NKSC prie KAM
Inovacijų ir mokymo skyrius
support@ims.nksc.lt

Lietuvoje tiekiamų vaizdo stebėjimo kamerų kibernetinio saugumo vertinimas

GAMINTOJŲ „Hikvision“ ir „Dahua“ PRODUKCIJOS PAVYZDŽIŲ ANALIZĖ

Įžanga

Nacionalinis kibernetinio saugumo centras (NKSC) prie Krašto apsaugos ministerijos atsižvelgdamas į visuomenės, žiniasklaidos ir valstybės institucijų poreikį įvertinti vaizdo stebėjimo kamerų kibernetinį saugumą, atliko šį Kinijos gamintojų „Hikvision“ ir „Dahua“ vaizdo stebėjimo kamerų vertinimą. Tyrimas atliktas nepriklausomai ir neįtakojus gamintojui, kai bendradarbiaujant su valstybės institucijomis, tyrimo objektai buvo paimti iš praktikoje naudojamų pavyzdžių.

Pagal NKSC atliktos apklausos rezultatus, „Hikvision“ ir „Dahua“ kameras šalyje naudoja 57 institucijos.

Vaizdo stebėjimo sistemų gamintoja „Hangzhou Hikvision Digital Technology Co., Ltd.“ („Hikvision“) yra Kinijos korporacija, įsteigta 2001 m., turinti 26 000 darbuotojų [1], listinguojama Kinijos Šendženo vertybinių popierių biržoje [2], produkciją tiekianti plačiai pasaulyje, valdo prekinį ženklą „Ezviz“ [3]. Įmonė 2020 m. pavasario gaminių kataloge pristatė daugiau nei 300 įvairių konfigūracijų produktų – internetinių, giliojo mokymo kamerų ir jų sprendimų, termovizijos įrenginių, vidaus ir išorės stebėjimo kamerų, vaizdo glaudinimo ir transliavimo sprendimų, plataus funkcionalumo apsaugos kompleksų. „Hikvision“ sprendimai orientuoti plačioms vartotojų grupėms – skirti naudoti pramonės, namų ūkių, paslaugų sferos sektoriuose, įmonės kuriamos technologijos taikytinos komercijos, eismo reguliavimo, bankininkystės, švietimo, statybų, miesto priežiūros, apsaugos sistemų funkcionalumui užtikrinti [4]. „Hikvision“ produkcija užima 22% pasaulinės vaizdo stebėjimo sistemų dalies, produkcija eksportuojama į daugiau nei 150 šalių [5]. Gamintojas vysto produktų plėtrą Europos Sąjungoje, gaminiai pristatomi tarptautinėse technologijų parodose ir konferencijose.

Kita tyrime nagrinėjama produkcija – gamintojo „Zhejiang Dahua Technology Co., Ltd.“ („Dahua“). „Dahua“ – Kinijos įmonė, įkurta 2001 metais, veiklą vystanti vaizdo stebėjimo technologijų sektoriuje [6], listinguojama Šendženo vertybinių popierių biržoje, turi 13 000 darbuotojų [7], produkciją tiekia daugiau nei į 180 šalių.

Kompanija turi keturis tyrimų institutus – naujų technologijų, didžiųjų duomenų tyrimų, mikrograndynų vystymo ir debesų kompiuterijos sistemų. Institutuose dirba daugiau kaip 6000 mokslininkų ir tyrėjų, vystančių veiklą dirbtinio intelekto, daiktų interneto, audiovizualinio turinio analizės, programinės įrangos kūrimo srityse. „Dahua“ 2016 m. buvo įregistravusi daugiau kaip 800 patentų [7].

Nepaisant tyrimų potencialo, „Dahua“ susidūrė su savo įrangos saugumo iššūkiais – remiantis įvairių šaltinių [14] informacija, jų įrangoje fiksuota įvairių kibernetinio saugumo pažeidžiamumų. 2016 m. buvo įvykdyta didelės apimties DDoS (*angl.* Distributed Denial – of – Service) ataka, kurioje dalyvavo „Dahua“ ir „Dahua OEM“ kameros [12]. Beveik milijonas „Dahua“ įrenginių buvo užkrėsti „BASHLITE“ kenkėjiška programa [13], [14]. „Dahua“ kameros turėjo pažeidžiamumą, įgalinantį perimti operacinės sistemos kontrolę į kameros administravimo panelę įvedus atsitiktinį vartotojo vardą

su per daug numatytųjų simbolių. Tai buvo išnaudota, o įrenginiuose įdiegta kenkėjiška programinė įranga leido kameras išnaudoti DDoS atakose bei jas pasitelkti neteisėtam vaizdų įrašymui.

Remiantis 2017 m. publikuotais straipsniais, kibernetinio saugumo tyrėjai aptiko „Dahua“ kamerų programinės įrangos pažeidžiamumą, kuris buvo suaktyvintas „Fortune 500“ bendrovės tinklo kamerose, o incidento metu duomenys buvo perduoti Kinijai [13]. Naudojantis interneto naršyklę, pažeidžiamumas leido pašaliniams asmenims nuotoliniu būdu atsisiųsti įrenginio vartotojo vardų ir slaptažodžių duomenų bazę ir vėliau prieiti prie kamerų valdymo [14]. Po šių incidentų „Dahua“ išleido programinės įrangos naujinį, kuris pašalino 11 produkto saugumo pažeidžiamumų [15]. Tačiau saugumo tyrėjai aptiko, kad atnaujintoje programinėje įrangoje visgi liko tas pats pažeidžiamumas, tačiau ši spraga buvo perkelta į kitą kodo dalį. Straipsnio autoriai tai apibūdino kaip tyčinį veiksmą, programiniame kode paliekant „atsargines duris“ (*angl*. Back – door) [15].

„Hikvision“ ir „Dahua“ tiekia savo elektronikos komponentus kitiems gamintojams kaip OEM (*angl.* Original Equipment Manufacturer). Apie 70 kitų prekės ženklų naudoja „Hikvision“ aparatinę įrangą, gali papildomai įrašyti savo programinę įrangą ir taip toliau platinti su savo prekės ženklu [25].

Tyrimo imtyje nagrinėti įrenginiai – Lietuvoje platinamos teritorijų stebėjimui skirtos kameros – „Hikvision“ vaizdo stebėjimo kamera „DS-2CD4C26FWD-AP“ ir „Dahua“ vaizdo stebėjimo kamera „DH-IPC-HFW5231EP-ZE“. Tyrime dalyvavusios produkcijos vaizdai patekti 1 paveiksle.

DS-2CD4C26FWD-AP DH-IPC-HFW5231EP-ZE

1 pav. Tyrime dalyvavusios „Hikvision“ ir „Dahua“ produkcijos vaizdai

„Hikvision“ kamera „DS-2CD4C26FWD-AP“ – lauko sąlygomis skirtas naudoti įrenginys, turintis išorinę linzę, 2MP rezoliucijos, palaikantis H.265+ audiovizialinio turinio glaudinimo technologiją [17]. „Dahua“ kamera „DH-IPC-HFW5231EP-ZE“ – išorės stebėjimui, valdoma kamera, turinti Ambarella S2LM Cortex-A9 600 MHz DSP procesorių, palaikantį audiovizualinio turinio glaudinimo H.265+/H.265/H.264+/H.264 formatus, veikianti Linux operacinės sistemos pagrindu [18]. Gaminių programinės įrangos versijos nėra nurodomos, tačiau jos buvo nustatytos ir pažymėtos tolesnio tyrimo aprašyme. Kameros Valstybės institucijoje naudojamos nuo 2018 m. (gaminamos nuo 2016 m.), o jų kainos: „Hikvision DS-2CD4C26FWD-AP“ – 621 Eur., „Dahua DH-IPC-HFW5231EP-ZE“ – 335 Eur.

Tyrime buvo atliekami veiksmai ir jų seka taip, kad kiti tyrėjai galėtų atkartoti NKSC analizės rezultatus ir turėtų gauti analogiškus rezultatus. Tyrimo metodika paremta:

1) programinės įrangos funkcionalumo analize;
2) kamerų kuriamų duomenų srautų struktūros ir turinio analizė;
3) aparatinės dalies ir elektronikos komponentų dekompozicija.

Aparatinės dalies tyrimo metu buvo atlikta įrenginiuose naudojamų mikroschemų atitikties analizė, įvertinta gaminio schemotechninė struktūra ir jo pagaminimo kokybė. Šiame tyrime įrenginiai buvo demontuoti iki ribos, kurią peržengus atgalinis surinkimas būtų galimas tik panaudojus precizinę įlitavimo / išlitavimo įrangą, tokiu atveju padidinant riziką negrįžtamai dėl proceso metu naudojamos aukštos temperatūros pažeisti mikrograndynuose esamą informaciją.

Tyrimo santrauka

Atlikus „Hikvision“ ir „Dahua“ stebėjimo kamerų dekompozicijos tyrimą nustatyta, kad 2018 m. pagamintoje „Hikvision“ kameroje yra naudojami programiniai sprendimai, parengti 2012 – 2015 m. laikotarpiu, turintys žinomų kibernetinio saugumo spragų, pažymėtų viešai prieinamoje pažeidžiamumų duomenų bazėje (*angl.* Common Vulnerabilities and Exposures – CVE). Buvo nustatyti 7 kameroje įdiegti programiniai paketai, turintys 61-ą CVE pateiktą pažeidžiamumą, iš kurių 23-ijų pažeidžiamumų grėsmingumo balas didesnis nei 6,8 (iš 10 galimų). Nustatyti pažeidžiamumai įgalina kameros informacijos perėmimą nuotoliniu būdu, žalingo kodo įvykdymą, kamera paveiki atkirtimo nuo paslaugos DoS (*angl.* Denial – of – Service) atakoms. Tirti tie programinio kodo paketai, kurie naudoti tirtuose pavyzdžiuose ir įdiegti įsigytose kamerose (*angl.* Out of the box).

Nustatyta, kad pagal nutylėjimą vartotojų autentifikavimas „Hikvision“ kameroje vykdomas nešifruotu ryšiu, naudojant riboto patikimumo 1999 m. sukurtą suvestinės prieigos vartotojų autentifikavimo technologiją (*angl.* HTTP Digest access autentication) [19]. Naudojant šį autentifikavimo mechanizmą, vartotojui jungiantis prie kameros, jo slaptažodžio reikšmė gali būti perimta, slaptažodis dekoduotas ir vėliau galimai panaudotas neteisėtam prisijungimui. Verta pažymėti, kad tirtame įrenginyje buvo rasti saugumo sprendimai, leidžiantys eliminuoti neteisėto vartotojų prisijungimo problemą, tačiau standartinėje konfigūracijoje jie nebuvo aktyvūs.

Tyrimo metu kameroje buvo aptikta įjungta ir funkcionuojanti nuotolinio valdymo aplinka „ISAPI“. ISAPI (*angl.* Intelligent Security Application Programming Interface) – „Hikvision“ naudojamas protokolas, įgalinantis tekstinių užklausų pagalba vykdyti įrenginio kontrolę nuotoliniu būdu. Protokolu mezgamu ryšiu perduodamų duomenų šifravimui panaudotas AES šifravimo standartas, CBC algoritmas, tačiau šifruoti duomenys (slaptažodis ir kita informacija) nėra autentifikuojami, todėl šifruota kameros valdymo trakto informacija gali būti modifikuota. Platesnis, 755 lapų apimties protokolo ir kameros funkcijų valdymo aprašas pateiktas „Hikvision“ puslapyje – *https://www.hikvision.com/content/dam/hikvision/en/support/download/firmware/firmware-with-cc/Hikvision%20ISAPI%20Core%20Protocol.pdf* .

Svarbu pažymėti, kad dėl vartotojo autentifikavimo technologijos trūkumų egzistuoja galimybė paveikti kamerą nuotoliniu būdu, tam panaudojant pagal nutylėjimą įjungtos „ISAPI“ aplinkos funkcionalumą. Tai galimai leistų neteisėtai perimti kameros turinio transliaciją, realiuoju laiku aktyvuoti ar deaktyvuoti kameros funkcijas (vaizdo atpažinimo, garso įrašymo ir kt.) ar trukdyti kameros veikimui.

Šio tipo kamerose nebuvo rasta automatinio atnaujinimo funkcionalumo. Programiniai atnaujinimai turi būti atsisiųsti ir įdiegti rankiniu būdu. Remiantis geolokacijos IP duomenų bazių informacija, kameros atnaujinimo nuoroda patalpinta „Hikvision“ puslapyje, esančiame Kinijoje registruotame serveryje, kuri savo ruožtu atlieka nukreipimą į Rusijoje registruotą serverį, iš kurio siunčiama į kamerą diegiama atnaujinimo rinkmena. Šiuose serveriuose galimai yra registruojamos iš vartotojų atėjusios užklausos, leidžiančios nusakyti vartotojo IP adresą, šalį, užklausos laiką, atsisiunčiamo naujinio versiją.

Kamerų valdymo galimybėms išplėsti gamintojas „Hikvision“ siūlo mobilią aplikaciją „Hik-Connect“. Nustatyta, kad ši aplikacija vykdo sujungimus su 9 IP adresais, esančiais Airijoje, Kinijoje, Singapūre, Tailande. Aplikacija naudoja potencialiai perteklinę informaciją – registruoja SIM kortelės IMSI ir ICCID identifikacinius numerius, mobilaus įrenginio IMEI identifikacinį numerį.

Elektronikos dekompozicija parodė, kad „Hikvision“ kameroje naudojamas uždaras procesorius „HK-2015-1 DP8181934“, skirtas vaizdo apdorojimui ir išorinių sąsajų komunikacijos funkcionalumui užtikrinti. Galima teigti, kad tai yra nestandartinis, rinkoje laisvai neprieinamas gaminys. Informacijos, nusakančios „Hikvision“ sukurto procesoriaus charakteristikas žinių bazėse nebuvo rasta, todėl sudėtinga iki galo įvertinti jo (o kartu ir kameros) turimas funkcijas, galimus darbo režimus.

