illumio

HOW TO STOP RANSOMWARE

Anatomy of a Failed Ransomware Attack: From Intrusion to Eviction in Hours

A global law firm uses Illumio to stop the breach before it damages the organization or its clients

It Should Have Been a Disaster...

A global law firm was hit by ransomware. But by using Illumio, they:

- Contained the attack to 12 servers across a hybrid cloud
- Isolated infected systems in seconds
- Stopped the attack in hours
- Prevented the loss of any data
- Protected their clients
- Preserved their business reputation

The Attack Timeline

MONDAY AFTERNOON:

A Phishing Email Arrives

An employee at the law firm receives an email from a client who had already been compromised. It contained malicious code disguised as a link to an Excel file. When the file didn't open, the employee contacts the IT help desk.

2:00 PM CENTRAL TIME:

The Attack Begins

The help desk technician copies the URL into a browser. A weaponized file automatically downloads, launches the malware, and infiltrates the machine.

2:00 PM – 3:40 PM:

The Attack Goes Undetected

The attackers use the technician's computer and the machine's access privileges to perform a slow and undetectable network scan. They find a SQL server they can access. They strike.

3:40 PM - 4:00 PM:

The Attackers Make Their Move

The attackers encrypt the server's database files, causing it to crash. The IT team sees the issue, investigates and concludes it was likely caused by ransomware.

4:00 PM – 4:50 PM:

Incident Response

The law firm orchestrates their war room and assembles an incident response team. They bring together IT and security staff with security consultants to track the spread of the ransomware and coordinate a response.

4:50 PM - 6:15 PM:

Understanding the Attack

Using Illumio's real-time application communications telemetry fed into the company's security information and event management (SIEM) tool, the incident response team identifies the "patient zero" help desk workstation and an additional 11 infected servers. Time is running out.

6:20 PM:

Illumio Ends the Attack

With just a couple clicks of a mouse on the Illumio console, the incident response team puts all 12 servers — including a Microsoft Azure cloud instance — into a ring-fence to quarantine with zero network access. They stop the attack cold.

6:20 PM – 1:00 AM:

Assessing the Damage

The attack ends, but there is still work to do. The incident response team needs to map the attack and see if the hackers stole any data, especially client data, which would require publicly reporting the incident and be a major blow to the firm's reputation.

TUESDAY – FRIDAY:

No Data Loss, Confirmed

The law firm hires a specialized incident response agency to investigate and provide a report on damage from the attack. When the investigation ends, the news could not have been better: No other systems had been infected and no data had been exfiltrated.

> Our security consultants told us they have never seen a company respond to a ransomware attack so fast. They said it's unheard of to limit an attack to a dozen systems. But we did, thanks to Illumio.

How Illumio Helped:
5 Steps to Defeating Ransomware

1. **Slow the Attack:** Before the attack, the firm had already greatly limited open pathways on its network by deploying Illumio's Zero Trust Segmentation access controls.
2. **ID 'Patient Zero':** By seamlessly integrating with other security tools, Illumio's communications telemetry helped pinpoint the first infected server.
3. **Visualize the Spread:** Illumio's real-time application communications map clearly showed the unusual activity from ransomware chatter.
4. **Stop the Attack:** Illumio's simple rule generation made it easy to create a policy in less than a minute to isolate the compromised servers.
5. **Aid the Investigation:** Illumio made it safe to access compromised server data and securely transfer it to a third-party firm for security analysis.

illumio

Stop Ransomware as Soon as It Strikes — With Illumio

Learn More: **www.illumio.com**
Go Deeper: **How to Stop Ransomware Attacks eBook**
Schedule a Chat: **Free consultation and demo**