Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

# NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

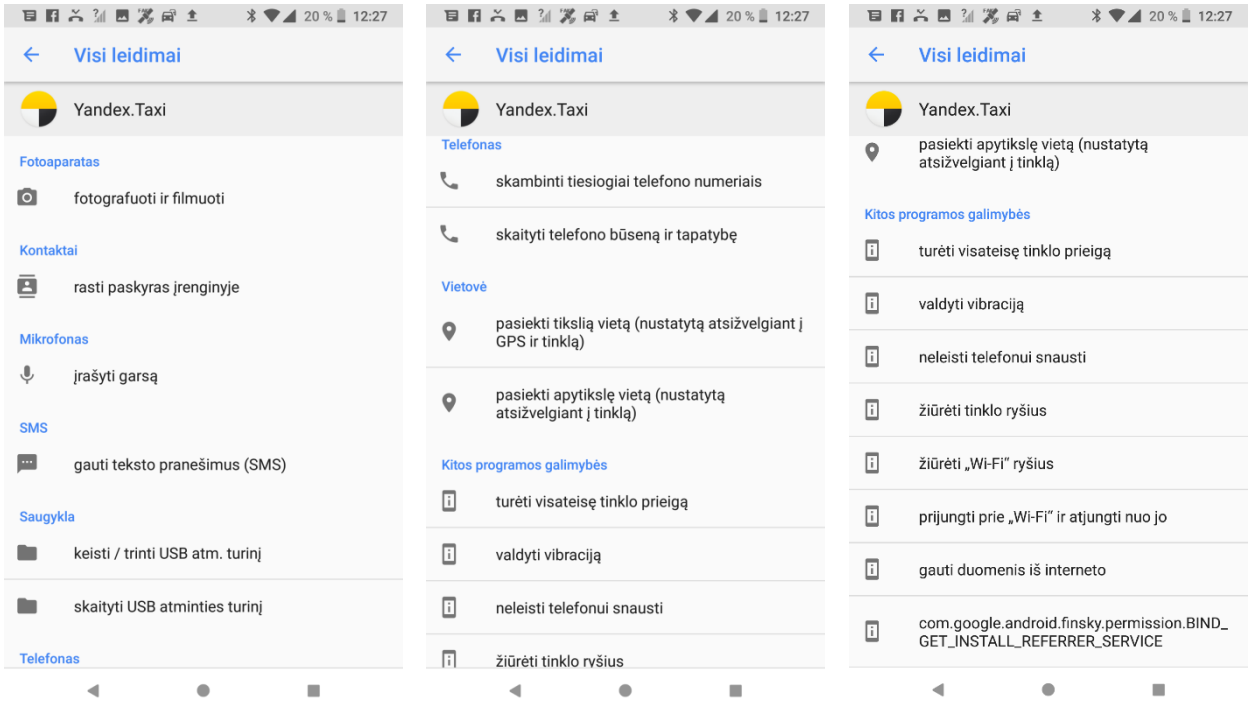
# INFORMACINIS BIULETENIS „YANDEX. TAXI“ PROGRAMĖLĖS TYRIMAS IR PROGRAMĖLIŲ NAUDOJIMO REKOMENDACIJOS

2018 m. rugpjūčio 3 d.

Nacionalinis kibernetinio saugumo centras (NKSC) prie Krašto apsaugos ministerijos atliko pirminę išmaniesiems įrenginiams skirtos „Yandex. Taxi“ programėlės analizę, kuri pradėta aktyviai platinti Lietuvoje nuo 2018 m. liepos 26 dienos.

Programinio kodo analizė parodė, kad ši programėlė reikalauja prieigos prie didelio kiekio jautrių duomenų ir leidimo naudotis įrenginio funkcijomis. Minima programėlė turi galimybę aktyvuoti įrenginio kamerą ir mikrofoną (vykdyti naudotojo aplinkos įrašymą), naudoti kontaktų sąrašą (galimybė gauti telefonų knygos, naudojamų paskyrų informaciją), vykdyti skambučių valdymą, įrenginio tapatybės ir veiklos būklės nustatymą, vykdyti trumpųjų pranešimų paslaugų valdymą (galimybė perimti gaunamus pranešimus), atlikti turinio, saugomo išmaniojo įrenginio atmintyje, modifikavimą, nustatyti tikslią (GPS) įrenginio buvimo vietą, atlikti tinklo prieigos valdymą (siųsti duomenis internetu, stebėti ir valdyti tinklo sujungimus, valdyti belaidžio tinklo (angl. Wi-Fi) prieigą).

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt




Pažymėtina ir tai, kad vėlesnės programėlės versijos ateityje gali padidinti reikalaujamų funkcijų prieigų kiekį.

Tačiau, nepaisant gausių reikalaujamų prieigų prie įrenginio funkcionalumų, ji yra pagaminta kokybiškai, tinkamai optimizuota, duomenų perdavimui naudoja šifruotus kanalus, standartinius protokolų prievadus.

NKSC analizės metu buvo nustatyta, kad programėlė šifruotais ryšio kanalais reguliariai jungėsi ir palaikė aktyvų ryšį su 11 unikalių IP adresų (iš kurių, 10 priklauso Rusijos Federacijai). Duomenų perdavimas vykdomas atsitiktinai.

Nustatyta, kad minima programėlė turi galimybę įvairiu laiku ir šifruotais ryšio kanalais užmegzti ryšį su skirtinguose Rusijos Federacijos regionuose esančiais adresais (pagal geolokacijos IP duomenų bazių informaciją) nepriklausomai nuo to, ar programėlė dirba budėjimo, ar aktyviuoju režimu. Pažymima, kad „Yandex. Taxi" palaiko nuolatinį ryšį su trimis adresais. Susisteminti pirminės analizės duomenys pateikti **1 lentelėje**.

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

**1 lentelė.** Pirminė programinio paketo tinklo srauto analizė (*Pastaba: IP adresai NKSC žinomi*)

| Komercinis pavadinimas: **Yandex. Taxi** | | | | | |
|---|---|---|---|---|---|
| Sisteminis pavadinimas: **ru.yandex.taxi** | | | | | |
| Eil. Nr. | Aktyvūs tinklo sujungimai | Miestas | Serverio vardas (*angl.* Hostname) | Perduodami duomenys programėlei esant budėjimo režime | Perduodami duomenys programėlei esant aktyviai |
| 1 | | Maskva | *.yandex.net | *Taip* | *Taip* |
| 2 | | Maskva | *.yandex.net | *Taip* | *Ne* |
| 3 | | Maskva | *.yandex.net | *Taip* | *Ne* |
| 4 | | New Jersey, Absecon | *.linode.com | *Taip* | *Taip* |
| 5 | | Jakaterinburgas | *.yandex.net | *Taip* | *Taip* |
| 6 | | Maskva | *.yandex.ru | *Ne* | *Taip* |
| 7 | | Jakaterinburgas | *.yandex.ru | *Ne* | *Taip* |
| 8 | | Jakaterinburgas | *.yandex.net | *Ne* | *Taip* |
| 9 | | Jakaterinburgas | *.yandex.net | *Ne* | *Taip* |
| 10 | | Maskva | *.yandex.net | *Ne* | *Taip* |
| 11 | | Maskva | *.yandex.ru | *Ne* | *Taip* |

Be to, kaip buvo pažymėta anksčiau, remiantis Lietuvos Respublikos Valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos 2018 m. Grėsmių nacionaliniam saugumui vertinimu – *„Rusijos žvalgybos ir saugumo tarnybos turi teisinius įgaliojimus ir techninių galimybių įgyti prieigą prie Rusijos ir užsienio valstybių piliečių, naudojančių rusiškas elektroninio komunikavimo platformas, duomenų“*. Grėsmių vertinime taip pat nurodoma: *„(...) grėsmė, kad asmeniniai duomenys nutekinami Rusijos žvalgybos ir saugumo tarnyboms, kyla visiems Lietuvos piliečiams, besinaudojantiems rusiškais socialiniais tinklais ir elektroninio pašto paslaugomis, pvz., odnoklasniki, mail.ru, yandex ir pan.“*.

