Harmony IoT
Airspace & Compliance Report

01/10/2022 - 20/10/2022

Prepared by Orchestra Group for:

Confidentiality Notice

Table of Contents

1. Introduction

This airspace security report is based on monitoring data gathered by Harmony IoT, the airspace security solution from Orchestra Group. Harmony IoT is a passive monitoring solution that provides visibility into all devices, known and unknown, operating in the wireless airspace. Harmony IoT identifies traffic anomalies, unauthorized devices operating in the airspace and suspicious activity. It also assesses the state of wireless security controls and conformance to compliance standards.

For each event you will find:

- A full description of the event along with a precise timeline and relevant detailed information about the participating devices.
- Potential threats caused by the event and their implications for the company.
- Suggested responses to the event according to best practices and the Harmony IoT cyber defense playbook.
- The event status (resolved, mitigated, ongoing, etc.).
- Heatmaps with the device numbers (when relevant).

For more information regarding the events please contact Orchestra Group directly.

Please note: No private or personal information is extracted regarding the corporate employees. The "Corporate Device" attribute is based solely on the system's machine learning algorithms.

[SS019] [NIST 800-153] [2018-ITA-020]

2. Executive Summary

Airspace security in commercial settings poses unique challenges. Unlike traditional wired networks, the wireless airspace offers no native visibility or control over devices operating in the airspace. This exposes organizations and their employees to a wide range of well-known attacks that can lead to serious data breaches, ransomware and denial of service. Without effective security controls, Wi-Fi connected laptops, smartphones, tablets, printers, conference room speakers, smart TVs and a host of IoT devices offer entry points that attackers can and have exploited.

This report provides the details of what was found during the monitoring period and offers analysis and recommendations. The report includes the security exposures and compliance violations that were found, and based on those findings, a set of recommendations for reducing airspace security risks.

Key findings in this report include the following:

- 5 compliance violations ('SS019', 'NIST 800-53').
- 2 possible 'Evil Twin' attacks. An attack technique typically used to mimic your corporate network, performing user credential theft or planting malware on your corporate devices.
- Possible 91 'similar SSIDs' were detected. This is an attack technique typically used for user credential theft or planting malware on your corporate devices.
- Possible 77 suspicious devices were detected. This can be used for user credential theft or planting malware on your corporate devices.
- 6 new corporate networks were detected and require your approval.
- 17 new corporate APs were detected and require your approval.
- 6 WPS APs were detected. They are vulnerable to the brute-force password breaking “Pixie Dust” attack.
- 14 Rogue Devices were detected. They can be planted on-premises by attackers to covertly collect data (Cameras, Microphones, and more).
- 11 Rogue APs were detected. They can be planted on-premises by attackers to lure unsuspecting users, leading to credential theft and planting malware.

The report also provides 2 recommendation(s) for addressing the issues found during the monitoring period.

The report is based on monitoring data collected from the Orchestra airspace.

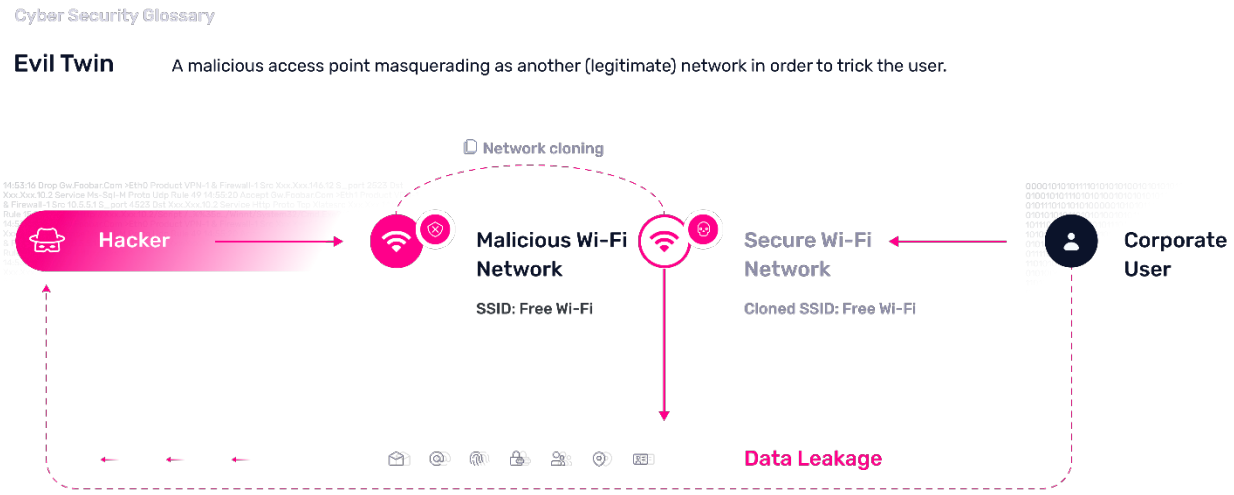
Establishing effective security controls over corporate wireless networks is not a one-time event. The use of wireless devices and IoT is constantly expanding. Continuous monitoring, policy enforcement and the ability to prevent attacks in real time are all necessary elements for safely gaining the many benefits of wireless.

3. Attacks & Incidents

This section discusses the attacks and incidents found in your airspace.

