3– SON / 2022 - YIL / 15 - NOYABR

MA'LUMOTLARNI INTELEKTUAL QIYOSIY TAHLILLASHGA ASOSLANIB POTENSIAL ZARARLI FAYILLARNI ANIQLASHNING TIZIMLI YONDASHUVINI ISHLAB CHIQISH.

SHerzod Sobirovich Karimov

ТАТУ Нурафшон филиали "Таълим сифатини назорат қилиш бўлими бошлиғи" PhD, доцент

Jo'rayev Otabek Isomiddinovich

Muhammad Al-Xorazmiy Nomidagi Toshkent Axborot Texnologiyalari Universiteti Farg'ona Filiali "Kompyuter injiniringi" fakulteti M1-21 magistri

Annotatsiya: *Ushbu maqolada ma'lumotlarni intelektual qiyosiy tahlillashga asoslanib potensial zararli fayillarni aniqlashning tizimli yondashuvini ishlab chiqish, ko'pgina yuqumli fayllar, jumladan, Morris Worm, birinchi internet qurti, kompyuterlar zararli fayllardan himoyalanishi to'g'risida yozilgan.*

Kalit so'zlar: *internet, fayl, tizm, intelektual, kiberjinoyatlar, ta'minot, viruslar, to'lov, josuslik, reklama, izolyatsiya, antivirus.*

Zararli fayl (zararli fayliy ta'minot so'zining portmanteausi (tovushlarni aralashtirib, ikkita so'zning ma'nosini birlashtirgan so'z)) bu kompyuter, server, mijoz yoki kompyuter tarmog'ini buzish, shaxsiy ma'lumotlarni o'g'irlash, ma'lumotlar yoki tizimlarga ruxsatsiz kirish, foydalanuvchining kompyuter xavfsizligi va maxfiyligi to'siqlarini buzib kirgan holda foydalanuvchilarni ma'lumotlarga kirishdan mahrum qiladigan har qanday fayliy ta'minotdir. Ushbu fayl keltirib chiqaruvchi holatga o'xshash vaziyatlar ham mavjud. Ba'zi kamchiliklar tufayli zarar keltiradigan fayliy ta'minot odatda fayliy ta'minot xatosi sifatida tavsiflanadi. Zararli fayllar Internetda jismoniy shaxslar va korxonalar uchun jiddiy muammolarni keltirib chiqaradi. Symantec kompaniyasining 2018-yildagi Internet xavfsizligi tahdidi hisobotiga (ISTR) ko'ra, 2017-yilda zararli fayllar soni 669 947 865 taga ko'paygan, bu 2016-yilgi ko'rsatgichlarga qaragandan ikki baravar ko'p degani. Zararli fayliy ta'minot hujumlari va kompyuter orqali sodir etilgan boshqa jinoyatlarni o'z ichiga olgan kiberjinoyatlar 2021-yilda jahon iqtisodiyotiga 6 trillion dollarga tushgan va ushbu miqdor yiliga 15 % miqdorda oshib bormoqda.

Zararli fayllarning ko'p turlari mavjud. Kompyuter viruslari, qurtlar, troyan otlari, to'lov fayli, josuslik fayllari, reklama fayllari va o'chiruvchi fayllar shular jumlasidandir. Zararli fayllardan himoya qilish strategiyala ularning turiga qarab farqlanadi, lekin ularning aksariyatini antivirus fayllari, xavfsizlik devorlarini o'rnatish, kunlik hujumlarni kamaytirish uchun muntazam himoyalarni qo'llash, tarmoqlarni bosqindan himoya qilish, muntazam zahira nusxalariga ega bo'lish va zararlangan tizimlarni izolyatsiya qilish orqali oldini olish mumkin. Zararli fayllar antivirus

fayllarini aniqlash algoritmlaridan qochish qobilyatiga ega qilib dasaturlanishga harakat qilishmoqda[8].

