KOMPYUTER TARMOQLARIDA RANSOMWARE HUJUMLARI VA ULARGA QARSHI HIMOYA USULLARI

Ibragimov Sh.M.[1], To'xtasinova G.A.[2]

[1]FarDU dotsenti, shavkat19702008@gmail.com

[2]FarDU talabasi, toxtasinovagulbahor29@gmail.com

Annotatsiya: *Ushbu maqolada zamonaviy kompyuter tarmoqlaridagi eng xavfli tahdidlardan biri - ransomware (to'lov talab qiluvchi zararli dastur) hujumlari va ularga qarshi samarali himoya usullari tadqiq etiladi. Tadqiqot doirasida ransomware hujumlarining texnik mexanizmi, tarqalish yo'llari hamda WannaCry, NotPetya va Colonial Pipeline kabi real hodisalar tahlil qilindi. Natijalar shuni ko'rsatmoqdaki, ushbu tahdidga qarshi bir qirrali texnik yechim samarasiz bo'lib, ko'p qatlamli himoya - zaxira nusxalash, patch management, EDR tizimlari, xodimlarni o'qitish va Zero Trust mikrosegmentatsiyasi - birgalikda qo'llanilgandagina yuqori darajadagi xavfsizlik ta'minlanadi.*

Kalit so'zlar: *kiberxavfsizlik, ransomware, zararli dastur, zaxira nusxalash, patch management, EDR, Zero Trust, mikrosegmentatsiya, fishing, kompyuter tarmog'i.*

KIRISH

Zamonaviy raqamli iqtisodiyot sharoitida kompyuter tarmoqlari davlat boshqaruvi, moliyaviy operatsiyalar, sog'liqni saqlash, ta'lim va kritik infratuzilma obyektlari uchun asosiy vosita sifatida xizmat qilmoqda. Shu bilan birga, ushbu tarmoqlarga qaratilgan kiberjinoyatchilikning yangi va juda xavfli shakli - ransomware, ya'ni to'lov talab qiluvchi zararli dasturlar hujumi - global miqyosda keng tarqalmoqda. Xalqaro hisobotlarga ko'ra, so'nggi yillarda ransomware hujumlari tufayli yetkazilgan jahon zarari yillik o'nlab milliard AQSh dollarini tashkil etib, har bir muvaffaqiyatli hujumning o'rtacha to'lov miqdori va tiklanish xarajati doimiy ravishda o'sib bormoqda [8].

Ushbu tahdidning halokatli miqyosini 2017-yildagi WannaCry epidemiyasi yaqqol namoyon etdi - bir necha kun ichida 150 dan ortiq davlatdagi 300 mingdan ziyod kompyuter zararlangan, shu jumladan Britaniya Milliy Sog'liqni Saqlash Xizmati (NHS) tizimi jiddiy shikastlangan edi. 2021-yildagi Colonial Pipeline quvuriga qaratilgan hujum esa AQShning Sharqiy qirg'og'idagi yoqilg'i ta'minotini bir necha kunga to'xtatib qo'ydi va kiberhujumlar nafaqat raqamli, balki jismoniy oqibatlarga ham olib kelishi mumkinligini ko'rsatdi. O'zbekiston Respublikasi sharoitida ham 2022-yilda qabul qilingan "Kiberxavfsizlik to'g'risida"gi Qonun kritik axborot infratuzilmasini himoyalash zaruriyatini huquqiy darajada mustahkamladi [7], bu esa mavzuning milliy miqyosdagi dolzarbligini yanada tasdiqlaydi.

Mazkur tadqiqotning maqsadi - ransomware hujumlarining texnik mexanizmi, tarqalish vektorlari va oqibatlarini chuqur tahlil qilish, shuningdek, ularga qarshi eng samarali himoya usullarini aniqlash va tizimlashtirishdan iborat. Ilgari surilayotgan asosiy gipoteza shundan iboratki, ransomware tahdidini samarali bartaraf etish faqatgina yakka texnik yechim bilan emas, balki texnik, tashkiliy va insoniy omillarni uzviy birlashtirgan ko'p qatlamli himoya strategiyasi orqali amalga oshirilishi mumkin.

