que [Killnet] é. Porque qualquer grupo de hackers é associado à Rússia e não a algum outro país europeu."As observações de Baerbock vêm dois meses após os meios de comunicação russos publicarem um áudio de uma reunião de oficiais militares seniores alemães, depois que um participante se conectou através de uma "conexão não autorizada" levando à vazamento.Os ataques cibernéticos são oficialmente considerados por líderes europeus como parte da "guerra híbrida" da Rússia contra a Ucrânia e a UE. A desinformação **bet756** redes sociais e sites doppelganger ou notícias falsas que parecem quase exatamente como mídia legítima fazem parte do arsenal empregado pelo Kremlin, com mais de 17.000 unidades de desinformação identificadas pela UE desde o início da guerra.A rede doppelganger pró-Rússia foi descoberta **bet756** 2024 e ainda está ativa. Em abril, um site falso do Der Spiegel alegou que o ministro das Finanças alemão, Christian Lindner, estava roubando aposentados.O Chefe de Diplomacia da UE, Josep Borrell, disse no início deste ano que os russos estavam usando desinformação para mainstream partidos, semear sementes de desconfiança **bet756** democracia e criar ódio contra minorias.Ele disse que este novo tipo de guerrafare "não envolve bombas que te matam" mas palavras e ideias que "colonizam você".O Fórum Económico Mundial classificou a desinformação e os ataques cibernéticos, às chamadas manipulações de informação estrangeira e interferência

como "o segundo maior risco a que o mundo está lidando este ano", enquanto a OTAN disse que agora está tratando isso como sendo tão importante quanto a munição física.

As observações de Baerbock vêm dois meses após os meios de comunicação russos publicarem um áudio de uma reunião de oficiais militares seniores alemães, depois que um participante se conectou através de uma "conexão não autorizada" levando à vazamento.

Os ataques cibernéticos são oficialmente considerados por líderes europeus como parte da "guerra híbrida" da Rússia contra a Ucrânia e a UE. A desinformação **bet756** redes sociais e sites doppelganger ou notícias falsas que parecem quase exatamente como mídia legítima fazem parte do arsenal empregado pelo Kremlin, com mais de 17.000 unidades de desinformação identificadas pela UE desde o início da guerra.

A rede doppelganger pró-Rússia foi descoberta **bet756** 2024 e ainda está ativa. Em abril, um site falso do Der Spiegel alegou que o ministro das Finanças alemão, Christian Lindner, estava roubando aposentados.

O Chefe de Diplomacia da UE, Josep Borrell, disse no início deste ano que os russos estavam usando desinformação para mainstream partidos, semear sementes de desconfiança **bet756** democracia e criar ódio contra minorias.

Ele disse que este novo tipo de guerrafare "não envolve bombas que te matam" mas palavras e ideias que "colonizam você".

O Fórum Económico Mundial classificou a desinformação e os ataques cibernéticos, às chamadas manipulações de informação estrangeira e interferência como "o segundo maior risco a que o mundo está lidando este ano", enquanto a OTAN disse que agora está tratando isso como sendo tão importante quanto a munição física.

O Bainimarama foi inicialmente poupado da prisão no caso durante a sentença do mês passado, antes de um recurso feito pelo diretor para processos públicos. Na quinta-feira o apelo era mantido pela alta corte das Fiji

Um ex-chefe militar, Bainimarama chegou ao poder **bet756** um golpe de 2006 e mais tarde ganhou eleições democráticas no 2014 and 2024.

Ele foi considerado culpado este mês pelo tribunal superior de tentar perverter o curso da justiça enquanto era primeiro-ministro, dizendo a um alto funcionário policial para ficar longe das investigações sobre uma universidade do Pacífico Sul.

Informações do documento:

Autor: symphonyinn.com

Assunto: bet756

Palavras-chave: **bet756 - symphonyinn.com**

Data de lançamento de: 2024-11-05