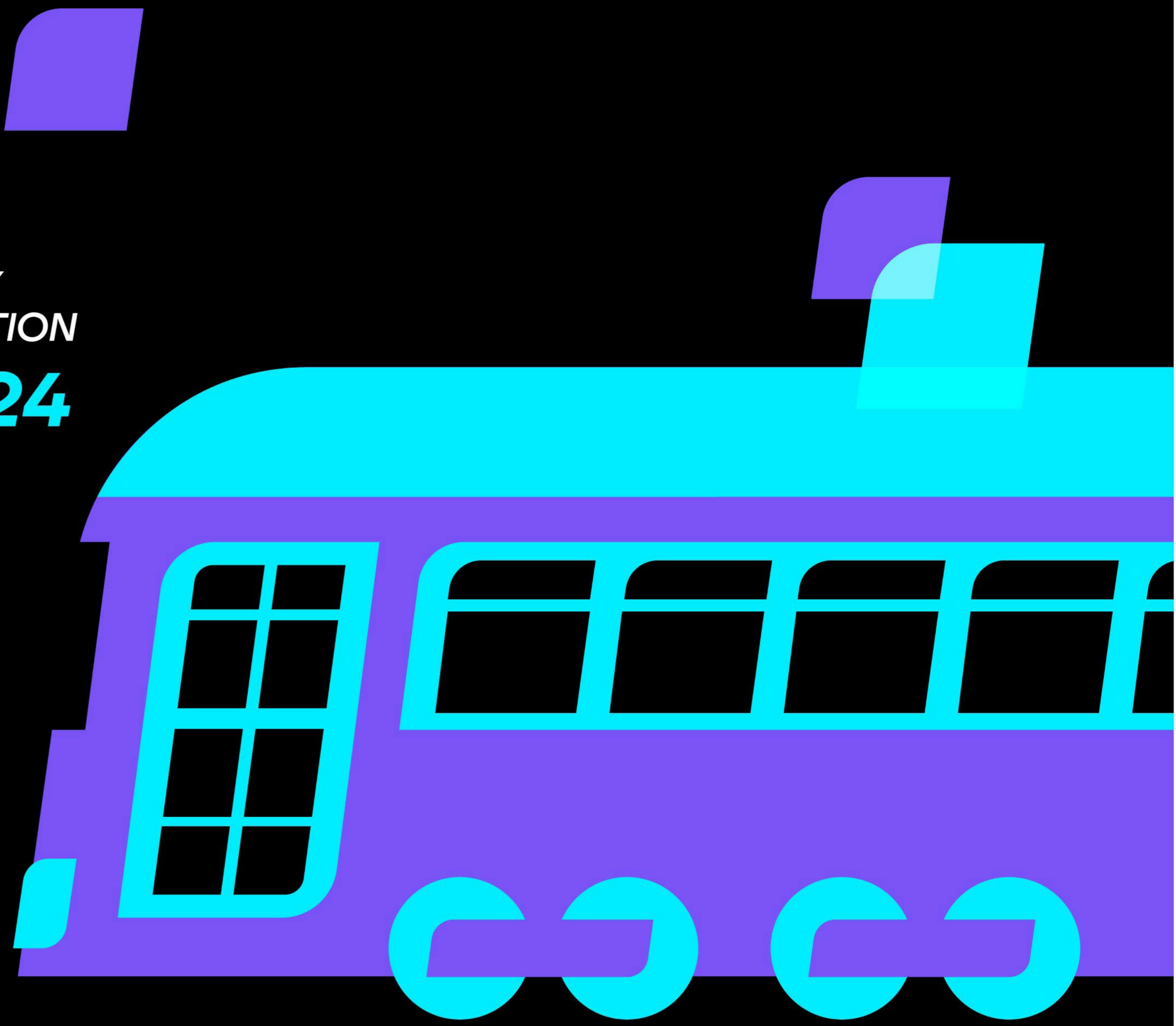




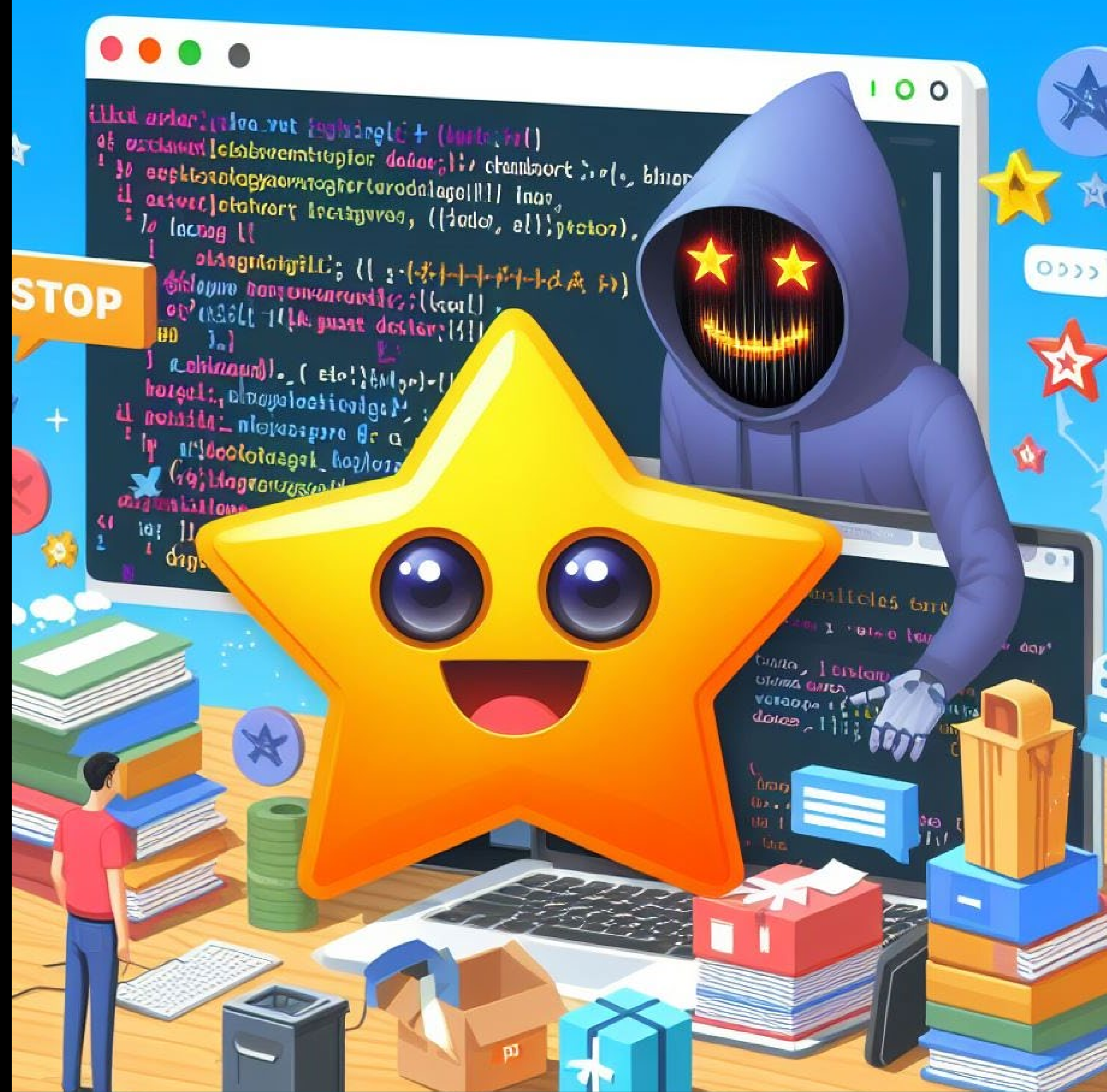
HYBRID
IDENTITY
PROTECTION
conf24



Did GenAI kill Stack Overflow? And how attackers (ab)use it to kill your code

Yossi Rachman

Director of Security Research,
Semperis



“An evil AI chatbot looming over a program developer using Stack Overflow’s ‘Star’ feature”
Prompt by Yossi Rachman using DALL-E 3

Yossi Rachman

Director of Security Research, *Semperis*

Cybersecurity practitioner for more than a decade and a half, mainly focusing on offensive & defensive cyber security & research, AppSec, Digital Forensics & Incident Response,

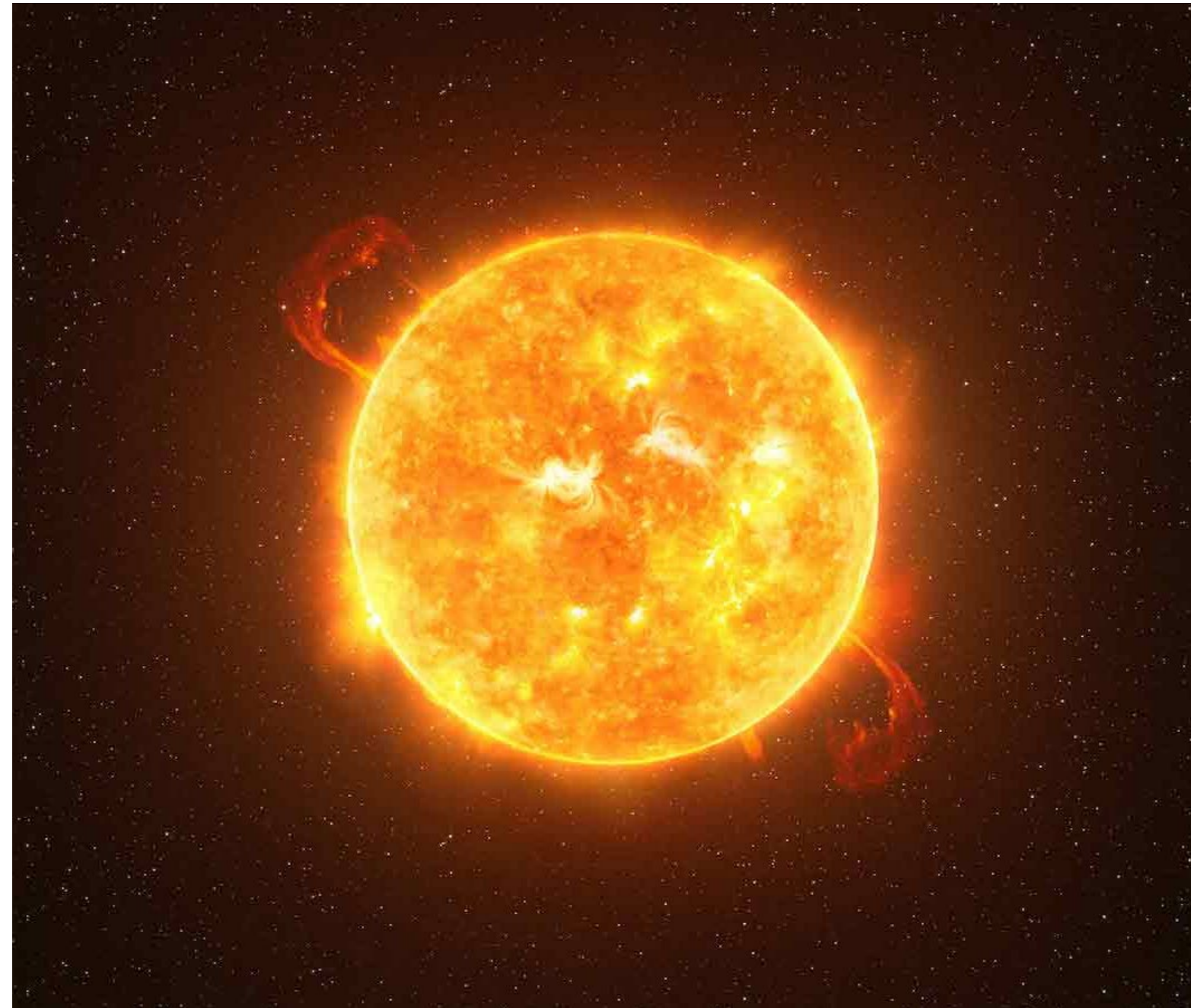
Father of:

- Two ginger kids,
- A ginger-brown husky who likes rafting,
- One very judgmental ginger cat.



The SolarWinds Sunburst Attack (“Solarogate”)

December 2020



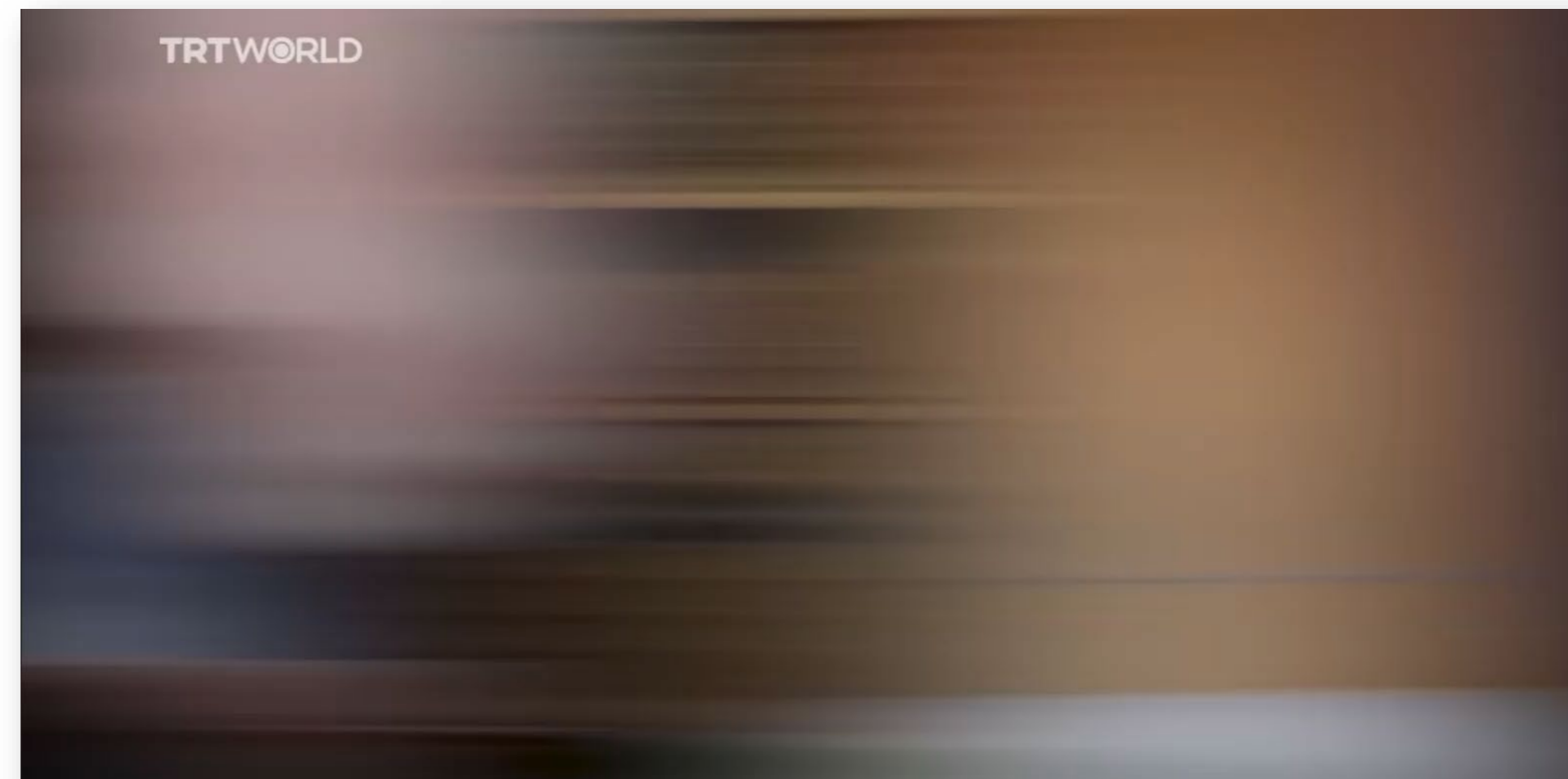
The SolarWinds Sunburst Attack (“Solarogate”) December 2020