Ransomware hujumlari muammosi so'nggi o'n yillikda xalqaro ilmiy hamjamiyatning faol tadqiqot yo'nalishlaridan biriga aylangan. W. Stallings o'zining "Network Security Essentials" asarida zararli dasturlarning klassifikatsiyasi va kriptografik himoya mexanizmlarini tizimli bayon etgan [1]. B. Schneier esa "Secrets and Lies" monografiyasida kiberhujumlarning muvaffaqiyati ko'pincha texnik zaifliklarga emas, balki insoniy omil va noto'g'ri sozlangan tashkiliy jarayonlarga bog'liq ekanligini asoslab bergan [2]. R. Anderson "Security Engineering" fundamental kitobida taqsimlangan tizimlarda ishonchli himoya arxitekturasini yaratishning asosiy prinsiplarini izchil ta'riflagan [11]. NIST mutaxassislari tomonidan tayyorlangan SP 800-207 hujjatida rasmiylashtirilgan Zero Trust modeli ransomware kabi lateral harakat qiladigan tahdidlarga qarshi an'anaviy perimetr asosidagi himoyaning cheklovlarini bartaraf etishning asosiy yo'li sifatida taklif etilgan [3]. R. Richardson va M. North o'z tadqiqotida ransomware'ning rivojlanish

bosqichlari va unga qarshi kurashning texnik usullari bo'yicha tizimli tahlil keltirgan [4], R. Kaur va N. Kaur esa so'nggi tadqiqotlarida ransomware'ni mashina o'rganish asosida aniqlashning istiqbolli yo'nalishlarini umumlashtirgan [10]. Mahalliy tadqiqotchilar - G'ulomov Sh.R. va Karimov I.X. o'z darsliklarida axborot xavfsizligi asoslarini O'zbekiston sharoiti bilan uzviy yoritgan [5], Usmonov Sh.Yu. esa milliy segmentdagi kiberhujumlar, jumladan ransomware hodisalarini tipologik tahlil qilgan [6]. ENISA Threat Landscape va Verizon DBIR yillik hisobotlari zamonaviy ransomware manzarasini aks ettiruvchi birlamchi statistik manba sifatida ushbu tadqiqotda keng foydalanildi [8][9].

Tadqiqotda bir nechta o'zaro bog'liq ilmiy usullar majmui qo'llanildi: tizimli yondashuv asosida ransomware tahdid ekotizimi yaxlit murakkab tizim sifatida o'rganildi; qiyosiy tahlil orqali turli himoya texnologiyalarining samaradorligi solishtirildi; keys-stadi usuli vositasida real hodisalar - WannaCry, NotPetya va Colonial Pipeline - batafsil o'rganildi; umumlashtirish usulidan foydalanilib, xorijiy va mahalliy manbalardagi amaliy tavsiyalar bir butun kompleks strategiya sifatida tizimlashtirildi. Ushbu metodologik majmua tadqiqot natijalarining ob'ektivligi va amaliy asoslanganligini ta'minlashga xizmat qildi.

Ransomware - maxsus toifadagi zararli dastur bo'lib, u jabrlanuvchining kompyuterini yoki butun tarmoq bo'ylab joylashgan fayllarni kuchli kriptografik algoritmlar, odatda AES-256 simmetrik shifrlash va RSA-2048 asimmetrik kalitli sxemalar yordamida shifrlaydi, so'ngra deshifrlash kaliti evaziga kriptovalyutada (odatda Bitcoin yoki Monero) to'lov talab qiladi. Zamonaviy ransomware oilalari - LockBit, Conti, REvil, BlackCat (ALPHV) - nafaqat shifrlash, balki "double extortion" (ikki tomonlama tovlamachilik) taktikasini ham qo'llaydi: fayllarni shifrlashdan oldin ularni tarmoqdan eksfiltratsiya qiladi va to'lov qilinmasa maxfiy ma'lumotlarni nashr etish bilan qo'rqitadi. So'nggi yillarda "triple extortion" sxemasi ham paydo bo'ldi - bunda jabrlanuvchining mijozlari, hamkorlari yoki hatto bemorlariga ham bevosita bosim o'tkaziladi, bu esa psixologik va huquqiy bosimni maksimal darajada kuchaytiradi.

