SUN'IY INTELLEKT VOSITALARIDAN NOTO'G'RI FOYDALANISH: AI VIRUSLAR VA BOTNETLAR XAVFI

Eshmurodov Mas'udjon Xikmatillayevich
Samarqand davlat arxitektura-qurilish universiteti, 140147, Samarqand, Uzbekistan.
ORCID ID: https://orcid.org/0009-0005-0667-8116
Eshmurodov.masudjon@samdaqu.edu.uz
https://doi.org/10.5281/zenodo.17559689

Annotatsiya. *Ushbu maqolada sun'iy intellekt (SI) texnologiyalarining noto'g'ri, zararli yoki qonunsiz maqsadlarda qo'llanilishi natijasida yuzaga kelayotgan yangi tahdidlar, xususan, AI asosidagi viruslar va botnetlar (AI-botnetlar) tahlil qilinadi. Maqola tahdidning texnik mohiyati, tarqalish mexanizmlari, aniqlash va profilaktika choralarini, shuningdek, huquqiy, axloqiy va siyosiy oqibatlarni o'rganadi. Yakuniy qismda amaliy tavsiyalar va kelgusidagi tadqiqot yo'nalishlari keltiriladi.*

Kalit so'zlar: *sun'iy intellekt, AI virus, botnet, AI-botnet, kiberxavfsizlik, tahdidlarni aniqlash, mitigatsiya, etik qonunchilik.*

MISUSE OF ARTIFICIAL INTELLIGENCE TOOLS: THE DANGER OF AI VIRUSES AND BOTNETS

Abstract. *This article analyzes emerging threats resulting from the misuse, malicious, or illegal application of artificial intelligence (AI) technologies, particularly AI-based viruses and botnets (AI-botnets). The paper explores the technical nature of these threats, their propagation mechanisms, detection and prevention measures, as well as their legal, ethical, and political implications. In conclusion, practical recommendations and potential future research directions are provided.*

Keywords: *artificial intelligence, AI virus, botnet, AI-botnet, cybersecurity, threat detection, mitigation, ethical legislation.*

НЕПРАВОМЕРНОЕ ИСПОЛЬЗОВАНИЕ ИНСТРУМЕНТОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ОПАСНОСТЬ ВИРУСОВ И БОТНЕТОВ НА ОСНОВЕ ИИ

Аннотация. *В данной статье анализируются новые угрозы, возникающие в результате неправомерного, вредоносного или незаконного использования технологий искусственного интеллекта (ИИ), в частности, вирусов и ботнетов на основе ИИ (ИИ-ботнетов). В статье рассматриваются техническая природа угрозы, механизмы её распространения, меры обнаружения и предотвращения, а также правовые, этические и политические последствия. В заключительном разделе представлены практические рекомендации и направления дальнейших исследований.*

Ключевые слова: *искусственный интеллект, вирус ИИ, ботнет, ИИ-ботнет, кибербезопасность, обнаружение угроз, минимизация, этическое законодательство.*

1. Kirish

Oxirgi yillarda SI texnologiyalarining tez sur'atda rivojlanishi kiberxavfsizlik sohasida ham yangi imkoniyatlar, ham yangi xavflarni keltirib chiqardi. SI hujumlarni avtonom tarzda tashkil etishi, o'zini moslashtira olishi va inson tomonidan aniqlashdan qochishi mumkin — bu esa an'anaviy kiberxavfsizlik modellarini qayta ko'rib chiqishni talab qiladi.

Maqola maqsadi — AI bilan qo'zg'atilgan viruslar va botnetlarning xususiyatlarini keng qamrovda yoritish va amaliy javob choralarini taklif qilish.

2. Adabiyotlar va ilgari olingan natijalar (Literature review)

Bu bo‘limda so‘nggi tadqiqotlar, sanoat hisobotlari va hukumat tavsiyalari sharhlanadi.

SI modellarining zararli foydalanilishi haqidagi adabiyotlar ikki asosiy yo‘nalishni ko‘rsatadi: 1) asosan axborot chiqarish (data exfiltration), dasturiy ta’minotga zarar yetkazish va ijtimoiy muhitni manipulyatsiya qilish uchun ishlatiladigan adversarial hamda generativ usullar; 2) mavjud botnet arxitekturalariga SI xususiyatlarini qo‘shish – hujumlarni dinamik ravishda boshqarish, yashirin kommunikatsiyani optimallashtirish va o‘z-o‘zini tiklash imkoniyatlari.