Detali informacija apie tyrimo rezultatus

Atlikus gaminių programinės įrangos funkcionalumo ir jos kuriamų srautų (gaunamų ir išsiunčiamų duomenų) analizę bei aparatinės dalies dekompozicijos tyrimus, buvo nustatyti žemiau aptariami faktai. Pažymėtina, kad buvo tirta programinės įrangos versija, kuri nustatyta sudiegta naudotojo tiriamame pavyzdyje. Analizuotos „Hikvision“ kameros atveju buvo V5.5.84 (detaliau 3 ir 6 pav.). Papildomi programinės įrangos naujinimai diegti ir tyrinėti nebuvo. Be to, gamintojo puslapyje pranešama apie šio modelio atnaujintą 2019-03-12 versiją V5.5.83 [26]. „Hikvision“ kibernetinio saugumo centras šio modelio kameros programinės įrangos saugumo naujinimų nepateikia [22].

1. **„Hikvision“ ir „Dahua“ kamerose pagal nutylėjimą įjungta tarnybinė aplinka, kuria kameras galima valdyti nuotoliniu būdu**

Tyrimo metu kameroje buvo aptikta įjungta ir funkcionuojanti nuotolinio valdymo aplinka „ISAPI“. ISAPI (*angl.* Intelligent Security Application Programming Interface) – „Hikvision“ naudojamas protokolas, įgalinantis tekstinių užklausų pagalba vykdyti įrenginio kontrolę nuotoliniu būdu.

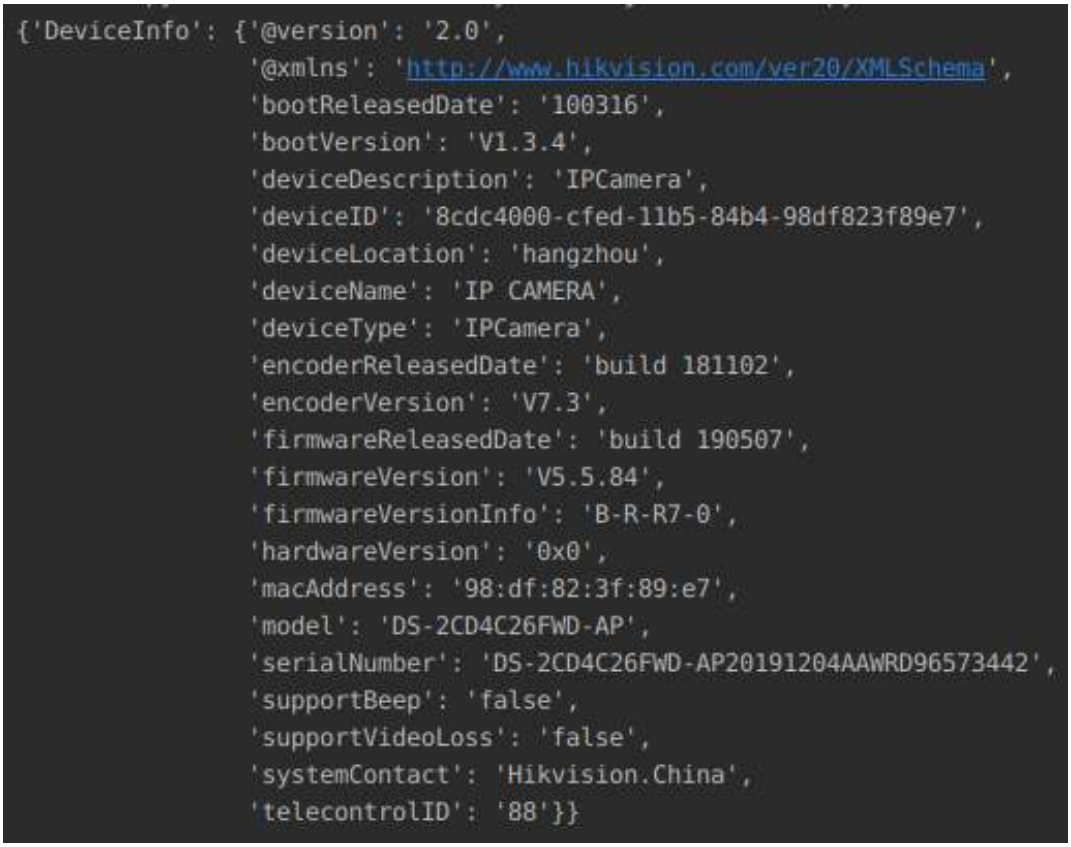
Protokolu mezgamu ryšiu perduodamų duomenų šifravimui panaudotas AES šifravimo standartas, CBC algoritmas, tačiau šifruoti duomenys (slaptažodis ir kita informacija) nėra autentifikuojami, todėl kameros valdymo trakto informacija gali būti modifikuota. Dėl duomenų autentifikavimo nebuvimo, kamera tampa paveiki „Chosen – chiphertext“, „Padding“ ir kitoms tokio pobūdžio atakoms. Platesnis, 755 lapų apimties protokolo ir kameros funkcijų valdymo aprašas pateiktas „Hikvision“ puslapyje – *https://www.hikvision.com/content/dam/hikvision/en/support/download/firmware/firmware-with-cc/Hikvision%20ISAPI%20Core%20Protocol.pdf*.

Svarbu pažymėti, kad dėl vartotojo autentifikavimo technologijos trūkumų, egzistuoja galimybė paveikti kamerą nuotoliniu būdu, tam panaudojant pagal nutylėjimą įjungtos „ISAPI“ aplinkos funkcionalumą. Tai galėtų leisti neteisėtai perimti kameros turinio transliaciją, realiuoju laiku aktyvuoti ar deaktyvuoti kameros funkcijas (vaizdo atpažinimo, garso įrašymo ir kt.), stabdyti kameros veikimą. Šis poveikis gali būti vykdomos to neatspindint kameros registracijos žurnaluose.

Tyrimo metu buvo suformuota specializuota užklausa ir ISAPI protokolu nusiųsta kameros SDK aplinkai. Kamera užklausą priėmė ir apdorojo, pateikė atsakymą. 2 paveiksle pateikta suformuotos užklausos ir gauto atsako vaizdas, pažymint ryšio protokolą, duomenų kiekius ir užklausos tipus.

2 pav. Suformuotos užklausos ir gauto atsako vaizdas, pažymint ryšio protokolą, duomenų kiekius ir užklausos tipus

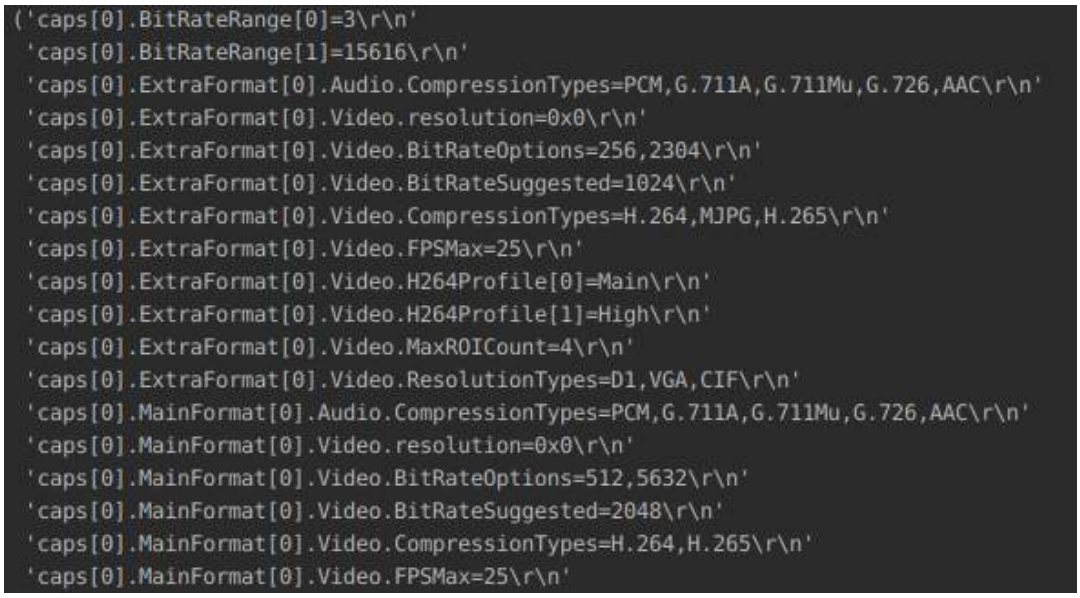
Į kamerą buvo išsiųsta suformuota 486 baitų dydžio užklausa, prašanti kameros pateikti jos tarnybinę informaciją. Šią užklausą „Hikvision“ kamera priėmė, apdorojo ir išvedė 1311 baitų dydžio atsakymą, pateiktą 3 paveiksle. Atsakyme atsispindi kameros programinių paketų versijos, modelis, MAC adresas ir kita tarnybinė informacija. Remiantis šia informacija, galima nustatyti tinkle naudojamus įrenginius, įvertinti potencialias jų spragas, sudarančias sąlygas neteisėtam kameros valdymo perėmimui.



3 pav. „Hikvision“ kameros sugeneruotas 1311 baitų dydžio atsakas

ISAPI sistemos funkcionavimo principas toks, kad pagal nutylėjimą įjungta „ISAPI“ plataus spektro kameros valdymo aplinka potencialiai gali būti išnaudota kameros vaizdo transliacijų perėmimui ar kitaip pažeisti vartotojų privatumą.

Analogiškas funkcionalumas buvo nustatytas ir tirtoje „Dahua“ (prog. Versija: V2.800.0000002.0.R, versijos parengimo data: 2019-01-11, WEB versija: V3.2.1.684680, ONVIF versija 16.12 (V2.4.3.651299), Security Baseline versija V1.4) kameroje. Kameros užklausos atsakas „Dahua“ atveju pateiktas 4 paveiksle.

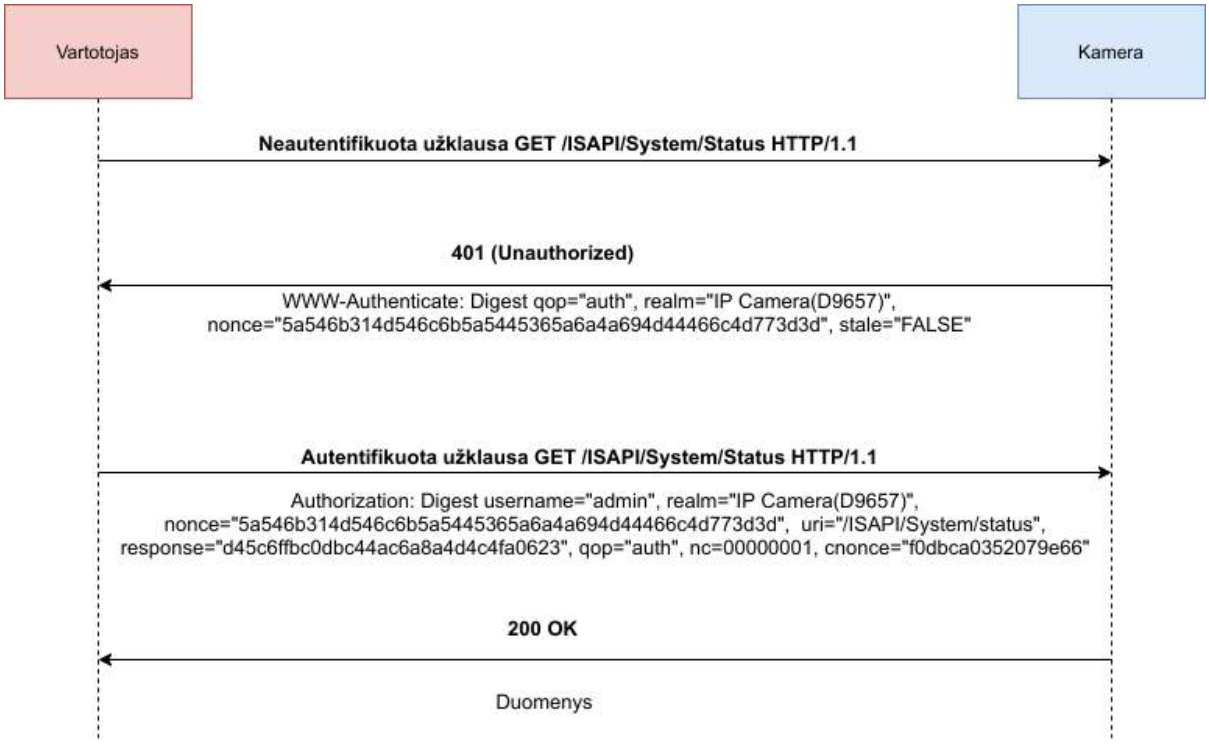


4 pav. „Dahua“ kameros sugeneruotas užklausos atsakas

2. Tirtose „Hikvision“ ir „Dahua“ kamerose naudojama nepakankamai saugi HTTP Digest autentifikacijos schema

Nustatyta, kad pagal nutylėjimą vartotojų autentifikavimas „Hikvision“ ir „Dahua“ kamerose vykdomas nešifruotu ryšiu, naudojant riboto patikimumo 1999 m. sukurtą suvestinės prieigos vartotojų autentifikavimo technologiją (*angl.* HTTP Digest access autentication) [19]. Naudojant šį autentifikavimo mechanizmą, vartotojui jungiantis prie kameros, jo slaptažodžio reikšmė gali būti perimta, slaptažodis dekoduotas ir panaudotas neteisėtam prisijungimui. Verta pažymėti, kad tirtame įrenginyje buvo rasti saugumo sprendimai, leidžiantys eliminuoti neteisėto vartotojų prisijungimo problemą, tačiau standartinėje konfigūracijoje jie nebuvo aktyvūs.

Pateikiamas detalesnis „Hikvision“ (analogiškas „Dahua“) kameros atveju naudojamos suvestinės prieigos vartotojų autentifikavimo mechanizmo aprašymas. Autentifikavimo procedūros tikslas – vartotojui saugiai ir tinkamai prisijungti prie kameros valdymo panelės. 5 paveiksle pateikta tyrimo metu atliktos suvestinės prieigos autentifikavimo technologiją prisijungimo prie kameros procedūros diagrama.