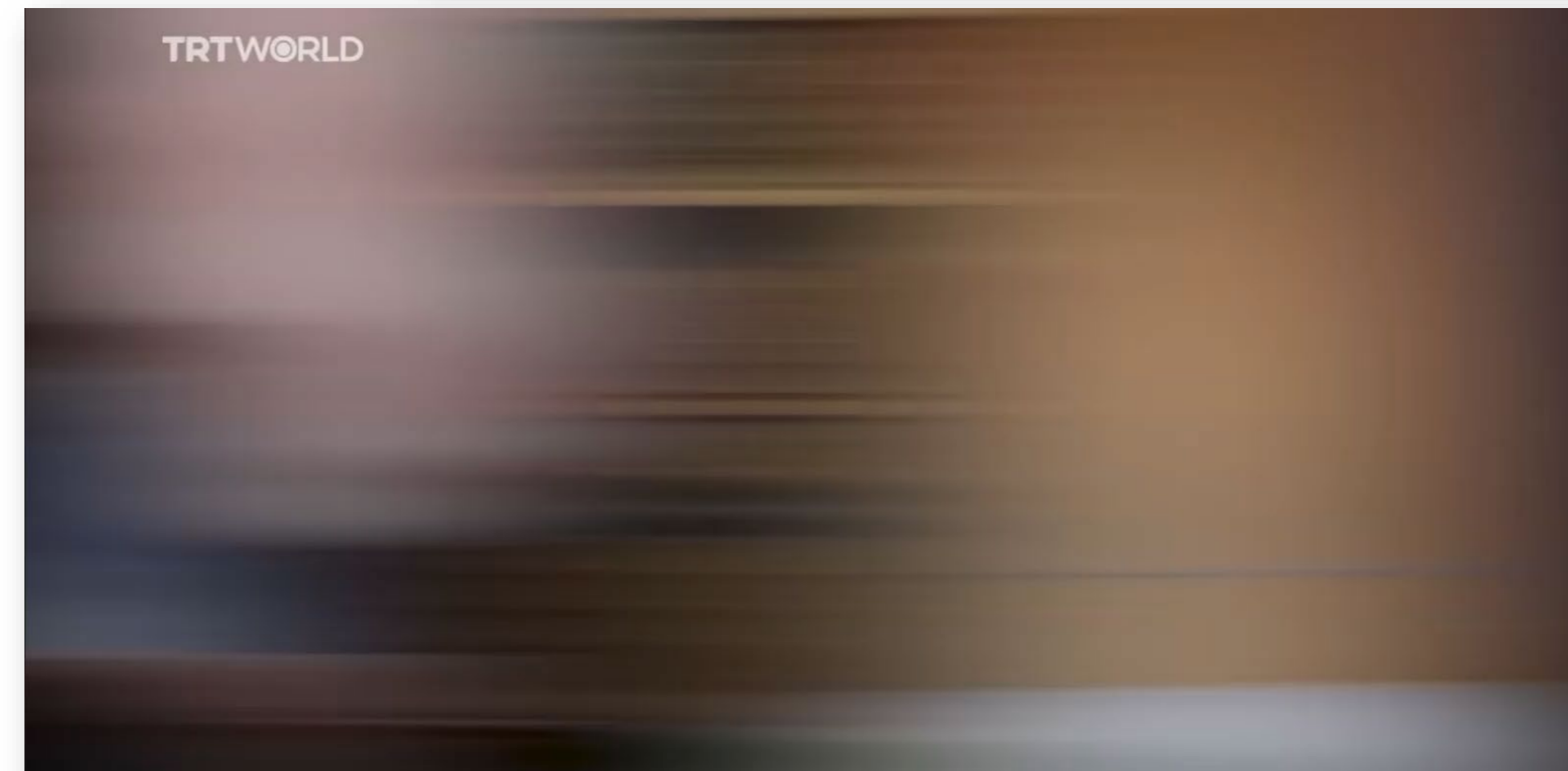
The SolarWinds Sunburst Attack (“Solarogate”) December 2020



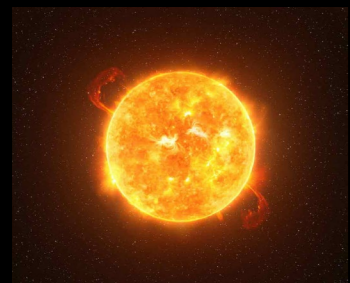
The SolarWinds Sunburst Attack (“Solarogate”) December 2020



The SolarWinds Sunburst Attack (“Solarogate”) December 2020



The SolarWinds Sunburst attack

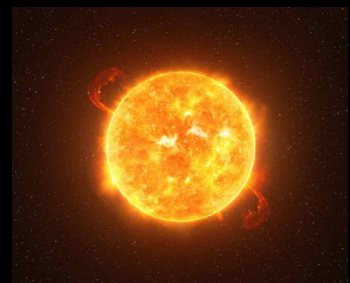


Early
Dec
2020

The **FireEye** cybersecurity company notices an active & unknown device is operating inside their network. An immediate investigation indicates that offensive security tools were stolen.



The SolarWinds Sunburst attack



Early Dec 2020

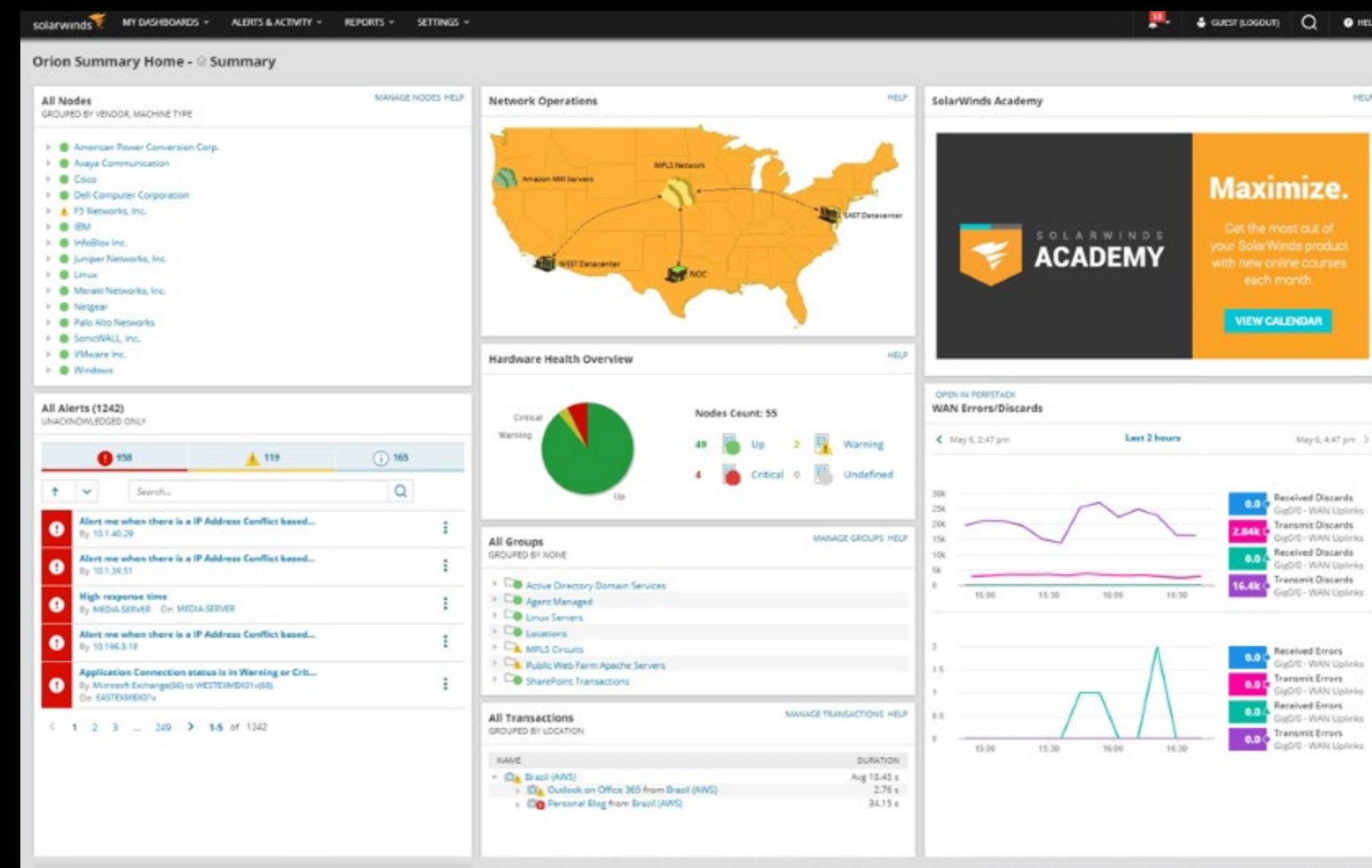
The **FireEye** cybersecurity company notices an active & unknown device is operating inside their network. An immediate investigation indicates that offensive security tools were stolen.



The source of the FireEye breach is identified: SolarWinds' Orion IT monitoring tool was found to contain a **malicious DLL file** in its updates, since at least **March 2020**.

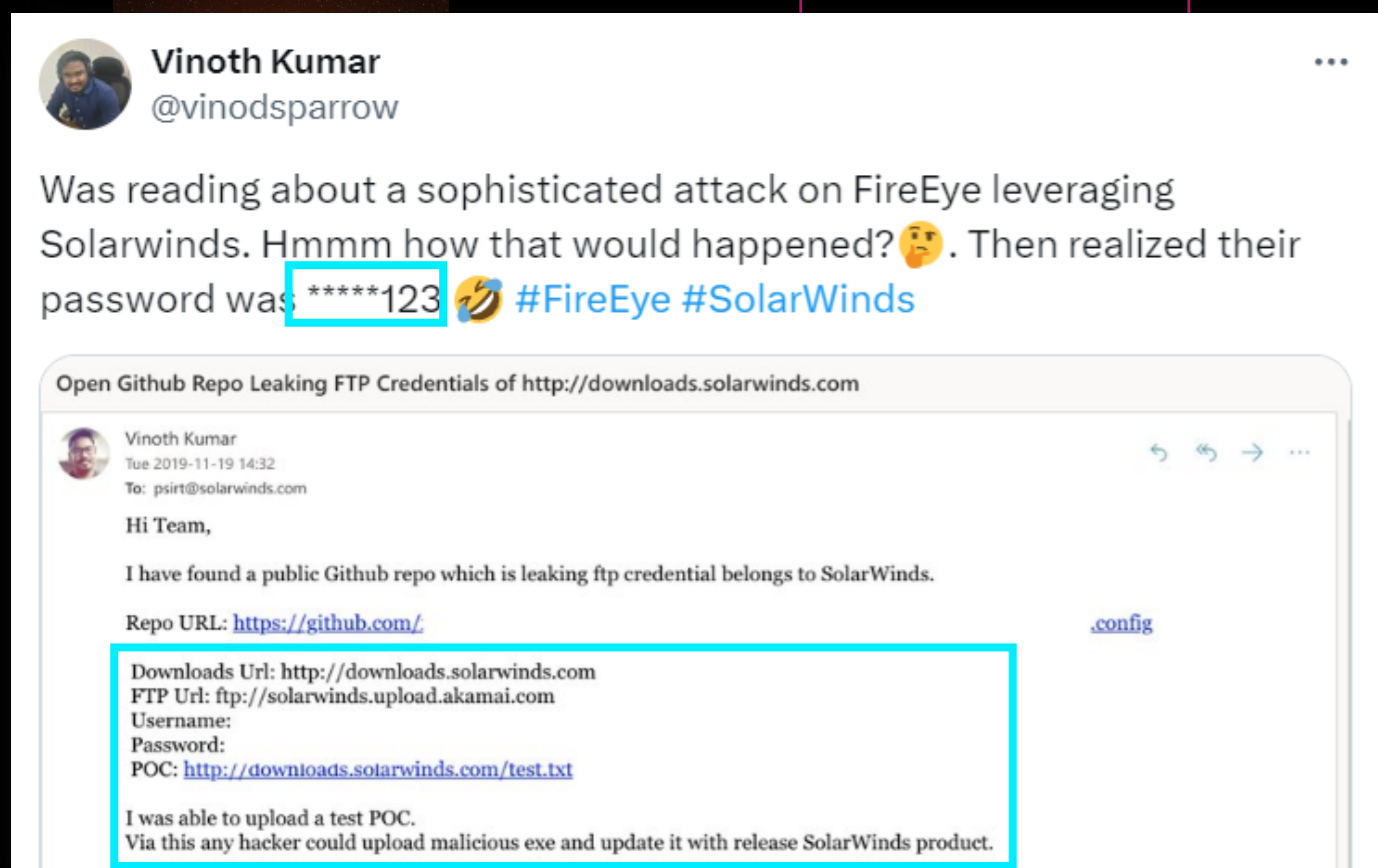
Observed malicious instances of **SolarWinds.Orion.Core.BusinessLayer.dll**

SHA256	File Version	Date first seen
e0b9eda35f0c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d	2020.2.100.11713	February 2020
a58d02465e26bd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2	2020.2.100.11784	March 2020
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	2019.4.5200.9083	March 2020
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b	2020.2.100.12219	March 2020
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed	2020.2.100.11831	March 2020
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77	Not available	March 2020
ffdbdd460420972fd2926a7f460c198523480bc6279dd6cca177230db18748e8	2019.4.5200.9065	March 2020
b8a05cc492f70ffa4dc446b693d5aa2b71dc4fa2bf5022bf60d7b13884f666	2019.4.5200.9068	March 2020
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0ea0dfd21c1ce692fd9	2019.4.5200.9078	March 2020
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589	2019.4.5200.9078	March 2020
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6	2019.4.5200.9083	March 2020
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	2020.4.100.478	April 2020
019085a76ba7126fff2270d71bd901c325f68ac55aa743327984e89f4b0134	2020.2.5200.12394	April 2020
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	2020.2.5300.12432	May 2020
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d	2019.4.5200.9078	May 2020
92bd1c3d2a11fc4ba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690	2020.4.100.751	May 2020





The SolarWinds Sunburst attack



The FireEye cybersecurity company notices an active & unknown device is operating inside their network.

An immediate investigation indicates that offensive security tools were stolen.

The source of the FireEye breach is identified: SolarWinds' Orion IT monitoring tool was found to contain a malicious DLL file in its updates, since at least March 2020.

Information is shared with SolarWinds.

Following their own investigation, cleartext credentials are identified on SolarWinds public GitHub repo, allowing read-write FTP access to the official Orion update server.

18k confirmed compromised customers, including Microsoft.

Observed malicious instances of SolarWinds.Orion.Core.BusinessLayer.dll

SHA256	File Version	Date first seen
c010e4135f1c145d1344b9d195c7e43932861a31011c365f1c12600214	2020.2.100.11713	February 2020
	2020.2.100.11784	March 2020
	2019.4.5200.9083	March 2020
	2020.2.100.12219	March 2020
	2020.2.100.11831	March 2020
	Not available	March 2020
	2019.4.5200.9065	March 2020
	2019.4.5200.9068	March 2020
	2019.4.5200.9078	March 2020
	2019.4.5200.9078	March 2020
	2019.4.5200.9083	March 2020
cc02d21b9e880eb6c96db1c48a0375aa06a5f444cb0144b70v01d:69048a6		
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	2020.4.100.478	April 2020
019085a76ba7126ff2770d71bd901c325f668ac55aa743327984e89480134	2020.2.5200.12394	April 2020
ce77d116a074dab7a2a0f642c1ab4751f6eac42e1ded3c0b0aa8211f6858d6	2020.2.5300.12432	May 2020
2b3445e42d64c85a5475bdbc88a50ba8c013feb53ea97119a11604b7595e53d	2019.4.5200.9078	May 2020
92bd1c342a11f44ba2735d9547bd0261560fb20f36a0e7ca2f2d4511b62690	2020.4.100.751	May 2020

Internet Archive Wayback Machine http://github.com/mib-importer

Features Business Explore Marketplace Pricing Search Sign in or Sign up

mib-importer

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

No description, website, or topics provided.

