



Incident Management

Fusing forensics and recovery for rapid response and restoration

Case Background

Our client, with an annual revenue over \$350M, 700 systems, and 400 users was impacted with BlackByte ransomware. Although EDR and 24/7 monitoring was in place before the incident, there was still a significant amount of exfiltration and encryption that occurred. The tactics used to exfiltrate data were not observed due to lack of visibility and encryption occurred due to misconfiguration of the EDR.

Business Challenge

The client needed to quickly contain and eradicate the threat actor and provide evidence to their parent organization that they were secure enough to resume operations and connectivity.

Unique Approach

MOXFIVE was responsible for containment, forensics, and recovery. We organized the chaos by overseeing and directing more than five different teams that were in the environment. We were able to put in work arounds due to the business challenges with network constraints that would have delayed their recovery for weeks. We were also able to provide insights into what data the threat actor had access to which contributed to reducing the ransomware payment by \$5 million dollars - a 94% decrease. We were also able to provide detailed documentation and briefs to partner organizations in order to re-establish connectivity quickly.

Conclusion

It's important to have an incident management layer as it enabled us to quickly address issues before they became problems. Being able to unify recovery, forensics, and negotiations helped ensure a rapid response and quick recovery.

RESULTS



Restored Tier 1 systems in three days. Remaining environments (Tier 2 and 3) restored in 16 days.



Sensitive data mapping helped reduce ransom by \$5 million dollars.



Quickly resolved containment issues and increased security posture for the business to resume operations.




Partnered with client to present debrief and resilience steps to parent organization.


OTHER USE CASES

- Business Email Compromise
- Extortion
- Compromise Assessment

MOXFIVE is a cybersecurity company helping organizations respond to incidents and minimize the risk of future attacks. Over the last decade, our team of experts has helped thousands of businesses respond to major incidents and saw firsthand that there needed to be a better way for organizations to get the technical expertise they need when they need it most. Through a combination of our technical experts and proprietary platform, we bring order to chaos and deliver a tailored incident response approach and resilience-minded path forward for clients of all sizes, faster and more efficiently.

 www.moxfive.com

 (833) 568-6695

 info@moxfive.com