

LLM Warning List

Overview of Malicious and Misused AI Models

Tool	Access/Distribution	Indentifiers
WormGPT Python-based BEC & phishing tool	Discord, Telegram, forums	None
FraudGPT Creates fake IDs, documents, malware	Subscription model	https://fraudgpt.org/
Mixtral Multi-model "Mixture of Experts" LLM	Download, Library Import, Open Source	• https://mistral.ai/ • 20.240.160.161/32 • 20.240.160.1/32 • 20.240.194.83/32 • 51.12.243.114/32
Grok Twitter (X) AI, can be misused	Subscription model	https://grok.com/
DarkBERT Dark Web-trained threat tool	Subscription model	None
Anthropic Claude Business automation & coding	Subscription model	• 160.79.104.0/23 • 34.162.46.92 • 34.162.102.82 • 34.162.136.91 • 34.162.142.92 • 34.162.183.95 • 2607:6bc0::/48
Deepchat (WhiteRabbitNeo) Uncensored exploit/malware tool	Open source, subscription	• https://deepai.org/ • https://deepchat.dev/ • https://github.com/OvidijusParsiunas/deep-chat • https://www.npmjs.com/package/deep-chat
GhostGPT Jailbroken GPT-3.5/DALLE	Dark Web, Telegram, subscription	• ./gst.sh • https://github.com/Deemocean/GhostGPT.git
DarkBARD Bard clone (possible scam)	Dark Web subscription	None
Poison GPT Data poisoning proof-of-concept	Unavailable	None

URL and IP Blocking is Only Marginally Effective Against LLM Threats

Many of the "dark" LLM tools available to Threat Actors continually change IP addresses, servers, and other identifying items. With this in mind, a defense-in-depth approach is more useful.

Additional Recommendations

- Staff Cybersecurity Training that includes the ethics and dangers of AI use
- Consider including AI-powered threat detection as a criterion for hardware and software upgrades
- Create policy that governs the adoption and use of AI technologies including LLMs
- AI-powered threat detection



NH Municipal Cyber Defense Program

The New Hampshire Municipal Cyber Defense Program (MCDP), managed by The ATOM Group, is a key initiative for enhancing New Hampshire's Cybersecurity Defense Services. Funded by the NH Department of Information Technology and the State and Local Cybersecurity Grant Program, it aims to protect public trust in technology by providing comprehensive Cybersecurity training.

The MCDP is critical to New Hampshire as it enhances cybersecurity readiness across municipal and public sector entities. This program stands out because it is customized based on the municipality's type, job description, and organization's existing cybersecurity readiness.

For more information, please contact:

Emily McGovern

Cyber Operations Specialist

NH Municipal Cyber Defense Program (MCDP)

Email:

emily@theatomgroup.com

Phone:

603.501.0003 x107

Website:

theatomgroup.com/mcdp

A+OM

