ZAMONAVIY KIBERHUJUMLAR VA ULARGA QARSHI HIMOYA CHORALARI

G'ulomov Sherzod Rajaboyevich[1], Normirzayev Farrux Abdurahimovich[2]

[1]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti. E-mail: sherzod.gulomov@tuit.uz
[2]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti E-mail: abdurahimovichfarrux@gmail.com

КАЛИТ СЎЗЛАР

kiberxavfsizlik, kiberhujum, kiberjinoyat, phishing, DDoS kiberhujumi, ransomware, zaif nuqtalarga kiberhujum, zararli dasturlar, internet, tarmoq, veb-sayt, mustahkam kalit so'z, ko'p faktorli autentifikatsiya.

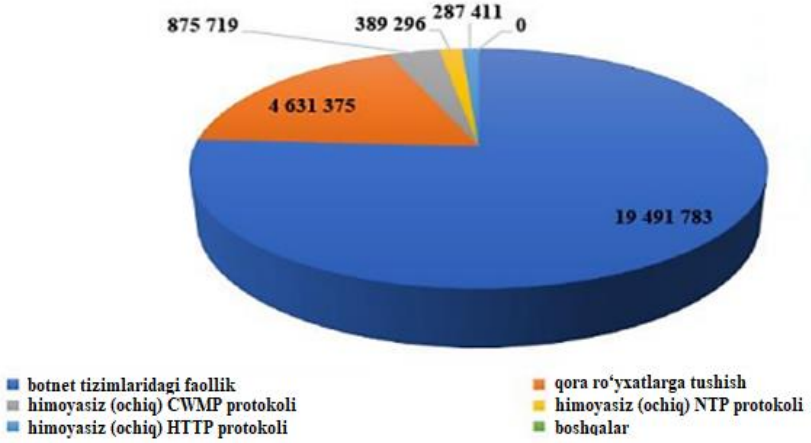
АННОТАЦИЯ

Ushbu maqolada zamonaviy kiberhujumlar, ularning turlari haqida ma'lumotlar berilgan. Phishing, DDoS hujumlari, ransomware, zaif nuqtalarga hujumlar va zararli dasturlar kabi hujumlarning asosiy xususiyatlari va ta'siri tavsiflanadi. Shuningdek, maqolada kiberhujumlarning axborot tizimlariga ta'siri, ulardan himoyalanish bo'yicha tavsiyalar va choralar ko'riladi. Oddiy foydalanuvchi yoki tashkilot tizimlardagi zaifliklarni kamaytirishi va jiddiy zararni oldini olishi uchun qanday himoya usullaridan foydalanish mumkinligini bilib olishi mumkin. Ushbu maqola axborot xavfsizligi mutaxassislari, xavfsizlik menejerlari va o'zini kiber tahdidlardan qanday himoya qilish haqida ko'proq ma'lumot olishni xohlaydiganlar uchun foydali bo'lishi mumkin.

I. KIRISH

Mamlakatimizda zamonaviy axborot-kommunikatsiya texnologiyalarini hayotning barcha jabhalariga joriy etilishi davlat organlari va tashkilotlarining hisobdorligi va ochiqligini kuchaytirishi, davlat xizmatlari qamrovi hamda tezkorligini oshirishi bilan birga kiberxavfsizlikka doir yangi tahdidlarni ham keltirib chiqarmoqda.

Xususan, kiberxavfsizlikni ta'minlash bo'yicha ko'rilayotgan chora-tadbirlarga qaramay parollarni buzib kirish, virusli dasturlarni tarqatish, kredit karta va boshqa bank rekvizitlaridagi mablag'larni o'zlashtirish, serverlardan foydalanuvchilarni shaxsiy ma'lumotlarini o'g'irlash xolatlari kuzatilmoqda. O'zbekiston Respublikasi Kiberxavfsizlik markazining 2020 yilgi hisobotidan ko'rish mumkinki milliy internet segmentida axborot va kiberxavfsizlikka tahdid soluvchi 27 000 000 dan ortiq zararli va shubhali tarmoq hodisalari kuzatilgan (1 - rasm) [1].



1 – rasm. Kuzatilgan tahdidlarning asosiy salmog'i.

© *G'ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich*

Bu kabi xolatlar global miqiyosda katta zararlarga olib kelmoqda.

Jumladan, 2022 yilda kiberjinoyatlarning global zarari taxminan 8,4 trillion dollarga baholangan. 2023 yilda Internetdagi noqonuniy faoliyat natijasida yuzaga kelgan hodisalarning zarari 11 trillion dollardan ortiq bo‘lishi kutilmoqda [2]. 2030 yilga kelib, butun dunyo bo‘ylab kiberjinoyatlarning yillik global zarari 90 trillion dollardan oshishi mumkin, bu jahon yalpi ichki mahsulotining hozirgi hajmi bilan teng [3].

II. KIBERHUJUMLAR, ULARNING OQIBATLARI, TURLARI VA ULARGA QARSHI HIMOYA CHORALARI

Kiberhujumlar - bu kompyuter tizimlari, ilovalari va ma'lumotlariga ruxsatsiz kirishga urinishlar hisoblanadi. Shuni ham ta'kidlash kerakki, kiberhujumlarni olib borishda texnologik innovatsiyalardan ham tobora keng foydalanilmoqda. Bu esa o‘z navbatida kiberhujumlarga qarshi kurashishni yanada qiyinlashtirmoqda. Ushbu maqolada biz zamonaviy kiberhujumlarning asosiy turlarini va ularga qarshi himoya choralarini ko‘rib chiqamiz.

