Trellix ADVANCED RESEARCH CENTER

TLP: Amber

Threat Intelligence Group

Advanced Research Center

Threat Landscape Report: Higher Education

February - May 2025

BLUF (Bottom Line Up Front):The higher education sector faces a complex and evolving threat landscape characterized by:

- Sophisticated state-sponsored APT groups (notably APT34) and cybercriminal organizations actively targeting academic institutions
- Dominant presence of information stealers (Agent Tesla leading with 83,973 detections)
- Five major ransomware groups conducting targeted campaigns (FOG, FUNKSEC, QILIN, MEDUSA, RANSOMHUB)
- Extensive abuse of legitimate tools for malicious purposes
- Active underground marketplace for educational data and access

Executive Summary

Higher education institutions are under siege from complex cyber attacks, ranging from sophisticated nation-state actors like Iran's APT34 to opportunistic cybercriminals. The threat landscape is dominated by stealthy information-stealing malware, with Agent Tesla being a particularly pervasive threat, alongside recent ransomware gang activities spearheaded by the aggressive FOG group, who are actively launching targeted attacks. This volatile environment is further compounded by a thriving black market where stolen educational data and illicit system access are openly traded.

Key Statistics

- Top Malware: Agent Tesla (83,973 detections)
- Most Active Ransomware Group: FOG (8 attacks)
- Peak Activity Period: Mid-March to Early April 2025
- Most Prevalent MITRE Technique: PowerShell (T1059.001) with 277,561 detections

Top Threat Actors

State-Sponsored Actors

1. **APT34 (Iranian)**
    - Campaign: Infrastructure Discovery
    - Target: Iraqi academic organizations
    - Notable TTPs: Domain impersonation, SSH key reuse

Unattributed Campaigns

1. **South Korean Campaign**
   - Vector: Malicious HWP Files
   - Timeline: March 13, 2025
   - Tools: Multiple executable components, BAT files

2. **US Universities Campaign**
   - Vector: Google Forms Phishing
   - Timeline: February 24, 2025
   - Tactics: Sophisticated phishing, web service abuse

Top Malware Families

1. Agent Tesla (83,973 detections)

- Sophisticated data exfiltration capabilities
- Multiple C2 channels
- Peak activity: Week 5 (36,893 detections)
- Notable TTPs: Obfuscated files, multi-channel exfiltration

2. Formbook (30,877 detections)

- Information stealer with advanced evasion
- Major peak: March 10 (10,853 detections)
- Strategic deployment patterns
- Notable gap in early April

3. Metasploit (26,101 detections)

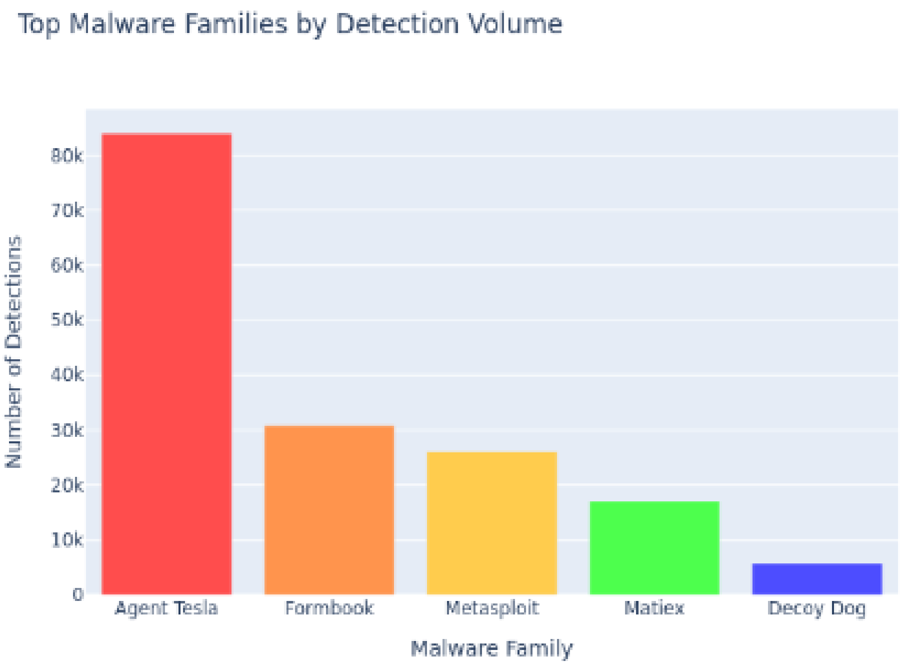
- Attribution: Russian state-sponsored actors
- Consistent detection rate (2,000-3,000 per week)
- Advanced post-exploitation activities

