corelight

RANSOMWARE DETECTION

THE CASE FOR OPEN NDR

CLOSE THE CASE ON RANSOMWARE

With an Open Network Detection & Response Platform, being hit by a ransomware attack doesn't mean all is lost. Open NDR gives you full visibility into adversary activity on your network, allowing you to see what was breached or exfiltrated, and gives you the evidence to make critical decisions for how your business responds. Case in point: one of our customers, confronted with a $10 million ransomware demand for stolen data, quickly determined the data had no real value, allowing them to shrug off the attack and say “no” to the demand.

This guide offers practical guidance and real-world examples that describe how Open NDR can provide essential context around ransomware demands, as well as techniques analysts watch for and the capabilities they use against adversaries and help your organization close other critical cybersecurity cases.

IN THIS GUIDE: **RANSOMWARE DETECTION** **RANSOMWARE READINESS** **THE OPEN NDR PLATFORM**

RANSOMWARE DETECTION WITH **OPEN NDR**

EARLY STAGE

ADVERSARY TECHNIQUES

Reconnaissance
Active scanning and gathering of information about the victim network.

Brute force
Relentless trial and error to gain access.

Self-signed or expired certificates
Creating self-signed SSL/TLS certificates used during targeting.

ICS/OT attacks
Various techniques, tools, and malware used to achieve intended effects on ICS/OT systems.

CORELIGHT DEFENSIVE CAPABILITIES

Encrypted Traffic Collection
This Corelight collection helps analysts identify the early stages of a ransomware attack, and includes inferences and detections around SSL, SSH, and RDP traffic.

- Corelight alerts on SSH and RDP brute-forcing activity and flags known RDP clients such as Metasploit Scanner.
- The included x.509 log shows certificate details for all TLS connections. The presence of self-signed or expired certificates can serve as an early warning indicator of malware infection that could lead to a ransomware attack.

ICS/OT Collection
Corelight's ICS/OT Collection delivers visibility into ICS/OT network communications, expediting incident response, and simplifying inventory management. It includes includes many of the most common ICS/OT protocols currently in use.

MID STAGE

ADVERSARY TECHNIQUES

Lateral movement
Entering and controlling remote systems on a network, after initial access has been acquired.

Command and control (C2)
Establishing communication with the command and control servers.

Other known methods
During the mid-stages of a ransomware attack, adversaries employ a number of techniques made transparent by Open NDR.

CORELIGHT DEFENSIVE CAPABILITIES

To see lateral movement, Corelight uses signature and behavioral detection techniques to discover enumeration attacks, file transfers, remote procedure calls, windows authentication, and opening privileged file shares which could indicate attackers are expanding further into an organization's assets. Other ways Open NDR exposes mid-stage activity:

Core Collection
Detects lateral movement techniques in MITRE ATT&CK® related to SMB and DCE-RPC traffic, such as indicators targeting Windows Admin Shares and Remote File Copy. Optionally extract detection-related files to enable investigations of suspicious traffic.

Entity Collection
Categorizes 375+ types of applications and writes a new field directly to the connection log for easy correlation, using a variety of techniques from DNS queries to certificate SNIs and protocol metadata. Includes application identifcation package.

C2 Collection
Alerts on a variety of well-known attacker frameworks using multiple network protocols that correlate with ransomware attacks, such as Cobalt Strike.

Corelight's Open NDR Platform detects ransomware families using open-source or commercial IDS rulesets supported by Suricata®, including Proofpoint's ET Pro with 72,000+ rules for exploits and malware families. Monitor SMB transactions linked to 4,500 filenames tied to known ransomware attacks using community detection work or custom scripts.

RANSOMWARE DETECTION WITH **OPEN NDR**

LATE STAGE

ADVERSARY TECHNIQUES

Exfiltration
Stealing data from a network**.**

CORELIGHT DEFENSIVE CAPABILITIES

Behavior-based hunting and detections:

- Conn.log and service-specific logs can determine if a data downloader has become a large uploader. You can set custom thresholds to send a notice about these hosts.
- Create custom Suricata signatures to check for watermarked outbound content.
- Identify DNS exfiltration with three types of detections for DNS tunneling (including ML), and alerts, in addition to dns.log data.
- Spot file upload, download, and keystroke activity with Secure Shell Protocol (ssh.log) inferences for file upload.
- Includes DCE_RPC calls for attacks like DCSync.

POST EVENT

CORELIGHT CAPABILITIES

Scope assessment
Investigate the origin and scope of an attack with the network evidence and Smart PCAP integrated within the Open NDR Platform. Corelight's continuous monitoring capability can validate containment and show what was taken, as well as total bytes transferred. Files can also be sent to a sandbox for further analysis.