Ransomware hujumlari turli yo'llar orqali amalga oshiriladi, ular orasida eng keng tarqalganlari - fishing xabarlari orqali yuboriladigan zararli ilovalar yoki havolalar, himoyasiz RDP (Remote Desktop Protocol) xizmatlari, yangilanmagan dasturiy ta'minotdagi ma'lum zaifliklarni ekspluatatsiya qilish, zaif parollar va ta'minot zanjiri (supply chain) orqali bilvosita yuqtirish. So'nggi yillarda ransomware-as-a-service (RaaS) biznes modelining paydo bo'lishi bilan ushbu tahdid o'ziga xos ma'noda demokratlashdi - texnik ko'nikmalarga ega bo'lmagan jinoyatchilar ham tayyor affiliate-platformalardan foydalanib, tezkor va oson tarzda murakkab hujum uyushtira oladigan bo'ldi. Bu hol hujumlar sonining global miqyosda keskin ko'payishiga sabab bo'lmoqda va mudofaachilar zimmasiga yanada og'irroq yuk tushirmoqda.

2017-yil may oyida tarqalgan WannaCry ransomware-worm Microsoft Windows operatsion tizimining SMBv1 protokolidagi EternalBlue nomli zaiflikdan foydalanib, hech qanday insoniy aralashuvsiz tarmoq bo'ylab o'z-o'zidan tarqalish imkoniyatiga ega edi. Microsoft mazkur zaiflik uchun MS17-010 patch'ni hujumdan ikki oy oldin chiqargan bo'lsa-da, ko'plab tashkilotlar uni o'z vaqtida o'rnatmagan edi. Natijada atigi 72 soat ichida 150 dan ortiq mamlakatdagi muhim infratuzilma obyektlari - kasalxonalar, temir yo'l tarmoqlari, telekommunikatsiya operatorlari va ishlab chiqarish korxonalari - falaj bo'ldi. Ushbu hodisa patch management siyosatining kiberxavfsizlikdagi hal qiluvchi ahamiyatini yaqqol namoyon qildi. Oldinroq, 2017-yil iyun oyidagi NotPetya ransomware niqobidagi destruktiv kiberqurol ko'rinishida paydo bo'ldi - uning asl maqsadi to'lov yig'ish emas, balki maksimal zarar yetkazish edi va Maersk, Merck, FedEx kabi global kompaniyalarga umumiy 10 milliard dollardan ortiq zarar keltirdi. 2021-yil may oyida DarkSide guruhi tomonidan Colonial Pipeline'ga qaratilgan hujum esa kompaniyani 4,4 million dollar to'lov to'lashga majbur qildi; hujumga olib kelgan asosiy sabab - ko'p bosqichli autentifikatsiyasiz ishlayotgan eskirgan VPN hisob qaydnomasi edi.

