KIBERJINOYATCHILIKNI OLDINI OLISHDA ZERO-DAY ZAIFLIKLARNI ANIQLASH VA BARTARAF ETISH

Sultonboyev Otabek Dilshodbek o‘g‘li
O’zbekiston Respublikasi IIV Akademiyasi 1-bosqich kurasanti.
Iminov Abdurasul Abdulatipovich
O’zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedraasi boshlig’i, podpolkovnik, fizika fanlari nomzodi, dotsent.

Annotatsiya:*Axborot texnologiyalari jadal rivojlanib borayotgan hozirgi davrda kiberxavfsizlik muammolari dolzarb masalalardan biriga aylanib bormoqda. Turli dasturiy ta'minot va tizimlardagi zaifliklardan foydalangan holda kiberjinoyatchilar korxonalar, davlat tashkilotlari va oddiy foydalanuvchilarga jiddiy zarar yetkazishi mumkin. Ayniqsa, zero-day zaifliklar — ya’ni ishlab chiquvchilar tomonidan hali aniqlanmagan va tuzatilmagan xavfsizlik nuqsonlari — eng xavfli kiberxavfsizlik tahdidlaridan biri hisoblanadi.*

Zero-day zaifliklar kiberjinoyatchilar tomonidan ekspluatatsiya qilingunga qadar aniqlanmasa, katta moliyaviy va axborot yo‘qotishlariga olib kelishi mumkin. Shuning uchun ushbu zaifliklarni erta aniqlash va ularni samarali bartaraf etish usullarini ishlab chiqish muhim ahamiyatga ega. Ushbu maqolada zero-day zaifliklarining mohiyati, ularni aniqlash usullari hamda kiberjinoyatchilikning oldini olish uchun qanday himoya choralarini ko‘rish mumkinligi haqida so‘z yuritiladi.

Kalit so‘zlar: *kiberxavfsizlik, kiberjinoyatchilik, zero-day zaifliklar, zaifliklarni aniqlash, axborot xavfsizligi, himoya choralar, ekspluatatsiya, dasturiy ta’minot, ma’lumotlar himoyasi, tahdidlarni aniqlash.*

Annotation:*With the rapid advancement of modern information technologies, cybersecurity threats are also increasing. Cybercriminals can exploit vulnerabilities in software and information systems to cause significant damage to organizations, government institutions, and individual users. In particular, zero-day vulnerabilities—security flaws that have not yet been identified and patched by developers—are among the most serious cybersecurity threats.*

If zero-day vulnerabilities are not detected or mitigated in time, cybercriminals can exploit them, leading to financial losses, data breaches, and system failures. Therefore, early detection, prevention, and effective mitigation of such vulnerabilities are crucial aspects of ensuring information security. This article explores the nature of zero-day vulnerabilities, methods for identifying them, and the protective measures used to prevent cybercrime.

Keywords: *cybersecurity, cybercrime, zero-day vulnerabilities, vulnerability detection, information security, protective measures, exploitation, software security, data protection, threat detection.*

Аннотация: *В нынешнюю эпоху, когда информационные технологии стремительно развиваются, проблемы кибербезопасности становятся одной из актуальных проблем. Используя уязвимости в различных программах и системах, киберпреступники могут нанести серьезный ущерб предприятиям, государственным организациям и обычным пользователям. В частности, уязвимости zero-day, то есть уязвимости безопасности, которые еще не были обнаружены и исправлены разработчиками, являются одними из самых опасных угроз кибербезопасности.*

Нулевой день может привести к огромным финансовым и информационным потерям, если уязвимости не будут обнаружены до тех пор, пока они не будут использованы киберпреступниками. Поэтому важно выявлять эти уязвимости на ранней стадии и разрабатывать методы их эффективного устранения. В этой статье рассказывается о природе уязвимостей zero-Day, методах их обнаружения и о том, какие защитные меры можно предпринять для предотвращения киберпреступности.