3.1 Attacks

3.1.1 Evil Twin



A malicious access point masquerading as another (legitimate) network. It copies another network's SSID to look exactly like another, already existing network.

Findings

Detected 2 issues of this type.

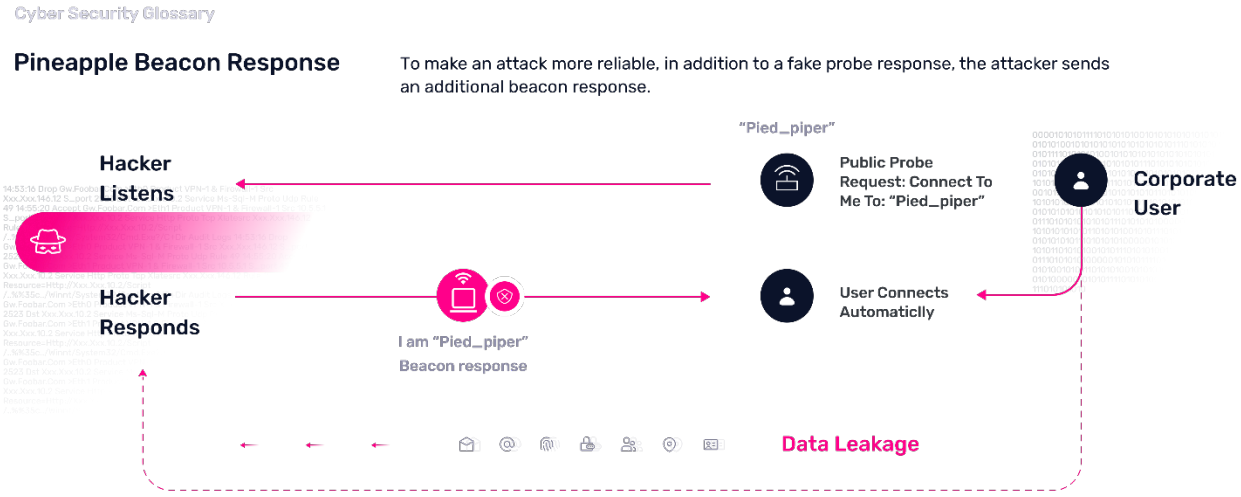
Risk

- Sensitive data theft from devices through network sniffing.
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high priority assets.
- Malware infection of devices through network exploits for complete remote control over the device.

Recommendation

- Block all devices from connecting to Evil Twin networks.

3.1.2 Pineapple Beacon Response



An attack where fake, targeted beacon frames are sent in response to a probe request, mostly to accompany a Karma attack with or without a Dogma attack, to give the fake access point more legitimacy (real networks send both beacons and probe responses).

We did not detect any issues of this type in your airspace.

Risk

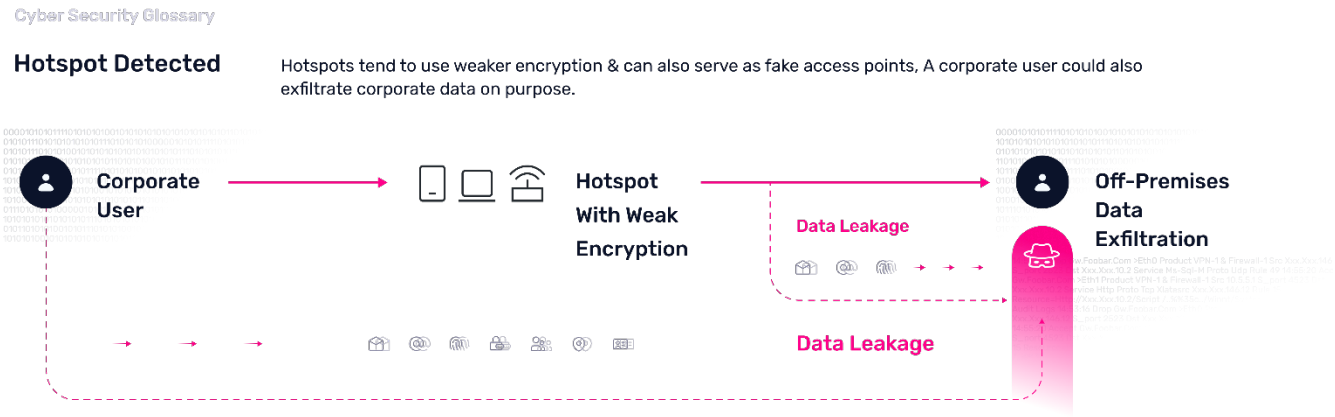
- Sensitive data theft from devices through network sniffing.
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high priority assets.
- Malware infection of devices through network exploits for complete remote control over the device.

Recommendation

- Prevent connections of on-premises devices to devices that use those probe requests.

3.2 Incidents

3.2.1 Corporate Device Connected To A Hotspot Network



Harmony IoT has detected the following corporate devices connected to an external secure/insecure network. This poses a risk to the corporate devices as these hotspots are not monitored by the organizations' cyber defenses and the external devices connected to these networks are able to compromise them.

Findings

Detected 52 issues of this type.

Risk

- Sensitive data theft from devices through network sniffing.
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high priority assets.
- Malware infection of devices through network exploits for complete remote control over the device.

