White Paper

How Corelight helps you hunt and respond to ransomware attacks

Introduction

File encryption takes just seconds to occur during a ransomware attack, so defenders must focus earlier in the attack lifecycle to find initial indicators like scanning, account compromise, and C2 communications. Notably, many of the toolkits and techniques used by ransomware leave indelible fingerprints on the network. Analysts can use these prints to root out the early stages of an attack and also accelerate investigation and containment verification if encryption has already occured.

Corelight's Open Network Detection and Response (NDR) platform gives defenders the network evidence and insight they need to effectively hunt and quickly respond to ransomware attacks. By integrating Suricata alerts with Zeek® logs and Smart PCAP, the platform delivers pivot-ready evidence for investigation and remediation.

Hunting for ransomware

Protocol visibility

Corelight transforms raw network traffic into rich, interlinked logs that let analysts easily track network connections across ports and protocols. The platform parses and logs dozens of different protocols, including those frequently abused in ransomware attacks such as:

- Remote Desktop Protocol (rdp.log)
- Server Message Block Protocol (smb_files.log)
- Secure Shell Protocol (ssh.log)

The network visibility that comes from Corelight's logs allows analysts to inventory connections, identify vulnerable systems, and spot behaviours that could indicate an ongoing ransomware attack such as an unauthorized user accessing systems via RDP. In addition, Corelight's x509.log captures certificate details for all TLS encrypted connections. The presence of self-signed or expired certificates can serve as another potential early warning indicator.

Corelight Encrypted Traffic Collection

To extend the platform's protocol logging capability, Corelight has developed proprietary encrypted traffic insights and detections that do not require break and inspect. Corelight's Encrypted Traffic Collection generates dozens of inferences and detections around SSL, SSH, and RDP traffic that analysts can use to identify the early stages of a ransomware attack.

For example, consider the use cases for RDP, which, according to the FBI, is "still by far the primary vector" for delivering ransomware. Corelight alerts on RDP brute-forcing activity and also flags the use of known RDP clients used in attacks, such as the Metasploit Scanner Client. These Corelight insights give analysts a fighting chance at identifying ransomware in the reconnaissance and initial access phase of the attack, before encryption occurs.

Corelight C2 Collection

Once a ransomware attack has established an initial foothold inside an organization a common next step is to establish a line of communication with the command and control (C2) server to receive further instructions and download additional payloads. These communications must cross the wire, and the Corelight C2 Collection illuminates this network activity with over 50 unique insights and detections that covers both known C2 toolkits and MITRE ATT&CK® C2 techniques to find novel attacks.

For example, Corelight alerts on the presence of C2 traffic associated with dozens of offensive toolkits, including those highly correlated with ransomware attacks such as Cobalt Strike, which the Cisco Talos Incident Response team reported was used in 66% of all ransomware attacks observed in Q4 2020. Proofpoint researchers reported in 2021 that the use of Cobalt Strike in cyberattacks was up 161% year-over-year. With the alerting capabilities delivered in the Corelight C2 Collection, security teams can spot ransomware C2s in the wild and potentially contain them before widespread encryption occurs.

Detecting known ransomware attacks

Corelight's Open NDR Platform offers two distinct capabilities for detecting known ransomware families. First, Corelight's support for Suricata means customers can run open source or commercial IDS rulesets that alert on ransomware families and toolkits. For example, customers can license Proofpoint's ET Pro ruleset from Corelight, which contains over 72,000 rules that cover numerous exploits and malware families connected with known ransomware attacks.

Second, Corelight's support for Zeek packages means organizations can write their own Zeek scripts to detect ransomware or leverage the ransomware detection work of the community, such as an open source Zeek ransomware detection package that monitors SMB transactions for more than 4,500 specific file names connected with known ransomware attacks.

Responding to ransomware attacks

When ransomware attacks successfully encrypt sensitive files and security teams must initiate containment and remediation efforts, Corelight's network evidence provides a time machine for analysts to quickly investigate how and where the breach began and assess its scope. This accelerated investigation can dramatically cut down on the time and cost associated with post-breach forensics. And where affected machines have been wiped and reimaged, Corelight's platform offers a continuous monitoring capability to ensure that containment has been 100% achieved.

Lastly, Corelight can also potentially support file recovery efforts post-ransomware attack via Corelight's file extraction and packet capture capabilities (delivered via Smart PCAP). Corelight's platform can extract and reassemble more than 200 file types such as PDFs and PPTs, and also selectively capture packets according to protocol with customizable byte depths. While these capture capabilities were designed primarily for forensic investigation purposes, they can also serve as file backups when the targeted files crossed the network prior to encryption by the ransomware attack.

corelight

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497