Agente de Ameaça Expõe Acidentalmente Operações Alimentadas por IA -

Data: 2025-09-10 17:50:07

Autor: Inteligência Against Invaders

Um agente de ameaças revelou involuntariamente seus métodos e atividades diárias após instalar o software de segurança Huntress em sua própria máquina operacional.

O incidente incomum deu aos analistas uma visão interna notável de como os invasores usam inteligência artificial (IA), ferramentas de pesquisa e automação para refinar seus fluxos de trabalho.

Por dentro dos fluxos de trabalho do invasor

De acordo com Huntress, o ator descobriu a empresa por meio de um anúncio do Google enquanto procurava soluções de segurança.

Depois de iniciar uma avaliação gratuita e baixar o agente, suas atividades foram registradas em detalhes. Os investigadores conseguiram confirmar a identidade do adversário por meio de um nome de máquina e histórico de navegador previamente conhecidos, que mostraram um comportamento de segmentação ativo.

Ao longo de três meses, Huntress observou o ator testando várias ferramentas de segurança, adotando plataformas de automação de fluxo de trabalho, como Make.com, e pesquisando APIs do Telegram Bot para agilizar as operações.

Os dados também revelaram um interesse em geradores de texto e planilhas orientados por IA para criar mensagens de phishing e gerenciar informações roubadas.

[Leia mais sobre IA no crime cibernético: NCSC do Reino Unido apóia divulgação pública para ameaças de desvio de proteção de IA](#)

A inteligência coletada revelou vários comportamentos-chave:

- Uso do Censys para procurar servidores Evilginx ativos
- Pesquisa em serviços de proxy residencial como LunaProxy e Nstbrowser para disfarçar o

tráfego

-

Reconhecimento de instituições financeiras, fornecedores de software e empresas imobiliárias

-

Ampla dependência do Google Tradutor para preparação de mensagens de phishing

O ator também acessou fóruns da dark web, como o STYX Market, navegou em repositórios de malware e tentou aproveitar o ROADtools Token eXchange para ataques relacionados à identidade.

Lições para defensores cibernéticos

Os analistas da Huntress vincularam a infraestrutura do adversário, hospedada no provedor canadense VIRTUO, a pelo menos 2471 identidades comprometidas ao longo de duas semanas. Muitas tentativas foram interrompidas por detecções existentes, incluindo criação de regras de e-mail mal-intencionadas e defesas contra roubo de tokens.

“Este incidente nos deu informações detalhadas sobre as atividades diárias de um agente de ameaças”, explicaram os pesquisadores da Huntress.

“Desde as ferramentas nas quais eles estavam interessados, até as maneiras como conduziram pesquisas e abordaram diferentes aspectos dos ataques.”

O caso destaca como [Erros dos invasores](#) pode fornecer aos defensores uma visão rara da arte contraditória, oferecendo lições valiosas para melhorar as estratégias de resposta e a precisão da detecção.