Táticas de trabalho remotas RPRC: Aproveitando plataformas de comparti

Data: 2025-08-29 08:29:18

Autor: Inteligência Against Invaders

Os trabalhadores de TI da RPDC alavancaram plataformas populares de compartilhamento de

código, como Github, Codesandbox e médio para cultivar portfólios de desenvolvedores

convincentes e posições remotas de terra sob identidades fabricadas.

Investigações revelam aproximadamente 50 ativas Github Os perfis operados por atores norte -coreanos, complementados por dezenas de perfis nos locais de nicho de freelancer e fórum.

Esses agentes empregam fotos de perfil DeepFake, currículos forjados hospedados em portais de vercel e freelancer e nacionalidades adotadas estrategicamente – predominantemente nós – para ignorar a verificação do empregador.

Essa rede é orquestrada pelo Departamento 53, canalizando US $ 250 milhões a US $ 600 milhões anualmente para os programas de armas da Coréia do Norte.

Os principais incidentes incluem o Operação Dream Job (2020), a violação de contratação do Knowbe4 (2024), o esquema agrícola de laptop de Christina Chapman (2019-2023) e o assalto de bybit (2025).

A cumplicidade da Rússia no recrutamento de trabalho de tecnologia da RPDC sob vistos de estudantes ressalta uma ameaça geopolítica ampliada

Com base em nossa análise anterior dos padrões de endereço de e-mail usados ??pelos trabalhadores norte-coreanos de TI, este artigo investiga sua atividade nas plataformas de compartilhamento de código e no ecossistema mais amplo de trabalho remoto.

Ao examinar os repositórios do GitHub, arremessos freelancers e retomar os artefatos, expomos as táticas sofisticadas que esses atores usam para se infiltrar nos mercados globais e financiar o regime da RPDC.

Github e perfis de compartilhamento de código

Investigadores identificado aproximadamente 50 contas ativas do github – como alchemist0803Assim, SkyCaptainesse branchdev98– Exibir alta frequência de comprometimento e diversidade de projetos.

Durante a investigação, houve 12 currículos encontrados. Da lista de currículos, eu rapidamente reduzi seu local adotado com títulos de emprego.

Sete perfis adicionais foram desativados, sugerindo rotação periódica de identidade. Além do GitHub, os agentes da RPDC mantêm presenças no Código e caixa, médio, remotehub, crowdworks e fóruns especializados para o WebRTC, AWSDocker, React.js e outras tecnologias sob demanda.

Os arremessos freelancers da amostra enfatizam a eficiência de custos, a entrega rápida e as habilidades de nicho, enquanto as consultas públicas em repositórios de código aberto servem como cobertura para o envolvimento da comunidade e a demonstração de habilidades.

Doze currículos fraudulentos foram descobertos nos locais Laborx, FlowCV e Pessoal. As nacionalidades alegadas incluem os EUA, Canadá, Japão, Polônia, Colômbia, Sérvia e Cazaquistão, com títulos de emprego que variam de desenvolvedor de blockchain ao arquiteto da IA.

Um perfil hospedado em Vercel usou um tiro na cabeça do DeepFake, verificado por ferramentas de detecção baseadas em IA, demonstrando a disposição dos agentes de empregar mídias sintéticas para evitar as verificações de identidade visual.

Incidentes de segurança e geração de receita

Esses trabalhadores clandestinos de TI são gerenciados pelo Departamento 53 sob o Ministério da Defesa Nacional da RPDC, gerando cerca de US $ 250 milhões a US $ 600 milhões por ano. Incidentes -chave:

Incidente	Linha do tempo	Detalhes	Impacto
Operação Job Dream	Agosto de 2020	Ofertas de emprego falsas do grupo Lazarus, entregando malware	Espionagem em mais de 12 países
Knowbe4 contratando	Jul 2024	Currículo sofisticado de AI-aprimorado levou à contratação incorreta	Lacunas de verificação expostas em empresas de segurança
Fazenda de laptop Chapman	2019–2023	Laptops dos EUA hospedados e então enviados perto da fronteira da DPRC	US $ 17 milhões lavados para financiamento de mísseis
Assalto de bybit	Fevereiro de 2025	Lazarus Phishing por infraestrutura comprometida da AWS	US $ 1,4 bilhão a US $ 1,5 bilhão de criptografia roubada

Historicamente, dependente da Rússia desde 1948, a Coréia do Norte intensificou a colaboração de TI sob o disfarce de programas de visto de estudantes – circunviar as sanções da ONU.

Operações recentes de Kimsuky Grupos adequados O uso de infraestrutura russa e endereços de e-mail destacam um nexo cibernético russia-DPRK coordenado.

O apoio militar de longa data da China à Coréia do Norte complica ainda mais a atribuição, pois muitos agentes da RPDC roçam o tráfego por meio de proxies chineses para obscurecer Pyongyang.

A fusão da RPDC de plataformas de código aberto, tecnologia Deepfake e identidades de capa multinacional representa uma ameaça global persistente.

À medida que os processos de contratação remotos evoluem, as organizações devem aprimorar a verificação da identidade, implantar a análise de imagem orientada por IA e os padrões comportamentais de referência cruzada entre as plataformas. Somente uma resposta unificada e com experiência em tecnologia pode conter o fluxo de financiamento ilícito, alimentando os programas de armas da Coréia do Norte.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.