HUJUM ZANJIRI (ATTACK CHAIN)

Maxkamova Dildora Begaliyevna
Muhammad al-Xorazmiy nomidagi TATU assistenti
Erkinov Shohjahon Sherali o'g'li
Xayriddinov Shaxboz Shavkatovich
Quyliyev Behro'z Sherzod o'g'li
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: *Ushbu maqolada kiberhujumlarning bosqichma-bosqich amalga oshirilish jarayoni – Hujum zanjiri (Attack Chain) tushunchasi tahlil qilinadi. Hujum zanjiri modeli kiberjinoyatchilarning tizimga kirishdan tortib, maqsadga erishishgacha bo'lgan harakatlarini ketma-ket bosqichlarda ifodalaydi.*

Kalt so'zlar: *Hujum zanjiri, Cyber Kill Chain, razvedka, ekspluatatsiya, command and control, lateral harakat, kiberhujum bosqichlari, proaktiv himoya, axborot xavfsizligi.*

Hujum zanjiri (Attack Chain yoki Cyber Kill Chain) — bu kiberhujumning bosqichma-bosqich rivojlanish jarayonini ifodalovchi konseptual modeldir. Mazkur model hujumchining dastlabki razvedkadan tortib, yakuniy maqsadga erishishigacha bo'lgan barcha harakatlarini tizimli ravishda tavsiflaydi. Ushbu tushuncha ilk bor Lockheed Martin kompaniyasi tomonidan "Cyber Kill Chain" nomi bilan ishlab chiqilgan bo'lib, zamonaviy kiberxavfsizlik strategiyalarining muhim metodologik asosi hisoblanadi. Keyinchalik MITRE ATT&CK modeli ushbu konsepsiyani yanada kengaytirib, taktik va texnik darajadagi hujum vektorlarini batafsil tasniflab berdi.

Hujum zanjiri modeli shuni ko'rsatadiki, kiberhujumlar odatda bir martalik emas, balki ketma-ket bosqichlardan iborat murakkab jarayondir. Har bir bosqich oldingisining natijasiga asoslanadi. Agar zanjirning biror bosqichi muvaffaqiyatsiz bo'lsa, hujumning umumiy samaradorligi pasayadi yoki butunlay to'xtaydi.

Shu sababli zamonaviy himoya strategiyasi hujumni faqat yakuniy bosqichda emas, balki har bir oraliq bosqichda aniqlash va to'xtatishga qaratilgan bo'lishi kerak.

Hujum zanjirining asosiy bosqichlari

Klassik Cyber Kill Chain modeli quyidagi asosiy bosqichlardan iborat:

1. Reconnaissance (Razvedka)
2. Weaponization (Zararli vosita tayyorlash)
3. Delivery (Yetkazib berish)
4. Exploitation (Ekspluatatsiya)
5. Installation (O'rnatish)
6. Command and Control (Boshqaruvni qo'lga olish)
7. Actions on Objectives (Maqsadga erishish)

Quyida har bir bosqich kengroq ilmiy tahlil qilinadi.

Reconnaissance (Razvedka bosqichi)

Razvedka — hujumning boshlang'ich bosqichi bo'lib, hujumchi nishon tizim haqida maksimal darajada ma'lumot to'plashga harakat qiladi. Bu bosqich passiv yoki aktiv shaklda amalga oshirilishi mumkin.

Passiv razvedkada hujumchi ochiq manbalardan (OSINT) foydalanadi. Masalan:

☐ Tashkilotning rasmiy veb-sayti
☐ Ijtimoiy tarmoqlar
☐ Xodimlarning LinkedIn profillari
☐ Domen nomlari va DNS yozuvlari

Aktiv razvedkada esa hujumchi to'g'ridan-to'g'ri tarmoqqa so'rov yuboradi, port scanning, xizmat aniqlash va versiya tekshiruvi kabi usullardan foydalanadi. Active Directory muhitida razvedka jarayoni quyidagilarni o'z ichiga olishi mumkin:

☐ Domen nomini aniqlash
☐ Domain Controller manzilini topish
☐ Foydalanuvchilar va guruhlarni enumeratsiya qilish
☐ LDAP orqali ma'lumot yig'ish

Razvedka bosqichi keyingi hujum strategiyasini aniqlash uchun asos yaratadi.

Weaponization (Zararli vosita tayyorlash)

Ushbu bosqichda hujumchi ekspluatatsiya qilish uchun maxsus zararli dastur yoki skript tayyorlaydi. Bu bosqich ko'pincha qurbon tizimdan tashqarida amalga oshiriladi. Masalan:

☐ Phishing hujumi uchun zararli hujjat yaratish
☐ Makrosli Word yoki Excel fayl tayyorlash
☐ Exploit kit ishlab chiqish
☐ Backdoor dastur tayyorlash

Active Directory kontekstida hujumchi credential harvesting vositalarini, Kerberos exploit skriptlarini yoki PowerShell asosidagi zararli modullarni tayyorlashi mumkin.

