ZARARLI DASTURIY VOSITALAR. RANSOMWARE HUJUMLARI, ULARNING TARQALISH STATISTIKASI VA PROFILAKTIKASI.

D.Ya.Irgasheva
(TATU),
D.U.Qurbonmurodov
(TATU)

Annotatsiya: *Ushbu maqolada zararli dasturiy vositalar va ularning turlari haqida nazariy ma'lumotlar keltirib o'tildi. Ransomware hujumlari, uning keng tarqalish sabablari va so'nggi statistikalarga to'xtalib o'tildi. Hozirgi kundagi ransomware guruhlari, ransomware guruhlarining asosiy e'tibor markazidagi sohalari va shu sohalarning hujumlar natijasida ko'rgan zararlari haqidagi ma'lumotlar taqdim etildi.*

Kalit so'zlar: *Zararli dasturiy vositalar, viruslar, troyan otlari,Adware,Spyware,Rootkits, Backdoors, mantiqiy bombalar, Botnet, Ransomware,Ryuk, Maze,LockBit, DearCry,Lapsus$.*

Kirish

Bugungi kunda axborot texnologiyalar rivoji insonlarning hayotini yengillashtirish bilan birga bir qator muammolarni ham keltirib chiqarmoqda. Axborot texnolgiyalari yutuqlaridan foydalangan ba'zi shaxslar har xil yo'llar bilan zararli harakatlarni amalga oshirmoqda. Zararli dasturiy vositalar yordamida boshqalarning maxfiy ma'lumotlariga ega chiqishmoqda. Ma'lumotlar o'girlanishi yoki ma'lumotlarning yo'q qilinishi bilan tahdid qilinib, firibgarlik orqali pul undirilmoqda. Bunda zararli dasturiy vositalar firibgarlarga keng imkoniyatlar eshikini ochib beryapti.

Zararli dasturiy vositalar foydalanuvchini ruxsatisiz hujumchi kabi g'arazli amallarni bajarishni maqsad qilgan vosita hisoblanib, ular yuklanuvchi kod (.exe), aktiv kontent, skript yoki boshqa ko'rinishda bo'lishi mumkin. Hujumchi zararli dasturiy vositalardan foydalangan holda tizim xafsizligini obro'sizlantirishi, kompyuter amallarini buzishi, maxfiy axborotni to'plashi, veb saytdagi kontentlarni modifikasiyalashi, o'chirishi yoki qo'shishi, foydalanuvchi kompyuteri boshqaruvini qo'lga kiritishi mumkin. Bundan tashqari, zararli dasturlar, hukumat tashkilotlaridan va korporativ tashkilotlardan katta hajmdagi maxfiy axborotni olish uchun ham foydalanilishi mumkin. Zararli dasturlarning hozirda quyidagi ko'rinishlari keng tarqalgan:

- viruslar: o’zini o’zi ko’paytiradigan programma bo’lib, o’zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi;

- troyan otlari: bir qarashda yaxshi va foydali kabi ko’rinuvchi dasturiy vosita sifatida o’zini ko’rsatsada, yashiringan zararli koddan iborat bo’ladi;

- Adware: marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko’rish rejimini kuzatib boruvchi dasturiy ta’minot;

- Spyware: foydalanuvchi ma’lumotlarini qo’lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod;

- Rootkits: ushbu zararli dasturiy vosita operasion tizim tomonidan aniqlanmasligi uchun o’z harakatlarini yashiradi;

- Backdoors: zararli dasturiy kodlar bo’lib, hujumchiga autentifikasiyani amalga oshirmasdan aylanib o’tib tizimga kirish imkonini beradi, masalan, administrator parolisiz imtiyozga ega bo’lish;

- mantiqiy bombalar: zararli dasturiy vosita bo’lib, biror mantiqiy shart qanoatlantirilgan vaqtda o’z harakatini amalga oshiradi.

- Botnet: Internet tarmog’idagi obro’sizlantirilgan kompyuterlar bo’lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi;

- Ransomware: mazkur zararli dasturiy ta’minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo’yib, to’lov amalga oshirilishini talab qiladi.[1]

Asosiy qism

Ransomware hujumlari, ularning tarqalish statistikasi va profilaktikasi

Ransomware - bu foydalanuvchi yoki tashkilotning kompyuteridagi fayllarga kirishini taqiqlash uchun mo'ljallangan zararli dastur. Ushbu fayllarni shifrlash va shifrni ochish kaliti uchun to'lovni talab qilish orqali kiberhujumchilar tashkilotlarni to'lovni to'lash ularning fayllariga kirishni qayta tiklashning eng oson va arzon usuli bo'ladigan holatga keltiradilar. Ba'zi variantlarda to'lovni to'lash uchun ransomware qurbonlarini qo'shimcha rag'batlantirish uchun ma'lumotlarni o'g'irlash kabi qo'shimcha funksiyalar qo'shildi[2].

