Aleksandr Suchkov *Marufa Azizova*

An’anaviy ruknimizning navbatdagi sahifasi robotlarga zarar yetkazuvchi omillar va ularning oqibatlari mavzusiga bag‘ishlanadi.

Buzg‘unchi kiberjinoyatchi – robot uchun ham xavflidir

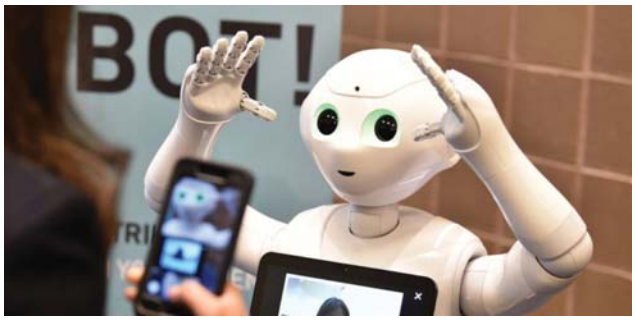
Robotlar ham ko‘p sonli elektronika qurilmalari kabi kiberjinoyatchidan jabr ko‘rishlari mumkin. IOActive kompaniyasi tadqiqotchilari o‘tgan yili SoftBank yapon kompaniyasi tomonidan ishlab chiqilgan robotlarda 50ta nosozlik, ya’ni zaifliklarni aniqladilar. Topilma haqida ishlab chiqaruvchiga ma’lumot berdilar, biroq undan munosib javob ola olmadilar. Shuning uchun joriy yil Security Analyst Summit 2018 konferensiyasida robot qurilmasi dasturiga buzib kirish bo‘yicha aniqlangan topilmalar-zaifliklarni ko‘rgazmali namoyish etishga qaror qildilar.

Robotlar dasturini ham buzib kirish mumkin!

Umuman olganda, dunyoda juda ko‘p turli robotlar mavjud: ular zavod sexlarida va omborlarda, qurilishlarda va hatto shifoxonalarda ishlaydilar. SoftBank Robotics elektron assistentlardan odamlar bilan ishlash uchun foydalanishni taklif qildi. NAO modeli talabalar va o‘quvchilarni dasturlash va robototexnika bilan tanishtiradi, shuningdek autizmli bolalarni o‘qitadi. Pepperning boshqa modeli xizmat ko‘rsatish sohasida foydalanish uchun yaratilgan — uning vazifalari salohiyatli mijozlar e’tiborini jalb qilish va xaridorlarga maslahat berishdir. IOActive tadqiqotchilari tomonidan aniqlanganidek, elektron assistentni u bilan bir tarmoqda bo‘lgan har bir foydalanuvchi nazorat qilishi mumkin. Mutaxassislar tomonidan aniqlangan zaifliklar masofadan turib, robotlarga buyruqlarni bajartirish imkonini beradi, ya’ni aslida, uning barcha harakatlarini boshqarishi mumkin.

Tadqiqotchilar NAO‘ni suhbatdoshidan bitcoinlardan talab qilishga majbur qilishdi, biroq haqiqiy jinoyatchilar robotni o‘z tasavvurlariga kelgan salbiy buyruqlarni bajarishga majbur etishi va robotning dasturiy qobiliyatini cheklashi mumkin. Aslida, Trojan-buzg‘unchi dastur bilan nafaqat NAO‘ning dasturini, balki ehtimol, ko‘proq biznesga yo‘naltirilgan Pepperni hamda boshqa robotlar modellarini ham chalg‘itish mumkin.

Bir tasavvur qiling-a: kunlardan birida robot-o‘qituvchi yoki do‘kon maslahatchi-konsultanti barcha odamlar oldida behayo haqoratli gaplar bilan xaridorga qo‘pollik qilishni boshlasa, ishlashni xohlamasligini e’lon qilib, o‘chib qolsa, hatto janjallashishga kirishib ketsa nima bo‘ladi?



Biroq robotni bezoriga aylantirish kimga kerak bo‘lishi mumkin?