5 pav. Suvestinės prieigos vartotojų autentifikavimo proceso „Hikvision“ kameroje diagrama

Tyrimo metu buvo atliktas suvestinės prieigos vartotojų autentifikavimo procesas, sudarytas iš penkių žingsnių:

1. Vartotojas kreipiasi į kameros autentifikavimo puslapį su prašymu nukreipti į autentifikavimo platformą (“Neautentifikuota užklausa GET /ISAPI/System/Status HTTP/1.1”). Užklausoje vartotojo vardas ir slaptažodis siunčiami nėra.
2. Kamera, gavusi vartotojo užklausą, pradeda autentifikavimo procesą ir vartotojui grąžina HTTP 1.1 standarto atsako kodą 401 „Unauthorized“, pridedant autentifikacijai reikalingą informaciją – apsaugos kokybės parametrą „qop“, autentifikavimo sritį „realm“, atsitiktinai sugeneruotą vienkartinę kriptografinę žymę „noce“, senumo indikatorių „stale“. Tyrimo metu iš kameros buvo gauta sekanti informacija: „WWW-Authenticate: Digest qop=”auth”, realm=”IP Camera(D9657)”, nonce=”5a546b …”, stale=”FALSE”“. Ši informacija yra priimama vartotojo naršyklėje.
3. Informaciją priėmusi naršyklė apdoroja gautą autentifikavimo srities identifikatorių „realm“ ir vartotojui išveda vartotojo vardo bei slaptažodžio įvedimo formą.

4. Vartotojui į formą suvedus vartotojo vardą ir slaptažodį, naršyklė (klientas) persiunčia gautą atsakymą, pridedant autentifikavimo antraštę turinčią atsako kodą. Tyrimo metu iš vartotojo kamerai buvo persiųsta sekanti informacija: „Authorization: Digest username=”admin”, realm=”IP Camera(D9657)”, nonce=”5a546b …”, uri=”/ISAPI/System/status”, response=”d45c6 …”, qop =”auth”, nc=0000001, cnonce=”f0dbca …”“. Vartotojo išsiųstame atsakyme matomas kameros vartotojo vardas „admin“ ir MD5 formatu užkoduotas kameros slaptažodis – „d45c6 ...“, kurį perėmus galima dešifruoti ir panaudoti neteisėtam kameros užvaldymui.
5. Kamera, gavusi vartotojo atsiųstą informaciją ją patikrina ir jai atitikus numatytas reikšmes, vartotoją autentifikuoja, grąžina HTTP 1.1 standarto atsako kodą 200 „OK”, išveda konfigūracijos panelės vaizdą. Išvestoje kameros konfigūracijos panelėje vartotojas gali atlikti kameros valdymo procedūras.

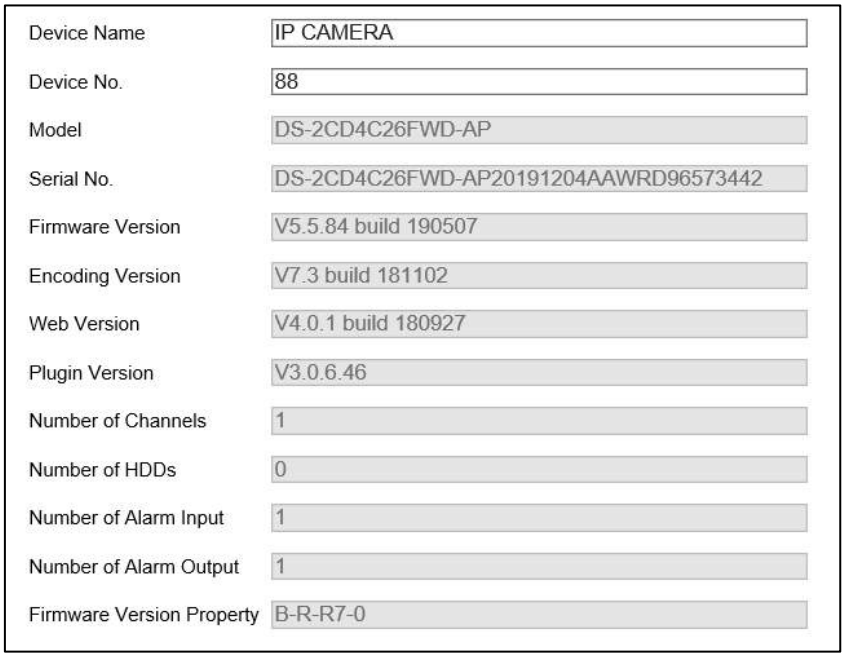
Žinomi suvestinės prieigos vartotojų autentifikavimo technologijos trūkumai:

- Kameros vartotojo autentifikacijos sistema neturi galimybės užtikrinti saugaus vartotojui pristatomos autentifikavimo sąsajos valdymo.
- Daugelis autentifikacijos standarte (RFC 2617) numatytų saugumo priemonių yra tik rekomendacinio pobūdžio, neprivalomos. Be to, standarte yra numatytos saugumo išlygos – jeigu sistemoje nėra nurodytas apsaugos kokybės parametras „qop“, procesai pradedami vykdyti sumažinto saugumo RFC 2069 standarto režimu. Šio tyrimo objekto atveju, apsaugos kokybės parametras „qop“ yra naudojamas.
- Naudojamas autentifikavimo mechanizmas yra paveikus duomenų perėmimo „angl. Man-in-the-middle (MITM)“ atakai. Vykstant autentifikavimo procedūrai, informacija tarp vartotojo ir autentifikavimo serverio yra nešifruota, turinti potencialą būti panaudota slaptažodžio dešifravimui. Dėl jautrios informacijos šifravimo stokos, duomenų perėmimas tampa racionalia priemone siekiant gauti įrenginio slaptažodį.
- Tam tikrais atvejais, siekiant sutaupyti resursus ir esant reikalui greitai vykdyti slaptažodžio patikrinimą, sistemose slaptažodis gali būti šifruojamas greitais, tačiau riboto saugumo algoritmais. Šio tyrimo objekto atveju – MD5.

Verta pažymėti, kad kameros autentifikacijos mechanizme taikomas MD5 algoritmas, kurtas 1992 m., neatitinka šio laikmečio saugumo reikalavimų. MD5 nebevystomas ir tarptautiniuose standartuose, skirtuose autentifikavimui, nenaudojamas nuo 2008 m. MD5 pakeitė SHA (*angl.* Secure Hash Algorithms), pavyzdžiui SHA-512.

3. „Hikvision“ kameroje naudojami programiniai paketai, turintys žinomų saugumo pažeidžiamumų

„Hikvision“ stebėjimo kameros dekompozicijos tyrime nustatyta, kad 2018 m. pagamintoje kameroje yra naudojami programiniai sprendimai, parengti 2012 – 2015 m. laikotarpiu, turintys žinomų kibernetinio saugumo spragų, pažymėtų viešai prieinamoje pažeidžiamumų duomenų bazėje (*angl.* Common Vulnerabilities and Exposures, CVE). „Hikvision“ kameros modelis ir pagrindinių programinių paketų versijos pateiktos valdymo panelėje, atvaizduotoje 6 paveiksle.



6 pav. Tirtos „Hikvision“ kameros konfigūracijos panelės vaizdas

Nustatyti 7 kameroje įdiegti programiniai paketai, kurių naudojamos versijos turinti 61-ą CVE pateikiamą pažeidžiamumą, iš kurių 23-ijų pažeidžiamumų grėsmingumo balas didesnis nei 6,8 (iš 10 galimų). Tirtų kamerų modeliuose panaudoti kitų gamintojų, tame tarpe atviro kodo programiniai paketai. Kadangi kamerų programinė įranga komponuota apie 2018 metus, dalis programinių paketų pasenę. Pavyzdžiui „Hikvision“ kameroje naudojamas „BusyBox“ 1.19.3, kai tuo tarpu gamintojas siūlo šiai dienai atnaujintą 1.31.1 versiją. 1 lentelėje pateiktas „Hikvision“ tirtoje kameroje naudojamų potencialiai nesaugių programinių paketų sąrašas, nurodant jų pavadinimus, versijas, CVE identifikacinį numerį, pažeidžiamumo publikavimo datą ir nustatytą pažeidžiamumo grėsmingumo lygį.

1 lentelė. „Hikvision“ kameroje potencialiai nesaugių programinių paketų sąrašas su nurodytu pažeidžiamumo grėsmingumo balu

Eil. Nr.	**Kameroje naudojamas programinis paketas**	**Kameroje naudojamo paketo versija**	**Paketo pažeidžiamumo CVE identifikacinis numeris**	**Pažeidžiamumo publikavimo data**	**Pažeidžiamumo grėsmingumo balas (iš 10)**
1	BusyBox	1.19.3	CVE-2018-20679	2019-01-09	5
			CVE-2016-6301	2016-12-09	7,8
			CVE-2015-9261	2018-07-26	4,3
			CVE-2013-1813	2013-11-23	7,2
			CVE-2011-2716	2012-07-03	6,8
2	iptables	1.4.18	CVE-2012-2663	2014-02-15	7,5
3	WPA_Supplicant	0.7.2	CVE-2019-11555	2019-04-26	4,3
			CVE-2019-16275	2019-09-12	3,3
			CVE-2015-4142	2015-06-15	4,3
			CVE-2015-4141	2015-06-15	4,3

Eil. Nr.	Kameroje naudojamas programinis paketas	Kameroje naudojamo paketo versija	Paketo pažeidžiamumo CVE identifikacinis numeris	Pažeidžiamumo publikavimo data	Pažeidžiamumo grėsmingumo balas (iš 10)
4	OpenSSL	1.0.11	CVE-2017-3735	2017-08-28	5
			CVE-2016-6306	2016-09-26	4,3
			CVE-2016-6304	2016-09-26	7,8
			CVE-2016-6303	2016-09-16	7,5
			CVE-2016-6302	2016-09-16	5
			CVE-2016-2842	2016-03-03	10
			CVE-2016-2183	2016-08-31	5
			CVE-2016-2182	2016-09-16	7,5
			CVE-2016-2181	2016-09-16	5
			CVE-2016-2180	2016-07-31	5
			CVE-2016-2179	2016-09-16	5
			CVE-2016-2178	2016-06-19	2,1
			CVE-2016-2177	2016-06-19	7,5
			CVE-2016-0800	2016-03-01	4,3
			CVE-2016-0799	2016-03-03	10
			CVE-2016-0798	2016-03-03	7,8
			CVE-2016-0797	2016-03-03	5
			CVE-2016-0705	2016-03-03	10
			CVE-2016-0704	2016-03-02	4,3
			CVE-2016-0703	2016-03-02	4,3
			CVE-2016-0702	2016-03-03	1,9
			CVE-2015-4000	2015-05-20	4,3
			CVE-2015-3197	2016-02-14	4,3
			CVE-2015-3196	2015-12-06	4,3
			CVE-2015-3195	2015-12-06	5
			CVE-2015-3194	2015-12-06	5
			CVE-2015-1792	2015-06-12	5
			CVE-2015-1791	2015-06-12	6,8
			CVE-2015-1790	2015-06-12	5
			CVE-2015-1789	2015-06-12	4,3
			CVE-2015-1788	2015-06-12	4,3
			CVE-2015-0293	2015-03-19	5
			CVE-2015-0289	2015-03-19	5
			CVE-2015-0288	2015-03-19	5
			CVE-2015-0287	2015-03-19	5
			CVE-2015-0286	2015-03-19	5
			CVE-2015-0209	2015-03-19	6,8
5	SQLite	3.7.10	CVE-2019-8457	2019-05-30	7,5
			CVE-2018-20506	2019-04-03	6,8
			CVE-2018-20346	2018-12-21	6,8
6	libxls	1.4.0	CVE-2018-20452	2018-12-25	6,8
			CVE-2018-20450	2018-12-25	4,3
7	GNU C Library	>= 2.21	CVE-2017-18269	2018-05-18	7,5
			CVE-2017-16997	2017-12-17	9,3
			CVE-2016-1234	2016-06-01	5
			CVE-2015-8984	2017-03-20	4,3
			CVE-2015-8983	2017-03-20	6,8
			CVE-2015-7547	2016-02-18	6,8
			CVE-2015-1781	2015-09-28	6,8
			CVE-2014-8121	2015-03-27	5
			CVE-2014-7817	2014-11-24	4,6

Nustatyti pažeidžiamumai įgalina kameros informacijos perėmimą nuotoliniu būdu, žalingo kodo įvykdymą, kamera pasižymi ribotu atsparumu atkirtimo nuo paslaugos DoS atakoms.

„Hikvision“ kameroje pagal nutylėjimą įjungti prievadai, skirti kameros funkcijoms valdyti ir vaizdo transliacijoms vykdyti. Atidarytų prievadų sąrašas su funkcijų aprašu pateiktas 2 lentelėje.

2 lentelė. „Hikvision“ kameros atidarytų prievadų sąrašas, nurodant nustatytą jų funkcionalumą

Eil. Nr.	Prievadas	Paslauga	Funkcionalumas
1	80/TCP	HTTP	Prievadas naudojamas pasiekti Web sąsaja. Ryšys nešifruotas. Galima „ISAPI“ komunikacija.
2	443/TCP	HTTPS	Naudojamas pasiekti šifruotą HTTPS Web sąsajos versiją. Pagal nutylėjimą, norint užšifruoti ryšį su kamera, privaloma į adreso lauką įvesti antraštę „https://“, kitaip bus naudojamas nesaugus HTTP ryšys. Galima „ISAPI“ komunikacija.
3	554/TCP	RTSP	Prievadas naudojamas užmegzti vaizdo transliacijos ryšį. Nustatyta teikiamos paslaugos programinė versija „Hikvision 7513 POE IP camera rtspd“.
4	8000/TCP	Nenusakyta	Atliekant prisijungimą, įvyksta TCP duomenų apsikeitimas (angl. Handshake), tačiau po jo prievadas nutraukia ryšį. „Hik-Connect“ aplikacijoje, esančioje vietiniame tinklo segmente, įvedus šį prievadą, galima atlikti komunikaciją su kamera, todėl darytina prielaida, jog prievado tikslas susijęs su „Hikvision Cloud“. „Hikvision“ dokumentacija apibrėžia, kad 8000 prievado paskirtis yra vartotojo dalies komunikacija su PCNVR serveriu.
5	8443/TCP	TCPWRAPPED	Atliekant prisijungimą, įvyksta TCP duomenų apsikeitimas (angl. Handshake), tačiau po jo prievadas nutraukia ryšį. Nustatyta paslauga – „tcpwrapped“.