Delivery (Yetkazib berish). Delivery bosqichida zararli vosita qurbon tizimga uzatiladi. Eng keng tarqalgan usullar:

☐ Phishing email
☐ Zararli havola (malicious link)
☐ USB qurilma
☐ Kompрometatsiya qilingan veb-sayt

AD muhitida ko'pincha phishing orqali domen foydalanuvchisining login-paroli qo'lga kiritiladi. Bu hujumning ichki bosqichiga o'tish imkonini beradi.

Exploitation (Ekspluatatsiya). Ekspluatatsiya bosqichida tizimdagi zaiflikdan foydalaniladi. Bu zaiflik:

☐ Zaif parol
☐ Yangilanmagan operatsion tizim
☐ Noto‘g‘ri konfiguratsiya
☐ Xavfsizlik siyosatining sustligi bo‘lishi mumkin.

Masalan, AD muhitida:

☐ Kerberoasting orqali xizmat hisobi buziladi
☐ Pass-the-Hash orqali autentifikatsiya amalga oshiriladi
☐ Noto‘g‘ri ACL orqali huquq oshiriladi.

Ekspluatatsiya bosqichi hujumchiga dastlabki kirishni beradi.

Installation (O‘rnatish bosqichi). Bu bosqichda hujumchi tizimga doimiy kirish imkoniyatini yaratadi. Masalan:

☐ Backdoor o‘rnatish
☐ Yangi administrator hisob yaratish
☐ Registry o‘zgartirish
☐ Rejalashtirilgan vazifa (Scheduled Task) yaratish

Active Directory muhitida zararli GPO o‘rnatilishi yoki yashirin xizmat hisobi qo‘shilishi mumkin.

Command and Control (C2). Command and Control bosqichida hujumchi kompрometatsiya qilingan tizim bilan aloqa o‘rnatadi. Bu bosqich uzoq muddatli nazoratni ta’minlaydi.

C2 kanallari:

☐ HTTP/HTTPS
☐ DNS tunneling
☐ Encrypted traffic

AD muhitida bu bosqich lateral harakatlar (lateral movement) uchun ishlatiladi. Hujumchi bir tizimdan boshqasiga o‘tib, Domain Controller tomon yaqinlashadi.

Actions on Objectives (Maqsadga erishish).Hujumning yakuniy bosqichi hujumchining asl maqsadini amalga oshirishdir. Bu quyidagilar bo‘lishi mumkin:

☐ Ma’lumot o‘g‘irlash
☐ Ransomware joylashtirish
☐ Domenni to‘liq egallash
☐ Maxfiy hujjatlarni chiqarish

Active Directory muhitida yakuniy maqsad odatda Domain Admin huquqini qo‘lga kiritishdir.

Hujum zanjirining AD muhitidagi tipik ssenariysi. Quyidagi ketma-ketlik AD muhitida tez-tez uchraydi:

1. Phishing orqali foydalanuvchi paroli olinadi
2. Ichki tarmoqqa kirish amalga oshiriladi
3. LDAP orqali domen strukturasi o‘rganiladi
4. Kerberoasting orqali xizmat hisobi buziladi

5. Privilege Escalation amalga oshiriladi
6. DCSync orqali administrator hash olinadi
7. Golden Ticket yaratiladi
8. Domen to‘liq nazorat qilinadi.

Bu jarayon ko‘pincha haftalar yoki oylar davomida yashirin amalga oshiriladi.Hujum zanjiri modeli kiberhujumlarni tizimli tahlil qilish imkonini beradi. Ushbu model asosida har bir bosqichda aniqlash va oldini olish mexanizmlarini ishlab chiqish mumkin. Zamonaviy kiberxavfsizlik strategiyasi proaktiv yondashuvni talab qiladi, ya’ni hujumni yakuniy bosqichda emas, balki dastlabki razvedka yoki ekspluatatsiya bosqichida aniqlash muhimdir. Active Directory muhitida hujum zanjirini tushunish xavfsizlik siyosatini to‘g‘ri shakllantirish, monitoring tizimlarini sozlash va Incident Response jarayonini optimallashtirish uchun asos bo‘lib xizmat qiladi.

XULOSA

Xulosa qilib aytganda, hujum zanjiri (Attack Chain) modeli kiberhujumlarning mantiqiy va ketma-ket rivojlanish jarayonini tushuntirib beradi. Har bir bosqich hujumning keyingi bosqichiga o‘tish uchun asos bo‘lib xizmat qiladi. Agar himoya tizimi ushbu zanjirning biror bosqichida hujumni to‘xtata olsa, butun hujum muvaffaqiyatsiz yakunlanadi.

Cyber Kill Chain modeli tashkilotlarga tahdidlarni tahlil qilish, xavfsizlik monitoringini kuchaytirish va samarali javob choralarini ishlab chiqish imkonini beradi. Ayniqsa, razvedka va yetkazib berish bosqichlarida aniqlangan tahdidlar katta zararlarning oldini oladi.

ADABIYOTLAR RO‘YXATI:

1. Lockheed Martin. Cyber Kill Chain® Framework Documentation.
2. MITRE Corporation. ATT&CK Framework for Enterprise.
3. SANS Institute. Intrusion Detection and Attack Lifecycle.
4. NIST. Computer Security Incident Handling Guide (SP 800-61).
5. ENISA. Threat Landscape Report.