Infrastructure Manufacturer Reclaims Control After Dual Ransomware Attacks

With potential financial, operational, and reputational consequences looming large, the client looked to Unit 42® to help protect operations and sensitive data.

Infrastructure Manufacturer Reclaims Control After Dual Ransomware Attacks

INDUSTRY MANUFACTURING | **COUNTRY** UNITED STATES

The Challenge

Dual ransomware attacks from Black Basta and LockBit crippled the operations of an infrastructure equipment manufacturer. The adversaries first exfiltrated sensitive data, then detonated ransomware that encrypted critical files within 24 hours. Unit 42® stepped in to help:

- Assess the scopes of the attacks and identify the initial access points and the extent of data exfiltration.
- Contain the threats by blocking ransomware indicators of compromise (IoCs) and initiate 24/7 threat monitoring.
- Eradicate the threat actors from the environment to prevent further lateral movement or damage and negotiate down the ransom demands.

The Results

73% reduction
In ransom payment due to expert negotiation

<5 days
To identify patient zero, the extent of data exfiltration, and block all known ransomware IoCs

2.5+ million
Files prevented from being exposed through negotiations

Unit 42's Rigorous Incident Response Approach for Superior Outcomes

Assess

Simultaneously assessed the scope of the ransomware attacks, utilizing existing firewall and VPN logs.

Investigate

Identified initial access point as a compromised contractor VPN account, immediately began threat actor negotiation, and discovered 3 TB+ of data was exfiltrated.

Secure

Blocked ransomware IoCs leveraging Cortex XDR® and initiated 24/7 threat monitoring. Successful negotiation led to a 73% reduction in the ransom demand.

Recover

Decrypted systems, restored data access, and helped the client regain operational capacity within 12 days.

Transform

Expanded Cortex XDR coverage from 70% to 100% of endpoints, implemented enhanced firewall rules, and provided ongoing threat monitoring through Unit 42 MDR.

"This attack was very challenging but Unit 42's knowledge, patience and guidance was invaluable."

Senior Director of Risk Management

Resolution Timeline

	Days 0–4 Crisis Intervention	Days 5–7 Decryption	Days 8–14 Restoration	Days 15–30 Fortification
Assess	Assessed firewall and VPN logs for initial visibility. Used Cortex Xpanse® to map the attack surface and identify potential vulnerabilities.	Determined full scope of the attack, including extent of data exfiltration — 3 TB+.		
Investigate	Identified Black Basta ransomware and initial access point as a compromised contractor VPN account without MFA.	Uncovered previous impact and data theft by LockBit.	Ensured system integrity and blocked further malicious activity.	
Secure	Blocked ransomware IoCs and initiated 24/7 threat monitoring.	Identified ~20 systems impacted by file encryption and 80 systems with attacker tool presence.	Rebuilt systems and restored data from backups, enabling the client to regain operational capacity within 12 days.	Implemented enhanced firewall rules to block identified IoCs. Continued 24/7 threat monitoring with Unit 42 MDR.
Recover		Initiated and successfully negotiated with Black Basta attackers, resulting in a 73% reduction in the ransom demand.	Expanded Cortex XDR deployment to cover 100% of endpoints to enhance visibility and protection.	Provided guidance to ensure long-term resilience against future attacks. Successfully negotiated with LockBit to prevent data exposure.
Transform				Ensured continuous security posture improvement through proactive threat hunting and ongoing monitoring.

Threat-Informed Incident Response

With Unit 42 Incident Response, stay ahead of threats and out of the news. Investigate, contain and recover from incidents faster and emerge stronger than ever before, backed by the full power of the world's leading cybersecurity company. Partner with us to gain peace of mind.

Backed by Industry's Best

Threat Intel

Extensive telemetry and intelligence for accelerated investigation and remediation

Technology

Palo Alto Networks platform for in-depth visibility to find, contain and eliminate threats faster, with limited disruption

Experience

Trusted experts who mobilize quickly and act decisively in over 1K incidents per year