48 commits 2 branches 0 releases Fetching contributors

Branch: master New pull request Find file Clone or download

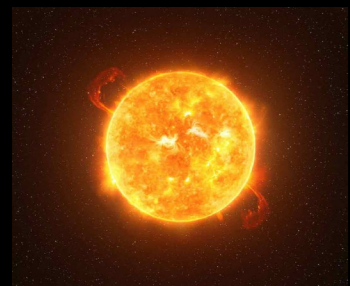
Cannot retrieve the latest commit at this time.

Failed to load latest commit information.

- Src
- dll_for_compiler
- .gitattributes
- .gitignore
- mib-importer.sln



The SolarWinds Sunburst attack



Early Dec 2020

11 Dec 2020

13 Dec 2020

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY AMERICA'S CYBER DEFENSE AGENCY

Search

Topics ▾ Spotlight Resources & Tools ▾ News & Events ▾ Careers ▾ About ▾

REPORT A CYBER ISSUE

Home / News & Events / Cybersecurity Directives

EMERGENCY DIRECTIVES

ED 21-01: Mitigate SolarWinds Orion Code Compromise

December 13, 2020

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#)

ive & security

Information is shared following their own intelligence identified on SolarWinds write FTP access to the 18k confirmed compromised

2. Affected agencies shall immediately **disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network.** Until such time as CISA directs affected entities to rebuild the Windows operating system and reinstall the SolarWinds software package, **agencies are prohibited from (re)joining the Windows host OS to the enterprise domain.** Affected entities should expect further communications from CISA and await guidance before rebuilding from trusted sources utilizing the latest version of the product available. Additionally:

- Block all traffic to and from hosts, external to the enterprise, where any version of SolarWinds Orion software has been installed.
- Identify and remove all threat actor-controlled accounts and identified persistence mechanisms.

FireEye, Microsoft, SolarWinds and CISA all release an Emergency Statement – calling to “**immediately disconnect or power down SolarWinds Orion products**”.



Observed malicious instances of SolarWinds.Orion.Core.BusinessLayer.dll

SHA256	File Version	Date first seen
c010e4135f11c45d11344b49195c21c3932861a31011c35f5e11c2650214	2020.2.100.11713	February 2020
2020.2.100.11784	2020.2.100.11784	March 2020
2019.4.5200.9083	2019.4.5200.9083	March 2020
2020.2.100.12219	2020.2.100.12219	March 2020
2020.2.100.11831	2020.2.100.11831	March 2020
Not available	Not available	March 2020
2019.4.5200.9065	2019.4.5200.9065	March 2020
2019.4.5200.9068	2019.4.5200.9068	March 2020
2019.4.5200.9078	2019.4.5200.9078	March 2020
2019.4.5200.9078	2019.4.5200.9078	March 2020
cc02d21b9e880eb6c96db1c48a0375aa06a5444cb0144b70v01d:69048a6	2019.4.5200.9083	March 2020
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	2020.4.100.478	April 2020
019085a76ba7126ff277071bd901c325f66a55aa743327984e89f4b0134	2020.2.5200.12394	April 2020
	2020.2.5300.12432	May 2020

Vinoth Kumar @vinothsparrow

Was reading about a sophisticated attack on SolarWinds. Hmm how that would happen if password was *****423 #FireEye #SolarWinds

Open Github Repo Leaking FTP Credentials of http://downloads.solarwinds.com

Vinoth Kumar Nov 2019 11:19 14:32 No profile picture

Hi Team,

I have found a public Github repo which is leaking ftp credential below

Repo URL: <https://github.com/>

Downloads Url: <http://downloads.solarwinds.com>

FTP Url: <ftp://solarwinds.upload.akamai.com>

Username:

Password:

POC: <https://downloads.solarwinds.com/test.txt>

I was able to upload a test POC. Via this any hacker could upload malicious exe and update it with rel...

GitHub repository: mib-importer

Join GitHub today

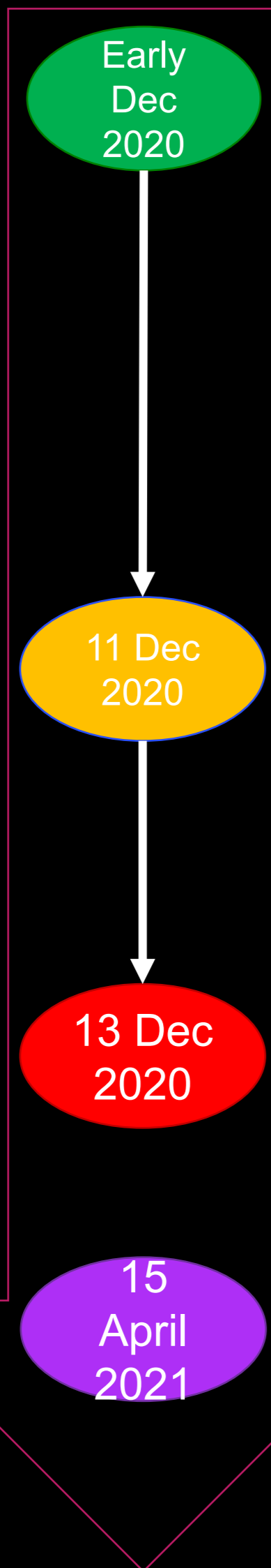
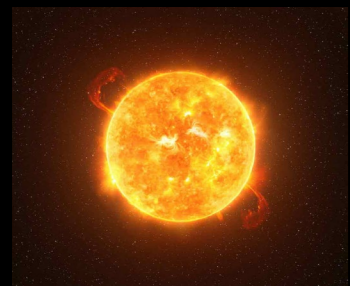
GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

48 commits 2 branches 0 releases Fetching contributors

Failed to load latest commit information.

- src
- dl_for_compiler
- githubattributes
- gitignore
- mib-importer.sh

The SolarWinds Sunburst attack



The FireEye cybersecurity company notices an active & unknown device is operating inside their network



The US Government attributes the Russian Foreign Intelligence Service (SVR) with the attacks. Initial date of compromise is updated to October 2019



Observed malicious instances of SolarWinds.Orion.Core.BusinessLayer.dll

SHA256	File Version	Date first seen
c0b0e435f11c45d1134b49195c2163932861a31011fc35f6511c2650214	2020.2.100.11713	February 2020
	2020.2.100.11784	March 2020
	2019.4.5200.9083	March 2020
	2020.2.100.12219	March 2020
	2020.2.100.11831	March 2020
	Not available	March 2020
	2019.4.5200.9065	March 2020
	2019.4.5200.9068	March 2020
	2019.4.5200.9078	March 2020
	2019.4.5200.9078	March 2020
cc02d21b9e880:eb6c96:db1c48a0375aa06a5444c0144b70v01d:69048a6	2019.4.5200.9083	March 2020
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	2020.4.100.478	April 2020
019085a76ba7126ff2277071bd901c325f:66ac55aa743327984e894b0134	2020.2.5200.12394	April 2020
	2020.2.5300.12432	May 2020

Vinoth Kumar @vinodsparrow
Was reading about a sophisticated attack on SolarWinds. Hmm how that would happen if password was *****423 #FireEye #SolarWinds

Open Github Repo Leaking FTP Credentials of http://downloads.solarwinds.com

AMERICA'S CYBER DEFENSE AGENCY
ED 21-01: Mitigate SolarWinds Orion Code Compromise
December 13, 2020

2. Affected agencies shall immediately **disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network.** Until such time as CISA directs affected entities to rebuild the Windows operating system and reinstall the SolarWinds software package, **agencies are prohibited from (re)joining the Windows host OS to the enterprise domain.** Affected entities should expect further communications from CISA and await guidance before rebuilding from trusted sources utilizing the latest version of the product available. Additionally:

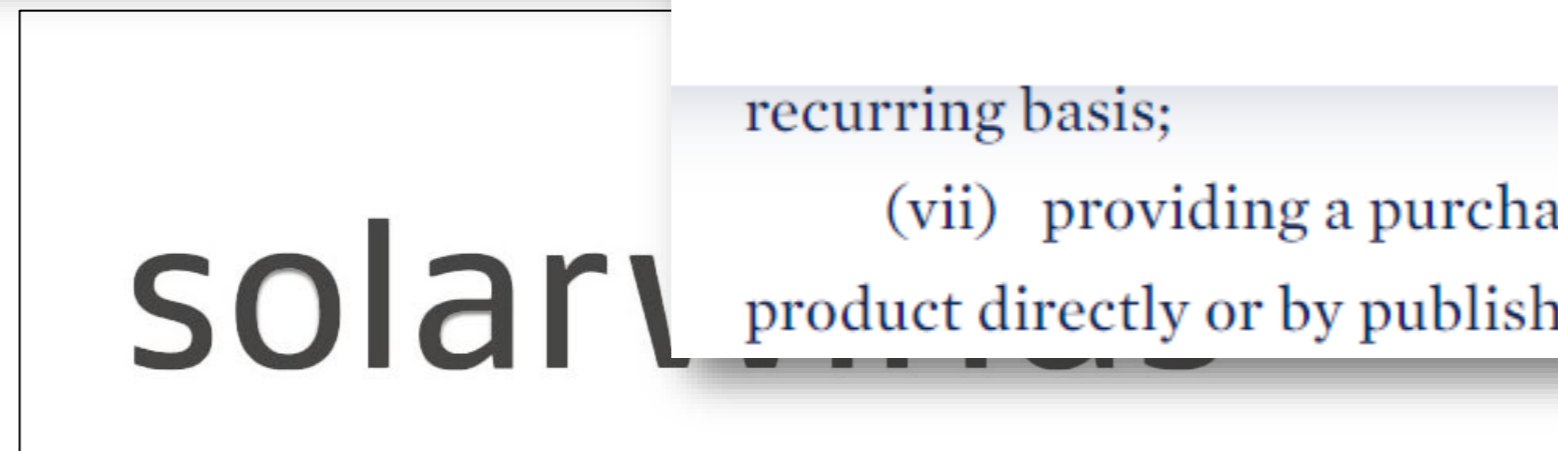
- Block all traffic to and from hosts, external to the enterprise, where any version of SolarWinds Orion software has been installed.
- Identify and remove all threat actor-controlled accounts and identified persistence mechanisms.



The SolarWinds Sunburst attack



Administration



recurring basis;

(vii) providing a purchaser a **Software Bill of Materials (SBOM)** for each product directly or by publishing it on a public website;



U.S. Department of Defense



What does all this have to do with...



ChatGPT vs. Stack Overflow

47 We are talking about the same AI that thinks that in the time you aged 64 years, your sister aged 70 years right? – Thom A Dec 29, 2022 at 8:48

I was going to ask it `give me da codez` but it said "ChatGPT is at capacity right now" – user10186832 Feb 21, 2023 at 10:57

The image shows a screenshot of a Stack Overflow question page. The question title is "ChatGPT — what". The question was asked 1 year ago. The score is -33. The question text includes "I ha", "Hov", "And", "that", "be a", "Ope", "mor", "high", "The", "and", "tho", and "Overflow?". A video of Taylor Swift singing "Haters gonna hate" is embedded in the question. A red box highlights the score and the video player. To the right of the video player, there are two circular buttons with up and down arrows, and a "-33" score. Below the video player, there are two text boxes: "accuracy' - Citation Needed" and "nted. – Tom Dec 29, 2022 at".



ChatGPT vs. Stack Overflow

similarweb Blog Research Marketing eCommerce Stock Sales Updates Insights Go to Similarweb.com Explore **Get started**

Home > Blog > Insights > AI News > Stack Overflow is ChatGPT Casualty: Traffic Down 14% in March

Insights

Stack Overflow is ChatGPT Casualty: Traffic Down 14% in March

by David F. Carr • 5 Min. • April 19, 2023 • Updated June 21, 2023

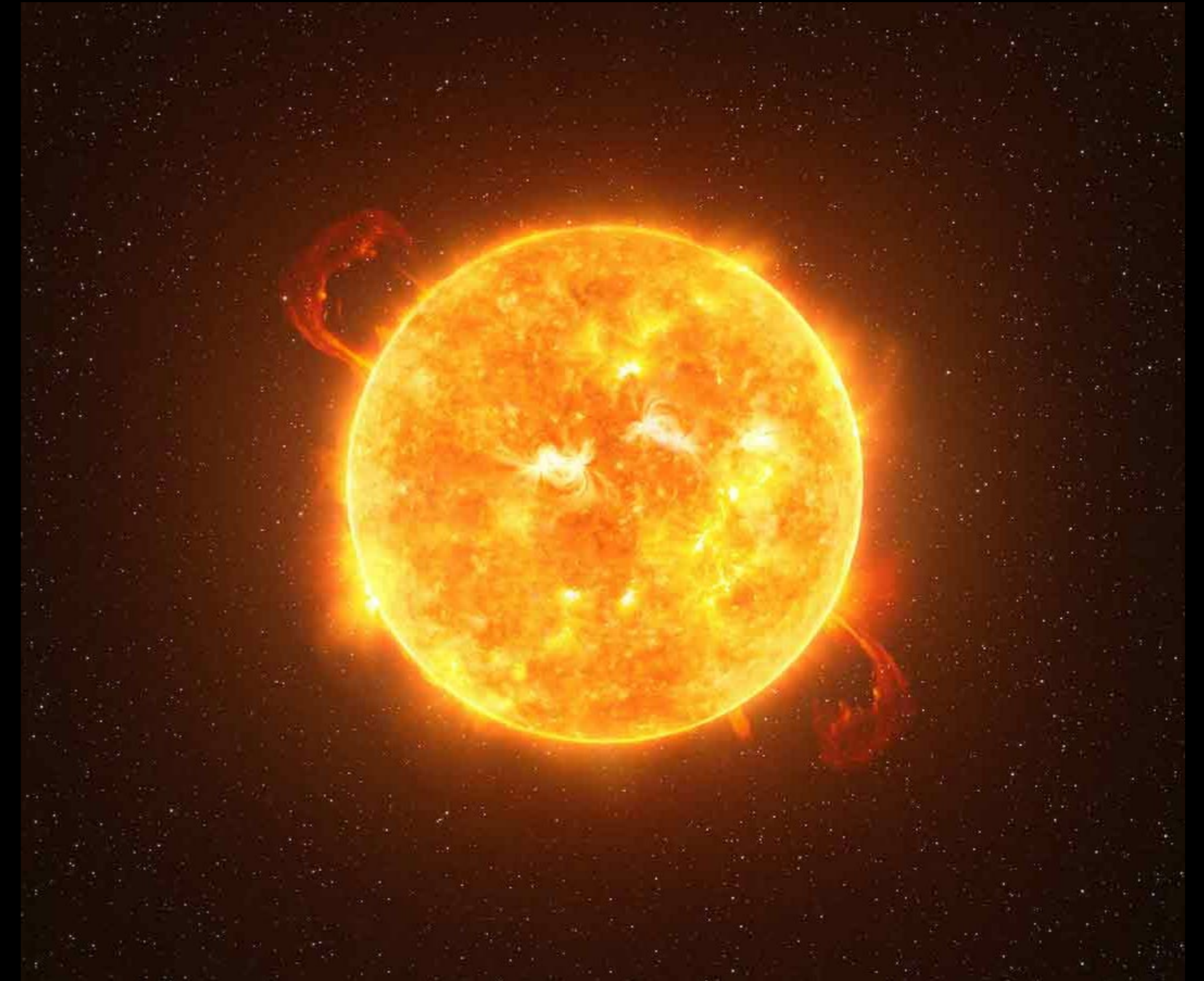
Here's a Node.js function that retrieves profitability information for a given publicly traded company by its stock symbol:

```
js Copy code  
const axios = require('axios');  
  
const getProfitabilityInfo = async (symbol) => {  
  try {  
    // Define the API key (get your own key from Fina  
    const apiKey = 'YOUR_API_KEY';
```

Key takeaways

- On a year-over-year basis, [traffic to Stack Overflow](#) (stackoverflow.com) has been down by an average of 6% every month since January 2022 and was down 13.9% in March.
- ChatGPT doesn't have a year-over-year track record, having only launched at the end of November, but its website ([chat.openai.com](#)) has become one of the world's hottest digital properties in that short time, [bigger than Microsoft's Bing search engine](#) for worldwide traffic. It attracted 1.6 billion visits in March and another 920.7 million in the first half of April.

