KOMPYUTER TROYAN VIRUSLARI

Ismatillayev Avazbek Ziyodullo o'g'li
Guliston Davlat Unversiteti
E-mail: aismatillayev21@gmail.com

ANNOTATSIYA

Kompyuter troyan viruslari maqolamizning asosiy maqsadi troyan viruslarning ishlashi bilan tanishish va bu virusga qarshi qanday choralar qo'llash munkinligini ko'rib chiqamiz.

Kalit so'zlar: Troyan viruslari, masofaviy kirish troyanlari, buzg'unchi troyanlar, proksi-troyanlar, FTP troyanlari, DoS troyanlari.

KIRISH

Troyan virusi - bu zararli dastur bo'lib, u zararli dastur sifatida namoyon bo'ladi.

Viruslardan farqli o'laroq, troyan otlari o'zlarini ko'paytirmaydi, lekin ular xuddi shunday halokatli bo'lishi mumkin. Troyan virusining eng hiyla turlaridan biri bu dastur bo'lib, u kompyuteringizni viruslardan xalos qiladi, lekin uning o'rniga tizimingizga viruslar kiritadi. Bu atama Troya urushi haqidagi yunon afsonasidan kelib chiqqan bo'lib, unda yunonlar o'zlarining dushmanlari - troyanlarga, go'yoki tinchlik qurbonligi sifatida ulkan yog'och otni berishadi. Ammo troyanlar otni shahar devorlari ichiga sudrab olgach, yunon askarlari otning ichi bo'sh qornidan yashirincha chiqib, shahar darvozalarini ochib, o'z vatandoshlariga Troyani to'kib tashlashga va qo'lga kiritishga imkon berishdi.

Troyan viruslari tizimlarni qanday buzishi va yetkazilgan zararga qarab toifalarga bo'linadi.

Troyan viruslaring yettita asosiy turi:

Masofaviy kirish troyanlari:

RATlar deb qisqartirilgan masofaviy kirish troyanlari tajovuzkorga jabrlanuvchining tizimini to‘liq boshqarishini ta’minlash uchun mo‘ljallangan. Buzg‘unchilar odatda bu troyan otlarini o‘yinlarda va boshqa kichik dasturlarda yashirishadi, ular shubhasiz foydalanuvchilar o‘zlarining shaxsiy kompyuterlarida bajaradilar.

Ma’lumotlarni yuborish troyanlari:

Ushbu turdagi troyan otlari tajovuzkorga parollar, kredit karta ma’lumotlari, jurnal fayllari, elektron pochta manzillari yoki IM kontaktlar ro‘yxati kabi nozik ma’lumotlarni taqdim etish uchun mo‘ljallangan. Ushbu troyanlar oldindan aniqlangan ma’lumotlarni (masalan, kredit karta ma’lumotlari yoki parollar) qidirishi mumkin yoki ular keyloggerni o‘rnatadi va barcha yozilgan tugmachalarni tajovuzkorga qaytarib yuboradi.

Buzg‘unchi troyanlar:

Ushbu troyan virusi fayllarni yo‘q qilish va o‘chirish uchun mo‘ljallangan va u boshqa troyanlarga qaraganda ko‘proq virusga o‘xshaydi. Ko‘pincha virusga qarshi dastur tomonidan aniqlanmasligi mumkin.

Proksi-troyanlar:

Ushbu turdagi troyan viruslari jabrlanuvchining kompyuteridan proksi-server sifatida foydalanish uchun mo‘ljallangan. Bu tajovuzkorga kompyuteringizdan har qanday narsani, jumladan, kredit kartalaridagi firibgarlik va boshqa noqonuniy harakatlarni amalga oshirishga va hatto boshqa tarmoqlarga qarshi zararli hujumlarni boshlash uchun tizimingizdan foydalanishga imkon beradi.

FTP troyanlari:

Ushbu troyan virusi 21-portni (FTP uzatish porti) ochadi va tajovuzkorga File Transfer Protocol (FTP) yordamida kompyuteringizga ulanish imkonini beradi. Xavfsizlik dasturlarini o‘chirib qo‘yuvchi troyanlar Bu yomon troyan virusi foydalanuvchi bilmagan holda antivirus dasturlari yoki xavfsizlik devorlari kabi kompyuter xavfsizligi dasturlarini to‘xtatadi yoki o‘ldiradi. U odatda boshqa turdagi troyanlar bilan birlashtirilib, “foydali yuk” hisoblanadi.

Xizmatni rad etish (DoS) troyanlari:

DoS troyanlari tarmoqni foydasiz trafik bilan to‘ldirish orqali uni tiz cho‘ktiruvchi hujum turidir. Ko‘pgina DoS hujumlari, masalan, Ping of Death va Teardrop hujumlari, TCP/IP protokollaridagi cheklovlardan foydalanadi. Ma’lum bo‘lgan barcha DoS hujumlari uchun tizim ma’murlari hujumlar natijasida etkazilgan zararni cheklash uchun o‘rnatishi mumkin bo‘lgan dasturiy ta’minot tuzatishlari mavjud. Ammo, viruslar singari, yangi DoS hujumlari ham xakerlar tomonidan doimo orzu qilinadi.

MUHOKAMA

Kompyuterda troyan virusini aniqlash va undan qanday qutulish bo‘yicha beshta qadam. 1-qadam. Xavfsiz rejim

Kompyuterda troyan otini aniqlash xavfsiz rejimda osonroq, chunki faqat minimal ilovalar ishlaydi. Kiberxavfsizlik bo‘yicha mutaxassislar troyan infektsiyalari kabi turli xil zararli dasturlarni topish uchun xavfsiz rejimni tavsiya qiladilar. Shunday qilib, xavfsiz rejimda kompyuterda troyan virusini qanday aniqlash mumkin:

"Ishga tushirish" tugmasini bosing.

"MSCONFIG" ni kiriting.

Tizim konfiguratsiyasi oynasi ochilganda, "Boot" tugmasini bosing.

"Xavfsiz rejim" ni belgilang.

Windows xavfsiz rejimda qayta ishga tushirilgach, tizim konfiguratsiyasi oynasini yana oching

"Ishga tushirish" ga o‘ting.

Har qanday shubhali ilovani tekshiring. Esingizda bo‘lsin, troyan oti o‘zini qonuniy dasturiy ta’minot sifatida ko‘rsatadi. Agar ilova notanish ko‘rinsa va noshir shubhali bo‘lsa, qo‘shimcha ma’lumot olish uchun uni Google-dan qidiring.

Dasturning zararli ekanligini tasdiqlaganingizdan so‘ng, uni o‘chiring.

"Ilova" ni, keyin esa "OK" ni bosing.

Chiqish, lekin kompyuterni hali qayta ishga tushirmang.

2-qadam. Vazifa menejeri

Troyan virusi butunlay o‘chirilganligiga ishonch hosil qilish uchun uning jarayonini Vazifa menejerida tugatishingiz kerak. Agar siz kompyuteringizdagi barcha faol ilovalarni ko‘rishni istasangiz, ularni Vazifa menejerida ko‘rasiz.

Ctrl+Alt+Del tugmalarini bosing.

"Jarayonlar" yorlig‘iga o‘ting.

Ishga tushirishda topilgan bir xil zararli dasturni qidiring.

Unga bosing va jarayonni yakunlang.

Bu troyan virusining kompyuterdagi faoliyatini to‘xtatishi kerak edi. Endi siz zararli dasturni o‘chirib tashlashingiz mumkin.

Qadam 3. Dasturlar va xususiyatlar

Dasturlar va xususiyatlar bo‘limida siz kompyuteringizda o‘rnatilgan barcha ilovalarni ko‘rasiz. Ishga tushirish va Vazifa menejerida topilgan zararli dasturlarni o‘chirib tashlashingiz mumkin. Dasturlar va funksiyalar orqali kompyuterda troyan virusini qanday aniqlash mumkin.

"Ishga tushirish" tugmasini bosing.

"Boshqarish paneli" ni tanlang.

"Dasturlar va xususiyatlar" bo‘limiga o‘ting.

Zararli dasturni o‘chirib tashlang.

Bundan tashqari, siz o‘rnatmagan boshqa keraksiz dasturlarni tekshirishingiz va uni olib tashlashingiz mumkin.

Kompyuterni qayta ishga tushirmasdan chiqing.

Qadam 4. Vaqtinchalik fayllarni tozalash

Troyan viruslarini olib tashlash va aniqlash vaqtinchalik internet fayllarini tozalash orqali tezroq bo‘ladi. TEMP papkasi zararli dastur o‘zining xavfsizlik sozlamalari zaifligi tufayli ko‘pincha yashiringan joy. Barcha vaqtinchalik fayllarni tozalash nafaqat troyan otidan darhol xalos bo‘ladi, balki kompyuterda biroz joy bo‘shatadi.

"Ishga tushirish" tugmasini bosing.

“%temp%” kiriting.

Barcha vaqtinchalik fayllarni tozalang.

Bu kompyuterdan zararli dasturlarning qoldiqlarini olib tashlashi kerak edi.

5-qadam. Zararli dasturlar skaneri

Agar kompyuteringiz zararli dasturlardan xoli ekanligiga ishonch hosil qilishni istasangiz, zararli dastur skanerini yuklab oling. Bu kompyuterni troyan virusi, to‘lov dasturi, josuslik dasturi, keylogger, rootkit, qurtlar va viruslar kabi zararli dasturlardan himoya qilish uchun mo‘ljallangan dastur.

U kompyuteringizga kirgan fayllarni chuqur skanerdan o‘tkazib, zararli dasturlarni fayl tizimiga zarar yetkazishidan oldin aniqlaydi, shuning uchun kompyuterda troyan virusini qanday aniqlash haqida tashvishlanishingiz shart emas. Bundan tashqari, muhim papkalarda yashiringan har qanday zararli dasturlarni aniqlash uchun kompyuteringizni muntazam ravishda tekshiradi.

Zararli dasturlar skanerini ishga tushirish troyan otini kompyuterdan aniqlash va olib tashlashning eng yaxshi usuli hisoblanadi. Internetda ishonchli va samarali zararli dasturlarni skanerlash dasturini qidiring. Yuklab olish uchun turli xil zararli dasturlar skanerlari mavjud, ammo kompyuteringizni zararli dasturlarning ilg‘or turlaridan himoya qila oladiganini tanlang.

XULOSA

Bu mavzuni tanlashda xozirgi kunda dolzarb muammoga aylanib borayotgan virus turlaridan biri bilan tanishtirish va o‘z o‘rnida uning imkoniyati tushuntirish bilan birgalikda ximoyalanish uchun nimalar qilish zarurligini sizlarga yetkazishdir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)

1. http://ru.wikipedia.org/wiki
2. https://enterprise.xcitium.com
3. https://github.com/topics/blocked-websites