CTI elemzés

SS7 protokoll sérülékenységei

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

NEMZETI KIBERBIZTONSÁGI INTÉZET

A telefonálás és a telefonos sérülékenységek rövid történelme

A telefonhálózatok működése a kezdeti időszakban még jelentős mértékben manuális kapcsolásra épült. A 20. század elején a hívások felépítését központi operátorok végezték, akik fizikailag kapcsolták össze a hívó és a hívott felet. Ez a modell az alacsony előfizetőszám mellett működőképes volt, azonban a hálózatok gyors növekedésével a skálázhatósági korlátok egyre nyilvánvalóbbá váltak. A fejlődés így az automatizált hívásfelépítés irányába mozdult el, ahol a tárcsázott számot a hálózat jelzési mechanizmusokon keresztül értelmezte.

A korai automatikus rendszerekben a tárcsás készülékek elektromos impulzusokkal továbbították a számjegyeket. A telefonközpont ezeket dekódolta, majd ennek alapján kapcsolta a hívást. Bár ez technológiai előrelépést jelentett, hamar megjelentek a megbízhatósági és hatótávolsági problémák, különösen nagy távolságú kapcsolások esetén. Ezt követően jelentek meg a tone alapú signaling megoldások, ahol a számjegyeket különböző frekvenciák reprezentálták. Ezek a rendszerek gyorsabbak és stabilabbak voltak, azonban a biztonság továbbra sem volt elsődleges tervezési szempont.

A korszak egyik kritikus sajátossága az volt, hogy a jelzés (signaling) és a beszédforgalom sok esetben ugyanazon a csatornán haladt. Ez a megoldás egyszerűbb infrastruktúrát tett lehetővé, viszont megnyitotta az utat a visszaélések előtt. Ha valaki képes volt a megfelelő jelek előállítására, akkor a hálózat működését is képes volt befolyásolni. Ez volt a korai telefonos sérülékenységek alapja.

A legismertebb példa a blue box jelenséghez kapcsolódik, amely a phone phreaking korszak egyik meghatározó technikája volt. A rendszer bizonyos esetekben a 2600 Hz-es hangot használta a vonal állapotának jelzésére. A támadók ezt kihasználva mesterségesen generálták ezt a frekvenciát, és így a hálózatot téves állapotba kényszerítették. A módszerrel lehetővé vált a hívások manipulálása, illetve akár ingyenes nemzetközi hívások kezdeményezése is. Steve Jobs és Steve Wozniak korai tevékenysége is ehhez a korszakhoz köthető, ami jól mutatja, hogy már ekkor is ismert volt a signaling manipuláció kockázata.

A probléma gyökere nem egy konkrét implementációs hiba volt, hanem a hitelesítés hiánya és a hálózaton belüli implicit bizalom. A távközlési rendszerek abból indultak ki, hogy a signaling jeleket csak megbízható hálózati elemek generálhatják, így nem építettek be erős ellenőrzési mechanizmusokat. Ez a feltételezés azonban a gyakorlatban nem állta meg a helyét.

A távközlési iparág válasza erre a problémára egy alapvető architekturális váltás volt. Megjelent a sávon kívüli jelzés (out-of-band signaling) koncepciója, amely elkülönítette a vezérlési információkat a beszédcsatornától. Ez a megközelítés vezetett el a common channel signaling rendszerekhez, majd később az SS7 protokollkészlethez, amely már dedikált signaling hálózatra épült.

Ez a váltás jelentős előnyöket hozott, például gyorsabb hívásfelépítést, jobb útvonalválasztást, valamint új szolgáltatások, például roaming és SMS támogatását. Ugyanakkor a biztonsági modell alapja továbbra is a hálózati szereplők közötti bizalom maradt. A rendszer abból indult ki, hogy aki hozzáfér a signaling hálózathoz, az legitim szereplő.

Ennek következtében a korábbi korszak problémái nem tűntek el, hanem protokollszintű sérülékenységekké alakultak. Az SS7 esetében már nem fizikai vagy akusztikai manipulációról beszélünk, hanem olyan logikai visszaélésekről, amelyek a hitelesítés hiányából, a jogosultságkezelés gyengeségeiből és a globális hálózati bizalmi modellből erednek.

Mi is az az SS7 és hogyan működik?

Az SS7 (Signaling System 7) egy nemzetközi telekommunikációs signaling protokollkészlet, amelyet az 1970-es években fejlesztettek ki a PSTN hálózatok (Public Switched Telephone Network) működésének támogatására. Feladata nem a hang továbbítása, hanem a hívásvezérlés, azaz a kommunikációt irányító jelzések kezelése. Az SS7 felel többek között a hívásfelépítésért, a hívásbontásért, az SMS továbbításáért, valamint olyan szolgáltatások működéséért, mint a roaming vagy az előfizető-kezelés.

A korábbi signaling rendszerekkel ellentétben az SS7 már sávon kívüli jelzést használ. Ez azt jelenti, hogy a vezérlőjelek nem ugyanazon a csatornán haladnak, mint a hangforgalom, hanem egy külön signaling hálózaton. Ez a megközelítés jelentősen javította a hatékonyságot, csökkentette a torlódást, és lehetővé tette a komplexebb szolgáltatások megjelenését. Ugyanakkor a biztonsági modell továbbra is a megbízható hálózati szereplők feltételezésére épült.

Az SS7 működése több logikai komponens együttműködésén alapul. Az STP (Signal Transfer Point) a signaling üzenetek irányításáért felel, és biztosítja, hogy azok a megfelelő célállomásra jussanak. Az SSP (Service Switching Point) kezeli a híváslogikát, tehát a

hívás felépítését és bontását. Az SCP (Service Control Point) pedig az előfizetői adatbázisokkal kommunikál, például ellenőrzi, hogy egy adott előfizető milyen szolgáltatásokra jogosult.

Az előfizetői adatok kezelésében kulcsszerepet játszik a HLR (Home Location Register), amely a felhasználó állandó adatait tartalmazza, például az előfizetés típusát és azonosítóit. Ezzel szemben a VLR (Visitor Location Register) ideiglenesen az adott területen tartózkodó előfizetők adatait tárolja, különösen roaming esetén. Ez a két adatbázis együtt biztosítja, hogy a hálózat mindig tudja, hol érhető el az adott előfizető.