Jinoyatchilarga bundan qanday foyda bo‘lishi mumkin deb so‘rarsiz? Ular birovning hayotini faqat shunchaki buzmaydilarku. Aslida, ular bu ishni shunchaki qilishlari ham mumkin — xakerlar bunday ishlarni ko‘ngilochish uchungina tez-tez amalga oshirib turadilar. Shuningdek, ular bunday ishni boshqa sababga ko‘ra — pul topish uchun ham qilishlari mumkin. O‘zingiz hisoblab ko‘ring: bir robot 10 ming dollar turadi. Agar u buzilsa, ta’mirlanishi yoki o‘zgartirilishi kerak. Ikkala tomon ham o‘zlari uchun yangi mablag‘ investitsiyalarini talab qiladi. Agar robotning mijozlarni qo‘rqitganligi sababli yo‘qotilgan vaqtning qiymatini va ishlab chiqaruvchi obro‘si haqida o‘ylasangiz, bu mablag‘ ancha ta’sirli ekanligini tushunasiz. Agar robot ishlab chiqarish jarayonida buzilgan bo‘lsa, unda xodimlarning hayoti va sog‘lig‘iga ta’siri yoki nosoz mahsulotni ishlab chiqarilishi xavfi yuzaga keladi.

Buzg‘unchi — faqat haqini to‘lash sharti bilan o‘zi yaratgan muammosini hal qilib berish uchun yordamini boshqalardan tezroq taklif qilishi mumkin, aks holda, baribir, mahsulot qaytarib yuboriladi. Biroq birinchi navbatda, bunday taklif egalari doimo o‘z so‘zlarida turmaydilar, ikkinchidan, zararlangan robot boshqasini buzib tashlashi ham mumkin, keyin esa to‘lov ikkinchi marta to‘lashi kerak bo‘ladi.

Nima qilish kerak?

Robotlar tobora faqat ommalashib bormoqda va ulardan voz kechish masalani hal qilmaydi: bu holda odamzod o‘tgan asr va hatto undan ham avvalgi asrga qaytishga majbur bo‘ladi. Yaxshisi, dasturchilar, ayniqsa, ishlab chiqaruvchilar robotlarning zaif tomonlariga e’tibor qaratishlari shart bo‘ladi.

Ilg‘or texnologiyalarni biror sohada halokatga sabab bo‘lmasligi uchun robot yaratuvchilari ishlab chiqarish boshlanishidan oldin xavfsizlik masalalari bo‘yicha puxta o‘ylab, ish yuritishlari kerak. Bu ishni hozirning o‘zidayoq boshlashlari, biroq kecha boshlasalar undan ham yaxshiroq bo‘lardi. Ishlab chiqarilgandan keyin esa — doim hushyor bo‘lib, zarur vaqtda, topilgan zaifliklar to‘g‘risida tezkor ma’lumotlarga javob berish va ularni bartaraf etishga tayyor turish kerak.

Zamonaviy yaxtalarga xakerlar ulana oladi

Zamonaviy dengiz kemalari ishlab chiqaruvchilari kema infratuzilmasining turli tarkibiy qismlarini hozirgi davrda rusumga aylangan, Internet tarmog‘iga ulash usuli trendidan qochishmadi. Natijada zamonaviy yaxtalar faqat navigatsiya tizimlari bilan emas, balki umumiy tarmoqqa marshrutizator va kommutatorlarga ulangan boshqa elektron qurilmalar bilan ham jihozlandi. Shu sababli yaxtalar birdan internetga ulanadigan boshqa qurilmalar kabi zaif bo‘lib qoldi. Ularda qo‘llaniladigan texnologiyalar zamonaviy xavfsizlik standartlarining paydo bo‘lishidan oldin ishlab chiqilgan va ishonchli himoyani ta’minlay olmaydi. Bundan tashqari, navigatsiya uskunalari axborot-ko‘ngilochar qurilmalari tarmog‘idan ajratilmaydi, Internet-ulanishning o‘zi hech qanday tarzda himoyalanmaydi — bu holat ro‘yxatini uzoq davom ettirish mumkin. Security Analyst Summit 2018 konferensiyasida ROSEN kompaniyalar guruhi a’zosi Shtefan Gerling (Stephan Gerling) bu muammolarning ba’zilari haqida to‘xtalib o‘tdi.

Yaxtaning bort tarmog‘iga ulangan qurilmalar soni talaygina — jumladan, kema harakatini nazorat qilish tizimi (KHNT), avtomatik identifikatsiya qilish tizimi (AIS), autopilot, GPS priyomnik(qabul qiluvchi)lari, radar, kameralar (shu jumladan, infraqizil kameralar), chuqurlik o‘lchagichlari, dvigatellarni boshqarish va ularning holatini kuzatish uchun qurilmalar (bugungi kunda ba’zilari bulut texnologiyasi orqali ishlaydi) va boshqalar.

