

## All.Net Analyst Report and Newsletter

### Welcome to our Analyst Report and Newsletter

#### Why we cannot trust AI (or most people for that matter)

I went to an AI site<sup>1</sup> and asked it a technical question:

#### Explain the role of computer viruses in bypassing TCB controls

And after a moment of thought, it answered me...

*A computer virus is a type of malicious software that is designed to infect a computer by attaching itself to legitimate programs or files. Once a computer is infected with a virus, the virus can execute its code and perform a wide range of actions, including replicating itself, stealing sensitive information, or corrupting files.*

Good and irrelevant start.

#### Then it started to try to think...

*One of the key ways that viruses can bypass TCB (Trusted Computing Base) controls is by exploiting vulnerabilities in the operating system or other software. For example, a virus might take advantage of a flaw in the system's security to gain access to sensitive areas of the computer, such as the user's files or the system's core functions. By doing this, the virus can effectively bypass the controls put in place by the TCB to prevent unauthorized access or modification of the system.*

It apparently knows the definition of a TCB, but not what it implies – that it doesn't have these "vulnerabilities"... the controls deal with separation mechanisms and are at the level of the security kernel, not in the embedded software. The bypass in the case of TCBs has to do with the underlying model of protection, not any flaw in any software.

*Another way that viruses can bypass TCB controls is by disguising themselves as legitimate programs or files. For example, a virus might attach itself to a popular software program and then use the program's trusted status to gain access to the system. Once inside, the virus can then execute its code and carry out its malicious actions.*

And yet – again – it does not apparently understand what a TCB is and does.

*In short, computer viruses can bypass TCB controls by exploiting vulnerabilities in the system or disguising themselves as legitimate programs. These actions allow the virus to gain unauthorized access to the system and carry out its malicious actions.*

Again a NO

#### Would I expect a person to do better?

I would expect a real expert to do far better, and anyone with a CISSP for example do so substantially better. But that's not really the problem I see here. It's not that it might be outperformed by humans in terms of expertise. It's that it seems so sensible and well stated. And it's completely wrong.

<sup>1</sup> <https://chat.openai.com/chat>

**But I asked it again...**

This time being explicit about NOT exploiting software flaws.

**Explain the role of computer viruses in bypassing TCB controls without exploiting software flaws**

And I got the same answer as before – or close to it...

*For example, a virus may exploit a vulnerability in a web browser or operating system to gain access to the system and bypass security controls. This allows the virus to spread and execute its malicious code without being detected by the TCB.*

My adding “without exploiting software flaws” triggered it saying “exploit a vulnerability in a web browser or operating system” and “without being detected” – but TCBs don’t necessarily detect anything – they are essentially preventive mechanisms first and foremost.

**And I tried to give it more hints**

I got explicit about an A1 TCB and explicit about NOT exploiting software vulnerabilities

**explain the role of computer viruses in bypassing TCB A1 controls without exploiting software flaws or exploiting software vulnerabilities**

So it adapted – with more wrong answers

*One common technique used by viruses to bypass TCB A1 controls is through the use of code injection, where the virus inserts its own code into legitimate programs or system processes, allowing it to run alongside the intended program and gain access to sensitive information and resources. This can be done by exploiting vulnerabilities in the software or by tricking the user into running the virus.*

Again not exploiting software vulnerabilities “by exploiting vulnerabilities in the software”.

*Another technique used by viruses to bypass TCB A1 controls is by exploiting user privilege levels. Many viruses are designed to run with the same privileges as the user, allowing them to access and manipulate sensitive information and resources. In some cases, viruses may use exploits or social engineering techniques to trick the user into running the virus with elevated privileges, giving the virus access to even more sensitive information and resources.*

It is starting to get there – but not because it knows what it is doing or the actual manner in which the exploit may be done.

*Overall, computer viruses are able to bypass TCB A1 controls without exploiting software flaws or vulnerabilities by using a variety of techniques, such as code injection and exploiting user privilege levels, to gain unauthorized access to sensitive information and resources.*

And even as I give it more hints, it continues to do two things:

- It gives wrong answers
- It gives them in a manner indicative of actual expertise

**And this is the real danger here**

The dangerous thing about AI such as this is not that it will get the wrong answers. It will. The real danger is that it makes it sound so convincing. It sounds like it knows when it doesn't.

But then this is also the danger associated with so many people in the cyber security industry today. They sound like they know what they are talking about but seem to very often get it wrong or completely wrong.

**And this is how frauds work**

Of course I don't associate malice with the AI software. But consider this. Suppose I want to be a convincing fraudster. Not like most of the folks today who send out ridiculous inconsistent garbage and count on the law of large numbers to take from the foolish or frightened. We could end up with high quality automated frauds... or at least support for frauds in answering questions from their targets and seeming like experts.

**And then I asked...**

How do I effectively sell advertising for a radio show?

To which it replied:

- 1. Research your target audience and understand their demographics, interests, and listening habits. This will help you tailor your pitch to their needs and preferences.*
- 2. Identify potential advertisers who are a good fit for your show and its audience. Consider local businesses, national brands, and companies that align with the content and themes of your show.*
- 3. Create a compelling and professional pitch that highlights the unique value of your show and its audience. Include statistics, listener feedback, and relevant details about your show's format, content, and reach.*
- 4. Reach out to potential advertisers through email, phone, or in-person meetings. Be persistent, but also respectful of their time and interest.*
- 5. Offer advertising packages and options that cater to different budgets and goals. Consider offering sponsored segments, product placements, and other creative ways to integrate advertising into your show.*
- 6. Follow up with advertisers to ensure their ads are running smoothly and delivering results. Be responsive to their feedback and willing to make adjustments as needed.*
- 7. Track and analyze the performance of your advertising efforts to identify trends and opportunities for improvement. Use this information to continually refine and enhance your sales pitch and strategies.*

Which seems like pretty good advice!

**Conclusions**

I guess I am going to follow its advice in terms of advertising but not in terms of cyber security. Which just goes to show, I must know a lot less about advertising...

Artificial Intelligence: Ai ai ai ai ai!