Az SS7 egyik kulcsfontosságú működési eleme a különböző signaling üzenetek cseréje. Például egy SMS küldésekor az üzenet először a felhasználó készülékéből a legközelebbi bázisállomáshoz jut, majd a hálózat az SS7 segítségével meghatározza a célhálózatot és az útvonalat. Az üzenet több hálózaton keresztül is továbbhaladhat, miközben a signaling réteg folyamatosan biztosítja a megfelelő irányítást.

A mobilhálózatok fejlődésével az SS7 szerepe tovább bővült, különösen a 2G és 3G hálózatokban, ahol ez a protokoll képezte a signaling infrastruktúra alapját. A 2000-es évektől kezdve azonban a távközlés fokozatosan átalakult, és megjelentek az IP-alapú hálózatok. Ennek következtében az SS7 működését is adaptálni kellett, amihez a SIGTRAN technológia nyújtott megoldást. A SIGTRAN lehetővé teszi, hogy az SS7 signaling üzenetek IP hálózatokon keresztül továbbítódjanak, miközben megőrzik az eredeti működési logikát.

Fontos hangsúlyozni, hogy bár a szállítási közeg IP-alapúvá vált, az azonosítás továbbra sem klasszikus hálózati címekhez kötődik. A mobilhálózatokban az előfizetők azonosítása elsősorban az IMSI (International Mobile Subscriber Identity) alapján történik, amely a SIM kártyában található egyedi azonosító.

Ez a modell teljesen eltér az internetes rendszerekben megszokott IP vagy MAC alapú azonosítástól.

Bár Európában a 2G és 3G hálózatok szerepe folyamatosan csökken, az SS7 továbbra is kritikus szerepet játszik a hálózatok közötti kommunikációban, különösen a nemzetközi roaming esetében. Emellett számos országban még mindig ezek a technológiák jelentik az alap mobil infrastruktúrát.

A biztonság szempontjából az SS7 egyik legfontosabb jellemzője, hogy nem tartalmaz beépített hitelesítési mechanizmusokat. A rendszer abból indul ki, hogy a signaling hálózathoz csak megbízható szolgáltatók férnek hozzá. Ez a feltételezés alapjaiban hibás és ez képezi az SS7 sérülékenységeinek kiinduló pontját.

Hozzáférés szerzése az SS7-hez

Az SS7 alapú támadások egyik legkritikusabb előfeltétele a signaling hálózathoz való hozzáférés. A rendszer sajátossága, hogy nem a végfelhasználói eszközök kompromittálása jelenti az elsődleges belépési pontot, hanem a telekommunikációs infrastruktúrához való csatlakozás. Amennyiben egy támadó képes legitim szereplőként megjelenni az SS7 hálózatban, akkor a rendszer logikájából adódóan széles körű műveletek végrehajtására válik képessé.

A biztonsági modell egyik alapvető gyengesége a globális bizalmi architektúra, amely feltételezi, hogy a hálózathoz csatlakozó entitások megbízható szolgáltatók. Ez a feltételezés a modern környezetben már nem állja meg a helyét, mivel a távközlési piac jelentősen fragmentálódott, és számos kisebb vagy kevésbé szabályozott szereplő is hozzáférést kap a rendszerhez. Egyetlen kompromittált vagy rosszindulatú szolgáltató elegendő lehet a teljes hálózat kihasználásához.

A hozzáférés megszerzésének egyik legelterjedtebb módja a hozzáférés vásárlása. Bizonyos, gyengén szabályozott piacokon működő szolgáltatók lehetőséget biztosítanak harmadik felek számára SS7 kapcsolódásra, jellemzően egy úgynevezett GT (Global Title) kiosztásával. A GT egy egyedi hálózati azonosító, amely lehetővé teszi a signaling üzenetek küldését és fogadását. A támadók számára ez kvázi belépőt jelent a globális signaling infrastruktúrába. Az ilyen hozzáférések ára jellemzően több ezer dolláros nagyságrendű, ami azt jelenti, hogy a támadás nem csak állami szereplők, hanem pénzügyileg motivált csoportok számára is elérhető.

Ez a modell különösen veszélyes, mivel a támadók nem saját infrastruktúrát építenek, hanem egy legitim szolgáltató identitását használják.

Ennek következtében a rosszindulatú forgalom gyakran nem különböztethető meg a valós signaling üzenetektől, ami jelentősen megnehezíti a detekciót és a visszakövetést.

A második jelentős hozzáférési útvonal a legitim szolgáltatók kompromittálása. Ebben az esetben a támadók közvetlenül egy meglévő operátor infrastruktúráját veszik célba, például rosszul konfigurált SS7 gateway-eket, elavult szoftvereket vagy nem megfelelően védett hálózati csomópontokat. Egy sérülékeny STP vagy más signaling komponens kompromittálása után a támadó már képes lehet saját üzeneteket injektálni a hálózatba.

Gyakori támadási vektor a hitelesítő adatok megszerzése, amely történhet phishinggel, malware-rel vagy belső szivárgás útján. Egy ilyen hozzáférés különösen értékes, mivel a támadó teljes mértékben legitim felhasználóként jelenik meg a rendszerben. A valós incidensek azt mutatják, hogy már egyetlen hibás tűzfalkonfiguráció is elegendő lehet ahhoz, hogy külső szereplők SS7 üzeneteket küldjenek egy operátor hálózatán keresztül.

A harmadik megközelítés a rádiós oldali támadások, amelyek célja az előfizetőhöz köthető azonosítók megszerzése. Ide tartoznak az úgynevezett IMSI-catcher eszközök, amelyek hamis bázisállomásként működnek. Ezek az eszközök erősebb jelet sugároznak, mint a valós cellatornyok, így a mobiltelefonokat arra kényszerítik, hogy hozzájuk csatlakozzanak. A támadás alapja a hálózatoldali hitelesítés hiánya, vagyis az, hogy a készülék nem tudja ellenőrizni a bázisállomás valódiságát.