Ransomware hujumlaridan eng ishonchli himoya vositalaridan biri - muntazam va ishonchli zaxira nusxalash tizimini joriy qilish hisoblanadi. Sanoat standarti sifatida "3-2-1" qoidasi qabul qilingan: ma'lumotlarning kamida uchta

nusxasi saqlanishi, ular ikki xil turdagi saqlash vositasida joylashtirilishi va bittasi masofaviy yoki offline muhitda, ya'ni tarmoqdan ajratilgan holatda saqlanishi kerak. So'nggi yillarda ransomware operatorlari zaxira nusxalarning o'zini ham shifrlashga harakat qilayotganini hisobga olib, o'zgarmas (immutable) va air-gapped zaxiralardan foydalanish muhim amaliyotga aylandi. Immutable backup texnologiyasi WORM (Write Once, Read Many) prinsipi asosida ishlaydi va belgilangan muddat ichida zaxira nusxalarini o'chirish yoki o'zgartirishni texnik darajada taqiqlaydi. Bundan tashqari, zaxira nusxalarning real tiklash jarayonini muntazam test qilib turish ham zarurdir, aks holda kritik vaziyatda nusxalarning haqiqiy ishlatilmasligi yoki noto'g'ri sozlanganligi faqat hujum paytida aniqlanishi mumkin - bu esa juda kech bo'lgan holdir.

Dasturiy ta'minotni muntazam yangilash va ma'lum zaifliklarni o'z vaqtida yopish - ransomware hujumlarining salmoqli qismini oldini olishga imkon beradi. WannaCry hodisasi, yuqorida ta'kidlanganidek, buning yorqin tasdig'idir. Zamonaviy tashkilotlar to'laqonli vulnerability management dasturini joriy qilishi, kritik zaifliklarni CVSS bahosi va ekspluatatsiya ehtimoli bo'yicha tabaqalashtirishi hamda Zero-Day Response Team ko'rinishida maxsus ichki guruh ajratishi zarur. Avtomatlashtirilgan patch deployment tizimlari - masalan, Microsoft WSUS, SCCM yoki uchinchi tomon korporativ yechimlari - yirik tarmoqlarda yangilanishlar jarayonini tizimli va tezkor amalga oshirishga imkon beradi.

Endpoint Detection and Response (EDR) hamda Extended Detection and Response (XDR) yechimlari kompyuter tarmog'idagi har bir qurilmada shubhali faoliyatni uzluksiz kuzatadi va xulq-atvor tahlili (behavioral analytics) asosida ransomware'ga xos jarayonlar - ommaviy fayl shifrlash, Volume Shadow Copy'ni o'chirish, zararli PowerShell buyruqlari, Mimikatz kabi credential-dumping vositalarining ishga tushirilishi - kabi belgilarni avtomatik aniqlaydi va real vaqtda blokirovka qiladi. SIEM tizimlari (Splunk, IBM QRadar, Microsoft Sentinel kabilar) esa butun tarmoq bo'yicha logikaviy korrelyatsiya orqali murakkab ko'p bosqichli hujum zanjirlarini aniqlashga yordam beradi. Zamonaviy xavfsizlik operatsiyalari markazi (SOC) tarkibida EDR, SIEM va SOAR platformalarining integratsiyasi

tahdidga javob qaytarish vaqtini bir necha soatdan bir necha minutga qisqartirishga imkon yaratadi.

Texnik vositalar qanchalik mukammal bo'lmasin, xodimlar kiberxavfsizlik borasida savodsiz bo'lsa, himoya tizimi faqat zaif eshikli qo'rg'onni eslatadi - bitta xodim tomonidan zararli ilovaga bosilgan bir lahzalik beparvolik butun kuchli texnik devorlarni ma'nosiz qilib qo'yishi mumkin. Verizon DBIR hisobotiga ko'ra, ransomware hujumlarining sezilarli qismi bevosita fishing orqali boshlanadi [9]. Shu sababli, xodimlarni muntazam ravishda kiberxavfsizlik bo'yicha o'qitish, fishing simulyatsiyalarini o'tkazish va tashkilotda kiberxavfsizlik madaniyatini shakllantirish strategik ahamiyat kasb etadi. Amaliyot shuni ko'rsatmoqdaki, yillik ikki-uch marta o'tkaziladigan trening va doimiy fishing-test dasturlari xodimlarning zararli xabarlarni aniqlay olish qobiliyatini sezilarli darajada oshirib, shubhali xabarlarni xavfsizlik xizmatiga xabar qilish madaniyatini ham shakllantiradi.