Bugungi kunda kiberhujumlarni asosiy turlari quyidagilardan iborat:

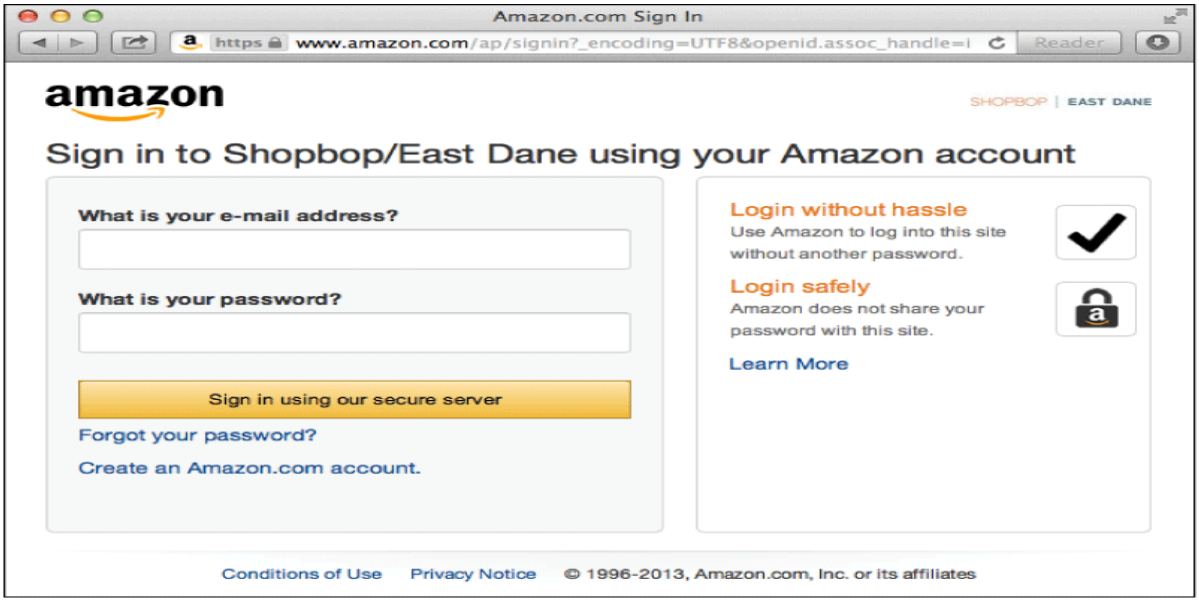
- Phishing;
- DDoS kiberhujumi;
- Ransomware;
- Zaif nuqtalarga kiberhujum;
- Zararli dasturlar;

Quyida ushbu kiberhujumlar nima ekanligini, ularning turlari, qanday ishlashi va ushbu turdagi kiberhujumlardan himoyalanish usullarini tadqiqi olib boriladi.

Phishing kiberhujumlari

Phishing - kiberhujumlarning eng keng tarqalgan turlaridan biri bo‘lib, biznes va oddiy foydalanuvchilar uchun tobora nozik va xavfli bo‘lib bormoqda.

Phishing - foydalanuvchilarning maxfiy ma'lumotlarini olish uchun ularni aldashga asoslangan kiberhujumlarning bir turi hisoblanadi. Ko‘pincha, bu kiberhujum banklar, ijtimoiy tarmoqlar yoki foydalanuvchi ishonadigan boshqa tashkilotlar nomidan rasmiy ko‘rinishdagi elektron pochta xabarlarini yuborish orqali amalga oshiriladi. Ushbu elektron pochta xabarlari asl nusxaga o‘xshash, lekin parollar, bank karta raqamlari, manzillar va boshqa ma'lumotlar kabi shaxsiy foydalanuvchi ma'lumotlarini to‘playdigan saytlarga soxta havolalarni o‘z ichiga oladi. Quyidagi rasmlarda (2 va 3-rasmlar) phishing saytni qo‘rishimiz mumkin.



2-rasm. Haqiqiy amazon sayti.

© *G‘ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich*



3-rasm. Soxta amazon sayti.

Bunda kiberjinoyatchilar haqiqiy sayt nusxasini yaratib foydalanuvchini ushbu veb-havolaga kirishga undaydi, so‘ngra uning shaxsiy ma’lumotlarini, ya’ni login va parolini, bank karta hisob raqamlarini qo‘lga qiritadi.

Phishing hujamlarini bir nechta turlari mavjud bo‘lib, ular quyidagilardan iborat:

1. **Bosqichma-bosqich phishing** - bunda, kiberjinoyatchilar foydalanuvchini o‘z ma’lumotlarini taqdim etishga ishontirish uchun bir necha bosqichlardan o‘tadi. Misol uchun, ular foydalanuvchidan soxta kirish sahifasiga o‘z ma’lumotlarini kiritishni so‘rashlari mumkin, so‘ngra barcha jarayon rasmiy ravishda sodir bo‘lgan degan tasavvurni hosil qilish uchun foydalanuvchini haqiqiy sahifaga yo‘naltiradi.

2. **Ijtimoiy phishing** – kiberjinoyatchilar foydalanuvchilarni aldash uchun ijtimoiy tarmoqlar, chatlar, forumlar va boshqa platformalardan foydalanishi mumkin. Masalan, ular o‘zlarini do‘stlar, hamkasblar yoki hatto oila a’zolari sifatida ko‘rsatishlari va maxfiy ma’lumotlarni so‘rashlari mumkin.

3. **Yo‘naltirilgan phishing** (inglizcha - spear phishing) - bu turda kiberjinoyatchilarga oldindan ma’lum foydalanuvchilar yoki tashkilotlarni tanlab, ularga soxta elektron pochta xabarlarini yuborishga asoslangan phishing turi hisoblanadi. Ushbu xatlar faqat tanlangan foydalanuvchilar yoki tashkilotlarga ma’lum bo‘lgan ma’lumotlarni o‘z ichiga olishi mumkin, bu ularni yanada ishonchli qiladi.