Recommendation

- Block corporate devices from connecting to corporate hotspots or an external network.

3.2.2 Watchlist Device Appeared

Cyber Security Glossary

Watchlist Device Appeared

The following device(s) is (are) on the customer's watchlist.

We did not detect any issues of this type in your airspace.

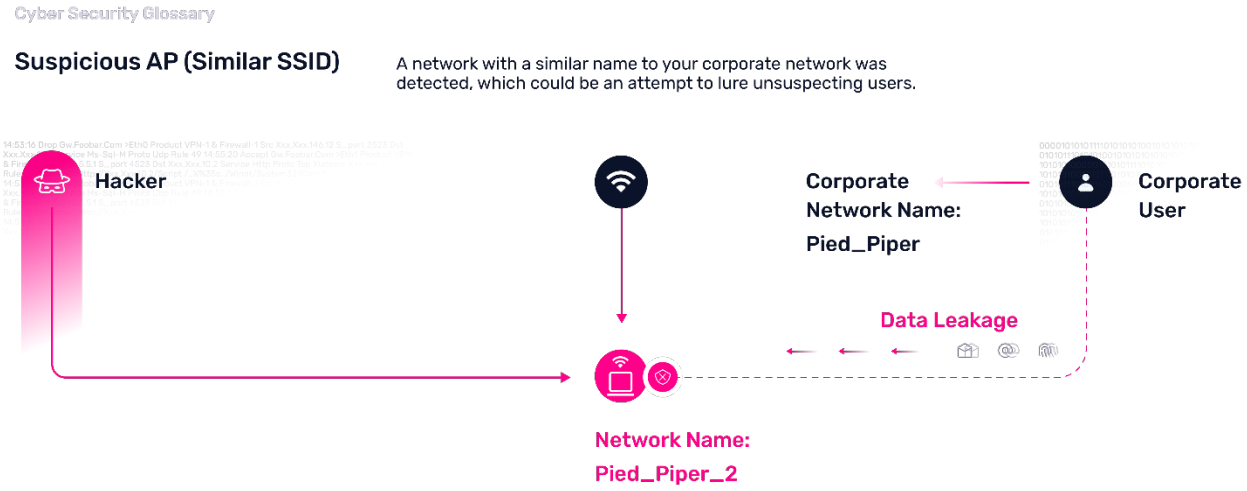
Risk

- Sensitive data theft.
- Unauthorized access or activity.

Recommendation

- Alert and mitigate unwanted devices.

3.2.3 Suspicious AP Detected (Similar SSID)



Similar SSIDs were detected being broadcasted. The presence of an access point with a similar SSID to yours could indicate an attempt to fool unsuspecting users into connecting to a malicious access point instead of the original one. Once connected, users are susceptible to data leakage of sensitive information such as their banking credentials and even malware injection through man-in-the-middle attacks.

Findings

Detected 91 issues of this type.

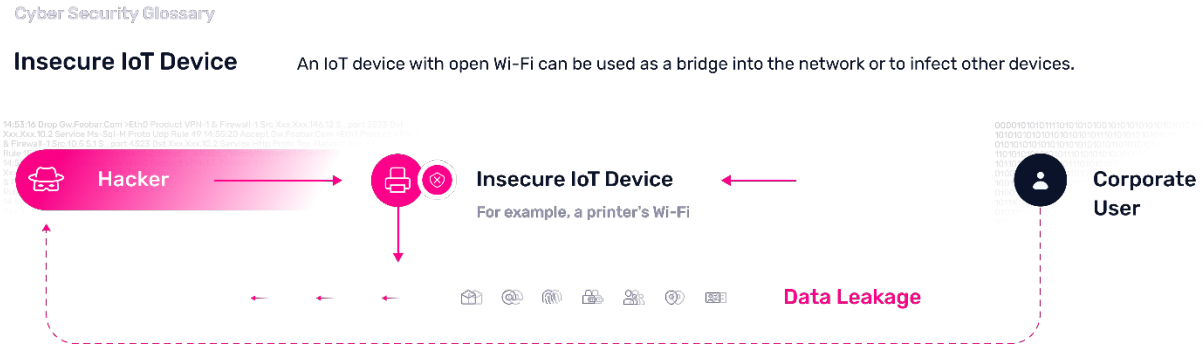
Risk

- Sensitive data theft from devices through network sniffing.
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high priority assets.
- Malware infection of devices through network exploits for complete remote control over the device.

Recommendation

- Approve or block similar SSID networks.

3.2.4 Insecure IoT Device



An IoT device on-premises that hosts an insecure network.

We did not detect any issues of this type in your airspace.

