KUDELSKI SECURITY

CASE STUDY

Incident Response

Kudelski Security delivers rapid containment and remediation for a high-impact cyber attack.

> *"We always realized the importance of good response. But before we took our IR retainer with Kudelski Security, we didn't really understand the full advantages it could bring: a highly skilled team that helped us through our security incident/breach and guided our actions."*
>
> – Head of Network & Security Operations, Global Beverage Company

In a Nutshell

- **Sector:** Food and Beverage
- **Size:** 19,000 employees, operations in 80 countries
- **Offering:** Managed Endpoint Detection & Response, Managed Endpoint Prevention, 24x7 Threat Monitoring and Hunting, Computer Security Incident Response Team (CSIRT) Retainer, Technical Account Manager
- **Engagement:** A 20-day 24x7 IR engagement following a large cyber attack.

DAY 1: DETECTION

Kudelski Security detected malicious behavior on some workstations, Christmas Eve, 2019. Investigation revealed a large incident impacting 200+ servers and workstations from offices on three continents.

DAY 1: ANALYSIS

The Kudelski Security team developed a crisis management strategy that enabled seamless communication between the client's leadership, their technical teams, and the Kudelski Security task force.

- Remote investigation kicked off immediately with the engagement of 15 Kudelski Security cyber intrusion experts from our Cyber Fusion Center (CFC).
- They worked around the clock, in Europe and the US, to establish an initial understanding of the attack: timeline, entry points, persistence, and pivoting systems.
- Forensic analysis was carried out to analyze the attack profile and establish indicators of compromise (IoCs).
- Further, we added new log sources (SIEM) to eliminate monitoring blind spots and facilitate correlation of threat data.

DAY 1: CONTAINMENT

- CFC teams isolated compromised systems using CrowdStrike technology.
- They supported the client in the implementation of a domain group policy object (GPO) to limit spread by blocking remote access to local accounts (the method for attacker lateral movements).
- The CFC then validated that containment worked.

CASE STUDY

Incident Response

Outcome

- Rapid detection of lateral movement in environment
- Real-time visibility of threat actor activities and footprint
- Immediate containment
- Full remediation across all geographies
- Resilience strengthened by remediation and hardening recommendations
- New IoCs and TTP discovered
- Support for Global CTO reporting
- Slide deck preparation for executive board reporting

DAY 2-18: ERADICATION & RECOVERY

- A war room was quickly set up in order to facilitate further analysis and steer remediation.
- The investigation revealed that the attackers had been present for a long time in parts of the environment that we were not yet monitoring with an objective of crypto mining.
- Further threat hunting and attack monitoring was carried out to discover new IoCs and validate eradication.
- We deployed CrowdStrike endpoint detection and response agents onto multiple systems and locations and were able detect new IoCs, and attacker tools and techniques within minutes. This rapid detection enabled further real-time monitoring, which in turn, supports enhanced threat detection and remediation.
- Through remediation, we rapidly got the client back to business-as-normal. The client restored compromised systems, set up monitoring rules to validate eradication, and reconnected systems to the network.

POST-INCIDENT ACTIVITY

The CFC teams provided further support after the incident:

- Identification of several resiliency gaps and recommendations on how to address them
- Reports for the Global CTO
- Reports for board and senior management

FINAL RESULT

In 20 days of round-the-clock action: attack contained, full remediation, risks reduced, resilience built.

Impact on business reduced to a minimum.

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY