Trend Micron uusi tutkimus analysoi kyberhyökkäysiä tieliikenteessä ja kuinka välttyä niiltä

2021-02-16 15:00 EET

Älyautojen tekniikka on haavoittuvainen kyberhyökkäyksille

Helsinki, 16. helmikuuta 2021 – Trend Micro kertoo uudessa tutkimuksessaan älyautojen turvallisuudesta ja kuvaa tilanteita, joissa kuljettajat voivat joutua omaa ja sivullisten turvallisuutta vaarantavien hyökkäysten kohteiksi.

Raportti paljastaa tutkittujen kyberuhkien laajuuden. Tutkijat arvioivat 29 kpl DREAD[1] -uhkamallin mukaista hyökkäysskenaariota kvalitatiivisessa riskianalyysissä. Ajoneuvoja vastaan voidaan hyökätä joko etänä ja/tai

paikallisesti. Esimerkiksi:

- Tietoliikennetelematiikkaan (ITS) kohdistuvat palvelunestohyökkäykset muodostavat suuren riskin, koska ne voivat ylikuormittaa älyautojen viestintäjärjestelmät.
- Älyautojen riskialttiit ja haavoittuvat järjestelmät ovat helppoja havaita, mikä lisää niiden väärinkäytön riskiä.
- Yli 17 % kaikista tutkituista hyökkäysvektoreista edustivat korkeaa riskitasoa. Niiden hyödyntäminen ei vaadi juurikaan ymmärrystä älyautojen tekniikasta, joten taitamatonkin hyökkääjä voi pystyä hyödyntämään niiden heikkouksia.

"Tutkimuksemme osoittaa, että hyökkääjillä on runsaasti mahdollisuuksia älyautojen teknologian väärinkäyttämiseen", kertoo Kalle Salminen, Trend Micron kyberturva-asiantuntija. "Onneksi mahdollisuudet hyökkäysten toteuttamiseen ovat kuitenkin rajallisia, eivätkä verkkorikolliset ole vielä keksineet hyviä keinoja niillä rahastamiseen.YK:n tuore asetus painottaa ITS-järjestelmien kyberturvallisuutta. Lisäksi työn alla on niitä koskeva ISO-standardi. Alan sidosryhmien täytyykin tunnistaa sitä koskevat kyberuhkat ja varautua niiden torjuntaan samalla, kun kaasutamme yhä vauhdikkaammin kohti tietoverkon kautta toimivia, autonomisia älyautoja." [2]

Vuosien 2018-2022 välillä toimitetaan maailmanlaajuisesti arviolta yli 125 miljoonaa henkilöautoa, jotka on kytketty valmiiksi tietoverkkoihin. Kehitteillä on kasvavassa määrin täysin itsenäisesti ajavia kulkuneuvoja. Tämä kehityskulku johtaa teiden päällä liikkuvaan monimutkaiseen digitaaliseen ekosysteemiin, johon kuuluu pilvipalveluja, esineiden internet, 5G ja muita avainteknologioita. Se tuo mukanaan myös uuden ja valtavan hyökkäyspinta-alan, joka sisältää mahdollisesti jopa miljoonia päätelaitteita ja loppukäyttäjiä.

Raportti varoittaa että alan kehittyessä verkkorikollisille, haktivisteille, terroristille, valtiollisille organisaatioille, sisäpiirin toimijoille ja häikäilemättömille opportunisteille avautuu monia mahdollisuuksia sekä uusiin ansaintatapoihin että sabotaaseihin. Tutkittujen 29:n hyökkäysvektorin kautta toteutettujen kyberhyökkäysten onnistumismahdollisuudet arvioitiin keskitasoiseksi. SaaS-pohjaisten sovellusten upottaminen kulkuneuvojen sähkö- ja elektroniikkajärjestelmiin on kuitenkin omiaan kasvattamaan onnistuneen hyökkäyksen vaaraa, etenkin kun verkkorikolliset kehittävät uusia ansaintatapoja.

Tutkimuksessa hahmoteltujen riskien lieventämiseksi älyautojen tietoturva on suunniteltava ottamaan huomioon kaikki kriittiset kohdat koko tiedontoimitusketjun turvaamiseksi. Trend Micro suosittelee seuraavia toimintatapoja älyautojen suojaamiseksi:

- Oleta, että järjestelmään tunkeudutaan joka tapauksessa. Varaudu siihen tehokkailla hälytysjärjestelmillä, jotta voit eristää tunkeutujan ja minimoida vahingot.
- Suojaa tiedontoimitusketju kokonaisuudessaan autojen sähkö- ja elektroniikkajärjestelmissä, verkkopalveluissa, taustasovelluspalvelimissa ja autojen operaattorikeskuksissa.
- Hyödynnä opittua vahvistaaksesi suojausjärjestelmiä ja estämään uusia hyökkäyksiä.
- Käyttökelpoisia suojaustekniikoita ovat muun muassa palomuurit, tietojen salaaminen, laitehallinta, sovellusten suojaaminen, haavoittuvuuksien skannaaminen, koodin allekirjoittaminen, tunkeutumisenhavaintajärjestelmät CAN-väylään ja haittahjelmien torjunta keskusyksikölle.

Trend Micro tarjoaa esineiden internet -kyberturvallisuusratkaisuja myös älyautoille. Lisätietoja täällä.

Lataa koko raportti, *Cyber Security Risks of Connected Cars*, alla.

[1] DREAD-analyysi arvioi kuinka suurta vahinkoa omaisuudelle voidaan aiheuttaa; kuinka helppoa hyökkäys on suorittaa ja toistaa; kuinka helppoa hyödynnettävän heikkouden löytäminen on ja kuinka moniin käyttäjiin se saattaa vaikuttaa.

[2] https://unece.org/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll-out-connected-vehicles

---

Trend Micro
Japanilainen vuonna 1988 perustettu Trend Micro on yksi kyberturvan globaaleista pioneereista. Kolmessa vuosikymmenessä yrityksestä on kasvanut maailman suurin riippumaton tietoturvaratkaisujen valmistaja. Trend Micro toimii 50 maassa ja työllistää yli 6000 tietoturva-alan

asiantuntijaa. Yhtiön valmistamat innovatiiviset tietoturvaratkaisut suojaavat tehokkaasti hybridipilviympäristöt ja tietoverkot sekä modernit työympäristöt päätelaitteineen ja palveluineen. Lisätietoja osoitteesta: www.trendmicro.com.

Yhteyshenkilöt

Natalie Majerski
Lehdistökontakti
Press contact
stockholmtrendmicro@archetype.co
+46 76-103 2010

Kalle Salminen
Lehdistökontakti
Cyber Security Expert, CISSP, CCSP, CEH - Trend Micro Suomi
Kalle_Salminen@trendmicro.com