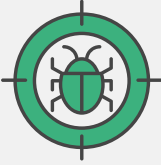




AI and automation are accelerating cyberattacks.

Key Findings

RECONNAISSANCE



BILLIONS
of malicious scans
detected daily by
FortiGuard

EXPLOITATION SPEED



<48 HOURS
from vulnerability
disclosure to
active exploit

ATTACK VOLUME



+26%
increase in
automated
attack activity

Shifting Attack Methods

CREDENTIAL THEFT



**Attackers don't break in.
They log in.**
Attackers have shifted from brute-force password attacks to using stolen credentials—usernames, passwords, cookies, and session tokens now drive most intrusions.

Brute force attacks **-22%**

AI-DRIVEN ATTACKS



Automation runs threats at scale
AI enables attackers to continuously conduct reconnaissance, testing, and exploitation across thousands of targets simultaneously.

Operations run **24/7**

Evolution Over Time

Then	Trend	Now
How attacks have changed		
Manual attacks	→	AI-assisted
Password guessing	→	Credential access
Periodic scans	→	Continuous scanning
7 days	→	<48 hours
Campaigns	→	Continuous operations

Defender Reality

Speed wins. Detection time determines security outcomes.

See the Data Behind These Trends

Download the 2026 Global Threat Landscape Report