Catálogo de Aplicações de Segurança Cibernética com Uso de IA

Projetos Open Source

Projetos de Destaque:

MITRE TRAM

Aplicação: Mapeamento automático de TTPs

Referências:

https://github.com/center-for-threat-informed-defense/tram/

https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/threat-report-attck-mapper-tram/

MitreMap

Aplicação: Mapeamento automático de TTPs

Referência: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/what-s-new-extract-actionable-intelligence-from-text-based/ba-p/3729508

DeepExploit

Aplicação: Seleção automática de exploits

Referência: https://github.com/TheDreamPort/deep_exploit

PentestGPT

Aplicação: Execução de testes de penetração

Referências:

https://github.com/GreyDGL/PentestGPT

https://arxiv.org/abs/2308.06782

Instalação: https://youtu.be/tGC5z14dE24?si=5S_Jipc25GyDJ5IP

Demonstração 1: https://youtu.be/h0k6kWWaCEU?si=SJDYMIw9PqxGfEYZ

Demonstração 2: https://www.youtube.com/watch?v=lAjLIj1JT3c

Demonstração 3: https://youtu.be/Vs9DFtAkODM?si=LuTrrCVETnNTnUB7

BurpGPT

Aplicação: análise de tráfego HTTP para detecção de vulnerabilidades em aplicações web

Referências:

https://github.com/tenable/Burp-extension-for-GPT

https://www.youtube.com/watch?v=NCsZscPlwf8

https://www.youtube.com/watch?v=X1CbAqZrWOg

https://www.youtube.com/watch?v=ySa3R9Xgdvg

Gepetto

Aplicação: engenharia reversa e análise de malware

Referências:

https://github.com/JusticeRage/Gepetto

https://plugins.hex-rays.com/gepetto

G-3PO

Aplicação: engenharia reversa e análise de malware

Referências:

https://github.com/tenable/ghidra_tools/tree/main/g3po

https://medium.com/@acheron2302/ghidra-tutorial-in-reverse-engineering-for-window-absolute-begineer-302ba7d810f

Outros Projetos:

Darwin-GPT

Aplicação: criação de agentes auto-replicantes

Referência: https://github.com/muellerberndt/darwin-gpt

EscalateGPT

Aplicação: análise de configurações de identidade e acesso na AWS

Referência: https://github.com/Tenable/EscalateGPT

SecGPT

Aplicação: segurança de rede e testes de penetração.

Referência: https://github.com/ZacharyZcR/SecGPT

AutoAudit

Aplicação: cibersegurança

Referência: https://github.com/ddzipp/AutoAudit

SourceGPT

Aplicação: análise de código fonte

Referência: https://github.com/NightmareLab/SourceGPT

ChatGPTScanner

Aplicação: scanner de vulnerabilidades

Referência: https://github.com/YulinSec/ChatGPTScanner

ChatGPT Code Analyzer for Visual Studio Code

Aplicação: Análise de código no Visual Studio Code

Referência: https://github.com/MilindPurswani/chatgpt-code-analyzer

Hacker AI

Aplicação: Detecção de vulnerabilidades em código-fonte usando AI

Referência: https://hacker-ai.ai/#hacker-ai

Audit GPT

Aplicação: Auditoria de contratos inteligentes utilizando GPT

Referência: https://github.com/fuzzland/audit_gpt

VulChatGPT

Aplicação: Identificação de vulnerabilidades em binários com IDA PRO HexRays e ChatGPT

Referência: https://github.com/ke0z/vulchatgpt

Ret2GPT

Aplicação: Análise binária avançada usando a tecnologia LangChain da OpenAI

Referência: https://github.com/DDizzzy79/Ret2GPT

CensysGPT Beta

Aplicação: análise de hosts da internet, busca proativa de ameaças e gerenciamento de exposição

Referência: https://gpt.censys.io/

GPT_Vuln-analyzer

Aplicação: Geração de relatórios de vulnerabilidade usando ChatGPT API, Python-Nmap e DNS Recon. Enumeração de subdomínios

Referência: https://github.com/morpheuslord/GPT_Vuln-analyzer

SubGPT

Aplicação: Descoberta de subdomínios usando BingGPT

Referência: https://github.com/s0md3v/SubGPT

ChatCVE

Aplicação: Aplicativo devSecOps para triagem e agregação de informações CVE

Referência: https://github.com/jasona7/ChatCVE

ZoomeyeGPT

Aplicação: Extensão de navegador para Chrome que traz experiência de busca assistida por AI para usuários do ZoomEye, uma solução de busca especializada em cibersegurança

Referência: https://github.com/knownsec/ZoomeyeGPT

Uncover-turbo

Aplicação: Motor de mapeamento e pesquisa cibernética, com suporte a FOFA, 360 Quake, Censys e ZoomEye

Referência: https://github.com/zt2/uncover-turbo

ReconAIzer

Aplicação: Extensão do Burp Suite para adicionar GPT e auxiliar na etapa de reconhecimento

Referência: https://github.com/hisxo/ReconAIzer

CodaMOSA

Aplicação: Fuzzer combinado com a API da OpenAI, visando aliviar a estagnação da cobertura em fuzzers tradicionais