Tyrimo metu 8000 prievado paskirties nepavyko nustatyti, tačiau pagal komunikacijos duomenis, šis prievadas yra specializuota valdymo sąsaja, turinti realizuotą prieigos kontrolės sąrašo (angl. Access-control list, ACL) funkcionalumą. Tyrimo metu prievadui buvo siunčiami paketai, kuriuos apdorojus kamera staiga užbaigdavo ryšį. Tyrimo ryšio seanso išrašas pateiktas 7 paveiksle. Būdamas atviras ir neapsaugotas šis prievadas gali būti išnaudotas atliekant buferio perpildymo ar kenkėjiško kodo įdiegimo kibernetines atakas.

7 pav. „Hikvision“ kameros ryšio seanso išrašas

„Hikvision“ kameros administravimo panelė nepalaiko visų naujausių interneto naršyklių versijų. Tyrimo metu buvo išbandyta 13 įvairių versijų naršyklių, veikiančių skirtingose operacinėse sistemose. Pastebėta, kad administravimo panelė korektiškai veikė su jau nebepalaikomomis ir saugumo spragų turinčiomis naršyklės, sukurtomis 2012 – 2016 m. Tikėtina tai susiję su kameros gamybos laikotarpiu 2016 – 2018 m. ir vėlesnio laikotarpio technologinio palaikymo trūkumu. Tikimės, kad šio tyrimo rezultatai įtakos gamintoją produkto kokybei ir saugumui skirti adekvatų technologinio palaikymo lygį.

Tyrimo metu su „Hikvision“ kamera išbandytų naršyklių sąrašas, nurodant jų sukūrimo metus ir funkcionavimo galimybes, pateiktas 3 lentelėje.

3 lentelė. Tyrimo metu su „Hikvision“ kamera išbandytų naršyklių sąrašas nurodant jų sukūrimo metus ir funkcionavimo galimybes

Eil. Nr.	Naršyklė, versija, operacinė sistema	Naršyklės agentas	Išleidimo data	Pavyko naudotis kameros valdymo panele
1	Firefox 75 Linux	Mozilla/5.0 (X11; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0	2020	Ne
2	Firefox 75 Windows	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0	2020	Ne
3	Chrome 81 Linux	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36	2020	Ne
4	Opera 69	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/82.0.4062.3 Safari/537.36 OPR/69.0.3623.0 (Edition developer)	2020	Ne
5	Safari 12 Mac OS X	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4 Supplemental Update) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15	2019	Taip
6	Edge 44	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/18.17763	2019	Ne
7	Firefox 56	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0	2017	Ne
8	Opera 12.14	Opera/12.80 (Windows NT 5.1; U; en) Presto/2.10.289 Version/12.02	2016	Taip
9	Firefox 33	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20120101 Firefox/33.0	2014	Taip
10	Chrome 34	Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36 Mozilla/5.0 (iPad; U; CPU OS 3_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B334b Safari/531.21.10	2014	Taip
11	Internet Explorer 11	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	2013	Taip
12	Safari 7	Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/537.75.14 (KHTML, like Gecko) Version/7.0.3 Safari/7046A194A	2013	Taip
13	Chrome 19	Mozilla/5.0 (Windows NT 6.0) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.36 Safari/536.5	2012	Taip

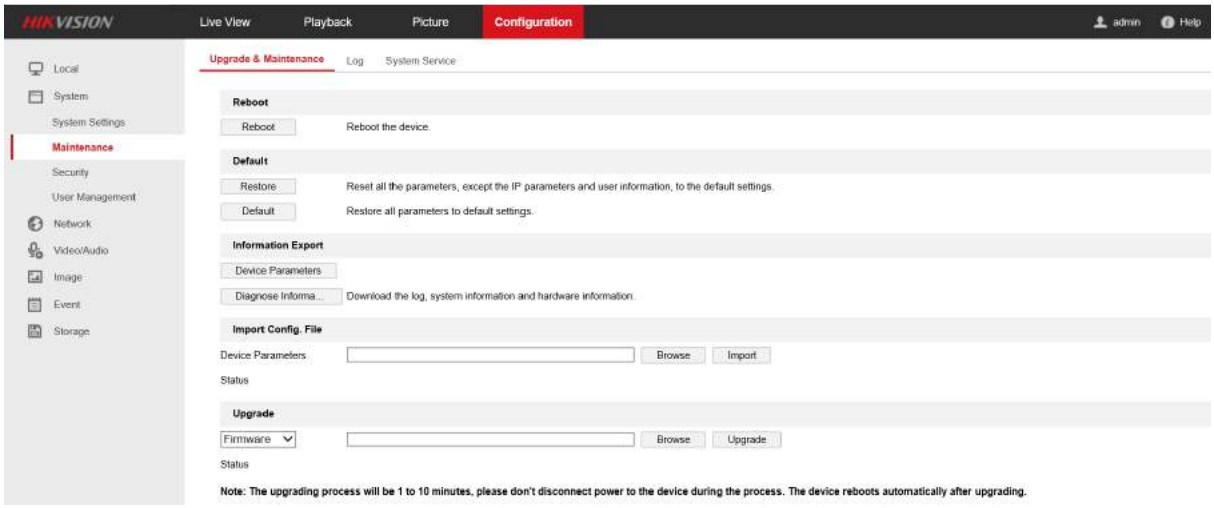
Kameros administravimo panelė suteikia galimybę naršyklėje stebėti fiksuojamą vaizdą. Nustatyta, kad norint matyti vaizdą, reikalingi „ActiveX“ technologijos plėtiniai, kuriuos galima parsisiųsti iš „Hikvision“ kameros. „ActiveX“ technologiniai plėtiniai naujose naršyklėse nėra palaikomi dėl žinomų kibernetinio saugumo spragų [20], todėl jų naudojimas yra nerekomenduojamas.

Situaciją su tiriamu „Hikvision“ kameros modeliu atspindi toks faktas, kad „Hikvision“ saugumo tyrimų centro (HSRC) platinami saugumo biuleteniai, kurių paskutinis datuojamas 2018 m. ir yra skirtas programinės įrangos versijai V5.5.53 [23], t .y. faktiškai tai senesnė nei konkrečiai tirto modelio versija V5.5.84.

4. „Hikvision“ kameroje nėra automatinio atnaujinimo funkcionalumo, naujinimų infrastruktūra išdėstyta Kinijos ir Rusijos serveriuose

Kameroje nebuvo rasta automatinio atnaujinimo funkcionalumo, naujinimai turi būti atsisiųsti ir įdiegti rankiniu būdu. Remiantis geolokacijos IP duomenų bazių informacija, kameros atnaujinimo nuoroda patalpinta „Hikvision“ puslapyje, esančiame Kinijoje registruotame serveryje, nukreipianti į Rusijoje registruotą serverį, iš kurio siunčiama į kamerą diegiama atnaujinimo rinkmena.

Šiuose serveriuose galimai yra registruojamos iš vartotojų atėjusios užklausos, leidžiančios nusakyti vartotojo IP adresą, šalį, užklausos laiką, atsisiunčiamo naujinimo versiją. „Hikvision“ administravimo panelės naujinimų diegimo sąsajos vaizdas pateiktas 8 paveiksle.



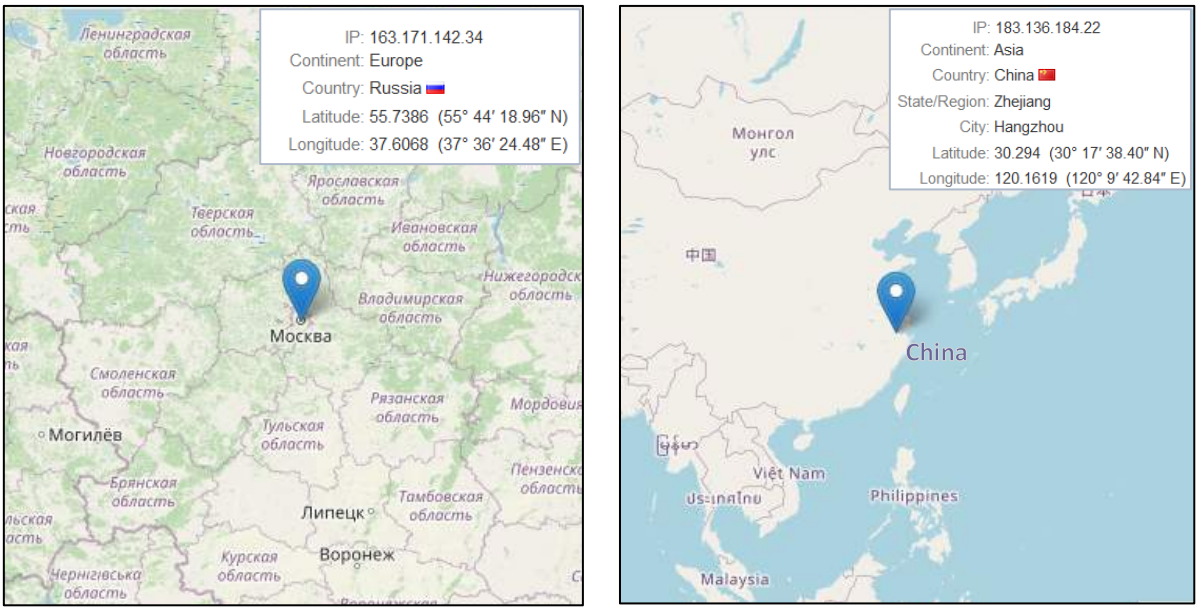
8 pav. „Hikvision“ administravimo panelės naujinimų diegimo sąsajos vaizdas

4 lentelėje pateiktas atnaujinimo adresų sąrašas, nurodant IP adresus ir šalis, nustatytas iš geolokacijos žinių bazių.

4 lentelė. „Hikvision“ kamerai taikomų naujinimų adresai

Eil. Nr.	Atnaujinimo adresas	IP adresas	Šalis
1	https://www.hikvision.com/en/products/IP-Products/Network-Cameras/Ultra-Series-SmartIP-/ds-2cd4c26fwd--ap-/	183.136.184.22	Hangzhou, Zhejiang,China, Asia
2	https://www.hikvision.com/content/dam/hikvision/en/support/download/firmware/ipc/4-series/ds-2cd4cx6fwd/firmware/IPC_R7_EN_STD_5.5.83_190218.zip	163.171.142.34	Rusija

9 paveiksle pateiktas kartografinis nustatytų šalių vaizdas, pažymint IP adresą.



9 pav. „Hikvision“ kameros atnaujinimų serverių geolokacijos vaizdai

Lietuvos Respublikos Valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos 2018 m. Grėsmių nacionaliniam saugumui vertinimo teigiama: *„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.“*.

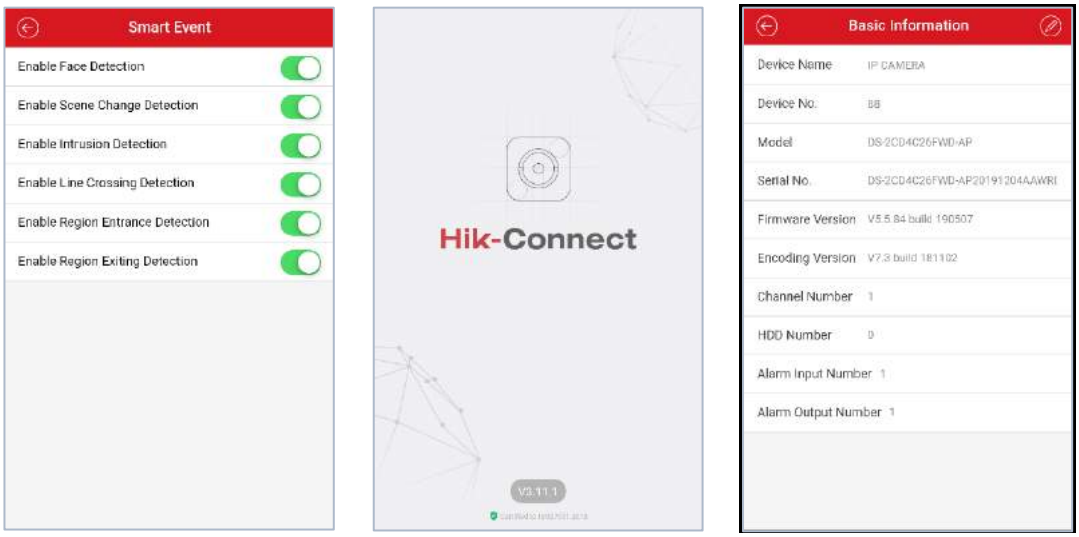
Dėl galimai paliekamų įrašų atnaujinimų serveriuose, kai kameros naudojamos Lietuvoje, rekomenduojama riboti programinės įrangos siuntimąsi iš šalių, kuriose negalioja BDAR reglamentas.

5. Nustatyta, kad „Hikvision“ parengta kamerų valdymo mob. aplikacija „Hik-Connect“ vykdo sujungimus su Kinija, Tailandu, Singapūru, Airija, registruoja SIM kortelės IMSI ir ICCID identifikacinius numerius bei mobilaus įrenginio IMEI identifikacinį numerį

Kamerų valdymo galimybėms išplėsti gamintojas „Hikvision“ siūlo mob. aplikaciją „Hik-Connect“ (tirta versija: 3.11.1.1023). Apibendrinus šios aplikacijos veikimo tyrimą, tiesioginių kibernetinio saugumo spragų nenustatyta, tačiau registruota, kad mob. aplikacija vykdo sujungimus su 9 IP adresais, esančiais Airijoje, Kinijoje, Singapūre, Tailande. Aplikacija taip pat renka vartotojo įrenginio informaciją, kaip SIM kortelės IMSI ir ICCID identifikacinis numeris bei mobilaus įrenginio IMEI identifikacinis numeris, kurios rinkimo tikslai nėra aiškūs. Tikėkimės, kad gamintojas atsižvelgs į tyrimo rezultatus ir teiksis plačiau paaiškinti kam ir kodėl renkama ši vartotojų įrenginių informacija.

Aplikacija skirta kameros vaizdui peržiūrėti, kamerai konfigūruoti, daryti nuotraukas ir vaizdo įrašus, turi galimybę perduoti garsą „Intercom“ tipo režimu (kamera ↔ telefonas), WiFi nustatymų atvaizdavimui QR kodais.

