Ransomware Detection: Catch the Kill Chain Before Encryption Begins

WireTrace detects ransomware activity across the entire kill chain - from initial reconnaissance through lateral movement, credential exposure, active encryption, and data exfiltration. 12 detection rules monitor network behavior passively, correlating multiple indicators per asset to raise high-confidence alerts before data is lost. Every detection is mapped to the MITRE ATT&CK framework. No agents required. No endpoint software. Pure network-level detection from passive traffic analysis.

WireTrace Ransomware Detection | Version 1.3 | 2026

12 Detection Rules | Full Kill Chain Coverage | MITRE ATT&CK Mapped | Zero Agents Required | Per-Asset Risk Scoring | OT/IT Isolation Monitoring

1. The Ransomware Kill Chain

Ransomware attacks follow a predictable sequence of network behaviors. WireTrace monitors each phase passively, detecting indicators that appear on the wire before encryption begins.

2. Detection Rules

Each of WireTrace's 12 ransomware detection rules targets a specific behavior in the kill chain. Rules operate independently and feed into the kill chain correlation engine, which scores cumulative indicators per asset.

Phase 1: Reconnaissance

Port Scanning / Network Enumeration

Detects when a single host probes multiple IP addresses on the same port or scans multiple ports across the subnet. This is the first visible sign of an attacker mapping your network - identifying which machines are reachable and what services are exposed. Ransomware operators use port scans to find SMB shares, RDP endpoints, and vulnerable services.

MITRE T1046 - NETWORK SERVICE DISCOVERY

SMB Share Enumeration

Detects a host enumerating available SMB/CIFS shares across the network. Attackers map shared folders to identify where files are stored, which shares are writable, and where to deploy ransomware payloads. This reconnaissance step directly precedes file encryption.

MITRE T1135 - NETWORK SHARE DISCOVERY

Phase 2: Lateral Movement

RDP Lateral Movement Spray

Detects a single host attempting RDP connections to multiple endpoints in rapid succession. Ransomware groups use Remote Desktop to move between machines after initial compromise, deploying payloads on each system they access. Spray patterns - many targets in a short window - are a hallmark of automated lateral movement.

MITRE T1021.001 - REMOTE DESKTOP PROTOCOL

OT/IT Isolation Violation

Detects network traffic crossing defined IT/OT boundaries. When an IT workstation begins communicating with industrial control systems, or when devices in operational zones initiate connections to corporate networks, WireTrace alerts immediately. This is how ransomware spreads from the enterprise network into critical infrastructure.

MITRE T1021 - REMOTE SERVICES (LATERAL MOVEMENT)

Phase 3: Credential Exposure

Cleartext Credential Exposure

Detects authentication credentials transmitted in cleartext over protocols such as HTTP Basic Auth, FTP, Telnet, SMTP, and SNMPv1/v2c. Exposed credentials are harvested by attackers to escalate privileges and move laterally without triggering lockout defenses. In OT environments, cleartext industrial protocols often carry default credentials that grant access to safety-critical systems.

MITRE T1552.001 - CREDENTIALS IN FILES / T1040 - NETWORK SNIFFING

SMB Protocol Downgrade

Detects when SMB sessions negotiate down to SMBv1 instead of using SMBv2 or SMBv3. The EternalBlue exploit (used by WannaCry, NotPetya, and many subsequent ransomware variants) targets vulnerabilities in SMBv1. A protocol downgrade to SMBv1 in a modern network is a strong indicator of exploitation or misconfiguration that leaves systems vulnerable.

MITRE T1210 - EXPLOITATION OF REMOTE SERVICES

Phase 4: Active Encryption

Mass SMB File Operations

Detects an abnormally high volume of file read-write operations from a single host across SMB shares. During active encryption, ransomware reads the original file, encrypts the content, writes the encrypted version, and deletes or renames the original. This creates a distinctive pattern of mass read-write-rename operations that differs dramatically from normal file access behavior.

MITRE T1486 - DATA ENCRYPTED FOR IMPACT

Known Ransomware File Extensions

Detects file operations involving known ransomware file extensions (.encrypted, .locked, .crypt, .rnsmwr, .cerber, .locky, .wcry, and hundreds more). When WireTrace observes files being renamed or created with these extensions, it indicates active encryption in progress. The detection database is updated continuously with extensions from new ransomware families.