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

## Mobiliųjų įrenginių programėlių grėsmės

NKSC perspėja, kad kenkėjiškų programų rizika jūsų mobiliajame įrenginyje reali: nusikaltėliai gali pavogti jūsų pinigus ir konfidencialią informaciją, šnipinėti jūsų veiksmus, šantažuoti dėl asmeninės informacijos atskleidimo, siųsti padidinto tarifo SMS žinutes jūsų sąskaita, išnaudoti įrenginius užkrato ar brukalo platinimui, kitų sistemų užvaldymui bei kibernetinėms atakoms vykdyti.

Taip pat reikia nepamiršti užšifruojančių bei išpirkos reikalaujančių virusų (angl. *ransomware*). Išpirkos reikalaujanti programinė įranga laiko įkaitu jūsų mobilųjį įrenginį ir duomenis dėl pinigų. Tokio tipo kenkimo programos užblokuoja jūsų įrenginių ekraną arba neleidžia pasiekti tam tikrų failų ir funkcijų. Gali tekti atkurti gamyklinius nustatymus, prarandant visus savo duomenis. Kartais ir po gamyklinių duomenų atstatymo įrenginiai lieka užvaldyti kenkėjiškų programų.

Deja, didelė visuomenės dalis vis dar neįvertina savo mobilaus prietaiso apsaugos svarbos. Žemiau pateikiami NKSC patarimai, kaip elgtis su savo mobiliuoju įrenginiu kasdieninėje veikloje, naudojantis mobiliosiomis programėlėmis, ir kaip apsisaugoti ar bent maksimaliai sumažinti mobiliųjų programėlių keliamas rizikas.

## Rekomendacijos

Naudokite aplikacijas tik iš oficialių programėlių parduotuvių (Google Play (Android) arba App Store (iOS)). Venkite programėlių iš trečiųjų šalių, nediekite į savo įrenginius piratinių ("nulaužtų") aplikacijų kopijų - jose dažniausiai būna įskiepytos kenkėjiškos funkcijos.

Būkite atsargūs su nuorodomis į programėles, kurias gaunate el. paštu ar trumposiomis teksto žinutėmis - jos gali apgaule priversti jus įdiegti trečiosios šalies ar nežinomų šaltinių programėles.

Prieš atsisiųsdami programėlę, pasidomėkite ja ir jos leidėjais. Paskaitykite kitų naudotojų paliktus atsiliepimus, peržiūrėkite įvertinimus.

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

Susipažinkite su programėlės leidimais - patikrinkite, kokius duomenis aplikacija gali pasiekti, ir ar ji gali dalytis jūsų informacija su trečiaisiais asmenimis. Įvertinkite, ar savo funkcijai atlikti nurodyti leidimai nėra pertekliniai.

Atnaujinkite visas savo programėles bei operacinę sistemą. Kuomet įmanoma, įjunkite automatinį programėlių atnaujinimą. Tai padės išvengti rizikų dėl pasenusių, pažeidžiamų aplikacijų versijų.

Nemodifikuokite savo operacinės sistemos, kad išgauti daugiau telefono galimybių (angl. *rooting* (Android), *jailbreaking* (iOS)). Tai panaikins esamas telefono apsaugas ir padidins kenkėjiškų programų keliamas rizikas. Taip pat tai gali pažeisti jūsų įrenginio garantinio aptarnavimo sąlygas.

Įdiekite mobiliesiems įrenginiams skirtą saugumo programėlę - ji patikrins visas jūsų įrenginyje esančias ir naujai įdiegtas programėles, įspėdama apie rastas kenkimo programas ar įtartiną veiklą.

Dažnai kurkite savo duomenų atsargines kopijas. Naudokitės specialia programine įranga, kuri padės lengvai kurti duomenų kopijas kompiuteryje arba naudokitės paslaugomis, kurios automatiškai darys kopijas į debesinę duomenų saugyklą.