4. **Baliq ovlash** (inglizcha - whaling) - yuqori mansabdor shaxslar va tashkilotlar rahbarlariga qaratilgan phishing turi hisoblanadi. Jinoyatchilar o‘zlarini kompaniya rahbarlari sifatida ko‘rsatishlari va moliyaviy tafsilotlar yoki parollar kabi konfidensial ma’lumotlarni so‘rashlari mumkin.

5. **Texnik phishing** - kiberjinoyatchilar maxfiy ma’lumotlarga kirish uchun zararli dasturlardan yoki axborotni himoyalash uchun tashkil qilingan xavfsizlik choralaridagi zaifliklardan foydalangan holda amalga oshiriladi.

Phishing kiberhujumlaridan himoyalanish uchun quyidagi tavsiyalarga amal qilish zarur:

1. **Yuboruvchini diqqat bilan tekshirish** – agar xat notanish manzildan kelgan bo‘lsa yoki manzil asl nusxaga o‘xshab, lekin matnda orfografik xato aniqlansa, bu soxta elektron pochta bo‘lishi mumkin.

© G‘ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich

2. **Shubhali xatlardagi ilovalar yoki havolalarni ochmaslik** - agar bunday mazmundagi xat kelishi kutilmayotgan bo‘lsa, uni ilovani ochmasdan yoki havolani bosmasdan o‘chirib tashlagan ma’qul.

3. **Veb-sayt URL manzilini tekshirish** - veb-saytga maxfiy ma’lumotlarni kiritishdan oldin URL manzilini tekshirish orqali rasmiy sayt ekanligiga ishonch hosil qilish.

4. Zararli dasturlar va kiberhujumni aniqlash va blokirovka qilish uchun **antivirus dasturlari** va **tarmoqlararo ekrandan (firewall) foydalanish**.

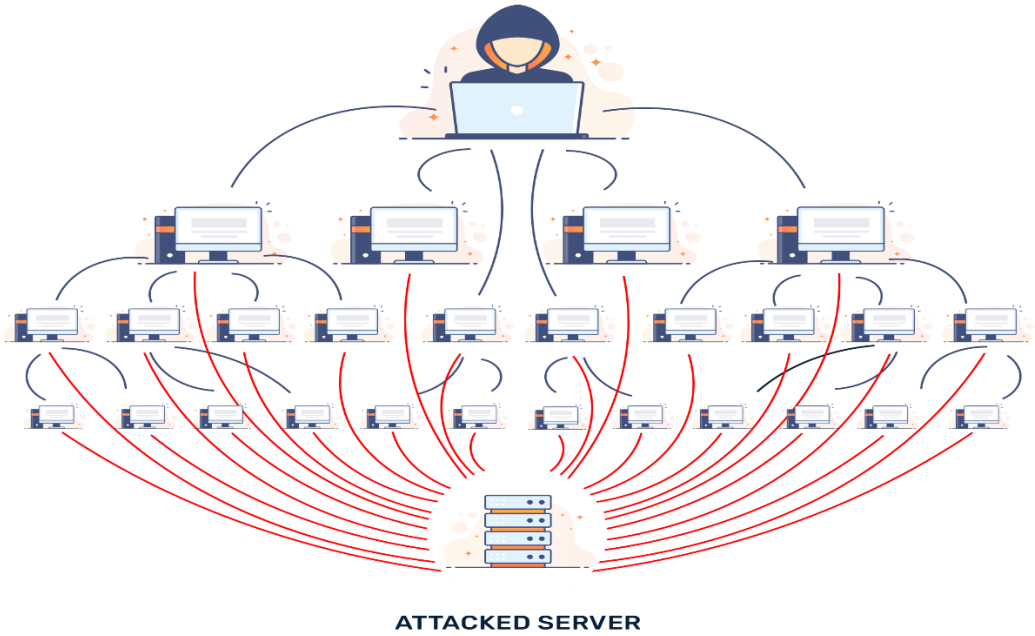
5. **Umumiy Wi-Fi tarmog‘idan foydalanishda ehtiyot bo‘lish** – ochiq Wi-Fi tarmoqlari ishlayotganda maxfiy ma’lumotlarni veb-sayt yoki ilovalarga kiritishdan saqlanish.

6. **Mustahkam kalit so‘zlar (parol) va ko‘p faktorli autentifikatsiyadan foydalanish** - mustahkam parollar va qo‘shimcha identifikatsiya tekshiruvi phishing kiberhujumi sodir bo‘lgan taqdirda ma’lumotlarni himoya qilishga yordam beradi.

7. **Xodimlarni malakasini oshirish** - xodimlarni malakasini oshirish phishing va boshqa turdagi kiberhujumlaridan himoyalanish uchun zarur hisoblanadi. Bu kiberjinoyat oqibatlarini bartaraf etishga sarflanadigan mablag‘lardan ancha arzonga tushadi.

DDoS kiberhujumlari

DDoS (Distributed Denial of Service) – bu kiberhujumlarning bir turi bo‘lib, unda kiberjinoyatchilar tarmoq resursini yoki serverni ko‘p sonli so‘rovlar bilan haddan tashqari yuklaydi, bu esa unga kirishni imkonsiz qilib qo‘yadi. Ushbu turdagi kiberhujum kompaniyalar va tashkilotlar uchun jiddiy muammolarga olib kelishi mumkin, chunki bu daromadning yo‘qolishiga, mahsuldorlikning pasayishiga va hatto veb-saytning to‘liq ishlamasligiga olib kelishi mumkin. Quyidagi 4-rasmda DdoS kiberhujumlarning umumiy ko‘rinishi keltirilgan [9].

