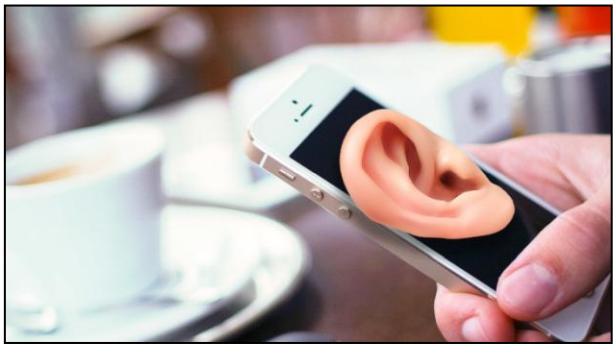
Ez a mobilhálózati hiba már nálunk is veszélyes lehet

Olyan hibát találtak, ami az 5G-s és 4G telefonokat is veszélyezteti. Például nagyon egyszerűen le lehet hallgatni őket.



Bár Európában egyelőre a kísérleti fázisnál tartanak a mobil operátorok az 5G-s szolgáltatásaikkal, már itt is valós veszélyt – mégpedig súlyosat – jelent az a biztonsági rés, amit kutatók fedeztek fel az új hálózatokban. A hálózat egy hibáját kihasználva gyakorlatilag teljesen védtelenné válhatnak az 5G-s és 4G-s telefonok is az illegális lehallgatással szemben. Emellett – szintén illegálisan – meg lehet határozni az ilyen készülékek földrajzi helyét.

A Purdue Egyetem és az Iowai Egyetem kutatói szerint a legnagyobb probléma az, hogy a jogosulatlan hozzáférés megszerzéséhez egyáltalán nem kell ismerni mélyen a mobilátviteli protokollokat – írja a Techcrunch.

200 dollárból megvan a lehallgató készülék

Az egyik hibát, melyet a jelfogadó protokollban találtak meg, Torpedo (a TRacking via Paging mEssage DistributiOn rövidítése) névre keresztelték a kutatók. A protokoll feladata az, hogy értesíti az egyes készülékeket, hogy bejövő hívást vagy más üzenetet kapnak.

A protokoll hibája révén a támadónak csupán annyit kell tennie, hogy rövid időn belül egymás után több hívást is kezdeményez, majd töröl, azaz leállít, utána a célzott készülékre lehet küldeni egy ún. paging üzenetet úgy, hogy annak fogadását már a készülék nem jelzi a felhasználónak. Ezzel új támadási felületet lehet nyitni a készüléken, és ráadásként nyomon követhetővé is válik.

