TARMOQ VA INTERNET.

Xalqaro Nordik Universiteti o'qituvchisi
Sofoyeva Fotima Davlatyorovna

Annotatsiya: Ushbu maqolada hozirgi kunda dolzarb mavzulardan biriga aylangan ma'lumotlarni web-qidiruv tizimlar himoyasi va unda uchraydigan muammolar, yechimlar berib o'tilgan. tarmoq va internet ma'lumotlar va statistik ma'lumotlar bilan to'ldirilgan. Shu bilan birga qidiruv tizimlarida axborot ma'lumotlarini olish uchun himoyalash uchun muhim tavsiya va maslahatlar berib o'tilgan.

Kalit so'zlar: PAN, LAN, MAN, WAN, TCP/IP, shina topologiyasi, yulduz topologiyasi, CSMA/CD, DARPA, ICANN, TLD, DNS, NNTP, FTP

Аннотация: В данной статье рассмотрена защита информационных веб-поисковых систем, ставшая одной из актуальных тем, а также возникающие в ней проблемы и пути их решения. сеть и Интернет наполнены информацией и статистикой. При этом были даны важные рекомендации и советы по защите информации в поисковых системах.

Ключевые слова: PAN, LAN, MAN, WAN, TCP/IP, топология «шина», топология «звезда», CSMA/CD, DARPA, ICANN, TLD, DNS, NNTP, FTP.

NETWORK AND INTERNET.

Sofoyeva Fatima Davlatyorovna.
Teacher of the International Nordic University

Abstract: In this article, the protection of information web-search systems, which has become one of the current topics, and the problems and solutions encountered in it are given. the network and the Internet are filled with information and statistics. At the same time, important recommendations and tips were given for the protection of information in search engines.

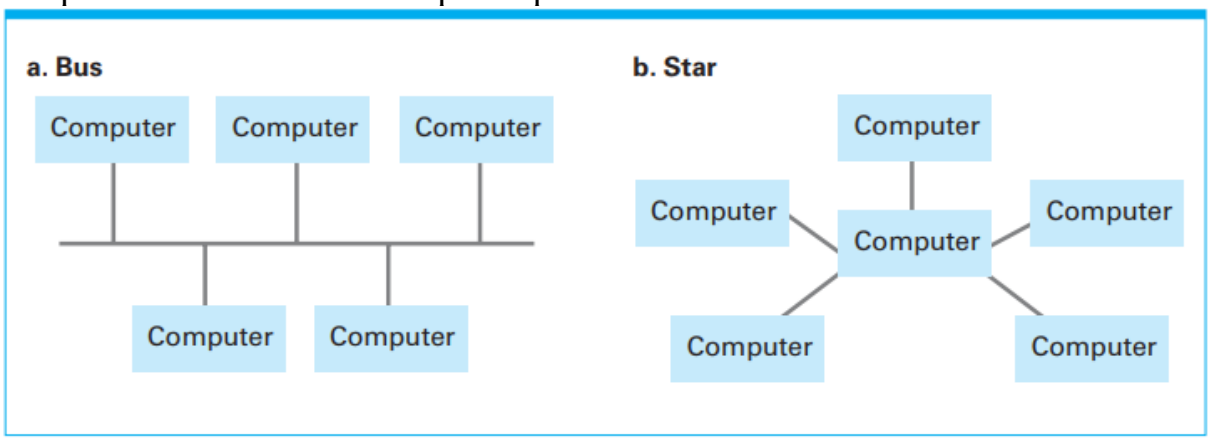
Keywords: PAN, LAN, MAN, WAN, TCP/IP, bus topology, star topology, CSMA/CD, DARPA, ICANN, TLD, DNS, NNTP, FTP

Kirish

Kompyuter tarmog'i ko'pincha **shaxsiy tarmoq (PAN)**, **lokal tarmoq (LAN)**, **metropoliten tarmoq (MAN)** yoki **mintaqaviy tarmoq (WAN)** deb tasniflanadi. PAN odatda qisqa masofali (odatda bir necha metrdan kamroq) aloqa uchun ishlatiladi, masalan, simsiz eshitish vositasi va smartfon o'rtasida yoki simsiz sichqoncha va shaxsiy kompyuter o'rtasida. Bundan farqli o'laroq, LAN odatda bitta bino yoki binolar majmuasidagi kompyuterlar to'plamidan iborat. Masalan, universitet kampusidagi yoki ishlab chiqarish zavodidagi kompyuterlar LAN orqali ulanishi mumkin. MAN - bu oraliq o'lchamdagi tarmoq, masalan, mahalliy

hamjamiyatni qamrab oladigan tarmoq. WAN - qurilmalarni uzoqroq masofaga bog‘laydi – masalan, qo‘shni shaharlarni yoki dunyoning qarama-qarshi tomonlarini.