Ransomware tezda zararli dasturlarning eng mashhur va ommabop turiga aylandi . So'nggi to'lov dasturi hujumlari shifoxonalarning muhim xizmatlarni taqdim etish qobiliyatiga ta'sir qildi, shaharlarda davlat xizmatlarini ishdan chiqardi va turli tashkilotlarga katta zarar yetkazdi.

Zamonaviy to'lov dasturi 2017 yildagi WannaCry epidemiyasi bilan boshlandi. Ushbu keng ko'lamli va ommabop hujum to'lov dasturi hujumlari mumkin va

potentsial foydali ekanligini ko'rsatdi. O'shandan beri to'lov dasturining o'nlab variantlari ishlab chiqildi va turli hujumlarda foydalanildi.

COVID-19 pandemiyasi ham ransomware hujumlari avj olishiga yordam berdi. Tashkilotlar tezda masofaviy ishlashga o'tishlari sababli ularning kibermudofaalarida bo'shliqlar paydo bo'ldi. Kiberjinoyatchilar ushbu zaifliklardan to'lov dasturini etkazib berish uchun foydalangan, natijada to'lovga qarshi hujumlar ko'paygan. 2020-yilning 3-choragida to‘lov dasturi hujumlari o‘sha yilning birinchi yarmiga nisbatan 50 foizga oshdi.

To'lov dasturining o'nlab variantlari mavjud bo'lib, ularning har biri o'ziga xos xususiyatlarga ega. Biroq, ba'zi ransomware guruhlari boshqalarga qaraganda samaraliroq va muvaffaqiyatli bo'lib, ularni olomondan ajralib turadi.[2]

- Ryuk - bu juda maqsadli to'lov dasturi variantiga misol. U odatda nayza phishing elektron pochta xabarlari orqali yoki masofaviy ish stoli protokoli (RDP) yordamida korporativ tizimlarga kirish uchun buzilgan foydalanuvchi hisob ma'lumotlaridan foydalanish orqali yetkaziladi. Tizim zararlangandan so'ng, Ryuk ma'lum turdagi fayllarni shifrlaydi (kompyuter ishlashi uchun muhim bo'lganlardan qochib), keyin to'lov talabini taqdim etadi. Ryuk to'lov dasturining eng qimmat turlaridan biri sifatida tanilgan. Ryuk o'rtacha 1 million dollardan ortiq to'lov talab qilmoqda . Natijada, Ryuk ortidagi kiberjinoyatchilar, birinchi navbatda, o'z talablarini qondirish uchun zarur resurslarga ega bo'lgan korxonalarga e'tibor berishadi.
- Maze(Labirint) ransomware fayl shifrlash va ma'lumotlarni o'g'irlashni birlashtirgan birinchi to'lov dasturi varianti bo'lgani bilan mashhur . Maqsadlar to'lovni to'lashdan bosh tortishni boshlaganda, Maze shifrlashdan oldin qurbonlarning kompyuterlaridan maxfiy ma'lumotlarni yig'ishni boshladi. Agar to'lov talablari bajarilmasa, bu ma'lumotlar ommaga oshkor qilinadi yoki eng yuqori narx taklif qiluvchiga sotiladi. Qimmatbaho ma'lumotlarning buzilishi ehtimoli to'lov uchun qo'shimcha rag'bat sifatida ishlatilgan. Maze ransomware ortidagi guruh o'z faoliyatini rasman yakunladi . Biroq, bu ransomware tahdidi kamaydi degani emas. Ba'zi Maze filiallari Egregor ransomware dasturidan foydalanishga o'tishdi va Egregor, Maze va Sekhmet variantlari umumiy manbaga ega deb hisoblanadi.
- REvil guruhi (shuningdek, Sodinokibi nomi bilan ham tanilgan) yirik tashkilotlarga mo'ljallangan to'lov dasturining yana bir variantidir. REvil - tarmoqdagi eng mashhur to'lov dasturlari oilalaridan biri. 2019 yildan beri rus tilida so'zlashuvchi REvil guruhi tomonidan boshqariladigan ransomware guruhi " Kaseya " va "JBS" kabi ko'plab yirik buzilishlar uchun javobgar bo'lgan.REvil an'anaviy ransomware

