SOLUTION BRIEF

DECEPTION FOR ATTACK DETECTION OF IOT DEVICES

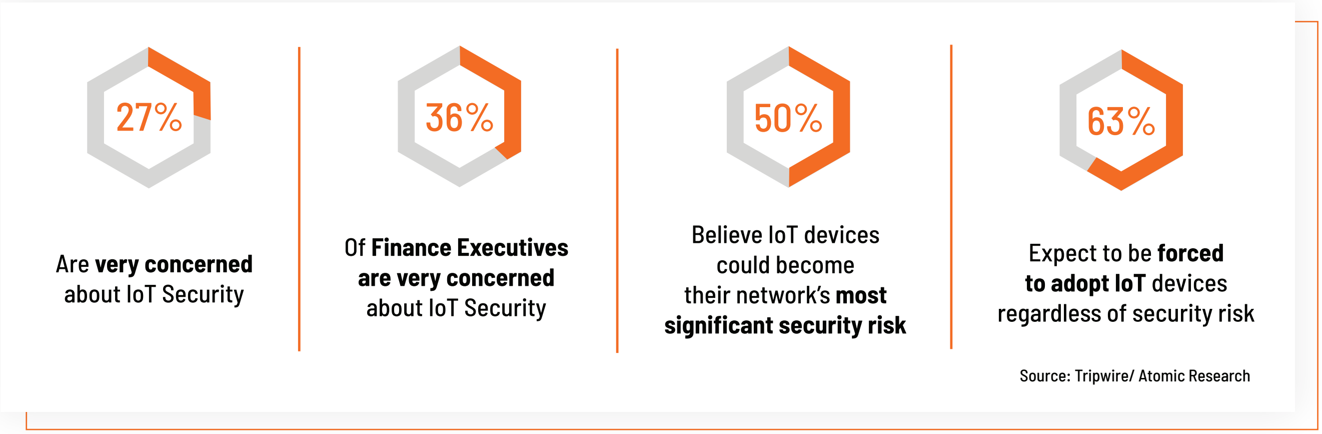
As the amount of devices connected to the Internet of Things (IoT) continues to explode, any organization concerned about their data and other critical assets must address the significant security complications surrounding these devices. This document will address those concerns with the latest in security 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. Deception is bridging the detection, prevention, and response to incidents, quickly becoming a critical asset of network security.

BACKGROUND

IoT systems and solutions are iterating rapidly, as emerging tools and technologies like smart speakers, machine learning, and 5G enable huge gains to efficiency and control at home and in the workplace. Business Insider Intelligence reports project that there will be more than 41 billion IoT devices by 2027, up from about 8 billion in 2019[1]. Additionally, Gartner, Inc. forecasts that the enterprise and automotive Internet of Things (IoT) market will grow to 5.8 billion endpoints in 2020, a 21% increase from 2019[2].

Utilities will be the highest user of IoT endpoints, totaling 1.17 billion endpoints in 2019, and increasing 17% in 2020 to reach 1.37 billion endpoints.

How Enterprise Executives View IoT Security



Source: Tripwire/ Atomic Research

[1] https://www.businessinsider.com/internet-of-things-report

[2] https://www.gartner.com/smarterwithgartner/lessons-from-iot-early-adopters/

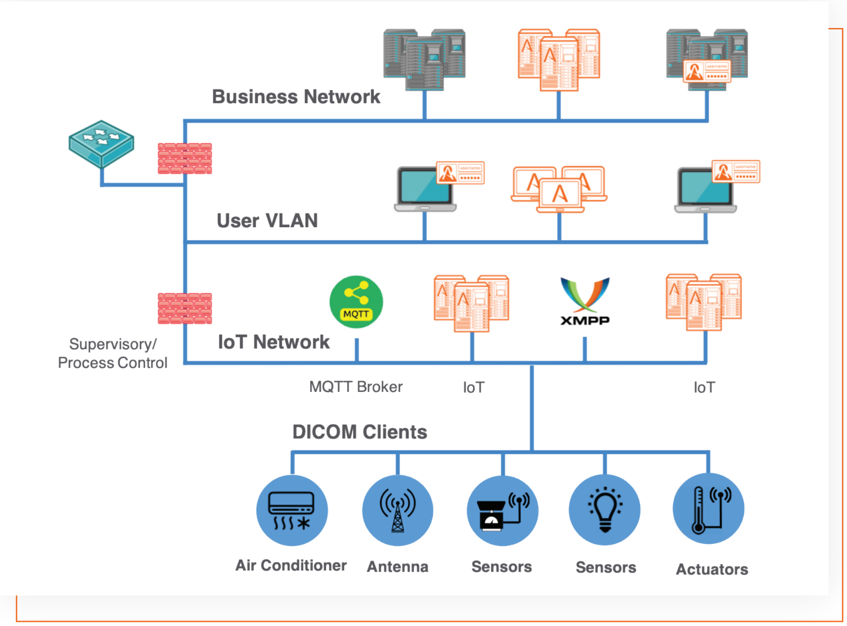
CHALLENGES

As IoT platforms continually make IoT applications faster and cheaper to develop, the growth of IoT connected devices will only accelerate. As the IoT ecosystem continues to accelerate, so do the cybersecurity threats associated with connected devices. Any device connecting to the Internet with an operating system comes with the possibility of compromise. If an attacker succeeds, these devices become backdoors into the organization. As organizations connect the projected 41 billion new devices in 2027, they create 41 billion new potentially exploitable devices for those 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 plaguing organizations for years, such as ransomware.

Organizations often overlook the security aspects of an IoT project, since the primary focus centers on service delivery and operations. As long as the deployment works, security is an afterthought. Even if it is part of the deployment plan, many IoT devices lack built-in security features, such as audit logs and malware protections. IoT devices can't run an antivirus solution if it even exists, and many devices lack the computing power to run one in the first place. Organizations may try to install compensating controls, such as firewalls, or deploying on a separate VLAN, but that does not prevent a device compromise. Often, they must rely on manufacturers to patch security flaws, which may not occur, and then deploy them to all the vulnerable devices. The lack of a central IoT management solution makes this a labor-intensive process.

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. Cybersecurity defenses will need to include the typical prevention techniques as well as visibility to catch in-network threats in real-time, identifying different threats, the level of those threats, and an incident response playbook to remediate infected systems. These new solutions will also have to address detection, which is not dependent on loading new software or gathering log data on these devices. The solutions must also address the long lifetimes of these devices, which can result in using end-of-life products that no longer have security updates available.



The ThreatDefend® platform provides in-network threat detection for all types of threat vectors, including ransomware, phishing, stolen credentials, and reconnaissance attacks. The ThreatDefend Deception platform decoys appear as production assets in the environment and are customized to fit into any landscape, creating a trap out of any network type, including IoT. The Attivo Networks IoT solution provides deployment of deception technology across widely used protocols, including XMPP, COAP, MQTT, HL7, 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 systems 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 the platform can quarantine and study their activities for detailed forensics. The Attivo analysis engine will analyze the attack techniques and the lateral movement activities of the attack, identify which systems are infected, and provide the signatures required to stop the attack. Security teams can then use the attack analysis 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®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.