„Hik-Connect“ aplikacijos vaizdų pavyzdžiai pateikti 10 paveiksle.



10 pav. „Hikvision“ aplikacijos „Hik-Connect“ vaizdai

„Hik-Connect“ programiniai paketai veikia įvairiose aparatinėse bazėse – mob. telefonuose, planšetiniuose kompiuteriuose ir kituose, „Android“ ir „iOS“ platformas palaikančiuose įrenginiuose. Mobilioji aplikacija „Hik-Connect“ nemokamai prieinama elektroninėse Google „Play“ ir Apple „App Store“ mob. programų parduotuvėse.

5 lentelėje pateikti mob. aplikacijos „Hik-Connect“ reikalavimai prieigai, nurodant prieigos paskirtį. Nustatyta, kad aplikacija reikalauja 5-ių tipų – kameros, mikrofono, duomenų saugyklos, telefono nustatymų, vietovės informacijos.

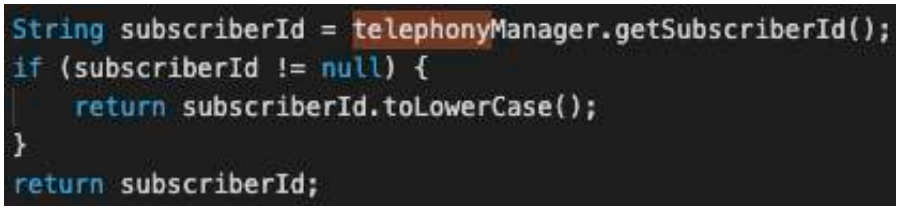
5 lentelė. „Hik-Connect“ reikalavimų prieigai sąrašas, nurodant prieigos paskirtį

Eil. Nr.	Reikalavimai prieigai	Prieigos paskirtis
1	Kameros prieiga	QR kodų skenavimui
2	Mikrofono prieiga	Garso perdavimui į kamerą
3	Duomenų saugykla	Nuotraukų ir vaizdo įrašų saugojimas telefono atmintyje
4	Telefono nustatymai	Mobilaus interneto ryšio stiprumo nustatymas
5	Vietovės informacija	Reikalingas norint gauti prieigą prie įrenginio naudojamos WiFi stoties nustatymų nuskaitymo

Atlikus kodo dekompoziciją, nustatyti mob. aplikacijos kodo fragmentai, sudarantys sąlygas platesnės informacijos rinkimui. 11 – 13 paveiksluose pateikti mob. aplikacijos programinio kodo fragmentai, kuriuose atsispindi galimas informacijos rinkimo funkcionalumas – SIM kortelės IMSI ir ICCID identifikaciniai numeriai bei mobilaus įrenginio IMEI identifikacinis numeris.

```
String deviceId = telephonyManager.getDeviceId();
if (deviceId != null) {
    return deviceId.toLowerCase();
}
return deviceId;
```

11 pav. getDeviceId() funkcija – mob. įrenginio IMEI identifikacinio numerio gavimo kodo fragmetnas



12 pav. getSubscriberID() – SIM kortelės IMSI identifikacinio numerio gavimo kodo fragmentas

13 pav. getSimSerialNumber() – SIM kortelės ICCID identifikacinio numerio gavimo kodo fragmentas

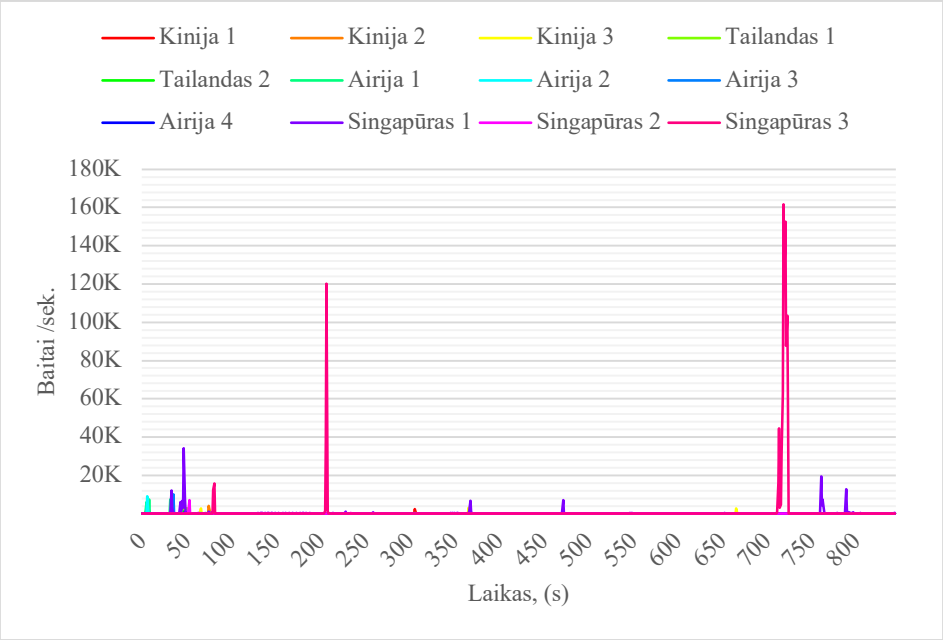
Atlikus „Hik-Connect“ mob. aplikacijos siunčiamų srautų analizę, nustatyta, kad aplikacija vykdo sujungimus su 9 IP adresais, esančiais Airijoje, Kinijoje, Singapūre, Tailande. Pirmą kartą paleidus „Hik-Connect“ aplikaciją, stebėtas santykinai didelis programėlės aktyvumas – 13 min. laikotarpyje buvo išsiųsta 165,367 kB, gauta – 70,647 kB duomenų. Tyrimas buvo atliktas „Android“ platformoje.

Duomenų perdavimo traktas buvo šifruotas. Nustatyta, kad adresu „sgplog.hik-connect.com“ buvo siunčiamos „Stun“ konfigūracijos JSON formatu, t. y. įvykių registracijos žurnalų informacija. Tinklo trakto informacija pateikta 6 lentelėje.

6 lentelė. „Hik-Connect“ duomenų mainų informacija, pirmojo paleidimo metu, 13 min. periode

Eil. Nr.	Adresas	Domenai	Paskirtis	Šalis	Siųstų duomenų kiekis, Baitai	Gautų duomenų kiekis, Baitai
1	34.253.44.101	api.hik-connect.com apieu-hik-connect-1187713652.eu-west-1.elb.amazonaws.com	Nežinoma	Airija	18567	5244
2	34.255.15.112	download.ezvizops.com	Nežinoma	Airija	8274	2076
3	47.74.230.132	apiisgp.hik-connect.com aliapisgp-hik-connect.com	Nežinoma	Singapūras	124058	34842
4	52.212.179.170	api.hik-online.com	Nežinoma	Airija	443	623
5	54.246.236.96	log.ezvizlife.com	Aplikacijos įvykių žurnalų siuntimas	Airija	7362	2198
6	150.109.178.162	–	Stun	Tailandas	0	14325
7	150.109.183.230	–	Stun	Tailandas	478	1910
8	161.117.5.66	sgplog.hik-connect.com sgplog.ezvizlife.com	Analitinių duomenų siuntimas	Kinija	1785	8118
9	203.205.239.188	rqd.sparta.mig.tencent-cloud.net android.bugly.qq.com	Bugly klientas	Kinija	4400	1311

Tinklo trakto grafikas pateiktas 14 paveiksle.



14 pav. Mob. aplikacijos „Hik-Connect“ duomenų mainų trakto grafikas pirmojo paleidimo metu

Mob. aplikacijai veikus ilgesnį laiko tarpą, aplikacija atlieka duomenų mainus su 5 IP adresais, pateiktais 7 lentelėje.

7 lentelė. Nusistovėjusios mob. aplikacijos „Hik-Connect“ kreipiniai

Eil. Nr.	Adresas	Domenai	Paskirtis	Šalis	Siųstų duomenų kiekis, Baitai	Gautų duomenų kiekis, Baitai
1	3.210.86.43	hiddns-1976889542.us-east-1.elb.amazonaws.com	Nenustatyta	JAV	578930	67801
2	3.223.178.216	usdclog-1571272846.us-east-1.elb.amazonaws.com		JAV	7737	3137
3	47.74.230.132	aliapisgp.hik-connect.com		Singapūras	19638	5283
4	52.22.111.191	usdclog-1571272846.us-east-1.elb.amazonaws.com		JAV	17789	18069
5	203.205.239.188	rqd.sparta.mig.tencent-cloud.net	Bugly klientas	Kinija	2384	9270

Sugretinus pirmojo paleidimo ir nusistovėjusios aplikacijos kreipinius, nustatyta, kad aplikacijoje yra du sutampantys IP adresai. 8 lentelėje pateikti sutapę IP adresai, pažymint į juos nukreipto srauto turinį.

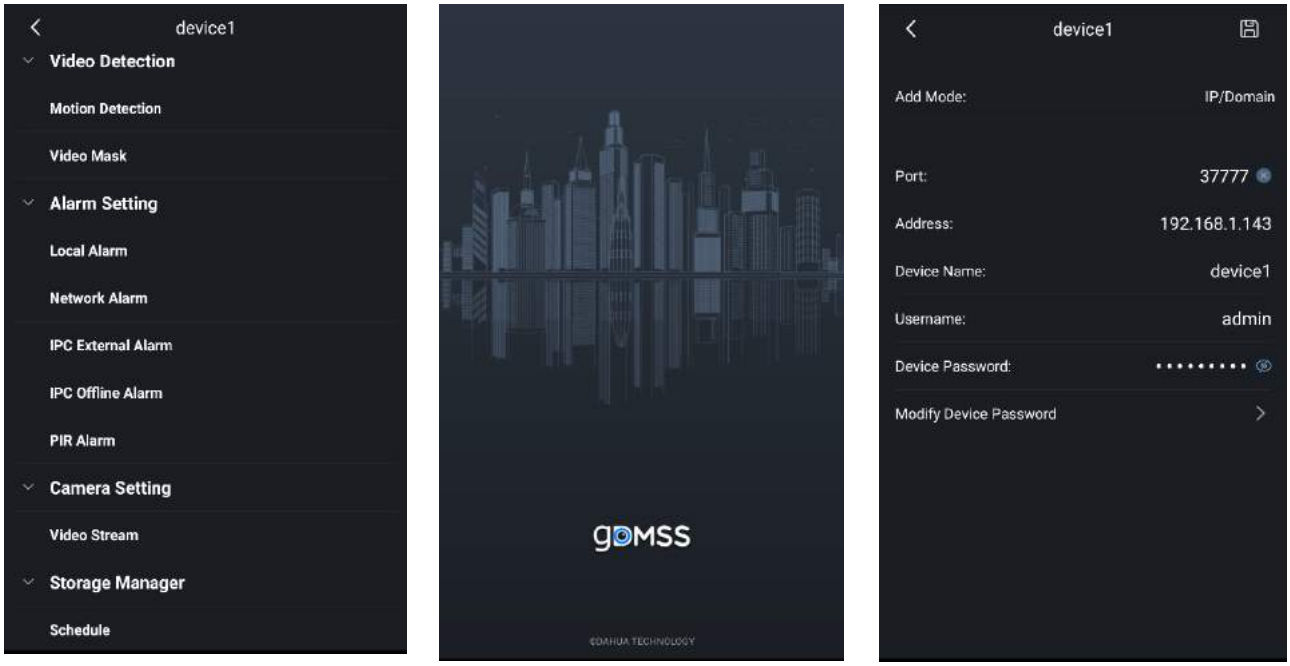
8 lentelė. „Hik-Connect“ sutapusių IP adresų sąrašas, pažymint į juos nukreipto srauto turinį

Eil. Nr.	IP adresas	Šalis	Srauto turinys
1	47.74.230.132	Singapūras	TLSv1.2 šifruotas turinys, kreipiasi į apiisgp.hik-connect.com
2	203.205.239.188	Kinija	HTML srautas, siunčia aplikacijos registracijos žurnalų informaciją

Pažymime, kad Android OS platformoje skirta naudoti mob. aplikacija „Hik-Connect“, esanti Google „Play“ el. parduotuvėje, 2020-04-28 Lietuvoje nebebuvo pasiekiama. Pokyčių mob. aplikacijų el. parduotuvėje Apple „AppStore“ nebuvo pastebėta, iOS įrenginiams skirtą aplikaciją buvo galima atsiųsti ir įsidiegti.

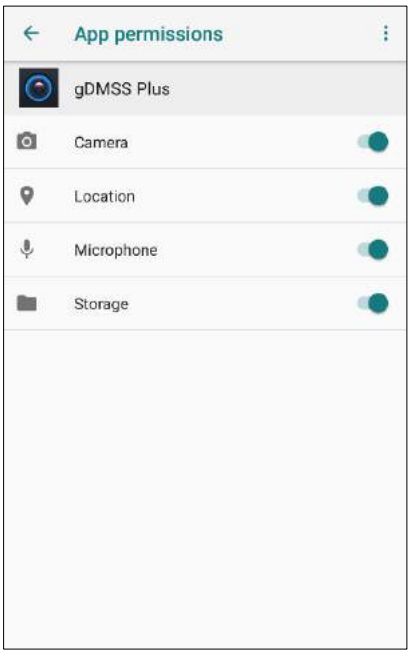
6. „Dahua“ kameros mob. aplikacja „gDMSS Plus“ vykdo sujungimus su Kinija, Vokietija, JAV. Priklausomai nuo šalies, aplikacija geba selektyviai vykdyti funkcijas

Kamerų valdymo galimybėms išplėsti gamintojas „Dahua“ siūlo mob. aplikaciją „gDMSS Plus“ (tirta versija: 4.90.000). Apibendrinus šios aplikacijos veikimo tyrimą, tiesioginių kibernetinio saugumo spragų nenustatyta, tačiau registruota, kad mob. aplikacija vykdo sujungimus su 26 IP adresais, esančiais JAV, Vokietijoje ir Kinijoje. Nustatyta, kad mob. aplikacija, priklausomai nuo šalies, kurioje veikia, geba selektyviai vykdyti funkcijas. „gDMSS Plus“ mob. aplikacijos vaizdai pateikti 15 paveiksle.