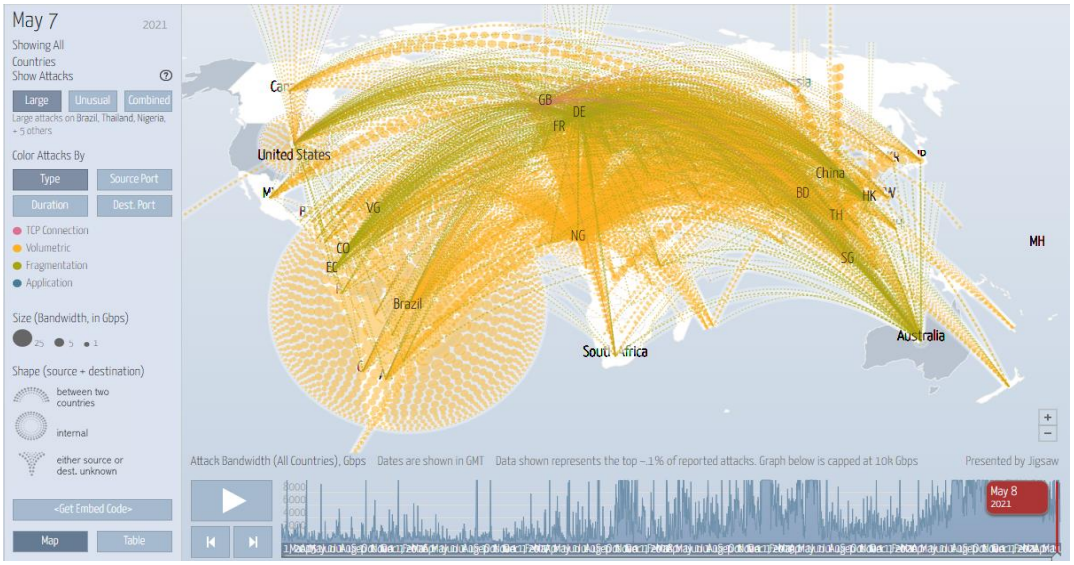


4-rasm. DdoS kiberhujumlarning umumiy ko‘rinishi.

Kiberjinoyatchilar kiberhujumni kuchaytirish uchun turli usullardan foydalanishi mumkin, masalan, tarmoq sathi protokollariga (UDP va ICMP kabi) yoki seansni to‘ldirish va ilovalarga kiberhujum bo‘lishi mumkin. Natijada, tarmoq resursi haddan tashqari yuklanadi va foydalanuvchi so‘rovlariga javob berishni to‘xtatiladi.

Avval yoki joriy vaqtda dunyo bo‘ylab qanday DDoS kiberhujumlari amalga oshirilganini https://www.digitalattackmap.com sayti orqali qo‘rishimiz mumkin (5-rasm).

© *G‘ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich*



5-rasm. Dunyo bo'ylab amalga oshirilayotgani DDoS kiberhujumlar.

DDoS kiberhujumini oldini olish kompaniyaning onlayn mavjudligi, ishonchliligi va xavfsizligini ta'minlash uchun muhim ahamiyatga ega.

Quyida DDoS hujumlarining ba'zi keng tarqalgan turlari ko'rib chiqiladi:

UDP Flood Attack - Bu hujum maqsadli serverni ko'p sonli UDP paketlari bilan to'ldiradi, bu esa serverning resurslarni tugatadi va uni ishdan chiqaradi.

ICMP Flood Attack - bu hujum maqsadli serverni ko'p sonli ICMP so'rovlari bilan to'ldirish orqali uni resurslarini tugatadi, bu esa haqiqiy foydalanuvchilarning serverga kirishiga to'sqinlik qiladi.

Application Layer DDoS Attack - ushbu turdagi hujum veb-ilovalardagi zaifliklarni nishonga oladi, masalan, buferni to'ldirish, SQL in'eksiyasi yoki saytlararo skript (XSS).

SYN Flood Attack - bu hujum maqsadli serverni ko'p sonli SYN so'rovlari bilan to'ldiradi, lekin hech qachon "qo'l siqish" jarayonini tugatmaydi. Bu server resurslari resurslari yuklamasini oshiradi va haqiqiy foydalanuvchilarning serverga kirishini cheklaydi.

IP-spoofing Attack - bu hujumda kiberjinoyatchi o'zining IP -manzilni o'zgartiradi va maqsadli serverni ko'p sonli so'rovlar bilan to'ldiradi, bu esa serverni ishdan chiqaradi.

Network Layer DDoS Attack - bu hujum tarmoqdagi marshrutizatorlar va boshqa qurilmalarni yo'q qilish va haqiqiy foydalanuvchilarning tarmoqqa kirishini oldini olish uchun mo'ljallangan.

Botnet DDoS Attack - Bu hujum keng ko'lamli DDoS hujumini boshlash uchun viruslangan qurilmalar tarmog'i bo'lgan botnetdan foydalanishni o'z ichiga oladi. Kiberjinoyatchilar botnet orqali bir nechta hujumlarni amalga oshiradilar, maqsad server resurslarini tugatish va haqiqiy foydalanuvchilarning serverga kirishiga to'sqinlik qilish.