Tarixi

O‘z-o‘zini qayta yaratuvchi kompyuter fayli tushunchasi murakkab avtomatlarning ishlashi haqidagi dastlabki nazariyalarga borib taqaladi. Jon fon Neyman nazariy jihatdan fayl o‘zini takrorlashi mumkinligini ko‘rsatib bergan. Bu hisob-kitoblar nazariyasida ma’qullik natijasi bo‘lib zimat qiladi. Fred Koen kompyuter viruslari bilan tajriba o‘tkazadi va Neymanning nazariyasini tasdiqlaydi. Oddiy shifrlash yordamida aniqlanishi va o‘zini o‘zi chalkashtirish kabi zararli fayllarning boshqa xususiyatlarini o‘rganadi. Uning 1987-yil doktorlik dissertatsiyasi kompyuter viruslari mavzusiga bag‘ishlangan. Virusning foydali yukining bir qismi bu kriptografik texnologiyaning kombinatsiyasidir. Uni hujum qilish uchun qo‘llash 1990-yillarning o‘rtalarida boshlangan va o‘rganilgan dastlabki to‘lov faylini o‘z ichiga oladi.

Internetga kirish keng tarqalgunga qadar, viruslar bajariladigan fayllar yoki floppi disklarning yuklash sektorlarini zararlash orqali shaxsiy kompyuterlarda tarqaladi. Ushbu fayllar yoki yuklash sektorlaridagi mashina kodi ko‘rsatmalariga o‘zining nusxasini kiritish orqali virus fayl ishga tushirilganda yoki disk yuklanganda o‘zini ishga tushiradi. Dastlabki kompyuter viruslari Apple II va Macintosh uchun yozilgan, biroq ular IBM PC va MS-DOS tizimlarining hukmronligi bilan kengroq tarqala boshlagan edi. „Yovvoyi (wild)“ faylidagi birinchi IBM PC virusi 1986-yilda Pokistondagi aka-uka Faruk Alvi tomonidan yaratilgan (c)Brain deb nomlangan yuklash sektori virusi bo‘lgan[14]. Zararli fayl distribyutorlari foydalanuvchini zararlangan qurilma yoki vositadan yuklash yoki ishga tushirish uchun aldaydi. Masalan, virus zararlangan kompyuterni unga ulangan har qanday USB flesh-diskiga avtomatik ishga tushiriladigan kod qo‘shishga majbur qilishi mumkin. USB dan avtomatik ishga tushirish uchun boshqa kompyuterga biriktirilgan har bir kishi o‘z navbatida zararlantiruvchini yuqtiradi.

Eski elektron pochta fayli potentsial zararli JavaScript kodini o‘z ichiga olgan HTML elektron pochtani avtomatik ravishda ochadi. Foydalanuvchilar yashirin zararli elektron pochta biriktirmalarini ham ishga tushirishlari mumkin. CSO Online tomonidan iqtibos keltirgan Verizon tomonidan 2018-yilda ma’lumotlar buzilishi bo‘yicha tekshiruvlar hisobotida aytilishicha, elektron pochta xabarlari zararli fayllarni yetkazib berishning asosiy usuli bo‘lib, butun dunyo bo‘ylab zararli fayllarni yetkazib berishning 92 foizini tashkil qiladi.

Birinchi qurtlar, tarmoq orqali yuqadigan yuqumli fayllar shaxsiy kompyuterlarda emas, balki ko‘p vazifali Unix tizimlarida paydo bo‘lgan. Birinchi mashhur qurt SunOS va VAX BSD tizimlarini yuqtirgan 1988-yildagi kompyuter qurti edi. Virusdan farqli o‘laroq, bu qurt o‘zini boshqa fayllarga kiritmagan. Buning o‘rniga, u tarmoq serveri fayllaridagi xavfsizlik teshiklaridan (zaifliklardan) foydalangan va o‘zini alohida

jarayon sifatida ishga tushirgan. Xuddi shu xatti-harakatni bugungi davr qurtlari ham qo‘llaydi.

1990-yillarda Microsoft Windows platformasining yuksalishi va uning ilovalarining moslashuvchan makroslari tufayli Microsoft Word va shunga o‘xshash fayllarning makro tilida yuqumli kod yozish imkoniyati paydo bo‘ldi. Ushbu so‘l viruslar ilovalar (bajariladigan fayllar) emas, balki hujjatlar va shablonlarni yuqtiradi, lekin Word hujjatidagi makrolar bajariladigan kod shakli ekanligiga tayanadi.

