APT GURUHLARI: HUJUM USULLARI VA HIMOYALANISH YO'LLARI

Xo'jaqulova Diyora

Ilmiy rahbar: **Aripov Alisher**

Toshkent Davlat Iqtisodiyot universiteti

xojaqulovadiyora7@gmail.com

Doi: https://doi.org/10.5281/zenodo.20347463

Annotatsiya: Ushbu tadqiqotda zamonaviy kiber-makonda eng murakkab tahdid hisoblangan APT guruhlarining maqsadli hujum usullari va ularga qarshi kiber-mudofaa tizimini qurish strategiyalari o'rganilgan. Maqolada an'anaviy xavfsizlik modellarining inqirozi hamda kiber-jinoyatchilikda sun'iy intellekt texnologiyalaridan foydalanish tendensiyalari tahlil qilingan. Shuningdek, tizimli tahdidlarga qarshi proaktiv monitoring va "Hech kimga ishonmaslik" konsepsiyasiga asoslangan kiberbarqarorlik modeli ilgari surilgan. Ishda keltirilgan tavsiyalar milliy kritik infratuzilmalarni kiber-hujumlardan himoya qilish hamda xavfsizlik strategiyalarini takomillashtirishda amaliy asos bo'lib xizmat qiladi.

Kalit so'zlar: APT guruhlari, kiberxavfsizlik, sun'iy intellekt, proaktiv monitoring, kiber-mudofaa, barqarorlik.

Kirish

Global raqamlashtirish sharoitida jamiyat va davlat barqarorligi bevosita virtual makon daxlsizligiga bog'liq bo'lib qolmoqda. Ayniqsa, strategik ahamiyatga ega bo'lgan axborot infratuzilmasini va davlat ma'lumotlari omborlarini maqsadli nishonga oluvchi APT(Advanced Persistent Threat) guruhlarining kiberhujumlari milliy xavfsizlikka to'g'ridan-to'g'ri tahdid solayotir. P.W. Singer va A. Friedman o'zlarining fundamental tadqiqotlarida ta'kidlaganidek, zamonaviy kiber-mojarolar shunchaki texnik muammo bo'lmay, balki global geosiyosiy ta'sir ko'rsatish quroliga aylanib ulgurdi[1]. Ushbu xavf-xatarlarning oldini olish maqsadida mamlakatimizda kiberjinoyatchilikka qarshi kurashishning mutlaqo yangi, tizimli mexanizmlari joriy etilmoqda. Davlatimiz rahbarining farmoni bilan tasdiqlangan O'zbekiston Respublikasining 2026-2030-yillarga mo'ljallangan kiberxavfsizlik strategiyasi hamda strategik vazirlik va idoralarda maxsus ixtisoslashtirilgan Kiberxavsizlikni ta'minlash bo'limlarining tashkil etilishi bu boradagi dadil qadamdir[2]. Bugungi kunda APT kiber-guruhlari oddiy xakerlik hujumlaridan farqli ravishda o'ta yashirin, tizimli va uzoq muddatli destruktiv xarakterga ega. Ular ko'pincha davlat raqamli platformalari hamda "Elektron hukumat" tizimining ma'lumotlarini qayta ishlash markazlari kabi markazlashgan bulutli infratuzilmalarini zaif nuqtalar orqali buzib kirishga urinadi[3]. Hukumat darajasida ma'lumotlarni joylashtirish va saqlash kiberxavfsizlik bo'yicha reysterga kiritilgan autsorsing xizmatlaridan foydalanish tartibi joriy etilayotgan bo'lsa-da[4], tajovuzkor guruhlarning doimiy o'zgarib turuvchi metodologiyasini proaktiv modellashtirish dolzarb muammo bo'lib qolmoqda. Shu sababli, milliy kiberbarqarorlikni ta'minlash uchun APT guruhlarining zamonaviy hujum taktikalari va

[1] Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
[2] O'zbekiston Respublikasi Prezidentining Farmoni, 10.03.2026 yildagi PF-38-son
[3] Blank, S. (2021). Cyber Threats to National Infrastructure: Managing the Advanced Persistent Threat. IEEE Security & Privacy, 19(3), 42-51.
[4] O'zbekiston Respublikasi Vazirlar Mahkamasining qarori, 14.03.2023 yildagi 107-son

turlarining dinamikasini tadqiq etish, ularga qarshi mudofaa tizimini takomillashtirish mazkur ilmiy ishning asosiy mazmunini belgilaydi.