Tarmoqlarni tasniflashning bir usuli tarmoq topologiyasiga asoslangan bo‘lib, u mashinalar ulangan tarmoqga ishora qiladi. Eng mashhur topologiyalardan bittasi bu shina bo‘lib, unda barcha qurilmalar shina deb ataladigan umumiy aloqa liniyasiga ulanadi (5.1a-rasm) va keyingisi yulduz bo‘lib, bitta qurilma markaz bo‘lib xizmat qiladi va yulduz shaklida ulanadi (5.1b-rasm). Shina topologiyasi 1990-yillarda Ethernet deb nomlanuvchi standartlar to‘plami ostida amalga oshirilganda ommalashgan va Ethernet tarmoqlari bugungi kunda ishlatiladigan eng mashhur tarmoq tizimlaridan biri bo‘lib qolmoqda.



1-rasm. Ikki mashhur tarmoq topologiyasi.

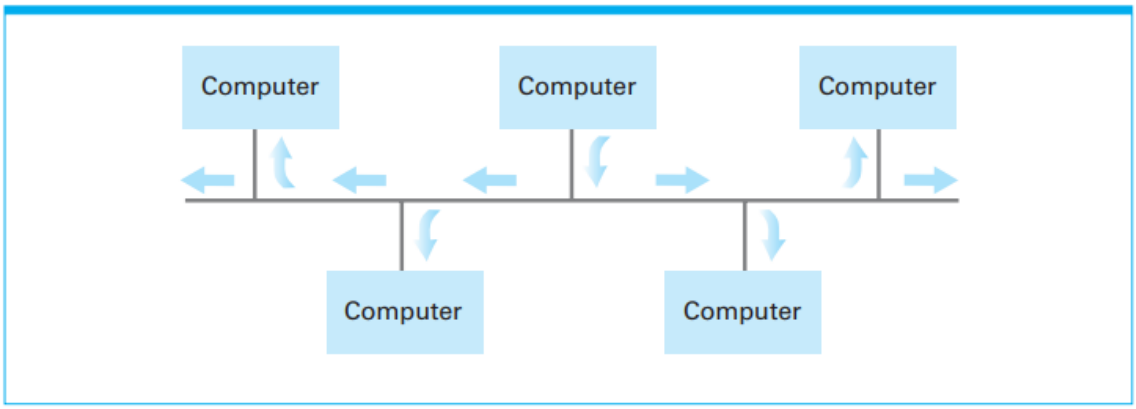
Yulduz topologiyasining tarixi 1970-yillarga borib taqaladi. U ko‘plab foydalanuvchilarga xizmat ko‘rsatadigan katta markaziy kompyuter paradigmasidan rivojlandi. Ushbu foydalanuvchilar tomonidan ishlaydigan oddiy terminallar o‘zlari kichik kompyuterlarga aylanganligi sababli, yulduz tarmog‘i paydo bo‘ldi. Bugungi kunda yulduz konfiguratsiyasi simsiz tarmoqlarda mashhur bo‘lib, u yerda aloqa radioeshittirish orqali amalga oshiriladi va kirish nuqtasi (AP) deb ataladigan markaziy mashina barcha aloqalar muvofiqlashtirilgan markaz bo‘lib xizmat qiladi.

Protokollar

Tarmoqning ishonchli ishlashi uchun faoliyatni amalga oshirish qoidalarini belgilash muhimdir. Bunday qoidalar protokollar deb ataladi. Protokol standartlarini ishlab chiqish tarmoq texnologiyalarini ishlab chiqishda ajralmas jarayondir. Protokol kontseptsiyasiga kirish sifatida tarmoqdagi kompyuterlar o‘rtasida xabarlarni uzatishni muvofiqlashtirish muammosini ko‘rib chiqaylik. Ushbu aloqani tartibga soluvchi qoidalarsiz, barcha kompyuterlar bir vaqtning o‘zida xabarlarni uzatishni talab qilishi yoki yordam kerak bo‘lganda boshqa qurilmalarga yordam bermasligi mumkin.

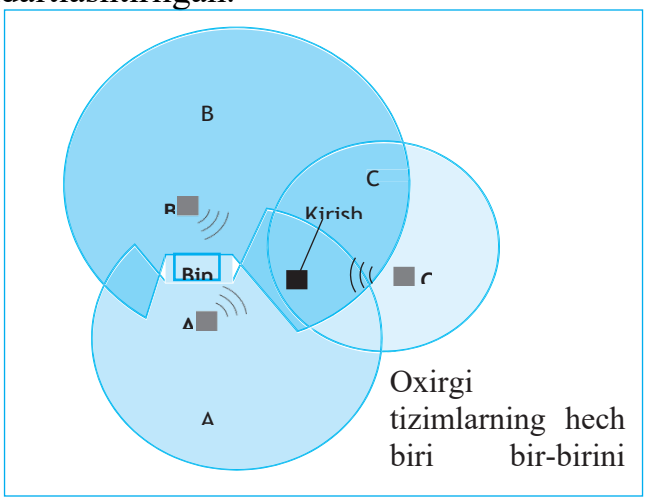
Ethernet standartlariga asoslangan shina tarmog‘ida xabarlarni uzatish huquqi CSMA/CD (Carrier Sense, Multiple Access with Collision Detection) deb nomlanuvchi protokol tomonidan boshqariladi. Ushbu protokol har bir xabar shinadagi barcha qurilmalarga uzatilishini talab qiladi (5.2-rasm). Har bir qurilma