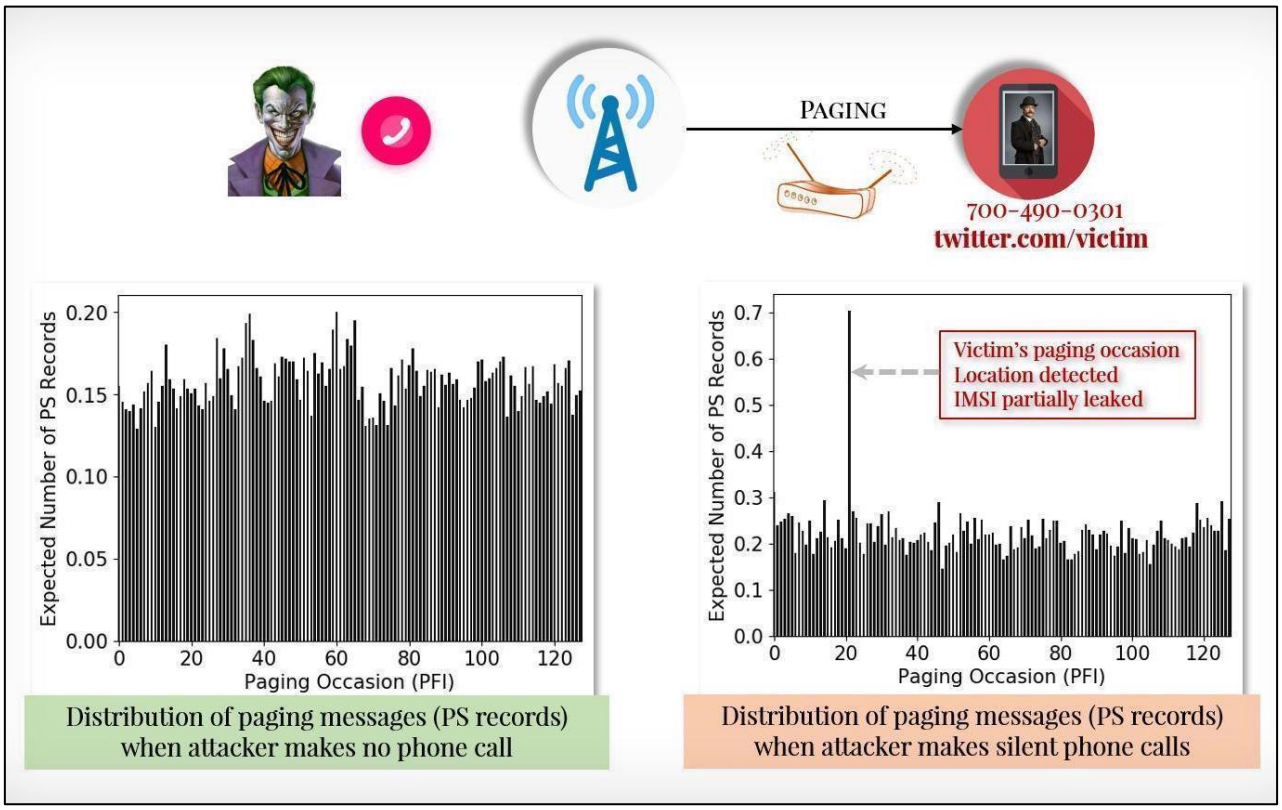
A másik hiba – ezt Piercernek nevezték el – a készülék egyedi IMSI (International Mobile Subscriber Identity) azonosítóját szolgáltatja ki a támadóknak mind a 4G-s, mind az 5G hálózatokon. Ennek az azonosítónak a birtokában egy 200 dolláros kütyüvel (egy ún. Stingray cellaszimulátor) is le lehet hallgatni a hívásokat.

A Torpedo hiba működési váza

A kutatók értesítették az érintett amerikai szolgáltatókat, de a Techcrunch cikke szerint azok egyelőre nem reagáltak. Szintén kapott értesítést a mobiloperátorok nemzetközi szervezete, a GSMA is. A kutatók egyelőre csupán a sérülékenység tényét publikálták, a részletes leírást, és a lehetséges támadásokra készített proof-of-concept kódot nem. Bár kíváncsian várjuk, hogy a kutatóknak az az állítása, hogy szaktudás nélkül hekkelhetők a mobilhálózatok, vajon hány amatőr hekker fantáziáját mozgatja meg.

Az egész világ érintett

Bár a kutatás alapvetően amerikai központú volt, de a probléma globális, valószínűleg az összes 4G és 5G mobilhálózatot érinti. Európában ugyan még csak tesztfázisban tartanak az 5G-s hálózatok – a Deutsche Telekom épp az MWC-n jelentette be, hogy már hat országban (köztük Magyarországon) 150 antennát állítottak fel. A DT esetében még nagyobb gondot okozhat a hiba, ugyanis a vállalat első körben épp az ipari szereplőknek, kritikus környezetbe akarja eladni az 5G-t.



(Forrás: Techcrunch)

A kutatók szerint a biztonsági rés befoltozása nem lesz egyszerű, mert a szabványügyi testületnek és a szolgáltatóknak közösen kell megtalálniuk a megoldást.

Forrás: https://bitport.hu/ez-a-mobilhalozati-hiba-mar-nalunk-is-veszelyes-lehet

Válogatta: Fonyó Istvánné