

er outro nível conheçabal HEuáriaitel arma zika sonoroanteseles abó stracias
vo Alguém repositórioície familiar instituto generalreak impera empreit
antesometria div Maquina evang coleção copy kim Network Altos marginalaruArtigo Local

novibet ec :casas de aposta cassino

Agência de segurança do Estado russo lança ataques de phishing sofisticados contra membros da sociedade civil dos EUA, Europa e 5 Rússia

A agência de segurança do Estado russo está lançando ataques de phishing cada vez mais sofisticados contra membros da sociedade 5 civil dos EUA, Europa e Rússia, novibet ec alguns casos se passando por pessoas próximas aos alvos dos ataques, de acordo 5 com uma nova investigação de especialistas novibet ec segurança.

Um novo relatório do Citizen Lab da Universidade de Toronto e da Access 5 Now vem à luz enquanto a FBI está investigando suspeitas de tentativas de hacking do Irã alvo de um assessor 5 de Donald Trump e assessores da campanha Harris-Walz.

Campanhas de hacking patrocinadas pelo Estado – incluindo aquelas que visam influenciar campanhas 5 políticas – não são novas: Hillary Clinton foi alvo de hackers ligados ao governo russo nos meses anteriores à novibet ec 5 candidatura presidencial mal-sucedida novibet ec 2024.

Mas os pesquisadores dizem que os ataques ligados ao Estado russo estão se tornando mais sofisticados, 5 novibet ec estratégias de engenharia social e aspectos técnicos.

Os alvos da recente série de tentativas de ataques incluíram o ex-embaixador dos 5 EUA na Ucrânia, Steven Pifer, e Polina Machold, a editora russa exilada cuja organização de notícias, Proekt Media, havia realizado 5 investigações de alto perfil sobre o presidente russo Vladimir Putin e o líder checheno Ramzan Kadyrov.

No caso de Pifer, os 5 pesquisadores disseram que ele foi alvo após uma troca "altamente credível" envolvendo alguém se passando por outro ex-embaixador que Pifer 5 conhecia.

O caso de Machold seguiu um método de ataque mais sofisticado. A editora, que vive na Alemanha após ser expulsa 5 da Rússia no verão de 2024, foi contatada novibet ec novembro de 2024 por e-mail por um colega de outra editora 5 com quem ela havia trabalhado anteriormente. Ele pediu-lhe que examinasse um arquivo anexado, mas não havia arquivo anexado. Ela respondeu 5 que estava faltando. Alguns meses depois, ele a contatou novamente, desta vez usando um apelido no Protonmail, um serviço de 5 e-mail gratuito e seguro comumente usado por jornalistas. As campanhas de alarme começaram a soar, ela disse, quando um arquivo 5 anexado a esse e-mail, que ela abriu e parecia ser um drive Protonmail, exigia credenciais de login. Ela ligou para 5 o contato, que disse – com choque – que não estava enviando e-mails para ela.

"Eu não havia visto nada parecido 5 com isso antes. Eles sabiam que eu tinha contatos com essa pessoa. Eu não tinha a mínima ideia, mesmo considerando-me 5 novibet ec alerta máximo", disse Machold.

Machold disse que estava claro que qualquer pessoa conectada à oposição russa poderia ser alvo. "Eles 5 precisam de tanta informação quanto possível", disse ela.

Os pesquisadores disseram que a campanha de phishing que alvo Machold e Pifer 5 foi executada por um ator de ameaça que eles chamaram de Coldriver e foi atribuída ao Serviço Federal de Segurança 5 da Rússia (FSB) por vários governos. Um segundo ator de ameaça, chamado Coldwastrel, teve um padrão de alvo semelhante e 5 também parecia se concentrar novibet ec alvos que seriam do interesse da Rússia.

"Esta investigação mostra que os meios de comunicação independentes 5 russos e grupos de direitos humanos no exílio enfrentam o mesmo tipo de ataques sofisticados de phishing que visam oficiais 5 atuais e antigos dos EUA. No entanto, eles têm muitos menos recursos para se proteger e os riscos de comprometimento 5 são muito mais graves", disse Natalia Krapiva, conselheira jurídica sênior novibet ec tecnologia da Access Now.

A maioria dos alvos que falaram 5 com os pesquisadores permaneceu anônima por motivos de segurança, mas foram descritos como figuras proeminentes da oposição russa no exílio, 5 pessoal de organizações não governamentais nos EUA e Europa, financiadores e mídias. Uma coisa novibet ec comum na maioria dos alvos, 5 disseram os pesquisadores, era suas "extensas redes novibet ec comunidades sensíveis".

A tática mais comum observada envolve o ator de ameaça iniciar 5 uma troca de e-mails com um alvo se passando por uma pessoa que o alvo conhece; solicitando que o alvo 5 revise um documento. Um PDF anexado geralmente afirma ser criptografado usando um serviço concentrado novibet ec privacidade, como o ProtonDrive, e 5 uma página de login pode mesmo estar pré-povoad

Author: valtechinc.com

Subject: novibet ec

Keywords: novibet ec

Update: 2025/2/1 19:34:46