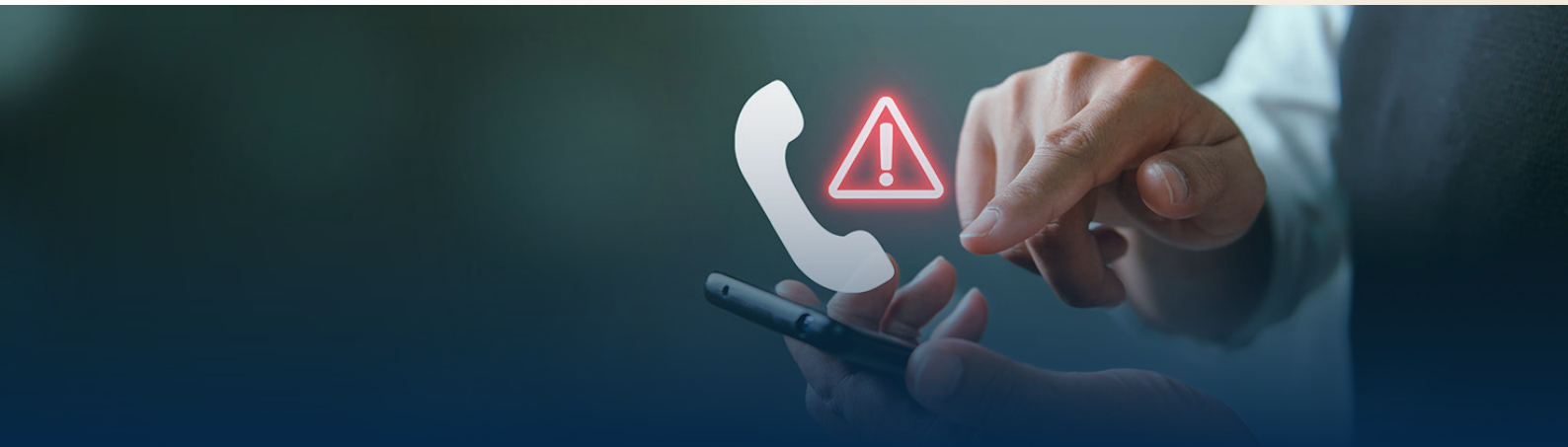
A kapcsolat létrejötte után a támadó képes kikényszeríteni az IMSI azonosító elküldését, illetve bizonyos esetekben a kommunikációt

gyengébb titkosításra vagy akár titkosítatlan módra degradálni. Modern hálózatok esetén a támadók gyakran alkalmaznak downgrade támadásokat, amelyek során az eszközt visszakényszerítik egy 2G vagy 3G környezetbe, ahol a védelem gyengébb.

Fontos kiemelni, hogy az IMSI-catcher önmagában nem biztosít teljes SS7 hozzáférést, azonban lehetővé teszi a célpont azonosítását. Az így megszerzett IMSI segítségével a támadó már képes lehet célzott SS7 lekérdezéseket indítani, amennyiben rendelkezik signaling hozzáféréssel.

Miután a támadó hozzáférést szerzett az SS7 hálózathoz, a további támadások végrehajtásához gyakran elegendő egyetlen adat, a telefonszám. A legtöbb támadási lánc első lépése az ehhez tartozó IMSI meghatározása, amely különböző signaling requestek segítségével megszerezhető. Ezt követően a támadó képes lehet hívások átirányítására, SMS-ek elfogására vagy a felhasználó helyadatainak lekérdezésére.

Az SS7 esetében tehát a támadási modell alapja nem egy klasszikus exploit, hanem a rendszerszintű bizalom kihasználása. A hálózat úgy lett megtervezve, hogy a résztvevők együttműködnek, nem pedig egymás ellen védekeznek. Ez a megközelítés a mai, erősen összekapcsolt és részben nyitott környezetben komoly biztonsági kockázatot jelent.



Telefonhívások és SMS üzenetek eltérítése

Az SS7 hálózat egyik legsúlyosabb sérülékenysége, hogy lehetővé teszi a hívások és SMS-ek átirányítását, megfelelő jogosultságok ellenőrzése nélkül. Amennyiben egy támadó hozzáfér a signaling hálózathoz, és rendelkezik a célpont telefonszámával vagy IMSI azonosítójával, akkor képes lehet beavatkozni a kommunikáció irányításába.

A támadások alapja az, hogy az SS7 hálózat a hívások felépítése során folyamatosan signaling üzeneteket használ a célállomás meghatározására. Ezek az üzenetek tartalmazzák, hogy az adott előfizető melyik hálózaton, melyik kapcsolón, illetve melyik VLR-en keresztül érhető el. Ha egy támadó képes ezt az információt manipulálni, akkor a hálózat a kommunikációt nem a valódi célhoz, hanem a támadó által meghatározott pontra irányítja.

A telefonhívások eltérítése tipikusan egy olyan folyamat, ahol a támadó módosítja az előfizetőhöz tartozó routing információkat. Ennek egyik módja az insert subscriber data request használata, amely eredetileg legitim célokra, például előfizetői profilok frissítésére szolgált. A támadó azonban ezt a requestet arra használhatja, hogy egy új, általa kontrollált VLR címet rendeljen az áldozathoz.

Amikor a hálózat egy bejövő hívás során lekérdezi, hogy hol található az előfizető, a manipulált adatok miatt a rendszer a támadó infrastruktúráját fogja visszaadni. Ennek következtében a hívás először a támadóhoz érkezik meg, aki azt továbbíthatja a valódi cél felé. Ez a modell lehetővé teszi a man-in-the-middle jellegű lehallgatást, miközben a kommunikáció mindkét fél számára zavartalannak tűnik.

Az SMS-ek esetében a támadás még közvetlenebb módon valósítható meg. Az SS7 hálózatban az üzenetek továbbítása során a rendszer a VLR és HLR információk alapján határozza meg, hogy hová kell kézbesíteni az adott üzenetet. A támadók ezt a mechanizmust használják ki az update location request segítségével.