Quyida DDoS kiberhujumlari oldini olish uchun zaruriy tavsiyalar yoritilgan:

1. **DDoS himoyasi xizmatlaridan foydalanish**: DDoS himoyasi xizmatlarini ko'rsatadigan StormWall, Servicepipe, InformConsulting kabi ko'plab ixtisoslashgan kompaniyalar mavjud. Ushbu kompaniyalar DDoS kiberhujumidan himoya qilish uchun trafikni filtrlash, xatti-harakatlarni tahlil qilish va boshqalar kabi turli xil himoya usullaridan foydalanadilar.

2. **Tarmoqni o'tkazish qobiliyatini oshirish**: DDoS kiberhujumidan himoya qilishning yana bir usuli tarmoq o'tkazish qobiliyatini oshirish. Bu internet xizmatining xarajatini oshirishi mumkin, ammo bu tarmoqni DDoS kiberhujumidan himoya qilishga yordam beradi.

(cc) BY © *G'ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich*

3. **CDN (Content Delivery Network) dan foydalanish**: CDN dunyoning turli burchaklarida joylashgan turli serverlar o‘rtasida trafikni taqsimlash orqali DDoS kiberhujumidan himoya qilishga yordam beradi. Bu har qanday individual serverdagi yukni kamaytirishi mumkin, bu esa uni DDoS kiberhujumiga nisbatan zaifligini kamaytiradi.

4. **Bulutli xizmatlardan foydalanish**: Bulutli xizmatlar DDoS kiberhujumidan himoya qilishga yordam berishi mumkin, chunki ular moslashuvchan infratuzilmaga ega va so‘rovlar keskin oshib ketganda tez masshtablashish imkoniyatiga ega. Bu serverlarning ortiqcha yuklanishini oldini oladi va DDoS kiberhujumi zararini kamaytiradi.

5. **Kiberxavfsizlik siyosatini yaxshilash**: Yaxshi xavfsizlik choralari ko‘p turdagi DDoS kiberhujumilarini oldini oladi. Bunga murakkab parollardan foydalanish, dasturiy ta’minotni muntazam yangilab turish, tizim hodisalarini kuzatish va hokazolar kiradi.

6. **Trafik monitoringi**: Trafik monitoringi DDoS kiberhujumi ko‘rsatishi mumkin bo‘lgan tarmoq xatti-harakatlaridagi anomaliyalarni aniqlashga yordam beradi. Bunga jurnal fayllarini kuzatish va tahlil qilish kiradi. Bu kiberhujum jiddiy zarar keltirgunga qadar zararni kamaytirish uchun choralarni ko‘rish imkonini beradi.

7. **“Load Balancers”dan foydalanish**: Load Balancers kiruvchi trafikni bir nechta serverlar bo‘ylab taqsimlashi mumkin. Bu DDoS kiberhujumi natijasida bitta serverni ortiqcha yuklash xavfini kamaytiradi.

8. **So‘rovlar sonini cheklash**: Agar veb-saytda so‘rovlarni sonini cheklash imkoniyati bo‘lsa, bitta IP manzildan yuborilayotgan so‘rovlar sonini cheklashi mumkin. Bu serverning haddan tashqari yuklanishi bilan bog‘liq DDoS kiberhujumini oldini oladi.

9. **DNSni to‘g‘ri sozlash**: DNSni to‘g‘ri sozlash trafikni o‘z serverlariga yo‘naltirish uchun soxta DNS sozlamalaridan foydalanadigan kiberjinoyatchilar bilan bog‘liq DDoS kiberhujumining oldini olishga yordam beradi.

Ransomware kiberhujumlari

Ransomware – bu kiberhujumlarning bir turi bo‘lib, unda kiberjinoyatchi foydalanuvchining fayllarini shifrlaydi va ularni deshifrlash uchun to‘lov talab qiladi.

Kompyuterni zararlash jarayoni foydalanuvchi zararli fayl yoki virusli havolani ochganda boshlanadi. Keyin ransomware muhim fayllarga kirishni bloklaydi. Agar foydalanuvchi fayllarni shifrlash jarayonida virusni olib tashlashga harakat qilsa yoki shunchaki kompyuterni qayta ishga tushirsa, tizim butunlay ishdan chiqadi.

Ko‘pincha, kiberjinoyatchilar identifikatsiya qilish va jinoiy javobgarlikka tortish jarayonini murakkablashtirish uchun kriptovalyutada to‘lovni talab qilishadi. Biroq, to‘lov to‘lanishiga qaramay, ma’lumotlarni tiklash kamdan-kam hollarda sodir bo‘ladi. Misol uchun, 2017 yil may oyida WannaCry kompyuter virusi butun dunyo bo‘ylab oddiy foydalanuvchilar, biznes va davlat idoralari kompyuter tizimlariga zarba berdi. Bu Windows operatsion tizimining eski versiyalaridagi aniqlangan zaifliklardan foydalanib amalga oshirildi. WannaCry ommaviy pochta jo‘natmalaridagi havolalar orqali tizimga kirib, uning ustidan nazoratni qo‘lga kiritadi, so‘ngra kompyuter fayllarini shifrlaydi. Shundan so‘ng ekranda fayllar shifrini ochish uchun 300 dollar to‘lashni talab qiluvchi xabar paydo bo‘ldi. To‘lov Bitcoin hamyoniga o‘tkazilishi talab etiladi. 3 kundan keyin bu miqdor ikki baravar oshib, 600 AQSH dollarini tashkil etdi. 7 kundan keyin shifrlangan fayllar butunlay o‘chirib tashlandi [4].