barcha xabarlarni kuzatib boradi, lekin faqat o‘ziga yuborilgan xabarlarni saqlaydi. Xabarni uzatish uchun qurilma shinada harakat oxirigacha kutadi va bu vaqtda u tarmoqni kuzatishda davom etayotganda uzatishni boshlaydi.



2-rasm. Shina tarmog‘i orqali aloqa

Esda tutingki, CSMA/CD barcha mashinalar markaziy AP orqali aloqa qiladigan simsiz yulduz tarmoqlariga mos kelmaydi. Buning sababi shundaki, qurilma o‘zining uzatmalari boshqasiniki bilan to‘qnashayotganini aniqlay olmasligi mumkin. Masalan, mashina boshqasini eshitmasligi mumkin, chunki o‘z signali boshqa mashinaning signalini o‘chiradi. Yana bir sabab, turli xil mashinalarning signallari bir-biridan ob’ektlar yoki masofa bilan bloklangan bo‘lishi mumkin, garchi ularning barchasi markaziy kirish nuqtasi bilan bog‘langan bo‘lsa ham (yashirin terminal muammosi deb nomlanuvchi holat, 5.3-rasm). Natijada simsiz tarmoqlar to‘qnashuvlarni aniqlashga emas, balki ularni oldini olishga harakat qilish siyosatini qabul qiladi. Bunday siyosatlar CSMA/CA bilan bir nechta kirish sifatida tasniflanadi, ularning aksariyati IEEE 802.11 va protokollarida belgilangan protokollar doirasida IEEE tomonidan standartlashtirilgan.



3-rasm. Yashirin terminal muammosi.

Internet, internet protokollari va ularning turlari.

Internetning eng yorqin namunasi 1960-yillarning boshlarida olib borilgan tadqiqot loyihalaridan kelib chiqqan. Maqsad turli xil kompyuter tarmoqlarini bir-

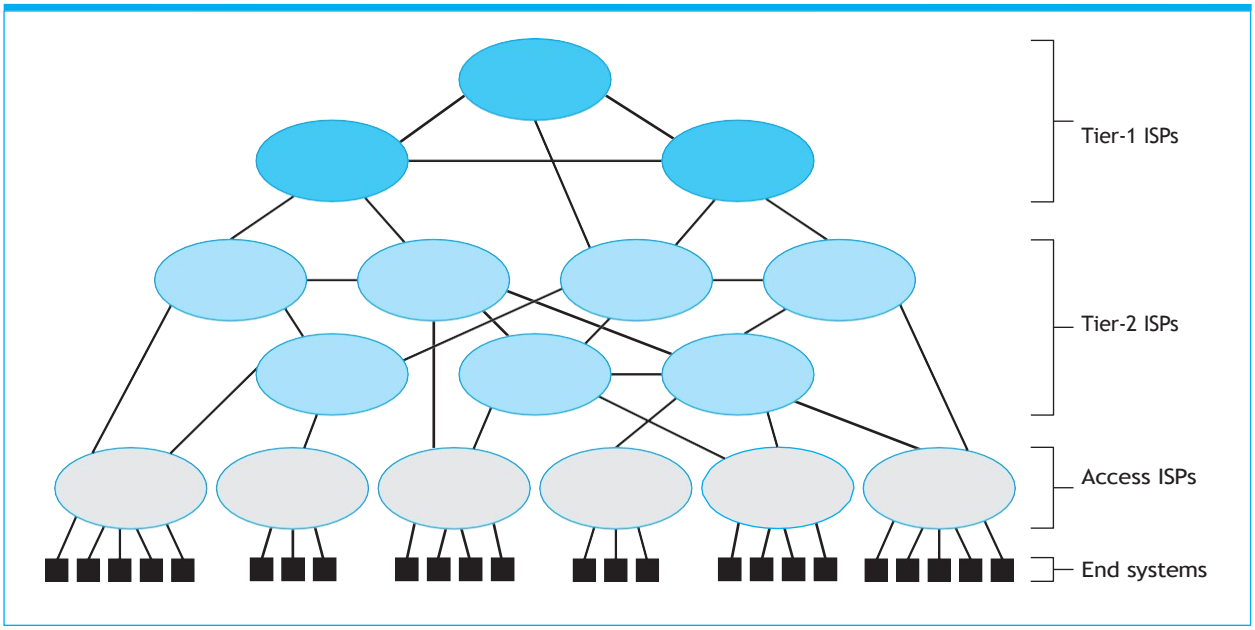
biriga bog‘lash qobiliyatini rivojlantirish bo‘lib, ular mahalliy ofatlar tufayli buzilmaydigan ulangan tizim sifatida ishlaydi. Ushbu ishlarning aksariyati AQSh hukumati tomonidan Mudofaa ilg‘or tadqiqot loyihalari agentligi (DARPA) orqali homiylik qilingan. Yillar davomida Internetning rivojlanishi hukumat homiyligidagi loyihadan akademik tadqiqot loyihasiga o‘tdi va bugungi kunda u millionlab kompyuterlarni o‘z ichiga olgan PAN, LAN, MAN va WAN larning butun dunyo bo‘ylab kombinatsiyasini bog‘laydigan tijorat tashkilotidir.

