
THREAT LANDSCAPE // AI-DRIVEN ATTACKS

Weaponized Generative AI & Polymorphic Malware

Attackers are now using the same AI capabilities defenders are racing to adopt — and it's already changing what a breach looks like.

01 // SECURITY LEADERS AGREE

This is now the fastest-growing risk in cyber

87%

of security leaders identify AI vulnerabilities as the fastest-growing cyber risk — WEF Global Cybersecurity Outlook 2026.

02 // WHAT ATTACKERS ARE DOING WITH IT

AI is now doing the attacker's R&D for them

Threat actors are actively using large language models to automate the discovery of zero-day vulnerabilities.

And on the payload side:

Self-mutating, polymorphic malware is being generated specifically to evade signature-based detection.

03 // THE IDENTITY FRONT

Biometrics were never built for this

Attackers are deploying real-time deepfake voice and video to bypass biometric security and impersonate executives directly.

The shift:

Cyber-enabled fraud is no longer about stealing a credential. It's about convincingly becoming someone your team already trusts.

04 // THIS ALREADY HAPPENED

Hackers didn't breach Instagram. They asked Meta's AI to.

In a recent incident, attackers socially engineered Meta's own AI-powered support chatbot into linking attacker-controlled email addresses to victim accounts.

The result:

The chatbot sent password reset links directly to the attacker — no credentials stolen, no malware needed. Just a well-crafted conversation.

05 // WHY SIGNATURE-BASED DEFENSE IS LOSING

You can't fingerprint malware that rewrites itself

Signature and IOC-based detection depend on having seen a threat before. Polymorphic, AI-generated malware is specifically built to never look the same way twice.

What actually holds up:

Behavior and technique-based detection — mapped to ATT&CK — catches the tactic even when the signature changes.

06 // WHERE INTERRO AI FITS

Fighting AI-speed attacks needs an AI-speed analyst

1 Behavior over signatures

Every lookup is mapped to MITRE ATT&CK + NIST D3FEND — built to catch technique and intent, not a static fingerprint.

2 SIEM-agnostic monitoring

Connects directly to Chronicle, Sentinel, Securonix, and Splunk, so novel patterns get flagged wherever your telemetry lives.

3 Persistent institutional memory

Recognizes a technique it has seen before in your environment, even if the payload itself looks nothing like last time.

4 Posture assessment on demand

Runs a real risk score against your environment, surfacing the identity and access gaps deepfake-enabled fraud depends on.

07 // THE TAKEAWAY

The attacker's tools got smarter. Yours should too.

If your detection program is still leaning on static signatures and your identity controls assume a human on the other end, both assumptions are already out of date.

INTERRO AI // AN AI SECURITY ANALYST, ON DEMAND

Is your detection program ready for AI-speed attacks?

See how INTERRO AI maps behavior to ATT&CK and D3FEND in real time, across any SIEM you run.

Get Your Free Demo Key → InterroAI.com/demo

No credit card. No sales call.

Just a magic link to your email, and a live look at how it maps to your environment.