Az update location üzenet célja normál esetben az, hogy a hálózat frissítse az előfizető aktuális helyét, például roaming során. Egy támadó azonban hamis requestet küldve átirányíthatja az előfizetőt egy általa kontrollált VLR-re, így a hálózat minden bejövő SMS-t és hívást erre a pontra fog irányítani. Ez gyakorlatilag teljes kommunikációs kontrollt jelent az áldozat felett.

Egy másik gyakran használt mechanizmus a forwardSMS funkció, amely lehetővé teszi, hogy egy üzenet egy alternatív célra kerüljön továbbításra. A támadó egy forwardSMS request segítségével közvetlenül utasíthatja az SMSC-t (Short Message Service Center) arra, hogy az üzenetet ne az eredeti címzettnek, hanem egy másik számra vagy rendszerbe küldje. Mivel az SS7 nem végez erős hitelesítést, ez a művelet gyakran észrevétlen marad.

Az SMS-ek eltérítése különösen kritikus a modern rendszerekben, mivel számos szolgáltatás használ SMS-alapú 2FA megoldásokat. Ha a támadó képes elfogni ezeket az üzeneteket, akkor gyakorlatilag megkerülheti a második hitelesítési faktort. Ez közvetlen hozzáférést biztosíthat banki fiókokhoz, e-mail szolgáltatásokhoz vagy kriptovaluta tárcákhoz.

Fontos megjegyezni, hogy az SS7 hálózaton az SMS-ek továbbítása nem biztosít end-to-end titkosítást, így a signaling szinten történő manipuláció teljes mértékben elegendő az üzenetek elfogásához.

A támadónak nincs szüksége az áldozat készülékéhez való fizikai hozzáférésre, és gyakran semmilyen látható jel nem utal a kompromittálódásra.

A támadások sikerességének kulcsa az, hogy a hálózat a beérkező signaling üzeneteket legitimnek feltételezi, és nem ellenőrzi azok eredetét megfelelő mélységben. Ez azt jelenti, hogy egy megfelelően kialakított request a hálózat számára normál működésnek tűnik, még akkor is, ha valójában rosszindulatú.

Az SS7 ezen sajátossága miatt a hívások és üzenetek eltérítése nem csupán elméleti lehetőség, hanem a gyakorlatban is többször bizonyított támadási módszer. A rendszer logikája lehetővé teszi, hogy egy támadó a kommunikáció útvonalát módosítsa, anélkül, hogy a végpontok ezt érzékelnék.

Helyadatok megszerzése

Az SS7 hálózat egyik leginkább rejtett, ugyanakkor rendkívül érzékeny visszaélési lehetősége a felhasználók helyadatainak lekérdezése. A rendszer eredeti célja az volt, hogy a hálózat mindig tudja, hol érhető el egy előfizető, például hívásfelépítés vagy roaming során. Ez a funkcionalitás azonban megfelelő ellenőrzések hiányában lehetőséget ad a célzott helymeghatározásra is.

A mobilhálózatok működéséből adódóan egy eszköz mindig kapcsolódik egy adott cellatoronyhoz, amely egy adott földrajzi területet fed le. A hálózat ezen információ alapján képes meghatározni az előfizető aktuális celláját, ami városi környezetben akár 100–500 méteres pontosságot is jelenthet. Ritkábban lakott területeken ez a pontosság jelentősen romlik, mivel a cellák mérete nagyobb.

A támadások alapja az, hogy az SS7 lehetővé teszi különböző signaling lekérdezések küldését az előfizető állapotáról és helyéről. Ezek a lekérdezések eredetileg teljesen legitim célokat szolgálnak, például roaming menedzsmentet vagy hívásirányítást, azonban megfelelő védelem hiányában visszaélésre is alkalmasak.

Az egyik legismertebb ilyen mechanizmus az ATI (Any Time Interrogation). Ez a request lehetővé teszi, hogy egy hálózati elem lekérdezze az előfizető aktuális állapotát a HLR-ből. A válasz tartalmazhatja a MSRN-t (Mobile Station Roaming Number) és a cellaazonosítót, amelyek alapján a felhasználó tartózkodási helye meghatározható. A támadók ezt úgy használják ki, hogy magukat egy legitim szolgáltatónak álcázva küldenek ATI requesteket. Mivel a rendszer nem végez megfelelő forrásellenőrzést, a lekérdezések gyakran sikeresen lefutnak.

A védekezési intézkedések miatt az ATI requestek ma már sok hálózatban szűrésre kerülnek, azonban a támadók más módszereket is alkalmaznak. Ilyen például a PSI (Provide Subscriber Information) request, amely még részletesebb adatokat ad vissza, beleértve az IMSI, az IMEI, valamint a hálózati státusz információit. A PSI segítségével a támadó nemcsak a helyadatokat, hanem az eszközre vonatkozó metaadatokat is megszerezheti.

Az SRI (Send Routing Information) request eredetileg a hívások útvonalának meghatározására szolgál, azonban mellékhatásként információt ad az előfizető aktuális hálózati elérhetőségéről és a kapcsolódó infrastruktúráról. A támadók gyakran kombinálják az SRI-t más lekérdezésekkel, például ATI vagy PSI requestekkel, így pontosabb képet kapnak a célpont helyzetéről.

Egy fejlettebb támadási modellben ezek a lekérdezések láncolva kerülnek felhasználásra. A támadó először megszerzi az IMSI azonosítót, majd különböző requestek segítségével lekéri az aktuális cellainformációkat, és ezt időben ismételve képes lesz a felhasználó mozgásának követésére. Ez a folyamat gyakorlatilag egy valós idejű követési képességet biztosít, minimális késleltetéssel.

Fontos különbség, hogy itt nem klasszikus értelemben vett GPS alapú helymeghatározásról van szó, hanem hálózati szintű lokalizációról. A pontosság ezért a cellasűrűségtől és a hálózat konfigurációjától függ, azonban sok esetben bőven elegendő egy személy mozgásának profilozására vagy egy adott helyszínen való jelenlétének igazolására.