Internet ulangan tarmoqlar to‘plamidir. Umuman olganda, bu tarmoqlar Internet provayderlari (ISP) deb nomlangan tashkilotlar tomonidan quriladi va xizmat ko‘rsatiladi. Tarmoqlarning o‘ziga nisbatan ISP atamasidan foydalanish ham odatiy holdir.

Misol tariqasida an’anaviy telefon kompaniyasi sifatida paydo bo‘lgan va boshqa aloqa xizmatlarini ko‘rsatish sohasini kengaytirgan kompaniyani keltirish mumkin.

1-darajali Internet-provayderlarga ulanish 2-darajali Internet-provayderlar bo‘lib, ular ko‘lami bo‘yicha ko‘proq mintaqaviy va o‘z imkoniyatlaridan kamroq kuchga ega. (1-darajali va 2-darajali provayderlar o‘rtasidagi farq ko‘pincha fikr masalasidir) Shunga qaramay, bu tarmoqlar aloqa biznesidagi kompaniyalar tomonidan boshqariladi.

1-darajali va 2-darajali provayderlar asosan Internet aloqa infratuzilmasini birgalikda ta’minlovchi marshrutizatorlar tarmog‘idir. Shunday qilib, ularni Internetning asosiy qismi deb hisoblash mumkin. Ushbu yadroga kirish odatda 3-darajali ISP deb ataladigan vositachi tomonidan ta’minlanadi. Kirish provayderi asosan mustaqil internet bo‘lib, ba’zan intranet deb ataladi va u alohida uylar va korxonalarni Internetga kirishni ta’minlash bilan shug‘ullanuvchi yagona organ tomonidan boshqariladi. Masalan, o‘z xizmatlari uchun haq oladigan kabel va telefon kompaniyalari, shuningdek, o‘z tashkilotlari ichidagi shaxslarga Internetga kirishni ta’minlashni o‘z zimmalariga olgan universitetlar yoki korporatsiyalar kabi tashkilotlar kiradi.



4-rasm. Internet tarkibi.

Shaxsiy foydalanuvchilar kirish provayderlariga ulanadigan qurilmalar oxirgi tizimlar yoki xostlar sifatida tanilgan. Ushbu so‘nggi tizimlar noutbuklar yoki shaxsiy kompyuterlar bo‘lishi mumkin, lekin tobora ko‘proq boshqa qurilmalar, jumladan telefonlar, videokameralar, avtomobillar va maishiy texnikalarni qamrab oladi. Axir, Internet aslida aloqa tizimidir va shuning uchun boshqa qurilmalar bilan aloqa qilishdan foyda ko‘radigan har qanday qurilma potentsial yakuniy tizimdir.

Internet Addressing

Internetga tizimdagi har bir kompyuterga noyob identifikatsiya manzilini belgilaydigan Internet bo‘ylab manzillash tizimi kerak. Internetda bu manzillar IP manzillar sifatida tanilgan (IP atamasi "Internet protokoli" ga ishora qiladi). Dastlab, har bir IP-manzil 32 bitdan iborat bo‘lgan, ammo manzillarning kattaroq to‘plamini ta’minlash uchun konvertatsiya qilish 128-bitli manzillarga ulanish jarayoni hozirda davom etmoqda. Ketma-ket raqamlangan IP-manzillar bloklari Internet ishini muvofiqlashtirish uchun tashkil etilgan notijorat korporatsiya bo‘lgan tayinlangan nomlar va raqamlar uchun Internet korporatsiyasi (ICANN) tomonidan provayderlarga beriladi. So‘ngra provayderlarga o‘z vakolatlari doirasidagi mashinalarga o‘zlarining berilgan bloklaridagi manzillarni ajratishga ruxsat beriladi. Shunday qilib, butun Internetdagi qurilmalarga noyob IP-manzillar beriladi.

