TOR-Unveil: Forensic Analysis Report

Chain of Custody

Report Generated:	2025-12-22 08:25:13 UTC
Analysis ID:	0a167906-b6f9-4e7f-82a9-6bf4e7b3ae11
PCAP Filename:	tor_only.pcap
Analysis Duration:	263.82s
Case ID:	AUTO
Investigator:	System
Agency:	TN Police Cybercrime Division

Executive Summary

This report presents the results of an automated TOR traffic analysis using the Flow Time-Density Correlation (FTDC) method. The analysis identified 20 potential guard nodes with an average confidence of 39.0%. The system analyzed network traffic patterns to probabilistically correlate TOR entry and exit nodes.

Analysis Overview

Metric	Value
Total Guard Candidates	20
Average Confidence Score	39.0%
Improvement Factor	1.00x
Circuit Paths Identified	10
Correlation Trend	stable

Top Guard Node Candidates

Rank	Nickname	IP Address	Country	Confidence	Flags
1	Ajax	206.189.6.56	NL	39.0%	
2	RebootToolsRela	212.34.148.78	XX	38.9%	

3	L4m0R	84.252.123.139	XX	38.6%	
4	skylarkRelay	95.111.230.178	FR	38.4%	
5	prsv	51.77.132.82	XX	38.1%	
6	mharelay	147.28.87.56	SE	37.9%	
7	chali2na	64.65.62.145	US	37.9%	
8	Unnamed	185.243.214.73	XX	37.7%	
9	marsmellow	20.224.145.181	NL	37.6%	
10	relayon0153	185.220.101.153	DE	37.6%	

Identified Circuit Paths

Path 1 (Confidence: 39.0%)

Role	Nickname	IP	Country
Guard	Ajax	206.189.6.56	NL
Middle	lisdex	152.53.144.50	DE
Exit	lisdex	152.53.144.50	DE

Path 2 (Confidence: 39.0%)

Role	Nickname	IP	Country
Guard	Ajax	206.189.6.56	NL
Middle	SharingIsCaring	188.195.48.170	DE
Exit	lisdex	152.53.144.50	DE

Path 3 (Confidence: 39.0%)

Role	Nickname	IP	Country
Guard	Ajax	206.189.6.56	NL
Middle	seele	104.53.221.159	US
Exit	lisdex	152.53.144.50	DE

Path 4 (Confidence: 39.0%)

Role	Nickname	IP	Country
Guard	Ajax	206.189.6.56	NL
Middle	hubbabubbaABC	83.108.59.221	NO
Exit	lisdex	152.53.144.50	DE

Path 5 (Confidence: 39.0%)

Role	Nickname	IP	Country
Guard	Ajax	206.189.6.56	NL
Middle	SENDNOOSEplz	204.137.14.106	US
Exit	lisdex	152.53.144.50	DE

Methodology

Flow Time-Density Correlation (FTDC) Analysis

The analysis employs a multi-factor correlation approach:

1. **Temporal Correlation:** Compares timing patterns between exit node traffic and potential guard node activity using sliding window analysis (50ms default).

2. **Bandwidth Correlation:** Analyzes bandwidth capacity and utilization patterns to identify relays capable of handling observed traffic volumes.

3. **Circuit Pattern Matching:** Uses weighted scoring across three dimensions: - Bandwidth Score (50%): Relay capacity vs. required throughput - Quality Score (30%): Uptime, flags, and reliability metrics - Network Proximity (20%): Geographic and AS-level proximity analysis

4. **Iterative Improvement:** Bayesian-like updating mechanism that refines confidence scores as more correlation data becomes available.

Confidence Interpretation:
- High (>70%): Strong correlation evidence, prioritize for investigation
- Medium (40-70%): Moderate correlation, requires additional validation
- Low (<40%): Weak correlation, consider as background noise

Legal and Technical Disclaimers

IMPORTANT: This report contains probabilistic correlation analysis results. The system does NOT: - Decrypt TOR traffic or compromise user anonymity through cryptographic attacks - Perform active network attacks or exploit vulnerabilities - Guarantee 100% accuracy in guard node identification

Results should be used as investigative leads requiring additional corroboration through traditional forensic methods. All analysis respects the integrity of the TOR network and is intended solely for lawful cybercrime investigation purposes.

Chain of Custody: This report was generated automatically by the TOR-Unveil system. Any manual modifications to this document invalidate its forensic integrity.