Investigating AI-Based Methods for Detecting Emerging Cyber Threats in Dark Web Forums

- Practical Applications & Implementation Methodologies

- Presented by: Mehrier Bin Touhid

- Date: April 4, 2025

DARK WEB BASICS:

HIDDEN NETWORK REQUIRING SPECIALIZED ACCESS (TOR) HUB FOR CYBERCRIMINAL ACTIVITIES AND DISCUSSIONS

Research Objectives:

- Explore AI-based detection methods
- Examine practical implementation strategies
- Understand real-world applications

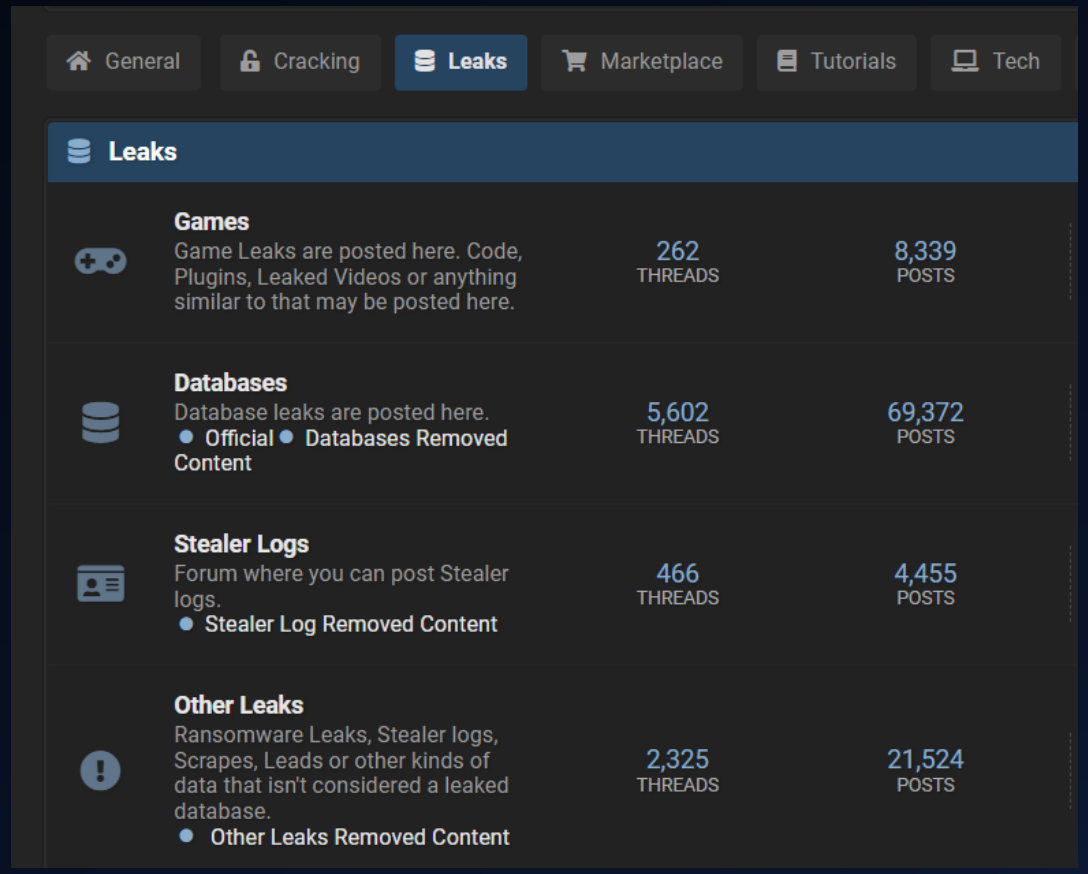
The Dark Web Threat Landscape

Key Forum Types:

- Cybercriminal discussion boards (BreachForums, XSS)
- Marketplaces for stolen data (15+ billion records available)
- Hacking service platform

Common Threats:

- Ransomware planning and services
- Credential sales and identity theft
- Zero-day exploits and malware distribution



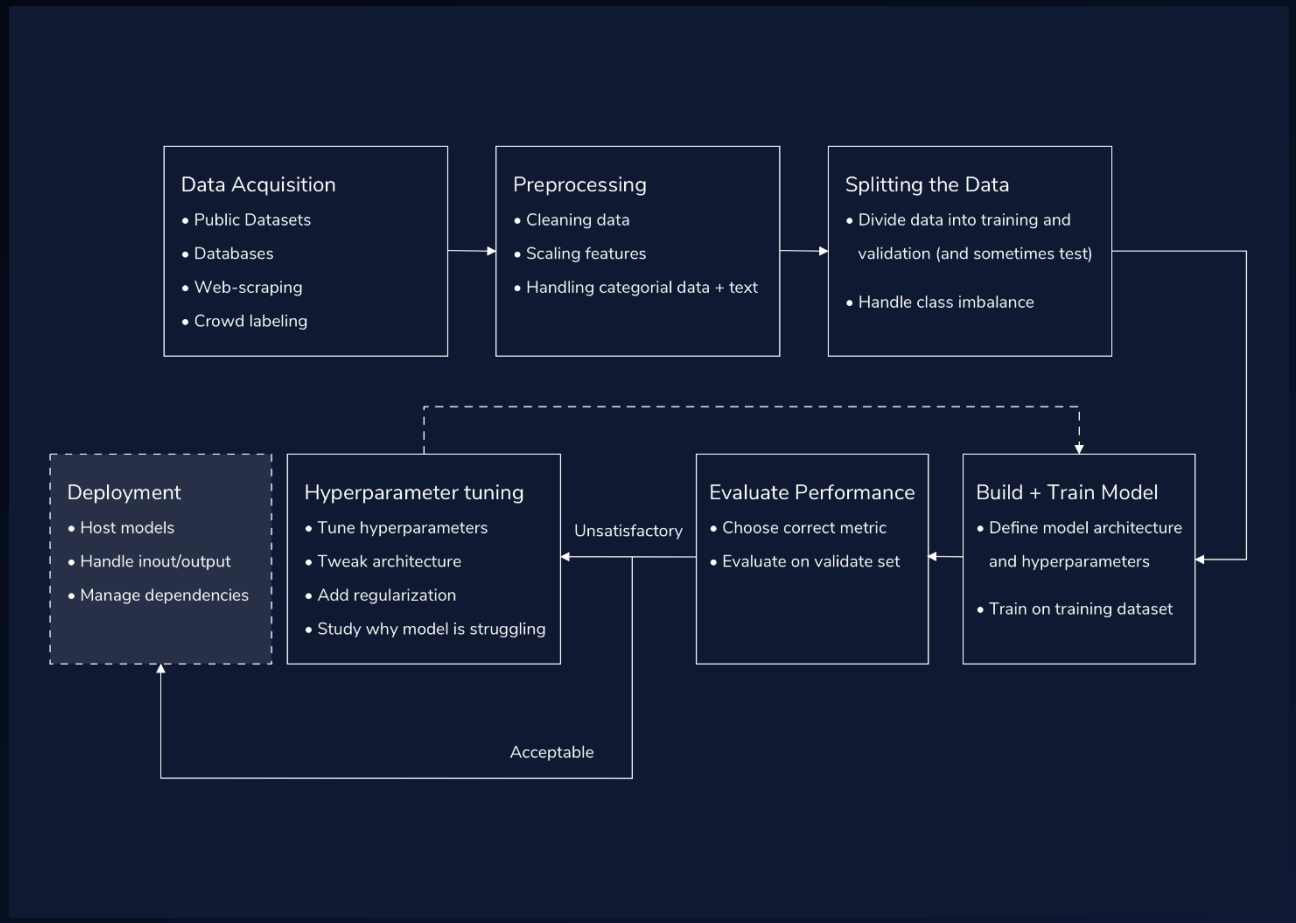
Specialized AI Models

- DarkBERT:
  - Language model specifically trained on dark web datasets[7]
  - Enhanced understanding of cybercriminal terminology
  - Superior performance in detecting coded communications[7]
- Anomaly Detection Systems:
  - Time-series analysis of behavioral patterns
  - Baseline deviation alerting
  - Real-time threat scoring algorithms

AI-Based Detection Methods

1. Machine Learning:
    1. Pattern recognition in forum discussions
    2. Anomaly detection in user behaviors
    3. Classification of threats by severity

2. Natural Language Processing:
    1. Processing cybercriminal slang and coded language
    2. Specialized models trained on dark web content
    3. Sentiment analysis to gauge threat intent



Practical Methodologies - Data Collection

- Dark Web Crawling:
  - Automated crawlers navigate Tor networks to index content
  - Collection from forums, marketplaces, and chat platforms
  - Tools scan 15+ billion pages daily across various channels
- Implementation Approach:
  - Deploy specialized crawlers that respect legal boundaries
  - Focus on relevant forums based on threat profile
  - Establish continuous monitoring schedules

Practical Methodologies - Analysis

NLP FOR THREAT DETECTION

- Process multilingual content and coded communications
- Detect keywords related to specific threats or targets
- Implementation: Integrate specialized models like DarkBERT with security infrastructure

SENTIMENT & BEHAVIORAL ANALYSIS

- Gauge tone and intent in discussions to prioritize threats
- Assess discussions for malicious planning vs. casual conversation
- Implementation: Train models on historical attack discussions

Automated Intelligence Processing

Threat Classification Systems:

- Categorize detected threats by type, severity, and relevance
- Apply risk scoring to prioritize security team focus
- Implementation: Create custom taxonomies for your industry threats

Visualization & Reporting:

- Transform complex data into actionable intelligence dashboards
- Enable quick decision-making with clear data presentation
- Implementation: Design dashboards for different stakeholders (technical vs. executive)

Real-World Application - Credential Monitoring

Practical Implementation:

- Configure automated scanning for company email domains
- Set up alerts for credential appearance on dark web marketplaces
- Integrate with identity management for automatic password resets

Case Example:

- Fortune 500 company detected 2,300+ exposed credentials
- Implemented forced password resets within 24 hours
- Reduced account takeover incidents by 73%

Real-World Application - Threat Actor Tracking

Practical Implementation:

- Create profiles of known threat actors targeting your industry
- Track linguistic patterns and cryptocurrency wallets
- Monitor for changes in tactics, techniques, and procedures (TTPs)

Implementation Tools:

- Platforms like DarkOwl Vision and Cybersixgill for continuous tracking
- Integrate findings with existing security information and event management (SIEM)

Implementation Strategy

Building a Dark Web Monitoring Program:

- Technology Selection: Choose appropriate AI tools for your threat profile
- Integration: Connect with existing security infrastructure
- Personnel: Train analysts on tool usage and alert triage

Response Playbooks:

- Develop automated and manual response workflows
- Create escalation paths based on threat severity
- Establish law enforcement collaboration protocols

Challenges & Limitations

- Technical Challenges:
  - Encryption barriers in private forums
  - Rapidly changing criminal communication methods
- Adversarial Techniques:
  - Criminals developing counter-AI measures
  - Use of code words and linguistic obfuscation
- Ethical Considerations:
  - Balancing security needs with privacy concerns
  - Ensuring legal compliance in monitoring activities

Conclusion

- AI methods provide powerful capabilities for dark web threat detection
- Practical implementation requires both technology and process
- Ongoing development and adaptation essential as threats evolve
- Questions?

References