**Smartfony z Androidem narażone na zaawansowane ataki phishingowe**

**Check Point Research, zajmujący się analizą zagrożeń cyberbezpieczeństwa, ujawnił lukę w telefonach firm Samsung, Huawei, LG i Sony oraz innych telefonach z systemem Android, która powoduje, że użytkownicy są narażeni na zaawansowane ataki typu phishing. Zagrożonych może być nawet połowa z 2,5 miliarda użytkowników Androida.**

Telefony z systemem Android, w których luka ta występuje korzystają z systemu komunikacji bezprzewodowej over-the-air (OTA), przez który operatorzy sieci telefonii komórkowej mogą wprowadzać ustawienia specyficzne dla danej sieci dla telefonów łączących się z siecią. Jednak Check Point Research stwierdził, że standard branżowy dla komunikacji OTA, tzn. Open Mobile Alliance Client Provisioning (OMA CP), obejmuje ograniczone metody uwierzytelniania. Hakerzy mogą wykorzystywać ten fakt do podszywania się pod operatorów sieci i do wysyłania do użytkowników fałszywych wiadomości. Wiadomości te mogą skłaniać użytkowników do akceptacji szkodliwych ustawień, które np. przekierowują ich ruch w internecie przez serwer proxy należący do hakera.

Badacze stwierdzili, że na tę formę ataku typu phishing najbardziej narażone są niektóre telefony Samsung, gdyż nie posiadają one kontroli autentyczności nadawców wiadomości OMA CP. Wystarczy, że użytkownik zaakceptuje CP, a złośliwe oprogramowanie zostaje zainstalowane na telefonie bez konieczności udowadniania przez nadawcę swojej tożsamości.

Telefony Huawei, LG i Sony posiadają pewną formę uwierzytelniania, ale do “potwierdzenia” swojej tożsamości hakerzy potrzebują jedynie międzynarodowego numeru tożsamości telefonicznej abonenta mobilnego (IMSI). Atakujący mogą uzyskać IMSI ofiary na różne sposoby, w tym tworząc złośliwą aplikację na system Android, która po zainstalowaniu odczytuje numer IMSI telefonu. Atakujący mogą także obejść konieczność posiadania numeru IMSI wysyłając użytkownikowi wiadomość tekstową, w której podszywają się pod operatora sieci i prosząc o akceptację wiadomości OMA CP chronionej kodem PIN. Jeśli użytkownik wprowadzi podany numer PIN i zaakceptuje wiadomość OMA CP, CP może zostać zainstalowany bez numeru IMSI.

- *Ze względu na popularność urządzeń z systemem Android, jest to krytyczna luka wymagająca podjęcia działań* - stwierdził Slava Makkaveev, Ekspert ds. Bezpieczeństwa w firmie Check Point Software Technologies. - *Bez silnego uwierzytelniania szkodliwy agent z łatwością może przeprowadzić atak typu phishing korzystając z systemu OTA. Gdy klient otrzyma wiadomość OMA CP, w żaden sposób nie jest w stanie upewnić się, czy pochodzi ona z zaufanego źródła. Naciśnięcie przycisku “akceptuj” może oznaczać wpuszczenie atakującego do telefonu.*

Specjaliści prowadzący badanie przedstawili jego wyniki producentom telefonów, których problem ten dotyczy, w marcu. Firma Samsung wprowadziła rozwiązanie eliminujące problem z atakami typu phishing w ramach aktualizacji bezpieczeństwa w maju (SVE-2019-14073), firma LG zrobiła to w lipcu (LVE-SMP-190006), a firma Huawei planuje wprowadzenie rozwiązań dla interfejsu użytkownika w zakresie OMA CP w następnej generacji smartfonów serii Mate i P. Firma Sony odmówiła potwierdzenia istnienia tej luki bezpieczeństwa, twierdząc, że jej telefony są zgodne ze specyfikacją OMA CP.