Ключевые слова: *кибербезопасность, киберпреступность, нулевой день уязвимости, обнаружение уязвимостей, информационная безопасность, защита меры, эксплойты, программное обеспечение, защита данных, обнаружение угроз.*

1. Zero-Day Zaifliklari Nima?

Zero-Day zaifliklari dasturiy ta'minot, operatsion tizim yoki qurilmalarda mavjud bo'lgan, ammo hali aniqlanmagan yoki tuzatilmagan xatolardir. Bu zaifliklar "Zero-Day" deb ataladi, chunki ular birinchi marta foydalanilganda, ular haqida hech qanday ma'lumot mavjud emas (ya'ni, "0-kun"). Zero-Day hujumlari odatda yuqori darajada tashkil etilgan va maqsadli bo'ladi.

Zero-Day Zaifliklarining Xususiyatlari:

Zero-Day Zaifliklari kiberxavfsizlik sohasidagi eng xavfli va qiyin muammolardan biridir. Bu zaifliklar dasturiy ta'minot, operatsion tizim yoki qurilmalarda mavjud bo'lgan, ammo hali aniqlanmagan yoki tuzatilmagan xatolardir. Ular "Zero-Day" deb ataladi, chunki ular birinchi marta foydalanilganda, ular haqida hech qanday ma'lumot mavjud emas (ya'ni, "0-kun"). Zero-Day hujumlari odatda yuqori darajada tashkil etilgan va maqsadli bo'ladi.

Aniqlanmagan: Zaiflik hali aniqlanmagan va tuzatilmagan.

Yuqori Xavfli: Zero-Day zaifliklari kiberjinoyatchilar tomonidan tezda foydalanilishi mumkin.

Maqsadli: Ko'pincha ma'lum bir tashkilot yoki shaxsga qaratilgan hujumlarda qo'llaniladi.

Zero-Day zaifliklari kiberjinoyatchilikda turli usullar bilan qo'llaniladi. Quyida eng keng tarqalgan usullar keltirilgan:

1. Maqsadli Hujumlar (Targeted Attacks):

APT (Advanced Persistent Threat): Zero-Day zaifliklari APT hujumlarida ko'p qo'llaniladi. Bu hujumlar ma'lum bir tashkilotga qaratilgan bo'lib, uzoq vaqt davomida amalga oshiriladi.

Davlatlararo Kiberhujumlar: Zero-Day zaifliklari davlatlar o'rtasidagi kiberhujumlarda qo'llaniladi. Masalan, Stuxnet virusi (2010) Iranning yadroviy dasturiga hujum qilgan.

2. Malware Tarqatish:

Zararli Dasturlar (Malware): Zero-Day zaifliklari orqali zararli dasturlar tizimga kirib, ma'lumotlarni o'g'irlash yoki tizimni buzish mumkin.

Ransomware: Zero-Day zaifliklari ransomware hujumlarida ham qo'llaniladi. Bu esa foydalanuvchilarning ma'lumotlarini bloklab, to'lov talab qilishga olib keladi.

3. Ma'lumotlarni O'g'irlash:

Ma'lumot Bazalariga Kirish: Zero-Day zaifliklari orqali ma'lumotlar bazasiga kirib, noqonuniy ravishda ma'lumotlarni o'g'irlash mumkin.

Shaxsiy Ma'lumotlarni O'g'irlash: Foydalanuvchilarning shaxsiy ma'lumotlari (parollar, bank ma'lumotlari) o'g'irlanishi mumkin.

2. Zero-Day Zaifliklari Qanday Qo'llaniladi?

Zero-Day zaifliklari kiberjinoyatchilikda turli usullar bilan qo'llaniladi. Quyida eng keng tarqalgan usullar keltirilgan:

1. Maqsadli Hujumlar (Targeted Attacks):

APT (Advanced Persistent Threat): Zero-Day zaifliklari APT hujumlarida ko'p qo'llaniladi. Bu hujumlar ma'lum bir tashkilotga qaratilgan bo'lib, uzoq vaqt davomida amalga oshiriladi.

Davlatlararo Kiberhujumlar: Zero-Day zaifliklari davlatlar o'rtasidagi kiberhujumlarda qo'llaniladi. Masalan, Stuxnet virusi (2010) Iranning yadroviy dasturiga hujum qilgan.

2. Malware Tarqatish:

Zararli Dasturlar (Malware): Zero-Day zaifliklari orqali zararli dasturlar tizimga kirib, ma'lumotlarni o'g'irlash yoki tizimni buzish mumkin.