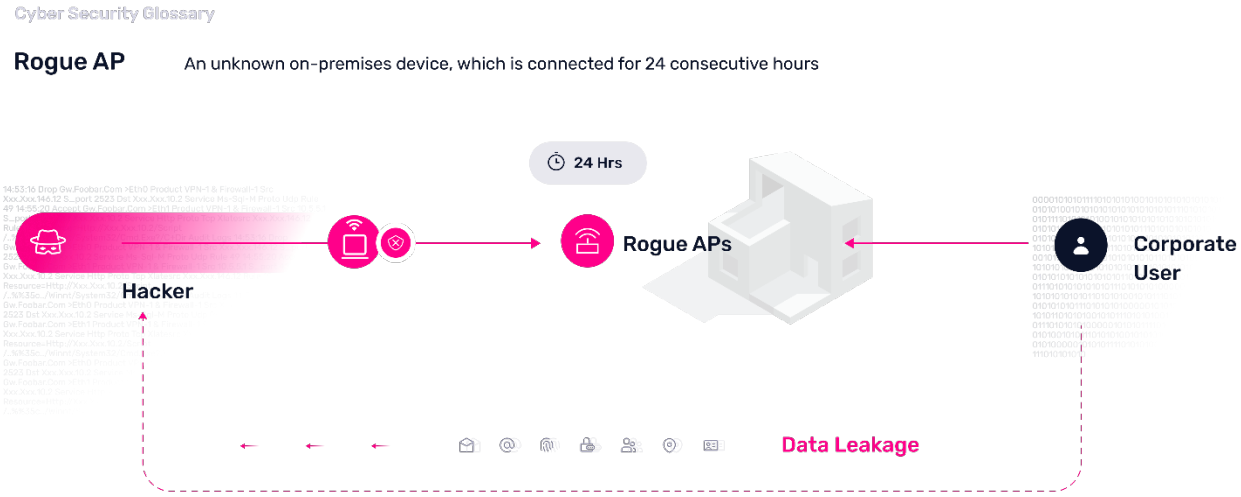
Risk

- IoT devices are highly vulnerable and could be exploited to infect anyone who interacts with them.
- Some IoT devices like smart printers and smart TVs are physically connected to the corporate network (via a cable) but also host a wireless network, thus acting as a bridge between the two networks.
- These devices can be used to exfiltrate sensitive data from devices by activating sensors (camera, microphone, screen recording, keyboard sniffing, etc.).

Recommendation

- IT should locate and handle the IoT device to disable/secure its network.
- Create rules that will limit those risks.

3.2.5 Rogue AP



An unknown on-premises access point, which was published for 24 consecutive hours, was detected.

Findings

Detected 11 issues of this type.

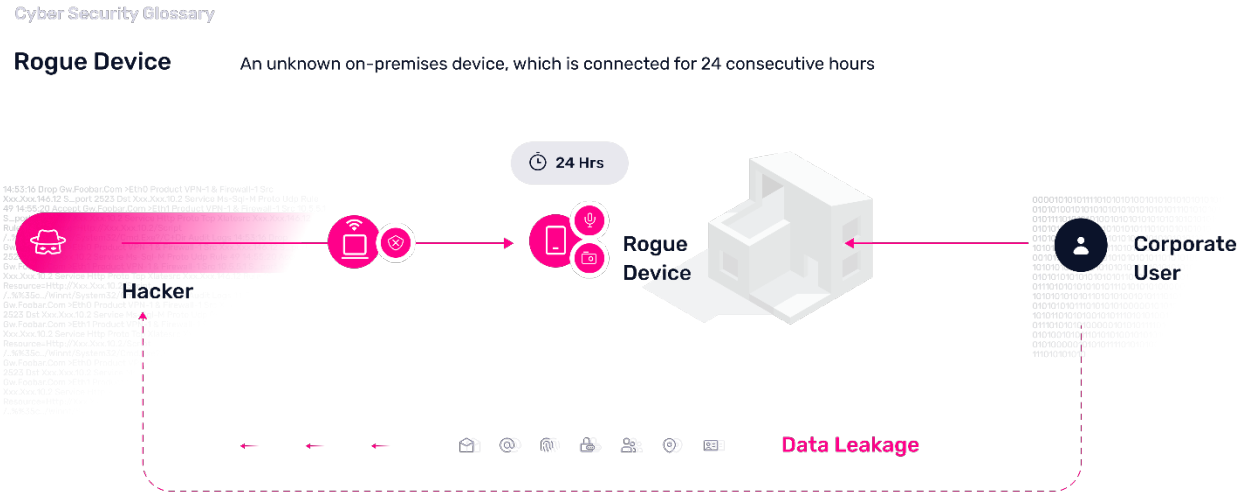
Risk

- A rogue AP can be used by an attacker as a remote antenna for constantly monitoring and potentially attacking your air-space

Recommendation

- Locate the AP and investigate it.
- Create a mitigation rule for this AP.

3.2.6 Rogue Device



An unknown on-premises device, which was published for 24 consecutive hours, was detected.

Findings

Detected 14 issues of this type.

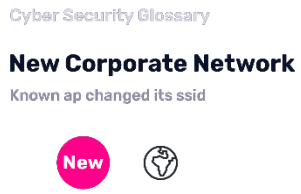
Risk

- This device could be used for filming or recording your activity.
- A rogue device can be used by an attacker as a remote antenna for constantly monitoring and potentially attacking your air-space.

Recommendation

- Locate the device and investigate it.
- Create a mitigation rule for this device.

3.2.7 New Corporate Network (Known Corporate AP Changed its SSID)



Findings

Detected 6 issues of this type.

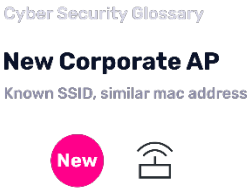
Risk

- If it is not a legitimate AP, it could be a potential Evil Twin attack that could lead to data leakage.

Recommendation

- If it is a known corporate network, authorize it via the user interface. If it is unknown, then block it using a mitigation rule.

3.2.8 New Corporate AP (Known Corporate SSID, new MAC)



This AP is similar to your corporate network. If you know it is legitimate, please approve it via the user interface. If you are not familiar with it, this could be an *Evil Twin* attack, attempting to lure unsuspecting users to connect to it. In this case we recommend creating a mitigation rule to prevent users from connecting to it.

Findings

Detected 17 issues of this type.

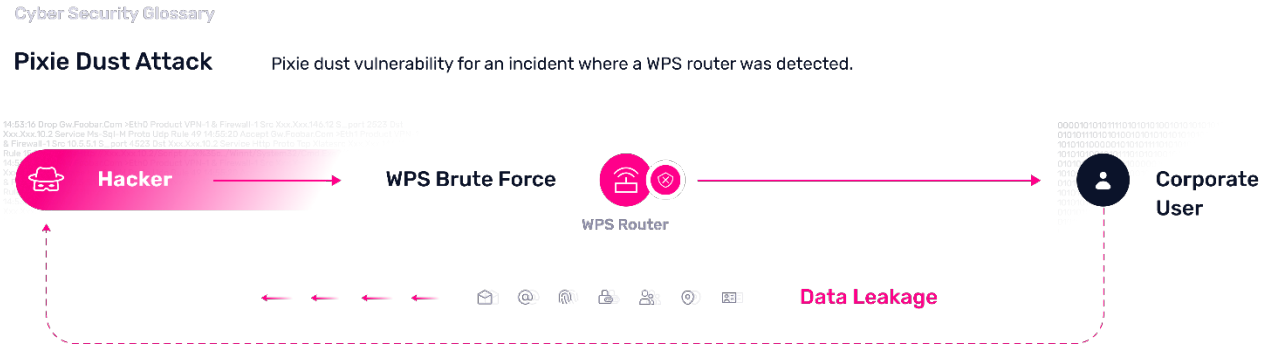
Risk

- If it is not a legitimate AP, it could be a potential Evil Twin attack that could lead to data leakage.

Recommendation

- If it is a known corporate network, authorize it via the user interface. If it is unknown, then block it using a mitigation rule.

3.2.9 Corporate AP WPS Enabled (Pixie Dust Vulnerability)



If a Wi-Fi network is properly configured with a strong encryption scheme and a strong password (for example, WPA2 and a 20 characters mixed alpha-numeric password), but has WPS enabled in its settings, attackers can brute force the WPS pin code (which is just 8 digits) instead of the actual password and gain access that way. It is significantly easier to crack an 8-digit password than a 20-character alpha-numeric password.

Findings

Detected 6 issues of this type.

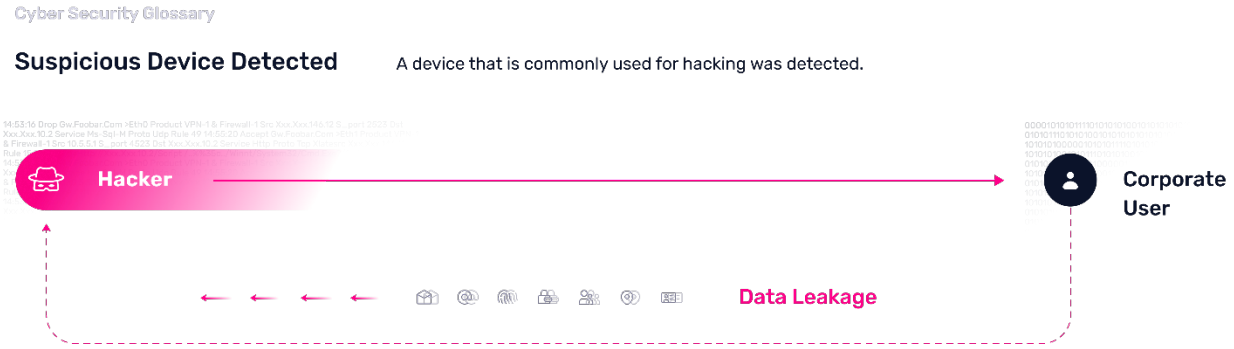
Risk

- Sensitive data theft from devices through network sniffing.
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high priority assets.
- Malware infection of devices through network exploits for complete remote control over the device.

Recommendation

- Disable WPS.

3.2.10 Suspicious Device Detected



A suspicious device is a device we want to pay special attention to, especially as it comes near your premises. These include external Wi-Fi antennas, known “Dropboxes”, wireless attack tools, cameras, etc.

Findings

Detected 77 issues of this type.

Risk

- Sensitive data theft from devices through network sniffing.
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high priority assets.
- Malware infection of devices through network exploits for complete remote control over the device.

Recommendation

- Approve, locate & investigate, or block the device.

3.2.11 Known Networks (Common public commercial networks)

Devices can automatically connect to networks they have connected to in the past. Attackers can easily mimic those networks (for example, “Starbucks”) and lure corporate employees.

We did not detect any issues of this type in your airspace.

Risk

- Sensitive data theft from devices through network sniffing.
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high-priority assets.
- Malware infection of devices through network exploits for complete remote control over the device.

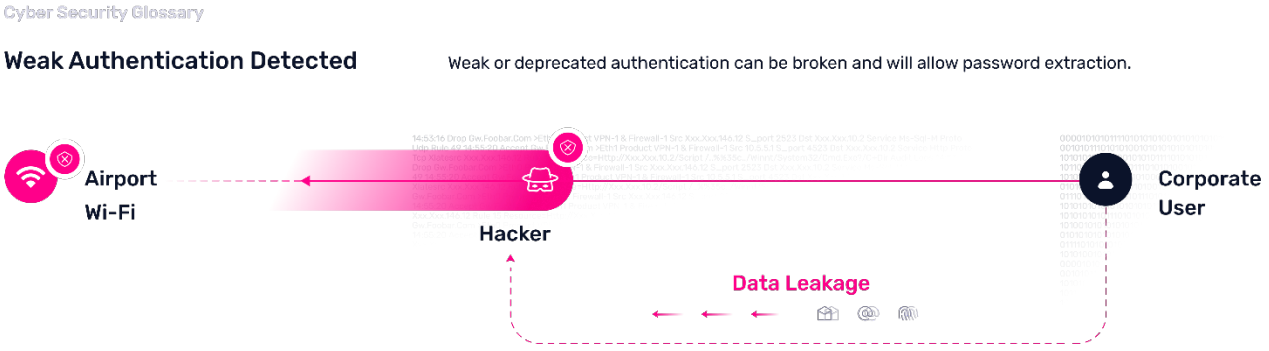
Recommendation

- Prevent connections of on-premises devices to known networks.

4. Network Hygiene

4.1 Insecure Communication

4.1.1 Insecure Authentication



Require and enforce the use of mutual certificate authentication (client and server) for all Enterprise Services Network (ESN) connected networks, specifically prohibiting pre-shared key authentication for ESN connected networks. If PSKs are used to establish network associations, no key MUST be shared across multiple endpoint devices.

Findings

There are 0 corporate and affiliated corporate networks with WPA2-PSK authentication.

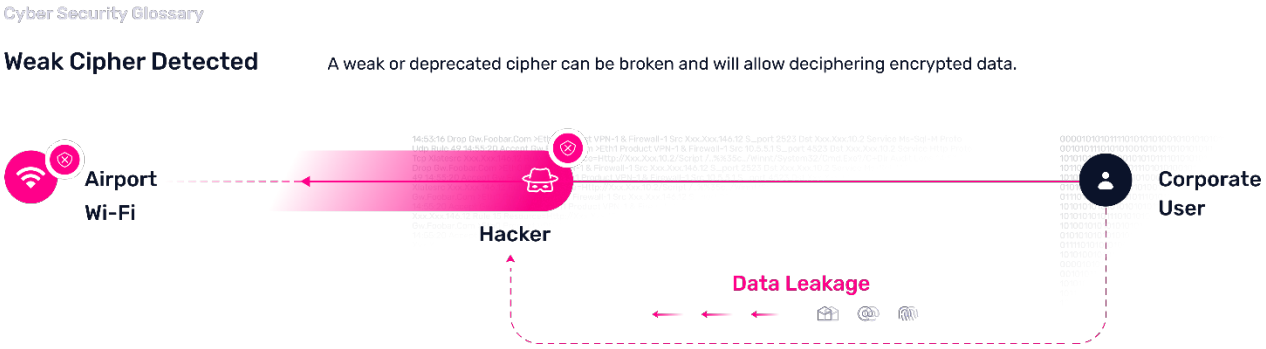
Risk

- Dictionary attacks and over-the-air attacks can be performed and are made only slightly harder with multiple unique credentials in use. If a malicious intruder obtains the PSK and captures the key handshake when a device joins the network, that individual can decrypt all of that device's traffic.

Recommendation

- Change the encryption key from PSK to MGT or Enterprise.

4.1.2 Insecure Ciphers (TKIP cipher)



TKIP ciphers were rendered obsolete and insecure.

Findings

The use of TKIP cipher is not recommended[2].

There are 0 corporate and affiliated corporate networks using deprecated TKIP ciphers.

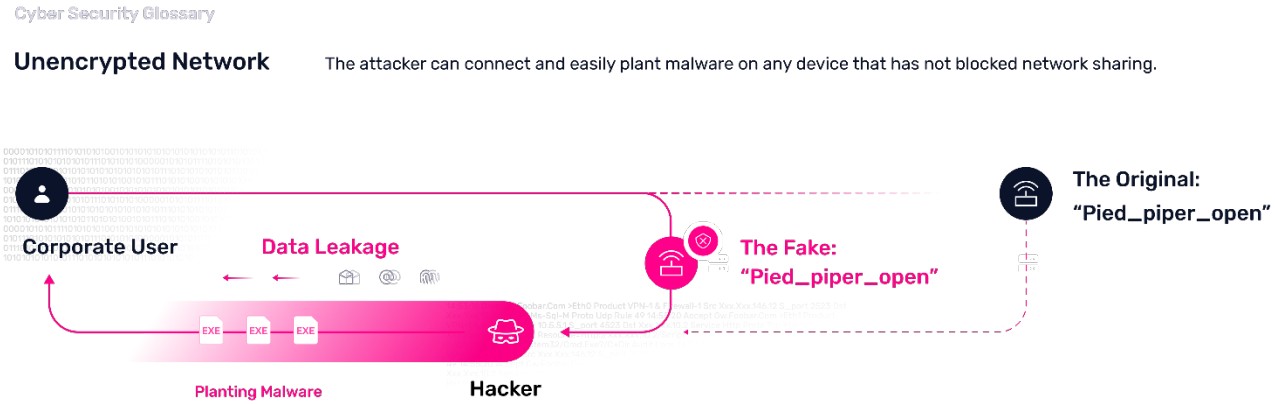
Risk

- Temporal Key Integrity Protocol is a deprecated cipher and is considered less secure.
- Data leakage.
- Malware proliferation.

Recommendation

- Change the cipher to AES-CCMP.

4.1.3 Insecure Encryption



An important principle of WLAN security is to separate WLANs with different security profiles.

We did not detect any issues of this type in your airspace.

Risk

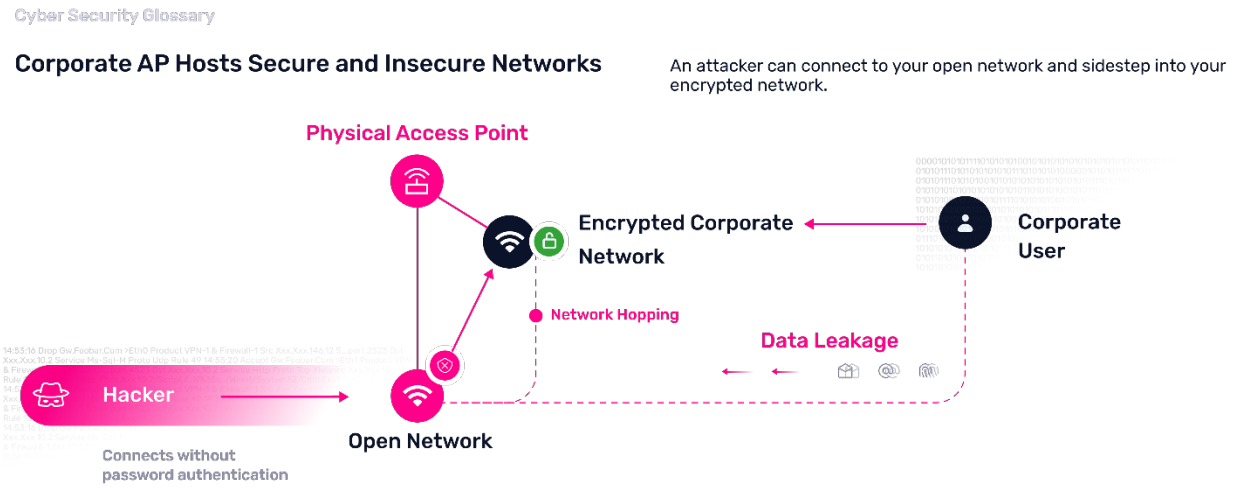
- Sensitive data theft from APs and devices through network sniffing.
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high priority assets.
- Malware infection of devices through network exploits for complete remote control over the device.

Recommendation

- Consider separating the network infrastructure to prevent data leakage.
- Isolate the infrastructure of secured networks from insecure networks.

4.2 Insecure WLAN Usage Patterns

4.2.1 Corporate AP Hosts Secure and Insecure Networks



The following corporate APs were hosting an insecure network and a secure network simultaneously. Even if the secured network is properly configured, attackers could connect through the insecure network, get on the access point exploiting a vulnerability and gain access to the secured network running on the same device.

We did not detect any issues of this type in your airspace.

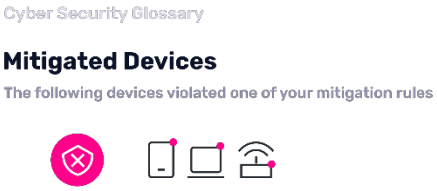
Risk

- Sensitive data theft from devices through network sniffing.
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high priority assets.
- Malware infection of devices through network exploits for complete remote control over the device.

Recommendation

- Approve or block the open network.

4.3 Mitigated Devices



4.3.1 Mitigated Access Points

The following APs had unauthorized connections that were blocked by Harmony IoTs Protectors based on a policy or rule violation. Using our proprietary mitigation method we can completely prevent devices from connecting to your networks

Findings

Based on your active rules the system mitigated the following 12 access points

Risk

- This is an indication that there was a risk and that it was mitigated by the Protectors

Recommendation

- Periodically review your rules and the affected connections to try and understand if you wanted those connections mitigated

4.3.2 Mitigated Stations

The following stations participated in unauthorized connections that were blocked by Harmony IoTs Protectors based on a policy or rule violation. Using our proprietary mitigation method we can completely prevent devices from connecting to your networks

Findings

Based on your active rules the system mitigated the following 37 clients

Risk

- This is an indication that there was a risk and that it was mitigated by the Protectors

Recommendation

- Periodically review your rules and the affected stations to try and understand if you wanted those connections mitigated

4.3.3 Mitigated Policy Rules

The following rules triggered Harmony IoTs Protectors to completely block connections between stations and APs