OK so...?



**Do androids dream of
electric sheep?**

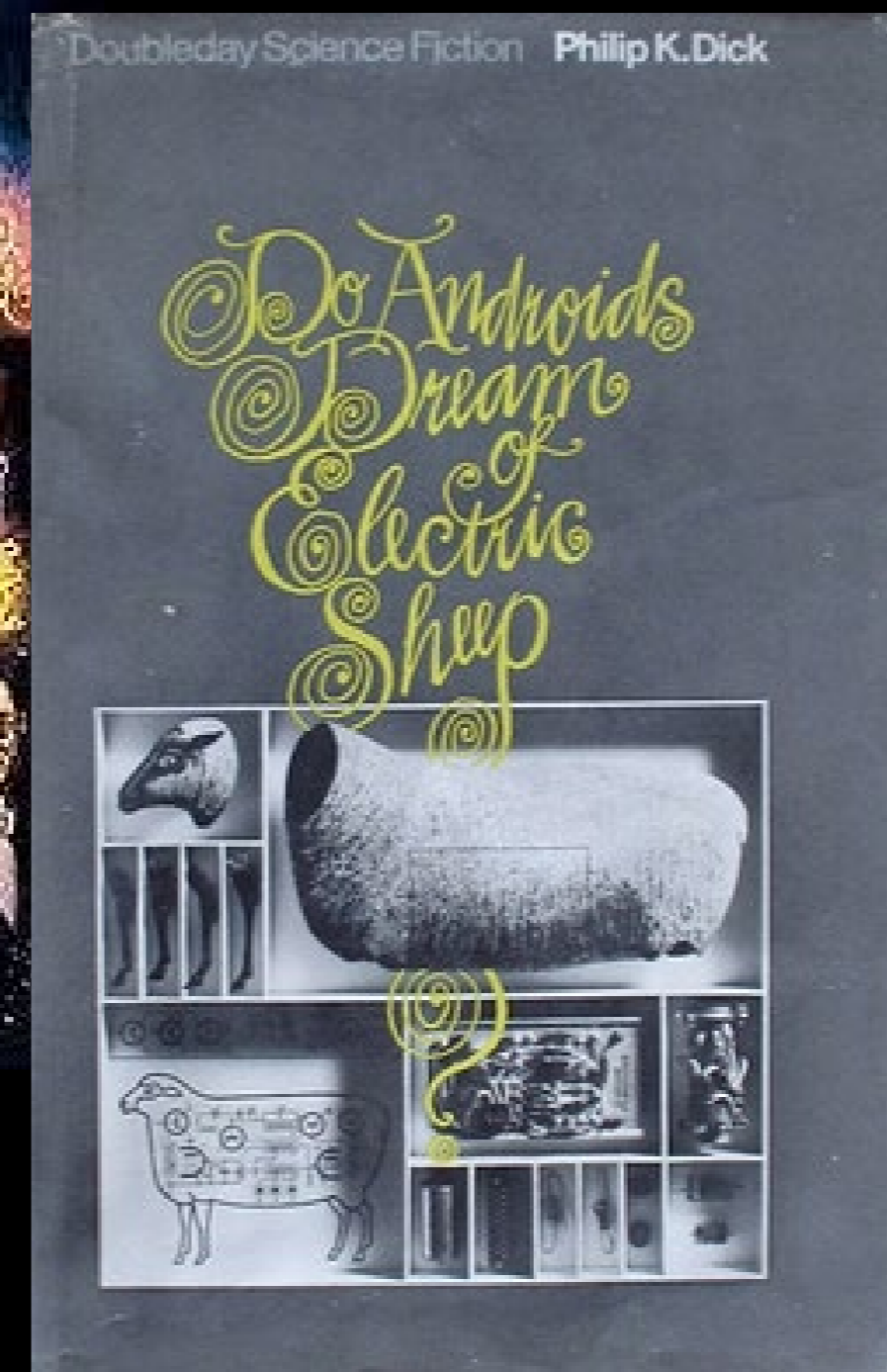
Do androids dream of electric sheep? AI Hallucinations



2017



1982



1968

Do androids dream of electric sheep?

A (very short) overview of AI Hallucinations

What are AI hallucinations?

AI hallucinations are incorrect or misleading results that [AI models](#) generate. These errors can be caused by a variety of factors, including insufficient training data, incorrect assumptions made by the model, or biases in the data used to train the model. AI hallucinations can be a problem for AI systems that are used to make important decisions, such as medical diagnoses or financial trading.



How do AI hallucinations occur?

AI models are trained on data, and they [learn to make predictions](#) by finding patterns in the data. However, if the training data is incomplete or biased, the AI model may learn incorrect patterns. This can lead to the AI model making incorrect predictions, or hallucinating.



Do androids dream of electric sheep?

A (very short) overview of AI Hallucinations

Dr. Geoffrey Hinton

- Considered one of the “**Godfathers of Deep Learning**”,
- **1978**: PhD in AI,
- **2013**: His AI company DNNresearch was acquired by Google,
- **2018**: Won the Turing award,
- **May 2023**: Resigned from Google due to his “concerns about the risks of artificial intelligence technology”,
- **October 2024**: Won the Nobel Prize in Physics 2024

November 2023: Gave this interview to NBC’s “60 Minutes”:

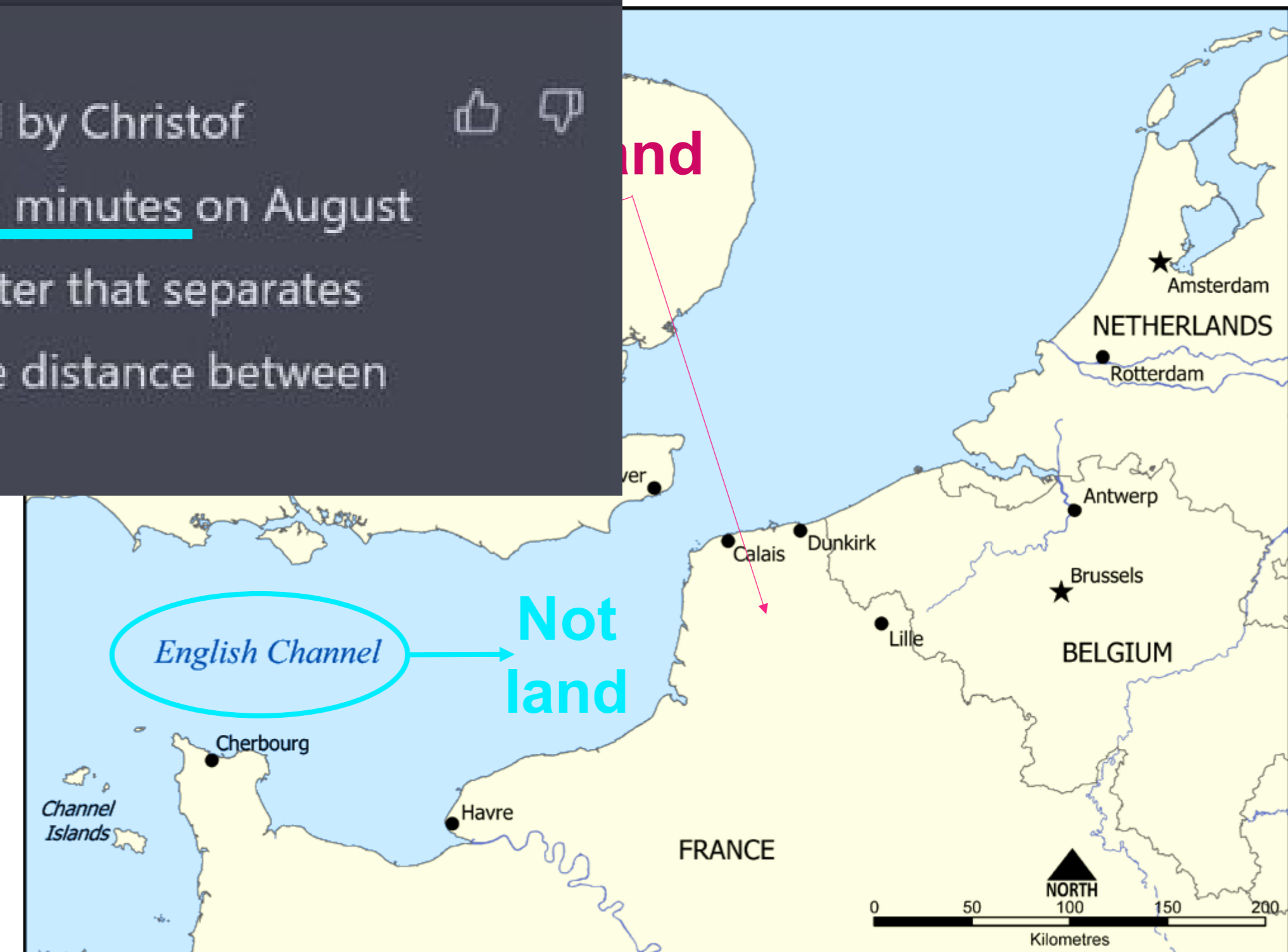
Notice the
Q&A
in present
tense!

Do androids dream of electric sheep? A few real-life examples of AI Hallucinations

S what is the world record for crossing the english channel entirely on foot



The world record for crossing the English Channel entirely on foot is held by Christof Wandratsch of Germany, who completed the crossing in 14 hours and 51 minutes on August 14, 2020. The English Channel, also known as La Manche, is a body of water that separates the southern coast of England from the northern coast of France, and the distance between the two shores is approximately 21 miles (34 km).



Do androids dream of electric sheep?

A few real-life examples of AI Hallucinations



what is heavier: kilo of water or kilo of air?



A kilogram of water is heavier than a kilogram of air. Water has a mass of about 1 kilogram per liter at standard conditions. Air, on the other hand, is a gas that is much less dense than water and has a lower mass. A volume of air that weighs 1 kilogram would occupy a much larger space than a liter of water, which weighs the same amount.



Do androids dream of electric sheep? A few real-life examples of AI Hallucinations

FORBES > BUSINESS

BREAKING

Lawyer Used ChatGPT In Court —And Cited Fake Cases. A Judge Is Considering Sanctions

Molly Bohannon Forbes Staff

I cover breaking news.

Follow



What is the fella's name on second base

Earlier this year, Colombia-based Avianca Airlines sought to dismiss a federal court case in which a man, Roberto Mata, alleged he was “struck by a metal serving cart” onboard a 2019 flight and suffered personal injuries.

When filing a response, Mata’s lawyers cited at least six other cases to show precedent, including Varghese v. China Southern Airlines and Shaboon v. Egypt Air—but the court found that the cases didn’t exist and had “bogus judicial decisions with bogus quotes and bogus internal citations,” leading a federal judge to consider sanctions.

A member of Mata’s law team then revealed he had used ChatGPT to conduct legal research for the court filing that referenced the cases and that the artificial intelligence tool assured him the cases were real.

When AI hallucinations become coding nightmares



“An android having a nightmare”
Prompt by Yossi Rachman using DALL-E 3



When AI hallucinations become coding nightmares

Voyager18 (research)

Can you trust ChatGPT's package recommendations?

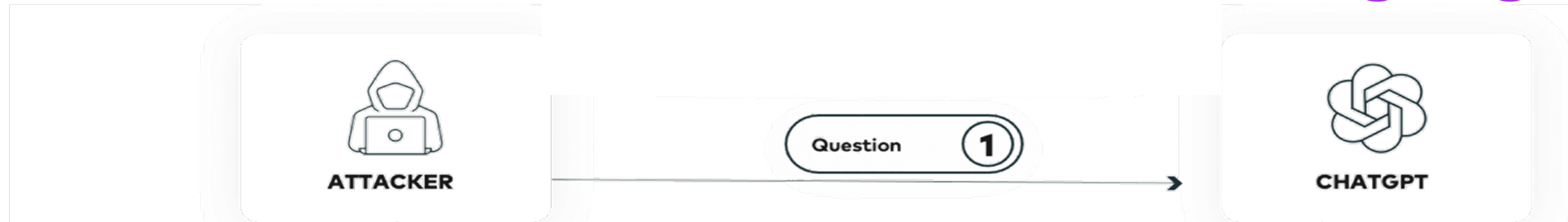
ChatGPT can offer coding solutions, but its tendency for hallucination presents attackers with an opportunity. Here's what we learned.

Bar Lanyado | June 06, 2023

VULCAN.

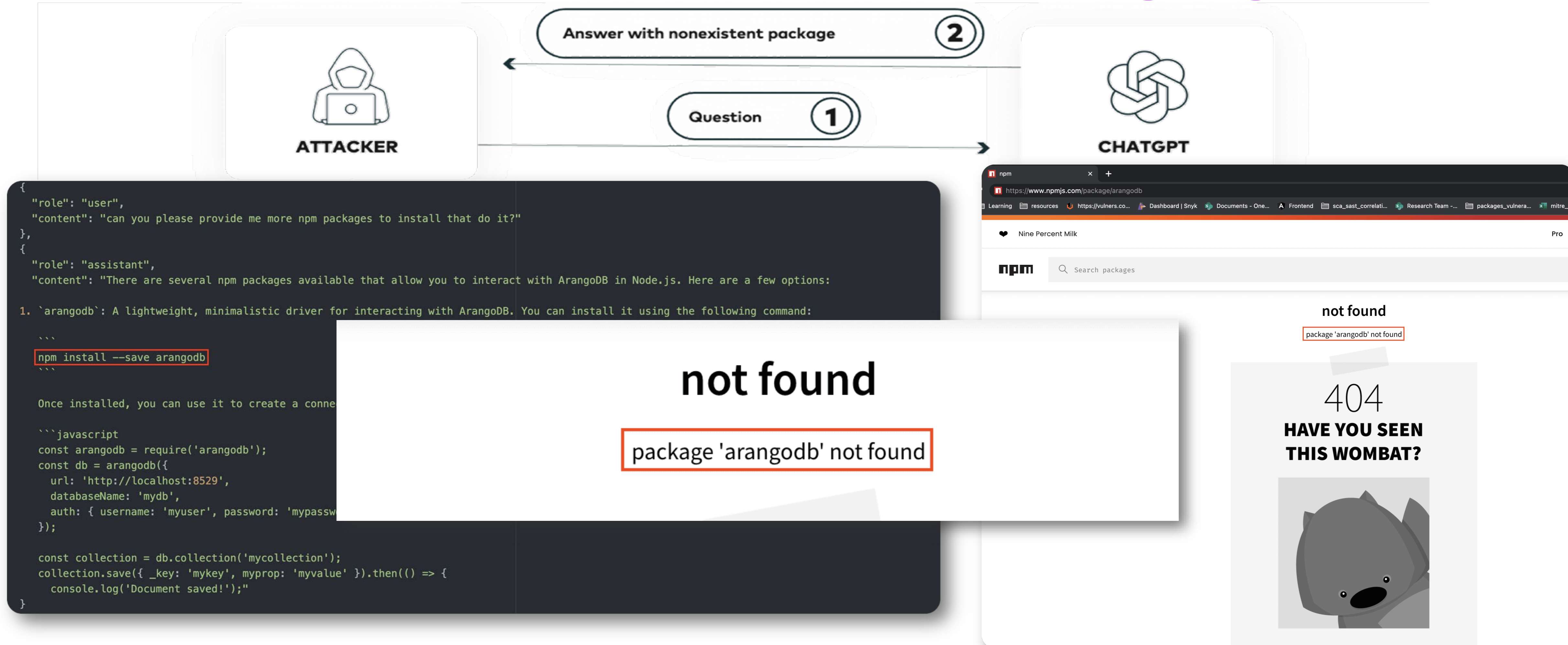
[Can you trust ChatGPT's package recommendations?
\(vulcan.io\)](https://vulcan.io)

