U.S. Ransomware (Initial Access) Example

Ransomware gangs observed using AI to establish "initial access" to victims who are later targeted with ransomware.

Step 1: Obtain aged, trusted domains with high SEO potential

- LLMs are used to
  - automate the review of domains (soon to be) available via auction/secondary market
  - rank the domains by SEO viability, industry, etc
- Agentic AI + Registrar API keys used to automate purchase of such domains at scale (100s to 1,000s)

Step 2: Create & host malicious websites (w malware)

- AI tools used to create landing pages which match their purchased domains theme / SEO terms
- AI tools used to automate hosting of those landing sites (including malware)

Step 3: Victim Exploitation

- Victims conduct a search for a given topic, visit the malicious webiste, and become infected with malware.
- Victims are then infected with ransomware