CYBER THOUGHTS

Crossing the Streams: Getting Hacked by ChatGPT

February 2023

CYBER THOUGHTS

AI Buzz. If we had to sum up February technology news in two words they would be: Generative AI. It seems that all anyone wants to talk about is ChatGPT, or its competitors, and Large Language Models (LLMs). Frankly, we are good with that given our focus, but it can be difficult to separate the real news from the hype, so we are here to help you. Also, we are on the road talking with people about AI. See our announcement here for more info.

With OpenAI and Microsoft generating headlines and buzz around the industry it was only a matter of time before other tech giants started to try to get in on the action. We've seen announcements from all of the usual suspects: Amazon, Google, and Meta. The notable exception at this point is Apple, but their career's site has it's own landing page and 115 open roles, so they appear to be hard at work.

Given that we often talk about Cybersecurity and hacking, it's notable to us that people can now be hacked directly by Bing's ChatGPT interface. The article below has more details, but in its rush to integrate ChatGPT into Bing search Microsoft appears to have opened up a whole new way for users to have their data stolen. Anytime new technology is being adopted new threats become apparent, and LLMs are no exception. It wouldn't surprise us if this time next year there is a new Gartner Quadrant of security companies that protect LLMs.

At the World Economic Forum, the Managing Director, Jeremy Jurgens, revealed that: "93 percent of those surveyed believe that a "catastrophic" cyber security event is likely in the next two years." - Via Forbes. Cybercrime is still on the rise and is projected to top $10 Trillion in total cost across the world by 2025. This is against the backdrop of general cost-cutting for US corporations, and specifically in tech. While the CISOs we've spoken with are talking about doing "more with less" they have been the least affected groups at their firms with regard to budget cuts. For this reason, it's reasonable to determine that cybersecurity may be the best port in which to weather an economic downturn.

The early-stage venture funding environment continues to heat up, albeit off of a giant drop off in the second half of 2022. As funding data becomes available, it is clear that most investors pulled back quite a bit in the later half of 2022, so the upswing now is off of a low base. The future will probably have muted investing as well since in Q4 venture funds raised 65% less YoY. Perversely, less capital in the system may imply better returns for the players left since there is less capital chasing deals. We feel fortunate to have a new fund and dry powder during this market correction. Below are a few of the articles that caught our attention this month. Moreover, we've inserted one or two sentences in italics, summarizing each article's importance. We hope you enjoy and appreciate the material.

WHAT WE'RE READING

Here's a curated list of things we found interesting.

Meta unveils a new large language model that can run on a single GPU

With the buzz around ChatGPT and Microsoft you should expect all the other major tech giants to begin to release their own efforts. Facebook / Meta just joined the fray.Meta announced a new AI-powered large language model (LLM) called LLaMA-13B that it claims can outperform OpenAI's GPT-3 model despite being "10x smaller." Smaller-sized AI models could lead to running ChatGPT-style language assistants locally on devices such as PCs and smartphones. It's part of a new family of language models called "Large Language Model Meta AI," or LLAMA for short.

Continue >>

You Can be Hacked via Bing's Chatbot

AI chatbots have become a new attack surface; a new way for malicous hackers to attack users. Maybe go back to Googling things for a while…
Bing Chat can see currently open websites. We show that an attacker can plant an injection in a website the user is visiting, which silently turns Bing Chat into a Social Engineer who seeks out and exfiltrates personal information. The user doesn't have to ask about the website or do anything except interact with Bing Chat while the website is opened in the browser.

Continue >>

Paid security features at Twitter and Meta spark cybersecurity concerns

Lytical advisor Charles Henderson is featured in this article on social media sites gating security features to paying users. To be clear, this is a "bad thing"(™). A world in which only the rich are safe online is dystopian in the extreme.
"The thing that strikes me is that security should be baked into everything we do, not a paid-for service," Charles Henderson, global head of IBM's X-Force threat management division, told me. "It should be on by default."

Continue >>

TRANSACTIONS

Deals that caught our eye.

Sumo Logic to be Acquired by Francisco Partners for $1.7 Billion

Sumo Logic (Nasdaq: SUMO), the SaaS analytics platform to enable reliable and secure cloud-native applications, today announced that it has entered into a definitive agreement to be acquired byFrancisco Partners. The all-cash transaction values Sumo Logic at an aggregate equity valuation of approximately $1.7 billion.

Continue >>

PODCASTS

This month we showcase a podcast from Y Combinator, the startup accelerator.
They delve into AI and specifically large language models (LLMs).

The REAL potential of generative AI

What is a large language model? How can it be used to enhance your business? In this conversation, Ali Rowghani, Managing Director of YC Continuity, talks with Raza Habib, CEO of Humanloop, about the cutting-edge AI powering innovations today—and what the future may hold.
They discuss how large language models like Open AI's GPT-3 work, why fine-tuning is important for customizing models to specific use cases, and the challenges involved with building apps using these models. If you're curious about the ethical implications of AI, Raza shares his predictions about the impact of this quickly developing technology on the industry and the world at large.

Continue >>

ABOUT LYTICAL VENTURES

Lytical Ventures is a New York City-based venture firm investing in Corporate Intelligence, comprising cybersecurity, data analytics, and artificial intelligence. Lytical's professionals have decades of experience in direct investing generally and in Corporate Intelligence specifically.

250 West 55th Street 37th Floor
New York, NY 10019
212.415.6600
communications@lyticalventures.com