A támadások detektálását jelentősen nehezíti, hogy a lekérdezések teljesen legitim signaling üzeneteknek tűnnek. Nem tartalmaznak kártékony kódot, nem okoznak szolgáltatáskimaradást, és nem generálnak feltűnő anomáliát. A visszaélés maga a funkcionalitás használata, nem pedig annak megkerülése.

Ez különösen veszélyessé teszi az SS7-et adatvédelmi szempontból. Egy támadó képes lehet hosszabb időn keresztül, észrevétlenül gyűjteni adatokat egy célpontról, beleértve annak napi rutinját, utazási szokásait vagy akár érzékeny helyszínekhez való kapcsolódását.

SS7 alapú DoS támadások

Az SS7 hálózat sérülékenységei nemcsak adatvédelmi vagy lehallgatási kockázatokat jelentenek, hanem lehetőséget adnak DoS (Denial of Service) típusú támadások végrehajtására is. Ezek a támadások a signaling infrastruktúrát célozzák, és céljuk a hálózat működésének részleges vagy teljes megzavarása.

A támadások alapja az, hogy az SS7 hálózat a signaling üzeneteket alapértelmezetten legitimnek tekinti, és nem végez mély ellenőrzést azok forrására vagy mennyiségére vonatkozóan. Ez lehetővé teszi, hogy egy támadó nagy mennyiségű vagy célzott signaling requestekkel túlterhelje a hálózati komponenseket.

Az egyik leggyakrabban kihasznált mechanizmus a Cancel Location request. Normál működés során ez a request arra szolgál, hogy egy előfizetőt eltávolítson egy adott VLR-ből, például amikor az előfizető hálózatot vált. Egy támadó azonban ezt a funkciót arra használhatja, hogy folyamatosan törölje az áldozat regisztrációs állapotát, így a felhasználó nem lesz képes hívásokat fogadni vagy SMS-eket kapni.

Ha a támadó ezt a requestet nagy mennyiségben küldi, akkor nemcsak egyéni felhasználókat, hanem a háttérben működő HLR rendszert is túlterhelheti. Mivel a HLR kulcsszerepet játszik az előfizetők állapotának kezelésében, a túlterhelése szélesebb körű szolgáltatáskimaradáshoz vezethet.

Egy másik súlyos támadási forma a Purge Mobile request használata. Ez a mechanizmus az előfizető teljes eltávolítását végzi a HLR adatbázisból, ami gyakorlatilag azt jelenti, hogy az adott felhasználó leválik a hálózatról. Tömegesen alkalmazva ez a módszer akár teljes régiókat érintő kiesést is okozhat.

A támadások nem mindig egyedi előfizetőket céloznak. A támadók gyakran alkalmaznak úgynevezett signaling flood technikákat, ahol nagy mennyiségű hibás vagy értelmetlen üzenetet küldenek a hálózatba. Ezek az üzenetek túlterhelik az STP csomópontokat, ami különösen kritikus, mert ha az STP nem képes feldolgozni a beérkező forgalmat, akkor a teljes signaling hálózatban késleltetés vagy blokkolás léphet fel. Ez közvetlen hatással van a hívásfelépítésre, az SMS kézbesítésre és más alapvető szolgáltatásokra.

A DoS támadások hatása nem korlátozódik egyetlen szolgáltatóra. Az SS7 hálózat globálisan összekapcsolt, így egy adott ponton generált túlterhelés más hálózatokra is átterjedhet. Ez azt jelenti, hogy egy lokális támadás is képes lehet nemzetközi szintű fennakadást okozni.

Különösen kritikus a helyzet olyan környezetekben, ahol a mobilhálózatok a vészhelyzeti kommunikáció alapját képezik. Egy SS7 alapú DoS támadás hatással lehet a segélyhívásokra, a katasztrófavédelmi rendszerekre, vagy akár más kritikus infrastruktúrákra is, amelyek a mobilhálózatra támaszkodnak.

A detektálás ebben az esetben is nehéz, mivel a támadások gyakran legitimnek tűnő requestekből állnak. A különbség nem a request típusában, hanem annak mennyiségében és mintázatában rejlik. Ezért a hagyományos védekezési mechanizmusok sok esetben nem elegendőek.

Az SS7 DoS támadások egyik legfontosabb sajátossága, hogy nem igényelnek komplex exploitokat vagy fejlett malware-t. A támadók egyszerűen a rendszer normál működését használják túl, ami jól mutatja a protokoll alapvető tervezési korlátait.

Egyéb támadási vektorok

Az SS7 sérülékenységei nem korlátozódnak néhány jól ismert támadási formára, hanem egy szélesebb, folyamatosan fejlődő fenyegetési spektrum részét képezik. A valós tapasztalatok azt mutatják, hogy a támadók különböző módszereket kombinálnak, és a signaling hálózat sajátosságait több irányból is kihasználják.

Egy átfogó képet ad erről az ENISA által, 2018-ban végzett felmérés, amelyben több tucat telekommunikációs szolgáltató vett részt. Az eredmények szerint a megkérdezettek jelentős többsége, közel 88%-a számolt be SS7 alapú incidensekről 2017-ben. Ez azt mutatja, hogy a probléma nem elméleti, hanem rendszerszinten jelen lévő fenyegetés.

Az egyik leggyakoribb támadási forma az SMS spam, amely az SS7 hálózaton keresztül nagy mennyiségben küldött, gyakran automatizált üzeneteket jelent. Bár ez elsőre kevésbé tűnhet kritikusnak, valójában komoly problémát jelent, mivel a signaling infrastruktúrát terheli, és gyakran kapcsolódik phishing kampányokhoz vagy más, célzott támadásokhoz.

Szintén gyakran fordulnak elő spoofing támadások, ahol a támadó manipulálja a hívóazonosítót vagy az üzenetek forrását. Ez lehetővé teszi, hogy a támadó legitim szolgáltatóként vagy megbízható félként jelenjen meg, ami növeli a social engineering támadások sikerességét. A spoofing különösen veszélyes, mivel a felhasználók gyakran megbíznak a megjelenített telefonszámokban.

