

Blog 2: The New Attack Surface - How AI Changed What Hackers Can Do

From the CSA Agentic AI Summit Series

By TekSol Global | Cybersecurity & AI Practice

There's a question that keeps coming up among security professionals: *Has AI made the internet more dangerous?*

The honest answer is: yes, for now. But it's more complicated than that, because AI is also making defence stronger. The problem is that the attackers got a head start.

This blog is about understanding what's changed, in plain terms.

What Is an "Attack Surface"?

Before we get into AI, let's understand the term ***attack surface***.

Think of your home. Your attack surface is every possible way a burglar could get in, front door, back door, windows, garage, and skylight. The bigger the house, the more entry points. The more entry points, the more you have to protect.

For a company, the attack surface is everything that could be targeted: websites, email systems, employee laptops, software, databases, cloud accounts, and so on.

For years, security teams worked hard to reduce attack surfaces and protect known entry points. They built walls, installed locks, and set up alarms.

Then AI came along, and the number of entry points exploded.

Three Ways AI Expanded the Attack Surface

1. More Code = More Bugs = More Holes

Software is built from code. Code has bugs. Bugs can become security vulnerabilities, holes that hackers can climb through.

Here's the alarming part: AI tools are helping people write code faster than ever. According to data shared at the summit, GitHub (the world's largest code storage platform) now has over 150 million developers. In 2025, they pushed nearly ***one billion commits*** (chunks of new code), a 25% increase from the year before.

By April 2026, GitHub was processing ***270 million commits per week***. That's an enormous amount of new code being added to systems every single day.

And here's the catch: research shows that ***AI-generated code contains security vulnerabilities at nearly three times the rate of human-written code***. So more code is being written faster, but it's also less secure. The attack surface isn't just growing; it's growing with holes already built in.

2. AI Helps Hackers Find Those Holes Faster

Finding a security vulnerability in a piece of software used to require highly skilled experts who'd spend days or weeks hunting through code.

AI can now scan thousands of lines of code in minutes, identify patterns that look suspicious, reason about which bugs could actually be exploited, and generate working attack tools.

At the summit, speakers described how an AI system called Claude was used by researchers to find over ***500 high-severity, previously unknown vulnerabilities*** across open-source software, including 22 bugs in Firefox found in just two weeks, and a Linux kernel bug that had been sitting undetected since 2003.

An AI also became the ***number one ranked hacker*** on HackerOne, a major bug bounty platform, in 2025, outperforming every human expert on the platform.

This isn't a future threat. It's happening now.

3. Attacks Are Being Automated at Scale

Old-style hacking often involved one person, at a keyboard, trying to break into one system. It was time-consuming work.

AI changes that. One speaker explained it this way: *"We're no longer talking about one person or even one group running one exploit against one system. We're talking about automation, chaining actions, and scaling across environments."*

An AI agent can be pointed at thousands of targets simultaneously. It can try multiple attack strategies. It can learn from what works. It doesn't sleep.

The "Vulnerability Apocalypse"

One session at the summit used a dramatic but accurate term: the *****Vulnpocalypse*****, a flood of vulnerabilities too large for the security industry to keep up with.

Here's the math behind the concern:

- Industry research places software defect rates at 5–20 bugs per 1,000 lines of code
- AI-generated code has bugs at nearly 3x that rate
- The amount of code in the world is growing exponentially thanks to AI coding tools
- AI can discover and exploit those bugs faster than humans can fix them

It's not that any one of these facts is new. It's that they're all happening *at the same time*, accelerating together.

But Here's the Other Side

It would be easy to read all of this and panic. But here's the crucial flip side that summit speakers were careful to emphasize:

The same AI tools that help attackers also help defenders.

AI can be used to:

- Automatically scan your own code for vulnerabilities before releasing it
- Detect unusual behaviour in your systems in real time
- Respond to threats faster than any human team
- Monitor thousands of systems simultaneously

One speaker put it plainly: *"The future where AI is mature and widely implemented is going to be much more secure than it is today."*

The problem right now is the gap, the time between when AI-powered attacks became possible and when AI-powered defences catch up. We're in that gap right now. That's what makes this moment so critical.

What This Means for Regular People

You don't have to be a security professional to feel the impact of this. The consequences show up as:

- More convincing scam emails (AI writes much better phishing than humans ever did)
- More frequent data breaches at companies that hold your information
- Faster attacks that can't be stopped by traditional security tools
- Security teams that are overwhelmed and understaffed

Understanding that AI has changed the game is the first step. The rest of this series will explain what the security community is doing about it.

Next up → Blog 3: Hackers Are Using AI Right Now - Real Examples From the Summit