Manzillash tizimi domen kontseptsiyasiga asoslangan bo‘lib, uni universitet, klub, kompaniya yoki davlat idorasi kabi yagona hokimiyat tomonidan boshqariladigan Internetning "mintaqasi" sifatida ko‘rish mumkin. Registratorlar deb ataladigan kompaniyalar tomonidan boshqariladigan jarayon ICANN da ro‘yxatdan o‘tgan bo‘lishi kerak. Bu rol ICANN tomonidan tayinlangan. Ushbu ro‘yxatga olish jarayonining bir qismi sifatida domenga Internetdagi barcha domen nomlari orasida noyob bo‘lgan mnemonik domen nomi beriladi. Domen nomlari ko‘pincha domenni

roʻyxatdan oʻtkazuvchi tashkilotni tavsiflaydi, bu ularning odamlar uchun foydaliligini oshiradi.

Misol tariqasida Marquette universitetining domen nomi mu.edu hisoblanadi. Nuqtadan keyingi qoʻshimchaga e'tibor bering. U domen tasnifini aks ettirish uchun ishlatiladi, bu holda edu qoʻshimchasi bilan koʻrsatilgandek "ta'lim". Ushbu qoʻshimchalar yuqori darajadagi domenlar (TLD) deb ataladi. Boshqa TLDlar orasida tijorat muassasalari uchun com, AQSH davlat muassasalari uchun gov, notijorat tashkilotlari uchun org, muzeylar uchun muzey, cheklanmagan foydalanish uchun ma'lumotlar va dastlab internet-provayderlar uchun moʻljallangan, ammo hozirda ancha kengroq miqyosda foydalaniladigan tarmoq kiradi. Ushbu umumiy TLDlarga qoʻshimcha ravishda, Avstraliya uchun au va Kanada uchun ca kabi ma'lum mamlakatlar uchun (mamlakat kodi TLD deb ataladi) ikki harfli TLDlar ham mavjud.

Internet ilovalari.

Internetning dastlabki kunlarida koʻpchilik ilovalar alohida, oddiy dasturlar boʻlib, ularning har biri tarmoq protokoliga amal qilgan. Newsreader ilovasi Network News Transfer Protocol (NNTP) yordamida serverlar bilan bogʻlangan, tarmoq boʻylab fayllarni roʻyxatga olish va nusxalash uchun dastur File Transfer Protocol (FTP) joriy qilingan yoki boshqa kompyuterga uzoq masofadan kirish uchun dastur Telnet protokolidan foydalangan holda, yoki Secure Shell (SSH) protokoli. Veb-serverlar va brauzerlar yanada murakkablashgani sayin, ushbu an'anaviy tarmoq ilovalari tobora koʻproq kuchli Hyper Text Transfer Protocol (HTTP) orqali veb-sahifalar tomonidan boshqarila boshlandi.

SMTP (Simple Mail Transfer Protocol) elektron pochta xabarini bir xostdan ikkinchisiga uzatishda tarmoqdagi ikkita kompyuterning oʻzaro taʻsir qilish usulini belgilaydi. Mail.skaro.gov pochta serverining tardis.edu domenidagi oxirgi foydalanuvchi "doctor" ga "dalek" dan elektron pochta xabarini yuborish misolini koʻrib chiqamiz. Birinchidan, mail.skaro.gov dagi pochta bilan ishlash jarayoni mail.tardis.edu dagi pochta serveri jarayoni bilan bogʻlanadi. Buni amalga oshirish uchun u DNS, boshqa tarmoq protokoli yordamida inson oʻqiy oladigan maqsad domen nomini toʻgʻri pochta serveri nomiga, soʻngra uning IP manziliga moslashtiradi. Xuddi shunday, serverning boshqa tomonidagi jarayon javob berganida, protokol oʻzini qoʻngʻiroq qiluvchiga identifikatsiyalashi kerakligini aytadi. Ularning SMTP almashinuvining transkripti quyidagicha koʻrinishi mumkin:

1. 220 mail.tardis.edu SMTP Sendmail Gallifrey-1.0; Fri, 23 Aug 2413 14:34:10
2. HELO mail.skaro.gov
3. 250 mail.tardis.edu Hello mail.skaro.gov, pleased to meet you
4. MAIL From: dalek@skaro.gov
5. 250 2.1.0 dalek@skaro.gov... Sender ok
6. RCPT To: doctor@tardis.edu
7. 250 2.1.5 doctor@tardis.edu... Recipient ok

8. DATA
9. 354 Enter mail, end with "." on a line by itself
10. Subject: Extermination.
11. EXTERMINATE!
12. Regards, Dalek
13. .
14. 250 2.0.0 r7NJYAEl028071 Message accepted for delivery
15. QUIT
16. 221 2.0.0 mail.tardis.edu closing connection

1-qatorda masofaviy pochta serveri jarayoni qo‘ng‘iroq qiluvchiga o‘z nomini, u gapirayotgan protokolni va boshqa qo‘shimcha ma’lumotlarni, masalan, protokol versiyasini, sana va vaqtni e’lon qilish orqali javob beradi. 2-qatorda pochta serverini yuborish jarayoni o‘zini tanishtiradi. 3-qatorda masofaviy server jo‘natuvchi server nomini tan oladi.

Tarmoq xavfsizligi.

Virus - bu kompyuterda allaqachon mavjud bo‘lgan dasturlarga o‘zini kiritish orqali kompyuterga zarar yetkazadigan dastur. Keyin, "xost" dasturi bajarilganda, virus ham bajariladi. Amalga oshirilganda, ko‘pgina viruslar o‘zlarini kompyuterdagi boshqa dasturlar ustidan nazorat qilishga harakat qiladi. Biroq, ba’zi viruslar operatsion tizim qismlarini buzish, ommaviy saqlashning katta bloklarini o‘chirish yoki ma’lumotlar va boshqa dasturlarni buzish kabi halokatli harakatlarni amalga oshiradi.

Worm - bu o‘zini tarmoq orqali uzatadigan, kompyuterlarda joylashadigan va o‘z nusxalarini boshqa kompyuterlarga yo‘naltiradigan avtonom dastur. Virus holatida bo‘lgani kabi, worm ham faqat o‘zini ko‘paytirish yoki ekstremal vandalizm uchun mo‘ljallangan bo‘lishi mumkin. Wormning o‘ziga xos oqibati - bu wormning takrorlangan nusxalarining hosil bo‘lishi, bu qonuniy ilovalarning ish faoliyatini yomonlashtiradi va oxir-oqibat butun tarmoq yoki internetda ortiqcha yuklama hosil qilishi mumkin.

Troyan oti - bu jabrlanuvchi tomonidan o‘z xohishi bilan import qilinadigan o‘yin yoki foydali yordamchi dasturlar to‘plami kabi kerakli dastur sifatida yashiringan kompyuter tizimiga kiradigan dastur. Biroq, kompyuterda troyan oti zararli ta’sir ko‘rsatishi mumkin bo‘lgan qo‘shimcha harakatlarni amalga oshiradi. Ba’zan bu qo‘shimcha harakatlar darhol boshlanadi. Boshqa hollarda, troyan oti ma’lum bir voqea, masalan, oldindan tanlangan sananing paydo bo‘lishi bilan qo‘zg‘atilgunga qadar harakatsiz yotishi mumkin. Troyan otlari ko‘pincha jozibador elektron pochta xabarlariga qo‘shimchalar shaklida keladi. Qo‘shimcha ochilganda (ya’ni, qabul qiluvchi ilovani ko‘rishni so‘raganda), troyan otining noto‘g‘ri harakatlari faollashadi. Shunday qilib, noma’lum manbalardan kelgan elektron pochta qo‘shimchalari hech qachon ochilmasligi kerak.

Zararli dasturiy ta’minotning yana bir ko‘rinishi josuslik dasturlari bo‘lib, u o‘zi joylashgan kompyuterdagi harakatlar haqida ma’lumot to‘playdigan va bu ma’lumotni hujumni qo‘zg‘atuvchiga qaytaradigan dastur hisoblanadi. Ba’zi kompaniyalar josuslik dasturlarini mijozlar profilini yaratish vositasi sifatida ishlatishadi va shu nuqtai nazardan, u shubhali axloqiy ahamiyatga ega. Boshqa hollarda, josuslik dasturi ochiqdan-ochiq zararli maqsadlarda, masalan, parollar yoki kredit karta raqamlarini qidirishda kompyuter klaviaturasida kiritilgan belgilar ketma-ketligini yozib olish uchun ishlatiladi.

Ayg‘oqchi dastur orqali ma’lumotni yashirincha olishdan farqli o‘laroq, fishing ma’lumotni shunchaki so‘rash orqali aniq olish usulidir. Fishing atamasi baliq ovlash so‘zi bo‘yicha o‘yindir, chunki bu jarayon kimdir "o‘lja oladi" degan umidda ko‘plab “tuzoqlar” qo‘yishdir. Fishing ko‘pincha elektron pochta orqali amalga oshiriladi. Jinoyatchi elektron pochta xabarlarini moliya instituti, hukumat byurosi yoki ehtimol huquqni muhofaza qilish organi sifatida yuboradi. Elektron pochta potentsial qurbondan qonuniy maqsadlar uchun zarur bo‘lgan ma’lumotni so‘raydi. Biroq, olingan ma’lumotlar jinoyatchi tomonidan dushmanlik maqsadlarida foydalaniladi.

Viruslar va josuslik dasturlari kabi ichki infektsiyalardan farqli o‘laroq, tarmoqdagi kompyuterga tizimdagi boshqa kompyuterlarda ishlaydigan dasturiy ta’minot ham hujum qilishi mumkin. Misol sifatida, kompyuterni xabarlar bilan ortiqcha yuklash jarayoni bo‘lgan xizmat ko‘rsatishni rad etish (DoS) hujumini keltirish mumkin. Kompaniya biznesini buzish uchun Internetdagi yirik tijorat veb-serverlariga qarshi xizmat ko‘rsatishni rad etish hujumlari boshlandi va ba’zi hollarda kompaniyaning tijorat faoliyatini to‘xtatib qo‘ydi.