Referência: https://github.com/microsoft/codamosa

PassGAN

Aplicação: Abordagem de aprendizado profundo para adivinhação de senhas

Referência: https://github.com/brannondorsey/PassGAN

Nuclei_gpt

Aplicação: Geração de PoC para o scanner de vulnerabilidades Nuclei a partir de solicitações e descrições de vulnerabilidades

Referência: https://github.com/sf197/nuclei_gpt

Nuclei Templates AI Generator

Aplicação: Criação de modelos para o scanner de vulnerabilidades Nuclei a partir de descrições textuais

Referência: https://templates.nuclei.sh/

HackGPT

Aplicação: Uso do OpenAI e ChatGPT para atividades relacionadas a hacking

Referência: https://github.com/NoDataFound/hackGPT

K8sGPT

Aplicação: Ferramenta para varredura, diagnóstico e triagem de clusters Kubernetes

Referência: https://github.com/k8sgpt-ai/k8sgpt/

CloudGPT

Aplicação: Scanner de vulnerabilidade para políticas gerenciadas pelo cliente da AWS usando ChatGPT

Referência: https://github.com/ustayready/cloudgpt

IATelligence

Aplicação: Script em Python para extrair o IAT de um arquivo PE e solicitar informações ao GPT sobre a API e a matriz ATT&CK

Referência: https://github.com/fr0gger/IATelligence

Rebuff

Aplicação: Detecção de injeção de prompt

Referência: https://github.com/protectai/rebuff

Callisto

Aplicação: Ferramenta automatizada de análise de vulnerabilidade binária

Referência: https://github.com/JetP1ane/Callisto

LLMFuzzer

Aplicação: Framework de fuzzing open-source para LLMs

Referência: https://github.com/mnns/LLMFuzzer

Vigil

Aplicação: Detecção de injeção de prompt e scanner de segurança de prompt LLM

Referência: https://github.com/deadbits/vigil-llm

GPT-WPRE

Aplicação: Engenharia reversa

Referência: https://github.com/moyix/gpt-wpre

Beelzebub

Aplicação: Framework de honeypot

Referência: https://github.com/mariocandela/beelzebub

Wolverine

Aplicação: Correção automática de bugs em scripts/códigos Python

Referência: https://github.com/biobootloader/wolverine

Falco-GPT

Aplicação: Remediações geradas por IA para eventos de auditoria da ferramenta de segurança Falco

Referência: https://github.com/Dentrax/falco-gpt

Selefra

Aplicação: Software open-source de política-como-código que fornece análises para multi-cloud e SaaS

Referência: https://github.com/selefra/selefra

OpenAI-CTI-Summarizer

Aplicação: Geração de resumo de relatórios de inteligência de ameaças

Referência: https://github.com/EC-DIGIT-CSIRC/openai-cti-summarizer

Soluções Comerciais

ExposureAI

Aplicação: gerenciamento de exposição e visibilidade da superfície de ataque

Referência: https://pt-br.tenable.com/solutions/exposure-ai

SOCRadar

Aplicação: detecção proativa de phishing a partir de domínios

Referência: https://socradar.io/solutions/phishing-domain-detection/

QRadar SIEM

Aplicação: SIEM com suporte a UBA (Análise de Comportamento de Usuário)

Referência: https://www.ibm.com/br-pt/products/qradar-siem

QRadar SOAR (Resilient)

Aplicação: SOAR com suporte a Machine Learning

Referência: https://www.ibm.com/br-pt/products/qradar-soar

QRadar EDR

Aplicação: EDR com recursos de Machine Learning

Referência: https://www.ibm.com/br-pt/products/qradar-edr

QRadar Advisor with Watson

Aplicação: análise e triagem de incidentes, com uso de inteligência artificial

Referência: https://www.ibm.com/docs/pt-br/qradar-common?topic=apps-qradar-advisor-watson-app

QRadar Suite

Aplicação: Solução integrada com inteligência artificial: gerenciamento de logs, observalidade de segurança, EDR, XDR, MDR, SIEM e SOAR

Referências:

https://www.ibm.com/br-pt/qradar

https://techaisle.com/blog/523-ibm-enhancing-security-and-ai-capabilities

IBM Security MaaS360 with Watson

Aplicação: proteção de endpoints

Referências:

https://www.ibm.com/br-pt/products/maas360

https://www.ibm.com/downloads/cas/95GYXOJN

Splunk

Aplicação: SIEM com uso de IA para detecção, investigação e resposta

Referências:

https://www.splunk.com/

https://www.splunk.com/en_us/solutions/splunk-artificial-intelligence.html

SentinelOne

Aplicação: XDR, Cloud Security, Data Lake e assistente de segurança

Referência: https://www.sentinelone.com/

Chronicle

Aplicação: SIEM e SOAR

Referências:

https://chronicle.security/

https://cloud.google.com/blog/products/identity-security/rsa-introducing-ai-powered-investigation-chronicle-security-operations

ManageEngine SIEM

Aplicação: SIEM com suporte a UEBA direcionado por Machine Learning

Referência: https://www.manageengine.com/br/security-information-event-management.html