Shuningdek, LockerGoga va MegaCortex zararli dasturlar oilasiga mansub 2019 yil sentabr oyida yaratilgan LockBit kabi zararli dasturlar kiberhujum uchun sarflanadigan vaqtni sezilarli darajada qisqartirdi. LockBit - bu kompyuter tizimlariga kirishni bloklaydigan va foydalanuvchidan ma’lumotlarni qayta tiklash uchun to‘lovni talab qiladigan zararli dastur hisoblanadi. Uni o‘ziga hos jihati shundaki, qo‘lda boshqariladigan LockerGoga va MegaCortex zararli dasturlar oilasiga mansub dasturlarda jabrlanuvchini kuzatish va ma’lumot to‘plash uchun bir necha hafta sarflangan bo‘lsa, LockBit zararli dasturi avtomatik tarzda mos qurbonni topishga, tarmoq bo‘ylab tarqalishga va zararlangan qurilmalardagi barcha ma’lumotlarni

(cc) BY © *G‘ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich*

shifrlashga o‘rtacha yarim soat oraligida vaqt sarflaydi [5].

Quyida Ransomware kiberxujumini ba’zi turlarini ko‘rib chiqiladi:

1. **Klassik ransomware**: fayllarga kirishni bloklaydigan va foydalanuvchidan to‘lovni talab qiladigan shifrlash virusi.

2. **Screen Locker**: kompyuter ekranini qulflaydigan va uni ochish uchun foydalanuvchidan to‘lovni talab qiladigan zararli dastur.

3. **Mobile Ransomware**: mobil qurilmalarga hujum qiladigan va ularga kirishni bloklaydigan, ularni qulfdan chiqarish uchun to‘lov talab qiladigan zararli dastur.

4. **Encrypting Ransomware**: qattiq diskdagi fayllarni shifrlaydigan va foydalanuvchidan shifrni ochish kaliti uchun to‘lovni talab qiluvchi shifrlash virusi.

5. **Scareware**: kompyuter virus bilan zararlanganligi haqida soxta xabar beruvchi dastur. Jabrlanuvchiga virusni olib tashlash uchun dasturiy ta’minotni sotib olish taklif etiladi, aslida esa virus yo‘q bo‘ladi.

6. **Leakware**: agar to‘lov to‘lanmasa, maxfiy ma’lumotlarni oshkor qilish bilan tahdid qiluvchi zararli dastur.

7. **RaaS** (Ransomware as a Service): bu hujum modelida Ransomware zararli dasturini ishlab chiquvchi ma’lum mablag‘ evaziga kiberjinoyatchilarga o‘z dasturlaridan foydalanishga imkon beradi.

Ransomware kiberhujumidan himoyalanish uchun quyidagilar tavsiya qilinadi:

1. Ma’lumotlarning zaxira nusxasini muntazam ravishda yaratish va ularni xavfsiz joyda saqlash.

2. Antivirus dasturlardan foydalanish, shuningdek, dasturiy ta’minot va operatsion tizimni doimiy yangilab borish.

3. Shubhali fayllar yoki havolalarni ochmaslik, ayniqsa ularni jo‘natuvchisi noma’lum bo‘lganda.

4. Kompaniya xodimlarini internet xavfsizligi qoidalariga o‘rgatish, jumladan, ularga bir xil parolni bir nechta saytlarda ishlatmaslik va shubhali xatlarni ochmaslik haqida tavsiya berish.

5. Kiberhujum sodir bo‘lgan taqdirda, darhol virus tarqalishini to‘xtatish va zararni kamaytirishga yordam beruvchi axborot xavfsizligi mutaxassislariga murojaat qilish va hakazo.

Zaif nuqtalarga kiberhujumlar

Zaif nuqtalarga kiberhujumlar – bu turdagi kiberhujumlarda kiberjinoyatchilar kompyuter tizimida, tarmoqda yoki ilovada mavjud zaiflik va kamchiliklardan foydalangan holda ularga kirishga urinadi. Quyida zaif nuqtalarga kiberhujumning eng keng tarqalgan turlari keltirilgan:

1. **Ilova zaifliklariga kiberhujum** - bunda kiberjinoyatchilar zaif nuqtalari aniqlangan ilovalar ishlayotgan tizimga ruxsat etilmagan kirishni amalga oshirishi mumkin. Kiberjinoyatchilar tomonidan ishlatiladigan eng keng tarqalgan zaifliklarga SQL in’eksiyasi, saytlararo skriptlar (XSS), kodlarni kiritish va boshqalar kiradi.

2. **Operatsion tizim zaifliklariga kiberhujum -** operatsion tizimlarda ham foydalanish mumkin bo‘lgan zaifliklar bo‘lishi mumkin. Operatsion tizimlar bilan bog‘liq eng keng tarqalgan zaifliklarga xizmat ko‘rsatishni rad etish, yadro zaifliklari, paketli kiberhujum uyushtirish orqali xizmat ko‘rsatishni rad etish va boshqalar kiradi.

3. **Tarmoq zaifliklariga kiberhujum -** tarmoq qurilmalarida ham ishlatilishi mumkin bo‘lgan zaifliklar mavjud bo‘lishi mumkin. Masalan, kiberjinoyatchilar trafikni ushlab turish uchun ARP-zaharlash kiberhujumidan, seanslarni to‘xtatish uchun DNS serverlariga kiberhujumdan, trafikni qayta yo‘naltirish uchun routerlarga kiberhujumdan va boshqalardan foydalanishi mumkin.

© *G‘ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich*

4. **Ijtimoiy muhandislik (Social Engineering)** - foydalanuvchilarni aldash usuli bo‘lib, bu maxfiy ma’lumotlarning chiqib ketishiga yoki tizimni buzishga olib kelishi mumkin. Bunga tashkilotlar yoki taniqli kompaniyalarning rasmiy elektron pochta xabarlari sifatida niqoblangan phishing elektron pochta xabarlari, rasmiy saytlarni taqlid qiluvchi soxta veb-saytlar va boshqalarni misol qilish mumkin.