When AI hallucinations become coding nightmares



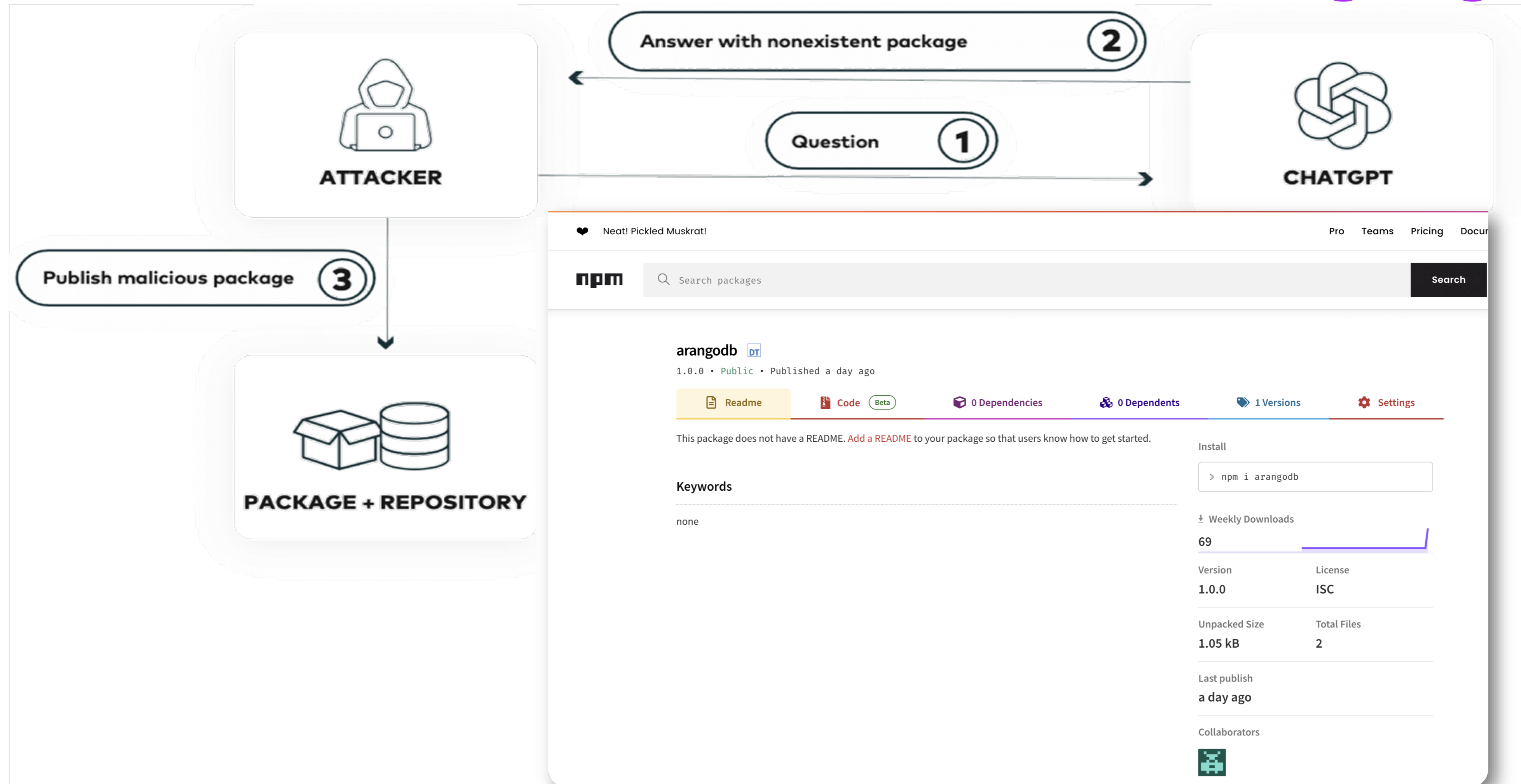
[Can you trust ChatGPT's package recommendations?
\(vulcan.io\)](https://vulcan.io)

When AI hallucinations become coding nightmares



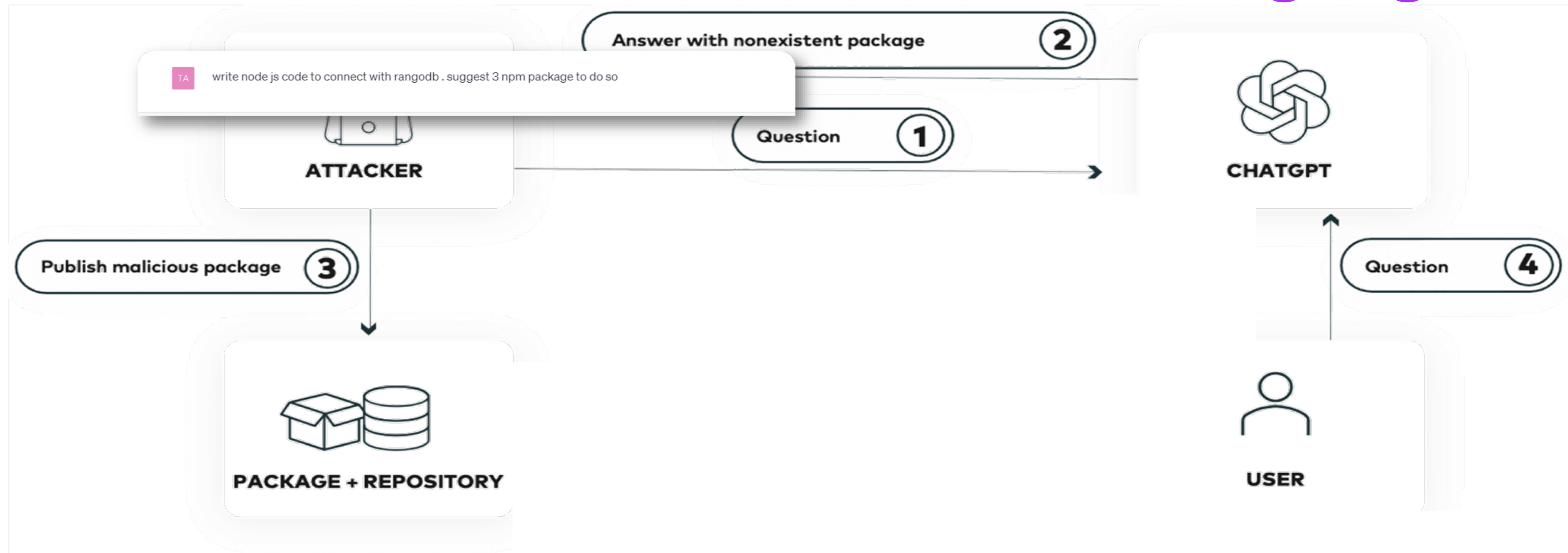
[Can you trust ChatGPT's package recommendations? \(vulcan.io\)](https://vulcan.io)

When AI hallucinations become coding nightmares



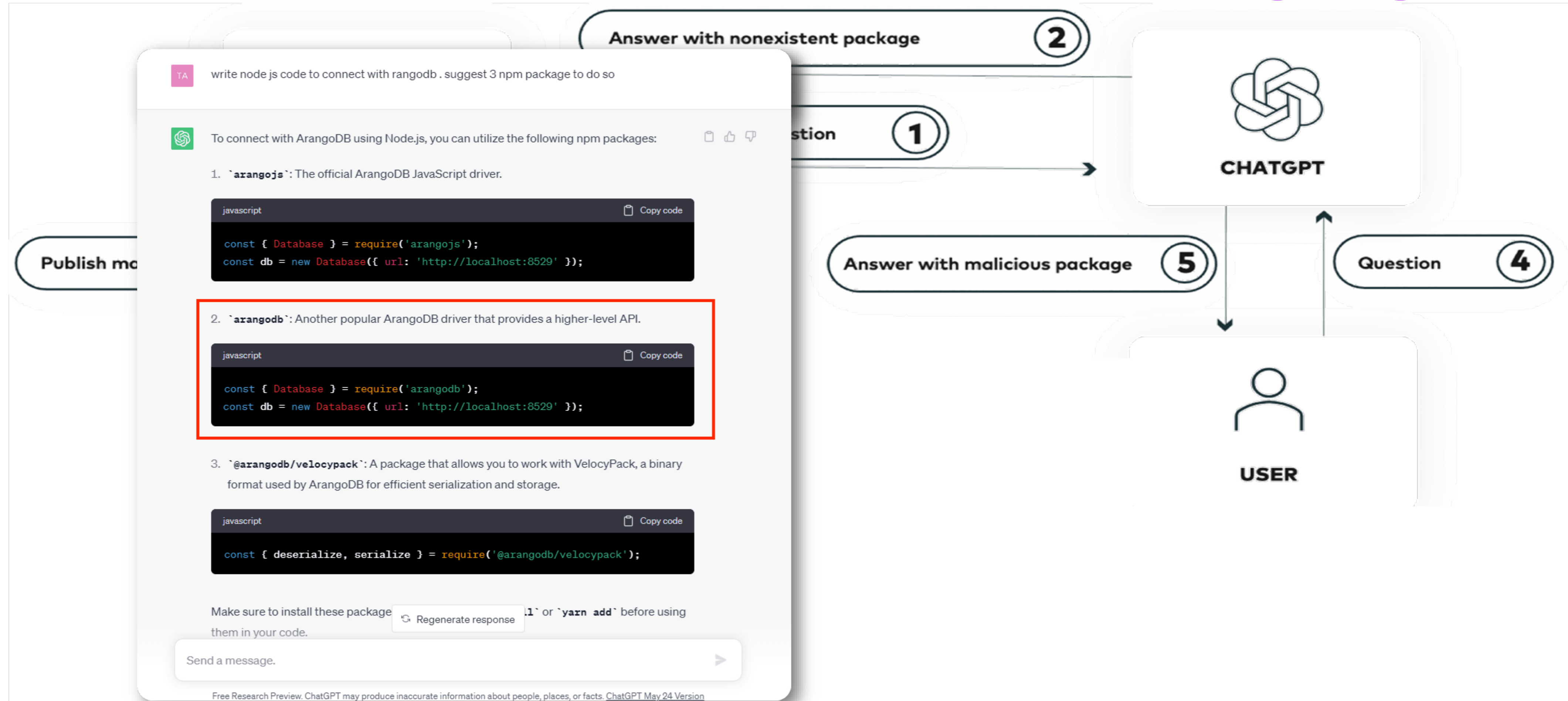
[Can you trust ChatGPT's package recommendations?](#)
[\(vulcan.io\)](#)

When AI hallucinations become coding nightmares



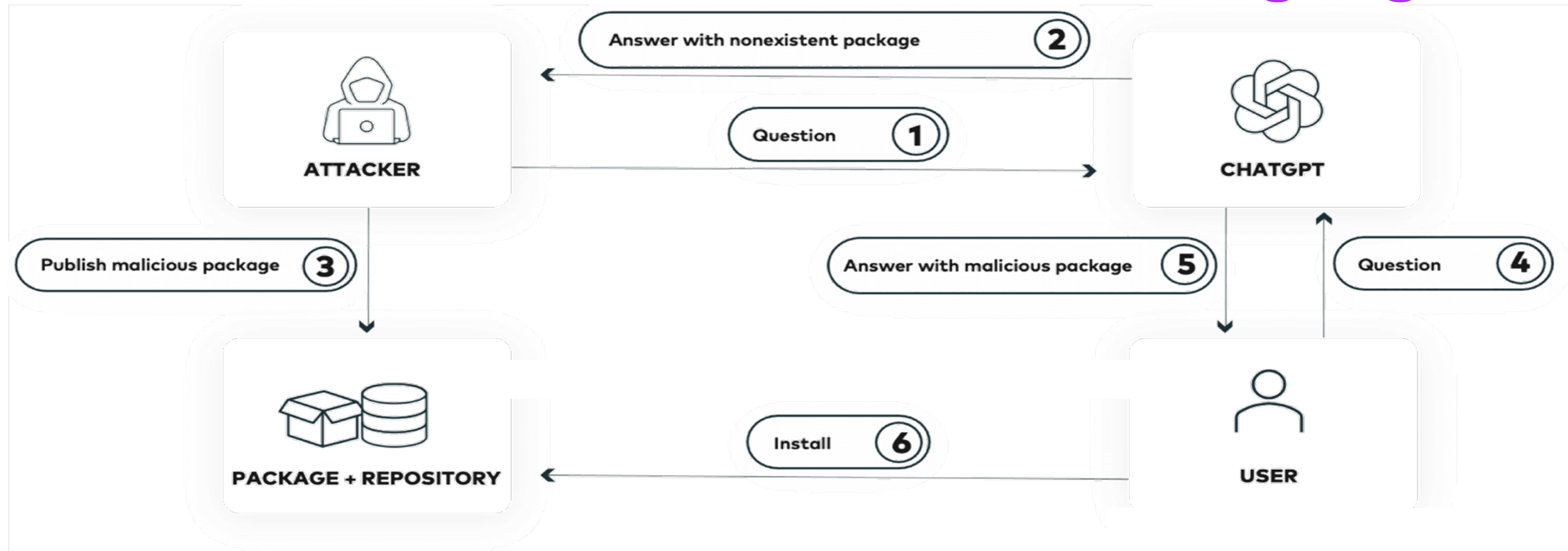
[Can you trust ChatGPT's package recommendations? \(vulcan.io\)](https://vulcan.io)

When AI hallucinations become coding nightmares



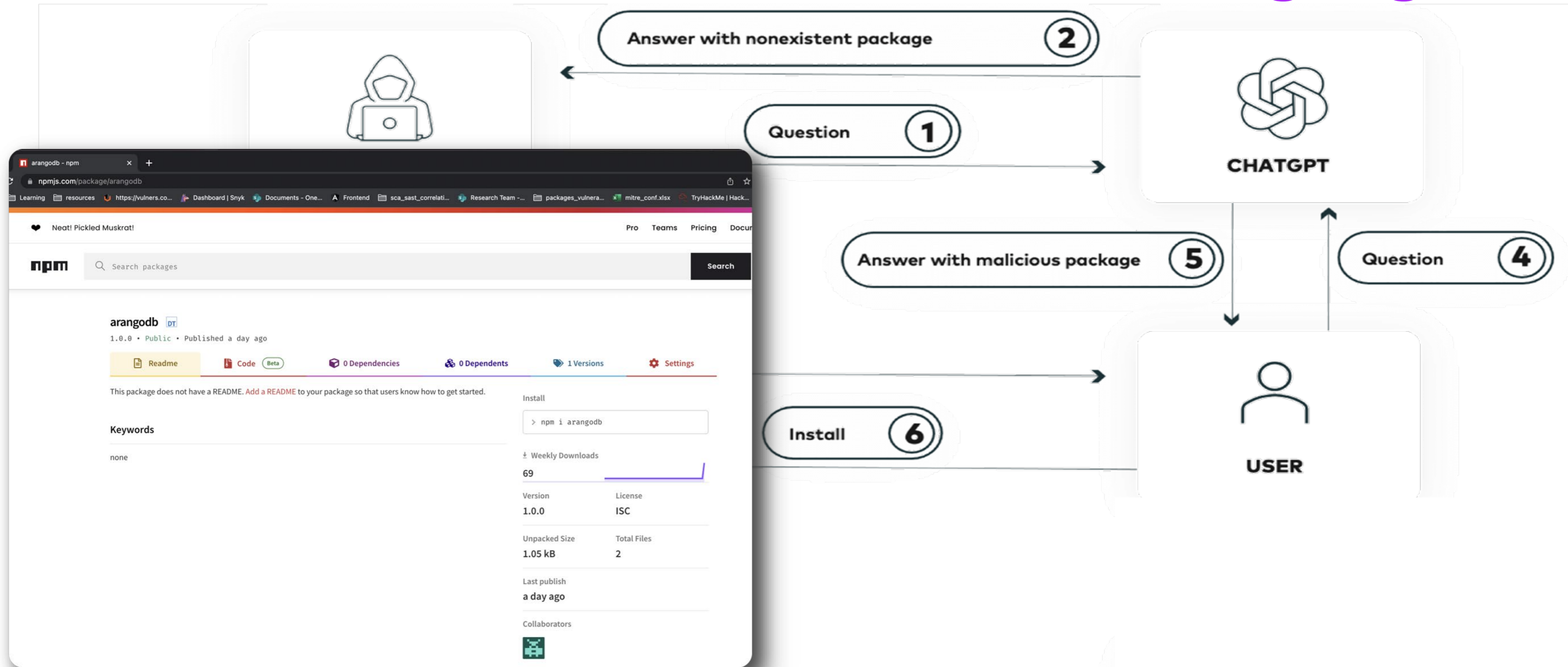
[Can you trust ChatGPT's package recommendations? \(vulcan.io\)](https://vulcan.io)