MITRE T1486 - DATA ENCRYPTED FOR IMPACT

Ransom Note Delivery

Detects the creation of ransom note files (README.txt, DECRYPT_FILES.html, HOW_TO_RECOVER.txt, and known variants) across multiple directories or shares. Ransomware drops instruction files in every directory it encrypts. Observing these files being written across the network is a high-confidence indicator that encryption is underway or complete.

MITRE T1491 - DEFACEMENT (INTERNAL)

Phase 5: Data Exfiltration

Data Exfiltration Volume Anomaly

Detects unusual volumes of outbound data transfer from assets that do not normally transmit large amounts of data externally. Modern ransomware groups practice "double extortion" - stealing data before encrypting it. WireTrace compares outbound data volumes against per-asset behavioral baselines to identify exfiltration before the ransom demand arrives.

MITRE T1041 - EXFILTRATION OVER C2 CHANNEL

Cross-Phase: Correlation

Kill Chain Correlation Scoring

Correlates multiple detection indicators per asset into a single kill chain risk score. A workstation that triggers port scanning, followed by SMB enumeration, followed by mass file operations, accumulates a higher risk score than any single indicator alone. This correlation reduces false positives by requiring multiple confirming signals before raising a critical alert. Each phase contributes weighted evidence to the overall assessment.

KILL CHAIN CORRELATION - MULTI-PHASE DETECTION

3. Real-World Detection Scenario

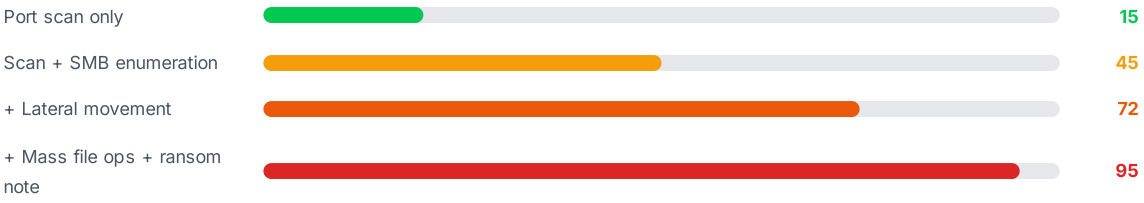
RANSOMWARE ATTACK - DETECTED AND CORRELATED IN SECONDS

1. **09:14:32 - Reconnaissance detected.** Workstation 10.1.5.87 begins scanning port 445 (SMB) across the 10.1.5.0/24 and 10.1.6.0/24 subnets. WireTrace detects the scan pattern and logs the first kill chain indicator. Risk score: Low.
2. **09:14:58 - SMB enumeration detected.** The same workstation connects to 12 SMB shares it has never accessed before. Share names, access permissions, and file listings are observed. Kill chain indicator #2 logged. Risk score: Medium.
3. **09:15:14 - RDP lateral movement detected.** Workstation 10.1.5.87 initiates RDP sessions to 10.1.5.22, 10.1.6.15, and 10.1.6.41 within a 16-second window. None of these connections existed in the baseline. Kill chain indicator #3. Risk score: High.
4. **09:15:31 - Mass file operations detected.** Over 2,400 file read-write-rename operations observed on \\10.1.6.15\shared in 17 seconds. Files are being read, then written with .encrypted extensions. Ransom note (DECRYPT_INSTRUCTIONS.html) detected in 3 directories. Kill chain indicator #4 and #5. Risk score: Critical.

CRITICAL ALERT: Ransomware kill chain confirmed on 10.1.5.87. Correlation score: 4/5 phases detected. Time from first indicator to critical alert: 59 seconds. Recommended action: Isolate host, block lateral movement, preserve evidence.

4. Per-Asset Risk Scoring

Every asset accumulates a ransomware risk score based on the kill chain indicators observed against it. The score reflects both the number of phases detected and the severity of each indicator.



Correlation advantage: A single port scan generates a low-severity finding. But when the same asset scans, enumerates shares, moves laterally, and begins mass file operations - the correlated score escalates to critical within seconds. This multi-signal approach dramatically reduces false positives while catching real attacks early.

5. MITRE ATT&CK Framework Mapping

Every WireTrace detection rule maps to specific MITRE ATT&CK techniques, providing a common language for security teams and enabling integration with existing threat intelligence workflows.