5. **Boshqaruv tizimlarining zaif tomonlariga kiberhujum** - boshqaruv tizimlarining zaif tomonlariga kiberhujum ma’lumotlar bazasini boshqarish tizimlari (DBMS), kontentni boshqarish tizimlari (CMS) va boshqa tizimlar kabi boshqaruv tizimlarining zaifliklaridan foydalanishga qaratilgan. Masalan, kiberjinoyatchilar maxfiy ma’lumotlarga ruxsatsiz kirish uchun ma’lumotlar bazasidagi zaifliklardan foydalanishlari mumkin.

6. **IoT (internet ashyolar) qurilmalaridagi zaif tomonlarga kiberhujum**: IoT qurilmalaridagi zaif tomonlarga kiberhujum aqlli uylar, avtomobillar va boshqa qurilmalarga qaratilgan. Masalan, bunga uyni signalizatsiyasini uchirish, aqlli avtomabilni avtohalokatga uchratish (Tesla misolida) va boshqalar kiradi.

Quyida zaif nuqtalarga kiberhujumlardan himoyalanishga yordam beradigan zaruriy chora-tadbirlar keltirilgan:

1. **Dasturiy ta’minotni va operatsion tizimni muntazam yangilab borish**. Dasturiy ta’minot ko‘pincha kiberjinoyatchilar tomonidan ishlatilishi mumkin bo‘lgan zaifliklarni o‘z ichiga oladi. Ishlab chiquvchilar ushbu zaifliklarni tuzatish uchun doimiy ravishda yangilanishlarni chiqaradilar. Ushbu yangilanishlarni muntazam o‘rnatish zarur.

2. **Mustahkam parollardan va ko‘p faktorli autentifikatsiyadan foydalish**. Parollarni murakkabroq qilish va turli saytlar uchun turli parollardan foydalish. Shuningdek, ko‘p faktorli autentifikatsiyadan foydalanish tavsiya etiladi.

3. **Barcha qurilmalarni antivirus dasturi bilan himoyalanganligiga ishonch hosil qilish**. Antivirus dasturi zaif nuqtalarga kiberhujumni aniqlash va oldini olishga yordam beradi.

4. **Zaif nuqtalarga kiberhujumdan himoya qiluvchi tarmoq qurilmalaridan foydalish**. Bunga tarmoqlararo ekranlar va kiberhujumni aniqlash vositalaridan foydalanish kiradi.

5. **Foydalanuvchilarni axborot xavfsizligi masalasida malakasini oshirish**. Foydalanuvchilar zaif nuqtalarga kiberhujumni qanday aniqlash va oldini olishni bilishlari kerak. Bunga foydalanuvchilarni phishing kiberhujumini tanib olishi, murakkab parollardan foydalanish va dasturiy ta’minotni yangilash bo‘yicha o‘rgatish kiradi.

6. **Axborotdan foydalanishga cheklovlar o‘rnatish**. Axborotga kirishga cheklovlar o‘rnatish va maxfiy ma’lumotlarga ruxsatsiz kirishni cheklash ma’lumotlar sizib chiqish xavfini kamaytiradi.

7. **Audit jurnallarini kuzatib borish**. Audit jurnallari zaif tomonlarga kiberhujumni xamda qanday ma’lumotlar buzilganligini aniqlashga yordam beradi.

8. **Eng kam imtiyozlar tamoyiliga rioya qilish**. Foydalanuvchilar to‘liq ma’muriy huquqlarga ega bo‘lmasligi, balki faqat kerakli kirish huquqlariga ega bo‘lishlari kerak. Bu tizimdagi zaifliklardan foydalanish xavfini kamaytiradi.

9. **Ma’lumotlarning zaxira nusxasini muntazam ravishda yaratish va ularni xavfsiz joyda saqlash.**

10. **Ruxsat etilmagan kirishlar oldi olinganligini test qilish va axborot xavfsizligi mavzusidagi yangiliklarni kuzatib borish**. Bu tizimdagi zaifliklarni aniqlash va ularni kiberjinoyatchilar tomonidan foydalanishdan oldin tuzatishga yordam beradi.

Zararli dasturlar

Zararli dasturiy ta’minotlar - bu kiberjinoyatchilar tomonidan kompyuterga zarar yetkazish, konfidensial ma’lumotlarni o‘g‘irlash yoki keyingi kiberhujum uchun kompyuterdan

© *G‘ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich*

foydalanish uchun yaratilgan dastur. Ular elektron pochta, veb-saytlar, tashqi qurilmalar, ijtimoiy tarmoqlar va boshqa ko‘plab kanallar orqali tarqatilishi mumkin.

Zararli dasturlar turli maqsadlarga ega bo‘ladi. Ulardan ba’zilari login va parollar, bank karta ma’lumotlari va boshqa konfidensial ma’lumotlarni o‘g‘irlashga qaratilgan bo‘lishi mumkin. Ayrim zararli dasturlar josuslik qilish uchun ishlatiladi.

Zararli dasturlarning bir necha xil turlari mavjud bo‘lib, ular quyida keltirilgan:

1. **Viruslar**. Bu boshqa dasturlarning kodiga, tizim xotira sohalariga, yuklash sektorlariga kirib boruvchi va ularni ishdan chiqaruvchi zararli dastur.

2. **Qurtlar**. Qurtlar viruslarga o‘xshaydi, lekin ular tarmoq orqali tarqalishi mumkin. Ular tarmoqdagi kompyuterlarni skanerlashi va ularga o‘zini nusxalashi mumkin.

