Greg and Dan Show April 3, 2023

The Dog Whistle Hack

- A technique, dubbed the "Near-Ultrasound Inaudible Trojan" (NUIT), allows an attacker to exploit smartphones and smart speakers over the Internet, using sounds undetectable by humans.
    - This is also known as a Dolphin Attack.
- The human hearing range is usually stated as 20Hz – 20KHz.
    - Very low tone to very high tone.
- Because of this, most microphones in electronics can “hear” that entire range.
- The older you get, the less likely you are to hear high-pitched sounds.
    - In your 20’s – 16KHz
    - In your 30’s – 15KHz
    - In your 40’s – 12KHz
    - A dog’s hearing range is 40Hz – 60KHz.
        - A dog whistle is in the range of 40KHz.
        - That’s why a dog can hear a dog whistle, but humans can’t.
- We use voice activation on a number of devices and systems such as:
    - Apple (Siri)
    - Alexa/Amazon Echo
    - Android (Google)
    - Microsoft (Cortana)

- So how does this attack work?
    - Record the appropriate wake-up word (Hey Siri, Alexa, etc.) and change the frequency to around 20KHz.
    - The device will hear the voice command, but the human victim will not.
    - The first voice command you issue is to silence the voice of the Siri, Alexa, etc., so the victim will not be tipped off that someone is issuing commands.
    - Now the attacker can issue any voice command using 20KHz as the frequency.

- How do we get the high-frequency commands to the targeted device?
    - Imbedded in a website.
    - Imbedded in a YouTube video or social media video.
    - Played in the background during a video chat or meeting.
- Smart homes are most vulnerable to these attacks.
    - For instance, telling Alexa to unlock the door if Alexa is connected to your smart lock.
- Any voice command that can be executed can be exploited using this attack.
- How can we prevent this?
    - Don’t use voice activation.
    - Use earphones during video meetings.
    - Apple/Siri only recognizes the owner’s voice.
    - To ultimately fix this vulnerability requires that all hardware have a different type of microphone that can filter out these high-frequency commands.