2025

elastic security labs

GLOBAL THREAT RESEARCH REPORT

EXECUTIVE SUMMARY

The age of patient, stealthy attacks is giving way to a new era of high-velocity threats.

Our year-over-year analysis reveals a clear strategic shift: adversaries are retooling for speed, weaponizing AI to generate novel threats at scale, and prioritizing immediate execution over prolonged stealth. This acceleration forces defenders to adapt to an attack lifecycle measured in minutes, not months, where rapid, context-rich decisions drawn from both real-time and historical data have become the key to effective defense.

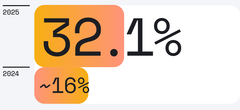
The 2025 Elastic Global Threat Report from Elastic Security Labs breaks down this new landscape.

Based on our analysis of global threat telemetry, we've identified the adversary behaviors and defensive innovations that matter most. Here's a preview of what you'll learn:

#01

Adversary priorities on Windows have flipped

The tactic category of **Execution** now accounts for **32.1%** of malicious behavior—doubling its previous share of ~16%—and surpassing **Defense Evasion** as the top tactic. This disrupts a three year trend and indicates a strategic shift toward immediate payload deployment over initial stealth.

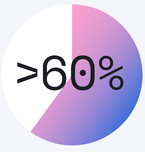


WHAT THIS MEANS FOR YOU

→ Attackers are no longer waiting to hide; they are focused on running malicious code immediately upon entry. This makes runtime memory protection and initial access prevention more critical than ever.

#02

The cloud attack surface is highly concentrated



Over 60% of all cloud security events boil down to just three adversary goals:

adversary goals

/Initial Access
/Persistence
/Credential Access

WHAT THIS MEANS FOR YOU

→ Across all major cloud platforms, this laser focus on **identity-based attacks** is a clear signal that hardening authentication flows and monitoring for anomalous privileged access are the most effective ways to defend your cloud workloads.

#03

AI weaponization is on the rise

+15.5%

We saw a 15.5% increase in 'Generic' threats, a trend likely fueled by adversaries using LLMs to quickly generate simple but effective malicious loaders and tools.

WHAT THIS MEANS FOR YOU

→ The rise of AI-generated threats dramatically increases the volume and variety of malware you face. This means relying less on static signatures and more on **behavioral analytics and AI-driven detection** to automatically identify and stop the flood of novel threats at scale.

#04

Browser credential theft is big business

>1 in 8

designed to steal browser data

Our analysis of over **150,000 malware** samples revealed that more than 1 in 8 are designed to steal browser data. This isn't for isolated use; these credentials are the raw material fueling the **access broker economy**, providing a steady supply of keys for other attackers to compromise corporate cloud accounts.

WHAT THIS MEANS FOR YOU

→ The browser is a primary battleground for your organization's most sensitive data. Infostealers have adapted to built-in browser protections, which means traditional identity controls are no longer enough.

These trends are deeply interconnected.

An adversary can use AI-generated malware to steal browser credentials, which are then used to gain initial access to a cloud account. Once inside, they immediately focus on execution to deploy ransomware or steal data. This report connects the dots, showing how these TTPs form the modern attack chain and, more importantly, how to break it at multiple points.

The threat landscape is complex, but by understanding malware and threat behaviors and leveraging advanced defenses, organizations can significantly improve their resilience.

STEP #1
focus on execution

STEP #2
gain initial access to a cloud account

STEP #3
use AI-generated malware

STEP #4
steal browser credentials

Elastic Security delivers the shared intelligence, advanced capabilities and insights you need to navigate today's threats and build a more secure future.