Barcha elektron guruh NMEA (National Marine Electronics Association) shinasi yordamida umumiy tarmoqqa birlashtirilgan. Ushbu standartning so‘nggi versiyasi NMEA 2000 (yoki N2K) deb ataladi. Qizig‘i shundaki, N2K barcha zamonaviy avtomashinalarda ishlatiladigan CAN shinalariga yaqin qarindoshdir.

Aleksandr Suchkov, Marufa Azizova

Dengiz elektronikasi Internetga ulanmagan bo‘lsa ham, unga muvaffaqiyat bilan hujum qilish mumkin. Eng tez-tez uchraydigan usullar — GPS signalini blokirovkalash va almashtirish, AIS identifikatsiyasini va boshqalarni bir xil ruhda o‘zgartirishdan iborat. Bu allaqachon nazariya emas: bunday hujumlar bir necha marta sodir bo‘ladi.

Hujum qilish vaqtida buzg‘unchilar boshqa kemalar bilan to‘qnashuvning oldini olish uchun port boshqaruvchi-dispetcherga uzatib turish maqsadida, AIS ma’lumotlarini to‘plashi va yuborishini e’tiborga olib, kemaning pozitsiyasi va tezligi haqida ma’lumotni o‘zgartirib turadilar, masalan, GPS signallariga hujum qilish yoki AIS’ni ulash har doim jiddiy shikast yetkazadigan kemalar to‘qnashuviga qadar va ba’zida insonlarga zarar yetkazilgungacha navigatsion muammolar bilan to‘la bo‘ladi.

Zamonaviy yaxtalarda NMEAga qo‘shimcha ravishda, boshqa tarmoqlar ham mavjud. Masalan, har kuni TCP/IP protokollaridan foydalangan holda, tarmoqda ishlaydigan ko‘ngilochar-o‘yin tizimlari ham bor. Ushbu tarmoqlarda ishlaydigan uskunalar ham juda oddiy standartga ega, ular: marshrutizator va kommutatorlarga, Wi-Fi ulanish nuqtalariga, VoIP telefonlariga, aqlli televizorlar va boshqa — barchasi oddiy uy yoki xonadonda uchraydigan qurilmalardir. Biroq uy tarmog‘idan farqli jihatlari ham mavjud: yaxtalardagi axborot-ko‘ngilochar tarmoq NMEA shinasiga maxsus shlyuz orqali ulanadi. Bir tomondan, bu yaxta egasi uchun qulay, chunki u smartfon yoki planshetdan barcha kema tizimlarini — illyuminator derazalaridan yorug‘lik tushishidan tortib, motorlargacha nazorat qilishga imkon beradi. Hatto autopilot ham maxsus simsiz qurilma bilan boshqarilishi mumkin.

Boshqa tomondan, ikkita tarmoq bir-biridan ajralmasligi sababli axborot va ko‘ngilochar tizimlar buzilganida, buzg‘unchilar NMEA tarmog‘iga chuqur kirib borishi mumkin. Axborot va ko‘ngilochar tarmoqlar, albatta, Internetga: sun’iy yo‘ldosh aloqasi, 4G/3G/2G yuqori tezlikda ma’lumotlar uzatish kanallari yoki Wi-Fi modullari orqali kirish imkoniga ega. Gerling yaxtalarning qay darajada himoyasizligini namoyish qilish uchun internet-ulanish va mahalliy tarmoqlarni o‘rnatish va monitoring qilish uchun yaxtalarning haqiqiy yechimlaridan birini o‘rgangan. Foydalanuvchilar qulayroq bo‘lishi uchun bu yechim Windows, iOS yoki Android ilovalari orqali masofadan boshqarishni qo‘llab-quvvatlaydi. Aynan shu yerda muammo mavjud edi.

Gap shundaki, haqiqatdan ham, har bir nazorat qilish dasturi planshet, mobil telefon yoki kompyuterda ochilganda FTP orqali marshrutizatorga ulanadi va XML faylini yuklaydi. Bu fayl marshrutizatorning to‘liq konfiguratsiyasi, jumladan, qat’iy kodli hisoblar, Wi-Fi tarmog‘ining SSID-identifikatori va unda parol oddiy shifrlanmagan matn shaklida bo‘ladi.

Jinoyatchilar tomonidan FTP protokoli xavfsiz emasligi sababli ushbu ma’lumotlar osongina qo‘lga olinadi, bundan keyin yaxta marshrutizatori va uning axborot-ko‘ngilochar tarmog‘ini to‘liq nazorat qila oladilar.