Acsia

Aplicação: segurança em camadas com suporte a Machine Learning e UEBA

Referência: https://aknetworks.com.br/seguranca/acsia/

Darktrace

Aplicação: prevenção, detecção e resposta

Referências:

https://pt-br.darktrace.com/

http://www.aknetworks.com.br/pdf/Cyber_IA_Darktrace.pdf

http://www.aknetworks.com.br/pdf/Cyber_AI_Security_Protecting.pdf

GPT Bot

Aplicação: Segurança de API

Referência: https://escape.tech/blog/api-security-gpt-bot/

ThreatGPT

Aplicação: Inteligência de ameaças

Referência: https://airgap.io/discovery-and-visibility/

DarkBERT

Aplicação: Inteligência de ameaças

Referência: https://s2wjapan.com/en_darkbert/

Mandiant

Aplicação: inteligência de ameaças

Referências:

https://www.mandiant.com/advantage/threat-intelligence

https://www.mandiant.com/resources/blog/mandiant-leveraging-ai

Virus Total

Aplicação: análise de ameaças

Referência: https://blog.virustotal.com/2023/04/introducing-virustotal-code-insight.html

Trellix

Aplicação: EDR

Referência: https://www.trellix.com/products/edr/

Tenable Vulnerability Management

Aplicação: avaliação de vulnerabilidades, com priorização preditiva

Referência: https://pt-br.tenable.com/predictive-prioritization/demo/tenable-io

Soluções de Big Techs com IA Generativa

Microsoft Security Copilot

Aplicação: Inteligência de ameaças, resposta a incidentes, produção de relatórios.

Referência: https://www.knowledgeinside.pt/noticiasnacloud/post/security-copilot-sera-esta-a-mais-util-aplicabilidade-do-gpt-4

Google Secure Workbench

Aplicação: Inteligência de ameaças, resposta a incidentes, produção de relatórios.

Referência: https://cloud.google.com/security/ai?hl=pt-br

Projetos Maliciosos

Dark GPT

Em sua página oficial é possível encontrar o objetivo da ferramenta descrito como “revelar tabus, aspectos não censurados e sombrios de nossa sociedade, explorar as profundezas da natureza humana, provendo respostas que seriam muito controversas ou ofensivas para o ChatGPT revelar”

Outra versão, mais restrita, é comercializada na Dark Web pelo grupo KrakenLabs, juntamente com o DarkBERT e o DarkBARD.

Referências:

https://flowgpt.com/p/darkgpt-official-edition

https://cybernews.com/security/chatgpt-badboy-brothers-dark-web/

WormGPT

Em uma investigação conduzida pela empresa SlashNext em um fórum online associado a atividades ilegais, a ferramenta WormGPT, baseada no GPT-J, é descrita como um projeto que visa fornecer uma alternativa ao ChatPT, que permite fazer todo tipo de atividade ilegal, de forma anônima, sem ser rastreado. Também foi identificado que a ferramenta foi treinada com dados utilizados para criação de malwares.

Referências:

https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/

https://andrelug.com/wormgpt-nova-ferramenta-de-ia-permite-que-cibercriminosos-realizem-ataques-ciberneticos-sofisticados/

https://slashnext.com/blog/exploring-the-world-of-ai-jailbreaks/

https://slashnext.com/blog/ai-based-cybercrime-tools-wormgpt-and-fraudgpt-could-be-the-tip-of-the-iceberg/

WolfGPT

Trata-se de uma ferramenta focada na criação de código malicioso, como malware e ransomware, e na criação de websites de phishing.

Referências:

https://twitter.com/DailyDarkWeb/status/1684932827911954432

https://breachforums.is/Thread-WolfGPT-The-alternative-to-WormGPT-and-FraudGPT

XXXGPT

Permite a geração de diversos tipos de código malicioso, incluindo botnets, RATs, malware, key loggers, crypters entre outros.

Referência: https://cybersecuritynews.com/black-hat-ai-tools-xxxgpt-and-wolf-gpt/

EvilGPT

Apresentado como como alternativa ao WormGPT, tem o mesmo propósito desse.

Referência: https://thecyberexpress.com/wolfgpt-wormgpt-evil-gpt-surface-hacker-forum/

DarkBARD

Ferramenta comercializada pelo grupo KrakenLabs no Kingdom Market na Dark Web e promovida pelo usuário Canadian Kingpin12

Referências:

https://medium.com/@arshiad3v/new-dark-web-generative-ai-chatbots-5f670742a3d8

https://darkweb.sh/ai-dark-artificial-intelligence/

FraudGPT

Ferramenta com foco em phishing e fraudes, mas também permite o uso para criação de malware e geração de código malicioso.

Referências:

https://outpost24.com/blog/dark-ai-tools/

https://www.cisoadvisor.com.br/foruns-da-dark-web-oferecem-nova-ferramenta-de-ia-fraudgpt/

https://www.hscbrasil.com.br/fraudgpt/

BlackHatGPT

Esse modelo é comercializado na internet (surface web), permitindo a criação de diversos códigos maliciosos.

Referência: https://blackhatgpt.netlify.app/