

# THE 2025 IDENTITY THREAT LANDSCAPE

## IDENTITY ATTACKS ARE ON SECURITY TEAMS' RADARS

### INCOMING TRANSMISSION

The perimeter has shifted, do you read?  
■■■

**SURVEY SAYS:**  
Responses from 500+ security professionals

Over 2/3 of organizations are significantly or extremely concerned about identity-based cyberattacks  
**Phishing, ransomware, and nation-state adversaries** make up the top three threats of concern for security teams



When it comes to initial access vectors, organizations are most concerned about **phishing, supply chain exposures, and malware infections** leading to follow-on attacks

## NO END IN SIGHT FOR MALWARE

Nearly one in two corporate users have been victims of an infostealer infection some time in their digital history

**LummaC2** dominated the infection count in 2025

## LEADING ENTRY POINTS FOR RANSOMWARE

**Phishing**



Exposed or weak APIs



Stolen cookies that enabled session hijacking



## OVERBLOWN CONFIDENCE

**86%** of security leaders express confidence in their ability to prevent major identity-based attacks

But **85%** were affected by ransomware in the past year

## AI IS FUELING THE PROBLEM

Nearly all security leaders (**92%**) acknowledge the threat of **AI-powered cybercrime** as a new driver of risk

GET THE 2025 IDENTITY THREAT REPORT ➤

# ***IDENTITY DEFENSE*** ***BLACK HOLES***

*IDENTITY EXPOSURES REQUIRE  
CONTINUOUS MONITORING AND REMEDIATION  
TO PREVENT ABUSE. **IT ONLY TAKES ONE EXPOSURE**  
**TO BRING DOWN THE SHIP...***

*BUT ACCORDING TO THE 2025 IDENTITY THREAT REPORT  
ORGANIZATIONS ARE STILL PLAYING CATCH-UP:*

**Only 50% of organizations** have visibility into infostealer malware infections on managed devices

**Only 41% of organizations** consistently revoke or reset credentials after a phishing attack, and **only 54% of organizations** routinely reset passwords after malware infections

**About 57%** don't have high capabilities to invalidate sessions exposed via malware

**A mere 38%** can detect historical identity exposures that create risk

**Less than 20%** are able to automate and optimize exposure remediation across systems

**About two-thirds** have no formal investigation protocols for identity-related incidents

Less than half of defenders (**47%**) have integrated AI into their own defenses

**GET THE 2025 IDENTITY THREAT REPORT** ➤



## IDENTITY THREATS AREN'T GOING AWAY

SpyCloud has recaptured **63.8 billion distinct identity records** from the dark web  
|  
A **24% increase** year-over-year

### TEAMS REPORT THEIR **TOP 4 PRIORITIES** OVER THE NEXT 12-18 MONTHS ARE:

- 1 Improved collaboration to break down silos and build new workflows
- 2 Stronger ransomware defenses
- 3 Investment in AI-powered tools
- 4 Better visibility and control over malware and phishing threats

**IDENTITY IS  
MISSION  
CRITICAL**

**IT'S TIME TO EXPAND YOUR  
MISSION SCOPE &  
DEFEND THE NEW PERIMETER**

**BENCHMARK YOUR PROGRAM & BUILD OPERATIONAL MATURITY TODAY**

**GET THE 2025 IDENTITY THREAT REPORT** ➤