Bastille

SECURITY FOR THE INTERNET OF RADIOS

WHITE PAPER

Security for the Internet of Radios

REAL THREATS, RIGHT NOW, READY OR NOT

bastille.net

Table of Contents

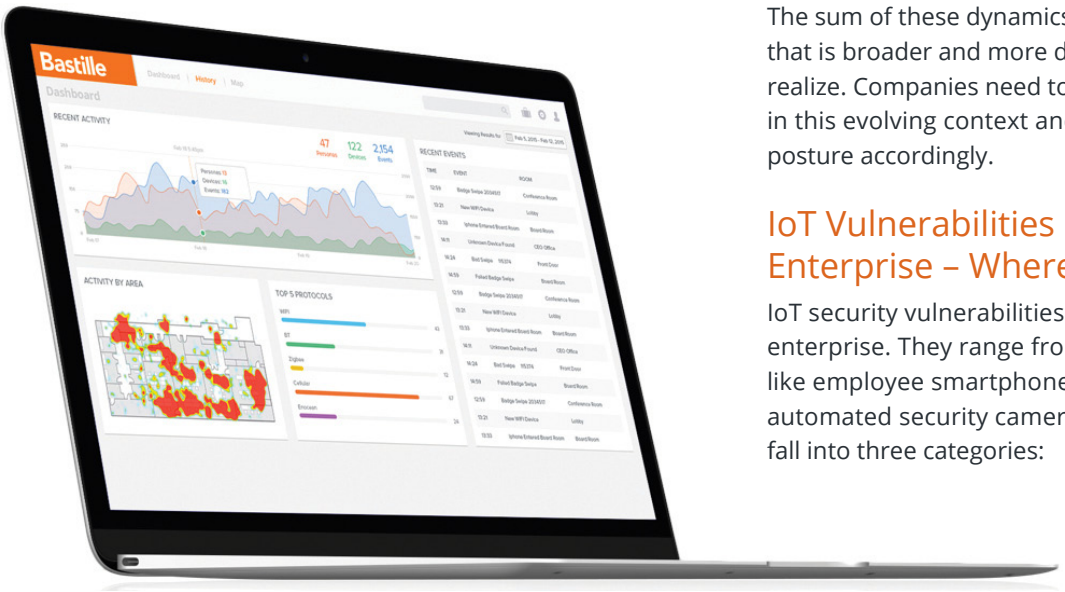
Threats are becoming more complex as criminals look for new ways to use technology in their quest for valuable data. As the number of connected devices grows to more than 50 billion by 2020, the IoT will provide an unprecedented expansion of new threat vectors and Enterprise companies need to be able to respond. Bastille is providing the security solutions to allow Enterprise companies to rapidly respond to this new threat vector.

It's Time to Take the Blinders Off

The Internet of Things is no longer a nebular IT security concern – it's a fully formed enterprise threat. By 2020, experts estimate that more than 25 percent of identified enterprise attacks will involve IoT. Disproportionately, IoT will account for less than 10 percent of IT security budgets.[1]

To stay ahead of this threat, smart enterprises are tackling this vulnerability head on. This starts with acknowledgment of three key dynamics shaping the IoT security landscape:

First, IoT security isn't an emerging threat – it's here. There is nothing "emerging" about IoT-related security threats. In 2016, 6.4 billion connected devices (or "things") will be in use worldwide with 5.5 million new ones connecting every day.[2] This means more attack vectors and more opportunity for exploitation.



Threats across the enterprise environment.

Second, IoT has blurred the line between personal, operational and enterprise security. An automobile's systems overtaken mid-drive? It's happened. Keystrokes intercepted? In less than 10 seconds. These are the kind of examples that come to mind when most people think of IoT security exploits. But, what about a perpetrator intercepting keystrokes or a building control system hack taking down a data center? These are real, enterprise-grade threats and point to a larger issue. The distinction between consumer and enterprise security is an outdated construct. Companies that don't embrace this view will find themselves attractive targets for cyberattack.

Third, WiFi security is not enough. Many companies rely on secure WiFi to protect against wireless threats. But, only a subset of wireless devices communicate across the RF spectrum using WiFi protocols. Billions more connect using non-WiFi protocols, which leaves these organizations wide open to nefarious activity.

The sum of these dynamics equates to a threat landscape that is broader and more dangerous than many enterprises realize. Companies need to understand their weaknesses in this evolving context and calibrate their security posture accordingly.

IoT Vulnerabilities in the Enterprise – Where Are They?

IoT security vulnerabilities are everywhere across the enterprise. They range from obvious personal devices like employee smartphones to "hidden" culprits like automated security cameras. These threats typically fall into three categories:

Employee-related threats: The usual suspects are employee's laptops, tablets and smartphones. While these are often governed by BYOD and IT policies, the security gains of these policies are marginal at best. Fifty-one percent of millennials in the workforce admit to knowingly disregarding these policies. Other threats include wearable mobile devices (FitBit, Apple Watch, Garmin, etc) as well as less conspicuous devices like wireless-enabled pacemakers and insulin pumps.

MOST VULNERABLE ENTERPRISE TARGETS

- **Data centers –** a simple 4G hotspot left behind can be a gateway to an information goldmine
- **Executive offices/boardrooms –** an antenna in a delivery package can put hackers in close proximity to targets
- **Automated building systems –** hackers can easily access HVAC, security and building access system data
- **Personal computer peripheral devices –** wireless keyboards and mice can give uncontrolled access to enterprise data

Vendor/Contractor-related threats: Mobility has transformed the service industry. Workers in construction and repair, vending, delivery and other services frequently use mobile handheld devices and RFID tracking technologies to perform tasks. Others have network access credentials. When Target was hacked in 2014, resulting in a massive credit card data breach affecting 70 million customers, the initial intrusion was traced back to an HVAC technician.

Industrial Control-related threats: These include basic automated building control systems like security and heating/cooling. They also include sophisticated supervisory control and data acquisition (SCADA) and distributed control systems found in industrial sectors (electrical, water, oil and gas) and critical infrastructure.

Why Conventional Wireless Security Can't Touch the IoT Threat

Conventional wireless security solutions focus on perimeter network defense. UTM, IPS, IDS and authentications solutions are great at preventing, detecting and monitoring threats coming over the network. But, they're inept at protecting against IoT-related attacks.

Bastille's sensors are installed on-premise and link to our SaaS cloud analytics platform.

Unlike traditional IT security exploits, IoT threats gain enterprise access through the broader Radio Frequency (RF) spectrum. It's not just a laptop or smartphone accessing corporate WiFi that presents a threat; it's any device enabled by Bluetooth, NFC, RFID, Z-Wave, ZigBee or 2G/3G/4G protocols.

It's no longer enough to protect the perimeter. Enterprises need to protect themselves against threats spanning the entire RF spectrum emerging on both legacy and tomorrow's IoT protocols.

COMMON DEVICE PROTOCOLS

- WiFi - wireless local area network using 2.4 gigahertz and 5 gigahertz radio bands
- Cellular - 2G, 3G, 4G, LTE
- Bluetooth/BLE - consumer mobile products and wearables
- ZigBee - Mesh network home automation
- Z-Wave - Mesh networking for industrial sensing
- DECT - Wireless headset
- Enocean - Low-power RF
- nRF24 - Mouse/keyboard detection

It's important to note that many devices connect to the RF spectrum are using proprietary protocols, which means enterprises can't get "under the hood" to inspect and fix vulnerabilities that arise in their unique IT ecosystem. Many of these device protocols were meant for a single use including IoT-enabled light bulbs, wireless keyboards and mice, and industrial controls like pressure sensors and water gauges. In most instances, these devices and their protocols don't support security patches – even when the manufacturer discovers a vulnerability.

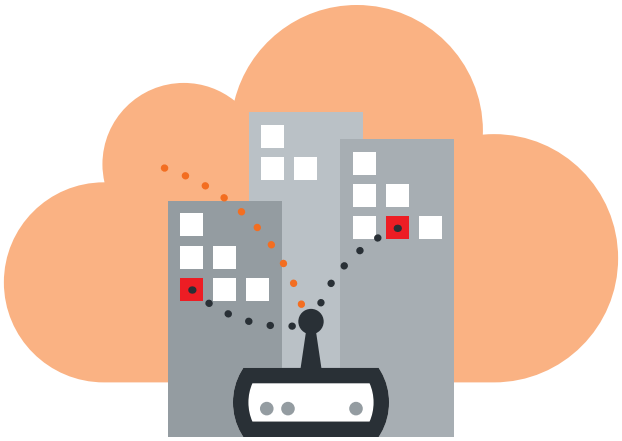
Why IoT Exposes a Fragmented Security Posture in the Enterprise

The IoT does more than expose cybersecurity gaps; it underscores a fragmented and outdated approach to enterprise-wide security.

In the past, security has been a departmentalized endeavor. Operational technology security has been within the purview of facilities management – think identity access management (e.g. building access) and other physical security measures. Infosec, on the other hand, has fallen under the jurisdiction of the IT department. To make matters worse, departments like sales and marketing often run their own cloud-based, micro IT ecosystems without any internal IT security oversight.

IoT is forcing companies to take a holistic view of security across all aspects of their operations, but there are several roadblocks. There are vast differences in how operational and IT security stakeholders identify, manage and fix vulnerabilities. The processes and tools for an admin tasked with assigning/revoking building access cards look very different compared to ones specified for managing network access or data security.