Zero Trust arxitekturasi va tarmoq mikrosegmentatsiyasi ransomware'ning tarmoq bo'ylab "lateral movement" (yonma-yon harakat) qilishini keskin cheklaydi. An'anaviy yassi (flat) tarmoq sharoitida bir kompyuter zararlangan zahoti ransomware bir necha soat ichida butun tarmoqni egallashi mumkin edi; aksincha, mikrosegmentatsiya qilingan tarmoqda har bir segment o'z mustaqil xavfsizlik chegarasiga ega bo'ladi va hujumchi bir segmentdan boshqasiga o'tish uchun alohida autentifikatsiya va avtorizatsiyadan o'tishi lozim. Identity-based access control, just-in-time (JIT) privilege management va eng kam imtiyozlar (least privilege) prinsipi ushbu arxitekturaning asosiy amaliy ifodalari sanaladi. Amaliy tajriba shuni ko'rsatmoqdaki, Zero Trust tamoyillarini izchil joriy qilgan tashkilotlarda ransomware hujumining tarmoq bo'ylab kengayishi dastlabki zararlangan qurilma darajasida to'xtatilishi ko'p hollarda muvaffaqiyatli amalga oshiriladi.

Hech qanday himoya mutlaq samarali emas, shu sababli har bir tashkilot oldindan ishlab chiqilgan Incident Response Plan (IRP) va Disaster Recovery Plan (DRP) ga ega bo'lishi kerak. Reja aniq rollarni, bosqichlarni, aloqa kanallari va tashqi mutaxassislar (forensika, huquqiy maslahatchilar, milliy CERT bilan o'zaro aloqa) bilan hamkorlik tartibini o'z ichiga olishi lozim. Tajriba ko'rsatmoqdaki, mashqlar

(tabletop exercises) orqali muntazam tekshirib borilgan reja haqiqiy hujum sodir bo'lganda tashkilotning tiklanish vaqtini bir necha kundan bir necha soatga qisqartirishi mumkin, bu esa moliyaviy va reputatsion zararlarni sezilarli darajada kamaytiradi.

Yuqorida bayon etilgan ilmiy tahlil va real keyslar asosida shuni aniq xulosa qilish mumkinki, ransomware tahdidiga qarshi yakka texnologiya yoki bir yoqlama yondashuv yetarli emas. Eng samarali natija ko'p qatlamli "defense in depth" (chuqurlikdagi himoya) strategiyasi orqali erishiladi, unda zaxira nusxalash, patch management, EDR/XDR, SIEM, xodim treningi va Zero Trust mikrosegmentatsiyasi birgalikda, yagona xavfsizlik ekotizimi doirasida ishlaydi. Xalqaro statistik ma'lumotlar shuni ko'rsatmoqdaki, barcha ushbu qatlamlarni izchil joriy qilgan tashkilotlarda ransomware orqali zararlanish ehtimoli va zararining hajmi bir-ikki qatlamli himoyaga ega tashkilotlarga nisbatan bir necha barobar pastroq bo'ladi. Ushbu raqamlar tadqiqot gipotezasini - ko'p qatlamli himoyaning ustunligi haqidagi tezisni - amaliy dalillar bilan to'liq tasdiqlaydi.

XULOSA

Ushbu tadqiqot kompyuter tarmoqlaridagi eng xavfli zamonaviy tahdidlardan biri - ransomware hujumlari va ularga qarshi himoyaning samarali mexanizmlarini har tomonlama tahlil qildi. Olingan natijalar shuni ko'rsatdiki, ransomware tahdidi zamonaviy raqamli iqtisodiyot uchun strategik xavf manbai bo'lib qolmoqda va uning oqibatlari nafaqat moliyaviy, balki ijtimoiy, siyosiy va hatto kritik infratuzilma obyektlari orqali jismoniy shaklda ham namoyon bo'lishi mumkin. Tadqiqot boshida ilgari surilgan gipoteza - ko'p qatlamli himoya strategiyasining yakka texnik yechimlardan ustunligi - ham nazariy asos, ham WannaCry, NotPetya, Colonial Pipeline kabi real amaliy misollar orqali to'liq tasdiqlandi.