Gerling bu jiddiy xatoga qo‘shimcha ravishda, marshrutizator operatsion tizimida administrator huquqlariga ega bo‘lgan foydalanuvchi hisobini topdi. Ishlab chiquvchilar, ehtimol, buni masofadan texnik yordam ko‘rsatish uchun qoldirgan bo‘lsa kerak.

Axborot-ko‘ngilochish tizimida kiber-jinoyatchilarni nazorat qilish xavfi nima?

Masalan, HTTP so‘rovlari, audio (Internet orqali uzatilgan ovozli xabarlar) yoki video (kuzatuv kamerasidan olingan ma’lumotlar), jumladan, har qanday trafikni ushlab turish kabilarni sanab o‘tish mumkin. Bu hali hech gap emas.

Bunday imkoniyatlar bilan nafaqat yaxtadagilar ustidan, hattoki ishtirokchilar ustidan ham josuslik qilishni boshlash, balki Wi-Fi-ga ulanishi mumkin bo‘lgan har qanday qurilmani ham buzish mumkin. Gerling topilgan barcha muammolarni ishlab chiqaruvchilarga ma’lum qilganidan so‘ng tarmoq protokoli FTP dan ishonchli bo‘lgan SSHga o‘zgartirildi. Bundan tashqari, marshrutizator uchun yangi dastur va dasturiy ta’minot ishlab chiqildi. Yangilangan dasturiy ta’minot ilgaridagi kabi qat’iy kodlangan hisobga olish ma’lumotlarini o‘z ichiga oladi, ammo ishlab chiquvchilar parolni «12345678» dan ishonchliroq ma’lumotga almashtirdilar. Biroq yo‘riqnoma operatsion tizimiga tuzatma o‘rnatilgandan keyin ham, faol administrator hisobi saqlanib qoldi.

Umuman olganda, bu tashvishli holat. Yaxtalar egalari va xaridorlariga jo‘yali maslahat berish qiyin. Bortdagi axborot va ko‘ngilochar tizimlar odatda tayyor yechim ko‘rinishida topshiriladi, ularning ko‘pchiligini tanlash mumkin. Ko‘p yaxtalar egalari uskunalar o‘rnatish va tarmoqni qurish bilan mustaqil shug‘ullanadilar. Biz faqat ma’lumot va ko‘ngilochar tizim yetkazib beruvchilarni e’tibor bilan tanlashingizni tavsiya etamiz.

O‘tkazilgan tadqiqotlar shuni ko‘rsatdiki, hatto murakkab va qimmatbaho narsalar — masalan, yaxta ham qandaydir oddiy, oson topish mumkin bo‘lgan zaifliklarga ega bo‘lishi mumkin. Masalan, yaxta egasiga va uning mehmonlariga josuslik qilish uchun kimdir foydalanishi mumkin. Boshqacha aytganda, sizning kemangiz bortida nimalar yuz berayotganini butun dunyo bilishishi mumkin.

Yaxtalarga egalik qiladigan yoki ularni ijaraga oladigan odamlar ko‘proq yuqori mavqega ega va taniqli shaxslar bo‘lishi mumkinligi nazarda tutilsa, ularning ishlab chiqaruvchilari, sinovdan o‘tkazuvchilar tizimlarni tayyorlash bosqichidayoq xavfsizlik masalalariga qanchalik jiddiy yondashishlari shartligini anglash mumkin. Bunda, ayniqsa, tizimni tayyorlash bosqichida ham, tadqiqotchilar va xavfsizlikni tekshiruvchilarning xizmatlaridan foydalanishda ham, mijoz yetkazib beruvchini ayblashi uchun to‘la huquqqa ega bo‘lishini bilishi zarur.

IT-xavfsizligi nuqtai nazaridan, yaxtalarning tarmoqqa ulanishi avtomobillarga juda o‘xshash, shuning uchun uni himoya qilish uchun avtomobildagi kabi usullardan foydalanish mumkin. Misol uchun, bortda kompyuter tizimlarining tarkibiy qismlari o‘rtasida ma’lumotlar almashinuvi himoyasini ta’minlaydigan infratuzilmada shlyuzni kiritish zarur. Mazkur turdagi shlyuzning variantlaridan biri — avtomobil ishlab chiqaruvchilari uchun foydalaniladigan KasperskyOS operatsion tizimiga asoslangan qurilmadir.

Manba: ***www.kaspersky.ru/blog***