Attivo NETWORKS®

Deception for Attack Detection of IoT Devices

As the amount of devices connected to the Internet of Things (IoT) continues to explode, the serious security complications surrounding these devices must be addressed for any organization concerned about their data and other critical assets. This document will address those concerns with the latest in security for connected devices—deception technology.

Deception techniques abandon the reliance on known attack patterns and signature monitoring, and instead use advanced luring techniques and engagement servers to entice an attacker away from valuable company servers. Bridging the detection, prevention, and response to incidents, deception is quickly becoming a critical asset of network security.

Background

There's no debate that the Internet of Things has been growing rapidly and will continue to see tremendous growth as technology expands with customer needs. And while 2015 is often referred to as the year of IoT, predictions are that the most significant growth is yet to come. BI Intelligence reports that $6 trillion will be spent on IoT solutions over the next five years with businesses as the top adopters to lower operating costs, increase productivity, and expand into new markets or develop new products. Additionally, Gartner estimates that 6.4 billion connected devices will be in use in 2016, up 30 percent from 2015. In 2016 alone, a predicted $546 billion will be spent on consumer devices while enterprises will top $868 billion with the use of connected devices. As IoT platforms continually make IoT applications faster and cheaper to develop, the growth of IoT connected devices will only accelerate.

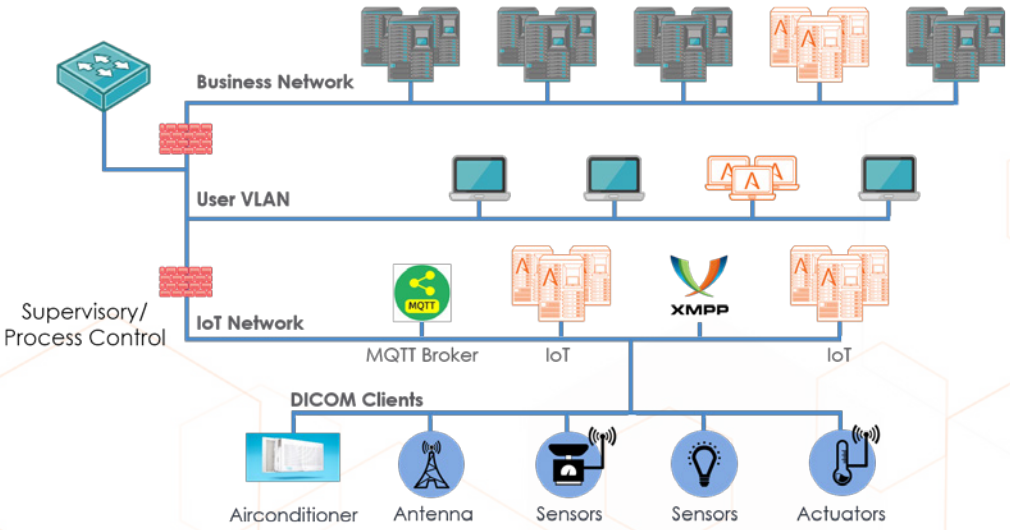
How Enterprise Executives View IoT Security

Source:Tripwire/Atomic Research

As the IoT ecosystem continues to accelerate, so do the cybersecurity threats associated with connected devices. As Ajay Kumar writes for TechTarget "Any device connecting to the Internet with an operating system comes with the possibility of being compromised, in turn becoming a backdoor for attackers into the enterprise". And as the projected 6.4 billion new devices are connected in 2016 alone, 6.4 billion new potentially exploitable devices are created for enterprises engaged in the IoT ecosystem. The new potentially exploitable devices are especially problematic given that IoT devices are just as susceptible to the types of cyberattacks that have been plaguing organizations, such ransomware, and as Nick Lewis writes for TechTarget, "While their attack surface may be smaller than a traditional desktop or server, when all IoT devices are added together, even minor security issues will turn into significant problems". In essence, the new surge in IoT devices will be a cyber attackers new haven.

Solution

As cyber attackers start to penetrate secure networks through IoT "backdoors", a new weapon must be added to the cybersecurity arsenal of every organization. A mature cybersecurity defense will include the typical prevention techniques as well as visibility to catch inside-the-network threats in real-time, identifying different threats, their threat levels, and an incident response playbook to remediate infected systems. The ThreatDefend™ platform provides inside-the-network threat detection for all types of threat vectors including ransomware, phishing, stolen credentials, and reconnaissance attacks. Appearing as the production assets of the environment it is placed in, the ThreatDefend Deception Platform is customized to fit into any landscape, which creates a trap out of any type of network, including IoT.



The Attivo Networks IoT solution provides deployment of deception technology across widely used protocols including XMPP, COAP, MQTT, and DICOM based PACS servers. These protocols are used by IoT vendors to support a wide array of applications that allow for more cohesive machine-to-machine communication and monitoring concerning critical data and machine status.

Customers can configure the Attivo ThreatDefend Deception Platform to look identical to the IoT devices on their network. The Attivo BOTsink® engagement servers and decoys appear as production IoT servers and services, deceiving attackers into thinking they're authentic. By engaging with decoys and not with production devices, the attacker reveals themselves and can be quarantined and studied for detailed forensics. The Attivo analysis engine will analyze the attack techniques, the lateral movement of the attack, which systems are infected, and provide the signatures required to stop the attack. The attack analysis can then be used to improve incident response by automatically or manually blocking and quarantining the attack through integration with third party prevention systems.

About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com