A szolgáltatók jelentős része számolt be helyadat lekérdezési kísérletekről, amelyek célja az előfizetők lokációjának meghatározása volt. Ezek a támadások gyakran nem járnak közvetlen

szolgáltatáskimaradással, ezért nehezebben észlelhetők, viszont komoly adatvédelmi kockázatot jelentenek.

Megjelentek továbbá különböző előfizetői csalások, amelyek során a támadók manipulálják az előfizetői adatokat vagy jogosultságokat. Ide tartozhat például a szolgáltatások jogosulatlan aktiválása, vagy olyan változtatások végrehajtása, amelyek pénzügyi előnyt biztosítanak a támadónak.

Az SMS eltérítés és a routing manipuláció szintén gyakori jelenség, amelyeket gyakran kombinálnak más támadási formákkal, például phishinggel vagy malware-rel. Ezek a módszerek különösen hatékonyak, ha a cél a hitelesítési folyamatok megkerülése vagy a felhasználói fiókok kompromittálása.

A jelentések alapján a támadók egyre gyakrabban alkalmaznak kombinált támadási láncokat, ahol több különböző technikát használnak egymás után vagy párhuzamosan. Például egy támadás kezdődhet IMSI megszerzéssel, majd folytatódhat helyadat lekérdezéssel, végül pedig SMS eltérítéssel. Ez a megközelítés jelentősen növeli a támadás hatékonyságát és nehezíti a detektálást.

Fontos megfigyelés, hogy az SS7 támadások jelentős része nem igényel fejlett technikai eszközöket vagy komplex exploitokat. A támadók gyakran a rendszer legitim funkcióit használják visszaélésszerűen, ami azt jelenti, hogy a védekezés nem egyszerűen technikai kérdés, hanem a jogosultságkezelés és a forgalomszűrés megfelelő kialakításán múlik.

A telekommunikációs szolgáltatók tapasztalatai alapján az egyik legnagyobb kihívás a láthatóság hiánya. Mivel a támadások gyakran nem okoznak azonnali szolgáltatáskimaradást, hanem háttérben zajlanak,

a detektálásuk speciális signaling monitoring megoldásokat igényel.

Az SS7 ökoszisztémában nincs egyetlen domináns támadási forma, hanem egy komplex, egymással összefüggő fenyegetési környezet van, ahol a támadók folyamatosan alkalmazkodnak a védekezési mechanizmusokhoz.

Esettanulmányok

Az SS7 sérülékenységei nem csupán elméleti kockázatot jelentenek, hanem a gyakorlatban is többször bizonyították, hogy valós környezetben, éles rendszerek ellen is sikeresen kihasználhatók. A következő példák jól szemléltetik, hogy a támadók milyen módon építik fel a támadási láncokat, és hogyan használják ki a signaling hálózat bizalmi modelljét.

Az egyik legismertebb példa a 2017-es németországi banki csalássorozat, ahol a támadók többlépcsős támadási láncot alkalmaztak. A folyamat során phishinggel megszerezték az áldozatok banki hitelesítő adatait és telefonszámát, majd ezt malware-rel egészítették ki, hogy stabil hozzáférést biztosítsanak.

Ezt követően SS7 hálózati manipulációval, egy „update location" típusú művelet segítségével, átirányították az áldozatoknak küldött OTP kódokat. Mivel a banki rendszerek SMS-alapú kétfaktoros hitelesítést (2FA) használtak, a támadók ezt teljes mértékben megkerülték, és a megszerzett egyszer használatos jelszavakkal jogosulatlan pénzügyi tranzakciókat hajtottak végre, miközben az áldozatok nem érzékeltek semmilyen rendellenességet. Az eset világosan rávilágított arra, hogy az

SMS-alapú hitelesítés önmagában nem biztonságos, amennyiben a mögöttes távközlési infrastruktúra sérülékeny.

Egy másik ismert példa a kriptovaluta tárcák feltörése, amelyet a Positive Technologies kutatói demonstráltak. A támadás során elegendő volt az áldozat neve és telefonszáma, hogy a támadók elindítsák az SS7 alapú lekérdezéseket. A folyamat során először megszerezték az IMSI azonosítót, majd ezt felhasználva képesek voltak SMS-ek elfogására, beleértve a belépéshez szükséges hitelesítési kódokat is.

Egy harmadik, gyakran hivatkozott eset a Ted Lieu amerikai kongresszusi képviselővel végrehajtott demonstráció. Ebben az esetben a kutatók a képviselő beleegyezésével hajtottak végre egy SS7 alapú támadást, amely során képesek voltak valós időben követni a helyzetét, valamint lehívni a hívásadatait.

A legújabb példák közé tartoznak a Salt Typhoon APT által végrehajtott műveletek, amelyek már egyértelműen állami szintű fenyegetést képviselnek. A támadások során több távközlési szolgáltató infrastruktúráját kompromittálták, és hozzáférést szereztek valós idejű kommunikációs adatokhoz, beleértve hívásokat, üzeneteket és egyéb metaadatokat.

Az SS7 sérülékenységei nem csupán pénzügyi vagy adatvédelmi kockázatot jelentenek, hanem nemzetbiztonsági szintű fenyegetést is, mivel a signaling hálózat kompromittálása lehetőséget teremt megfigyelésre, adatgyűjtésre és akár politikai folyamatok befolyásolására. A bemutatott esetek közös jellemzője, hogy a támadók nem klasszikus szoftverhibákat használtak ki, hanem a rendszer legitim működését fordították saját céljaikra, ami különösen megnehezíti a védekezést, hiszen az ilyen támadások nem hagyományos exploitokra épülnek, hanem a működési logika visszaélésszerű kihasználására.

Az SS7 napjainkban

A modern távközlési környezetben az SS7 szerepe jelentősen átalakult, de nem szűnt meg. Európában a mobilhálózatok túlnyomó része ma már 4G és 5G technológiákra épül, amelyek signaling szinten elsősorban a Diameter protokollt használják. Ez az architektúra IP-alapú működést, nagyobb skálázhatóságot és fejlettebb szolgáltatáskezelést tesz lehetővé.

