Il 5G è agli esordi ma ci sono già problemi di sicurezza

Ago 08, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Il nuovo standard si trascina alcuni problemi ereditati dai suoi predecessori. Possibile mappare tutti i dispositivi e "sabotare" l'autonomia dei device IoT.

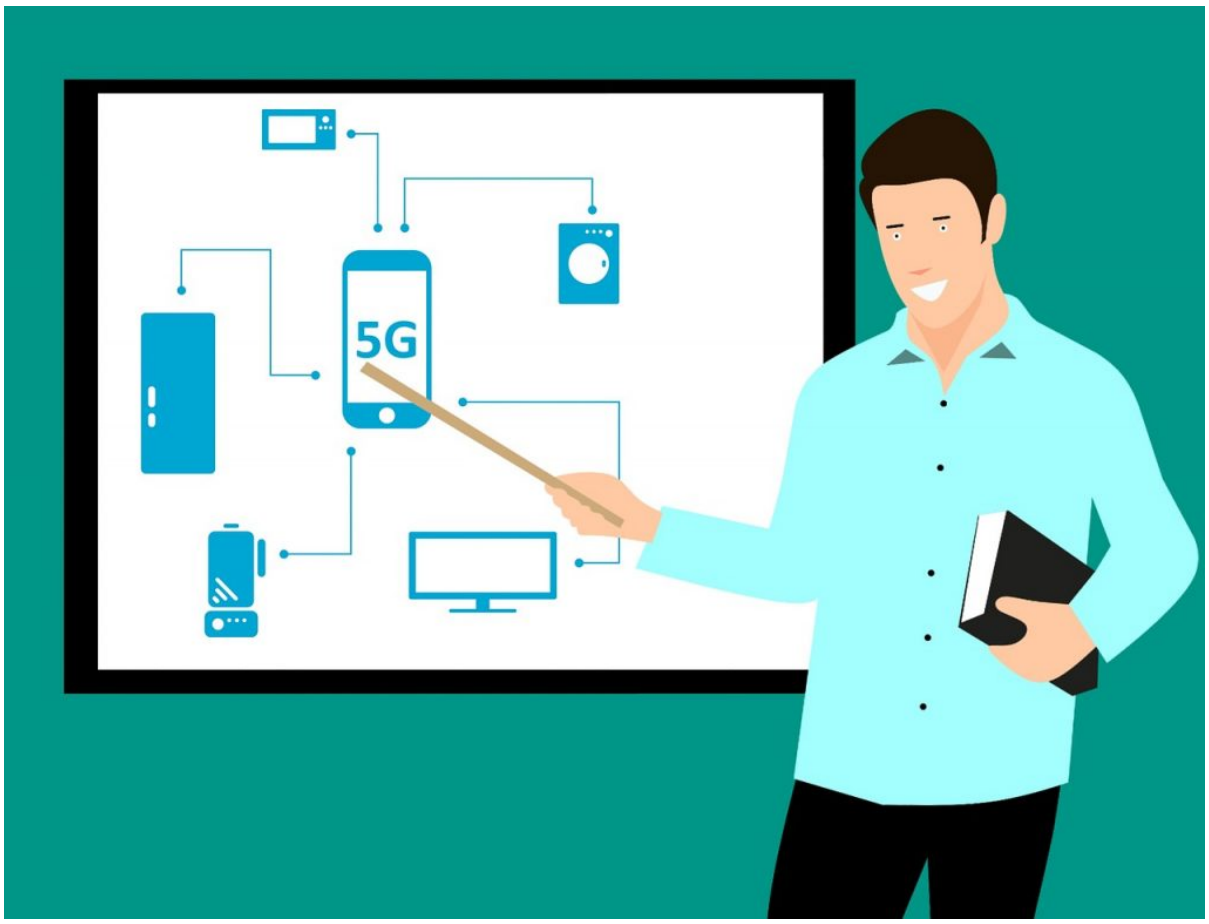
Mentre buona parte dell'opinione pubblica aspetta la nuova tecnologia 5G come la rivoluzione che trasformerà il nostro mondo in maniera radicale, dalle parti di Las Vegas emerge qualche dato preoccupante riguardo il livello di sicurezza garantito dalla nuova rete.