15 pav. „Dahua“ aplikacijos „gDMSS Plus“ vaizdai

Aplikacija reikalauja prieigos teisių prie 5 mobiliojo įrenginio posistemių – kameros, vietovės, mikrofono ir duomenų saugyklos. Aplikacijos prieigos reikalavimų langas pateiktas 16 paveiksle.



16 pav. „Dahua“ aplikacijos „gDMSS Plus“ vaizdas. Reikalavimai prieigai

Mob. aplikacija „gDMSS Plus“ vykdo kreipinius į 26 IP adresus, esančius JAV, Vokietijoje ir Kinijoje. Mobiliosios aplikacijos kreipinių adresai pateikti 9 lentelėje.

9 lentelė. „gDMSS Plus“ duomenų mainų informacija

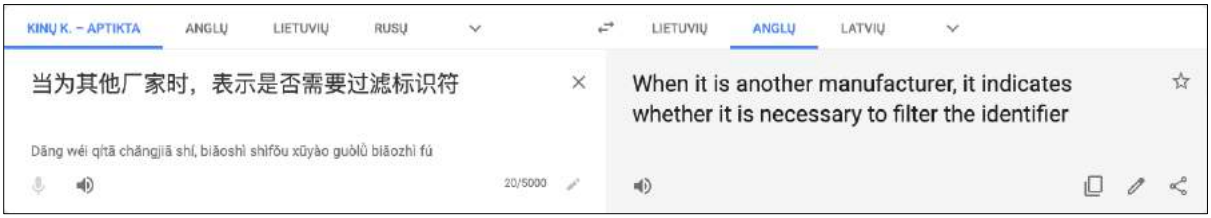
Eil. Nr.	Adresas	Domenai	Šalis	Gautų duomenų kiekis (Baitais)	Siųstų duomenų kiekis (Baitais)
1	8.209.64.86	–	Vokietija	0	74
2	8.209.76.211	–	Vokietija	0	74
3	13.52.30.245	www.easy4ipcloud.com	JAV	0	74
4	18.194.4.59	appservices-fk.easy4ipcloud.com	Vokietija	12417	5250
5	18.195.71.118	app-vpc-fk.easy4ipcloud.com	Vokietija	13764	4265
6	18.195.191.151	app-vpc-fk.easy4ipcloud.com	Vokietija	0	751401
7	35.166.79.94	appservices-or.easy4ipcloud.com	JAV	0	6570
8	47.91.78.28	–	Vokietija	0	74
9	47.91.87.124	–	Vokietija	0	74
10	47.91.91.46	–	Vokietija	0	74
11	47.91.93.246	–	Vokietija	38016	149785
12	47.91.95.169	–	Vokietija	72298	134224
13	47.254.146.226	–	Vokietija	0	74
14	47.254.171.9	–	Vokietija	0	1200
15	52.8.60.34	www.easy4ipcloud.com	JAV	0	74
16	52.41.182.28	mobile-server-or-470527425.us-west-2.elb.amazonaws.com	JAV	305729	21817
17	52.57.50.253	app-vpc-fk.easy4ipcloud.com	Vokietija	376342	53960
18	54.215.119.215	www.easy4ipcloud.com	JAV	0	74
19	54.241.202.176	www.easy4ipcloud.com	JAV	0	74
20	54.241.203.224	www.easy4ipcloud.com	JAV	422	385
21	116.62.177.243	www.dahuap2pcloud.com	Kinija	209	146
22	118.178.90.50	–	Kinija	47881	305392
23	118.178.252.108	www.dahuap2pcloud.com	Kinija	208	73
24	121.40.103.45	–	Kinija	127789	311944
25	184.169.249.245	–	JAV	876	2388
26	223.6.252.231	–	Kinija	14120	6530

Tyrimų metu buvo atlikta mob. aplikacijos programinio kodo dekompozicija. Nustatyta, kad priklausomai nuo šalies, įrenginio gamintojo ar kitų parametrų, mob. aplikacija keičia savo elgseną. 10 lentelėje pateiktas programinio kodo pavyzdys, kinų kalboje esantys komentarai (nevykdomos programinio kodo vietos) išversti 17 paveiksle.

10 lentelė. „gDMSS Plus“ aplikacijos programinio kodo segmentas

```
<OEMRestrict>
        <!—基线版本为DH →
        <identifier>DH</identifier>
        <!—当为其他厂家时，表示是否需要过滤标识符 →
        <isIdentifier>false</isIdentifier>
        <!—door 模块，alarm 模块是否存在 →
        <enableDoorAlarm>true</enableDoorAlarm>
</OEMRestrict>
```

19 paveiksle atliktas kinų kalboje esančių programinio kodo komentarų vertimas laisvai prieinama Google priemone „Google Translator“ [21].



17 pav. Išverstas programinio kodo segmentas

Išverstame mob. aplikacijos „gDMSS Plus“ kometare nurodoma: „Kai nustatytas kitas gamintojas, reikalinga filtruoti identifikatorių“. 11 ir 12 lentelėse programinio kodo dalis, naudojanti minėtus identifikatorius.

11 lentelė. „gDMSS Plus“ aplikacijos programinio kodo segmentas

```
java.lang.String r1 = "PushSelfShowLog"
java.lang.StringBuilder r2 = new java.lang.StringBuilder
r2.<init>()
java.lang.String r3 = "not EMUI system or not in China, open google play web, referrer: "
java.lang.StringBuilder r2 = r2.append(r3)
java.lang.StringBuilder r2 = r2.append(r0)
java.lang.String r2 = r2.toString()
com.huawei.hms.support.log.a.b(r1, r2)
```

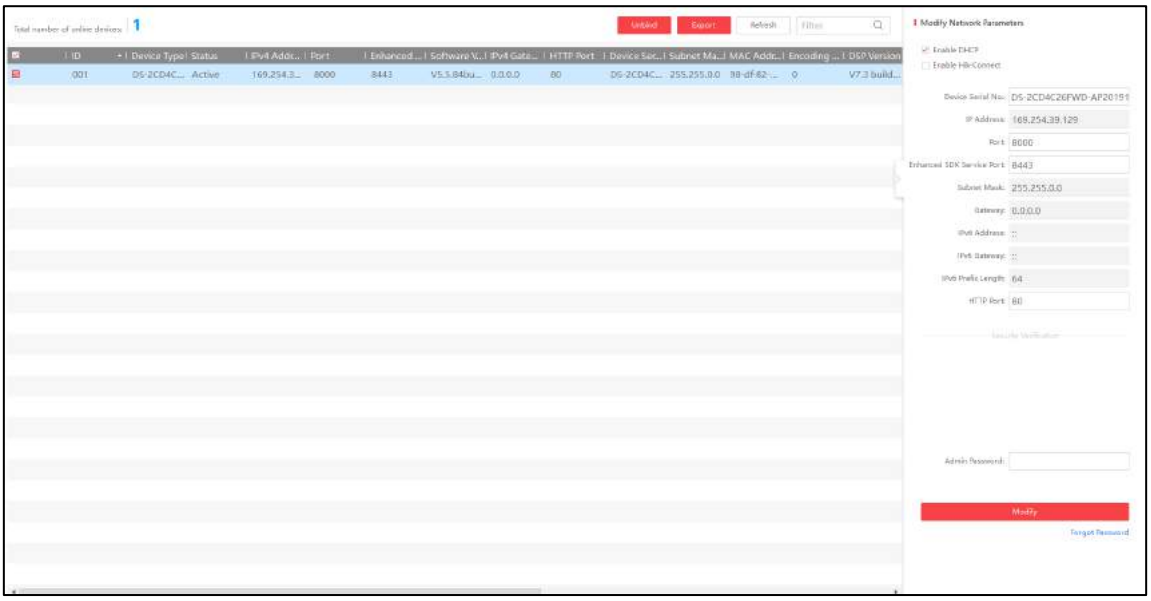
12 lentelė. „gDMSS Plus“ aplikacijos programinio kodo segmentas

```
java.lang.String r0 = "PushSelfShowLog"
java.lang.StringBuilder r2 = new java.lang.StringBuilder
r2.<init>()
java.lang.String r3 = "It is China device, open Huawei market web, referrer: "
java.lang.StringBuilder r2 = r2.append(r3)
java.lang.StringBuilder r2 = r2.append(r1)
```

Galima teigti, kad aplikacija seka indikacinių parametrų pokytį ir priklausomai nuo jų verčių, gali pakeisti savo funkcionalumą.

7. Kamerų infrastruktūroje naudojami uždari, nestandartiniai protokolai

Nustatyta, kad „Hikvision“ savo gaminių aptikimui tinklo infrastruktūroje naudoja uždarą SADP (angl. Search Active Device Protocol) protokolą, kuris nėra šifruojamas. SADP kilmę pagrindžiančių šaltinių nebuvo rasta, jo specifikacija uždara ir viešai neprieinama. „Hikvision“ kamerų aptikimui naudojamas programinis įrankis „SADP Tool“, veikiantis minėtu SADP protokolu. „SADP Tool“ įrankio vaizdas pateiktas 18 paveiksle.



18 pav. „Hikvision“ kamerų aptikimui taikomo programinio įrankio „SADP Tool“ vaizdas

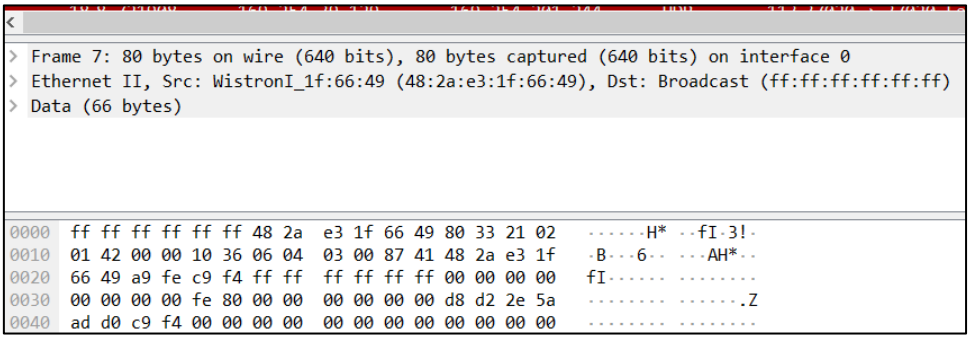
Atliekant įrenginių paiešką, programinė įranga „SADP Tool“ tinklui siunčia nešifruotus UDP protokolo transliuojamuosius (angl. Broadcast) paketus, turinčius XML struktūrą. 13 lentelėje pateiktas transliuojamo UDP paketo vaizdas.

13 lentelė. „SADP Tool“ transliuojamo UDP paketo turinys

```
<?xml version="1.0" encoding="utf-8"?>
<Probe>
<Uuid>2D551517-4514-4213-AD57-843B12920D34</Uuid>
<Types>inquiry</Types>
</Probe>
```

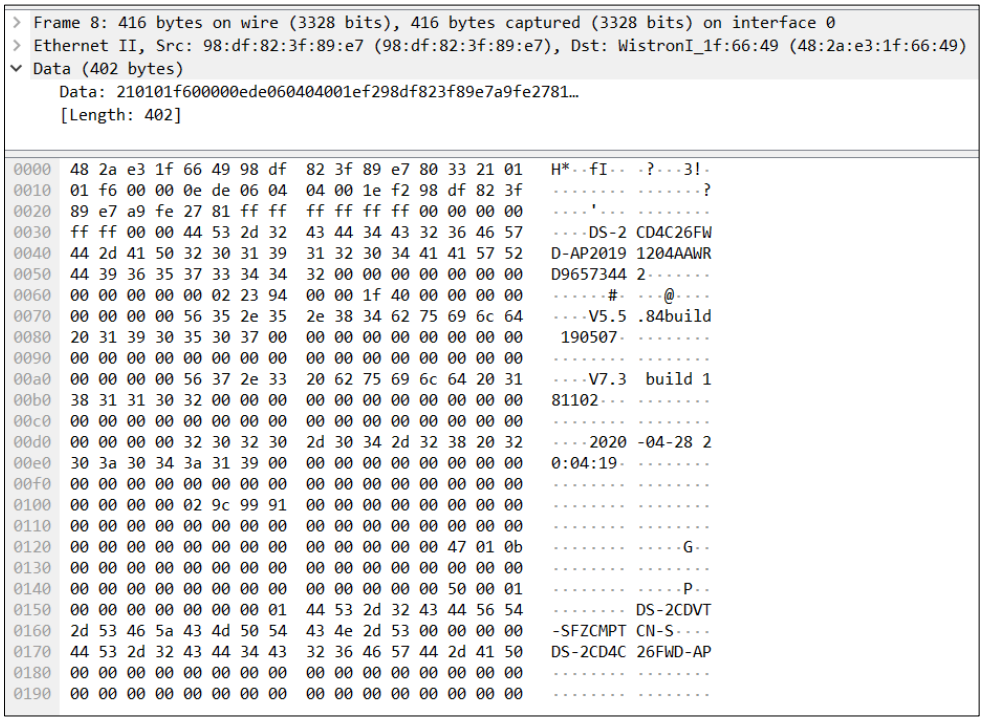
Tai yra užklausos (angl. „Inquiry“) paketas, turinti unikalią identifikacinę vertę „<Uuid>2D551517-4514-4213-AD57-843B12920D34</Uuid>“, kuri naudojama sinchronizuotam kameros atsakui į gautą „SADP Tool“ užklausą.

Papildomai „SADP Tool“ išsiunčia 80 baitų Ethernet kadrus (angl. Frames) (66 baitų turinio) su specifiniu, nestandartiniu EtherType (0x8033) kadro tipu. IEEE ši verte registruota VIA Systems (*http://standards-oui.ieee.org/ethertype/eth.txt*). Siunčiami baitai neatitinka ASCII išraiškos. Siunčiamų Ethernet kadrų vaizdas pateiktas 19 paveiksle.



19 pav. „SADP Tool“ papildomai siunčiamo 66 baitų turinio Ethernet kadro vaizdas

Nustatyta, kad kamera į siunčiamas užklausas atsako per Ethernet paketus ir per UDP protokolą. Ethernet pakete yra pateikiamas kameros modelis, aparatinės įrangos versija ir data. Per UDP protokolą siunčiami likusieji parametrai, kurie reikalingi kameros valdymui (kameros IP adresas, aktyvus prievadas). Srauto dekonstrukcijos vaizdas pateiktas 20 paveiksle.



