"Bezpečností díra" děsí majitele vozů Fiat Ducato a Iveco Daily

S trochou nadsázky lze konstatovat, že byla doba ledová, bronzová a dnes je doba softwarová. I obytné vozy totiž lze vykrást beze stopy, počítačem. Názorná ukázka před zraky diváků na výstavě Caravaning Brno 2017 demonstrovala jednoduchost, s jakou je možné dostat se do všech vozů Fiat Ducato od roku 2006 až doposud, pokud je odemykáte originálním dálkovým ovládáním v klíčku...

Co přesně se stalo? Objevují se případy, kdy byly vozy vykradeny bez zjevného poškození zámků či oken, a dlouho se nevědělo, jak k tomu dochází. Firma Thitronik, zabývající se zabezpečením vozů plynovými detektory i speciálním zabezpečením na míru konstruovaným pro obytné vozy a karavany, byla první, kdo již na výstavě Caravan salon Düsseldorf vysvětlila, jak je to možné.

Nejdříve ale trochu teorie. V principu existují dva základní způsoby kódování dálkového ovládání vozu. Pevným a plovoucím kódem. Pevný kód je velmi jednoduché prolomit takzvaným opakováním signálu „replay attack" nebo vysíláním velkého množství náhodných kódů na příslušné frekvenci, a tak se už dlouhé roky u automobilek prakticky nepoužívá. Plovoucí kód je na prolomení složitý, protože existuje algoritmus, na základě kterého se kód mezi ovladačem a autem pořád mění, a tak je zbytečné ho načítat, protože podruhé již nefunguje. No a Fiat ve vozech Ducato bohužel používá právě kód pevný. Jednoduchým modulem na principu rádia (za pár korun z internetu) si nahrajete kód klíčku v okamžiku, kdy vozidlo odemykáte, když to situace umožní, tak i kód zamykací, aby bylo možné vozidlo i zamknout, a tím si vlastně vytvoříte další klíč, aniž by o tom někdo věděl. Zloděj tedy v klidu sedí někde na kraji kempu či parkoviště s mobilem, ke kterému má připojený malý modul rádia, a čeká, až stisknete ovladač. Pak už si auto odemkne, kdy on sám chce.

Obrovskou nevýhodou takového "digitálního" vloupání je, že je naprosto nezjistitelné a beze stopy. Klasická situace - nikdo nic neviděl, nikdo nic neslyšel, pojišťovna vám zřejmě také nic nedá (není nic poškozeno, což je většinou podmínka plnění), a navíc se o vloupání pravděpodobně dozvíte až s odstupem času, protože když k vozu přijdete, nic „divného" nezpozorujete až do doby, kdy začnete hledat chybějící věci. Podívejte se na youtube video z přiloženého QR kódu, kde je na příkladu krásně vidět, jak to v praxi probíhá.

Jak se účinně bránit

Způsobů, jak se proti replay attack účinně bránit, je hned několik. Postačí, když budete odemykat klíčkem a ne dálkovým ovladačem. Nebo, pokud již máte namontovaný autoalarm s extra neoriginální klíčenkou-přívěškem, používejte ten a budete s největší pravděpodobností chráněni. Pozor ale na alarmy, které se ovládají originální klíčenkou Fiat. Alarm je instalovaný až za napadnutelnou část, tedy za klíčkem, a tak i tento alarm lze deaktivovat opakováním signálu.

Přesně to se také stalo po přednášce na výstavě Caravaning Brno, kde se o tomto tématu také mluvilo. Jeden z diváků nevěřil, že jeho alarm lze takto otevřít. Alarm byl kvalitní a v pořádku, ale ovládal se právě dálkovým ovladačem v klíčku Fiat. Chvilku po přednášce se tak hlouček lidí přesunul k vozu tohoto pána, a… vozidlo bylo způsobem replay attack během pár vteřin otevřeno, beze stopy, bez alarmu.

Velmi povedené řešení obrany prodává Thitronik. Řeší ty z vás, kteří nechcete další přívěšek na klíče. Produkt safe.lock nahrazuje originální destičku s plošnými spoji (vysílač) v klíčku za novou s plovoucím kódem a dále obsahuje jednotku s přijímačem do vozu. Po instalaci tedy vše vypadá jako originál, ale jste chráněni plovoucím kódem. Pro ty náročnější z vás je možné systém Thitronik rozšířit o hlídání úniku propan butanu, pokusu o uspání K.O. plynem, hlídáním oken a dveří senzory, či speciálním „alarmovým lankem" můžete hlídat například kola v držáku za vozem.

Nejspíš zde není důvod panikařit nebo opouštět vůz v obavách, ale určitě je dobré o tom vědět a umět se účinně bránit. Navíc, když i opravdu dobré řešení není drahé.

Jan VOGL, Zenec