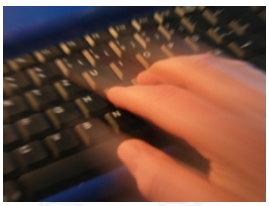

DDoS-Attacken per Smartphone: Das Angriffsszenario der Zukunft? - IT-Sicherheitsspezialist ESET wehrt Angriff von mobilem Botnet ab

Der europäische IT-Sicherheitsspezialist ESET hat in diesem Jahr erstmals einen DDoS-Angriff per Mobile-Botnet aufgedeckt. Die Täter attackierten mit infizierten gekaperten Zombie-Smartphones die internationale ESET-Webseite. Der erfolgreich abgewehrte Angriff ermöglichte es den Security-Experten, dieses neu aufkommende Angriffsszenario und die dahinterliegenden Strukturen detailliert zu analysieren.

"DDoS-Angriffe werden normalerweise immer noch über PCs oder Server realisiert. Die Zeiten ändern sich jedoch gerade. Mobile Geräte werden leistungsfähiger und ihre Internetanbindung wird schneller", erklärt Lukas Stefanko, Android Malware Researcher bei ESET. "Wenn ihr Anteil am gesamten Internetdatenverkehr im Consumer-Bereich die von Computern übertreffen wird, werden Kriminelle sie noch häufiger für ihre Angriffe verwenden."

Fake-App verwandelt Handys in Zombie-Smartphones

ESETs Analysen ergaben, dass die DDoS-Attacke mithilfe einer App namens "Updates for Android" erfolgte, die bis Januar 2020 mehr als 50.000 Downloads verzeichnete. Um der Anwendung einen legitimen Touch zu verleihen und diese zu bewerben, stellten die Angreifer eine eigens dafür eingerichtete Webseite online.

Zudem setzten die Angreifer auf ein zweistufiges Vorgehen: In der ursprünglichen Version fehlte der Anwendung die bösartige Funktionalität. Das erklärt auch, warum es die App in den Play-Store geschafft hatte. Erst zwei Wochen vor dem Angriff wurde die Malware per Update ausgespielt und in die installierte App implementiert.

Analog zu einem PC-Botnet ermöglichte der Schadcode, jedes infizierte Smartphone individuell anzusteuern. Die für einen DDoS-Angriff notwendigen Befehle verteilten die Kriminellen dann per Command & Control Konsole. Im Sekundentakt riefen so die ferngesteuerten Zombie-Smartphones die anvisierten Webseiten auf. An der durchgeführten Attacke, die circa sieben Stunden andauerte, waren etwa zehn Prozent der infizierten Geräte beteiligt.

Angreifer legen eigenes Botnet ungewollt offen

Die Ziele des Angriffs bleiben indes im Dunkeln. "Wir können nur spekulieren", sagt Stefanko. "Unter dem Strich war der einzige Effekt des Angriffs, dass die Angreifer ihr Botnetz offengelegt haben. Praktisch existiert dieses DDoS-Tool nicht mehr." Die entsprechende App wurde an Google gemeldet und umgehend aus dem Play Store entfernt. Die Anwendung kann allerdings noch aus inoffiziellen Quellen bezogen werden. ESET-Sicherheitslösungen erkennen den Trojaner als Trojan.Android/Hiddad.AJN.

"Unsere Erkennungssysteme haben wir umgehend modifiziert und weiter verbessert", so Stefanko. "Aufgrund unserer Erfahrungen besteht nun die Möglichkeit, dass wir ähnliche Trojaner an Google melden können." Einige der Verbesserungen wurden bereits in die Technologien implementiert, die innerhalb von Googles App Defense Alliance zum Einsatz kommen, zu der auch ESET gehört.