3. **Troyanlar**. Troyanlar foydali dasturlar sifatida yashiringan zararli dasturlardir. Bunday dasturlarni yuklab olib, o‘rnatilganida, ular tizimga kirishi va konfidensial ma’lumotlarni o‘g‘irlashi mumkin.

4. **Advar**. Reklama dasturi (inglizcha - “advertising software”) foydalanuvchi ruxsatisiz reklamalarni ko‘rsatuvchi zararli dastur. Bu tiziminni sekinlashtirishi va ish faoliyatini yomonlashtirishi mumkin.

5. **Spam**. Zararli veb-saytlar yoki viruslarga havolalar bo‘lishi mumkin bo‘lgan elektron pochta xabari. Agar ushbu havolalar bosilsa, kompyuter zararlanishi mumkin.

6. **Rootkitlar**. Rootkitlar - bu kompyuterdagi tizim fayllariga kira oladigan yashirin dasturlar. Ular ma’lumotlarni o‘zgartirishi, yashirishi, tizim boshqaruvini qo‘lga olishi mumkin, bu esa ularni aniqlash va uchirib tashlashni qiyinlashtiradi.

7. **Spyware**. Josuslik dasturi - bu foydalanuvchi onlayn faoliyatini, jumladan u tashrif buyurgan veb-saytlar, kiritgan parollar va shaxsiy ma’lumotlarni kuzatishi mumkin bo‘lgan zararli dastur.

Zararli dasturlardan himoyalanish uchun quyidagi amallarni bajarish tavsiya etiladi:

1. Kompyuterlar va mobil qurilmalarga antivirus dasturlarini o‘rnatish va uni muntazam ravishda eng so‘nggi versiyasiga yangilash.

2. Faqat ishonchli manbalardan olingan rasmiy va tasdiqlangan ilovalar va dasturlardan foydalanish.

3. Notanish va ishonchsiz manbalardan olingan elektron pochta ilovalarini yoki fayllarni hech qachon ochmaslik.

4. Agar kerak bo‘lsa, parol yoki boshqa autentifikatsiya vositalaridan foydalangan holda kompyuter yoki mobil qurilmaga kirishni cheklash.

5. Operatsion tizim va boshqa dasturiy ta’minotni so‘nggi versiyalarga yangilash.

6. Umumiy Wi-Fi tarmoqlaridan foydalanganda ehtiyot bo‘lish. Parollar yoki bank kartasi ma’lumotlari kabi maxfiy ma’lumotlarni kiritmaslik.

7. Kompyuterda zararli dastur mavjudligini muntazam ravishda tekshirib turish va agar ular topilsa, ularni o‘chirib tashlash.

8. Foydalanuvchilarni shubhali havolalarni bosmaslik yoki noma’lum jo‘natuvchilarning ilovalarini ochmaslik kabi asosiy xavfsizlik tamoyillariga o‘rgatish.

III. XULOSA

Xulosa qilib aytadigan bo‘lsak, zamonaviy kiberhujumlar butun dunyo bo‘ylab oddiy foydalanuvchilar, biznes va hukumatlar uchun jiddiy xavf tug‘dirmoqda. Texnologiyaga qaramlik kuchayib borayotganligi kibertahdidlarning turlarini va ularning oldini olish uchun ko‘rilishi zarur bo‘lgan himoya choralarini qo‘llash juda muhimdir. Zamonaviy kiberhujumlardan himoyalanishning eng yaxshi usuli bu kiberxavfsizlikka proaktiv yondashish bo‘lib, u xavfsizlik bo‘yicha eng so‘nggi tajribalarni tatbiq qilishni, mustahkam xavfsizlik

(cc) BY © *G‘ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich*

choralarini qo‘llashni va muntazam xavfsizlik auditini o‘tkazishni o‘z ichiga oladi.

Kiberxavfsizlik bo‘yicha hech qanday yechim ishonchli bo‘lmasada, texnik yechimlar va xodimlarni malakasini oshirishning kombinatsiyasi kiberhujum xavfini sezilarli darajada kamaytiradi. Kiberxavfsizlikdan samarali himoya qilish bo‘yicha maslahat bera oladigan ishonchli kiberxavfsizlik mutaxassislari bilan ishlash ham muhim. Keng qamrovli kiberxavfsizlik strategiyasiga sarmoya kiritib, oddiy foydalanuvchilar, korxonalar va hukumatlar o‘zlarini kiberhujumning potensial halokatli oqibatlaridan himoya qilishlari mumkin. Shuni esda tutish zarur, kiberxavfsizlik haqida gap ketganda, **oldini olish har doim davolashdan ko‘ra yaxshiroqdir**.

IV.ADABIYOTLAR

1. O‘zbekiston Respublikasi Kiberxavfsizligi - 2020 yil hisoboti // https://csec.uz/uz/news/maqolalar/o-zbekiston-respublikasi-kiberxavfsizligi-2020-yil-his
2. https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/#statisticContainer
3. https://www.vesti.ru/finance/article/2481467
4. Берова Д.М., Кибератаки как угроза информационной безопасности. 2018 // https://cyberleninka.ru/article/n/kiberataki-kak-ugroza-informatsionnoy-bezopasnosti
5. Шифровальщик LockBit – что нужно знать // https://www.kaspersky.ru/resource-center/threats/lockbit-ransomware
6. Kevin Mitnick. The Art of Invisibility: The World’s Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data, 2017, pages 320
7. Christopher Hadnagy. Social Engineering: The Science of Human Hacking, 2018, pages 322
8. Thomas Kranz. Making Sense of Cybersecurity, 2022, pages 288
9. What Are Distributed Denial of Service Attacks? https://bunny.net/academy/network/what-are-distributed-denial-of-service-ddos-attacks/

© *G‘ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich*