National Infrastructure Protection Plan
NIPP Challenge

Location Detection of Rogue Base Stations/IMSI Catchers

SITUATIONAL AWARENESS

Rogue base stations, also known as international mobile subscriber identity (IMSI) catchers, are devices that masquerade as cell phone towers, tricking cell phones within a certain radius into connecting to the device rather than a tower. During recent pilot tests conducted over the public airwaves, DHS detected anomalous activity that appeared to be consistent with rogue technology being used in proximity to sensitive facilities such as the White House. Some rogue base stations may have advanced features allowing interception and alteration of communication content. As a result of unknown capabilities, there is a need to detect rogue base stations in order to better protect the communication sector's critical infrastructure.

METHODOLOGY

Researchers from the University of Washington (UW) and Subject Matter Experts (SMEs) from T-Mobile conducted detailed analysis to identify anomalous activity. Using the unique access and subject matter expertise of internal network operations, these researchers were able to differentiate between normal network traffic and potentially malicious activity associated with rogue base stations. These indicators formed the basis for the development of potential signature detection methods.

Through the NIPP Challenge, the project team developed an initial algorithm that would allow counterintelligence, government agencies and corporations to identify rogue base stations and protect sensitive data from being misdirected. The eventual goal of this technology, through additional validation processes, is to develop tools so industry can identify and confirm whether specific activities are cell sites or rogue base stations.

This project utilized prior research conducted jointly by T-Mobile and UW. As part of the project, the researchers developed updates to existing sensors and prepared network logging capabilities to collect network event logs at specific field test areas where rogue base station activity has previously been recorded. This data

Source: FEMA Photo Library

set was used as the initial starting point for the research project. Using the detection signatures and gathered data as inputs, the researchers were able to differentiate between normal network traffic and potentially malicious traffic associated with rogue base stations during several laboratory-based testing events.

RESULT

The project resulted in a white paper providing research findings and a proposal for the development of a tested algorithm. Moving forward, the goal of this algorithm is to mitigate and remediate man-in-the-middle attacks. Additionally, the project outputs produced a set of best practices for the communications industry when mitigating threats by rogue base stations.

Source: FEMA Photo Library