Trustwave®
SpiderLabs®

2024 Education Threat Landscape

DOWNLOAD THE REPORT

TRUSTWAVE THREAT INTELLIGENCE BRIEFING & MITIGATION STRATEGIES

K-12 and primary schools handle sensitive data concerning minors, while higher education institutions and universities must safeguard intellectual property data, making them prime targets for cyberattacks.

These attacks not only threaten the safety and security of teachers and administrators, but they put the privacy of students, staff, and other associated entities at risk.

Emerging and Prominent Trends

SHIFT TOWARDS ONLINE EDUCATION

THIRD-PARTY SECURITY RISKS

RANSOMWARE ATTACKS

1.8M
Public-facing devices

30%
Share of ransomware incidents attributed to LockBit

74%
Exploit attempts are Log4J

The Education Threat Landscape

THREAT ACTORS

- LockBit 3.0
- Rhysida
- CLOP or Cl0p
- Akira
- ALPHV aka BlackCat
- Medusa
- Vice Society
- No Escape
- Royal
- Pirat-Networks

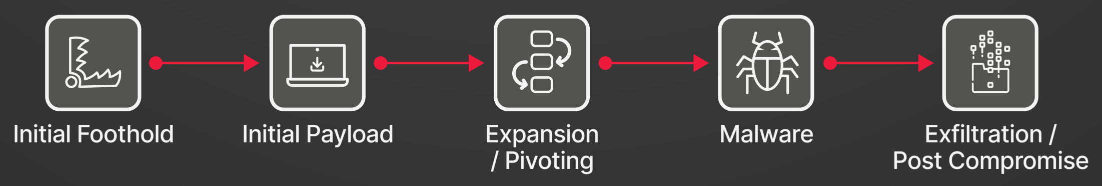
THREAT TACTICS

- Phishing and Social Engineering
- Exploitation of Applications and Databases
- Drive-by Compromise
- Abuse of Valid Account Credentials and Password Attacks
- Access Brokers, Auctions and WebShells
- Powershell and User Execution Techniques

What Makes Education's Attack Surface Unique?

- BYOD Dilemma
- Complex Infrastructure
- Data Trove
- Exposed Systems & Services
- Resource Scarcity
- Legacy Risks

Learn About the Attack Flow in Education



Get actionable mitigations against threat actors, their tactics, and attack flow to keep your institution out of the headlines.

DOWNLOAD THE REPORT

Trustwave SpiderLabs
2024 Education Threat Landscape
TRUSTWAVE THREAT INTELLIGENCE BRIEFING AND MITIGATION STRATEGIES