varianti sifatida boshlangan bo'lsa-da, u vaqt o'tishi bilan rivojlandi. Ular fayllarni shifrlash bilan birga korxonalardan ma'lumotlarni o'g'irlash uchun Double Extortion texnikasidan foydalanadilar . Bu shuni anglatadiki, tajovuzkorlar ma'lumotlar shifrini ochish uchun to'lovni talab qilishdan tashqari, agar ikkinchi to'lov amalga oshirilmasa, o'g'irlangan ma'lumotlarni tarqatish bilan tahdid qilishlari mumkin.

- LockBit - bu 2019-yil sentabr oyidan beri ishlayotgan ma'lumotlarni shifrlash uchun zararli dastur va yaqinda Ransomware-as-a-Service (RaaS) . Ushbu to'lov dasturi xavfsizlik qurilmalari va IT/SOC guruhlari tomonidan tezda aniqlanishining oldini olish usuli sifatida yirik tashkilotlarni shifrlash uchun ishlab chiqilgan.
- DearCry. 2021-yil mart oyida Microsoft Microsoft Exchange serverlaridagi to‘rtta zaiflik uchun himoyalarni chiqardi. DearCry - bu Microsoft Exchange-da yaqinda ochilgan to'rtta zaiflikdan foydalanish uchun mo'ljallangan to'lov dasturining yangi variantidir. DearCry ransomware ma'lum turdagi fayllarni shifrlaydi. Shifrlash tugagandan so'ng, DearCry to'lov xabarini ko'rsatadi va foydalanuvchilarga to'lov dasturi operatorlariga o'z fayllarini shifrlashni o'rganish uchun elektron pochta xabarini yuborishni buyuradi.
- Lapsus$ - Janubiy Amerikadagi to'lov dasturlari guruhi bo'lib, u ba'zi yuqori darajadagi maqsadlarga kiberhujumlar bilan bog'liq. Kiberguruh tovlamachilik bilan mashhur bo'lib, agar o'z qurbonlari talablari bajarilmasa, maxfiy ma'lumotlarni oshkor qilish bilan tahdid qiladi. Guruh Nvidia, Samsung, Ubisoft va boshqalarni buzish bilan maqtandi. Guruh zararli dastur fayllarini ishonchli qilib yashirish uchun o'g'irlangan manba kodidan foydalanadi.

Quyida biz ransomware hujumlarining tarqalish statistikasini keltirib o’tamiz.:

- 2020-yildan 2022-yilning 2-choragigacha bo‘lgan davrda ransomware hujumlari hajmi 2021-yilning ikkinchi choragida 188,9 million hujum bilan eng yuqori cho‘qqiga chiqdi;
- Ransomware 2022-yilda zararli dasturlarning eng keng tarqalgan shakli bo‘lib qolmoqda. U kiberjinoyatchilarga nisbatan past xavf tug‘dirgan holda katta miqdorda pul undirish qobiliyati tufayli mashhurligi oshdi [3];
- Ransomware 2022 yilning 1-choragida fishingdan keyin ma’lumotlar buzilishining ikkinchi asosiy sababidir ;
- 2021 yilda dunyo bo'ylab 623,3 million to'lov dasturi hujumi sodir bo'lgan va 2020 yilda 304,6 million hujum aniqlangan;
- 2022-yilning birinchi yarmida 236,1 million to‘lovga urinishlar bo‘lgan ;
- Maqsadli mashinalarning aksariyati Windows va Mac-ga asoslangan bo'lsa-da, Linux to'lov dasturi 146% ga o'sdi[4];

