Ransomware Attack Prevented: CYREBRO Incident Response Case Study

Global Manufacturing Company

Ransomware prevented

Mitigation steps in detailed report

Security hygiene enhanced

Immediate IR activated

About the Company

A global manufacturing company was established well over a century ago, with over 5,000 employees today and an annual revenue of over 1 billion USD. The company began moving past legacy tools and switching out the old to implement the new, although not all areas of the organization got the same amount of attention. For large multinational corporations, it's always harder to implement new or changing processes and technologies. Yet, a sufficient number of cybersecurity tools and processes must exist to defend against an attacker especially considering the rapid changes in the digital transformation and simplicity of remote work.

The Challenge

The manufacturing company received an alert that a "housekeeping event" occurred on its Domain Controller. In IT, "housekeeping" is a term that describes when IT personnel or software clear logs from a system or device, often to free up storage space.

In this case, the housekeeping event was indicative of a serious breach identified at the end of the Kill Chain. This means the attacker had finished manipulating the network and cleaned their tracks making it difficult for analysts to investigate the case. Prior to this alert, the manufacturing company was unaware that an attacker had infiltrated their network and was making lateral moves across their infrastructure. Adding insult to injury, the attacker had deployed ransomware into the company's network and activation could hit at any moment, turning a manageable cyber-attack into a time bomb with potentially catastrophic results.

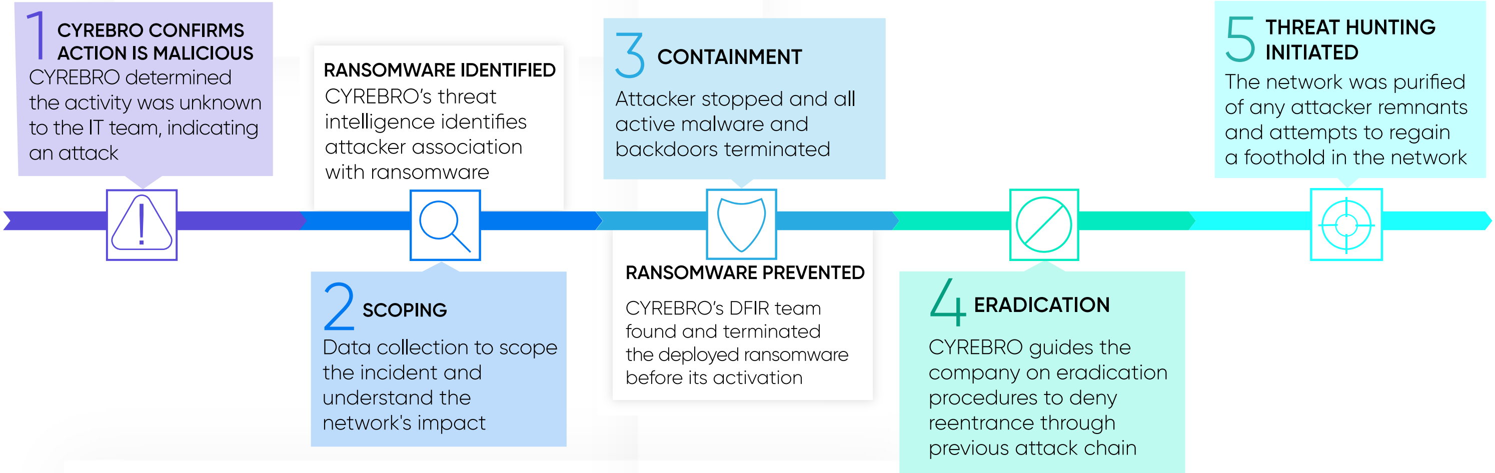
CYREBRO Investigation

Throughout the investigation, CYREBRO uncovered the actions and steps the attacker executed. After discovering that the attacker is known for ransomware, the DFIR team located the deployed ransomware. CYREBRO identified the threat as an APT and learned the attacker made their way into the manufacturing company's network through the RDS server that was connected to the internet and was unrestricted.

Once inside, they were able to move laterally across the network, harvest credentials for high privileged accounts, and gain access to the Domain Controller server. Clearing logs is a sign the attack is at the end of the Kill Chain, raising the urgency and time sensitivity of this incident.

Because CYREBRO's threat intelligence team identified that the attacker is known for ransomware attacks, together with the DFIR team they were able to quickly find and stop the ransomware from activating. A full IR was performed for the manufacturing company, from scoping to recovery. To conclude the investigation CYREBRO provided a detailed report of the investigation and launched a threat hunting project to eliminate any remnants from the manufacturing company's breached network.

Incident Response Timeline



1 CYREBRO CONFIRMS ACTION IS MALICIOUS
CYREBRO determined the activity was unknown to the IT team, indicating an attack

RANSOMWARE IDENTIFIED
CYREBRO's threat intelligence identifies attacker association with ransomware

2 SCOPING
Data collection to scope the incident and understand the network's impact

3 CONTAINMENT
Attacker stopped and all active malware and backdoors terminated

RANSOMWARE PREVENTED
CYREBRO's DFIR team found and terminated the deployed ransomware before its activation

4 ERADICATION
CYREBRO guides the company on eradication procedures to deny reentrance through previous attack chain

5 THREAT HUNTING INITIATED
The network was purified of any attacker remnants and attempts to regain a foothold in the network

Solution

Due to the severity and urgency of a housekeeping event, a quick response was vital for recovery and damage control. The manufacturing company had the CYREBRO SOC Platform in place, which was collecting the relevant and critical initial signs of the infiltration for investigation. This enabled CYREBRO's IR team to execute a very necessary swift and accurate investigation and response.

The CYREBRO Threat Intelligence team concluded that the malicious actor was known for ransomware attacks and the attack would have ended in a network-wide encryption of data. A copy of that ransomware was found on one of the servers, but no indication of execution was found.

CYREBRO performed a threat hunting project, which increased visibility over the client's network, detection of more attack remnants, and detection of attacker attempts to regain a foothold in the network and react accordingly. This step was the final step in ensuring the purity of the breached network.

The CYREBRO DFIR team was able to execute a complete IR process, removing the attacker from the network and denying all of their actions that threatened the manufacturing company's network.

Investigation Results

CYREBRO's investigation and immediate IR prevented a very serious ransomware attack along with potentially devastating financial and reputational damage. The payment of the ransom is only one issue (although the US average cost of a ransomware payment alone is growing past $6 million), the cost of business downtime can reach up to ten times the amount of the payment. Ultimately, CYREBRO rid the company of the attacker and any changes they made, enabling business to continue. Through quick and decisive actions, the company's security posture was hardened, as opposed to needing to pick up the pieces after a ransomware attack.

Benefits

Ransomware averted

Full-blown ransomware attack prevented, saving millions of dollars in lost data, systems, downtime, and lawsuits.

Immediate IR

Once breached, incident response was immediate with 0 ramp up time as CYREBRO's SOC platform was already in place.

Security hygiene enhanced

Recommendation to implement organizational and systematical best practices and identification of bad IT practices to correct.

Threat hunting

Visibility increased over the network, detecting any attack remains and attempts to regain a foothold in the network.

Detailed incident report

Full report of the incident, complete with details and can be presented to the company's stakeholders with simplicity and clarity.

False-positive elimination

Costly time consuming false positive verification eliminated and real positive identified.