Nieuwe ransomware bedreigt Android-gebruikers

16 augustus 2016

Tot voor kort kwam kwaadaardige code op smartphones doordat onoplettende gebruikers een foute app hadden geïnstalleerd. Maar tegenwoordig slagen cybercriminelen erin om ransomware en andere malware op apparaten te krijgen zonder enige interactie met of actie van de gebruiker. Het bezoeken van een gemanipuleerde website is voldoende. Malware wordt dan met een zogenaamde drive-by-infectiemethode op het apparaat geïnstalleerd. G DATA's experts leggen deze infectiemethode uit in het nieuwe G DATA Mobile Malware Report, dat nu online beschikbaar is.

"Smartphones en tablets zijn erg populaire doelwitten voor cybercriminelen en de aanvallen zijn kwalitatief sterk verbeterd in het afgelopen jaar," vertelt Christian Geschkat, product manager voor mobiele oplossingen bij G DATA. "Gebruikers moeten werk maken van het beveiligen van hun smartphone met betrouwbare beveiligingssoftware. Ook is het verstandig om je besturingssysteem en alle apps op je apparaat altijd up-to-date te houden. Hiermee worden bijna alle gevaren afgewend."
Hoe werken drive-by-infecties?

Online criminelen hacken webservers en ontwikkelen speciaal geprepareerde websites. Vervolgens lokken ze gebruikers naar deze sites met behulp van spammails en advertenties. Door misbruik te maken van beveiligingslekken in het Android-besturingssysteem, kan de malware bij het bezoeken van een dergelijke site ongemerkt op het systeem van het slachtoffer komen.

9.468 nieuwe malware samples per dag

In de eerste helft van 2016 werden 1.723.265 nieuwe malware samples voor Android ontdekt. Gemiddeld komt dit neer op 9.468 nieuwe malware apps voor Android per dag of elke 9 seconden een nieuw stuk malware. Dat betekent een toename van meer dan 30% vergeleken bij de tweede helft van 2015. In de eerste helft van 2016 werd al meer nieuwe malware voor Android gevonden dan in heel 2014.