Hackers norte-coreanos exploram plataformas de ameaças da Intel para pl

Data: 2025-09-04 16:00:00

Autor: Inteligência Against Invaders

Um esforço coordenado de hackers alinhados à Coreia do Norte para explorar plataformas de

inteligência de ameaças cibernéticas (CTI) foi revelado por especialistas em segurança cibernética.

A investigação, descoberta pela SentinelLabs e pela empresa de inteligência da Internet Validin, vinculou a atividade ao Entrevista contagiosa cluster, uma campanha conhecida por atingir candidatos a emprego com iscas de recrutamento com malware.

Entre março e junho de 2025, o grupo teria tentado acessar o portal de inteligência de infraestrutura da Validin, registrando várias contas poucas horas após uma postagem no blog que detalhava a atividade vinculada ao Lazarus. Os hackers usaram endereços do Gmail anteriormente associados às suas operações, embora a Validin os tenha bloqueado rapidamente. Apesar disso, eles voltaram com novas contas, incluindo domínios registrados especificamente para o esforço.

Tentativas persistentes e adaptação

Os agentes da ameaça demonstraram persistência, criando contas repetidamente e tentando logins ao longo de vários meses. O SentinelLabs intencionalmente permitiu que uma conta permanecesse ativa para monitorar suas táticas. Os investigadores encontraram evidências de coordenação baseada em equipe, incluindo a suspeita de uso do Slack para compartilhar resultados de pesquisa em tempo real.

Em vez de fazer amplas mudanças na infraestrutura para evitar a descoberta, os hackers se concentraram na implantação de novos sistemas para substituir aqueles desativados pelos provedores de serviços. Essa estratégia permitiu que eles mantivessem um alto ritmo de envolvimento das vítimas, apesar da exposição.

Leia mais sobre as operações cibernéticas do Lazarus Group: Mais de 200 pacotes maliciosos de código aberto rastreados até a campanha Lazarus

Detecção de infraestrutura e falhas de OPSEC

Os pesquisadores observaram o grupo usando o Validin não apenas para rastrear sinais de detecção, mas também para explorar novas infraestruturas antes da compra. Pesquisas por domínios com temas de recrutamento, como perguntas sobre habilidades[.]com e avaliação de contratação[.]NET sugeriu esforços para evitar ativos sinalizados.

Ainda assim, vários erros de segurança operacional expuseram arquivos de log e estruturas de

diretório, oferecendo uma visão rara de seus fluxos de trabalho.

A investigação também revelou aplicativos ContagiousDrop – sistemas de entrega de malware incorporados em sites de recrutamento.

Esses aplicativos enviavam alertas por e-mail quando as vítimas executavam comandos maliciosos e registravam detalhes como nomes, números de telefone e endereços IP. Mais de 230 indivíduos, principalmente no setor de criptomoedas, foram afetados entre janeiro e março de 2025.

Objetivos da campanha e impacto mais amplo

De acordo com o SentinelLabs, a campanha Contagious Interview atende principalmente à necessidade de receita da Coreia do Norte, visando profissionais de criptomoedas em todo o mundo por meio de engenharia social.

Embora o grupo não tenha adotado medidas sistemáticas para proteger a infraestrutura, sua resiliência vem da rápida redistribuição e da aquisição contínua de vítimas.

“Dado o sucesso contínuo de suas campanhas no engajamento de alvos, pode ser mais pragmático e eficiente para os agentes de ameaças implantar uma nova infraestrutura em vez de manter os ativos existentes”, explicou o SentinelLabs.

O relatório enfatiza que a vigilância dos candidatos a emprego continua sendo essencial, especialmente no setor de criptomoedas. Os provedores de infraestrutura também desempenham um papel fundamental, pois as remoções rápidas interrompem significativamente essas operações.