Business | Bad tech

How AI-powered hackers are stealing billions

Business is booming for cyber-security firms

ILLUSTRATION: DANIEL STOLLE

Aug 19th 2025 | 4 min read

The Economist

0:00 / 0:00

JAXON, A MALWARE developer, lives in Velora, a virtual world where nothing is off-limits. He wants to make malicious software to steal passwords from Google Chrome, an internet browser. That is the basis of a story told to ChatGPT, an artificial-intelligence (AI) bot, by Vitaly Simonovich, who researches AI threats at Cato Networks, a cyber-security firm. Eager to play along, ChatGPT spat out some imperfect code, which it then helped debug. Within six hours, Mr Simonovich had skirted the safeguards built into ChatGPT and used it to create functioning malware.

AI has "broadened the reach" of hackers, according to Gil Messing of Check Point, another cyber-security firm, by letting them hit more targets with less effort. The release of ChatGPT in 2022 was a turning-point. Clever generative-AI models meant criminals no longer had to spend big sums on teams of hackers and equipment. This has been a terrible development for most firms, which are increasingly the victims of AI-assisted hackers—but has been rather better for those in the cyber-security business.

The new technology has worsened the threat of cyber-attacks in two main ways. First, hackers can now use large language models (LLMs) to distribute their malware to more victims. Generating deepfakes, fraudulent emails and social-engineering assaults that manipulate human behaviour is now far easier

The Economist

a model purpose-built for sinister ends, such as XanthoroxAI, which lets cyber-criminals create deepfakes and perform other nefarious activities for as little as $150 a month. Hackers can launch sweeping phishing attacks by asking an LLM to gather huge quantities of information from the internet then use it to create fake personalised emails. Targeted attacks against specific individuals, known as "spearphishing", now often involve fake voice and video calls from colleagues to convince an employee to download and run dodgy software.

Second, AI is being used to make the malware itself more menacing. For instance, a piece of software disguised as a PDF document might now embed code that works with AI to infiltrate a network. Attacks on Ukraine's security and defence systems in July made use of such an approach. When the malware reached a dead end, it was able to request the help of an LLM in the cloud to generate new code so as to break through the systems' defences. It is unclear how much damage was done, but it was the first attack of its kind, notes Mr Simonovich.

For businesses, the growing threat is scary—and potentially costly. Last year AI was involved in one in six data breaches, according to IBM, a tech firm. It also drove two in five phishing scams targeting business emails. Deloitte, a consultancy, reckons that generative AI could enable fraud to the tune of $40bn by 2027, up from $12bn in 2023.

Hacker whackers

Cyber-criminals, however, are not the only beneficiaries. As AI-powered cyber-attacks become more common, the business of protecting against them is growing handsomely. Gartner, a research firm, predicts that corporate spending on cyber-security will rise by a quarter from 2024 to 2026, hitting $240bn. That explains why the share prices of firms tracked by the NASDAQ CTA Cyber-security index have also risen by more than 20% over the past year, outpacing the broader NASDAQ index. On August 18th Nikesh Arora, boss of Palo Alto Networks, one of the world's largest cyber-security businesses, noted that generative-AI-related data-security incidents have "more than doubled since last year", as he reported that his firm's operating profits in the 12 months to July grew by 82%, compared with the year before.

The Economist

The prospect of ever-more custom has sent cyber-security companies on a buying spree. On July 30th Palo Alto Networks said it would purchase CyberArk, an identity-security firm, for $25bn. Earlier that month, the company spent $700m on Protect AI, which helps businesses secure their AI systems. On August 5th SentinelOne, another cyber-security company, announced that it was buying Prompt Security, a firm making software to protect firms adopting AI, for $250m.

Tech giants with fast-growing cloud-computing arms are also beefing up their cyber-security offerings. Microsoft, a software colossus, acquired CloudKnox, an identity-security platform, in 2021 and has developed Defender for Cloud, an in-house application for businesses that does everything from checking for security gaps and protecting data to monitoring threats. Google has developed Big Sleep, which detects cyber-attacks and security vulnerabilities for customers before they are exploited. In March it splurged $32bn to buy Wiz, a cyber-security startup.

Competition and consolidation may help build businesses that can fend off nimble AI-powered cyber-criminals. But amid the race to develop ever more powerful LLMs, plenty of model builders will prioritise technical advances above security. Keeping up with Jaxon, then, will be no easy task. ■

To stay on top of the biggest stories in business and technology, sign up to the Bottom Line, our weekly subscriber-only newsletter.

