

Staatstrojaner

Quellen-TKÜ

Die Quellen-TKÜ ist quasi eine Online-Durchsuchung "light". Dabei wird zwar die selbe Software wie bei der Online-Durchsuchung eingesetzt, allerdings soll hier nur der live ein- und ausgehende Datenverkehr mitgeschnitten werden. Das Durchforsten von gespeicherten Inhalten ist hierbei nicht erlaubt und angeblich bei eingesetzter Software - durch entsprechende Modifikationen - auch nicht möglich.

Entstanden ist dieses Konstrukt, weil Online-Durchsuchungen einen sehr extremen Eingriff in die Privatsphäre sind, werden sie manchmal von Richter*innen auf Grund von "Unverhältnismäßigkeit" nicht genehmigt. E2E-Verschlüsselung verhindert aber eine effektive TKÜ bei Serviceanbietern. Also wird diese "abgespeckte" Schadsoftware eingesetzt, da sie eher richterlich genehmigt wird. So können sämtliche Up- und Downloads (hier sind auch Chat-Nachrichten mit gemeint) jeweils vor der Verschlüsselung, oder nach der Entschlüsselung, auf den Endgeräten mitgelesen werden.

Statistiken Quellen-TKÜ

[Hier](#) findet ihr mehr Details zu der Statistik der **Quellen-TKÜ**

Online-Durchsuchung

Wenn von Staatstrojanern die Rede ist, dann ist meist die Online-Durchsuchung gemeint. Hierbei werden betroffene Geräte mit Schadsoftware infiziert, sodass die Angreifer (i.d.R. Cops) vollen Zugriff auf das Gerät haben. Das bedeutet sie können sowohl live mitverfolgen was gerade auf dem Gerät gemacht wird, Kameras und Mikro's anschalten, Standorte abrufen, als auch gespeicherte Inhalte wie Nachrichten, Bilder, Kontakte, Kalender, Notizen einsehen und ausleiten. Die Vorteile davon liegen auf der Hand. Betroffene bemerken die Maßnahmen überhaupt nicht. Geräte müssen eventuell noch nicht einmal beschlagnahmt werden und Festplattenverschlüsselung wird somit "nutzlos" gemacht.

Statistiken Online-Durchsuchung

Statistiken Online-Durchsuchung

Hier findet ihr mehr Details zu den obigen beiden Statistiken zur **Onlinedurchsuchung**

Es ist daher mit Blick auf Online-Durchsuchung und Quellen-TKÜ zu beachten, dass die eingesetzten Softwares aus unterschiedlichen Quellen stammen. Der berühmte Staatstrojaner Pegasus der NSO-Group, oder Predator von Intellexa erfordern extrem teure Lizenzkosten.

Aus von der New York Times geleakten Predator Files ist beispielsweise zu erkennen, dass eine Lizenz zum Infizieren von 20 iOS oder Android Geräten, mit 12 monatiger Garantie, 13,6 Mio € (Euro) kosten soll. Die zu Verfügung gestellte Schadsoftware ist dabei "nur" eine 1-click-solution, bei der die Zielpersonen noch selber auf irgendeinen Link klicken müssen.

Einen Reboot von infizierten iPhones überlebt der Trojaner nicht, dafür müssen nochmal 2,4 Mio € gezahlt werden. Für Sim-Karten aus anderen Ländern, als dem agierenden, müssen 3,5 Mio € extra fließen.

Hier lässt sich also feststellen, dass eine solche Lösung sehr teuer ist. Allerdings haben deutsche (und andere) Behörden auch schon eigene Staatstrojaner gebaut, von denen aber zumindest bisher nicht bekannt wurde, dass sie remote infizieren können, sondern über Hardwarezugriff verfügen müssen.

Daher sollten Geräte auch physisch geschützt werden, denn die Behörden dürfen unter Umständen, wie bei der Wohnraumüberwachung auch, in eure Wohnung einbrechen und auf eurer Hardware heimlich Schadsoftware installieren. Um dem vorzubeugen ist es ratsam, Teile die zum Öffnen der Hardware bewegt werden müssen, so zu bearbeiten, dass ihr einen solchen Zugriff sofort bemerkt.

Quellen-TKÜ+

Die Quellen-TKÜ+ stellt lediglich weiteres ein juristisches Konstrukt dar, auf das wir aber hier nicht eingehen wollen, da es bei einem Staatstrojaner bleibt. Falls ihr mehr darüber lesen wollt, gibt es dazu eine Stellungnahme des CCC.

Zitat aus der Stellungnahme des CCC

Die nur rechtlich definierte Trennung zwischen den „Payloads“ der heimlichen Schadsoftware, die nunmehr drei Trojaner-Varianten („Quellen-TKÜ“, „Quellen-TKÜ+“ und „Online-Durchsuchung“) hervorgebracht hat, ist technisch nicht begründbar [...]

Durch die oben skizzierten Infektionswege und den zwingend damit einhergehenden tiefen Veränderungen in den Sicherheitsmechanismen der angegriffenen Systeme wird deutlich, dass eine technische Abgrenzung zwischen dem Staatstrojaner zur Festplatten-Durchsuchung („Online-Durchsuchung“) und dem Trojaner zum Abhören der laufenden Kommunikation („Quellen-TKÜ“) sowie der mittlerweile dritten Trojaner-Variante („Quellen-TKÜ+“ oder „Kleine

Online-Durchsuchung“), die auch gespeicherte Inhalte und Umstände der Kommunikation erfassen darf, in der Praxis bei ehrlicher Betrachtung weder zuverlässig zu gewährleisten noch überhaupt klar zu umreißen ist. Die „technischen Vorkehrungen“, die alle drei Staatstrojaner-Varianten unterscheiden sollen, könnte man zwar zu implementieren versuchen, allerdings scheitert offenbar das BKA seit mehr als einem Jahrzehnt daran, Trojaner-Varianten zu entwickeln oder zu kaufen, die alle grundrechtlich gebotenen Vorgaben sicher erfüllen.

Letztlich bleibt die Unterscheidung aller drei Trojaner-Varianten eine juristische und zudem theoretische, die mit den Realitäten der Trojaner- Branche und mit den technischen Notwendigkeiten beim erfolgreichen Infizieren eines informationstechnischen Geräts nicht zusammengehen.

Hierzu gab es auch einen früheren Fall, bei dem der CCC 2011 einen Staatstrojaner zerlegt hat und dabei zeigte, dass dieser natürlich technisch alles mit dem System machen konnte. Daraufhin, hat das Bundesverfassungsgericht das Gesetz 2016 auch für teilweise Verfassungswidrig erklärt.

Version #1

Erstellt: 14 Januar 2025 18:52:40 von ESC-IT Migration Bot

Zuletzt aktualisiert: 14 Januar 2025 18:52:40 von ESC-IT Migration Bot