tagesschau

EXKLUSIV Spähsoftware

Wie "Pegasus" aufs Handy kommt

Stand: 18.07.2021 18:01 Uhr

Die Software "Pegasus" der israelischen Firma NSO ist eines der mächtigsten Überwachungswerkzeuge der Welt. Das Programm kann heimlich auf Handys installiert werden, ohne dass das Opfer etwas davon ahnt.

Den Namen "Pegasus" habe man gewählt, weil die Software ein trojanisches Pferd sei, und zwar eines mit Flügeln, das direkt auf das Handy fliegt - so erzählte es Shalev Hulio, Chef der israelischen Firma NSO, einst in einem Interview. Es ist kein physischer Zugriff auf das Gerät notwendig. Das Spionageprogramm kann aus der Ferne installiert werden, klammheimlich, ohne dass es die Zielperson mitbekommt - und sogar ohne dass das Opfer irgendetwas tun muss.

"Vermeiden Sie unnötige Risiken: Sie müssen sich zu keiner Zeit in der Nähe des Ziels oder des Geräts aufhalten", hieß es vor einigen Jahren in der Broschüre von NSO. Der geflügelte Trojaner "Pegasus" ist der Verkaufsschlager der Firma. Weltweit nutzen Geheimdienste und Polizeibehörden das Programm, um damit umfassend und unbemerkt Zielpersonen auszuspähen.

Haben es die Angreifer geschafft, "Pegasus" auf ein fremdes Handy aufzuspielen, haben sie die komplette Kontrolle über das Gerät. Sie können sämtliche Daten vom Handy kopieren oder etwa heimlich das Mikro oder die Kamera aktivieren und sogar verschlüsselte Nachrichten lesen. Ein wesentlicher Grund für die Beliebtheit der umstrittenen Software dürfte aber die Tatsache sein, dass "Pegasus" vergleichsweise einfach auf das Handy aufgebracht werden und dies kaum verhindert werden kann.

"Es gibt keine wirksame Möglichkeit für einen Benutzer, gegen diese Art von Angriffen vorzugehen", sagt der IT-Sicherheitsexperte Claudio Guarnieri von Amnesty

International. NSO bietet seinen Kunden verschiedene Möglichkeiten an, wie Handys von Zielpersonen infiziert werden können - je nach Gerätetyp oder Betriebssystem können sie mehr oder weniger aufwändig sein.

Mit und ohne Klick

Die "klassische" Methode, mit der "Pegasus" auf ein Handy gelangt, funktioniert mithilfe einer fingierten Nachricht. Die Zielperson wird dazu verleitet, einen Link oder eine Datei anzuklicken, und startet so den Download unwissentlich selbst, etwa über eine Textnachricht oder eine E-Mail. Sobald man darauf klickt, installiert sich der Trojaner. Für seine Kunden stellt NSO dazu eine Art Baukasten zur Verfügung, mit der fingierte E-Mails oder Textnachrichten möglichst realitätsnah und plausibel gestaltet werden können.

Die Firma NSO hat jedoch noch einen anderen, beängstigenden Weg gefunden, wie "Pegasus" unbemerkt auf ein Mobiltelefon installiert werden kann - einen Weg, gegen den die Opfer komplett wehrlos sind. Es ist kein Klick mehr nötig. Das Handy muss nur angeschaltet und mit dem Netz verbunden sein. Der Angreifer verschickt eine Nachricht, die nicht auf dem Handy angezeigt wird. Sie bringt das Gerät dazu, die Spionagesoftware zu laden und zu installieren.

Sicherheitsexperten von Amnesty International fanden auf mehreren, auch aktuellen iPhones Spuren der "Pegasus"-Software, die anscheinend auf diesem Weg auf das Gerät gelangt war. Ihrer Analyse zufolge kann das Spähprogramm unter Ausnutzung des internetbasierten Dienstes iMessage aus der Ferne installiert werden. Die NSO-Kunden müssen dafür nur die Telefonnummer der Zielperson eingeben. Das Smartphone empfängt dann automatisch Daten, die aus dem Internet heruntergeladen werden. In diesem Fall ist es der Trojaner "Pegasus".

