To Nicole Frazer
From Alex Crooks
Date 10/24/17
Subject: Krack Attacks

Earlier this month, researchers from the KU Leuven university in Belgium discovered a key flaw in the WPA2 WiFi encryption protocol that could allow attackers to intercept consumers credit card numbers, passwords, photos and other sensitive information. The flaws, dubbed "Key Reinstallation Attacks," or "Krack Attacks," are not particular to any specific products, but rather anything that uses a standard wireless connection. That means that just about every router, smartphone and PC out there could be impacted, especially Linux and Android devices, which the researchers said may be "particularly devastating".

Due to a bug in the WPA2 standard, these devices don't force the client to demand a unique encryption key each time. Rather, they allow a key to be cleared and replaced by an "all-zero encryption key,". Whereas an encryption key should look like a long, complex series of numbers, for example, 5722afd9cae3e3fab, the bug would change the encryption key to one single number, zero, and would appear as, 00000000000000. This means any user could access the program. In some cases, a script can also force a connection to bypass HTTPS, exposing usernames, passwords and other critical data.

To exploit this flaw, attackers find a vulnerable WPA2 network, make a copy of it, impersonate the MAC address, and then change the WiFi channel. This fake network acts as a "man in the middle," so when a device attempts to connect to the original network, it can be forced to bypass it and connect to the rogue one.

The system takes advantage of a flaw in the "handshake" method to direct users to the malicious network. Neither WiFi passwords nor secret keys can be obtained, the researchers say, as the hack works by forging the entire network. As such, but hackers can still eavesdrop on traffic, making it particularly dangerous for corporations.

The implications of this discovery are disturbing for several reasons. The first is that it exposes, yet again, the flaws present in wireless technology, which is used in every level of government, as demonstrated by a letter from Rep. Ted Lieu (CA-31) to Secretary Kelly that detailed the vulnerability of wireless networks throughout Trump properties. The implications of this means that attackers could gain highly sensitive information, without having to possess much computer hacking skill.

Second, it exposes another flaw that may be exploited to affect members of the general public. With the news of major leaks that expose private information, more and more people seek to buy this information on the dark web, knowing that the process to find and prosecute identity thieves is so long and arduous that they will face little to no repercussion.

A solution to this issue was created almost as soon as it was presented, and the flaw was not made available to the general public, so there is no immediate need for panic. Similarly, any website that has a a secure http connection, (HTTPS) would not be affected.