Ransomware: Zero-Day zaifliklari ransomware hujumlarida ham qo'llaniladi. Bu esa foydalanuvchilarning ma'lumotlarini bloklab, to'lov talab qilishga olib keladi.

3. Ma'lumotlarni O'g'irlash:

Ma'lumot Bazalariga Kirish: Zero-Day zaifliklari orqali ma'lumotlar bazasiga kirib, noqonuniy ravishda ma'lumotlarni o'g'irlash mumkin.

Shaxsiy Ma'lumotlarni O'g'irlash: Foydalanuvchilarning shaxsiy ma'lumotlari (parollar, bank ma'lumotlari) o'g'irlanishi mumkin.

3. Zero-Day Hujumlarini Aniqlash va Ularga Qarshi Kurashishning Ilg'or Usullari

Zero-Day hujumlarini aniqlash va ularga qarshi kurashish juda murakkab jarayon bo'lib, ilg'or texnologiyalar va yondashuvlarni talab qiladi. Quyida batafsil usullar keltirilgan:

1. Xulq-atvor Analizi (Behavioral Analysis):

Normal va G'ayritabiiy Faoliyatni Aniqlash: Tizimdagi normal va g'ayritabiiy faoliyatni aniqlash orqali Zero-Day hujumlarini aniqlash.

Misollar: Tizimda kutilmagan fayllar yoki jarayonlar paydo bo'lsa, ularni tekshirish.

2. Sandbox Texnologiyasi:

Shubhali Dasturlarni Izolyatsiya Qilish: Shubhali dasturlarni izolyatsiya qilingan muhitda (sandbox) ishga tushirib, ularning xatti-harakatlarini kuzatish.

Misollar: Zero-Day zararli dasturlarni aniqlash va ularning ta'sirini kamaytirish.

3. Yorliqlar va Imzolar (Signatures and Heuristics):

Zararli Dasturlarning Imzolarini Aniqlash: Ma'lum zararli dasturlarning imzolarini aniqlash orqali Zero-Day hujumlarini oldini olish.

Heuristik Analiz: Yangi va noma'lum zararli dasturlarni aniqlash uchun heuristik analizdan foydalanish.

4. Sun'iy Intellekt va Mashina O'rganish:

AI va ML Texnologiyalari: Sun'iy intellekt (AI) va mashina o'rganish (ML) texnologiyalari yordamida kiberhujumlarning oldindan bashorat qilinishi va aniqlanishi.

Misollar: Tizimdagi g'ayritabiiy faoliyatni avtomatik ravishda aniqlash.

5. Tezkor Tuzatish (Patch Management):

Zaifliklarni Tezda Tuzatish: Zero-Day zaifliklari aniqlangach, ularni tezda tuzatish (patch) uchun protseduralarni joriy etish.

Muntazam Yangilanishlar: Tizimlarni muntazam ravishda yangilash va xavfsizlik yangilanishlarini o'tkazish.

6. Kiberxavfsizlik Monitoringi:

SIEM Tizimlari: SIEM (Security Information and Event Management) tizimlari orqali real vaqtda kiberhujumlarni aniqlash.

Doimiy Kuzatuv: Tizimlarni doimiy ravishda kuzatib borish va shubhali faoliyatni aniqlash.

7. Hujumlarni Simulyatsiya Qilish (Red Teaming):

Zaifliklarni Aniqlash: Tizimlarning zaif tomonlarini aniqlash uchun hujumlarni simulyatsiya qilish.

Misollar: Zero-Day zaifliklarini oldindan aniqlash va bartaraf etish.

4. Zero-Day Zaifliklarini Oldini Olish Uchun Proaktiv Chora-Tadbirlar

Zero-Day zaifliklarini oldini olish uchun proaktiv chora-tadbirlar ko'rish juda muhim. Quyida batafsil chora-tadbirlar keltirilgan:

1. Xavfsizlikni Dastlabki Bosqichda Kiritish (Security by Design):

Dasturiy Ta'minotni Xavfsiz Ishlab Chiqish: Dasturiy ta'minot yoki tizimlarni ishlab chiqish jarayonida xavfsizlikni asosiy qism sifatida ko'rib chiqish.

