Criminal Infrastructure Assessment

Scareware Distribution Network Analysis

Classification: Criminal Infrastructure Analysis
Date: August 17, 2025
Source: Threat Intelligence Collection from Known Criminal Actor's URL Database
Assessment Confidence: High

Executive Summary

Analysis of URLs recovered from a known criminal actor's collection reveals a sophisticated scareware distribution network employing multi-domain redirect chains, advanced victim tracking, and geographic targeting capabilities. The operation demonstrates professional-grade infrastructure with sophisticated traffic management and conversion optimization typical of organized cybercrime operations.

Technical Infrastructure Analysis

Primary Domains Identified

Domain	Role	Status	Notes
gatewaylogin.info	Initial Entry Point	Active	No visible port specification
systemchainloop.com	Traffic Management Hub	Confirmed Malicious	Documented notification spam campaigns
boostedsheild.com	Final Conversion Target	Active	Misspelled "shield" - evasion technique

Traffic Flow Architecture

gatewaylogin.info

↓

https://d2go4oghubcc7395lmm0.systemchainloop.com/NL/04/

↓

boostedsheild.com (final conversion)

URL Parameter Intelligence

Campaign Tracking:

- cid=adb65c801e8f940749a8 - Campaign identifier for conversion attribution
- extclickid=d2go4h8hubcc7395ljjg - External click tracking system
- clickid=d2go4oghubcc7395lmm0 - Internal click tracking system

Victim Segmentation:

- list=2 - Victim categorization/targeting list assignment
- lp_key=17554ff8697f79035ebfb3d2703c0034c817a15438 - Landing page variant selector
- language=en-US - Language-based targeting
- browser=Chrome - Browser-specific content delivery
    - may change based chosen browser

Geographic Targeting:

- /NL/04/ - Netherlands geographic targeting, campaign variant 04
- Subdomain prefix d2go4oghubcc7395lmm0 - Dynamic tracking identifier

---

Malware Analysis

Scareware Implementation

Analysis of HTML/JavaScript payload reveals:

Social Engineering Tactics:

- Fake McAfee antivirus interface impersonation
- False virus detection claims (7 critical viruses)
- Urgency-driven messaging ("Do not close this window!")
- Fabricated threat names (Win32/CryptoLocker.X9Zr, Russian Trojan)

Technical Evasion:

- Heavy JavaScript obfuscation with anti-debugging techniques
- Browser history manipulation to prevent back navigation
- Fullscreen activation attempts
- Audio alerts for psychological manipulation

Conversion Optimization:

- Fake countdown timers (55% discount expiring)
- Multiple psychological pressure points
- Progressive disclosure of "threats"
- Professional UI mimicking legitimate software

Threat Assessment

Operation Sophistication Level: HIGH

Indicators of Professional Operation:

- Multi-domain redirect infrastructure
- Sophisticated victim tracking and segmentation
- Geographic targeting capabilities
- A/B testing framework for landing page optimization
- Affiliate/campaign management system
- Anti-analysis and evasion techniques

Criminal Infrastructure Capabilities

Traffic Management:

- Dynamic subdomain generation
- Geographic content delivery
- Browser and language-specific targeting
- Campaign variant management

Victim Processing:

- Detailed tracking through conversion funnel
- Segmentation based on multiple factors
- Conversion optimization testing
- Payment processing integration

Risk Assessment

Threat Level: MEDIUM-HIGH

Target Profile:

- General consumer population
- Focus on English-speaking markets
- Chrome browser users prioritized
- Geographic expansion evidenced (Netherlands targeting)

Attack Vector:

- Initial access through compromised/malicious websites
- Social engineering via fake security warnings
- Payment fraud through fake antivirus sales
- Potential credential harvesting

Operational Scale Indicators

Volume Metrics:

- Multiple simultaneous campaigns (list=2+ suggests segmentation)
- Geographic expansion (NL targeting from likely US-based operation)
- Professional conversion tracking infrastructure
- Affiliate network integration

Recommendations

Immediate Actions

1. **Block all identified domains** in organizational security controls
2. **Monitor for domain variants** using similar naming patterns
3. **Alert users** to scareware tactics and fake McAfee interfaces
4. **Report domains** to relevant abuse contacts and law enforcement

Intelligence Collection

1. **Continue monitoring** redirect chains for new infrastructure
2. **Track campaign identifiers** for operational intelligence
3. **Document geographic targeting** expansion patterns
4. **Correlate with payment processor** intelligence if available

Defensive Measures

1. **Implement DNS filtering** for known malicious domains
2. **Deploy user education** regarding scareware tactics
3. **Monitor for fake antivirus** installation attempts
4. **Enhance browser security** policies to prevent full-screen abuse

---

Intelligence Gaps

- Payment processing infrastructure details
- Full extent of domain portfolio
- Attribution to specific criminal groups
- Complete victim processing workflow

Appendix

IOCs (Indicators of Compromise)

Domains:

- gatewaylogin.info
- systemchainloop.com

- boostedsheild.com

Campaign Identifiers:

- cid: adb65c801e8f940749a8
- lp_key: 17554ff8697f79035ebfb3d2703c0034c817a15438

File Signatures:

- Fake McAfee interface implementations
- JavaScript with specific obfuscation patterns
- Audio files: beep.mp3 (alert sounds)

Assessment prepared based on technical analysis of criminal infrastructure. Recommend correlation with additional threat intelligence sources for comprehensive threat picture.