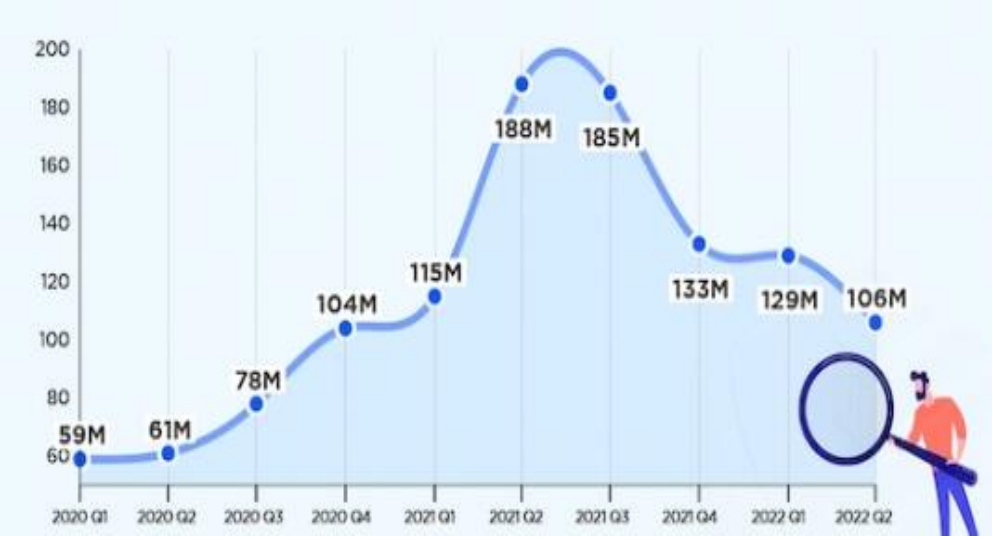
•2021 yilda tashkilotlarning 76 foizi bir yoki bir nechta to'lov dasturi hujumiga uchragan . Ulardan[5]:

- 42% spam elektron pochta xabarlaridan zararli havolalarni bosish kabi foydalanuvchi harakatlaridan kelib chiqqan;
- 43% menejerlar yoki ma'murlarning beparvoligi (dasturiy ta'minot yamoqlari, hisobga olish ma'lumotlari va boshqalar bilan bog'liq xavflar);

•2021 yilda xakerlar hujumlarning 65 foizida ma’lumotlarni muvaffaqiyatli shifrlashdi , bu 2020 yilda qayd etilganidan 54 foizga ko‘p;

•2021-yilda ransomware hodisalari 82 foizga oshgan , 2020-yildagi 1474 hujumdan farqli ravishda 2686 ta hujum;

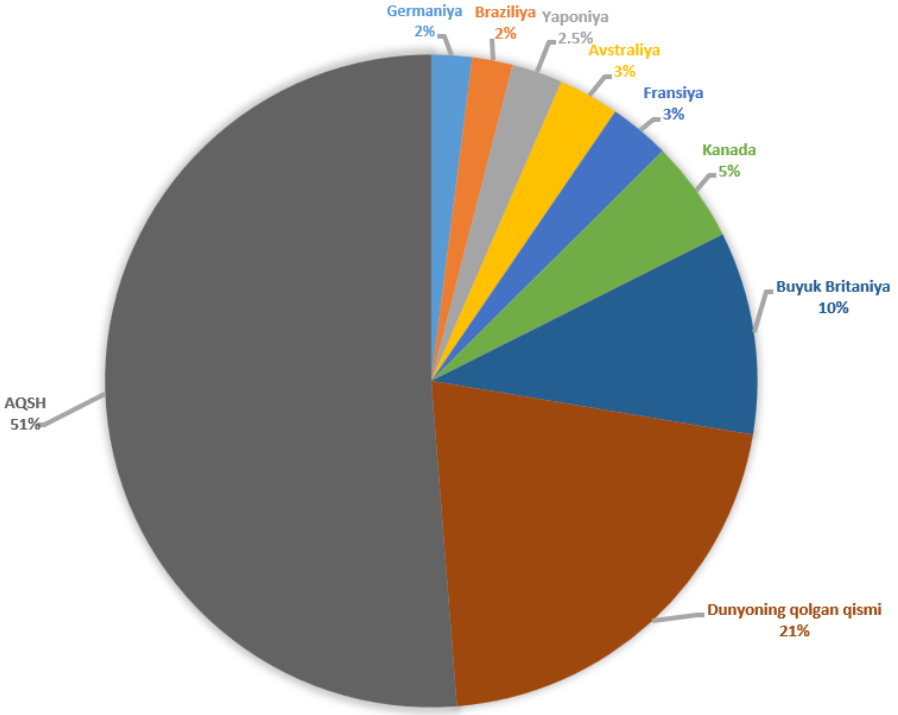
•2022-yilning birinchi yarmida har bir tashkilotda 707 ta ransomware hujumlariga urinish bo‘lgan .