Software-Schwachstellen ausgenutzt

Ob diese Methode in ähnlicher Form auch bei Android-Geräten funktioniert, konnten die Sicherheitsexperten von Amnesty International nicht verifizieren. Die Organisation hat Apple auf die Sicherheitslücke aufmerksam gemacht. Die Firma selbst teilte auf Anfrage mit, diese Art von Attacken würde die überwältigende Mehrheit der Nutzer nicht bedrohen. Sie arbeite aber natürlich durchgängig daran, die Sicherheit aller Kunden zu gewährleisten.

Allerdings ist klar: Hacker weltweit versuchen stetig neue Lücken in den Systemen zu finden - und verkaufen sie teils für viel Geld an Geheimdienste oder Firmen wie NSO. Die Hersteller der Geräte laufen in diesem Rennen meist hinterher.

IT-Forscher von Citizen Lab an der Universität Toronto haben sich angesehen, wie frühere Versionen von "Pegasus" funktionierten. Dabei stellten sie fest, dass das Programm eine Kette von Software-Schwachstellen, sogenannte Exploits, in Betriebssystemen wie iOS oder Android ausnutzt. Darunter waren auch für Hacker besonders nützliche Schwachstellen, sogenannte "Zero-Day Exploits". Dabei handelt es sich um Sicherheitslücken, die quasi sofort für Angriffe ausgenutzt werden, bevor die Hersteller Gegenmaßnahmen ergriffen haben. Teilweise sollen von dem NSO-Trojaner

drei solcher "Zero-Days" nacheinander verwendet worden sein, um Zugriff auf ein Telefon zu bekommen.

Verschiedene Wege zum Smartphone

Eine weitere Möglichkeit, Geräte mit dem "Pegasus"-Trojaner zu infizieren, funktioniert über ein WLAN-Netzwerk oder das lokale Mobilfunknetz. Dazu muss sich das Handy in einen manipulierten Sendemast oder einen Router einloggen. Die Firma NSO verkauft etwa Geräte, die vorgeben, ein Mobilfunkmast zu sein - IMSI-Catcher. Ihr Signal ist stärker als das aller umliegenden Masten, sodass sich das Handy damit verbindet. Der Angreifer schaltet sich also sozusagen zwischen das Mobiltelefon und einen echten Sendemast. Wenn dann der Nutzer eine Website - etwa die Google-Seite - aufruft, wird der Datenstrom in Sekundenbruchteilen auf Server von NSO umgeleitet. Auf das Handy wird über das Netzwerk die Überwachungssoftware aufgespielt.

Einmal auf dem Mobiltelefon installiert, kann "Pegasus" nicht nur Überwachungsmaßnahmen ausführen oder die gespeicherten Daten durchsuchen. Die Software ist offenbar auch in der Lage, wichtige Sicherheitsupdates des Herstellers zu unterdrücken, mit denen etwa Schwachstellen im Betriebssystem geschlossen werden könnten. So stellt der Trojaner sicher, dass er über längere Zeit auf dem Handy funktionieren kann.

Der Hersteller gibt an, dass er seine Technologie nur an überprüfte staatliche Stellen verkaufe. Und zwar ausschließlich zum Zweck der Terrorismus- und Kriminalitätsbekämpfung. Dafür werde die Software weltweit "tagtäglich" eingesetzt, wie NSO mitteilt, man sei auf einer "lebensrettenden Mission".

An der Recherche zu diesem Text hat Hannes Munzinger mitgearbeitet.

MEHR ZUM THEMA

EXKLUSIV *18.07.2021 - 18:01 Uhr*
"Pegasus-Projekt"
Journalisten in Ungarn überwacht

Zurück zur Startseite