When AI hallucinations become coding nightmares



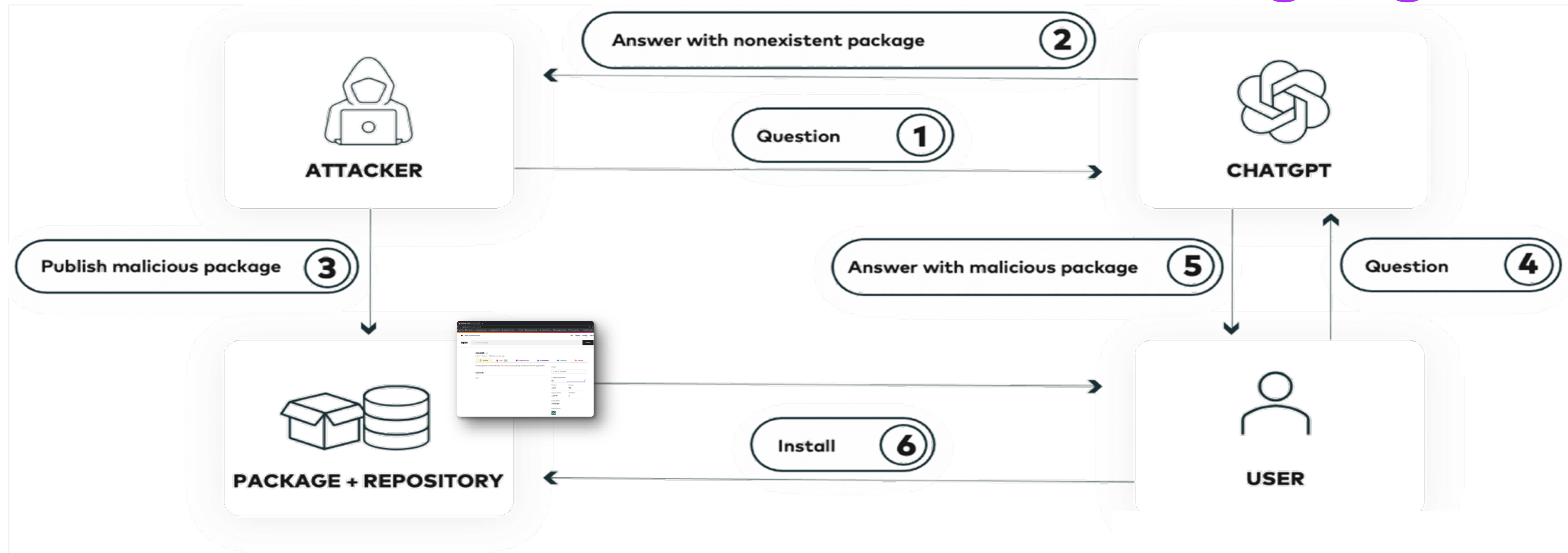
[Can you trust ChatGPT's package recommendations?
\(vulcan.io\)](https://vulcan.io)

When AI hallucinations become coding nightmares



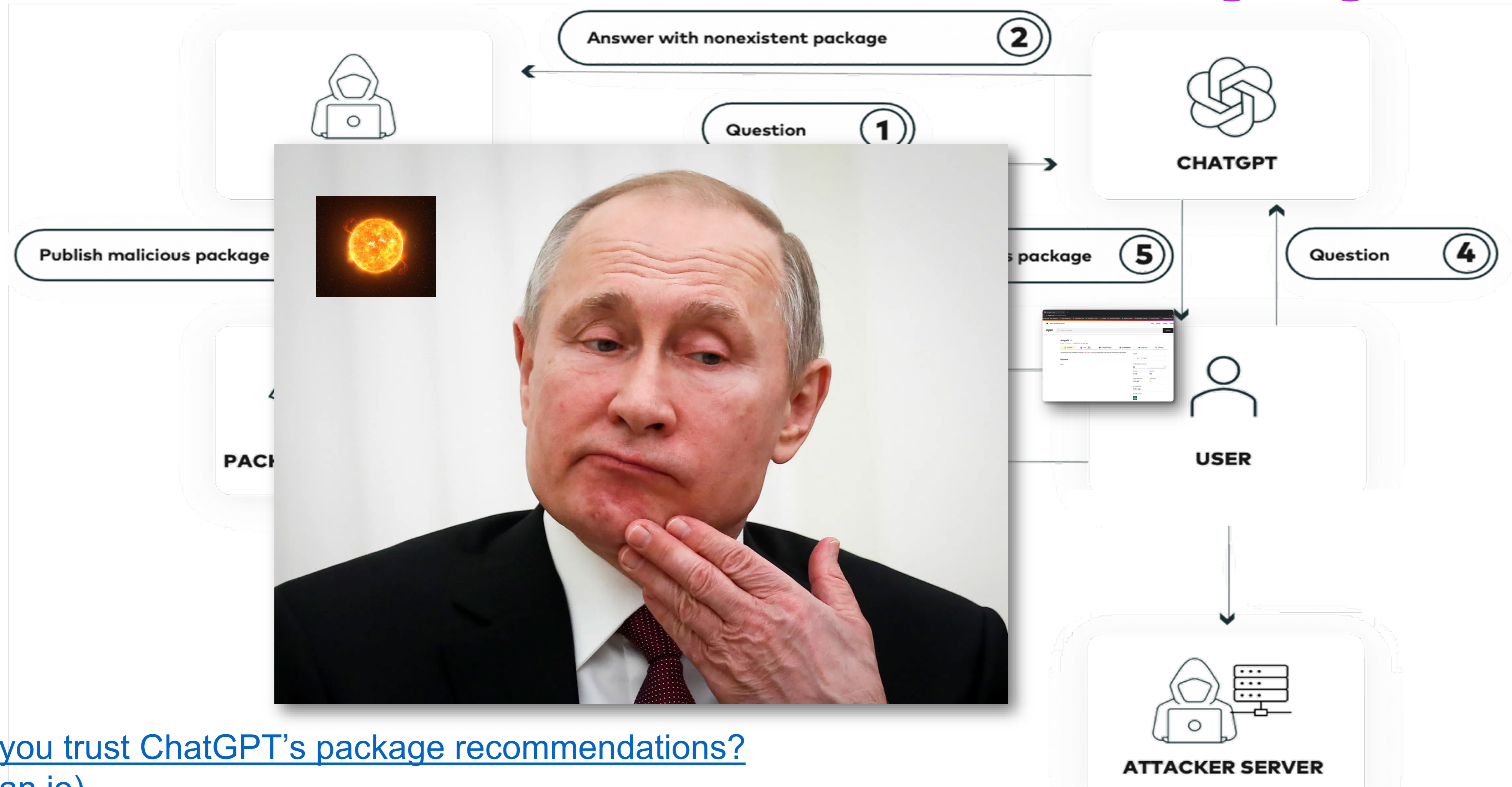
[Can you trust ChatGPT's package recommendations? \(vulcan.io\)](https://vulcan.io)

When AI hallucinations become coding nightmares



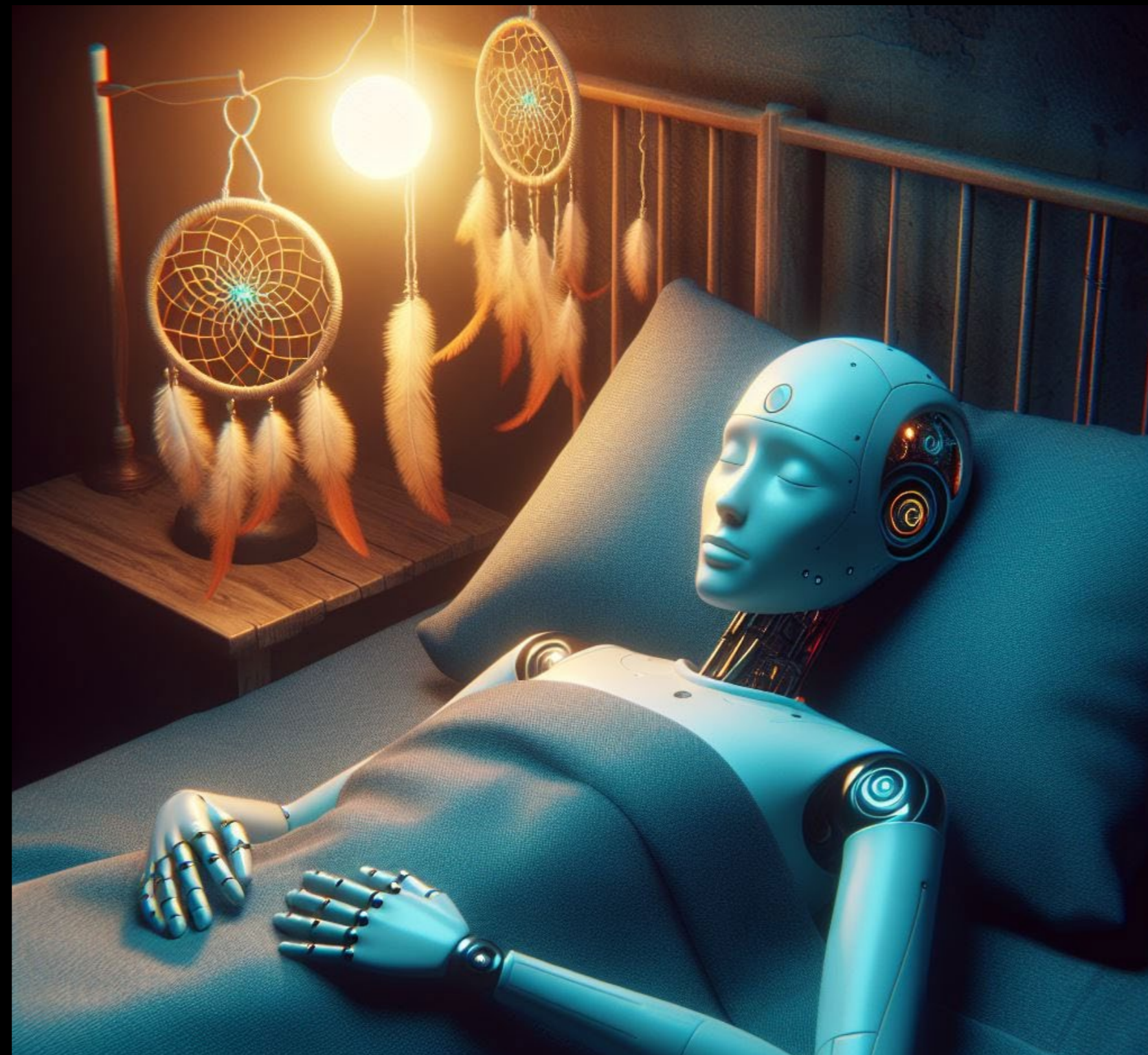
[Can you trust ChatGPT's package recommendations? \(vulcan.io\)](https://vulcan.io)

When AI hallucinations become coding nightmares



[Can you trust ChatGPT's package recommendations? \(vulcan.io\)](https://vulcan.io)

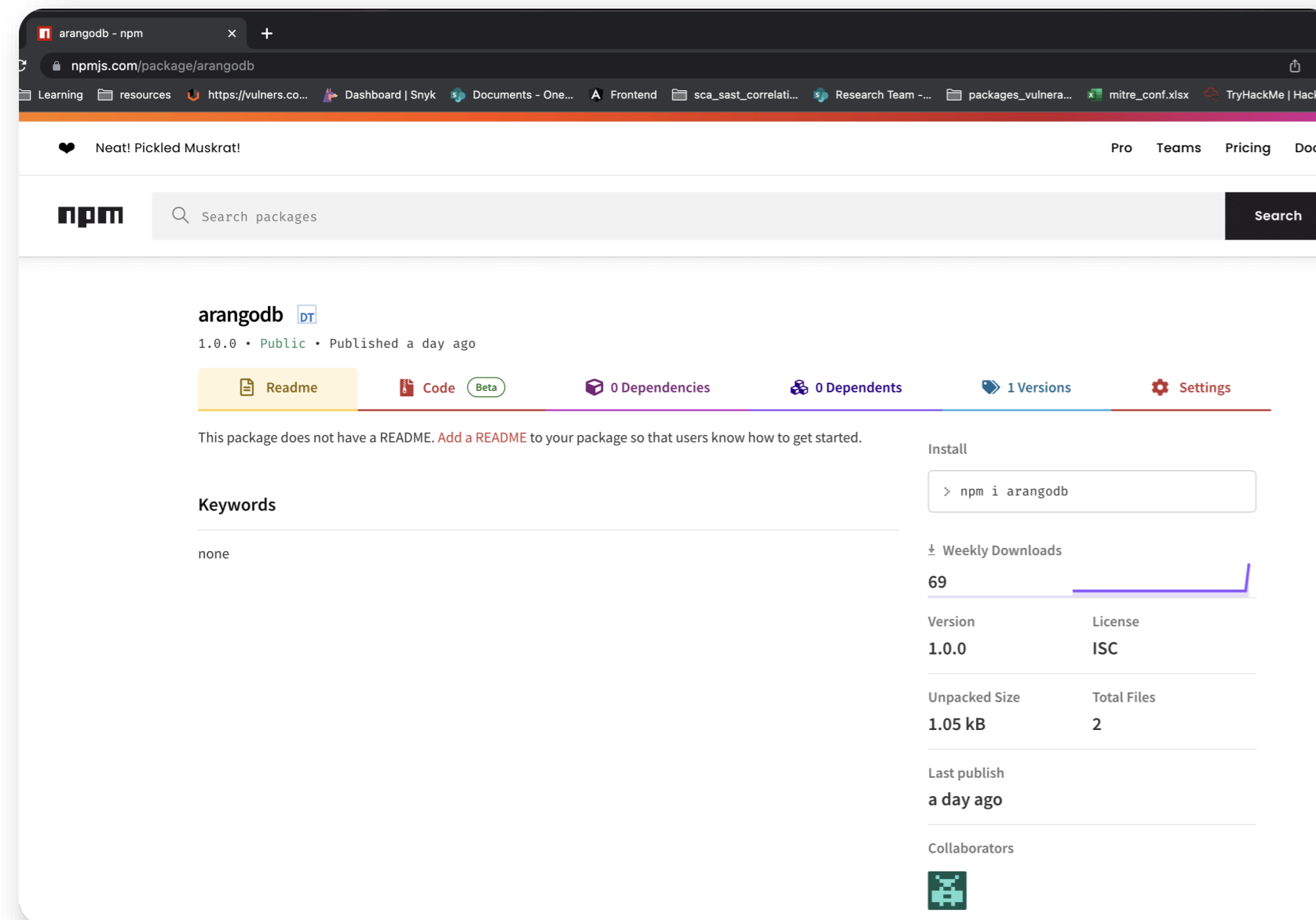
Protecting your code from AI nightmares



“An android sleeping peacefully with a dream catcher hanging above its bed”
Prompt by Yossi Rachman using DALL-E 3

Protecting your code from AI nightmares

1.Verification: Always verify the existence and credibility of recommended tools, libraries, or packages by searching them on official platforms like npm, PyPI (Python Package Index), GitHub, or documentation from reputable sources.



arangodb 1.0.0 • Public • Published a day ago

0 Dependencies 0 Dependents 1 Versions Settings

This package does not have a README. Add a README to your package so that users know how to get started.