DETECTION RULE	MITRE TECHNIQUE	TACTIC
Port Scanning	T1046 - Network Service Discovery	Discovery
SMB Enumeration	T1135 - Network Share Discovery	Discovery
RDP Lateral Movement	T1021.001 - Remote Desktop Protocol	Lateral Movement
OT/IT Isolation Violation	T1021 - Remote Services	Lateral Movement
Cleartext Credentials	T1552.001 / T1040	Credential Access
SMB Protocol Downgrade	T1210 - Exploitation of Remote Services	Lateral Movement
Mass File Operations	T1486 - Data Encrypted for Impact	Impact
Ransomware Extensions	T1486 - Data Encrypted for Impact	Impact
Ransom Note Delivery	T1491 - Defacement	Impact
Data Exfiltration	T1041 - Exfiltration Over C2	Exfiltration
Kill Chain Correlation	Multi-phase correlation	All Phases

6. OT/ICS-Specific Detection

Ransomware targeting industrial environments has unique characteristics. WireTrace detects IT-to-OT lateral movement that generic IT tools cannot see.

IT-to-OT Boundary Crossing

WireTrace monitors communication between Purdue levels. When an IT workstation (Level 4-5) initiates connections to PLCs, RTUs, or HMIs (Level 0-2), it triggers an isolation violation alert. Ransomware spreading from corporate email into the plant floor is detected at the network boundary, not after it reaches the controller.

Industrial Protocol Monitoring

WireTrace parses industrial protocols at the command level. Unauthorized Modbus writes, unexpected S7Comm programming sessions, or anomalous EtherNet/IP commands are detected even if the attacker uses legitimate protocol syntax. The behavioral baseline knows what is normal for each industrial device.

7. Medical Environment Detection

Healthcare networks face unique ransomware risks due to the mix of medical devices, clinical systems, and traditional IT infrastructure on shared networks.

DICOM/HL7 Access Monitoring

WireTrace monitors file operations and protocol activity on medical imaging and clinical messaging systems. Unusual access patterns to DICOM storage (unexpected PACS queries, bulk image retrieval) or HL7 message floods are detected as potential ransomware indicators or data theft precursors.

Medical Device Segmentation

WireTrace validates that medical devices remain within their intended network segments. When a ventilator or patient monitor begins communicating with unexpected hosts - particularly those showing other kill chain indicators - the correlation engine factors the medical context into the risk score.

8. File Activity Monitoring

WireTrace tracks file operations across six protocols, creating a forensic audit trail that is essential for ransomware investigation and recovery.

SMB/CIFS

Read, write, create, delete, rename operations on Windows file shares. The primary vector for ransomware file encryption on enterprise networks.

FTP / TFTP

File uploads, downloads, and directory listings. Monitors both standard FTP and TFTP used in industrial firmware updates and network device configurations.

NFS

Network File System operations on Linux/Unix shares. Tracks file access patterns that reveal unauthorized data access or bulk file manipulation.

HTTP

File transfers over web protocols. Detects bulk file downloads, unusual upload patterns, and web-based data exfiltration attempts.

DICOM

Medical imaging file operations. Monitors study retrieval, image storage, and query patterns on PACS and imaging devices.

Forensic Timeline

Every file operation is logged with timestamp, source, destination, file path, and operation type. Creates a complete forensic timeline for incident response and recovery.

9. Threat Intelligence Integration

WireTrace's ransomware detection is enhanced by built-in threat intelligence feeds that identify known malicious infrastructure.

IoC Matching

Observed IP addresses, domains, and URLs are matched against threat intelligence feeds in real time. Known command-and-control servers, ransomware distribution sites, and exfiltration endpoints are flagged immediately. An infrastructure whitelist prevents false positives from known-good services like CDNs and cloud providers.

Vulnerability Context

Assets with known vulnerabilities exploited by ransomware groups are prioritized in the risk assessment. WireTrace correlates CVE data with observed firmware versions and service banners to identify which assets are most likely to be targeted in the next stage of an attack.

10. Passive Detection Advantage

No agents. No endpoint software. No network changes. WireTrace detects ransomware activity from a passive copy of network traffic. The sensor connects to a SPAN port or network TAP in receive-only mode - zero packets transmitted onto the monitored network. This means ransomware detection works on every device, including systems where agents cannot be installed: industrial controllers, medical devices, IoT sensors, legacy systems, and embedded appliances. Detection begins the moment traffic is observed, with no deployment to individual endpoints.

Detect Ransomware Before Encryption Begins

See WireTrace's kill chain detection in action. Schedule a demo and we will show you how passive network analysis catches ransomware at every stage of the attack. wiretrace.io | sales@wiretrace.io