football studio real bet - symphonyinn.com

Autor: symphonyinn.com Palavras-chave: football studio real bet

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

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

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

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

Mas os pesquisadores dizem que os ataques ligados ao Estado russo estão se tornando mais sofisticados, **football studio real bet** estratégias de engenharia social e aspectos técnicos.

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

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

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

"Eu não havia visto nada parecido com isso antes. Eles sabiam que eu tinha contatos com essa pessoa. Eu não tinha a mínima ideia, mesmo considerando-me **football studio real bet** alerta máximo", disse Machold.

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

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

"Esta investigação mostra que os meios de comunicação independentes russos e grupos de direitos humanos no exílio enfrentam o mesmo tipo de ataques sofisticados de phishing que

visam oficiais atuais e antigos dos EUA. No entanto, eles têm muitos menos recursos para se proteger e os riscos de comprometimento são muito mais graves", disse Natalia Krapiva, conselheira jurídica sênior **football studio real bet** tecnologia da Access Now.

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

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

Estudantes de niversidade **football studio real bet** todo os EUA têm protestado desde 7 outubro 2024 com vigílias, manifestações e marcha pedindo um cessar-fogo na Gaza para suas universidades se alienarem da Israel. Enquanto alguns desses protestos levaram a lutas aquecida sobre política externa eventos mais proeminentes envolveram testemunho do Congresso Abismo dos presidentees universitários "Esta semana prisões Mais De 100 estudantes Columbia revigoraram o movimento estudantil E agora é chutando fora Em todos Os lugares!

Como sociólogo de movimentos sociais, estudo como os movimento selecionam e mudam táticas para obter uma resposta dos seus oponentes. Nas próximas semanas veremos dezenas das outras universidades surgirem porque ativistas encontraram a tática que chama atenção da administração **football studio real bet** um momento crítico: durante as finais do ano passado ou no início deste mês (ver mais).

Em 2011, fui organizadora do Occupy LA e acabei escrevendo minha dissertação sobre movimentos sociais distribuídos **football studio real bet** rede. A expansão da iniciativa foi auxiliada pelas mídias social, depois por uma tecnologia emergente popular entre os jovens; a invenção de um smartphone capaz para usar aplicativos ou transmitir {sp}s via streaming (streaming).

Informações do documento:
Autor: symphonyinn.com
Assunto: football studio real bet
Palavras-chave: **football studio real bet - symphonyinn.com**
Data de lançamento de: 2024-08-27