Eslatma: Bu bo‘limda foydalanilgan manbalar ro‘yxati maqolaning oxirida ko‘rsatildi.

3. AI viruslar va AI-botnetlar: texnik ta’rif va xususiyatlar

3.1. AI virus — ta’rif

AI virus — bu SI texnologiyalari yordamida tayyorlangan yoki boshqariladigan zararli dastur bo‘lib, o‘zini moslashtirish, maqsadga yo‘naltirish, xulq-atvorini yashirish va aniqlovchi mexanizmlardan qochish qobiliyatiga ega.

3.2. AI-botnet — ta’rif

AI-botnet — ko‘p sonli qurilmalar (kompyuterlar, IoT qurilmalari va boshqalar)dan tashkil topgan tarmoq bo‘lib, ularning ishini markaziy yoki tarqatilgan AI boshqaruv modeli boshqaradi. AI-botnetlar o‘zini optimallashtiruvchi hujum strategiyalarini ishlab chiqishi, komandalarni sath va vaqtga mos ravishda dinamik tarqatishi va qiyin aniqlanadigan trafik xususiyatlarini hosil qilishi mumkin.

3.3. Xususiyatlar va farqlash

- **Avtonomiya:** hujum jarayonining ko‘p qismi avtomatlashtirilgan.
- **Moslashuvchanlik:** real vaqt ma’lumotlariga qarab xatti-harakatni o‘zgartiradi.
- **Qat’iy yashirinlik:** anomaly detection tizimlaridan qochish uchun adversarial texnikalar.
- **O‘rganish qobiliyati:** ilgari qilingan hujumlar asosida strategiyasini yaxshilaydi.

4. Noto‘g‘ri foydalanish ssenariylari

4.1. Avtomatlashtirilgan phishing va ijtimoiy muhandislik

Generativ modellar yordamida yuqori sifatli, shaxsiylashtirilgan phishing xabarlar va ovozli xabarlar yaratish.

4.2. Mavjud xavfsizlik vositalarini hushyor qiluvchi hujumlar

Anomaly detection va SI asosidagi himoya tizimlarini aldash uchun adversarial namunalar yaratish.

4.3. IoT va sanoat tizimlariga hujumlar

Kuchsiz IoT qurilmalarini AI-botnetlarga jalb qilish orqali DDoS hujumlarini yanada samarali qilish.

4.4. Avtonom zararli kodning evolyutsiyasi

Kod fragmentlarini genetik algoritmlar yoki RL (Reinforcement Learning) yordamida o‘zgartirib, analog antiviruslardan yashinish va yangi zaifliklardan foydalanish.

4.5. Keng ko‘lamli desinformatsiya kampaniyalari

AI yordamida generatsiyalangan multimodal (matn, rasm, audio, video) kontent orqali siyosiy va ijtimoiy manipulyatsiya.

5. Aniqlash va monitoring usullari

5.1. Model-xususiyatga asoslangan monitoring

Tarmoq va tizim chaqiruvlarining (API chaqiriqlari, model inference loglari) xususiyatlariga e’tibor qaratish.

5.2. Anomaliya deteksiyasi va SI yordamida profil tuzish

AI yordamida normal xatti-harakat profillarini yaratib, ulardan chetga chiqishlarni aniqlash.

5.3. Adversarial hujumlarni aniqlash

Model inference jarayonida adversarial signallarni aniqlash va ularga qarshi qatlamlar (defensive distillation, input sanitization).

5.4. Sandboxing va dinamik tahlil

Shubhali kodni izolyatsiyalangan muhitda ishga tushirish va uning o‘zgaruvchan xatti-harakatlarini kuzatish.

6. Mitigatsiya va himoya choralari

6.1. Texnik chora-tadbirlar

- *Kuchsiz joylarni yangilash:* qurilmalar va dasturiy ta’minotni muntazam yangilash.
- *Model xavfsizligi:* modelning hujjatlangan va cheklangan API-lari, kirish cheklovlari (rate limiting), autentifikatsiya va authorization.
- *Input validatsiyasi va sanitatsiyasi:* modelga yuborilayotgan ma’lumotlarni filtrdan o‘tkazish.
- *Adversarial training:* modelni potentsial hujum namunalariga nisbatan mustahkamlash.
- *Monitoring va loglarni markazlashgan tahlil qilish.*

6.2. Tizimli va operatsion choralar

- *Zararlangan qurilmalarni tez izolyatsiyalash va karantin:* botnetning tarqalishiga yo‘l bermaslik.
- *Zaxira rejalar va tiklash (incident response) protokollari.*
- *Kiber-xavfsizlik xodimlarini doimiy ravishda qayta tayyorlash va treninglar.*

6.3. Sektor darajasidagi chora-tadbirlar

- *IoT yetkazib beruvchilari uchun xavfsizlik standartlari va sertifikatlash.*
- *ISP va bulut provayderlari bilan hamkorlik:* shubhali trafikni bloklash va tracing.

