Zscaler Research Finds Cybercrime Economics Are Shifting as AI Trades Mass Volume for Lethal Precision

June 10, 2026

While total phishing volume declined for the second year in a row, ThreatLabz identified 413,524 AI-generated site instances, underscoring how quickly adversaries can scale high-fidelity phishing

News Highlights

- **Quality Over Quantity:** Phishing volume fell 20% for the second year in a row as attackers recalibrate to high-fidelity, AI-accelerated lures.
- **Services Sector Surge:** Targeted hits against the Services sector jumped 65.5%, as adversaries exploit trust-based workflows like billing and renewals.
- **The Encryption Blind Spot:** 95.2% of phishing attempts now hide in encrypted traffic, bypassing legacy security stacks that lack deep TLS inspection.
- **"Text-to-Site" Weaponization:** ThreatLabz identified over 413,000 AI-generated phishing instances, proving how easily attackers can now spin up polished, malicious sites.
- **MFA Under Threat:** Sophisticated kits like "BlackForce" are being deployed to hijack active sessions and bypass multi-factor authentication in real-time.
- **Reconnaissance Exposed**: Deception telemetry recorded 89.9 million hostile interactions from 1.37 million unique attacker IPs in six months, revealing large-scale scanning and credential validation before compromise.

LAS VEGAS, June 10, 2026 (GLOBE NEWSWIRE) -- Zenith Live 2026 -- Zscaler, Inc. (NASDAQ: ZS), the cybersecurity platform for the AI era, today announced the release of the Zscaler ThreatLabz 2026 Phishing and Initial Access Report. Based on the comprehensive telemetry across the world's largest inline security cloud, spanning phishing activity, encrypted sessions, and deception decoy interactions, the research reveals a fundamental shift in the economics of cybercrime: while overall phishing volume dropped for the second consecutive year (down 20% year-over-year (YoY)), the effectiveness and sophistication of attacks have surged.

Threat actors are increasingly utilizing AI-powered "text-to-site" tools and real-time session hijacking kits to bypass multi-factor authentication (MFA). Crucially, adversaries are heavily cloaking these sophisticated campaigns, with 95.2% of phishing attempts now hiding within encrypted traffic to bypass legacy security stacks. Furthermore, newly unveiled deception telemetry, capturing nearly 90 million hostile interactions, reveals that attackers are aggressively scanning and probing enterprise identities and collaboration platforms long before the initial compromise occurs.

"We are witnessing a strategic recalibration in the way adversaries approach initial access," said Deepen Desai, Chief Security Officer, Zscaler. "The decline in raw phishing volume isn't a sign of retreat; it's a sign of evolution. Attackers are trading quantity for quality, using GenAI to eliminate traditional 'tells' like poor grammar and generic lures. With 95% of phishing now hiding in encrypted traffic, organizations can no longer afford to leave their TLS traffic uninspected. A Zero Trust architecture is the only way to break the attack chain, from discovery to data exfiltration."

How Adversaries Are Using GenAI for High-Fidelity Initial Compromise
The report highlights how AI has become the primary engine for modern intrusion. ThreatLabz identified 413,524 AI-generated site instances, with nearly 10% flagged as explicitly malicious. Tools like Manus AI, Blackbox AI, and Lovable AI are being weaponized to spin up polished, brand-consistent phishing portals in minutes, tasks that previously required days of manual development.

These AI-generated lures are particularly effective at mimicking trusted workflows. The Services sector bore the brunt of this shift, experiencing a 65.5% YoY surge in hits as attackers exploited trust-based interactions like billing, onboarding, and support renewals.

Additional Findings From the 2026 Report Include:

- **The Global Landscape:** The U.S. remains a top target for email phishing attacks; Brazil saw a 2,522% surge in phishing hosting, becoming a top-five global origin.
- **Industry Breakdown:** Manufacturing and Government remain primary targets for email phishing attacks, with Government hits up 50% as attackers pursue high-value intelligence.
- **Credential Harvesting Trends:** Microsoft and Google are the most imitated brands for phishing attacks, showing continued focus on compromising enterprise identity systems.
- **Detection Evasion:** Encryption is now the default for cybercriminals, with 87% of malicious activity delivered via HTTPS.
- **Hostile Scanning Activity:** Attackers are leveraging legitimate cloud infrastructure for reconnaissance, using over 121,000 unique Public Cloud-hosted IPs to probe environments.

Deception Technology Unmasks Attacker Intent
Zscaler telemetry from global decoys captured nearly 90 million hostile interactions across 1.37 million unique attacker IPs. This data confirms that adversaries are aggressively probing collaboration and identity platforms to find weak spots, and test assumptions about what defenses will give.

Mitigating the Path to Compromise
To counter these evolving threats, the Zscaler Zero Trust Exchange™ platform delivers the AI security platform built on Zero Trust that:

1. **Minimizes Attack Surface Discovery**: Reduces exposure by hiding applications behind a cloud-delivered proxy, while leveraging Deception technology to surface reconnaissance attempts via scanning, probing, and credential validation attempts early.
2. **Helps Eliminate Initial Compromise**: Blocks AI-enabled phishing and session-based attacks with AI-driven inline inspection, including full TLS/SSL inspection, to expose threats hiding in encrypted traffic.
3. **Stops Lateral Movement**: Connects users directly to applications and enforces Zero Trust access controls to prevent attackers from moving from a single foothold to broader environments.
4. **Prevents Data Loss**: Reduces breach impact with AI-powered data protection to identify sensitive data in motion and prevent unauthorized sharing or exfiltration.

For a deeper dive into the findings and best practices for securing your organization, download the full Zscaler ThreatLabz 2026 Phishing and Initial Access Report at https://www.zscaler.com/campaign/threatlabz-phishing-initial-access-report.

Methodology
ThreatLabz analyzed over 500 trillion daily signals from the Zscaler Zero Trust Exchange, blocking over 9 billion threats daily. The report is based on data collected from January to December 2025, supplemented by deception telemetry observed between October 2025 and March 2026.

About Zscaler
Zscaler (NASDAQ: ZS) is a pioneer and global leader in zero trust security. The world's largest businesses, critical infrastructure organizations, and government agencies rely on Zscaler to secure users, branches, applications, data & devices, and to accelerate digital transformation initiatives. Distributed across 160+ data centers globally, the Zscaler Zero Trust Exchange™ platform combined with advanced AI combats billions of cyber threats and policy violations every day and unlocks productivity gains for modern enterprises by reducing costs and complexity.

Media Contact
Nick Gonzalez, Director of Global Public Relations, press@zscaler.com