4. Matiex (17,157 detections)

- Advanced masquerading techniques
- Highest activity: March 24 (8,170 detections)
- Sophisticated evasion capabilities

5. Decoy Dog (5,786 detections)

- Advanced cryptographic capabilities
- Consistent detection pattern with gradual decline
- Sophisticated internal proxy usage



Non-Malicious Tools Used In Attacks

System Administration Tools

- Tools: Systeminfo, ipconfig, Nltest
- Detection Period: Week of April 21, 2025
- Purpose: System reconnaissance and network mapping
- MITRE Techniques: T1082, T1016, T1482

Certificate and Registry Tools

- Tools: certutil, Regsvr32
- Primary Misuse: Payload delivery and system modification
- MITRE Techniques: T1218, T1202

Password Recovery Tools

- Tools: Mail PassView, WebBrowserPassView
- Purpose: Unauthorized credential extraction
- MITRE Techniques: T1555, T1555.003

Distribution of Tool Categories

- System Administration Tools: 33.3%
- Credential Recovery Tools: 22.2%
- Certificate/Registry Tools: 22.2%
- Scripting Tools: 11.1%
- Dual-Use Network Tools: 11.1%

Ransomware Activity

Top Ransomware Groups

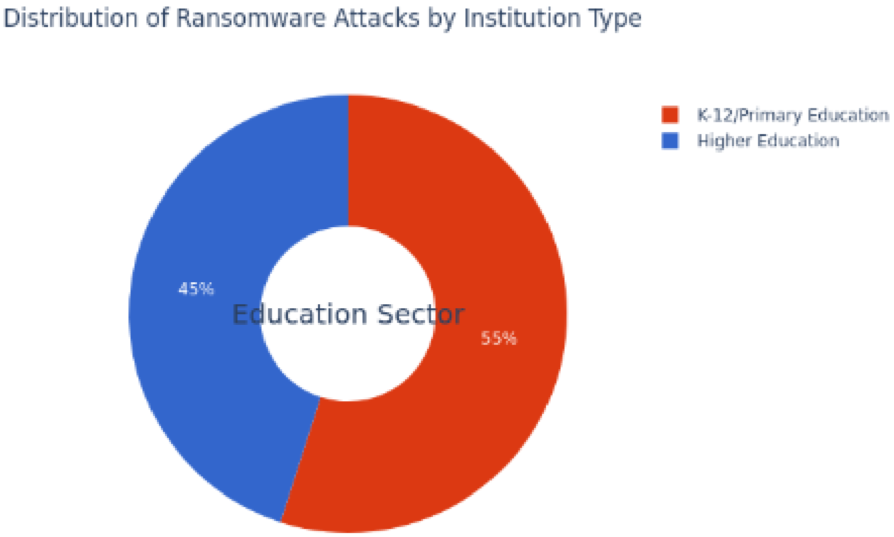
1. **FOG (8 attacks)**
    - Notable Victims: University of Notre Dame Australia (62 GB)
    - Geographic Spread: USA, Australia, Chile
    - Data Volume Range: 5-171 GB

2. **FUNKSEC (7 attacks)**
    - Focus: Higher Education
    - Notable Victims: Sorbonne Université (50 GB)
    - Distinctive Feature: Use of AI tools (WormGPT)

3. **QILIN (6 attacks)**
    - Target Pattern: Smaller institutions
    - Geographic Spread: USA, Australia
    - Focus: Mixed Education Sector

4. **MEDUSA (5 attacks)**
    - Focus: Public School Districts
    - Largest Data Volume: 2.40 TB
    - Geographic Focus: USA

5. **RANSOMHUB (5 attacks)**
    - Geographic Focus: USA
    - Limited public disclosure
    - Mixed institutional targeting



Attack Characteristics

- **Institution Size Distribution:**
  - Large (3000+ employees): 28%
  - Medium (300-3000 employees): 32%
  - Small (<300 employees): 40%
- **Geographic Distribution:**
  - United States: 62%
  - Europe: 20%
  - Australia: 10%
  - Other: 8%
- **Data Exfiltration Patterns**:
  - Small attacks: 5-50GB
  - Medium attacks: 50-200GB
  - Large attacks: >200GB (up to 2.40TB)

Underground Forum Intelligence

Key Activities

- Active trading of educational data and access credentials
- Multiple threat actors specializing in educational institution targeting
- Services primarily advertised on Telegram channels

Services Offered

1. **Educational System Access**
    - University network penetration
    - School website compromise
    - Administrative system access
    - Grade management system infiltration