Ko‘pgina yuqumli fayllar, jumladan, Morris Worm, birinchi internet qurti, tajriba hamda shunchaki hazil sifatida yozilgan. Bugungi kunda zararli fayl Black Hat Xakerlar va hukumatlar tomonidan shaxsiy, moliyaviy yoki biznes ma’lumotlarini o‘g‘irlash uchun foydalaniladi. Bugungi kunda USB portiga ulanadigan har qanday qurilma — hatto chiroqlar, fanatlar, dinamiklar, o‘yinchoqlar yoki raqamli mikroskop kabi tashqi qurilmalar — zararli fayllarni tarqatish uchun ishlatilishi mumkin. Sifat nazorati yetarli bo‘lmasa, ishlab chiqarish yoki yetkazib berish jarayonida qurilmalar yuqishi mumkin.

Maqsadlar

Zararli fayl ba’zan hukumat yoki korporativ veb-saytlarga qarshi himoyalangan ma’lumotlarni to‘plash yoki umuman ularning faoliyatini to‘xtatish uchun keng qo‘llaniladi. Biroq, zararli fayl shaxsiy identifikatsiya raqamlari yoki rekvizitlari, bank yoki kredit karta raqamlari va parollar kabi ma’lumotlarni olish uchun jismoniy shaxslarga qarshi ishlatilishi mumkin.

Keng tarmoqli ravishda Internetga kirishning o‘sishidan beri zararli fayllar ko‘proq foyda olish uchun ishlab chiqilmoqda. 2003-yildan beri keng tarqalgan virus va qurtlarning aksariyati foydalanuvchilarning kompyuterlarini noqonuniy maqsadlarda nazorat qilish uchun mo‘ljallangan. Infeksiyalangan „zombi kompyuterlar“ elektron pochta spamlarini yuborish, bolalar pornografiyasi kabi kontrabanda ma’lumotlarini joylashtirish yoki tovlamachilik shakli sifatida tarqatilgan xizmat ko‘rsatishni rad etish hujumlarini amalga oshirish uchun ishlatilishi mumkin.

Foydalanuvchilarning veb-sahifalarini ko‘rishni kuzatish, keraksiz reklamalarni ko‘rsatish yoki sheriklik marketingi daromadlarini qayta yo‘naltirish uchun mo‘ljallangan fayllar josuslik fayllari deb ataladi. Spyware fayllari viruslar kabi tarqalmaydi; Buning o‘rniga ular odatda xavfsizlik teshiklaridan foydalanish orqali o‘rnatiladi. Ular, shuningdek, foydalanuvchi tomonidan o‘rnatilgan bog‘liq bo‘lmagan fayliy ta’minot bilan birga yashirilishi va paketlanishi mumkin. Sony BMG rootkiti noqonuniy nusxa ko‘chirishning oldini olishga mo‘ljallangan edi; ammo foydalanuvchilarning tinglash odatlari oshkor bo‘lib qoldi va beixtiyor qo‘shimcha xavfsizlik zaifliklarini yuzaga keltirdi.

Ransomware to‘lov to‘lanmaguncha foydalanuvchining o‘z fayllariga kirishiga to‘sqinlik qiladi. To‘lov faylining ikkita varianti mavjud, ular kripto ransomware va locker ransomware. Locker ransomware shunchaki kompyuter tizimini uning tarkibini

shifrlamasdan bloklaydi, kripto ransomware esa tizimni bloklaydi va uning mazmunini shifrlaydi. Misol uchun, CryptoLocker kabi fayllar fayllarni xavfsiz va faqat katta miqdorda pul to‘lagan holda ularni shifrlaydi.

Ba’zi zararli fayllardan firibgarlik orqali pul ishlab chiqarish uchun foydalaniladi, bu kompyuter foydalanuvchisi saytdagi reklama havolasini bosgandek ko‘rinadi va reklama beruvchidan to‘lov undirib olishga urinadi. 2012-yilda hisob-kitoblarga ko‘ra, barcha faol zararli fayllarning taxminan 60-70 foizi qandaydir reklama tomosha qilish orqali yuzaga kelgan firibgarlikdan foydalangan va barcha reklama bosishlarining 22 foizi firibgarlikdir.

Jinoiy pul ishlab chiqarishdan tashqari, zararli fayllar ko‘pincha siyosiy maqsadlar uchun sabotaj uchun ishlatilishi mumkin. Masalan, Stuxnet juda aniq sanoat uskunalarini buzish uchun mo‘ljallangan. Ular siyosiy maqsadli hujumlar bo‘lib, ular yirik kompyuter tarmoqlariga tarqalib, ularni yopib qo‘ydi, jumladan, „kompyuterni o‘ldirish“ deb ta’riflangan fayllarni ommaviy o‘chirish va asosiy yuklash yozuvlarini buzish kabi ko‘niklamalarni o‘z ichiga oladi. Bunday hujumlar Sony Pictures Entertainment kompaniyasiga (2014-yil 25-noyabrda Shamoon yoki W32 deb nomlanuvchi zararli fayllardan foydalangan holda) qilingan (Disttrackva Saudi Aramco (2012-yil avgust).

Turlari

Ushbu toifalar bir-birini istisno qilmaydi, shuning uchun zararli fayllar bir nechta usullardan foydalanishi mumkin.

Troya oti

Troyan oti bu zararli fayl bo‘lib, jabrlanuvchini uni o‘rnatishga ko‘ndirish uchun o‘zini oddiy, foydali fayl yoki yordamchi fayl sifatida namoyon qiladi. Troyan oti odatda fayl ishga tushirilganda faollashtiriladigan yashirin halokatli funktsiyaga ega. Bu atama Troya shahriga yashirincha bostirib kirishda foydalanilgan troyan oti haqidagi qadimgi yunon hikoyasidan olingan.

Troyan otlari odatda ijtimoiy injeneriyaning ba’zi shakllari orqali tarqaladi, masalan, foydalanuvchi shubhasiz ko‘rinishga ega bo‘lgan elektron pochta ilovasini (masalan, to‘ldirilishi kerak bo‘lgan muntazam shakl) yoki mashinada yuklab olish orqali aldaganida. Ularning foydali yuki har qanday bo‘lishi mumkin bo‘lsa-da, ko‘plab zamonaviy shakllar orqa eshik vazifasini bajaradi, tekshirgich bilan bog‘lanadi (uyga qo‘ng‘iroq qilish), keyinchalik zararlangan kompyuterga ruxsatsiz kirish imkoniyatiga ega bo‘lishi mumkin, maxfiy ma’lumotlarni o‘g‘irlash uchun keylogger kabi qo‘shimcha fayllarni o‘rnatishi mumkin, kriptominatsiya fayllari yoki reklama fayllari. troyan operatoriga daromad olish uchun[39]. Troyan otlari va orqa eshiklarni o‘z-o‘zidan aniqlash oson bo‘lmasa-da, kompyuterlar sekinroq ishlayotgandek ko‘rinishi mumkin, protsessor yoki tarmoqdan og‘ir foydalanish tufayli ko‘proq issiqlik yoki fan shovqini chiqaradi, chunki kriptominatsiya fayli o‘rnatilganda paydo bo‘lishi mumkin.

Kriptominerlar manbalardan foydalanishni cheklashi va/yoki aniqlashdan qochish uchun faqat bo‘sh vaqtlarda ishlashi mumkin.

Kompyuter viruslari va qurtlaridan farqli o‘laroq, troyan otlari odatda o‘zlarini boshqa fayllarga kiritishga yoki boshqa yo‘l bilan tarqalishga harakat qilmaydi.

2017-yil bahorida Mac foydalanuvchilari Proton Remote Access Trojan (RAT)[41] ning yangi versiyasiga duch kelishdi brauzerni avtomatik to‘ldirish ma’lumotlari, Mac-OS kalitlari zanjiri va parollar omborlari kabi turli manbalardan parol ma’lumotlarini chiqarishga o‘rgatilgan.

Yengillashuv

Antivirus / Zararli fayllarga qarshi fayl

Anti-zararli fayllar (ba’zan antivirus deb ham ataladi) zararli fayllarning ayrim yoki barcha turlarini bloklaydi va olib tashlaydi. Masalan, Microsoft Security Essentials (Windows XP, Vista va Windows 7 uchun) va Windows Defender (Windows 8, 10 va 11 uchun) real vaqtda himoyani ta’minlaydi. Windows zararli fayllarni olib tashlash vositasi tizimdan zararli fayllarni olib tashlaydi[43]. Bundan tashqari, Internetdan bepul yuklab olish uchun bir nechta qobiliyatli antivirus fayllari mavjud (odatda notijorat maqsadlarda foydalanish uchun cheklangan).Sinovlar ba’zi bepul fayllarni tijorat fayllari bilan raqobatbardosh ekanligini aniqladi.

Odatda, antivirus fayllari zararli fayllarga qarshi quyidagi usullar bilan kurashishi mumkin:

Haqiqiy vaqtda himoya: Ular kompyuterda zararli fayllarni o‘rnatishdan real vaqt rejimida himoya qilishlari mumkin. Zararli fayllardan himoyalanishning bu turi virusga qarshi himoya bilan bir xil ishlaydi, chunki zararli fayllarga qarshi fayl barcha kiruvchi tarmoq ma’lumotlarini zararli fayllarga skanerlaydi va u duch kelgan har qanday tahdidlarni bloklaydi.

O‘chirish: Zararli fayllarga qarshi fayllardan faqat kompyuterga allaqachon o‘rnatilgan zararli fayllarni aniqlash va o‘chirish uchun foydalanish mumkin. Ushbu turdagi zararli fayllarga qarshi fayl Windows reestri, operatsion tizim fayllari va kompyuterda o‘rnatilgan fayllarni skanerlaydi va topilgan har qanday tahdidlar ro‘yxatini taqdim etadi, bu foydalanuvchiga qaysi fayllarni o‘chirish yoki saqlashni tanlash yoki solishtirish imkonini beradi. bu ro‘yxat mos keladigan fayllarni o‘chirib tashlaydigan ma’lum zararli fayl komponentlari ro‘yxatiga.

Sandboxing: Xavfli deb hisoblangan ilovalarni (masalan, ko‘pchilik zaifliklar o‘rnatilishi mumkin bo‘lgan veb-brauzerlar) sinovdan o‘tkazishni ta’minlang.

Haqiqiy vaqtda himoya

Odatda kirish yoki real vaqtda skaner deb ataladigan zararli fayllarga qarshi fayliy ta’minotning o‘ziga xos komponenti operatsion tizim yadrosi yoki yadrosiga chuqur kirib boradi va ma’lum zararli fayllarning o‘zi qanday ishlashga urinishiga o‘xshash tarzda ishlaydi foydalanuvchining tizimni himoya qilish uchun xabardor qilingan ruxsati. Har qanday vaqtda operatsion tizim faylga kirsa, kirish skaneri faylning

zararlangan yoki yo‘qligini tekshiradi. Odatda, zararlangan fayl topilganda, ijro etish to‘xtatiladi va tizimning qaytarib bo‘lmaydigan shikastlanishining oldini olish maqsadida fayl keyingi zararni oldini olish uchun karantinga qo‘yiladi. Aksariyat AVlar foydalanuvchilarga ushbu xatti-harakatni bekor qilishga imkon beradi. Bu operatsion tizimning ishlashiga sezilarli ta’sir ko‘rsatishi mumkin, ammo ta’sir darajasi virtual xotirada qancha sahifa yaratishiga bog‘liq.

Sandboxing

Ko‘pgina zararli fayliy ta’minot komponentlari brauzer ekspluatatsiyasi yoki foydalanuvchi xatosi natijasida o‘rnatilganligi sababli, xavfsizlik fayllari (ularning ba’zilari zararli fayllarga qarshi bo‘lsa-da, ko‘pchilik bo‘lmasa-da) brauzerlarni „sandbox“ qilish uchun (aslida brauzerni kompyuterdan va shuning uchun har qanday zararli fayldan ajratib turadi) sabab bo‘lgan o‘zgarish) har qanday zararni cheklashda ham samarali bo‘lishi mumkin.