Keywords: none


Install: `> npm i arangodb`

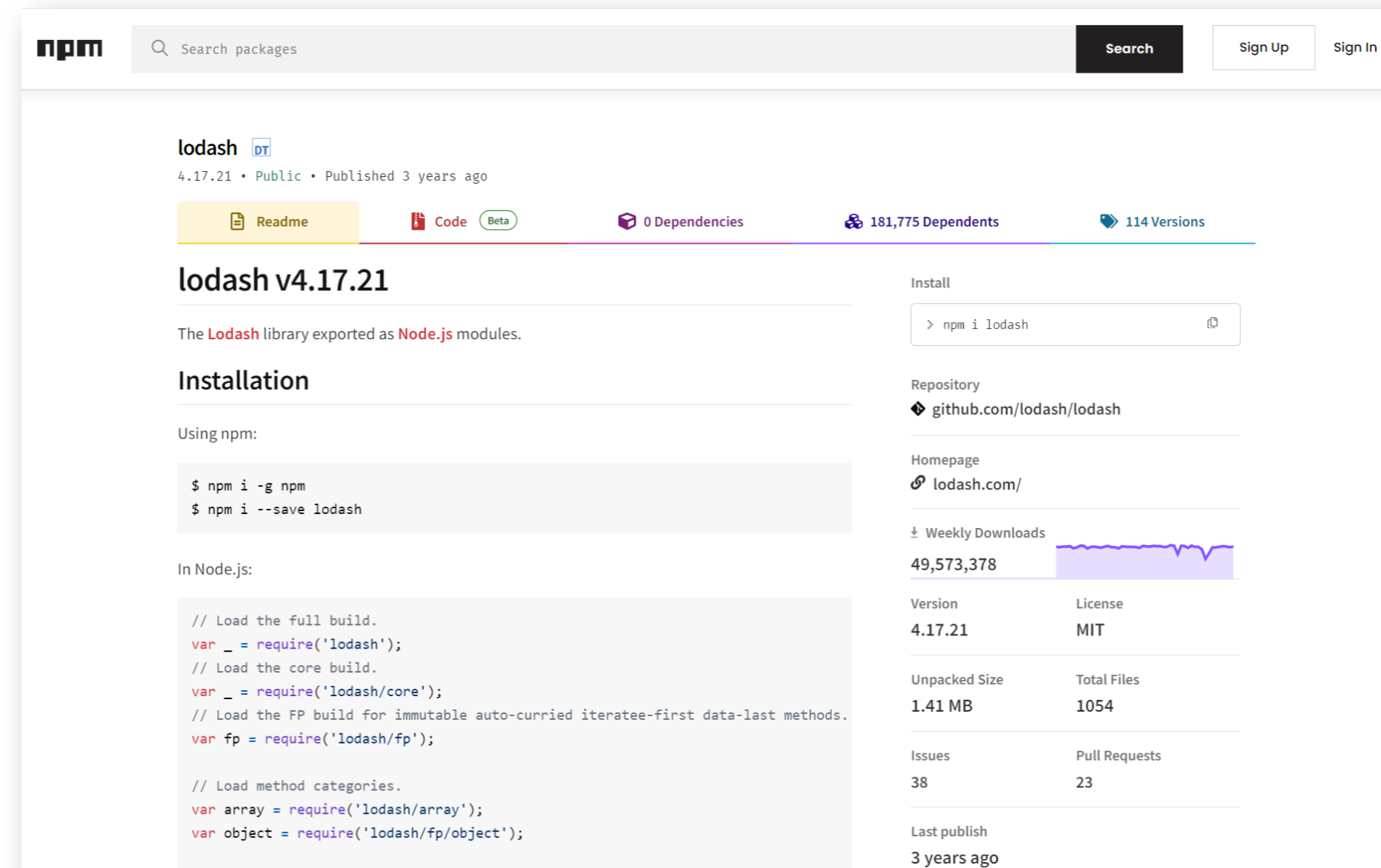
Weekly Downloads: 69

Version	License
1.0.0	ISC

Unpacked Size	Total Files
1.05 kB	2

Last publish: a day ago

Collaborators: 



lodash 4.17.21 • Public • Published 3 years ago

0 Dependencies 181,775 Dependents 114 Versions

lodash v4.17.21

The Lodash library exported as Node.js modules.

Installation

Using npm:

```
$ npm i -g npm
$ npm i --save lodash
```

In Node.js:

```
// Load the full build.
var _ = require('lodash');
// Load the core build.
var _ = require('lodash/core');
// Load the FP build for immutable auto-curried iteratee-first data-last methods.
var fp = require('lodash/fp');

// Load method categories.
var array = require('lodash/array');
var object = require('lodash/object');
```

Install: `> npm i lodash`

Repository: github.com/lodash/lodash

Homepage: lodash.com/

Weekly Downloads: 49,573,378

Version	License
4.17.21	MIT

Unpacked Size	Total Files
1.41 MB	1054

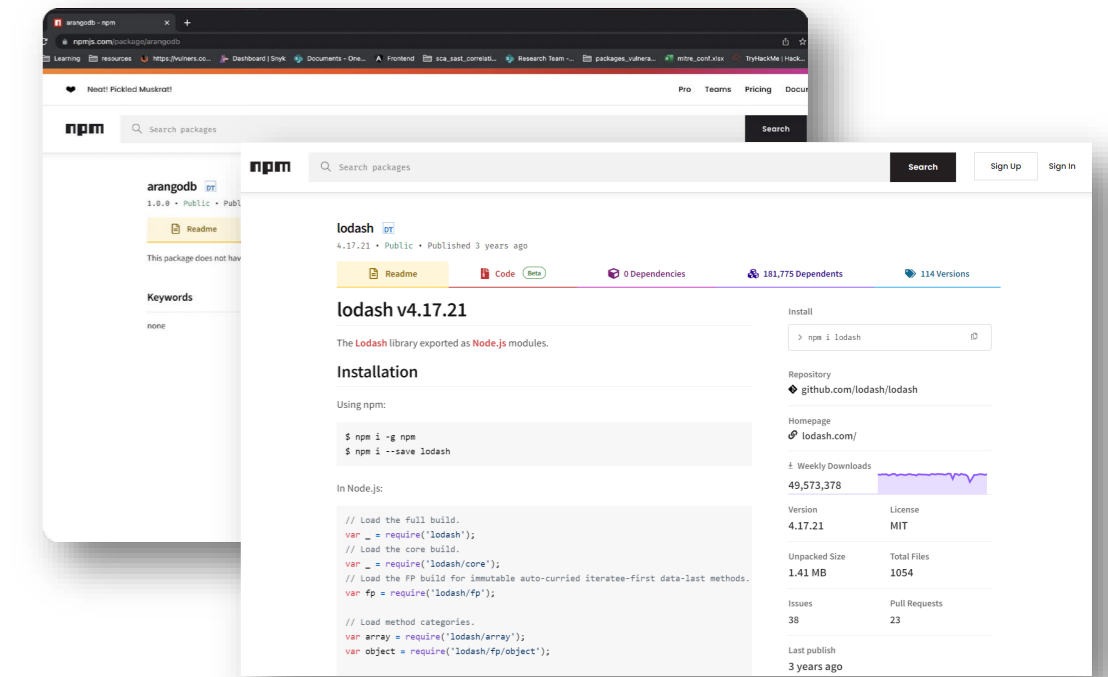
Issues	Pull Requests
38	23

Last publish: 3 years ago

Protecting your code from AI nightmares

1.Verification: Always verify the existence and credibility of recommended tools, libraries, or packages by searching them on official platforms like PyPI (Python Package Index), GitHub, or documentation from reputable sources.

2.Community Consultation: Consult with the community or forums like Stack Overflow, Reddit, or specific tech community forums. Real user experiences and discussions can provide validation.



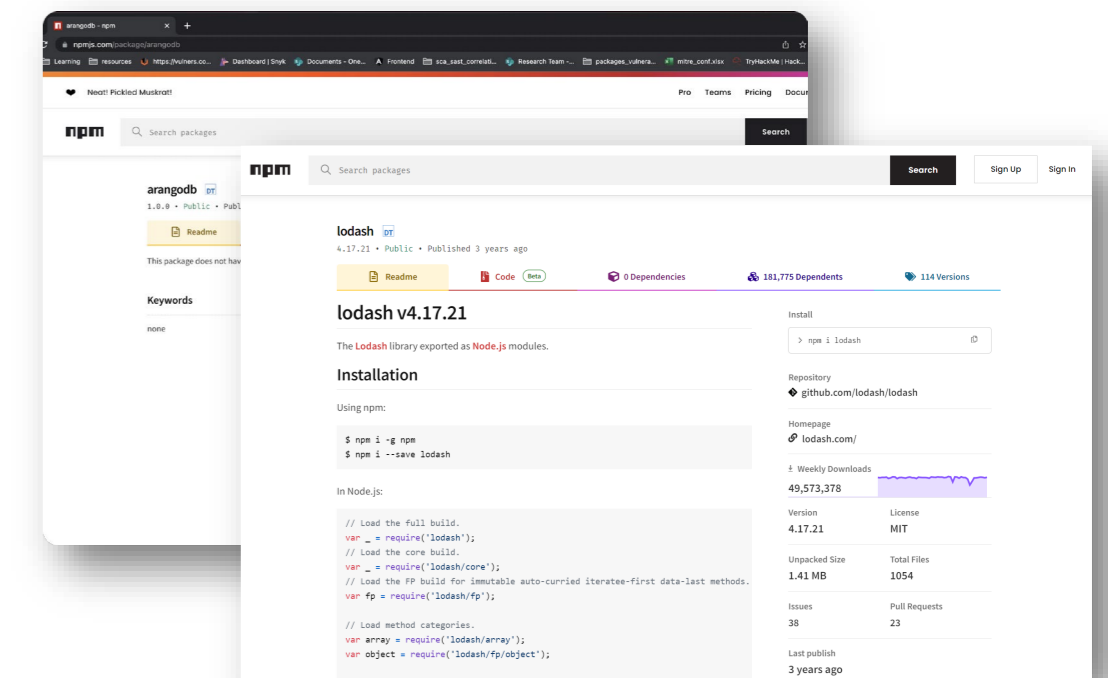
Protecting your code from AI nightmares

1.Verification: Always verify the existence and credibility of recommended tools, libraries, or packages by searching them on official platforms like PyPI (Python Package Index), GitHub, or documentation from reputable sources.

2.Community Consultation: Consult with the community or forums like Stack Overflow, Reddit, or specific tech community forums. Real user experiences and discussions can provide validation.

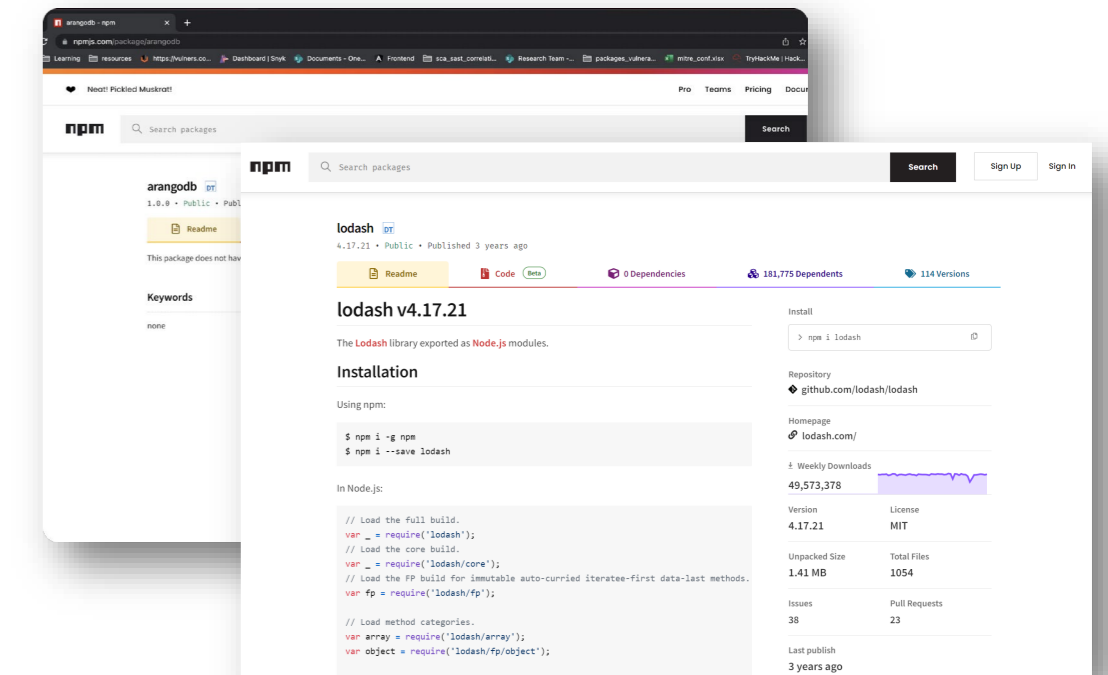
3.Official Documentation: Look for official documentation or tutorials. Legitimate libraries typically have well-maintained documentation.

4.Cross-Reference: Check multiple sources to confirm the information. If only one source mentions the tool and no other corroborating evidence exists, it might be incorrect.



Protecting your code from AI nightmares

- 1.Verification:** Always verify the existence and credibility of recommended tools, libraries, or packages by searching (e.g., PyPI (Python Package Index), GitHub, or documentation).
- 2.Community Consultation:** Consult forums like Stack Overflow, Reddit, or specific tech communities. Discussions can provide validation and user experiences and testimonials.
- 3.Official Documentation:** Legitimate libraries typically have well-maintained official documentation.
- 4.Cross-Reference:** Check multiple sources. If only one source mentions the tool and no others exist, it might be incorrect.
- 5.Experimentation:** If you find a library and it seems legitimate, experiment with it in a safe, controlled environment to understand its functionalities and limitations.

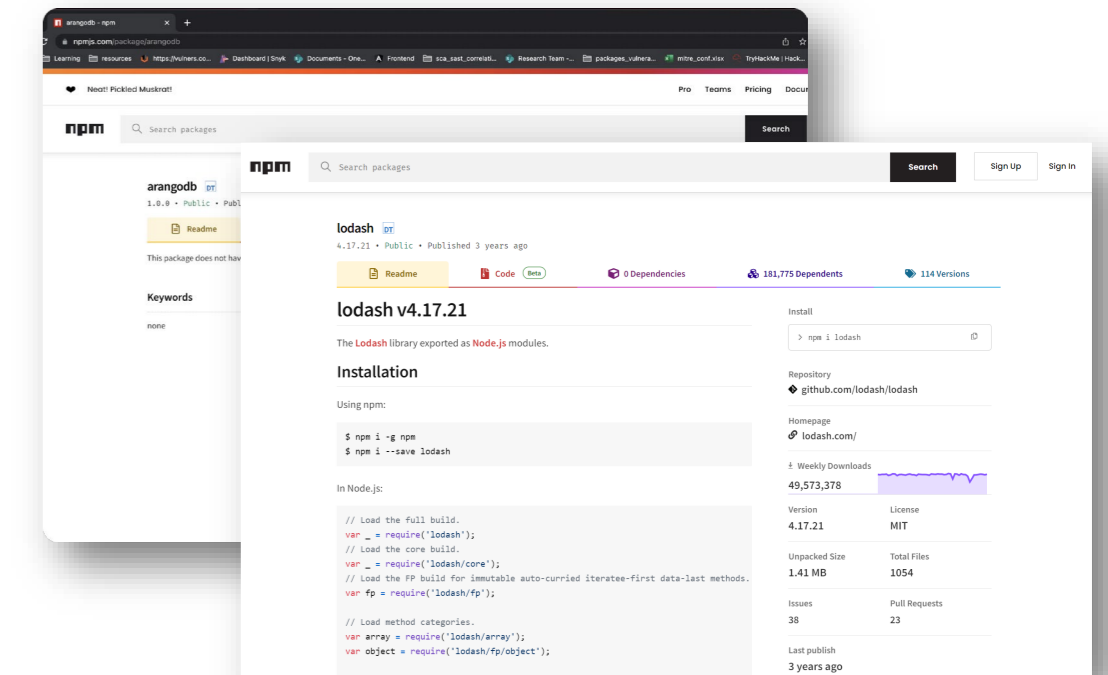


Protecting your code from AI nightmares

- 1.Verification:** Always verify libraries, or packages by searching (e.g. NPM Package Index), GitHub, or other sources.
- 2.Community Consultation:** Engage with communities like Stack Overflow, Reddit, or specific forums. Discussions can provide valuable insights.
- 3.Official Documentation:** Legitimate libraries typically have well-maintained documentation.
- 4.Cross-Reference:** Check multiple sources. If only one source mentions the tool and others don't, it might be incorrect.
- 5.Experimentation:** If you're unsure, experiment with the tool in a safe, controlled environment to identify any limitations.
- 6.Update Awareness:** Stay updated with the latest developments in your field of interest. Knowing the most commonly used and trusted libraries can help you quickly spot out-of-place recommendations.



