BD and Attivo Networks Provide Visibility and Detection of Cyberattacks on IoT Medical Devices

Collaboration Advances Medical Device CyberSecurity

Attivo Networks® Receives Validation for Attivo BOTsink® Deception-Based Threat Detection through BD Product Security Partnership Program.

Joint Solution Brief

Attivo Networks® has expanded its IoT portfolio and received certification for Attivo BOTsink® deception-based threat detection through the BD (Becton, Dickinson and Company) Product Security Partnership Program. The Attivo Networks ThreatDefend™ Detection and Response Platform provides decoys and lures to misdirect potential attackers away from production assets. As a result of this collaboration, the BOTsink® solution decoys now offer software to create mirror-match decoy authenticity on certain BD products. This produces an environment where a potential attacker cannot discern between real and fake assets; ultimately, revealing their activities as they try to scan systems or attempt to download malware onto these devices.

Challenges

The Internet of Things (IoT) is revolutionizing the healthcare industry by changing the way professionals deliver care to patients and how patient data is collected, shared and stored. This new innovation comes with many benefits, however with the increased use of internet connected devices, comes additional security risks. These connected devices can become the target for medical device tampering and become a primary target for ransomware attacks as threat actors seek monetary gain in return for restoring services. Additionally, medical device networks are often overlooked in the IT security monitoring infrastructure providing attackers opportunities to infiltrate and persist in the network undetected.

In a survey of 370 professionals in the medical device/IoT field, over one-third experienced a cybersecurity incident in the past year.[1] If the medical device/IoT field mimics other industry trends, the number of incidents is only going to increase. What is particularly alarming, though, is that since medical devices are built to last longer than most technology, the devices weren't initially built to cope with the 2018 threat landscape.[2]

To combat the evolving attack surface, organizations need tools that stay one step ahead of attackers by not only preventing attacks but also detecting and responding to them early.

The ThreatDefend Deception and Response Platform

The Attivo Networks ThreatDefend™ Platform, which includes the BOTsink deception servers, creates an in-network deception environment designed to outmaneuver modern-day attackers and deceive them into revealing their presence. Dynamic deception and decoys that run production asset software are designed to replicate production servers, end-points, and specialty devices such as IoT medical devices, Industrial Control devices, and Point-of-Sale (POS) terminals. High-interaction network and end-point deception lures and decoys reduce time to detection, while automated attack analysis, high-fidelity alerts, third-party integrations, and playbooks accelerate incident response. Visibility tools provide attack path vulnerability assessments and time-lapsed replays, empowering teams with insight into attacker lateral movement and security gaps.

About Attivo Networks

Attivo Networks® is the leader in deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber-attacks. The Attivo ThreatDefend™ Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. Attivo Camouflage dynamic deception techniques and decoys set high-interaction traps to efficiently lure attackers into revealing themselves. Advanced attack analysis and lateral movement tracking are auto-correlated for evidence-based alerts, forensic reporting, and automatic blocking and quarantine of attacks.

www.attivonetworks.com

Attivo NETWORKS

BD

Joint Solution Brief

The Joint Solution

The Attivo BOTsink deception solution complements protections for certain BD products by placing decoys that appear as production IoT devices to confuse, trip up, and ultimately detect attackers. BD employed a rigorous evaluation of the Attivo BOTsink technology to ensure it is compatible with certain BD products and performs as indicated. Additionally, the Attivo solution provides attack analysis with indicators of compromise and attacker tactics, techniques, and procedures along with actionable forensics for remediation and threat hunting to identify compromised systems from all places within the network.

Key Benefits:

- Detection of attacks on corporate assets and medical devices
- Visibility into network time-lapsed changes
- Identify and record attacker lateral movement
- Improve time-to-respond with 3rd party integrations to isolate and block attacks

Use Case: Ransomware:
Windows-based devices, including medical devices, are vulnerable to malware that targets these operating systems, as demonstrated by the WannaCry outbreak in 2017. However, the Attivo Networks deception platform can efficiently detect when such infections occur, stall the attack, and prevent the ransomware from spreading, all while giving early warning of the infection.

Use Case: Early Detection
Windows-based devices, including medical devices, can also be leveraged by attackers to establish and maintain persistence on a network and spread throughout the environment. Medical device networks are often overlooked in the IT security monitoring infrastructure providing attackers opportunities to infiltrate and persist in the network undetected. Without a way to detect when attackers are in these systems and networks, the security team remains blind to such activity and creates an opportunity for the intruder to stay hidden within the environment. The Attivo Networks BOTsink® solution can detect when attackers are using the medical device network to conduct malicious activities.

Conclusion

The combination of early detection, attack analysis, and comprehensive forensic information provides a highly efficient platform for detection of advanced threats and continuous threat management. By using decoys to obfuscate the medical device landscape for attackers inside the network, organizations can better protect their medical device infrastructure.

[1] The Internet-of-Things. A revolutionary digital tool for the healthcare industry

[2] IoT Medical Devices a Major Security Worry in Healthcare, Survey Shows