20 pav. Dekonstruoto srauto vaizdas

Dekonstruotas UDP srauto turinys pateiktas 14 lentelėje.

14 lentelė. Dekonstruotas UDP srauto turinys

```
<?xml version="1.0" encoding="UTF-8"?>
<ProbeMatch>
<Uuid>2D551517-4514-4213-AD57-843B12920D34</Uuid>
<Types>inquiry</Types>
<DeviceType>140180</DeviceType>
<DeviceDescription>DS-2CD4C26FWD-AP</DeviceDescription>
<DeviceSN>DS-2CD4C26FWD-AP20191204AAWRD96573442</DeviceSN>
<CommandPort>8000</CommandPort>
<HttpPort>80</HttpPort>
<MAC>98-df-82-3f-89-e7</MAC>
<IPv4Address>169.254.39.129</IPv4Address>
<IPv4SubnetMask>255.255.0.0</IPv4SubnetMask>
<IPv4Gateway>0.0.0.0</IPv4Gateway>
<IPv6Address>::</IPv6Address>
<IPv6Gateway>::</IPv6Gateway>
<IPv6MaskLen>64</IPv6MaskLen>
<DHCP>true</DHCP>
<AnalogChannelNum>0</AnalogChannelNum>
<DigitalChannelNum>1</DigitalChannelNum>
<SoftwareVersion>V5.5.84build 190507</SoftwareVersion>
<DSPVersion>V7.3 build 181102</DSPVersion>
<BootTime>2020-04-28 20:04:19</BootTime>
<Encrypt>true</Encrypt>
<ResetAbility>false</ResetAbility>
<DiskNumber>0</DiskNumber>
<Activated>true</Activated>
<PasswordResetAbility>true</PasswordResetAbility>
<PasswordResetModeSecond>true</PasswordResetModeSecond>
```

<DetailOEMCode>1</DetailOEMCode>
<SupportSecurityQuestion>true</SupportSecurityQuestion>
<SupportHCPlatform>true</SupportHCPlatform>
<HCPlatformEnable>true</HCPlatformEnable>
<IsModifyVerificationCode>flase</IsModifyVerificationCode>
<Salt>c453b4260140373c9836b6eaa2deebcc732c611a3dee061933e9872c7a4a1ffd</Salt>
<DeviceLock>true</DeviceLock>
<SDKServerStatus>false</SDKServerStatus>
<SDKOverTLSServerStatus>false</SDKOverTLSServerStatus>
<SDKOverTLSPort>8443</SDKOverTLSPort>
</ProbeMatch>

Kamerai atsakius, užmezgamas ryšys su „SADP Tool“ aplinka, pradedama autentifikacijos procedūra. Vartotojui vedant slaptažodį „SADP Tool“ aplinkoje, jis (ir kiti kamerą nusakantys parametrai) išsiunčiami įrenginiui. Atsakymo žinutės vaizdas, kurioje atsispindi užšifruotas slaptažodis ir kiti kamerą nusakantys parametrai, pateiktas 15 lentelėje.

15 lentelė. Autentifikacijos procedūra. Atsakymo žinutės vaizdas

<?xml version="1.0" encoding="utf-8"?>
<Probe>
<Uuid>C1B9469F-4AF3-4C2D-A804-1914B20856C2</Uuid>
<Types>update</Types>
<PWErrorParse>true</PWErrorParse>
<MAC>98-df-82-3f-89-e7</MAC>
<Password
bSalt="true">07KxrTkVovYOpNhRU9PT86VsXjJKixPAbDr4hT35PSQOjXUfoDucDuDExMvl0CYhHpJw
K0KtLdfQpOOJTzSiGA==</Password>
<IPv4Address>169.254.39.129</IPv4Address>
<CommandPort>8000</CommandPort>
<HttpPort>80</HttpPort>
<IPv4SubnetMask>255.255.0.0</IPv4SubnetMask>
<IPv4Gateway>0.0.0.0</IPv4Gateway>
<IPv6Address>::</IPv6Address>
<IPv6Gateway>::</IPv6Gateway>
<IPv6MaskLen>64</IPv6MaskLen>
<DHCP>true</DHCP>
<SDKOverTLSPort>8443</SDKOverTLSPort>
</Probe>

Komunikcija tarp „SADP Tool“ ir „Hikvision“ kameros vykdoma nešifruotu ryšiu, todėl egzistuoja galimybė perimti kameros tinklo traktą nusakančią informaciją ir užšifruotą slaptažodį.

Hikvision kameros turi galimybę būti integruotos į kitas informacines sistemas panaudojant „Hikvision-CGI“ aplinką arba ONVIF (Open Network Video Interface Forum) sąsają. Apie tai kaip vyksta integracija į CGI aplinką informacijos nėra daug. ONVIF yra pramoninis IP technologija veikiančių saugos (IP kameros, NVR, vaizdo registratoriai ir kt.) produktų integravimo standartas, tačiau, remiantis internetiniais šaltiniais [24], „Hikvision“ 2019 m. spalį buvo pašalinta iš šios organizacijos.

8. „Dahua“ kameroje tarnybinio ryšio užmezgimas vykdomas per išorines sistemas

Nustatyta, kad „Dahua“ kameroje veikia SSH (*angl.* Secure Shell) šifruoto komandinio ryšio servisas, kuris pagal nutylėjimą yra išjungtas. Įjungus jį, galimas šifruotas SSH ryšys su kamera standartiniu, 22-uoju prievadu. SSH vartotojo vardas – „admin“, o specializuotas SSH slaptažodis sudaromas prie simbolių sekos „7ujMko0“ pridėjus bendrosios „admin“ vartotojo paskyros slaptažodį.

Prisijungus prie SSH serviso, gaunamos 4-ių informacinio pobūdžio komandų sąrašas. SSH aplinkos vaizdas pateiktas 21 paveiksle.

21 pav. „Dahua“ kameros SSH aplinkos vaizdas

Komanda „getDateInfo“ išveda įrenginio datą, „diagnose“ pateikia tarnybinę informacija apie sistemos konfigūraciją, „help“ išveda 4-ių pavaizduotų informacinių komandų sąrašą, „shell“ komanda gali būti naudojama gauti pilną komandinę eilutę, tačiau ji yra prieinama tik „Dahua“ atstovams.

Vartotojui, suvedusiam „shell“ komandą, yra pateikiamas prašymas įvesti savo „domeno paskyros“ (angl. „Domain Account“) pavadinimą. Jį suvedus (tyrimo atveju, „8888“ yra galiojantis paskyros pavadinimas), ekrane yra pateikiamas QR kodas. Išvesto QR kodo vaizdas pateiktas 22 paveiksle.

22 pav. „Dahua“ kameros SSH aplinkoje išvestas QR kodas

Nuskenavus QR kodą, gaunamas sekantis URL adresas: „https://svsh.dahuatech.com/svsh.html?v=2&u=8888&t=mGctcVCqd3f9j46zg%2FUPVkMtF5p03hrqBYkcjuPdr%2F9mduZBq1dDVvYINXMYNZw%2BFQzawHliCyyVtbnoE3w6wUXI9wdvjiDSVYz5JzZeiXjC7%2FB5Jne3ZBk7lb6sNFU8qnV45TgkOoKWkBCvKK4ixW9g1nH0MOaXBBgSd3o24YM81PQL5iSV6yX72T%2FrCrNMqAmdt8nE46syeBxPxcFVydCu835LAvAtFHDlth23FfWN5Bq%2BDAQ%2Ft7xmmS4znVOFGhG3OZL%2Blq4aZi%2FbSMKNd5lMOqv1s1%2FV0kY9OvicgacX8tBGQxXXNicbit23hALhECp5RIqNKX41LufA0nhAfw%3D%3D“. Naršyklėje aktyvavus nurodytą adresą, vartotojui yra pateikiamas prisijungimo langas, kuriame jo prašoma įvesti savo domeno slaptažodį. Šio slaptažodžio kilmė nėra žinoma, tačiau tikėtina jog tai yra „Dahua“ atstovo slaptažodis. Slaptažodžio įvesties formos vaizdas, gaunamas aktyvavus nuorodą, pateikta 23 paveiksle.

23 pav. Slaptažodžio įvesties forma nuotolinėje „Dahua“ aplinkoje

Aptartas kameros prieigos funkcionalumas skirtas „Dahua“ atstovams prisijungti prie kamerų nuotoliniu būdu, kad atlikti aptarnavimo darbus. Tam kameroje yra integruota specializuota „Dahua“ duomenų bazė ar identifikavimo mechanizmas, įgalinantis aukštos privilegijos nuotolinį prisijungimą

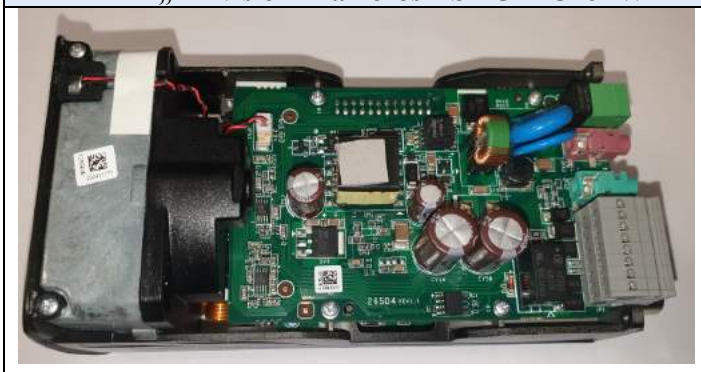
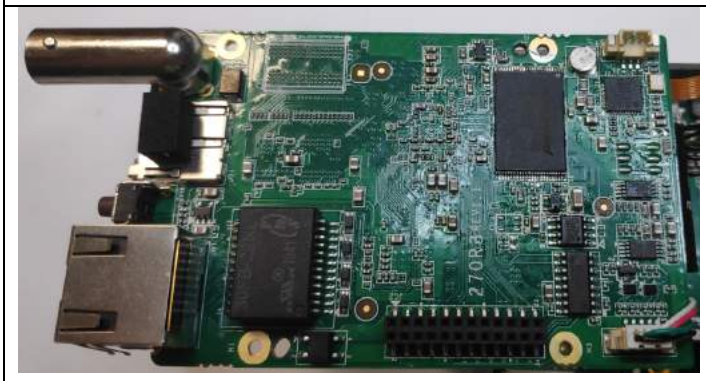
šifruotu ryšiu. Siekiant užtikrinti gerą produkcijos aptarnavimo ir palaikymo kokybę, toks funkcionalumas yra suprantamas, tačiau kelia riziką jog gali būti išnaudotas nesankcionuotiems prisijungimams įvykdžius kibernetinę ataką.

9. Gaminiuose įgyvendinti tipiniai elektroninių mazgų sprendimai, realizacija atlikta ekonominėje gamybos bazėje

Elektronikos dekompozicija parodė, kad „Hikvision“ kameroje naudojamas pačios įmonės sukurtas uždaras procesorius „HK-2015-1 DP8181934“, skirtas vaizdo apdorojimui ir išorinių sąsajų komunikacijos funkcionalumui užtikrinti. Galima teigti, kad tai yra nestandartinis, rinkoje laisvai neprieinamas gaminys. Informacijos, nusakančios „Hikvision“ sukurto procesoriaus charakteristikas žinių bazėse nebuvo rasta, todėl sudėtinga vertinti jo (o kartu ir kameros) turimas funkcijas, galimus darbo režimus.

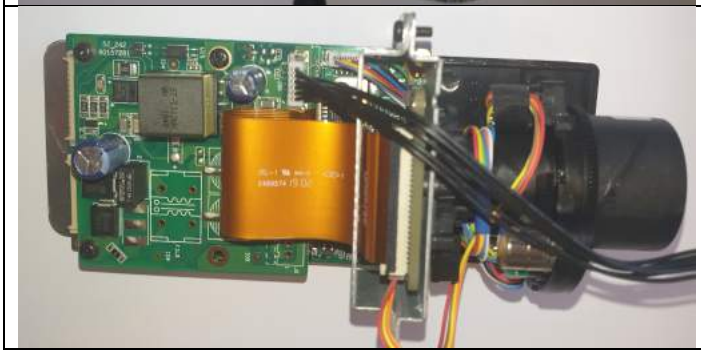
Gaminių elektronikos elementinę bazę sudaro gamintojų „Realtek“ (Taivanas), „SK Hynix“ (Pietų Korėja), „Winbond“ (Taivanas), „Ambarella“ (JAV / Kinija), „Samsung“ (Pietų Korėja), „Broadcom“ (JAV), „Aishi“ (Kinija) komponentai. Galima teigti, kad įrenginiuose veikianti programinė įranga yra pritaikyta funkcionuoti konkrečių lustų rinkinių bazėje. 16 ir 17 lentelėse pateikiami „Hikvision“ ir „Dahua“ kamerų elektronikos dekompozicijos tyrimų rezultatai.