Xavfsizlikni Tekshirish: Muntazam ravishda xavfsizlikni tekshirish va zaifliklarni aniqlash uchun auditlar o'tkazish.

2. Zaifliklarni Faol Qidirish (Vulnerability Hunting):

Zaifliklarni Aniqlash: Tizimlarda mavjud bo'lishi mumkin bo'lgan zaifliklarni faol ravishda qidirish va ularni oldindan bartaraf etish.

Bug Bounty Dasturlari: Tashqi mutaxassislardan yordam olish uchun Bug Bounty dasturlarini joriy etish.

3. Xalqaro Hamkorlik va Ma'lumot Almashish:

Ma'lumot Almashish Platformalari: Zero-Day zaifliklari haqida ma'lumot almashish uchun xalqaro hamkorlikni rivojlantirish.

Kiberxavfsizlik Tashkilotlari: Kiberxavfsizlik tashkilotlari va davlatlar o'rtasida ma'lumot almashish platformalari yaratish.

4. Foydalanuvchi Xabardorligini Oshirish:

Ogohlantirish va O'qitish: Foydalanuvchilarni Zero-Day hujumlari haqida ogohlantirish va ularni xavfsizlik choralarini ko'rishga undash.

Phishing Hujumlariga Qarshi Kurashish: Phishing hujumlari va boshqa kiberjinoyatchilik usullari haqida o'qitish.

5. Kiberxavfsizlik Strategiyasini Ishlab Chiqish:

Keng Qamrovli Strategiya: Zero-Day hujumlariga qarshi kurashish uchun keng qamrovli kiberxavfsizlik strategiyasini ishlab chiqish.

Muntazam Yangilanishlar: Tizimlarni muntazam ravishda yangilash, zaifliklarni tekshirish va hujumlarni simulyatsiya qilish.

5. Zero-Day Zaifliklarini Oldini Olishda Kelajakdagi Texnologiyalar:(1-rasm

(1-rasm).

Zero-Day zaifliklarini oldini olishda kelajakda quyidagi texnologiyalar muhim rol o'ynashi kutilmoqda:

1. Kvant Kriptografiyasi:

Kvant Shifrlash: Kvant kompyuterlari yordamida shifrlash usullarini yanada xavfsizroq qilish.

Kvant Xavfsizlik Algoritmlari: Zero-Day hujumlariga qarshi kurashish uchun kvant xavfsizlik algoritmlarini ishlab chiqish.

2. Sun'iy Intellektning Rivojlanishi:

AI va ML Texnologiyalari: Sun'iy intellekt va mashina o'rganish texnologiyalarini yanada rivojlantirish orqali Zero-Day hujumlarini aniqlash va bartaraf etish.

Avtomatik Tizimlar: Kiberhujumlarni avtomatik ravishda aniqlash va bartaraf etish tizimlarini yaratish.

3. Blockchain Texnologiyasi:

Ma'lumotlarni Himoya Qilish: Blockchain texnologiyasi yordamida ma'lumotlarni himoya qilish va kiberhujumlarni oldini olish.

Decentralized Xavfsizlik: Markazlashtirilmagan xavfsizlik tizimlarini yaratish.

XULOSA

Zero-Day zaifliklari kiberxavfsizlik sohasidagi eng murakkab muammolardan biridir. Ularni oldini olish uchun proaktiv chora-tadbirlar, ilg'or texnologiyalar va xalqaro hamkorlik zarur. AI, mashina o'rganish, sandbox texnologiyasi kabi yondashuvlar Zero-Day hujumlarini aniqlash va bartaraf etishda muhim rol o'ynaydi. Shuningdek, foydalanuvchi xabardorligini oshirish va kiberxavfsizlik strategiyasini ishlab chiqish ham juda muhimdir.

FOYDALANILGAN ADABIYOTLAR:

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
2. Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice. Pearson.
3. Kaspersky Lab. (2021). Zero-Day Exploits: The Invisible Threat.
4. Symantec. (2022). Internet Security Threat Report.
5. MITRE Corporation. (2023). CVE (Common Vulnerabilities and Exposures) Database.
6. Shostack, A. (2014). Threat Modeling: Designing for Security. Wiley.
7. NIST. (2020). National Vulnerability Database (NVD).
8. Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group.