The problem is that IoT is blurring the lines between these areas of the business, and some companies are already paying the price. As mentioned earlier, it was a vulnerability exposed through a HVAC technician's mobile device that took down a retail giant. In another instance, a 4G hotspot planted inside of a data center exposed one company to massive data exfiltration. These are just two examples where the disconnect between physical and IT security have threatened the reputation and financial health of a business.



MouseJack Case Study

MouseJack is a collection of security vulnerabilities affecting non-Bluetooth wireless mice and keyboards. Bastille's research team tested seven vendor's products and discovered that it was possible for an attack to take complete control over a victim's computer using a $15 dongle.

Wireless mice and keyboards commonly communicate using proprietary protocols operating in the 2.4GHz ISM band. These devices work by transmitting radio frequency packets to a USB dongle plugged into a user's computer. When a user presses a key on their keyboard or moves their mouse, information describing the actions are then sent wirelessly to the USB dongle. The dongle listens for these radio frequency packets and transmits the actions to the user's computer.

In order to prevent eavesdropping, most vendors encrypt the data being transmitted by wireless keyboards, however it appears that the same security was not built into the mouse communications. The communication between the dongle and mice tested by the research team showed that there was no authentication in place, leaving the dongle unable to determine the difference between commands originating from the user's mouse and those coming from an attacker. This results in the ability for an attacker to pretend to be a mouse and transmit their own packets to the dongle.

Specifics of the discovered vulnerabilities vary from vendor to vendor, but they generally fall into one of three categories:

1. KEYSTROKE INJECTION, SPOOFING A MOUSE

When processing received RF packets, some dongles do not verify that the type of packet received matches the type of device that transmitted it. Under normal circumstance, a mouse will only transmit movement/clicks to the dongle, and a keyboard will only transmit keypresses. If the dongle does not verify that the packet type and transmitting device type match, it is possible for an attacker to pretend to be a mouse, but transmit a keypress packet. The dongle does not expect packets coming from a mouse to be encrypted, so it accepts the keypress packet, allowing the attacker to type arbitrary commands on the victim's computer.

2. KEYSTROKE INJECTION, SPOOFING A KEYBOARD

Most of the tested keyboards encrypt data before transmitting it wirelessly to the dongle, but not all of the dongles tested required that encryption to receive the data. This makes it possible for an attacker to pretend to be a keyboard, and transmit unencrypted keyboard packets to the dongle.

3. FORCED PAIRING

It is possible to bypass pairing mode on some dongles and pair a new device without any user interaction. In the case where a victim only has a mouse, but is using a dongle vulnerable to keystroke injection by spoofing a keyboard, an attacker can pair a fake keyboard with the dongle, and use it to type arbitrary commands on the victim's computer.

Attacker generates an unencrypted keystroke sequence

Attacker's USB dongle transmits an unencrypted keystroke sequence

Victim's USB dongle receives and types the unencrypted malicious keystrokes

SOLUTION

Bastille Networks Solves the IoT Security Dilemma

Bastille's IoT security solution gives companies full situational awareness and control of all wireless devices within their facility. Its technology tracks the location and activity of all internet-connected and wireless devices on premise. As a result, security executives can prevent the theft of valuable information and protect employees throughout their environment.

How It Works

Bastille deploys a mesh network of proprietary radio frequency (RF) sensors throughout the customer facility. These sensors are able to track the location and emissions of all wireless devices within their environment. Bastille's system sends updates and alerts to end-users to help immediately stop ongoing intrusions and threats.

Bastille provides the situational awareness required to:

- Identify wireless devices or protocols that may pose a risk to the environment
- Prevent intruders from hacking into the facility network
- Prevent unwanted personnel from entering secure areas
- Prevent the unwanted transmission (exfiltration) of information from the facility
- Report on or control access and egress within the facility

C-Suite Radio (RF) Vulnerability Protection: The C-Suite has the most access to valuable information about strategy, financial results, customers, partners, employees and intellectual property. In particular, executive boardrooms, suites, and even homes hold, carry, and publish very sensitive information in both oral and written formats. Whether you are a Fortune 500 corporation or a mid-sized business, keeping the C-Suite protected is a top priority.

Facility/Campus Headquarters Radio (RF) Vulnerability Protection: Many organizations are interested in understanding employee behavior and what types of devices are entering their offices and campuses. Large organizations with sensitive data want to know the movements of devices in their environment in order to get a holistic view of all the activity in the radio frequency spectrum within their combined premises.

Call Center Radio (RF) Vulnerability Protection: Call Centers deal with very sensitive customer data such as personally identifiable information, including social security numbers, bank financial records such as credit card details, and the like. The top priority is keeping that data protected. The attack vector that Call Centers are most vulnerable to are their employees and the devices that they bring along.

Data Center Radio (RF) Vulnerability Protection: The Data Center contains the crown jewels for an organization. In addition to the IT equipment we all think about, Data Centers are loaded with industrial equipment (chillers, lighting, power, etc.) and often frequented by contractors. Many vectors expose a Data Center to risk, and as a result, Data Center security has long been the recipient of significant budget and attention from both physical and cyber security organizations. Data Centers have the highest physical security for any organization, often employing mantraps, biometrics, and expanded video coverage. On the cyber side, large budgets are deployed for endpoint security and intrusion prevention for the wired infrastructure.

TSCM: Technical Surveillance Counter Measures: There are many ways for bad actors to exfiltrate information from an organization. For example, covert transmitters can create voice or data channels that are difficult to detect. These devices commonly use wireless protocols at unmonitored frequencies. For data exfiltration, cellular protocols are the most prevalent example of an "out-of-band" network that can move large amounts of data. Organizations are finding it harder and harder to monitor the entire radio frequency spectrum of protocols and bands for anomalous and/or high volume exfiltration signatures.

SOLUTION

C-Suite Radio (RF) Vulnerability Protection

The C-Suite has the most access to valuable information about strategy, financial results, customers, partners, employees and intellectual property. In particular, executive boardrooms, suites, and even homes hold, carry, and publish very sensitive information in both oral and written formats. Whether you are a Fortune 500 corporation or a mid-sized business, keeping the C-Suite protected is a top priority.

The Problem: Inconsistent Monitoring

Many critical meetings and data pass through the executive suites and boardrooms, which makes this area susceptible to bugs, International Mobile Subscriber Identity (IMSI) catchers, and other nefarious tools used to listen and record. Typical solutions try to solve this problem by point-in-time methods, such as bug sweeps, which prove to be very costly and ineffective. In order to fully protect the C-Suite, the radio frequency spectrum needs constant monitoring to understand the transmissions of devices in the environment.

In the C-Suite, it is imperative to monitor for unauthorized access to secured areas, based on badge level or known and unknown employees. The boardroom is often required to be a no-device-allowed zone, but enforcing this policy can be time consuming, costly, and ineffective.

C-SUITE VULNERABILITIES INCLUDE:

- Unauthorized employee access
- Tailgating and other methods of entry to high risk areas
- Rogue wireless devices and networks being used for data exfiltration and eavesdropping through the RF spectrum

Typical security solutions have very little visibility into the radio frequency space, allowing for no knowledge of the devices in call centers and how they are behaving, making BYOD policy enforcement very difficult.

The Requirements for a C-Suite Radio Security Solution

A C-SUITE RADIO SECURITY SOLUTION NEEDS TO:

1. Provide visibility into the wireless networks, traffic, and devices operating in your environment
2. Inform you of the attach surface for each of these devices
3. Alert on active wireless attacks on those devices through your existing SIEM systems
4. Suggest best practices for minimizing the attack surface and mitigating an attack in action

SPECIFICALLY, A SOLUTION MUST:

- Detect all devices operating in the wireless spectrum between 100 kHz and g GHz, to include WiFi, cellular, Bluetooth, and the hundreds of other protocols in the Internet of Things (IoT)
- Capture the wider RF spectrum; not just specific protocols
- Provide awareness into any wireless threats, including active attacks, rogue networks, and misconfigured devices
- Have the ability to track the movement of devices – which include radios – to augment existing security measures
- Show device movements to help enforce access policies
- Enforce company BYOD/IoT policies
- Detect unauthorized access
- Detect data exfiltration through wireless devices
- Allow the physical security to quickly detect and localize any malicious devices
- Include geofencing capabilities to understand and protect areas with sensitive data
- Detect vulnerable devices being installed
- Detect rogue cell towers which can send signals into your C-Suite

What Kind of Organizations Need This Solution?

- All organizations that have centralized meeting facilities and executive office suites where sensitive matters are housed.

SOLUTION

Facility/Campus Headquarters Radio (RF) Vulnerability Protection

Many organizations are interested to understand employee behavior and what types of devices are entering their offices and campuses. Large organizations with sensitive data want to know the movements of devices in their environment in order to get a holistic view of all the activity in the radio frequency spectrum within their combined premises.

The Problem

Currently organizations do not have an all-inclusive view into the wireless devices and traffic in their corporate office environments. In order to protect from the emerging threats associated with the wireless spectrum, campuses must first recognize the devices and protocols in their airspace.

Understanding employees' patterns and their associated devices gives a view into the insider threat scenario. Rogue devices, data exfiltration, misconfigured equipment, personnel accountability, and insider threats are all possible via nefarious devices. Additionally, this data helps the corporate real estate department understand traffic flows and workplace productivity to help with future real estate planning.

