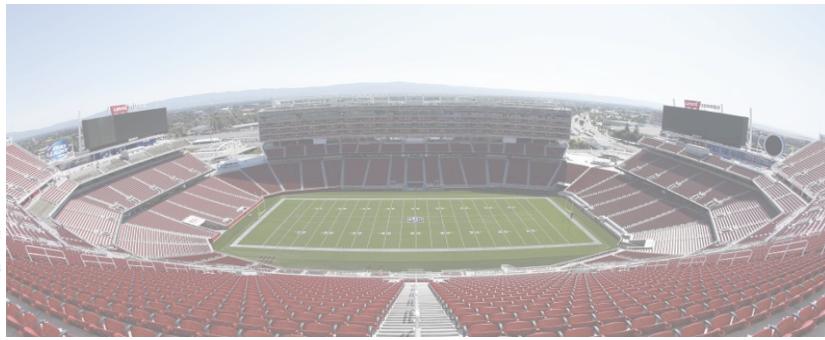# Pwnie Express Partners with Norwich University to Identify & Neutralize Cyber Threats at Super Bowl 50

> *"With five critical networks to monitor, it was crucial that we had a platform which could quickly show us what threats needed our immediate attention. Through Pulse, we were able to see the full gamut of threats to the operational networks at Super Bowl 50 and focus our response activity accordingly."*
>
> – Phil Susmann, Vice President Strategic Partnerships Norwich University

Highlights

- Pwnie Express Sensors were deployed in Levi's Stadium

- On 7 Feb 16, Pwnie Express stood up a remote SOC to monitor all networks and devices during Super Bowl 50

Findings

- Over 1,200 APs

- Over 55,000 Wireless Clients

- Over 35,000 Bluetooth Devices

- Live-streaming cameras

- Attempted de-authorization of high-priority network

Assessing the Environment

Levi's Stadium is home to the San Francisco 49ers and is world renowned as one of the most "high-tech" event spaces in the world, boasting over 1,200 Wireless Access Points, specifically designed to provide consistent, secure connectivity to each of its 77,000+ guests on demand. This year, Levi's Stadium served as host to Super Bowl 50 (SB50), *the* premier American sporting event.

Norwich University, in partnership with local, state and Federal law enforcement, was tasked to provide cyber security and threat detection support during this event.

Event Objectives

To achieve success during this event, Norwich needed to execute the following objectives:

1. **Monitor & Protect** - critical infrastructure and devices during Super Bowl 50
2. **Identify & Alert** - any indications of malicious activity during Super Bowl 50 – including Denial of Service (DoS) attacks, Man in the Middle (MITM) attacks, and rogue aerial drone activity.

The priority was to look for Man-in-the-Middle Attacks on the free network, protect the team's wireless networks, the ticketing network and to look for drones or drone controllers during the event.

In evaluating solutions to achieve these objectives, the Norwich team selected the Pwnie Express Pulse Platform as the leading technology to solve this problem due to its ease of deployment, powerful real-time threat detection engine and it's simple yet intuitive user interface.

Why Pwn Pulse?

Pwn Pulse is a SaaS platform designed to continuously discover all wired, WiFi and Bluetooth devices in the vicinity of each of an organization's locations, all in real-time.

Plug-and-play sensors continuously monitor the airspace and that data is pushed securely to Pulse automatically. Pulse's underlying analytics engine evaluates this data in real-time to provide full scope device threat visibility, intelligence and alerting.

Right-sizing Sensor Deployment

The Pwn Pro sensor was an ideal choice for Levi's Stadium, but how many were necessary to achieve the objective? Since the Pwn Pros operate in receive-only mode, the sensing range is much longer than if it were also tasked to operate as an access point. Levi's Stadium covers 1.85 million square feet, so it was important to right-size the deployment to ensure complete coverage and visibility. To that end, the Norwich team executed an on-site environmental assessment, identifying ideal sensor placement and coverage required in order to achieve the objectives.

Pre-Event Reconnaissance & Setup

Prior to the event, Norwich and Pwnie Express established a remote Security Operations Center (SOC) and monitored the environment with Pulse to identify & characterize the access points (BSSID, ESSID, vendors, encryption level) as well as volume and type of clients in the environment. The team also received the list of high-priority networks and devices in the stadium.

The Event

As over 71,000 fans filed into the stadium, the SOC monitored and analyzed the networks and devices in action, with over 55,000 devices active in the stadium and over 1,200 priority access points. Data usage by fans (>9 TB) and overall (>10 TB) set event records., as did the number of unique and concurrently connected WiFi users.

Pwnie Express was able to identify numerous open access points that appeared during the game, many of which were high-definition cameras capable of capturing and broadcasting live content, a serious intellectual property risk to the NFL.
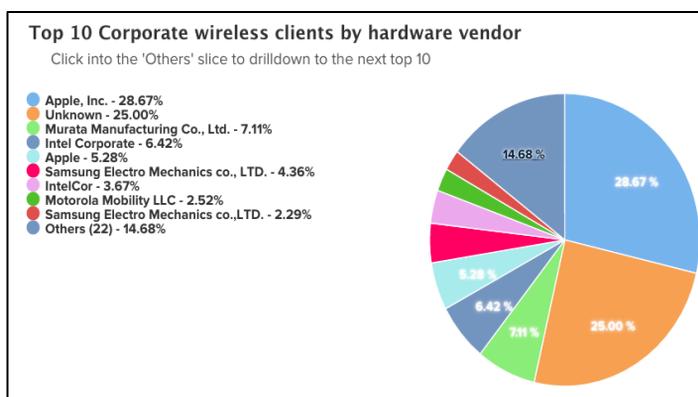
Additionally, Pwn Pulse discovered over 35,000 **Bluetooth** devices. Increasingly, this type of technology is used to not only guide users to specific locations within a geographic area, but it can also be used to conduct malicious activity. Being able to see these devices in real time, made it possible to validate appropriate device behavior.

Finally, the remote SOC identified de-authorization packets being sent to a guest network being used by an event-critical organization. This type of activity is indicative of an attempt to prevent this network from operating effectively. This is a common behavior of a malicious actor attempting to subvert a high-value network.

Best Practices & Lessons Learned

The value of full spectrum visibility for the purpose of real-time security operations cannot be overstated. Pre-event intelligence and a SOC based on Pulse made it easy to quickly identify areas of concern, investigate threats and respond quickly.

Conclusion

Ticket holders pay a premium not just to see the game but to experience a once-in-a-lifetime event, the Super Bowl. Increasingly, connected devices are part of that experience and are instrumental to event success. The challenges that major event IT staff will have to address moving forward are daunting. With visibility, monitoring and detection at the forefront of the event cyber security strategy, achieving these objectives are well within the realm of the possible.

About Pwnie Express

Pwnie Express provides the industry's only solution for continuous detection, identification and classification of wireless, wired and Bluetooth devices putting organizations at risk. Connected devices represent one of the fastest growing threats, unaddressed by existing security solutions. The Pwnie Express SaaS platform, Pulse, provides complete device coverage, including employee owned (BYOx), rogue and corporate devices. To learn more about Pwnie Express visit www.pwnieexpress.com.