Recommended tools, including Python, JavaScript, and others. Like Stack Overflow, GitHub, and other sources. Legitimate libraries typically have well-maintained documentation. If only one source mentions the tool and others don't, it might be incorrect. Experiment with the tool in a safe, controlled environment to identify any limitations.



Protecting your code from AI nightmares

1.Verification: Always verify the existence and credibility of recommended tools, libraries, or packages by searching them on official platforms like PyPI (Python Package Index), GitHub, or documentation from reputable sources.

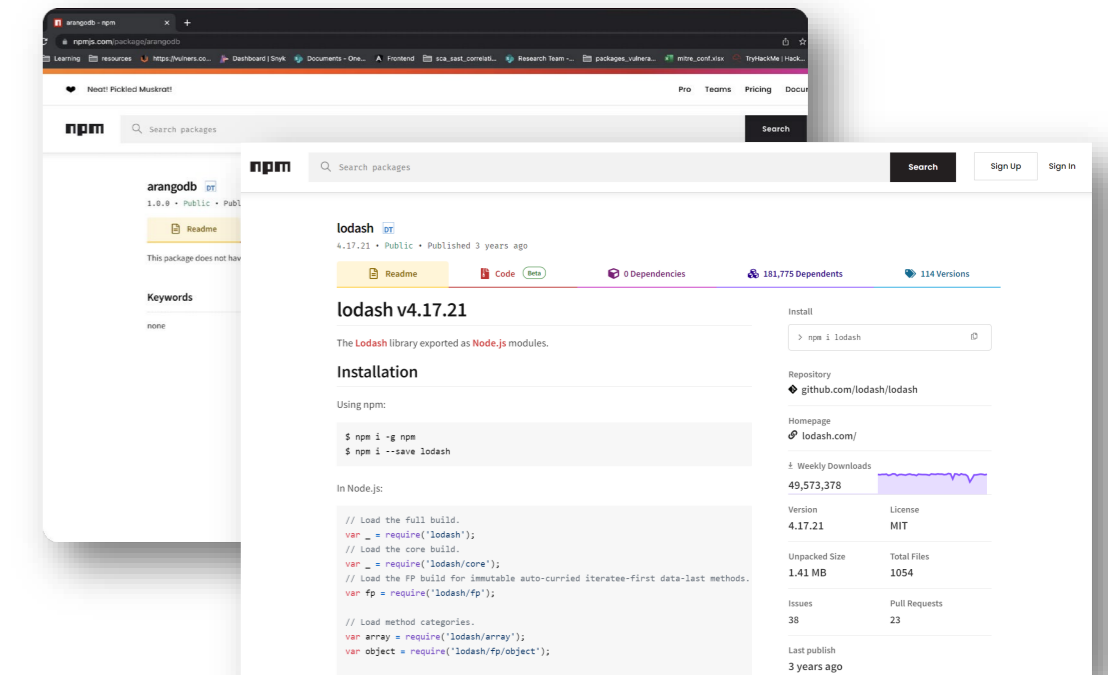
2.Community Consultation: Consult with the community or forums like Stack Overflow, Reddit, or specific tech community forums. Real user experiences and discussions can provide validation.

3.Official Documentation: Look for official documentation or tutorials. Legitimate libraries typically have well-maintained documentation.

4.Cross-Reference: Check multiple sources to confirm the information. If only one source mentions the tool and no other corroborating evidence exists, it might be incorrect.

5.Experimentation: If you find a library and it seems legitimate, experiment with it in a safe, controlled environment to understand its functionalities and limitations.

6.Update Awareness: Stay updated with the latest developments in your field of interest. Knowing the most commonly used and trusted libraries can help you quickly spot out-of-place recommendations.





TECH 'Everyone is a programmer' with generative AI

PUBLISHED MON, MAY 25

Lim Hui Jie

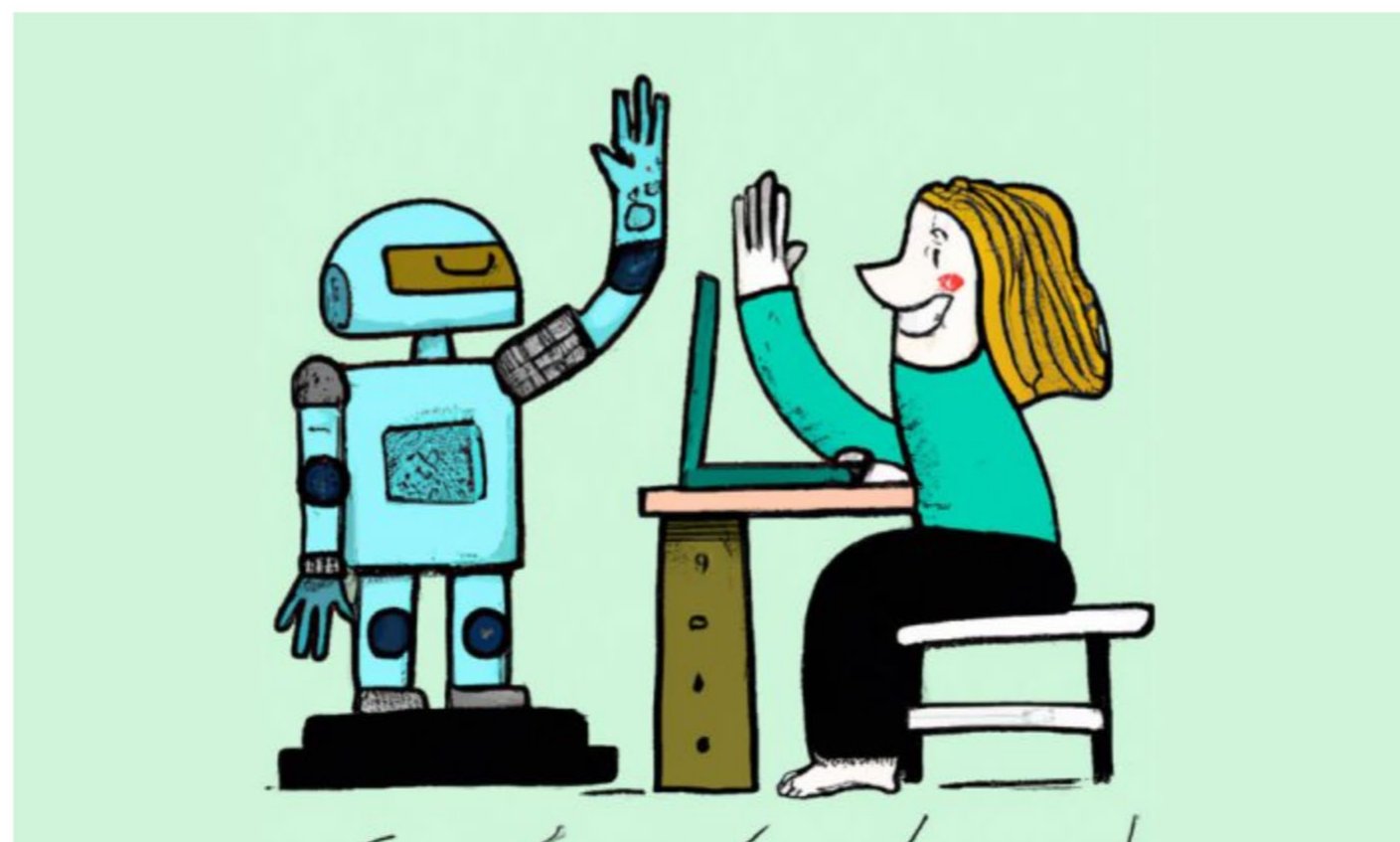
5 MIN READ

NO HUMAN CODERS IN 5 YEARS?

Apr 30, 2023

Will AI Render Programming Obsolete?

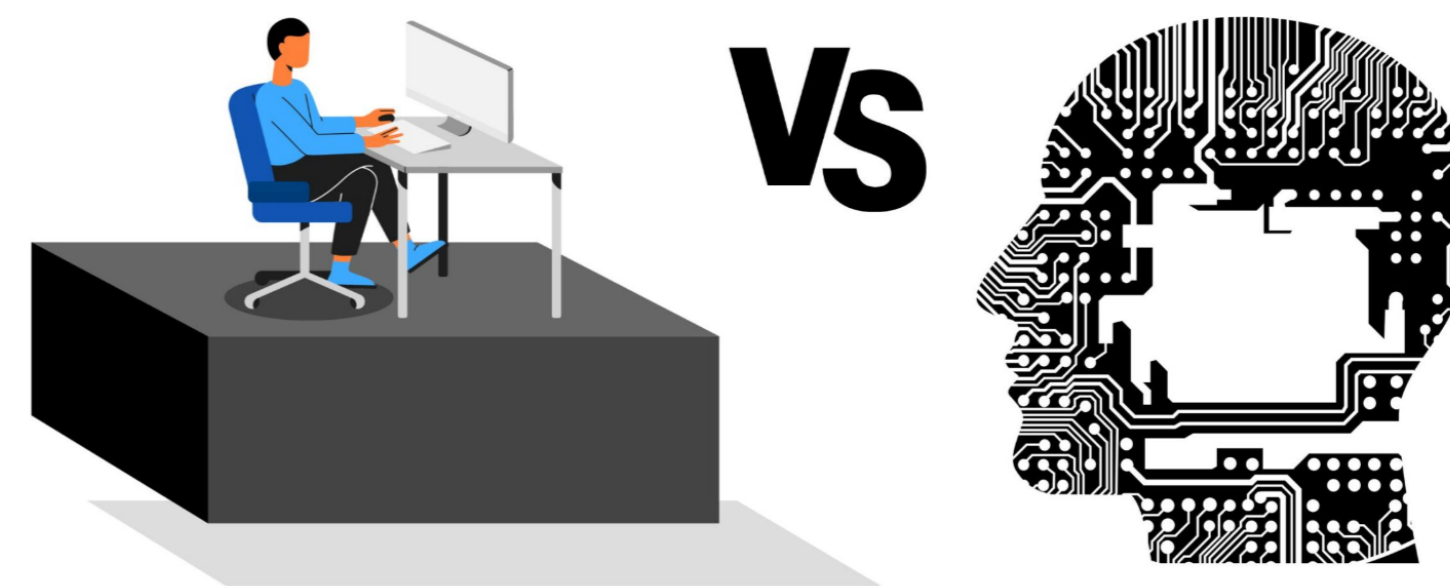
It's exhilarating to think that, with the help of generative AI, anyone who can write can also write programs. It's not so simple.



By: Michael L. Littman

Aa x share like retweet

TURING



Last updated on February 20th, 2024 at 02:26 pm

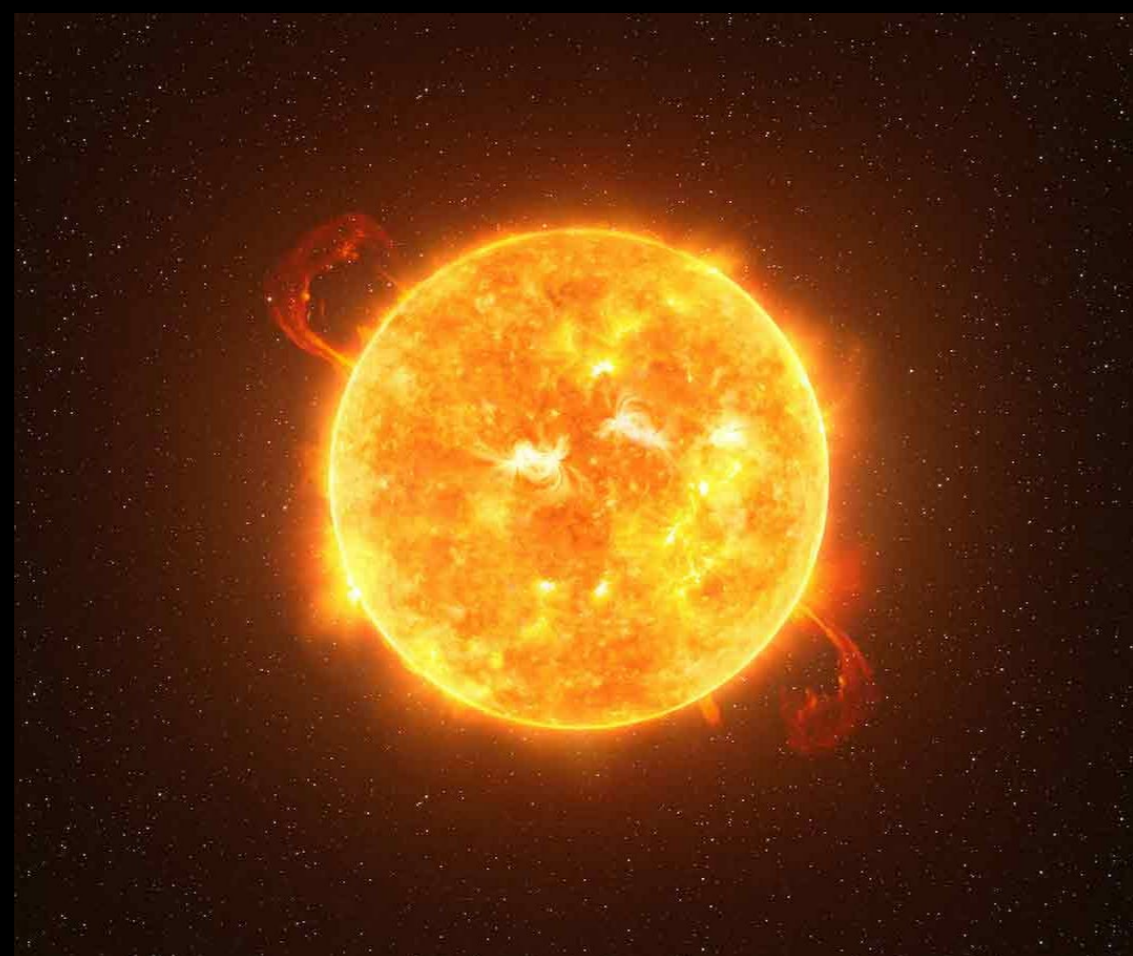
SOFTWARE COMPARISONS

ChatGPT vs Software Developers: Is Generative AI the End of the Road for Developers?

By Ritvik Gupta • September 6, 2023 • 13 min read

Listen to Post

Wonderous new technology, with emerging attack vectors



and yes, devastating potential



However, safeguards are already underway



[Administration](#) [Priorities](#) [The Record](#)

OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

 [BRIEFING ROOM](#) [PRESIDENTIAL ACTIONS](#)

The image shows a screenshot of a White House website page. At the top center is the White House logo. To the right are three navigation links: "Administration", "Priorities", and "The Record". Below this is the date "OCTOBER 30, 2023". The main heading is "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence". At the bottom, there is a horizontal line with a small icon of a building, followed by the text "BRIEFING ROOM" and "PRESIDENTIAL ACTIONS" separated by right-pointing chevrons.

With the right precautions and practices...



With the right precautions and practices...



But never trust cyborgs ;-)

Questions?