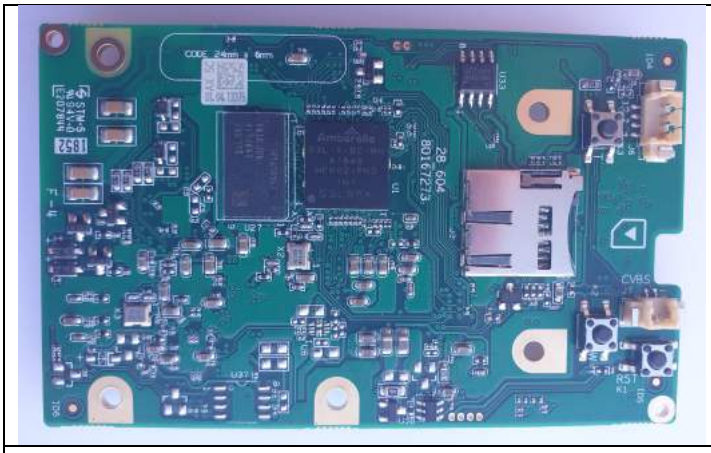
16 lentelė. „Hikvision“ kameros elektronikos dekompozicijos tyrimo rezultatai

„Hikvision“ kameros DS-2CD4C26FWD-AP aparatinės dalies apžvalga	
	Kameros vaizdas nuėmus viršutinę korpuso dalį. Matoma filtravimo dalis ir impulsinio maitinimo komponentai. Reikėtų atkreipti dėmesį, kad įėjimo filtravimui naudojami varistoriai (mėlyna spalva) nėra reikiamai apsaugoti nuo vibracijų, todėl kamerą montuojant zonoje, kuri vibruoja, kyla pavojus sugadinti įėjimo apsaugą, o atitrūkęs komponentas gali užtrumpinti maitinimo grandinės komponentus taip sukeliant įrenginio užsidegimo riziką.
	Kameros vaizdas nuėmus apatinę korpuso dalį. Matoma pagrindinė valdymo plokštė. Plokštėje matoma RAM atmintis, pagrindinis apdorojimo procesorius, kameros duomenų priėmimo FFC kabelio jungtis, Ethernet sąsajos „Realtek“ firmos PHY lustas.
	Pateikiama pagrindinės valdymo plokštės kita pusė. Matome magnetikus skirtus Ethernet signalų filtravimui kairėje ir pastoviąją ROM atmintį dešinėje. Taip pat paruošta vieta RAM atminties lusto įlitavimui, kurio paskirtis gali būti kaupti tam tikrus duomenis. Kamera gali būti taikoma keletui rinkų arba kameros su papildomu RAM lustu gali būti leidžiamos tam tikra imtimi.
	Pagrindinis vaizdo apdorojimui ir išorinių sąsajų komunikacijai priimti/transliuoti naudojamas unikalus, pačios firmos gamintas HK-2015-1 DP8181934 lustas. Sprendžiant iš matomos aparatinės dalies, galima teigti, kad lustas palaiko DDR3 (mažiausiai 2 Gbit) RAM atmintį ir 8 bitų magistralės pločio lygiagrečiai jungiamą išorinę 1 Gbit ROM atmintį. Procesoriaus veikimo dažniai ir konkrečios specifikacijos nežinomos.

	Naudojama H5TQ2G63GFR 2 Gbit DDR3 išorinė SDRAM atmintis. Tai Pietų Korėjos įmonės „SK Hynix“ gaminama atmintis, veikianti 1.5 V įtampa, 1600 MHz dažniu. Atmintis yra standartiniame BGA96 korpuse. Reikia atkreipti dėmesį, kad apatinėje montažinės plokštės dalyje palikta vieta papildomam atminties lusto įlitavimui.
	Naudojama NAND tipo, Winbond gamintojo W29N01HVSINA 1 Gbit išorinė atmintis, kuri yra TSOP-48 korpuse. Atmintis organizuota 128 M x 8 išdėstymu, maitinama 3,3 V įtampa.

17 lentelė. „Dahua“ kameros elektronikos dekompozicijos tyrimo rezultatai

„Dahua“ kameros DH-IPC-HFW5231EP-ZE aparatinės dalies apžvalga	
	Ethernet ryšio linija plokštę pasiekia ne vytos poros tipo laidais. Dėl šios priežasties gali kilti komunikacijos su kamera problemų.
	Pateikiamas kameros viršaus vaizdas, be korpuso. Kamera susideda iš maitinimo plokštės (pateiktos paveiksle) ir žemiau esančios pagrindinės plokštės. Naudojama impulsinė maitinimo grandinės realizacija reikiamoms įtampoms išgauti.

	Pagrindinės plokštės vaizdas iš viršaus, nuėmus laikančiąją konstrukciją, kuri taip pat atlieka aušinimo funkciją. Matomas pagrindinis apdorojimo lustas centre, kairiau laikinoji RAM atmintis, SD kortelės lizdas dešinėje. Matomi 3 valdymo mygtukai, kurie yra prieinami neišardžius kameros, atidarius baterijos talpinimo dangtelį.
	Pateikiamas pagrindinės plokštės apatinės pusės vaizdas. Šioje plokštėje matomas pastoviosios atminties ROM lustas, Ethernet PHY, magnetikai, visos komunikacinės jungtys, kurios priima signalus iš kameros sensoriaus, išorinių periferijų signalus, maitinimo linijas.
	Naudojamas „Ambarella“ gamintojo S3L-K-B0-RH pagrindinis apdorojimo lustas. Šis lustas gali koduoti H.265 ir H.264 standartais, įrašinėti 5 mln. 30p vaizdą. Lustas paremtas ARM Cortex A9 CPU, kuris veikia 1 GHz dažniu.
	Naudojama „Samsung“ firmos 2 Gbit DDR3L K4B2G1646F RAM atmintis. Atmintis sumontuota standartiniame 96 FBGA korpuse. Atmintis naudoja 1.35/1.5 V įtampą.

	Kameroje naudojamas „Winbond“ gamintojo 25Q256JVEQ serijinė FLASH atmintis. Tai 256 Mbit talpos atmintis, kuri palaiko dvigubą ir keturgubą lygiagrečią SPI sąsają. Atmintis gali dirbti iki 532 MHz dažniu ir perduoti 66 MB/s nuolatinio duomenų srauto.
	Ethernet sąsajai naudojamas „Broadcom“ gamintojo BCM54811 siųstuvas/imtuvas. Lustas palaiko 1000BASE-T, 100BASE-TX ir 10BASE-T greičius.

Tyrimo išvados ir rekomendacijos

1. Kamerose veikia nuotolinio valdymo aplinka, įgalinantis tekstinių užklausų pagalba vykdyti įrenginio kontrolę nuotoliniu būdu, kuri duomenų šifravimui naudoja AES šifravimo standartą, CBC algoritmą, tačiau šifruoti duomenys (slaptažodis ir kita informacija) nėra autentifikuojami, todėl kameros valdymo trakto informacija gali būti modifikuota. Dėl duomenų autentifikavimo nebuvimo, kamera tampa paveiki kibernetinėms atakoms, dėl ko galimas neteisėtas kameros turinio transliacijos perėmimas, realiuoju laiku aktyvuotos ar deaktyvuotos kameros funkcijos (vaizdo atpažinimo, garso įrašymo, kameros veikimo stabdymo ir kt.). Nustatyta, kad vartotojų autentifikavimas kamerose vykdomas nešifruotu ryšiu, naudojant tik HTTP, kartu su MD5 algoritmu. Vartotojui jungiantis prie kameros, jo slaptažodžio reikšmė gali būti perimta, slaptažodis dekoduotas ir panaudotas neteisėtam prisijungimui.

Atsižvelgiant į šias išvadas, rekomenduotina vaizdo stebėjimo kameras izoliuoti atskirame fiziniame arba specifiškai parametrizuotame loginiame tinkle, neturinčiame prieigos prie tarnybinių, vietinių ar viešųjų interneto tinklų.

2. Kamerose naudojami programinės įrangos paketai turi didelį skaičių žinomų kibernetinio saugumo spragų, pažymėtų viešai prieinamoje pažeidžiamumų duomenų bazėje. Pasinaudojus šiomis spragomis, yra tikimybė prieš kameras realizuoti kibernetines atakas, tokias kaip atkirtimo nuo paslaugos (DoS) ar kenkėjiško kodo įterpimas. Programinės įrangos atnaujinimo nuoroda patalpinta „Hikvision“ puslapyje, esančiame Kinijoje registruotame serveryje, nukreipianti į Rusijoje registruotą serverį, iš kurio siunčiama į kamerą diegiama atnaujinimo rinkmena.

Rekomenduojama organizacijoms neatskleisti savo tapatybės ir nesisiųsti atnaujinimų iš nutolusių serverių, nepriklausančių NATO ar ES. Geras sprendimas būtų organizuoti programinės įrangos atnaujinimų platinimą iš Lietuvoje registruotų serverių, kuriame būtų talpinami iš anksto patikrinti programų atnaujinimo paketai.

3. Kamerų valdymo galimybėms išplėsti, naudojamos išmaniesiems įrenginiams skirtos mobilios aplikacijos. Aplikacijos vykdo sujungimus su užsienyje esančiais serveriais (JAV, Kinijoje, Singapūre ir kitais), taip pat renka vartotojo įrenginio informaciją, kaip SIM kortelės IMSI ir ICCID identifikacinis numeris bei mobilaus įrenginio IMEI identifikacinis numeris, kurios rinkimo tikslai nėra aiškūs. Gamintojas naudoja uždarą protokolą kamerų aptikimui, tarnybiniam prisijungimui, serviso darbams, tačiau komunikcija vykdoma nešifruotu ryšiu. Toks funkcionalumas kelia papildomą riziką jog galės būti išnaudotas nesankcionuotiems prisijungimams įvykdžius kibernetinę ataką. Taip pat, egzistuoja galimybė perimti kameros tinklo traktą nusakančią informaciją ir užšifruotą slaptažodį.

Rekomenduotina vykdyti realaus laiko kamerų prievadų aktyvumo ir formuojamų kreipinių auditą, blokuoti perteklines užklausas ar srautus, naudoti ugniasienes su konkrečiam kameros modeliui verifikuotomis prieigos instrukcijomis (*angl.* White-list). Specialiomis priemonėmis užtikrinti kameros kuriamų srautų (audiovizualinio turinio ir tarnybinio trakto) šifravimą iki informacijos priėmimo įrenginio. Kamerų saugumo kontrolę galima atlikti atskiru specializuotu aparatiniu saugumo priedėliu, prie kameros prijungtu Ethernet sąsaja, neturinčiu įtakos kameros pagrindiniam funkcionalumui. Saugumo priedėlio funkcija – realiame laike užtikrinti prieigos kontrolę, kreipinių stebėseną, anomalijų aptikimą, kameros srauto šifravimą, specializuoto kamerų tinklo realizaciją.

Šaltiniai

[1] Hikvision Company Profile. *https://www.hikvision.com/en/about-us/company-profile/*.
[2] Reuters. „About Hangzhou Hikvision Digital Techgy Co., Ltd.“. *https://www.reuters.com/companies/002415.SZ*.
[3] Hikvision finansinė ataskaita (2019 m. I-mas pusmetis). *https://www.hikvision.com/content/dam/hikvision/en/brochures/hikvision-financial-report/Hikvision%202019%20Half%20Year%20Report.pdf*.
[4] Hikvision 2020 m. pavasario produktų katalogas. *https://us.hikvision.com/sites/default/files/manual/pqg_q1_2020_digital.pdf*.
[5] South China Morning Post. „Here’s what you need to know about Hikvision, the camera maker behind China’s mass surveillance system“. *https://www.scmp.com/tech/big-tech/article/2185123/heres-what-you-need-know-about-hikvision-camera-maker-behind-chinas*.
[6] Asmag. „DAHUA TECHNOLOGY CO., LTD. Company introduction“. *https://www.asmag.com/suppliers/companyinfo.aspx?co=dahuatech*.
[7] IFSEC GLOBAL. „Dahua Technology: The world’s second-largest video surveillance brand by market share“. *https://www.ifsecglobal.com/video-surveillance/profile-dahua-technology/*.
[8] VICE. „How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet“. *https://www.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs*.
[9] Ars Technica. „Brace yourselves—source code powering potent IoT DDoSes just went public“. *https://arstechnica.com/information-technology/2016/10/brace-yourselves-source-code-powering-potent-iot-ddoses-just-went-public/*.
[10] HackRead. „BASHLITE malware turning millions of Linux Based IoT Devices into *DDoS botnet“ https://www.hackread.com/bashlite-malware-linux-iot-ddos-botnet/*.
[11] SecurityWeek. „BASHLITE Botnets Ensnare 1 Million IoT Devices“. *https://www.securityweek.com/bashlite-botnets-ensnare-1-million-iot-devices*.
[12] IPVM. „Dahua Backdoor Uncovered“. *https://ipvm.com/reports/dahua-backdoor*.
[13] Breaking Defense. „Hacker Heaven: Huawei’s Hidden Back Doors Found“. *https://breakingdefense.com/2019/07/hunting-huaweis-hidden-back-doors/*.
[14] KrebsonSecurity „Dahua, Hikvision IoT Devices Under Siege“. *https://krebsonsecurity.com/tag/dahua-backdoor/*.
[15] Tripwire. „Dahua security camera owners urged to update firmware after vulnerability found“. *https://www.tripwire.com/state-of-security/featured/dahua-security-camera-owners-urged-update-firmware-vulnerability-found/*.
[16] Reuters. „South Korea's Hanwha likely to win from surveillance rivals' blacklisting: industry experts“. *https://www.reuters.com/article/us-usa-trade-china-hanwha/south-koreas-hanwha-likely-to-win-from-surveillance-rivals-blacklisting-industry-experts-idUSKBN1WN0B5*.
[17] Hikvision. Kameros specifikacija. *https://www.hikvision.com/en/products/IP-Products/Network-Cameras/Ultra-Series-SmartIP-/ds-2cd4c26fwd--ap-/*.
[18] Dahua. Kameros specifikacija. *https://www.dahuasecurity.com/asset/upload/uploads/soft/20181218/DH-IPC-HFW5231E-ZE_Datasheet_20181215.pdf*.
[19] RFC 2617 protokolo aprašymas. *https://tools.ietf.org/html/rfc2617*.
[20] CVE. ActiveX pažeidžiamumų sąrašas. *https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-12735/Microsoft-Activex.html*.
[21] Laisvai prieinama priemonė „Google Translator“. *https://translate.google.com/intl/en/about/*.
[22] „Hikvision“ programinės įrangos sąrašas. *https://us.hikvision.com/en/support-resources/firmware*.
[23] „Hikvision“ pažeidžiamumų atnaujinimai. *https://us.hikvision.com/en/support-resources/documentation/special-notices/update-buffer-overflow-vulnerability*.
[24] „ONVIF“ pranešimas. *https://securitytoday.com/articles/2019/10/14/onvif-suspends-dahua-and-hikvision.aspx*.
[25] „Hikvision“ OEM sąrašas. *https://ipvm.com/reports/hik-oems-dir*.
[26] „Hikvision“ programinės įrangos aprašas. *https://www.hikvision.com/content/dam/hikvision/en/support/download/firmware/ipc/4-series/ds-2cd4cx6fwd/release-notes/IPC%20R7%20V5.5.83%20Release%20Note--External.pdf*.