Findings

Mitigation was performed for 4 of your active rules

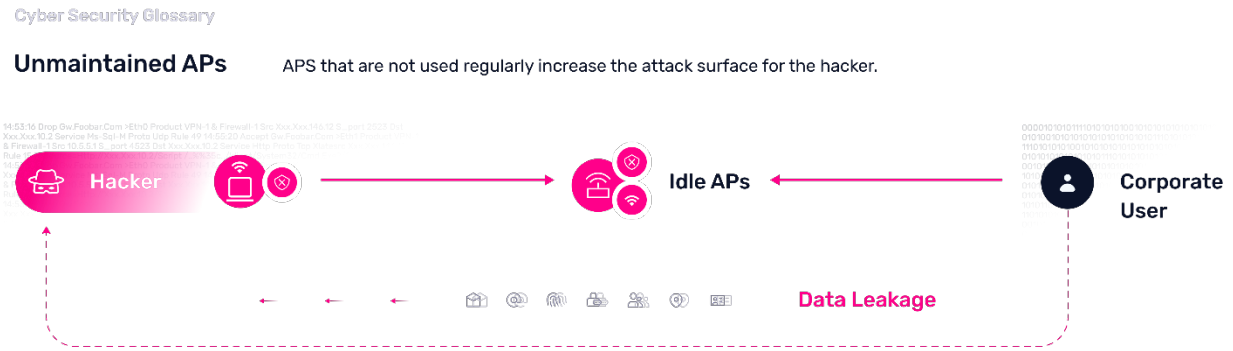
Risk

- This is an indication that there was a risk and that it was mitigated by the Protectors

Recommendation

- Periodically review your rules and the affected connections to try and understand if you wanted them mitigated

4.4 Idle APs



Unneeded network connections, network services and ports on managed endpoints, access points and authentication servers MUST be disabled to reduce your attack surface. For example, if a device is already connected to a wired network access point, WLAN access is usually redundant and should be disabled.

We did not detect any issues of this type in your airspace.

Risk

- Idle APs are unnecessary attack surfaces that invite an attack and demand more management.
- Inactivity might indicate an issue that could lead to a breach or be a sign of deprecated software or configuration.
- Their inactivity might indicate that other APs are experiencing overload and that could allow for easier obfuscation of an attack on the other APs.

Recommendation

- Repair, investigate or disable these APs.

5. Compliance Overview

Source	Possible Violation	Violation
SS019 10.7.4	There MUST be both attack monitoring and vulnerability monitoring to support WLAN security. The monitoring solutions for the wireless network should provide most, if not all, of the following detection capabilities: ATTACKS • Unauthorized WLAN devices, **including rogue APs and unauthorized client devices.** • Unusual WLAN usage patterns, such as extremely high numbers of client devices using a particular AP, abnormally high volumes of WLAN traffic involving a particular client device, or many failed attempts to join the WLAN in a brief period. • DoS attacks and conditions (e.g., network interference). Many denial-of-service attacks are detected by counting events during periods of time and alerting when the threshold values are exceeded. For example,many events involving the termination of WLAN sessions can indicate a DoS attack. • Impersonation and man-in-the-middle attacks. • Any radio frequency jamming signal emanating from an attacker or from an accidental source. VULNERABILITIES WLAN devices that are misconfigured or using weak WLAN protocols and protocol implementations.	Found
SS019 10.2.11 / 2018-ITA-020	**Insecure Authentication** - Require and enforce the use of mutual certificate authentication (client and server) for all ESN connected networks, specifically prohibiting pre-shared key authentication for ESN connected networks. If *PSKs are used to establish network associations, no key MUST be shared across multiple endpoint devices*.	Not Found
SS019 10.3.1	**Insecure Cipher (WEP and TKIP)** must be disabled in the configuration of all the AP or WLAN devices that are misconfigured or using weak WLAN protocols and protocol implementations.	Not Found
NIST 800-153 / SS019 10.7.4	**Unusual WLAN usage patterns**, such as extremely high numbers of client devices using a particular AP, abnormally high volumes of WLAN traffic involving a particular client device, or many failed attempts to join the WLAN in a short period of time.	Found
SS019 10.2.6	**Idle Corporate Networks** - Unneeded network connections, network services and ports on managed endpoints, access points and authentication servers MUST be disabled to reduce attack surface. For example, if a device is already connected to a wired network access, WLAN access is usually redundant and should be disallowed.	Not Found

6. Recommendations

Recommended action items:

Suspicious Device Detected

Keeping continuous tracking of suspicious devices. Keep the firmware of the company's devices updated. Activate mitigation of suspicious devices.
Why? Our DB is updated regularly to detect known suspicious (hacking tools) and exploitable devices. Our mitigation capability allows blocking those risky connections. Regularly update your firmware and software to keep your devices protected from the most recent hacks and vulnerabilities.

Hotspot Connection Detected

Block corporate devices from connecting to corporate hotspots or an external network.
Why? Using a device as a hotspot usually means using a less secure connection out of the scope of your cybersecurity tools, whilst inviting unknown users to connect to it (especially if it is not password protected). External networks pose the same threats.

7. Data Summary

Total Events	287
Total Attacks	2
Devices Seen (New / Total)	7027 / 10747
Networks Seen (Total)	1979
Devices Mitigated (Total)	37
Devices Mitigated (Corporate)	34
Devices Mitigated (Non-Corporate)	3
Networks Mitigated (Total)	10
Networks Mitigated (Corporate)	0
Networks Mitigated (Non-Corporate)	10