ALISON

Za šesť mesiacov roka 2019 došlo k väčšiemu počtu kybernetických útokov v automobilovom segmente než za celý minulý rok. Vzniká úplne nový typ kriminality.

Na cestách rastie počet vozidiel pripojených do siete a v doprave sa presadzujú inteligentné služby, čo však prináša aj rast nahlásených prípadov kybernetickej kriminality. Mediálnym hitom sa koncom leta stalo opakované heknutie Tesly S.

V prvom polroku 2019 bolo hlásených 82 incidentov, čo predstavuje takmer trojnásobok oproti rovnakému obdobiu predchádzajúceho roka (32 incidentov). Pri tejto intenzite možno v druhej polovici roku 2019 očakávať rastúci počet incidentov, takže v porovnaní s rokom 2018 bude tohtoročná bilancia dvoj- až trojnásobná.

- 65 % všetkých incidentov typu black-hat viedlo k škodám na majetku, ku krádežiam, k poškodeniu dobrého mena a ohrozeniu účastníkov cestnej premávky
- 47 % prípadov znamenalo prekonanie systémov bezkľúčového otvárania automobilov
- 18 % tvorili útoky na servery a ich cieľom boli celé vozové parky
- 8 % prípadov boli prelomy na mobilnej platforme
- 6,5 % incidentov boli prelomy palubnej diagnostiky vozidiel (OBD)

Analýza spoločnosti Upstream opakovane upozorňuje, že v prípade vozidiel pripojených do siete je jedným z najčastejších vektorov útoku ich systém bezkľúčového odomykania.

Experti, ktorí vytvorili kópiu diaľkového kľúča od Tesly Model S, svoj kúsok zopakovali. Podarilo sa im prelomiť aj náhradný systém a netrvalo to ani rok.

V roku 2018 bezpečnostní špecialisti z belgickej Katolíckej univerzity v Leuvene odhalili závažný nedostatok zabezpečenia automobilov Tesla. Stačilo im bežné vysielacie zariadenie na to, aby prelomili šifrovanie diaľkového otvárania Modelu S a za niekoľko sekúnd vytvorili kópiu kľúča. Kópiou sa im podarilo auto odomknúť a odísť s ním bez toho, aby sa dotkli kľúča skutočného majiteľa. Spoločnosť Tesla vzápätí vyrobila novú verziu svojho diaľkového kľúča, ktorá mala bezpečnostnú trhlinu zaceliť, a výskumníkom poslala sumu 10 000 USD.

Prešiel necelý rok a výskumník Lennert Wouters na konferencii o kryptografickom hardvéri a zabudovaných systémoch v Atlante oznámil, že jeho tím odhalil metódu na prekonanie šifrovania diaľkového kľúča Modelu S znova. Zraniteľnosť postihuje aj nové kľúče.

Znova by tak bolo možné vytvoriť kópiu kľúča a s vozidlom odísť bez vedomia jeho majiteľa. Nový útok je účinný na menšiu vzdialenosť a trvá o niekoľko sekúnd dlhšie než predchádzajúca metóda. Vedci tentoraz nevykonali ukážku celého útoku tak ako minulý rok – len dokázali jeho reálnosť. Tesla

priznala riziko zneužitia metódy zlodejmi a nasadzuje softvérovú opravu, ktorá sa cez internet zasiela do vozidiel.

Zraniteľnosť diaľkového kľúča spočíva v chybnej konfigurácii, čím sa výrazne skracuje čas potrebný na prelomenie šifrovanej komunikácie. V rámci zosilnenia ochrany 40-bitové šifrovanie z predchádzajúcej verzie bolo nahradené výrazne bezpečnejším 80-bitovým šifrovaním v nových kľúčoch. Hoci takéto zdvojnásobenie dĺžky šifrovacieho kľúča za normálnych okolností sťaží prelomenie šifry až biliónnásobne, kvôli chybnej realizácii môžu hekeri problém redukovať na prelomenie dvoch 40-bitových kľúčov.

Útok z roku 2018 vyžadoval tabuľku niekoľkých miliárd vopred vypočítaných kľúčov na základe všetkých možných kódov, ktoré mohol diaľkový kľúč odoslať. Nový útok vyžaduje vytvorenie dvoch takýchto tabuliek. Výpočet každej z nich trvá niekoľko týždňov a Wouters preto už druhú tabuľku nevytváral. Tesla mu však napriek tomu v apríli tohto roku udelila odmenu za odhalenie chyby vo výške 5 000 USD.

V roku 2018, tesne predtým, ako vedci zverejnili prelomenie pôvodného diaľkového kľúča, zaviedla Tesla funkciu, ktorá umožnila vodičom podmieniť naštartovanie vozidla zadaním PIN kódu. Náprava chyby však vyžadovala inštalovanie bezpečnostnej aktualizácie a zároveň kúpu nového diaľkového kľúča. Toho roku Tesla zasiela do modulov bezkľúčového otvárania vo vozidlách bezpečnostnú aktualizáciu, no modul už automaticky a bezdrôtovo aktualizuje aj samotný kľúč a mení jeho konfiguráciu bezdotykovo.