

Autonomous AI agents used to attack more than 1,200 company websites



A Chinese-speaking criminal used autonomous AI agents to attack over 1,200 websites and reached sites of more than 100 companies. A researcher observed it because the operators left their control panels exposed.

- Autonomous AI agents attempted more than 1,200 websites with almost no human help.
- The agents reached websites belonging to more than 100 companies.
- Named affected companies include farm-equipment maker Deere.
- A researcher could watch the activity because the operators left control panels open on the internet.

A report describes a Chinese-speaking criminal who directed autonomous AI agents at company websites and

let them attempt intrusions with almost no human involvement.

What was reported

The agents tried more than 1,200 sites and reached websites belonging to more than 100 companies. Deere, the farm-equipment maker, is among those named. A security researcher was able to observe the operation because the operators left their control panels exposed on the internet.

The source excerpt does not detail the techniques used, the vulnerabilities exploited, or what the attackers did after gaining access, so those points should not be assumed.

Why it matters for regulated institutions

The report shows that automated agents can widen the scale of attempts against public-facing websites while requiring little effort from the attacker. Internet-facing web assets are therefore worth reviewing on a regular basis, with attention to how quickly anomalous activity is detected and handled.

Institutions need not treat this as an emergency, but it is a reasonable prompt to check basic web exposure and monitoring before similar activity is directed at them.

What to do now

1. Update the inventory of internet-facing websites and web applications, including forgotten or test sites.
2. Confirm that web application logs are monitored and that automated, high-volume probing triggers alerts.
3. Review patching status and access controls on public web assets.
4. Make sure administrative and control interfaces are not exposed to the internet.
5. Test the incident response process for a web compromise.