A security breach is every company’s worst nightmare. Learn what one company did after the incident.

A large media company must be accountable to its advertisers, customers and users to protect their information. Major data security breaches that make the news damage a company’s brand, and can lead to catastrophic financial loss, customer mistrust and legal penalties. Once malware has infiltrated a network, the effects can be incredibly damaging.

No organization wants to be the next headline, so when this company found evidence of a possible malware infiltration, it took immediate action.

**What was the best way to approach this challenge?**

* Provide immediate incident response services, scouring the network for malicious code.
* Analyze all information collected for malware and signs of intrusion.
* Isolate the incident to prevent further damage and provide recommendations to help prevent a future attack.

**PROJECT OVERVIEW**

**Organization Size:**
More than 10,000 employees

**Organization Industry:**
A large broadcast media company

**Challenge:**
To isolate a network compromise, determine the cause and remediate issues to avoid future attacks.

**IMPACT**

* Isolated security incident immediately
* Received recommendations for remediating issues
* Obtained intelligence on the cause of the compromise
* Maintained reputation and credibility
INCIDENT RESPONSE SERVICES:
Immediate Response and Remediation

Pinpointing the Infection
Optiv used hardware and software technology, as well as the client’s existing security controls, to pinpoint possibly infected assets within the network and critical servers.

Isolating the Incident
Then, they analyzed all information to see if malware was indeed present. Fortunately, Optiv was able to isolate the situation and found that no sensitive information had yet been lost.

Performing Analysis
Optiv performed binary analysis and deep-dive reverse engineering to examine the issue and pinpoint the attack surface in the environment.

Remediation
Optiv then communicated its recommendations for remediation based on how the network was attacked in the first place.

Preventing a Future Attack

The realization that your organization might be under attack is a terrifying feeling. When this large media company found evidence of a compromise, it immediately reached out to Optiv for incident response services.

Because of Optiv’s rapid, strategic response, the security incident was isolated and the loss of sensitive information was prevented. As a result, the client:

- Stopped the attack in its tracks and isolated any damage.
- Understood why the breach happened, and how to prevent future attacks.
- Received a remediation plan to bring the incident to a close.
- Kept its reputation and creditability strongly intact