Security Incident Response for a Warranty Solutions Provider

Company Background

The client provides warranty solutions and facilities management services to organizations in the HVAC/R and plumbing industries. They're a subsidiary of one of our Managed Service Provider (MSP) clients.

Business Challenge

The client called us because their IT environment was infected by ransomware that had encrypted their servers. This was an issue not only for the company contacting us but also for their parent company (the Stratosphere MSP customer) and a sister company, a P&C insurance provider, due to the fact that all three organizations operated in a single shared hosted server environment.

Stratosphere Networks Solution

Although we had done some project work for them, the client wasn't using our managed cybersecurity services – which we recommend to reduce the chances of a data breach and facilitate rapid remediation and eradication of threats in the event of an incident. However, our team was still able to resolve the issue quickly with our incident response services.

First, after an immediate assessment of the incident, our team of security analysts instructed the client to shut everything down to contain the spread of the infection. Although in a managed environment we would have the ability to gather forensic information from the systems first, the fact that this was not a current customer and did not have any of our tools in the environment necessitated immediate containment as a top priority.

Next, we dispatched our Computer Security Incident Response Team (CSIRT) to the site. We worked with the customer's IT team to create a temporary quarantine network. After that, we began bringing machines online one-by-one to deploy our security solutions, perform triage, and identify/remediate any threats. We confirmed that TrickBot malware had infected their IT environment with Ryuk ransomware. Our team triaged and cleaned up the affected machines with the following advanced cybersecurity solutions:

- Network Managed Detection and Response (MDR)
- Security Information and Event Management (SIEM)
- Endpoint MDR
- Next-gen endpoint AEP protection platform with deep learning malware detection, exploit prevention and anti-ransomware features.

Additionally, to ensure the ransomware didn't spread to the other two companies sharing the client's hosted server environment, our CSIRT team also worked in parallel with our Cybersecurity Engineering team to proactively deploy our MDR and AEP protection solutions to those organizations. During this time we also actively monitored their environments for signs of ransomware.

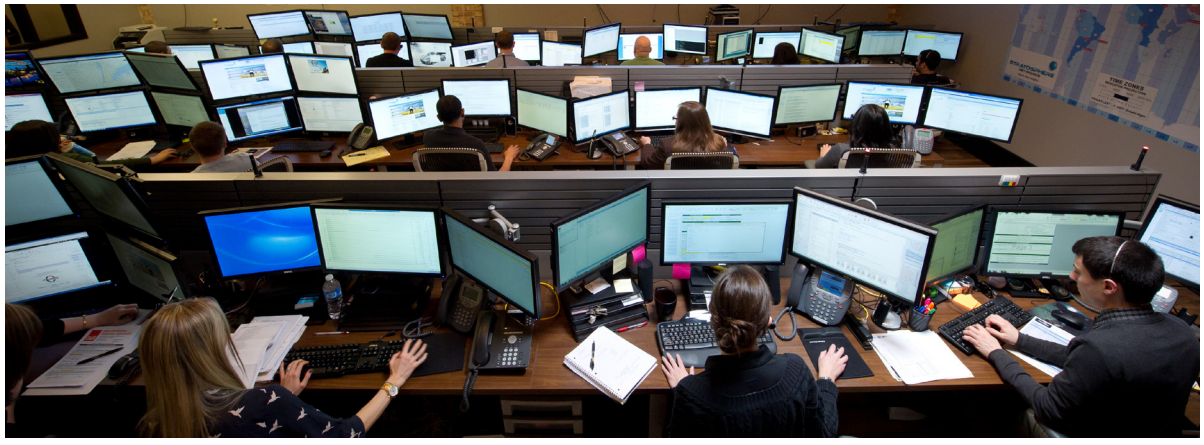
Ultimately, we implemented these tools for approximately 300 endpoints and completely restored the client's business operations in just two and a half days. In that time frame, we also contained the ransomware, got the client back up and running, and successfully implemented proactive prevention and detection countermeasures against ransomware infection for the client's parent and sister companies.

Benefits

The client now receives protection from Stratosphere's Managed Security Services Provider (MSSP) offering, including the following solutions, features and advantages:

- Network and endpoint MDR
- SIEM
- Anti-virus and AEP endpoint software
- Security Operations Center as a Service (SOCaaS)
- Continued incident response services
- Proactive threat hunting and analysis
- Malware detection
- Crisis handling guidance
- Data breach notification
- Overall reduced data breach risk level

Ultimately, we advise businesses to implement our proactive managed security services to dramatically reduce the chances of breaches like these occurring in the first place and ensure efficient and rapid remediation if there is an incident.



Our state-of-the-art Security Operations Center