1-rasm. 2020 - 2022 yillarda ransomware hujumlarining o'sishi.

Ransomware tomonidan nishonga olingan mamlakatlar.

Ransomware jinoiy guruhlari daromadni ko'paytirish uchun asosan boy mamlakatlarni nishonga oladi.



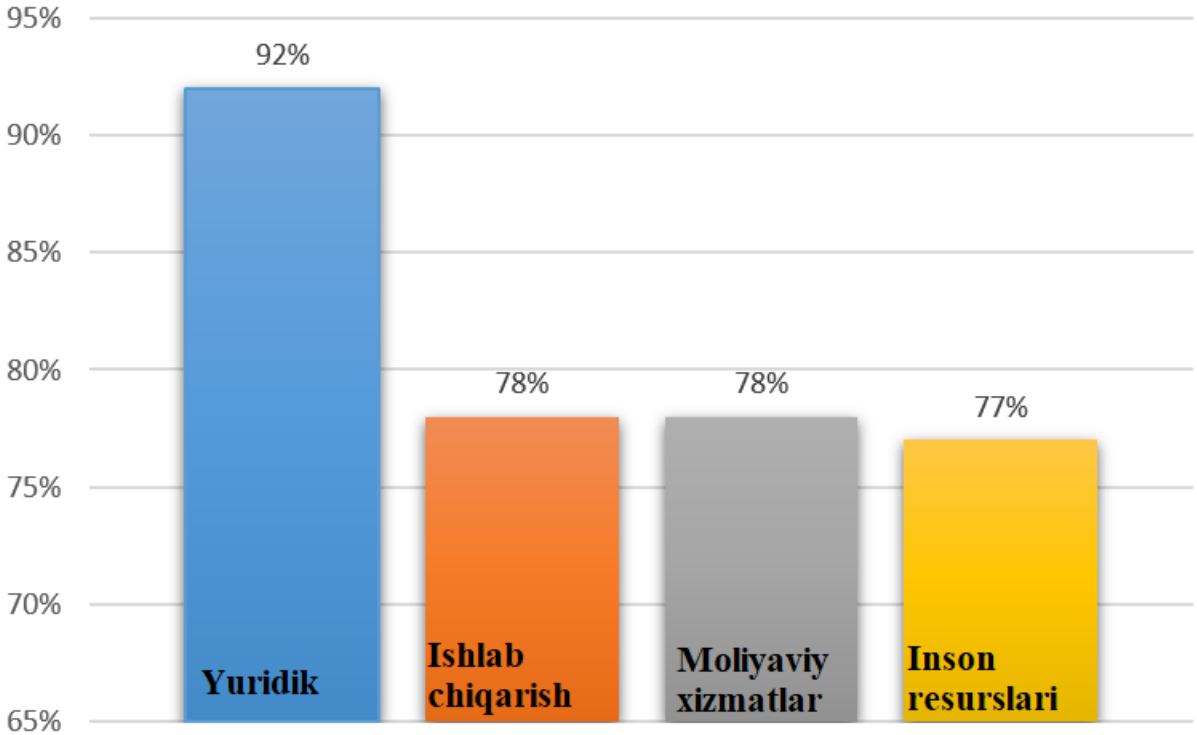
2-rasm. Ransomware hujumlarining davlatlar bo’yicha taqsimoti.

• 2021 yil holatiga ko'ra, AQSH ransomware hujumlari bo'yicha dunyodagi yetakchi nishon bo'lib qolmoqda , bu hodisalarning 51% dan ortig'ini tashkil qiladi. Boshqa davlatlar qatoriga quyidagilar kiradi:

- Buyuk Britaniya - 10%
- Kanada - 5%
- Fransiya - 3%
- Avstraliya - 3%
- Yaponiya - 2,5%
- Braziliya - 2%
- Germaniya - 2%
- Dunyoning qolgan qismi - 21% [5]

Ransomware tomonidan nishonga olingan sohalar

Sanoatning barcha tarmoqlari ransomware tomonidan nishonga olinishi mumkin bo'lsa-da, ba'zi tarmoqlar boshqalarga qaraganda ko'proq himoyasiz.



3-rasm. Ransomware tomonidan nishonga olingan sohalar taqsimoti

• 2021-yilda to‘lov dasturlari eng ko‘p zarar ko‘rgan tarmoqlar qatoriga yuridik (92%), ishlab chiqarish (78%), moliyaviy xizmatlar (78%) va inson resurslari (77%) kiradi[6].

