References & Success Stories

KPMG Cyber Incident Response Services

October 2021

KPMG's Incident Response Experience

#1: Canadian Financial Institution	
Client Industry	Financial Sector
Project Description	KPMG was engaged by a client to provide data recovery services for laptops belonging to an executives of the institution that suffered a malware attack which deleted sensitive data that was not backed-up.
KPMG's Roles & Responsibilities	KPMG performed the following activities: • Imaged and collected data (including laptops) for forensic analysis • Conducted analysis to determine the source of compromise • Implemented various workflows and software tools to recover deleted data
Deliverables	Deliverables included: • Report with summary of findings outlining the results of KPMG's investigation • Recovery of deleted data from laptops

#2: Government Institution	
Client Industry	Provincial Government Organisation
Project Description	KPMG was retained by a client to assist in investigating a potential automated botnet attack against one of their third-party service providers, directly affecting government's ability to deliver services.
KPMG's Roles & Responsibilities	KPMG performed the following activities: • Obtained network and web server logs • Enriched the logs using GeoIP in order to gather additional analytic data point. • Using open-source data analytic tools, identified evidence of attacker reconnaissance, testing and bot attacks against the public webserver. • Identified unrelated attacks that were previously unknown to the third-party service provider
Deliverables	Deliverables included: • Incident response report outlining our findings and recommendations for the third-party service provided.

KPMG's Incident Response Experience (Continued)

#3: Private Organization	
Client Industry	Manufacturing Industry
Project Description	KPMG engaged by a manufacturing industry client to assist in investigating a potential employee misconduct who was also the IT administrator and responsible for managing the client's entire IT and security infrastructure.
KPMG's Roles & Responsibilities	KPMG performed the following activities: • Assumed entire network and security infrastructure was compromised. • Setup covert communication framework to covertly discuss engagement progress. • Obtained workstation logs, server logs and office 365 logs to identify the unauthorized activities performed by the IT administrator. • Performed a review of logs and correlated the activities to identify the root cause, using open-source data analytic tools • Identified any other attacks that may have occurred and have been undetected by client's security tools.
Deliverables	Deliverables included: • Incident response report outlining our findings and recommendations • Summary of the employee activities
#4: Large Financial Organization	
Client Industry	Financial Institution
Project Description	KPMG was engaged by a large financial company to assist with a digital forensic investigation. Specifically, KPMG was engaged to identify data exfiltration which may have occurred after the client identified suspicious activity originating from a computer system belonging to an employee.
KPMG's Roles & Responsibilities	KPMG performed the following activities: • Performed forensic imaging of the computer system belonging to the employee. • Utilized specialized software to analyze artifacts for activities such as externally connected devices, internet searches, and accessed files and folders.
Deliverables	Deliverables included: • Report with summary of findings and recommendations related to clients' data exfiltration incident. • Summary of suspected employee's malicious activity.

KPMG's Incident Response Experience (Continued)

#5: Retail	
Client Industry	Retail
Project Description	KPMG was engaged by a retail client who was targeted by an unauthorized user that accessed its network and installed a ransomware which encrypted a large amount of critical data in the weeks leading to one of their busiest online sale weekends of the year: "Black Friday" and "Cyber Monday." Many of the company's critical systems were unavailable after the attack. The unauthorized user was demanding Bitcoins (about $250,000 at the time of the incident) to decrypt the data. The client needed to restore its data and get its systems back in production as quickly as possible.
KPMG's Roles & Responsibilities	KPMG performed the following activities: • Imaged and collected data (including servers) for forensic analysis • Deployed an intrusion detection system and monitoring tools on endpoints to detect the presence of unusual activities on the endpoints and on network • Identified how the unauthorized user gained access to the network • Assisted client restore data from back-ups and immediately blocked the access.
Deliverables	Deliverables included: • Report with summary of findings outlining the results of KPMG's investigation related to the cyber security incident

home.kpmg/socialmedia