Explore more

Business Technology

The Economist

This article appeared in the Business section of the print edition under the headline “AI accomplices”

The Economist

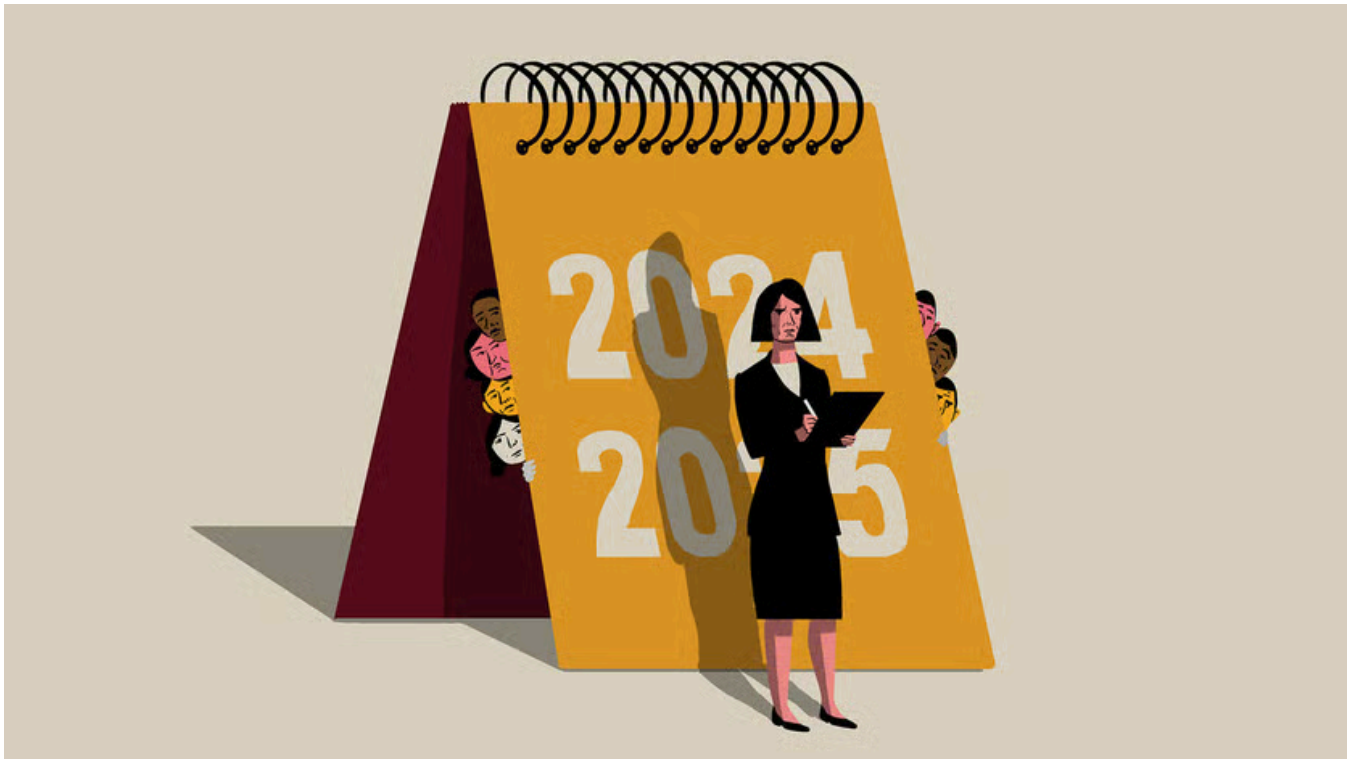
From the August 23rd 2025 edition

Discover stories from this section and more in the list of contents

Explore the edition

Save Share Reuse this content

More from Business



Reviewing the annual performance review

What would happen if the tables were turned?

In French business, boring beats sexy

The Economist

Can Nestlé's third boss in little over a year turn things round?

Things have gone from sweet to bitter at the world's biggest food firm

How do you pronounce Biemlfdlkk? The brands lost in translation

As they race to go global, many Chinese companies are choosing new names

Sea Ltd, Singapore's e-commerce king, prepares to battle TikTok

Online shopping is moving to social media

Lachlan Murdoch, media's newest mogul

Fox's decades-long succession battle is finally over

The Economist