Amaliy jihatdan korxona va tashkilotlar zamonaviy ransomware hujumlariga bardosh berish uchun "3-2-1" prinsipiga asoslangan immutable zaxira nusxalash, avtomatlashtirilgan patch management, EDR/XDR va SIEM kuzatuv tizimlari, xodimlar uchun muntazam kiberxavfsizlik o'quv dasturlari, Zero Trust

mikrosegmentatsiyasi va sinovdan o'tgan Incident Response Plan'ni birgalikda, yagona ekotizim sifatida joriy qilishlari tavsiya etiladi. Ushbu kompleks yondashuv nafaqat ransomware, balki boshqa ko'plab zamonaviy kiberhujumlarga qarshi ham mustahkam himoya bazasini shakllantiradi.

O'zbekiston Respublikasi sharoitida ransomware muammosini hal qilish milliy kiberxavfsizlik ekotizimini yanada mustahkamlash, CERT-UZ faoliyatini kengaytirish, davlat organlari va xususiy sektor o'rtasida tahdidlar bo'yicha operativ ma'lumot almashish mexanizmlarini yaratish hamda yuqori malakali kiberxavfsizlik kadrlarini tayyorlashni talab etadi. Kelajakdagi tadqiqotlar yo'nalishi sifatida sun'iy intellekt asosida ransomware xulq-atvorini erta prognozlash, postkvant kriptografiya sharoitida zaxira nusxalarning uzoq muddatli himoyasini ta'minlash va avtomatlashtirilgan incident response tizimlarini ishlab chiqish ko'rib chiqilishi maqsadga muvofiq bo'ladi. Taqdim etilgan xulosalar axborot xavfsizligi mutaxassislari, tarmoq administratorlari va ilmiy tadqiqotchilar uchun amaliy asos bo'lib xizmat qilishi mumkin.

ADABIYOTLAR RO'YXATI

1. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. – New York: Pearson, 2017. – 464 p.

2. Schneier B. Secrets and Lies: Digital Security in a Networked World. – Indianapolis: Wiley, 2015. – 448 p.

3. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture // NIST Special Publication 800-207. – Gaithersburg: National Institute of Standards and Technology, 2020. – 50 p.

4. Richardson R., North M. Ransomware: Evolution, Mitigation and Prevention // International Management Review. – 2017. – Vol. 13, No. 1. – P. 10–21.

5. G'ulomov Sh.R., Karimov I.X. Axborot xavfsizligi asoslari: Darslik. – Toshkent: TATU, 2020. – 312 b.

6. Usmonov Sh.Yu. O'zbekiston milliy segmentida kiberhujumlar tahlili va ularga qarshi kurash masalalari // Muhammad al-Xorazmiy avlodlari ilmiy-amaliy jurnali. – 2022. – №3(21). – B. 45–52.

7. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni. – 2022-yil 15-aprel, O'RQ-764-son. – Toshkent: Qonun hujjatlari ma'lumotlari milliy bazasi, 2022.

8. ENISA Threat Landscape 2024. – Athens: European Union Agency for Cybersecurity, 2024. – 178 p.

9. Verizon. 2024 Data Breach Investigations Report (DBIR). – New York: Verizon Business, 2024. – 100 p.

10. Kaur R., Kaur N. Ransomware Detection: A Systematic Literature Review // Computers & Security. – 2023. – Vol. 131. – P. 103–128.

11. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. – Indianapolis: Wiley, 2020. – 1232 p.