Kfz-Diebstahl: Ein OBD-Stecker mit Ringantenne ermöglicht eine Kommunikation zwischen der Bordelektronik und dem Smartphone. Über eine App werden Informationen ausgelesen, die für das Anlernen eines Schlüsselrohlings notwendig sind.

Diebstahl per Smartphone

Die Experten der Kfz-Forensik des Bundeskriminalamtes sind hinter einen neuen Diebstahl-Modus gekommen: Mittels App und Internet wird die Elektronik des Autos überlistet und ein Kfz-Schlüsselrohling „angelernt", mit dem das Auto entwendet wird.

Am Abend noch das Auto gut versperrt abgestellt, doch am nächsten Morgen fehlt jede Spur des Wagens. Moderne Autos haben immer mehr elektronische Komponenten, die nicht nur mit dem Lenker, sondern auch mit der Außenwelt durch beispielsweise eine WLAN-, Internet- oder Bluetooth-Verbindung kommunizieren können.

Die fortschreitende Technisierung hat jedoch nicht nur positive Seiten. Längst sind Kriminelle in der Lage, das Signal eines Transponderschlüssels abzufangen, sich Zugang zum Fahrzeug zu verschaffen und den Rohling eines Fahrzeugschlüssels zu programmieren – oder auch die elektronische Wegfahrsperre zu deaktivieren. Der Täter kann sich innerhalb weniger Minuten Zugang zum Fahrzeug verschaffen – mit oder ohne Beschädigung – und ist dann auch in der Lage, es zu stehlen. Die Experten der Kfz-Forensik des Bundeskriminalamtes haben eine neue Diebstahlsmethode identifiziert: Das Stehlen eines Autos mittels App am Smartphone.

Key-Learning as a Service (KlaaS). Die Experten der Kfz-Forensik im *Cybercrime-Competence-Center (C4)* des Bundeskriminalamtes haben eine neue Kfz-Diebstahlsmethode identifiziert: Das Stehlen eines Autos mittels App am Smartphone.

Bei der Festnahme von Kfz-Dieben in Salzburg wurden Mitarbeiter der Kfz-Forensik des Bundeskriminalamtes hinzugezogen, um das sichergestellte Kraftfahrzeug zu untersuchen. Nachdem die Experten nicht nur die elektronischen Beweismittel des Kraftfahrzeuges ausgewertet, sondern auch das sichergestellte Smartphone eines Tatverdächtigen analysiert hatten, stießen sie auf zwei ihnen noch unbekannte Apps, die sich später als Key-Learning-Apps herausstellten.

Bei der Untersuchung ergab sich für die Ermittler eine neue Vorgehensweise: Damit der Täter einen neuen Fahrzeugschlüssel anlernen kann, muss er zunächst in das Fahrzeuginnere gelangen, um an die OBD-Diagnose-Schnittstelle (zumeist im Fußraum des Lenkerplatzes) zu gelangen. Dort wird der OBD-Stecker mit Ringantenne eingebracht, wodurch eine Kommunikation mit der Bordelektronik ermöglicht wird. Anschließend kommt das Smartphone zum Einsatz: Mittels Bluetooth wird eine Verbindung zum OBD-Gerät

KRIMINALPRÄVENTION

Sicherheitstipps

- Verwenden Sie einen OBD-Saver. Dieser schützt den OBD-Stecker und kann einen unbefugten Zugriff auf die Elektronik und Steuergeräte des Autos verhindern.
- Durch einen individuellen Stromunterbrecher, der im Fahrgastraum versteckt eingebaut wird, können Sie die Elektrik (Zündspule, Anlasser, Benzinpumpe) auf Knopfdruck unterbrechen, bevor Sie aussteigen. Der Motor lässt sich dadurch nicht starten. Kfz-Dieben fehlt meist die Zeit, um nach der Stromtaste zu suchen.
- Lassen Sie sich von einer Fachwerkstätte eine Alarmanlage in Ihr Auto einbauen. Schalten Sie diese nach dem Verlassen des Fahrzeuges immer ein.
- Durch ein Ortungssystem kann der Standort eines gestohlenen Fahrzeuges abgerufen werden. Dadurch steigt die Chance auf die Auffindung.
- Achten Sie beim Versperren des Autos darauf, dass es auch wirklich versperrt ist. Diebe können mit Störsendern das Schließsignal des Funkschlüssels unterbinden.
- Bewahren Sie den Kfz-Schlüssel nicht direkt im Eingangsbereich des Hauses auf und verwenden Sie einen Keyless-Go-Schutz. Dieser wirkt wie ein faradayscher Käfig, wodurch das Signal des Schlüssels nicht abgefangen und bis zum Auto verstärkt werden kann.

und über das Mobilfunknetz ins Internet hergestellt. Wenn der Nutzer die App aufruft, erscheint eine grafische Oberfläche am Display des Smartphones. Über die Diagnoseschnittstelle (OBD) können Informationen zu Steuergeräten und Fehlern eines Kraftfahrzeugs ausgelesen werden.

Neu programmierter Schlüssel. Sobald eine Verbindung ins Internet und zum OBD-Gerät besteht, kann der Anlernprozess gestartet werden. Dazu werden vom Fahrzeug und der elektronischen Wegfahrsperre jene Parameter und Informationen ausgelesen und abgerufen, die für das Anlernen eines neuen Schlüssels notwendig sind. All diese Daten werden via App über das Internet an einen Server übertragen. Auf diesem Server wird dann anhand der übermittelten Fahrzeuginformationen eine Schlüssel-ID mit Sicherheitsinformationen errechnet, zurück an das Smartphone geschickt und mittels App verarbeitet.

Mit der Funktion „Lost all Keys“ können sämtliche Schlüssel-IDs gelöscht werden, wodurch der Schlüssel des eigentlichen Kfz-Besitzers unbrauchbar wird. Nachdem diese Funktion ausgeführt wurde, kann der Fremdschlüssel mit den Informationen, die vom Server generiert wurden, angelernt werden. Somit ist die ursprüngliche elektronische Wegfahrsperre außer Kraft gesetzt und neu programmiert, wodurch der Täter das Auto ohne Beschädigungen zu verursachen, entwenden kann.

Ausgetrickste Elektronik. Wie die Vorgehensweise der Diebe zeigt, ist die Elektronik der Kraftfahrzeuge alles andere als unüberwindbar. Viele Eingriffe und Manipulationen am Fahrzeug oder der Steuergeräte werden aufgezeichnet, was nicht nur für die Rekonstruktion von Unfällen hilfreich ist, sondern auch bei der Ausforschung der Täter.

Die elektronischen Komponenten eines Fahrzeuges sind oftmals nicht ausreichend vor einer missbräuchlichen Verwendung geschützt, denn OBD-Diagnose- und Programmiergeräte sind frei im Handel erhältlich, ebenso Schlüsselrohlinge. Durch einfache Maßnahmen kann das Risiko, Opfer eines Kraftfahrzeug-Diebstahls zu werden, minimiert werden.

Romana Tofan