Xizmat hujumini rad etish qisqa vaqt ichida ko‘p sonli xabarlarni yaratishni talab qiladi. Buni amalga oshirish uchun tajovuzkor odatda signal berilganda xabarlarni ishlab chiqaradigan ko‘plab shubhasiz kompyuterlarga dasturiy ta’minot o‘rnatadi. Keyin, signal berilganda, bu kompyuterlarning barchasi (ba’zan botnet deb ataladi) maqsadni xabarlar bilan to‘ldiradi. Demak, xizmat hujumlarini rad etishning o‘ziga xos xususiyati shundaki, sherik sifatida foydalanish uchun shubhasiz kompyuterlarning mavjudligi. Shuning uchun barcha shaxsiy kompyuter foydalanuvchilari foydalanilmayotganda Internetga ulangan kompyuterlarini tark etishlari tavsiya etilmaydi. Hisob-kitoblarga ko‘ra, kompyuter Internetga ulangandan so‘ng, kamida bitta buzg‘unchi 20 daqiqa ichida uning mavjudligidan foydalanishga harakat qiladi. O‘z navbatida, himoyalanmagan shaxsiy kompyuter Internetning yaxlitligiga jiddiy tahdid soladi.

Keraksiz xabarlarning ko‘pligi bilan bog‘liq yana bir muammo - spam deb ataladigan keraksiz elektron pochta xabarlarining ko‘payishi. Biroq, xizmat hujumini rad etishdan farqli o‘laroq, spam hajmi kamdan-kam hollarda kompyuter tizimini bosib olish uchun yetarli. Buning o‘rniga, spamning ta’siri spamni qabul qiluvchi odam haqidagi ma’lumotlarni olishdir. Yuqorida aytib o‘tganimizdek, spam viruslar va boshqa zararli dasturlarni tarqatishi mumkin bo‘lgan troyan otlarini qo‘zg‘atish va

fishing uchun keng qo‘llaniladigan vosita ekanligi bu muammoni yanada kuchaytiradi.

Himoya va yaxshilash

Firewall butun tarmoqlar yoki domenlarni emas, balki alohida kompyuterlarni himoya qilish uchun ham ishlatiladi. Misol uchun, agar kompyuter veb-server, nom serveri yoki elektron pochta serveri sifatida ishlatilmayotgan bo‘lsa, u holda bunday ilovalarga yo‘naltirilgan barcha kiruvchi trafikni blokirovka qilish uchun ushbu kompyuterda firewall o‘rnatilishi kerak. Darhaqiqat, buzg‘unchining kompyuterga kirishining bir usuli mavjud bo‘lmagan server tomonidan qoldirilgan "teshik" orqali aloqa o‘rnatishdir. Xususan, josuslik dasturlari tomonidan to‘plangan ma’lumotlarni olishning usullaridan biri zararlangan kompyuterda yashirin serverni o‘rnatishdir, bu orqali zararli mijozlar josuslik dasturlari topilmalarini olishlari mumkin. To‘g‘ri o‘rnatilgan xavfsizlik devori ushbu zararli mijozlarning xabarlarini bloklashi mumkin.

Filtrlovchi konnotatsiyalarga ega bo‘lgan yana bir profilaktik vosita bu proksi-serverdir. Proksi-server - bu mijozni serverning salbiy harakatlaridan himoya qilish maqsadida mijoz va server o‘rtasida vositachi bo‘lgan dasturiy ta’minot birligi. Proksi-serversiz mijoz to‘g‘ridan-to‘g‘ri server bilan bog‘lanadi, ya’ni server mijoz haqida ma’lum miqdorni o‘rganish imkoniyatiga ega. Vaqt o‘tishi bilan, tashkilotning intranetidagi ko‘plab mijozlar uzoq server bilan shug‘ullanar ekan, bu server intranetning ichki tuzilishi haqida ko‘plab ma’lumotlarni to‘plashi mumkin - keyinchalik zararli harakatlar uchun ishlatilishi mumkin bo‘lgan ma’lumotlar. Bunga qarshi turish uchun tashkilot ma’lum bir xizmat turi (FTP, HTTP, telnet va boshqalar) uchun proksi-server o‘rnatishi mumkin. Keyin, har safar intranet ichidagi mijoz shu turdagi server bilan bog‘lanishga harakat qilganda, mijoz haqiqatda proksi-server bilan bog‘lanadi. O‘z navbatida, proksi-server mijoz rolini o‘ynab, haqiqiy server bilan bog‘lanadi. Shu vaqtdan boshlab proksi-server xabarlarni oldinga va orqaga uzatish orqali haqiqiy mijoz va haqiqiy server o‘rtasida vositachi rolini o‘ynaydi. Ushbu tartibga solishning birinchi afzalligi shundaki, haqiqiy server proksi-server haqiqiy mijoz emasligini bilishning imkoni yo‘q va aslida u haqiqiy mijozning mavjudligidan hech qachon xabardor emas. O‘z navbatida, haqiqiy serverda intranetning ichki xususiyatlarini o‘rganish imkoniyati yo‘q. Ikkinchi afzallik shundaki, proksi-server serverdan mijozga yuborilgan barcha xabarlarni filtrlash imkoniyatiga ega. Masalan, FTP proksi-serveri barcha kiruvchi fayllarni ma’lum viruslar mavjudligini tekshirishi va barcha zararlangan fayllarni bloklashi mumkin.

