INCIDENT RESPONSE

GLOBAL MANUFACTURER

CASE STUDY

CSIS prevents a high severity incident from becoming a complete crisis scenario.

Customer Profile

A global innovator within the medical-device manufacturing industry headquartered in Denmark.

Service Overview

The CSIS Security Analyst Team detected, investigated, and remediated a high-severity incident, which, had it gone undetected, could have led to a devastating loss of data.

The Attack

The CSIS Managed Detection and Response (MDR) Team was notified via the Microsoft Sentinel Platform of a low-criticality alert. The alert was escalated immediately upon investigation, and the Initial Triage confirmed the incident was, in fact, of high severity. Malware detection had been confirmed on our customers' endpoint.

The MDR Analyst Team promptly contained the malware and prevented further lateral movement through file quarantine and process execution stop. Microsoft Defender for Endpoint (MDE) blocked the Command and Control from connecting successfully. The machine had been effectively isolated, and the MDR Analyst Team could securely proceed with the investigation.

After scanning the dropped malware, CSIS's customer was instructed to localize the infected drive and to ship the collected drive to the CSIS MDR Team for further analysis.

Quick escalation from the CSIS MDR Analyst Team and prompt remediation by CSIS's customer resulted in containing the malware with minimal impact.

The CSIS MDR Engineering Team took the next steps: blocking the IOCs in the customer's Microsoft Defender for Endpoint and creating custom queries for Threat Hunting activities.

Further analysis revealed a previously unidentified malware, now known as "Raspberry Robin". https://redcanary.com/blog/raspberry-robin/

Key takeaways

While handling this incident, the CSIS Team provided a professional and prompt response, which was crucial in the containment and remediation of this cyber attack, even when faced with advanced malware which has previously been unidentified.

In CSIS's dedication to ongoing prevention and hardening of our customer's security posture, CSIS issued a full forensic report on how to best prevent such an attack from happening in the future.

Rest Assured

The leader in actionable and intelligence-driven
detection and response services