7. Huquqiy va axloqiy masalalar

7.1. Jinoyat va mas’uliyat

AI bilan yaratilgan zararli kod va u orqali sodir etilgan zararlarda kim javobgar bo‘lishi savoli murakkab — ishlab chiquvchi, model egasi yoki modelni ishlatgan foydalanuvchi?

Hodisalarning kontekstiga qarab, huquqiy normativlarni moslashtirish talab etiladi.

7.2. Axloqiy muammolar

AI vositalarining funktsiyalarini cheklash, mas’uliyatli tadqiqot prinsiplarini joriy etish va xavfsizlikni “by design” tamoyili bilan birlashtirish muhim.

7.3. Siyosat va xalqaro hamkorlik

AI-botnetlarga qarshi kurash xalqaro miqyosda hamkorlikni, razvedka va texnik almashishni talab qiladi. Milliy qonunchilik hamda xalqaro bitimlar muvofiqlashtirilishi lozim.

8. Amaliy tavsiyalar

1. **Korporativ siyosat:** SI modellari va ular orqali beriladigan xizmatlar uchun aniqlangan xavf baholash va foydalanish protokollari ishlab chiqilsin.
2. **Xavfsizlik sinovlari:** ishlab chiqilgan SI modellariga penetration testing va red-team mashqlari o‘tkazilsin.
3. **Kirish nazorati:** model inference va API chaqiriqlari uchun kuchli autentifikatsiya va cheklovlar joriy etilsin.
4. **Ma’lumotni himoya qilish:** trening ma’lumotlarining anonimligi va maxfiyligini ta’minlash.

5. **Monitoring va o‘z vaqtida javob:** loglarni markazlashtirish, anomaliya tizimlarini rivojlantirish va gatvolar (playbooks) tayyorlash.

6. **Xalqaro hamkorlik:** davlatlararo hamkorlik, standartlar va ko‘rsatmalarni ishlab chiqish.

9. Kelajakdagi tadqiqot yo‘nalishlari

- AI-botnet arxitekturalarining tarkibi va ularni aniqlash uchun yangi indikatorlar (IoC) ishlab chiqish.
- Avtonom zararli kodning o‘zini-o‘zi o‘qitish jarayonlarini modellashtirish va ularga qarshi strategiyalar.
- Generativ modellarning zararli foydalanishini oldini olish uchun watermarking, provenance va model-watermark texnologiyalarini takomillashtirish.

Foydalanilgan adabiyotlar

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
2. Brundage, M. et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.
3. Various industry whitepapers on AI security and adversarial ML.
4. NIST, ENISA va boshqa tashkilotlarning AI va kiberxavfsizlik bo‘yicha tavsiyalariga murojaat qilindi.
5. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
6. Eshmurodov M.X., Xaydarov J.K., Axmedova A.E.,Islamov K.S. Kiber tahdidlarni aniqlashda mashinaviy o‘rganish texnologiyalarining roli // *Modern Science and Research, 4(6), 574–577.*
7. Eshmurodov M.X., Shaimov K.M., Elmurodov B.E., G‘aybulov Q.M. Sun’iy intellekt yordamida kiberxavfsizlikni mustahkamlash: zamonaviy yondashuvlar va algoritmlar // *Modern Science and Research, 4(5), 1758–1761.*
8. M.X.Eshmurodov, I.S.Karimov, Q.M.Gaybulov, B.E.Elmurodov. SI asosida avtomatlashgan kiberhujumlar va ularga qarshi himoya usullari // NEW RENAISSANCE international scientific journal, Volume 2, Issue 6, 2025, ISSN: 3030-3753, 1225-1227 b.
9. M.X.Eshmurodov, K. M. Shaimov, Q.M.Gaybulov. One-dimensional elliptic equation solution using the straight-line method for heat transfer problems // NEW RENAISSANCE international scientific journal, Volume 2, Issue 4, 2025, ISSN: 3030-3753, 130-136 b.