A technológiai váltás ellenére az SS7 továbbra is jelen van a háttérben, elsősorban a legacy rendszerek támogatása és a hálózatok közötti interoperabilitás miatt. A legfontosabb terület, ahol az SS7 szerepe megmaradt, a nemzetközi roaming, ahol különböző generációjú hálózatoknak kell együttműködniük. Ez azt jelenti, hogy még egy modern 4G vagy 5G előfizető esetében is előfordulhat, hogy a kommunikáció bizonyos részei SS7 alapú signalingon keresztül történnek.

Magyarországon és Európában a 3G hálózatok kivezetése nagyrészt már megtörtént, és a következő években a 2G fokozatos lekapcsolása is napirenden van. Ugyanakkor a 2G továbbra is fontos szerepet tölt be, különösen olyan területeken, ahol a megbízhatóság és az alacsony adatforgalom a prioritás.

Számos ipari és hétköznapi rendszer még mindig a 2G infrastruktúrára támaszkodik. Ide tartoznak például különböző IoT eszközök, riasztórendszerek, liftek, valamint egyes járművek segélyhívó rendszerei. Ezek az eszközök gyakran hosszú életciklussal rendelkeznek, és nem frissíthetők könnyen újabb hálózati technológiákra. Ez a helyzet azt eredményezi, hogy a 2G és vele együtt az SS7 is hosszabb ideig velünk marad, mint azt elsőre feltételeznénk.

Globális szinten a helyzet még összetettebb. Számos fejlődő régióban a 2G és 3G hálózatok továbbra is meghatározóak, így az SS7 nemcsak jelen van, hanem sok esetben elsődleges signaling protokollként működik. Ez azt jelenti, hogy a sérülékenységek nem csupán örökségként maradnak fenn, hanem aktívan relevánsak a mai napig.

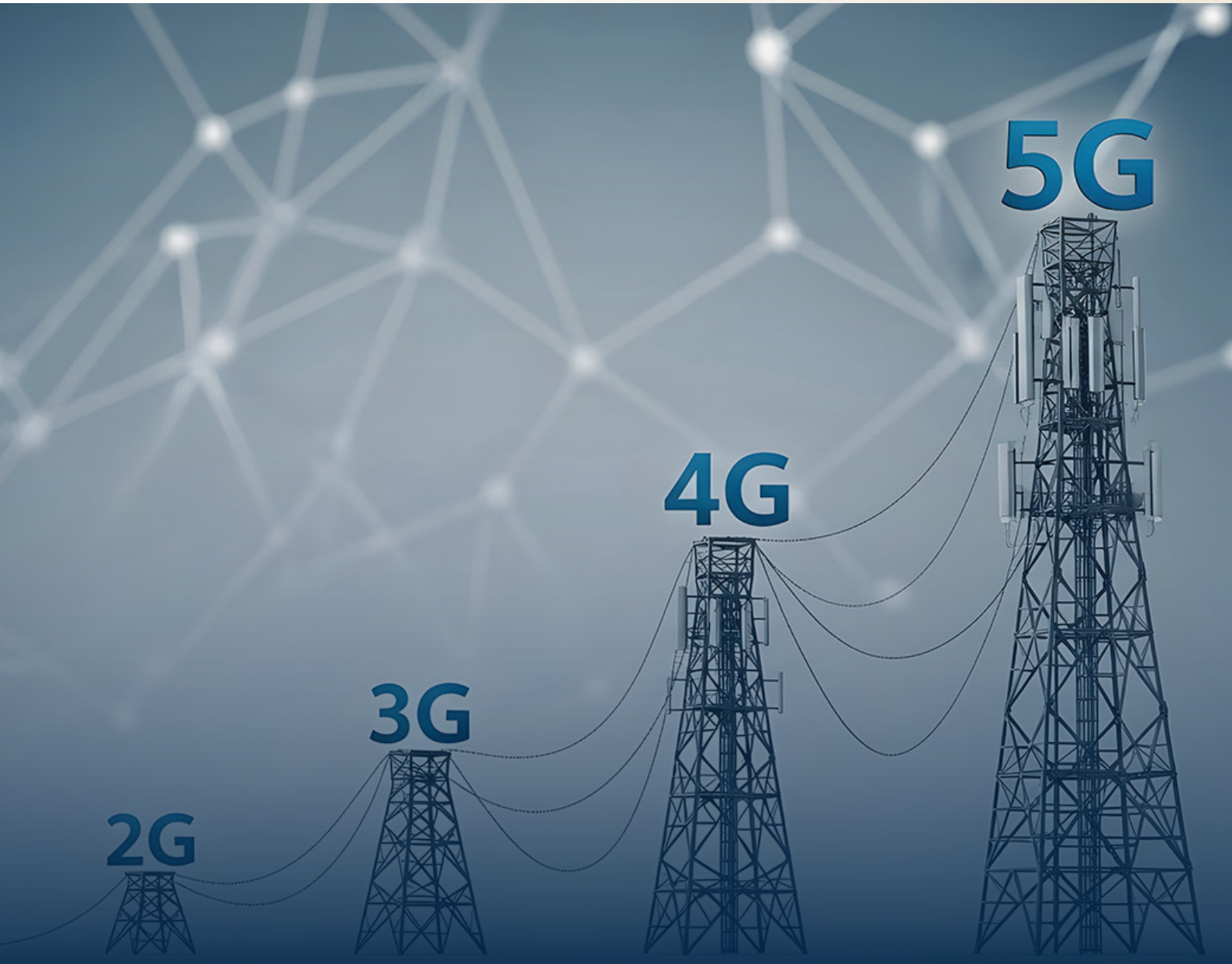
A modern hálózatokban az SS7 gyakran nem önállóan jelenik meg, hanem más technológiákkal együtt. A SIGTRAN lehetővé teszi, hogy az SS7 signaling üzenetek IP hálózatokon keresztül továbbítódjanak, ami egyszerre növeli a rugalmasságot és bővíti a támadási felületet. Az IP-alapú működés miatt a signaling infrastruktúra egyre inkább közelít az IT rendszerek világához, ahol a hagyományos távközlési bizalmi modell már nem elegendő.