Veb-sayt xavfsizligini skanerlash

Veb-sayt zaifliklarini skanerlash veb-saytni tekshiradi, zararli fayllarni aniqlaydi, eskirgan fayliy ta’minotni ko‘rsatishi va saytning buzilishi xavfini kamaytirish uchun ma’lum xavfsizlik muammolari haqida xabar berishi mumkin.

Tarmoqni ajratish

Tarmoqni kichikroq tarmoqlar to‘plami sifatida tuzish va ular orasidagi trafik oqimini qonuniy ekanligi ma’lum bo‘lganiga cheklash, yuqumli zararli fayllarning kengroq tarmoq bo‘ylab o‘zini ko‘paytirish qobiliyatiga to‘sqinlik qilishi mumkin. Software Defined Networking bunday boshqaruv vositalarini amalga oshirish usullarini taqdim etadi.

„Air gap“ izolyatsiyasi yoki „parallel tarmoq“

Oxirgi chora sifatida kompyuterlar zararli fayllardan himoyalanishi mumkin va zararlangan kompyuterlarning ishonchli ma’lumotlarni tarqatish xavfi „havo bo‘shlig‘i“ (ya’ni ularni boshqa barcha tarmoqlardan butunlay uzib qo‘yish) va kirish va kirish ustidan yaxshilangan boshqaruvni qo‘llash orqali sezilarli darajada kamayishi mumkin. fayliy ta’minot va ma’lumotlarning tashqi dunyodan chiqishi. Biroq, zararli fayliy ta’minot ba’zi holatlarda havo bo‘shlig‘ini kesib o‘tishi mumkin, chunki havo bo‘shlig‘i bo‘lgan tarmoqqa fayliy ta’minotni kiritish zarurati tufayli va ulardagi aktivlarning mavjudligi yoki yaxlitligiga zarar etkazishi mumkin. Stuxnet maqsadli muhitga USB drayv orqali kiritilgan zararli fayllarga misol bo‘lib, ma’lumotlarni o‘chirishga hojat qoldirmasdan atrof-muhitda qo‘llab-quvvatlanadigan jarayonlarga zarar etkazadi.

AirHopper, BitWhisper, GSMem, va Fansmitter tadqiqotchilar tomonidan taqdim etilgan texnikalar bo‘lib, ular himoyalanmagan kompyuterlarda elektromagnit, termal va akustik emissiyalar yordamida ma’lumotlarni chiqarishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI.

1. *„Defining Malware: FAQ“. technet.microsoft.com. 10-sentabr 2009-yil.*

2. *Cani, Andrea; Gaudesi, Marco; Sanchez, Ernesto; Squillero, Giovanni; Tonda, Alberto (2014-03-24).*

3. *New York, NY, USA: Association for Computing Machinery. 157–160-bet.*

4. *Brewer, Ross (2016-09-01).„Ransomware attacks: detection, prevention and cure“. Network Security (inglizcha). 2016-jild, № 9. 5–9-bet.*

5. *Fred Cohen, „Computer Viruses“, PhD Thesis, University of Southern California, ASP Press, 1988.*

6. *Young, Adam. Malicious cryptography - exposing cryptovirology. Wiley, 2004 — 1–392 bet.*

7. *„Boot sector virus repair“. Antivirus.about.com (10-iyun 2010-yil). 12-yanvar 2011-yilda asl nusxadan arxivlandi. Qaraldi: 27-avgust 2010-yil.*

8. *Avoine, Gildas. Computer system security: basic concepts and solved exercises. EFPL Press, 2007 — 20 bet.*

9. *„USB devices spreading viruses“. CNET. CBS Interactive. Qaraldi: 18-fevral 2015-yil.*

10. *Fruhlinger. „Top cybersecurity facts, figures and statistics for 2018“. CSO Online (10-oktabr 2018-yil). Qaraldi: 20-yanvar 2020-yil.*