File recovery
Corelight file extraction can support file recovery efforts by extracting and reassembling more than 200 file types, such as PDFs and PPTs. Selectively capture packets according to protocol with customizable byte depths.

Validation
The Open NDR Platform can provide a timeline detailing every external and internal host compromised in an attack, validating scope. Additionally, continuous monitoring ensures containment has been achieved.

TEAM READINESS TIPS FOR RANSOMWARE

MONITOR

OBSERVE PRIVILEGED ACCOUNTS

Falling victim to a ransomware attack correlates with the number of privileged accounts, as well as the latitude those accounts have to move freely on your network.

- ☑ Look for privilege escalation and enumeration attacks

TRAIN

MAINTAIN READINESS

Incident response time is critical to disrupting ransomware attacks. Keep your team trained through regular ransomware response exercises that simulate a real world attack and learn how to use network data to identify risk.

- ☑ Conduct monthly IR ransomware training exercises
- ☑ Include Red Team/pentest
- ☑ Look for visibility gaps, write detections

THREAT HUNT

ACTIVELY HUNT

Network threat hunting refines organizational knowledge and security posture by exposing hidden vulnerabilities and incorrect assumptions, often catching adversaries in action and reducing their dwell time.

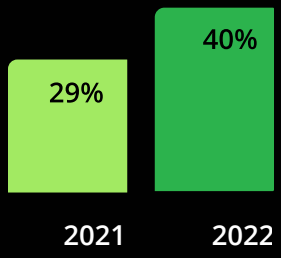
- ☑ Set clear goals for each hunt
- ☑ Ensure you have the ability to measure outcomes
- ☑ Document your activity
- ☑ Repurpose your findings to improve detections

CLOSE VISIBILITY GAPS **WITH NDR**

Adding NDR to endpoint (EDR) and SIEM solutions gives enterprises a complete picture of their security posture and operational state. Open NDR gives a complete view of *everything* connected to the network—including cloud, OT, and ICS environments.

NDR'S **DEFENSIVE ADVANTAGE**

Recent industry reports confirm the targets and techniques attackers exploit are evolving. Proactively defend against these and other novel approaches with Open NDR.



FIGHT BACK AGAINST EXFILTRATION

Data exfiltration is on the rise. NDR can show you unusual network traffic patterns that could be indicative of potential data theft.

PROTECT CLOUD & ICS NETWORKS

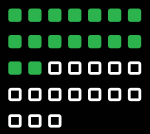
Cloud exploit cases surged by 95% year over year.[2] Corelight's Open NDR Platform transforms cloud traffic into security-centric evidence.

MEET COMPLIANCE REQUIREMENTS

Open NDR can help meet requirements for NIST, GDPR, SOX Act, PCI-DSS, and more.

DETECT THE MOST COMMON INITIAL ATTACK VECTORS[1]

Exploits and phishing accounted for 54% of initial attack vectors last year.[1] Open NDR provides effective detection against both techniques.



EXPOSE ATTACKS IN MOTION

Attackers dwell a median of 16 days prior to detection in compromised environments.[1] Open NDR provides historical evidence needed to expose activity across the full attack lifecycle (validation & recovery included).

DETECT KNOWN & UNKNOWN EXPLOITS

Open NDR provides evidence to help detect known and zero-day threats, including malware, ransomware, tunnels, backdoors, attacker tools & frameworks, and more.

1. Per M-TRENDS 2023 Mandiant Special Report https://mandiant.widen.net/s/dlzgn6w26n/m-trends-2023
2. Per CrowdStrike 2023 Global Threat Report https://www.crowdstrike.com/global-threat-report/

WHY **OPEN?**

- **Open Core—**Open NDR is powered by proven open-source technologies Zeek® and Suricata® with over 25 years of insights being continuously improved by a community of elite defenders.
- **Open Data—**Open data formats easily integrate with existing SIEM, XDR, or datalake solutions. Avoid vendor lock-in: your data is yours to keep.
- **Open Detections—**Gain broad coverage and detect emerging threats (e.g., SolarWinds with Zeek). Open detections can be customized and extended and are continuously updated.

FROM THE CREATORS OF zeek®

LEARN ABOUT THE OPEN NDR PLATFORM ›

TRUSTED BY

CROWDSTRIKE

MANDIANT NOW PART OF Google Cloud

Microsoft

splunk>

"Corelight helps you to find bad things happening like sneaky viruses or hackers trying to get in."

—G2.com validated review

CLOSE YOUR NEXT CASE WITH **OPEN NDR**

corelight

info@corelight.com | 888-547-9497