Ransomware attacks rise with AI use, but ransom payments decline



Dark Reading reports that more ransomware groups are using AI to write convincing phishing emails and find sensitive data quickly. Attacks are increasing, while ransom payments are declining.

- Ransomware attacks are increasing, according to the report.
- Ransom payments are declining despite the rise in attacks.
- Large language models and other AI systems help groups craft convincing phishing emails.
- AI also helps attackers identify sensitive data quickly.

A Dark Reading report describes a shift in the ransomware landscape: attacks are increasing, driven in part by AI, while payments made to attackers are declining.

What the report says

According to the source, large language models and other AI systems allow a growing number of ransomware groups to produce convincing phishing emails and to identify sensitive data quickly. These two capabilities lower the effort needed to gain a foothold and to decide what to steal or encrypt.

The source headline also points to a decline in payments. The excerpt available to us does not give figures, time periods or reasons, so we do not draw conclusions about causes or scale.

What it means for institutions

The practical point is that phishing that reads naturally is harder for staff to spot by language quality alone, and that attackers can locate valuable data faster once inside. A fall in payments should not be read as a fall in risk, since attack volume is reported to be rising.

Regulated institutions are best served by reviewing the basics that limit both the entry point and the impact: email defenses, user awareness, knowing where sensitive data resides, and tested recovery. These steps reduce exposure whether or not a ransom is ever paid.

What to do now

1. Review email security controls and phishing detection, assuming lures will be well written and free of obvious language errors.
2. Update awareness training to stress verification of unusual requests rather than spotting poor grammar.
3. Map where sensitive data is stored and tighten access and monitoring around it.
4. Test backup restoration and the ransomware response playbook, including decision-making on ransom demands.
5. Report progress against your NCA ECC and SAMA CSF controls on email protection, data protection and incident response.