Foydalangan adbiyotlar

1. Rajabov S. et al. Tasavvurli, umumiy-tasavvurli va raqamli-tasavvurli qoidalarni tahlil //Science and Education. – 2024. – T. 5. – №. 5. – C. 262-268.
2. Rajabov S. TASAVVURLI, UMUMIY-TASAVVURLI VA RAQAMLI-TASAVVURLI QOIDALARNI TAHLILI //Raqamli iqtisodiyot va axborot texnologiyalari. – 2024. – T. 4. – №. 1. – C. 113-119.
3. Абдуллаев M. ORGANIZATION OF WASTE PROCESSING IN SOLVING ENVIRONMENTAL PROBLEMS IN UZBEKISTAN //Nordic_Press. – 2024. – T. 1. – №. 0001.
4. Qobilov A. et al. ASSOTSIATIV QOIDALAR VA BOZOR SAVATLARINING TAHLILI //Raqamli iqtisodiyot va axborot texnologiyalari. – 2023. – T. 3. – №. 3. – C. 115-120.
5. Rajabov S. B. et al. Social mining and it is development stages //Science and Education. – 2023. – T. 4. – №. 4. – C. 1342-1345.
6. Oybek o‘g’li O. N., Urinovich K. A., Baxtiyorovich R. S. RAQAMLI IQTISODIYOT SHAROITIDA SOLIQLAR VA BOSHQA MAJBURIY TOLOVLARNI AMALGA OSHIRISHDA RAQAMLI TEXNOLOGIYALARDAN FOYDALANISH //Архив научных исследований. – 2022. – T. 5. – №. 5.
7. Ziyadullayevich S. A., Mirzaliev S. M., Bakhtiyorovich R. S. IMPROVING THE PROGRESSES OF WASTE PRODUCTS PROCESSING THE AUTOMATED MANAGEMENT SYSTEM //Galaxy International Interdisciplinary Research Journal. – 2022. – T. 10. – №. 5. – C. 372-381.
8. Mirzarakhimova A., Abdulakhatov M. Analysis of Healthcare Services in the Digital Economy //Proceedings of the 7th International Conference on Future Networks and Distributed Systems. – 2023. – C. 410-414.
9. Abdulakhatov M. M., Avlokulova S. S. TECHNOLOGY OF SEARCH ORGANIZATION IN VIRTUAL E-SHOPS WITH IMAGE RECOGNITION //Архив научных исследований. – 2022. – T. 2. – №. 1.
10. Kobilov A., Abdulakhatov M., Jaloliddinova M. PECULIARITIES OF THE USE OF ARTIFICIAL INTELLIGENCE IN THE EDUCATIONAL PROCESS //Raqamli iqtisodiyot va axborot texnologiyalari. – 2021. – T. 1. – №. 3. – C. 32-37.
11. Nigmanov A. U. XITOY SANOAT TARMOQLARIDA ENERGIYA SAMARADORLIGINI OSHIRISH TAHLILI //XXI Asr: Fan va ta’lim masalalari (XXI Век: Вопросы науки и образования). – 2024. – T. 1. – C. 146-162.
12. Нигманов А. У. и др. ERKIN IQTISODIY ZONALARDA INVESTITSIYA FAOLIYATINI AMALGA OSHIRISHNING ASOSIY

YONALISHLARI //ГЕОГРАФИЯ: ПРИРОДА И ОБЩЕСТВО. – 2020. – Т. 1. – №. 2.

13. Bobojonov J. B. O. XXR investitsion siyosatining istiqboldagi tendensiyasi //Science and Education. – 2024. – Т. 5. – №. 10. – С. 203-209.

14. Нигманов А. УЗБЕКСКО-КИТАЙСКОЕ ЭНЕРГЕТИЧЕСКОЕ СОТРУДНИЧЕСТВО //Sharq ma'shali/Восточный факел. – 2022. – Т. 14. – №. 1. – С. 127-135.

15. Sofoyeva F. JDK, JRE va JVM. Dasturlash muhitini tayyorlash //Nordic_Press. – 2024. – Т. 3. – №. 0003.

16. Sofoyeva F. Java dasturining asosiy tushunchalari //Nordic_Press. – 2024. – Т. 3. – №. 0003.