2. **Data Manipulation Services**
    - Grade changes
    - Student database access
    - Academic records manipulation

Threat Actor Landscape

Notable actors identified:

- Adrian4798
- ASHER HACK
- Bandit_Hack
- HACKER ANTONIO
- Sergey ⚓

Attack Methods

- DDoS attacks on educational websites
- Database exploitation
- Grade manipulation systems
- Network infiltration techniques
- Administrative system compromise

Market Characteristics

- Cryptocurrency payment preferred
- Private negotiation for pricing
- "Professional" services with guarantees
- Strong presence in Spanish and English language channels

MITRE ATT&CK Techniques

Top 5 Observed Techniques

1. **PowerShell (T1059.001)**
    - Total Detections: 277,561
    - Associated Actor: Hafnium

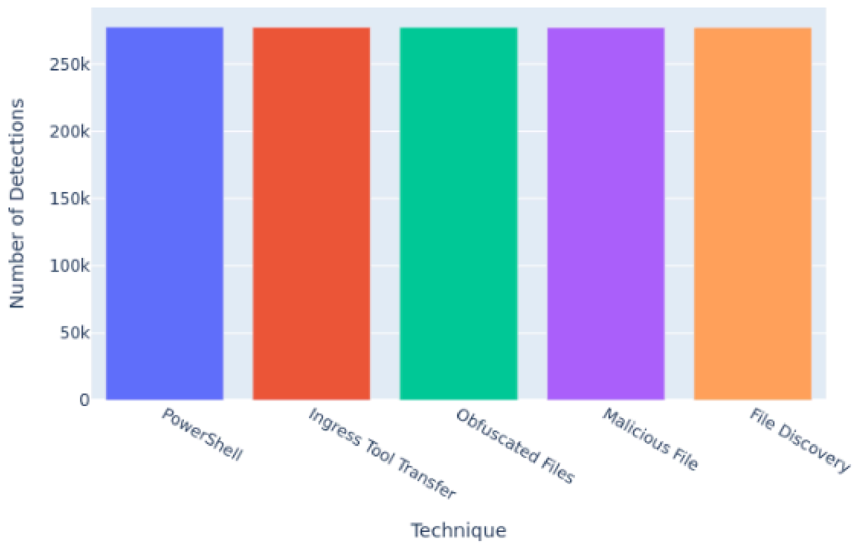
   - Key IOC: MD5: 2024ea60da870a221db260482117258b

2. **Ingress Tool Transfer (T1105)**
   - Total Detections: 277,385
   - Associated Campaign: IT Supply Chain campaign
   - Heavy use of Microsoft cloud services

3. **Obfuscated Files or Information (T1027)**
   - Total Detections: 277,299
   - Used in both phishing and supply chain attacks
   - Peak activity: March 2025

4. **Malicious File (T1204)**
   - Total Detections: 277,263
   - Associated with Google Forms phishing campaign
   - Strong correlation with web-based delivery

5. **File and Directory Discovery (T1083)**
   - Total Detections: 277,089
   - Often follows successful initial access
   - Strong correlation with lateral movement



Top MITRE ATT&CK Techniques by Detection Volume

Conclusion

The findings paint a picture of a higher education sector facing a relentless barrage of cyber threats. The prevalence of information stealers, coupled with the persistent targeting by ransomware and the exploitation of legitimate tools, creates a formidable challenge. The existence of underground communities selling access to compromised academic resources only intensifies the urgency for institutions to strengthen their defenses, sharpen threat detection capabilities, and grow a strong culture of security awareness to protect against the evolving threats targeting the higher education sector.

1. **Threat Actor Diversity**

   - Mix of state-sponsored APTs and cybercriminal groups
   - Strong presence of Iranian (APT34) and Russian actors
   - Organized ransomware groups with specific education sector focus

2. **Attack Sophistication**

   - Advanced malware deployment (Agent Tesla leading with 83,973 detections)
   - Sophisticated ransomware operations (31 total attacks across top 5 groups)
   - Strategic use of legitimate tools for malicious purposes

3. **Target Distribution**

   - Balanced targeting between higher education (45%) and K-12 (55%)
   - Geographic focus on US institutions (62% of ransomware attacks)
   - Preference for smaller institutions (40% of targets)

4. **Emerging Trends**

   - Increasing use of AI tools in attacks (e.g., WormGPT by FUNKSEC)
   - Growing underground market for educational access
   - Rising sophistication in data exfiltration techniques

May 2025 Classification: TLP: White
"In the face of evolving cyber threats, protection isn't just an option—it's a necessity for global stability."