• 2021-yilda chakana savdo tarmog‘ida ransomware hujumlarining eng sezilarli o‘sishi kuzatildi — 100%. 2020 yilga nisbatan texnologiya sektori 89 foizga, sog‘liqni saqlash sohasi esa 30 foizga o‘sdi.

Ransomware hozirda kiberjinoyatchilar uchun foydali texnikaga aylandi va hech bir korxona yoki tashkilot bu zararli dastur tahdididan himoyalanmagan. Ransomware nihoyatda makkor va zararli dastur bo’lib, odatda fishing elektron pochta xabarlari orqali tarqalsa ham, u biznesdagi zaifliklar va orqa eshiklardan ham foydalanadi. Qurbon bo'lib qolmaslik va ma'lumotlar, fayllaringiz bloklanib qolmasligi uchun amalga oshirishingiz mumkin bo'lgan ba'zi ransomware hujumlaridan himoyalash usullarini keltirib o’tamiz[7]:

•Xodimlarni tarbiyalash. Xodimlaringizni o'qitish zararli dastur hujumlaridan himoya qilishning birinchi chizig'idir. To'lov dasturi asosan elektron pochta havolalari va qo'shimchalar orqali kiritilganligi sababli, xodimlaringizni xavfsiz ko'rishni mashq qilishlari uchun zarur bo'lgan bilimlar bilan qurollantirish va elektron pochta odatlari ko'plab zararli dastur hujumlarining oldini oladi. Ishchilaringizga fishing hujumlarini qanday aniqlashni va qalqib chiquvchi oynalarni bosmaslik,

havolaning URL manzillarini tekshirmaslik va elektron xatlardagi havolalar yoki biriktirmalarni, ayniqsa noma'lum xabarlarlarni ochmaslik kabi eng yaxshi amaliyotlarni o'rgating. Trening bir seans emas, balki xodimlaringiz xavfsiz odatlarni saqlab qolishlari va yangi tahdidlarga mos kelishini ta'minlash uchun doimiy amaliyot bo'lishi kerak.

- Muhim ma'lumotlarga kirishni nazorat qilish. Identifikatsiya va kirishni boshqarish korxonalarga muhim ma'lumotlarga kirishni nazorat qilish imkonini beradi. Kompaniyalar foydalanuvchi faoliyatini nazorat qilish, foydalanuvchi rolini o'zgartirish, faoliyat to'g'risida hisobotlarni yaratish va biznes siyosatini yaratish va amalga oshirish uchun texnologiyalar va vositalardan foydalanadi. Buzilgan hisob ma'lumotlari biznes tarmog'ingizga va uning ma'lumotlariga kirish nuqtasini ishlab chiqishi mumkin. Shuning uchun, har bir foydalanuvchi ega bo'lishi kerak bo'lgan huquqlarni aniqlash uchun muntazam ravishda xavfsizlikni baholashni amalga oshirishingiz va tashkilotingiz bo'ylab izchil foydalanuvchi siyosati va rollarini amalga oshirish uchun IAM tizimlaridan foydalangan holda qo'shimcha himoya qatlamini kiritish orqali xavfni yo'q qilishingiz kerak. Ransomware hujumlarida identifikator va kirish boshqaruvini tatbiq etish kompaniyangiz aktivlarini xakerlik, fishing va zararli dastur hujumlarining ortib borayotgan tahdidlaridan osongina himoya qilishi mumkin.
- Tizimlaringizni zaxiralash.Biznesingizning muhim ma'lumotlari xavfsizligini ta'minlash uchun tizimlaringizning zaxira nusxasini saytdan tashqarida ham, mahalliy sifatida ham qilishingiz kerak. Tizimlaringizning zaxira nusxasini yaratish ma’lumotlaringizni kiberjinoyatchilarga kirish ehtimoli kamroq bo‘lgan joyda xavfsiz saqlaydi, biroq hujum sodir bo‘lgan taqdirda eski fayllaringizni o‘chirib tashlash va zaxira ma’lumotlari yordamida ta’mirlashni ancha osonlashtiradi. Masalan, siz biznes tizimlaringizni himoya qilish uchun bulutga asoslangan yechimdan foydalanishingiz mumkin. Bulutdagi ma'lumotlaringizning zahira nusxasini yaratish uni to'lov dasturi infektsiyasidan himoya qiladi va himoya qatlamini qo'shadi.
- Kuchli parol xavfsizligini joriy qilish. Ma’lumotlaringizni xavfsizligini ta’minlash uchun siz eng yaxshi parol xavfsizligi amaliyotlarini va korporativ parol menejerini o‘z ichiga olgan parolni boshqarish usulidan foydalanishingiz kerak. Instant Checkmate tadqiqotiga ko'ra, har to'rt kishidan uchtasi bir nechta saytlar uchun bir xil paroldan foydalanadi, uchdan biri esa juda zaif parollardan foydalanadi. Axborot xavfsizligini ta'minlash uchun bir nechta kuchli parollardan foydalaning, ayniqsa nozik ma'lumotlar uchun.

