VIGILANT

SUCCESS STORY

Client:
NATIONAL RETAILER

Solution:
VIGILANTMEDR

VigilantMEDR Saves Thousands of Customers' Credit Card Data from Ransomware Attack

Using a strong, intelligent, and complete approach to endpoint security, VigilantMEDR is able to protect point-of-sale systems with increased efficiency.

Attack Impact Resistance

24/7/365 Managed Threat Hunting

Visibility and Analysis

BUSINESS CHALLENGE

Point-of-Sale (POS) systems are a high volume, high usage aspect of everyday business and therefore carry a particularly dangerous risk. The technology is ever-evolving and in need of regular updates to keep the security up-to-date from the vendor side. Threat actors find these enticing targets irresistible, as they look to gain access by exploiting a vulnerability. Once the infiltration phase is complete, malware is installed to spread through the system and steal customer data, such as credit card information – exfiltrated to another location accessible by the attacker.

VIGILANT SOLUTION

A large retail client* using POS technology unwittingly encountered a hacker by uploading a routine software update with an embedded malware attack package hidden inside. Because the attack had evaded the vendor's anti-viruses and firewalls, it slid undetected into the client's system. The malware immediately started collecting credit card data and began preparing to send it offshore to Europe. Fortunately, **VigilantMEDR** through our Adaptive Intelligence Process, immediately saw the change in network behavior.

**Note: for security reasons, Vigilant never reveals the identity of our clients.*

OUTCOME

The reality of the modern cyber dilemma is that even "good practices" with trusted allies and Point-of-Sale tech vendors can still result in vulnerabilities. In this case, with VigilantMEDR in place, the client was spared a disaster. Our collaborative Vigilant Hunt Team instantly notified the client, and we fully remediated the system as well as notified the vendor of their breach. As a result, a potentially expensive and damaging attack was prevented, while thousands of their customers' credit card data was saved and secured.

Why MEDR?

The best security never cuts corners but instead combines protection preservation elements like: endpoint detection and response and an adaptive intelligence process (human, automated and artificial). Vigilant Managed Endpoint Detection and Response (MEDR) sets a new standard in stopping breaches with unparalleled real-time and historical visibility across endpoint events and activities – to detect when something's not right and quickly act to eliminate the threat – every time.