

The UNext INSIDER

June, 2023

A SONG OF FIRE & AI

When fire was invented, one set of people probably saw it as a life-changing miracle, but some people also would have considered it an uncontrollable source of danger that could pose an existential risk. Generative AI, as we go along the path to Artificial General Intelligence, is our generation's equivalent to the invention of fire.

With the rise of ChatGPT, we've unlocked doors to new digital dimensions, without fully knowing which are good and which could be sinister. Crossing a whopping number of 1 million users within just 5 days of its launch, ChatGPT is a force to be reckoned with. Today, it has over 100 million users and close to 1.8bn visitors per month.

Statistics also reveal that close to 53% of the average users cannot differentiate between the content written by a human and that by ChatGPT.

We're onto something here, aren't we?



THE DARKSIDE OF **GENERATIVE AI**

headlines, assignments and homework, it is also being actively used by attackers and hackers for illicit purposes. Criminals have always been a few steps ahead in leveraging a new tool or technology to cause harm and with ChatGPT, they've proved this yet again. Attackers are using ChatGPT to write malware

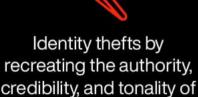
While ChatGPT is being creatively used by humans to write love letters, email

codes that can also autonomously mutate. Not just that, ChatGPT is being used to target diverse target groups through instances of:



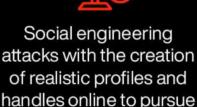


attacks, where text with accurate grammar, tone and language make malicious mails and spams trustable



for extortion

institutions and banks



people for personal information or money



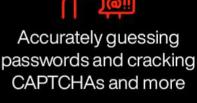
personal details or

money





stalling the stock market a few weeks ago?)



When it comes to tackling this, experts believe conflict is the resolution. While Generative AI is being used as a medium to trigger such actions, it is also the remedy. Websites and products can be made more secure with patched loopholes by running codes through Generative Al for bugs and vulnerabilities, paving the way for automated testing.

THE CONFLICT IS THE

RESOLUTION

techniques. As cybersecurity threats continue to rise, the wise antidote is to have a strong team of cybersecurity professionals, who can harness the power of AI to tackle complex attacks and mitigate them. At the age of digital transformation, what remains a priority is data and the first steps in

some rules from the Art of War as the battle against machine-backed humans has just begun.

protecting it is to educate professionals on possible forms of attack. It's time to implement

However, the larger solution is to insulate a building rather than deploying firefighting



What Do You Think? Is Your Enterprise

Workforce Competent Enough To Mitigate

Advanced Cyber Threats?

Connect Now

Reach out to us for tailored talent