•Muntazam rejalashtirilgan xavfsizlik tekshiruvlarini o'tkazish. Agar siz mobil qurilmalaringiz va kompyuterlaringizda har hafta skanerlashdan o'tmasangiz, tizimingizda o'rnatilgan barcha xavfsizlik dasturlari samarali bo'lmasligi mumkin. Ushbu skanerlar sizning xavfsizlik dasturingizda ikkinchi himoya qatlami sifatida ishlaydi. Ular odatda real vaqtda tekshiruvchi qo'lga kirita olmaydigan tahdidlarni aniqlaydi.

•OS va dasturiy ta'minot yangilanishlarini qo'llash. Zaifliklarni samarali boshqarish va dasturiy ta'minot va apparat tizimlarini muntazam ravishda tuzatish kiberhujumlarning oldini olish uchun foydalanishingiz mumkin bo'lgan to'lov dasturiga javob berishning eng oson usullaridan biridir. Zararli dastur odatda dasturiy ilovalar yoki operatsion tizimlardagi xatolar va xavfsizlik bo'shliqlaridan foydalanadi. Shuning uchun, to'lov dasturining oldini olishda muvaffaqiyat qozonish uchun barcha mobil qurilmalar va kompyuterlarga eng so'nggi yamoq va yangilanishlarni o'rnatish juda muhimdir.

Xulosa

Mahalliy hukumatlar, moliya institutlari va sog'liqni saqlash provayderlaridan tortib o'rta va kichik biznesgacha bo'lgan har qanday tashkilot ransomware hujumlari xavfi ortib borayotgani bilan kurashmoqda. Shu sababli, korxonalar zararli dastur hujumlari va ma'lumotlar buzilishi davrida hushyor bo'lishlari kerak. Ransomware hujumining turli usullarini va ularni oldini olish, aniqlash va tiklashga yordam beradigan to'g'ri qadamlarni bilish tashkilotingizga umumiy ta'sirni kamaytirishi mumkin. Umid qilamizki, ushbu maqolada muhokama qilingan maslahatlar tashkilotingizning axborot aktivlarini xavfsiz saqlashga va to'lov dasturi hujumini muvaffaqiyatli bo'lishidan oldin to'xtatishga yordam beradi.

FOYDALANILGAN ADABIYOTLAR:

[1]. S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: o‘quv qo‘llanma. – T.: «Aloqachi», 2020

[2]. Ransomware Attack – What is it and How Does it Work? Link: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/

[3]. 2022 Ransomware The True Cost to Business Link: https://www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf

[4]. X-Force Threat Intelligence Index 2022 https://www.ibm.com/downloads/cas/ADLMYLAZ

[5]. 2021 Ransomware Attack Report Link: https://www.blackfog.com/2021-ransomware-attack-report/
[6]. 93 Must-Know Ransomware Statistics [2023]
Link: https://www.antivirusguide.com/cybersecurity/ransomware-statistics
[7]. RANSOMWARE ATTACK PREVENTION AND RESPONSE SOLUTIONS Link: https://identitymanagementinstitute.org/ransomware-attack-prevention-and-response-solutions/

Irgasheva Durdona Yakubdjanovna
DSc, professor,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti huzuridagi pedagog kadrlarni qayta tayyorlash va ularning malakasini oshirish tarmoq markazi direktori
(+998 90) 317-61-38, durdona.ya@gmail.com

Qurbonmurodov Diyorbek Ulug'bek o'g'li
(+99894) 308-48-00, qurbonmurodovdiyorbek@gmail.com
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti talabasi

D.Ya.Irgasheva, D.U.Qurbonmurodov