KPMG cyber response aids a global telecom's threat recovery

The Challenge: Responding to a sophisticated global cyberattack

A global telecommunications provider operating in over 30 countries faced a critical cybersecurity incident involving a sophisticated Advanced Persistent Threat (APT) group. The breach was not a typical ransomware or disruption campaign, but a long-term covert operation aimed at strategic intelligence collection. The attackers exploited vulnerabilities in supply chain equipment and identity management systems, enabling them to move laterally across jurisdictions including North America, Africa, Europe, and Asia.

The attackers who were later identified as a nation-state-aligned group used highly sophisticated techniques such as spoofing legitimate network devices and reconfiguring systems in real time without disrupting operations, making detection extremely difficult. Their objective was to extract sensitive subscriber data, including identities, locations, and metadata that could be used for surveillance or targeting to avoid detection, maintain access, and leverage the ISP access to laterally move into high value networks of clients. Upon identifying the emerging and complex nature of this incident the clients team identified the need to engage KPMG to contain the threat and protect sensitive subscriber data.

The Solution: End-to-end incident response and forensic support

KPMG was engaged to provide a comprehensive suite of services, including incident response, forensic data analysis, threat hunting, and crisis management. To battle the threat, KPMG rapidly deployed a cross-functional team of specialists to support the client's internal response. They also brough in forensic experts in network and host analysis to trace attacker movement and identify compromised systems.

Furthermore, data specialists were engaged to manage and analyze the vast volumes of forensic data being generated and security engineers reconfigured existing monitoring to accelerate data extraction and reduce the noise caused by excessive query results, ensuring timely and actionable insights.

In parallel, threat hunting teams worked to identify indicators of compromise and uncover hidden attacker activity across the environment whilst crisis and incident management advisors supported executive-level decision-making and communications, ensuring the client had a clear understanding of the evolving threat landscape and the actions required. KPMG also provided continuous reporting and strategic recommendations, including containment strategies to reduce attacker mobility, remediation plans addressing legacy systems and logging gaps, and improvements to identity management practices.

As the investigation progressed, the scope of KPMG's support expanded significantly. And the services that were offered by KPMG grew to include data analytics, SOC expertise, data extraction and preservation, SIEM logging and monitoring enhancements, and long-term security transformation planning. This evolution reflected the client's growing trust in KPMG's ability to deliver end-to-end solutions that addressed both immediate threats and systemic vulnerabilities.

The Outcome: Containment, resilience, and a path to secure recovery

While the investigation remains ongoing, KPMG's intervention significantly reduced the attackers' ability to maneuver within the client's environment. Critical systems were secured, and a clear roadmap for secure recovery and long-term remediation was established. The client is now better positioned to detect and respond to future threats, with improved operational processes and a more resilient security posture. The evolving collaboration has also enabled the client to access a broader range of services—from data preservation to SOC transformation—ensuring readiness for future challenges.

To learn more about our Cyber Incident Response services and how we can help your organization, click here: Cyber response - KPMG Canada. **If you have experienced or have a question about a cyber incident, contact our team of incident response specialists email us at cyberincident@kpmg.ca or call our Toll-free telephone number: 1-844-576-4911**

Contact us

Our dedicated team is here to support your organization's unique needs.

Alexander Rau
Partner, Advisory Services - Cybersecurity
KPMG in Canada
+1 416-777-3450
alexanderrau@kpmg.ca

Guillaume Clément
Partner, Advisory, Cybersecurity
KPMG in Canada
+1 418-653-5335
guillaumeclement@kpmg.ca