FACILITY/CAMPUS HEADQUARTERS SECURITY VULNERABILITIES INCLUDE:

- Unauthorized devices on premises
- Individuals in unauthorized areas
- The wireless threat surface associated with the devices in the RF spectrum
- Improperly configured devices which can leave an open gateway for attackers to eavesdrop on activities and other nefarious activities

The Requirements for a Facility Radio Security Solution

AN OFFICE FACILITY RADIO SECURITY SOLUTION NEEDS TO:

1. Provide visibility into the wireless networks, traffic, and devices operating in your environment,
2. Inform you of the attack surface for each of these devices,
3. Alert on active wireless attacks on those devices through your existing SIEM systems, and
4. Suggest best practices for minimizing the attack surface and mitigating an attack in action.

SPECIFICALLY, A SOLUTION MUST:

- Detect all devices operating in the wireless spectrum between 100 kHz and 6 GHz, to include WiFi, cellular, Bluetooth, and the hundreds of other protocols in the Internet of Things (IoT)
- Capture the overall wider RF spectrum, not just specific protocols
- Provide awareness into any wireless threats including active attacks, rogue networks, and misconfigured devices
- Have the ability to track the movement of devices, which include radios, to augment existing security measures
- Show device movements to help enforce access policies
- Enforce company BYOD/IoT policy
- Detect unauthorized access
- Detect data exfiltration through wireless devices
- Allow the physical security to quickly detect and localize any malicious devices
- Include geofencing capabilities to understand and protect areas with sensitive data
- Detect vulnerable devices being installed
- Detect rogue cell towers which can send signals into your facility

What Kind of Organizations Need This Solution?

- Fortune 2000, financial services, technology and other companies with large facilities.

SOLUTION

Call Center Radio (RF) Vulnerability Protection

Call Centers deal with very sensitive customer data such as personally identifiable information including social security numbers, bank financial records such as credit card details, and the like. The top priority is keeping that data protected. The attack vector that Call Centers are most vulnerable to are their employees and the devices that they bring along.

The Problem

Call centers handle large volumes of requests by telephone daily. Many of those requests involve the transfer of highly sensitive data and records. Call center protection has become very complex with the influx of wireless devices that can easily capture records for data exfiltration. Centers want their employees to be device free in order to guard against unauthorized activities, but accomplishing this goal is a challenge. One of the unauthorized activities includes bringing devices into an area that is not approved for cell phones or laptops. For example, an employee with a cell phone or other wireless device can take pictures of sensitive data displayed on a monitor and backhaul it out of the center.

CALL CENTER SECURITY VULNERABILITIES INCLUDE:

Rogue wireless devices and networks being used for data exfiltration

- Security teams have little visibility into the Radio Frequency Spectrum; therefore monitoring the influx of devices into call centers is difficult.

Improperly configured devices

- Unencrypted DECT headsets and devices using other protocols leave an open gateway for attackers to eavesdrop on activities

DECT Network Scanning

- The nature of DECT's base-station selection criteria means the FP constantly transmits RFPI information, easily exposing it to network discovery and scanning attacks. In these attacks, attackers are able to identify and eavesdrop on the activity of DECT networks.
- Many DECT devices do not implement the optional encryption capabilities available in the DECT Standard Cipher (DSC) algorithm. Further, it is very difficult for consumers to know if their selected DECT hardware supports encryption, leaving many consumers and businesses vulnerable to audio recording and eavesdropping attacks.
- Typical security solutions have very little visibility into the radio frequency space allowing for no knowledge of the devices in call centers and how they are behaving, making BYOD policy enforcement very difficult.

The Requirements for a Call Center Radio Security Solution

A CALL CENTER RADIO SECURITY SOLUTION NEEDS TO:

1. Provide visibility into the wireless networks and traffic operating in your environment,
2. Inform you of the devices in your environment and their behaviors,
3. Alert on active wireless attacks on those devices through your existing SIEM systems, and
4. Suggest best practices for minimizing the attack surface and mitigating an attack action.

SPECIFICALLY, A SOLUTION MUST:

- Detect all devices operating in the wireless spectrum between 100 kHz and 6 GHz, to include WiFi, cellular, Bluetooth, and the hundreds of other protocols in the Internet of Things (IoT)
- Provide awareness of any wireless threats including active attacks, rogue networks, and misconfigured devices
- Detect ingress and egress: Have the ability to track the movement of devices, both authorized and unauthorized, which include radios, to augment existing security measures
- Show device movements to help enforce access policies
- Detect unauthorized access
- Detect data exfiltration through wireless devices
- Include geofencing capabilities to understand and protect specific areas
- Detect vulnerable devices being installed
- Detect misconfigured devices
- Enforce company BYOD/IoT policy

What Kind of Organizations Need This Solution?

- Call Centers
- Organizations with wireless headsets that handle sensitive/confidential data

SOLUTION

Data Center Radio (RF) Vulnerability Protection

The Data Center contains the crown jewels for an organization. In addition to the IT equipment we think about, Data Centers are loaded with Industrial equipment (chillers, lighting, power, etc.) and often frequented by contractors. Many vectors expose a Data Center to risk, and as a result, Data Center security has long been the recipient of significant budget and attention from both physical and cyber security organizations. Data Centers have the highest physical security for any organization, often employing mantraps, biometrics, and expanded video coverage. On the cyber side, large budgets are deployed for endpoint security and intrusion prevention for the wired infrastructure.

However, there is an attack vector capable of penetrating Data Center walls and bypassing the firewalls, namely radio frequency (RF) based attacks.

The Problem

Data Centers consist of many computers, industrial equipment, and personnel, all having components that may communicate wirelessly. These wireless devices operate on a variety of wireless protocols, which are susceptible to a variety of attacks.

Security professionals need to lock down threat vectors in Data Centers. Rogue devices, data exfiltration, misconfigured equipment, personnel accountability, and insider threats are all possible via nefarious devices.

Company controlled WiFi networks may be protected to some extent by existing products, but other wireless traffic is largely a blind spot. In a Data Center environment, an attacker exfiltrating data over LTE could easily go undetected because no traffic is going over the Data Center's network.

Data Center operators are not always aware of the wireless transceivers in the equipment they control. More equipment today is being shipped with a "radio ready" control system in addition to the Ethernet or Console control system that the Data Center intends to employ. However, we have found that the radio control system, ZigBee or Z-Wave for example, is usually default "ON" when it is shipped. In addition, default passwords (0000) are used that are simple to find from a Google search. As a result, without the knowledge of Data Center personnel who aren't using it, the Radio Ready client is constantly beaconing for a radio controller to pair with it and give it instructions. For instance, a misconfigured ZigBee interface on a chiller could enable an attacker to interrupt Data Center operations. Knowledge of all wireless transmitters in a Data Center makes it possible to minimize the wireless attack surface.

DATA CENTER SECURITY VULNERABILITIES INCLUDE:

Rogue wireless devices and networks being used for data exfiltration

- Typical exfiltration prevention techniques involve monitoring corporate networks and preventing the use of USB ports for storage. However, by utilizing cellular or other "hard to see" protocols, attackers can bypass these controls.
- Nefarious devices such as pwn plugs and pineapples that are left in Data Centers to specifically steal data and backhaul that data out over cellular.

Improperly configured devices

- Network infrastructure, e.g. a laptop connected to the network, has an open Bluetooth stack beaconing for a keyboard.
- Data Center equipment can employ proprietary or industry ICS protocols for managing aspects of the equipment or environment. Security professionals have no visibility into these devices and protocols and whether they are properly configured.
- Employees and contractors who unknowingly carry a compromised cell phone, which once attached to an internal WiFi network, open a 4G channel and begin beaconing out packets to the attackers abroad.

Typical security solutions have no visibility into what devices exist and operate within the radio frequency spectrum, let alone if they are doing something nefarious.

SOLUTION

TSCM: Technical Surveillance Counter Measures

There are many ways for bad actors to exfiltrate information from an organization. For example, covert transmitters can create voice or data channels that are difficult to detect. These devices commonly use wireless protocols at unmonitored frequencies. For data exfiltration, cellular protocols are the most prevalent example of an "out-of-band" network that can move large amounts of data. Organizations are finding it harder and harder to monitor the entire radio frequency spectrum of protocols and bands for anomalous and/or high volume exfiltration signatures.

The Problem

Surveillance devices are becoming cheaper and easier to access. There are countless numbers of inexpensive bugs, pwn plugs, and listening devices that can be purchased over the counter and over the Internet. They can be installed, have their own computers, and have their own cellular backhaul prepaid chips. These devices are not going over the wire, through normal security teams' monitoring systems. Instead, the devices backhaul the data through unmonitored protocols.

Typically, when an organization needs to conduct a bug-sweep, they hire an outside firm to do a one-time, point-in-time sweep that is rendered obsolete once the firm leaves. This is not only costly and time consuming, but also very disruptive. Unfortunately, most corporations only use bug-sweeps once per quarter, or in close proximity to a 'sensitive moment or event', leaving themselves susceptible to attack.

SURVEILLANCE VULNERABILITIES INCLUDE:

Rogue Wireless Devices and Networks being used for Data Exfiltration

- Typical exfiltration prevention techniques involve monitoring corporate networks and preventing the use of USB ports for storage. However, by utilizing cellular or other "hard to see" protocols, attackers can bypass these controls
- Nefarious devices such as pwn plugs and pineapples that are left to specifically steal data and backhaul that data out over cellular

Unauthorized video systems planted in an organization

The Requirements for a Technical Surveillance Counter Measure Solution

A TSCM SECURITY SOLUTION NEEDS TO:

1. Provide visibility into the wireless networks, traffic, and devices operating in your environment,
2. Inform you of the attack surface for each of these devices,
3. Alert on active wireless attacks on those devices through your existing SIEM systems, and
4. Suggest best practices for minimizing the attack surface and mitigating an attack in action.
5. Operate 24x7 to catch out-of-hours transmission of data

SPECIFICALLY, A SOLUTION MUST:

- Detect all devices operating in the wireless spectrum between 100 kHz and 6 GHz, to include WiFi, cellular, Bluetooth, and the hundreds of other protocols in the Internet of Things (IoT)
- Detect current and future protocols without requiring hardware upgrades
- Detect known and unknown emitters via observing energy patterns
- Provide awareness of any wireless threats including active attacks and rogue networks
- Detect data exfiltration via wireless devices
- Be always on
- Detect unauthorized devices
- Detect vulnerable devices being installed
- Detect anomalous wireless activity originating from the campus
- Alert on a wireless attack surface introduced by the installation of new equipment
- Detect rogue cell towers which can send signals into your facility

What Kind of Organizations Need This Solution?

- Fortune 2000, financial services, technology, and other companies with sensitive data or high risk areas

The Requirements for a Data Center Radio Security Solution

A DATA CENTER RADIO SECURITY SOLUTION NEEDS TO:

1. Provide visibility into the wireless networks, traffic, and devices operating in your environment,
2. Inform you of the attack surface for each of these devices,
3. Alert on active wireless attacks on those devices through your existing SIEM systems, and
4. Suggest best practices for minimizing the attack surface and mitigating an attack in action.

SPECIFICALLY, A SOLUTION MUST:

- Detect all devices operating in the wireless spectrum between 100 kHz and 6 GHz, to include WiFi, cellular, Bluetooth, and the hundreds of other protocols in the Internet of Things (IoT)
- Capture wider spectrum not just specific protocols
- Provide awareness of any wireless threats including active attacks, rogue networks, and misconfigured devices.
- Have the ability to track the movement of devices, which include radios, to augment existing security measures.
- Show the movements of devices to help enforce access policies.
- Detect unauthorized access
- Detect data exfiltration via wireless devices (large volume of wireless data leaving the Data Center premises over the cellular network)
- Allow the Data Center operator to quickly detect and localize any malicious LTE or 3G modems
- Include geofencing capabilities to understand and protect the location(s) of a customer's servers within a colocation facility
- Be always on
- Detect unauthorized devices entering the Data Center
- Detect vulnerable devices being installed
- Detect anomalous wireless activity originating from the Data Center (independently from the protocol)
- Detect misconfigured devices
- Enforce company BYOD/IoT policy
- Alert on a wireless attack surface introduced by the installation of new equipment in the Data Center, e.g. an HVAC system with ZigBee or a MouseJack vulnerable keyboard
- Detect rogue cell towers which can send signals into your facility

What Kind of Organizations Need This Solution?

- Fortune 2000, financial services, technology, and other companies that manage their own Data Centers
- Data Center companies (hosting providers, etc.)
- Cloud infrastructure providers

Securing Enterprise Assets from IoT Risks

It's not difficult to make a business case for IoT security. Most enterprises are critically vulnerable without the millions of new mobile devices and sensors coming online each day. When we factor in the exponential impact of IoT, the attack surface becomes shockingly porous. Consider this:

- Among organizations with over 5,000 computers, more than 90 percent have an active breach at any given time.[3]
- Approximately 90 percent of all IT networks will have an IoT-based security breach within the next two years.[4]
- More than half of IoT device manufacturers are unable to address product threats stemming from weak security practices.[5]

To solve these challenges, CISOs must have an active role in shaping and executing business strategy. Security is no longer an IT or operational conversation; its one to be had with all C-level stakeholders. CISOs need to develop and champion holistic, enterprise-wide security strategies that monitor, manage and neutralize IoT-related threats at every juncture across the organization.

Visibility into these threats is crucial. Enterprises need tools that will help them identify airborne threats and allow for preemptive response. Which devices are accessing corporate air space? Where? What protocols are they using? Are they permitted? Who do they belong to? This scale of ambient detection enables security teams to see IoT risks in real time and mitigate them before an attack transpires.

Enterprises that aren't already tackling the IoT security threat should be warned. IoT has opened the door to countless vulnerabilities across all facets of the business. The IoT security threat is here and evolving at a pace that is unprecedented. Staying ahead of it is crucial to the health of the business.

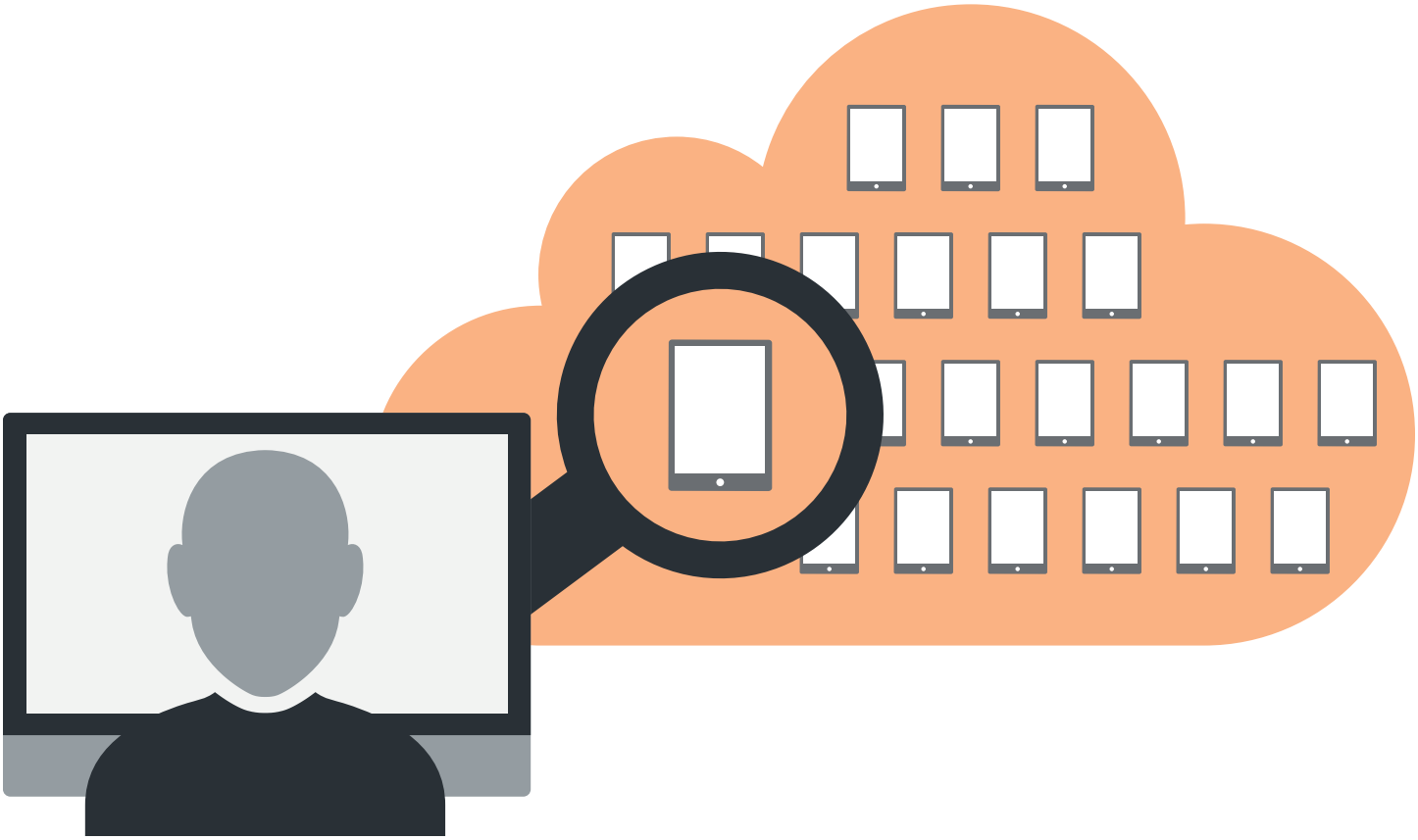
[1] Source: Gartner, Inc., Predicts 2016: Security for the Internet of Things, December 2015

[2] Source: Garner, Inc., Press Release "Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015," November 2015

[3] Source: TechCrunch.com, "Why Breach Detection Is Your New Must-Have, Cyber Security Tool," November 2014

[4] Source: IDC, Press Release "IDC Reveals Worldwide Internet of Things Predictions for 2015," December 2014

[5] Source: Gartner, Inc., Predicts 2016: Security for the Internet of Things, December 2015



About Bastille

Launched in 2014, Bastille is the leader in enterprise threat detection through software-defined radio. Bastille provides full visibility into the known and unknown mobile, wireless and Internet of Things devices inside an enterprise's corporate airspace–together known as the Internet of Radios. Through its patented software-defined radio and machine learning technology, Bastille senses, identifies and localizes threats, providing security teams the ability to accurately quantify risk and mitigate airborne threats that could pose a danger to network infrastructure. For more information, visit www.bastille.net and follow on Twitter @bastillenet.

COMPANY RECOGNITION

TEAM AWARDS

- Darpa Spectrum Challenge
- Darpa Shredder Challenge
- GNU Radio Hacking Challenge

Bastille

497 LAKE AVE, SANTA CRUZ, CA 95062
INFO@BASTILLE.NET / 800.530.3341