Fontos megjegyezni, hogy bár a Diameter és más modern protokollok bevezetése javított bizonyos biztonsági aspektusokon, de ezek sem tekinthetők teljes mértékben biztonságosnak. A távközlési signaling rendszerek közös jellemzője, hogy komplex, globálisan összekapcsolt infrastruktúrák, ahol a biztonság nagymértékben függ a résztvevők együttműködésétől.

Az SS7 jelenlegi helyzete tehát egy átmeneti állapotként írható le. A protokoll szerepe csökken, de nem szűnik meg, és a hozzá kapcsolódó sérülékenységek továbbra is kihasználhatók maradnak, különösen a hálózatok közötti kapcsolódási pontokon. A legfontosabb felismerés, hogy az SS7 nem egy elavult, megszűnő technológia, hanem egy tovább élő infrastruktúraelem, amely a modern hálózatok mélyebb rétegeiben működik. Ennek megfelelően a hozzá kapcsolódó kockázatok sem tűnnek el, hanem átalakulnak és részben rejtettebbé válnak. A jövő szempontjából ezért nem elegendő a technológia kivezetésére támaszkodni. Szükség van a signaling

forgalom aktív monitorozására, a forrásalapú szűrésre, valamint a nemzetközi együttműködés erősítésére, mivel a fenyegetés globális jellegű.

Összességében az SS7 sérülékenységeinek kora nem ért véget, hanem egy új szakaszba lépett, ahol a támadások kevésbé látványosak, viszont továbbra is jelentős hatással lehetnek a távközlési és digitális ökoszisztémára.



Források

Veritasium (2024) *Exposing The Flaw In Our Phone System* https://www.youtube.com/watch?v=wVyu7NB7W6Y (Letöltve: 2026. március 19.)

How2Lab (2025) *SS7 Vulnerabilities: How Hackers Exploit Telecom Networks* https://www.how2lab.com/tech/mobile-communication/ss7-vulnerabilities (Letöltve: 2026. március 19.)

Rutgers University *Signaling System 7 (SS7)* https://people.cs.rutgers.edu/~rmartin/teaching/fall04/cs552/readings/ss7.pdf (Letöltve: 2026. március 19.)

Patton Electronics. *Introduction to SS7 Signaling* https://www.patton.com/whitepapers/intro_to_ss7_tutorial.pd (Letöltve: 2026. március 19.)

Kanika Sharma, Reve Systems (2024) *What is Signaling System 7 (SS7)? A Definitive Guide* https://www.revesoft.com/blog/sms-platform/what-is-signaling-system-7/ (Letöltve: 2026. március 19.)

Simbase *Unveiling the Backbone of Mobile Connectivity: Understanding the Visitor Location Register (VLR) * https://simbase.com/iot-dictionary/visitor-location-register (Letöltve: 2026. március 19.)

Infobip *What is HLR (home location register)?* https://www.infobip.com/glossary/hlr-home-location-register (Letöltve: 2026. március 19.)

Tobias Engel, media.ccc.de (2014) *SS7: Locate. Track. Manipulate.* https://www.youtube.com/watch?v=-wu_pO5Z7Pk (Letöltve: 2026. március 19.)

Swati Khandelwal, The Hacker News (2017) *Hacker Exploit SS7 Flaws to Drain German Bank Accounts* https://thehackernews.com/2017/05/ss7-vulnerability-bank-hacking.html (Letöltve: 2026. március 19.)

Sharyn Alfonsi, CBS News (2016) *Hacking Your Phone* https://www.cbsnews.com/news/60-minutes-hacking-your-phone/ (Letöltve: 2026. március 19.)

Luana Pascu, Bitdefender (2017) *2FA fail; hackers exploit SS7 flaw to drain bank accounts* https://www.bitdefender.com/en-us/blog/hotforsecurity/2fa-fail-hackers-exploit-ss7-flaw-to-drain-bank-accounts (Letöltve: 2026. március 19.)

U.S. House of Representatives (2017) *Bank Info Security: Bank Account Hackers Used SS7 to Intercept Security Codes* https://lieu.house.gov/media-center/in-the-news/bank-info-security-bank-account-hackers-used-ss7-intercept-security-codes (Letöltve: 2026. március 19.)

Patrick Howell O'Neill, CyberScoop (2017) *Researchers steal bitcoin by exploiting SS7 vulnerabilities* https://cyberscoop.com/ss7-bitcoin-hack-positive-technologies/ (Letöltve: 2026. március 19.)

NquiringMinds (2025) *Salt Typhoon Cyberattacks Expose Major Vulnerabilities in US Digital Infrastructure* https://nquiringminds.com/cybernews/salt-typhoon-cyberattacks-expose-major-vulnerabilities-in-us-digital-infrastructure/ (Letöltve: 2026. március 19.)

ENISA (2018) *Signalling Security in Telecom SS7/Diameter/5G* https://www.enisa.europa.eu/sites/default/files/publications/Interconnect%20Security%20SS7-Diameter.pdf (Letöltve: 2026. március 19.)

NMHH (2024) *Minden érintettnek készülnie kell a 2G kivezetésére* https://nmhh.hu/cikk/254821/Minden_erintettnek_keszulnie_kell_a_2G_kivezetesere (Letöltve: 2026. március 19.)

Neural Technologies *Telecom Signaling Explained: SS7 and Diameter in 5G* https://www.neuralt.com/news-insights/how-ss7-and-diameter-enable-4g-and-5g-network-evolution (Letöltve: 2026. március 19.)

Bodnár Csaba, Villanyautósok (2023) *Egy hónap múlva teljesen megszűnik a 3G Magyarországon* https://villanyautosok.hu/2023/10/12/egy-honap-mulva-teljesen-megszunik-a-3g-magyarorszagon/ (Letöltve: 2026. március 19.)

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

Kibertámadás!
podcast

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet

titkarsag@nki.gov.hu

nki.gov.hu

+36 (1) 325 7672

2026