Vážené čtenářky, vážení čtenáři,

že se na mobilní platformy stále častěji soustřeďují hackeři, je jasné už delší dobu. Pomáhá k tomu nejen obrovská základna uživatelů, ale i jejich relativně malé povědomí o tom, jak se chránit. Tentokrát však k ohrožení přispěla i technologie, která obvykle slouží samotným mobilním operátorům.

Útočníci totiž mohou zneužít speciální typ zpráv SMS používaných operátory k poskytování internetového nastavení u telefonů se systémem Android. Tyto SMS zprávy pak hackerům mohou posloužit k zahájení důvěryhodných phishingových útoků, které mají za následek únos internetového provozu uživatele.

Podle expertů firmy Check Point u některých poskytovatelů mobilních služeb implementace standardu Open Mobile Alliance Client Provisioning (OMA CP) umožňuje posílat tyto speciální zprávy komukoliv.

OMA CP ve své původní podstatě dovoluje v nových zařízení připojujících se k sítím operátora udělat nastavení specifická pro síť, jako jsou server zpráv MMS, domovská stránka prohlížeče či internetová proxy adresa. Když taková zpráva přijde, uživatelé jsou vyzváni, aby potvrdili, že nastavení přijali. Vědci ale zjistili, že na zařízeních od společností Samsung, Huawei, LG nebo Sony (ty jediné testovali, podobné to může být i u jiných výrobců) taková indikace neexistuje.

Kvůli tomu pak lze vykonat některé velmi důvěryhodné phishingové útoky, protože velká většina uživatelů pouze přijme zprávu od svého operátora a automaticky souhlasí s instalací nastavení. Konfigurace může zahrnovat internetový proxy server, který ovládají útočníci, což přinutí uživatele, aby svůj internetový provoz směrovali přes tento proxy. Důsledky si může každý domyslet.

Samotný Android přitom neobsahuje funkce pro zpracování zpráv OMA CP, takže výrobci telefonů implementují tuto funkci do firmwaru svých zařízení sami. Z tohoto důvodu mohou existovat rozdíly ve způsobu, jakým se tyto zprávy zpracovávají včetně různého uživatelského rozhraní.

OMA CP podporuje volitelnou autentizaci pomocí kódů IMSI nebo PIN, ale Check Point zjistil, že třeba Samsung přijímá zcela neověřené zprávy. Na testovaných zařízeních Huawei, LG a Sony sice zprávy OMA CP vyžadovaly ověření, ale není těžké to obejít.

Čísla IMSI, která se používají k identifikaci účastníků v mobilních sítích, by totiž měla být teoreticky soukromá, ale nejsou. Služby na internetu poskytují zpětná vyhledávání IMSI, která mohou odhalit IMSI uživatele na základě čísla jejich mobilního telefonu, uvedli vědci. Mnoho legitimních aplikací pro Android má navíc oprávnění ke čtení IMSI zařízení, takže vytvoření nepoctivé aplikace pro shromažďování takových čísel by nevyvolávalo žádné podezření.

A i když útočník nemůže získat IMSI cílového zařízení, stále může zahájit útoky přes OMA CP pomocí možnosti ověření prostřednictvím PIN. To by však vyžadovalo poslat dvě zprávy místo jedné. První zprávou by byla klasická SMS vydávající se za operátora a sdělující uživatelům, že se chystají přijímat nastavení sítě chráněná PIN, který zvolil útočník. Druhou zprávou by byla zpráva OMA CP chráněná předtím oznámeným kódem PIN.

Samsung už problém vyřešil vydáním bezpečnostní aktualizace firmwaru, podobně jako LG, Huawei se chystá vše opravit v nových telefonech a podle Sony o chybu nejde, takže není co opravovat.

Rady, jak se vyhnout této kompromitaci, je neinstalovat nic, co vám operátor posílá, a spíše si vše nastavit sám. Operátoři navíc sami mohou zablokovat zprávy OMA CP, které nepocházejí z jejich systémů. Jinak by totiž hackerům stačil ke kompromitaci vašeho mobilu pouze velice levný USB GSM modem a běžný software.

S přáním příjemně stráveného podzimu třeba i nad stránkami nejnovějšího Security Worldu

Pavel Louda
vedoucí projektu

Obsah