Nel corso del **Black Hat USA 2019**, infatti, i ricercatori di **Kaitiaki Labs** hanno esposto qualche "problemino" che il 5G si trascina come eredità dagli standard precedenti. A riportarlo è **Kaspersky**, in un articolo su uno dei suoi blog.

Il problema di fondo è che il protocollo prevede, come accadeva con 3G e 4G, che le trasmissioni vengono crittografate solo in una fase successiva al primo collegamento tra i dispositivi e la rete. Le prime informazioni trasmesse, quindi, sono in chiaro.

Solo che, con il protocollo 5G, questa debolezza diventa più rilevante. **Il nuovo protocollo, infatti, fonda la sua efficacia sulla capacità di offrire connessioni con caratteristiche diverse a seconda della tipologia di dispositivo o sulla specifica funzionalità a cui fa riferimento il traffico**.

Detto in parole povere: al momento della connessione i dispositivi forniscono molte più informazioni rispetto a quanto facessero prima con i vecchi protocolli.



Risultato: pirati informatici e cyber-spioni possono sapere se il device è in grado di effettuare chiamate, inviare SMS, se gestisce comunicazioni tra veicoli (nel caso di automobili a guida autonoma), conoscere le frequenze che utilizza e i protocolli.

La tecnica, battezzata **MNmap** (Mobile Network mapping) permette in pratica di rilevare quale tipo di dispositivo si collega.

Non solo: analizzando i vari tipi di servizi attivi i ricercatori spiegano di essere in grado di ottenere molte altre informazioni dalle quali è possibile capire, per esempio, se si ha a che fare con un iPhone o un Android, un modem o un dispositivo IoT.

Il tutto parte dal fatto che ci sono 5 produttori di hardware:

Intel, **Huawei**, **Mediatek**, **Samsung** e **Qualcomm**. Ognuno di loro, per impostazione predefinita, utilizza alcune specifiche funzionalità. Mappandole è possibile capire quale modem viene usato e, di conseguenza, si riduce il campo a una lista di dispositivi. Incrociando questa informazione con i dati di cui sopra, individuare il dispositivo specifico diventa piuttosto facile.

Al di là di MNmap, i ricercatori sono riusciti anche a testare un attacco **Man in The Middle** (MiTM) che permetterebbe, in questo caso, di prendere di mira i dispositivi che utilizzano il 5G. Uno dei possibili obiettivi di un attacco del genere può essere quello di ridurre la banda disponibile inviando false informazioni alla rete, per esempio "strozzando" la connessione di un iPhone (normalmente 1Gbps) a soli 2Mbps.

Ma è possibile anche degradare l'autonomia dei dispositivi IoT. Uno degli sbandierati vantaggi del 5G, infatti, è la possibilità di gestire il funzionamento dei dispositivi in maniera "intelligente", facendo in modo che si attivino solo quando è necessario, arrivando a ottenere un'autonomia straordinaria, addirittura di 10 anni.

Un intervento attraverso un attacco MiTM potrebbe modificare i parametri per fare in modo che il device rimanga attivo e in costante ricerca di una connessione, riducendo l'autonomia a un quinto.

Tutti questi problemi sarebbero stati risolti con la release 14 dello standard 5G, che per il momento, però, non è stata implementata da nessun operatore sul mercato. Secondo i ricercatori potremo vedere le prime reti "sicure" solo dal prossimo anno e, per allora, chissà cos'altro sarà saltato fuori.

Condividi l'articolo

Double Dragon: il gruppo APT41 ha colpito anche l’Italia

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/08/08/il-5g-e-agli-esordi-ma-ci-sono-gia-problemi-di-sicurezza/