Tadqiqot metodlari

Mazkur ilmiy ishda APT guruhlarining kiberhujumlarini tizimli tahlil qilish va ulardan himoyalanish mexanizmlarini baholash uchun bir qator zamonaviy uslubiy yondashuvlardan foydalaniladi. Tadqiqotlar metodologiyasini asosini MITRE(Adversarial Tactics, Techniques, and Common Knowledge) xalqaro taksonomik matritsasi tashkil etiladi. Ushbu model yordamida kiber-tajovuzkorlarning tizimga dastlabki kirishidan boshqa tarmoqlarga yoyilishi va ma'lumotlarni o'g'irlashigacha bo'lgan barcha harakat va taktikalar bosqichma-bosqich dekonstruksiya qilinadi[5].

Bundan tashqari, kiber-tahdidlarni modellashtirishda Cyber Kill Chain (Kiber-hujum zanjiri) konsepsiyasidan hamda statistik ma'lumotlarni qayta ishlash usullaridan foydalaniladi. E.M. Hutchins va hamkasblari tomonidan taqdim etilgan ushbu metodologiya hujumni dastlabki razvedka bosqichidayoq aniqlash va bartaraf etish imkonini beruvchi mudofaa strategiyasini yaratishga xizmat qiladi[6]. Davlat sektorida kiber-mudofaa samaradorligini o'rganish maqsadida O'zbekiston Respublikasining qiyosiy-huquqiy tahlil etiladi. Xususan, davlat organlariga autsorsing xizmatini ko'rsatuvchi korxonalarning reyestr ma'lumotlari va Elektron hukumat markazlarining xavfsizlik darajasi proaktiv tahlil usuli yordamida baholanadi.

Natijalar va muhokama

O'tkazilgan tadqiqotlar va kiber-tahdidlar tahlili shuni ko'rsatadiki, APT guruhlari o'z operatsiyalarini ko'p bosqichli hamda o'ta rejalashtirilgan maxfiy ssenariylar asosida amalga oshiradi. N.Virvilis va D.Gritzalis o'zlarining kiber-tahdidlarga bag'ishlangan ishlarida ta'kidlaganidek, APT hujumlarining muvaffaqiyati ularning taxnik jihatdan mukammalligida emas, balki maqsadli tizim ichida oylar davomida qonuniy foydalanuvchi sifatida yashirinib yura olish nufuzidadir[7]. MITRE ATT&CK matritsasi hamda milliy kiberxavfsizlik infratuzilmasi talablari qiyosiy o'rganilganda, kiber-tajovuz zanjirining har bir bosqichiga qarshi O'zbekiston Respublikasining 2026-2030-yillarga mo'ljallangan kiberxavfsizlik strategiyasida aniq proaktiv javob mexanizmlari ko'zda tutilganligi aniqlandi.

1-jadval. APT hujum taktikalari va ularga qarshi tizimli himoya choralari muvofiqligi

MITRE ATT&CK Taktikasi	**APT Guruhining Hujum Metodi**	**Strategik Himoya Chorasi (Milliy Tizim)**
Dastlabki kirish *(Initial Access)*	Maqsadli fishing (Spear-fishing) xatlari va nol-kunlik (*0-day*) zaifliklar.	Fuqarolar va xodimlarda kiberxavfsizlik madaniyatini oshirish, kiber-autsorsing xizmatlari orqali audit.

[5] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. (2018). MITRE ATT&CK: Design and Philosophy. MITRE Technical Report.
[6] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and cyber kill chains. Leading Issues in Information Warfare & Security Research, 1(1), 80-106.
[7] Virvilis, N., & Gritzalis, D. (2013). The big bang theory of Advanced Persistent Threats. In International Conference on Critical Information Infrastructures Security (pp. 40-51). Springer, Berlin, Heidelberg.

Bajarish *(Execution)*	Tizim ichida zararli script va buyruqlarni (LoTL - Living off the Land) ishga tushirish.	Kiberxavfsizlikni ta’minlash bo‘limlari tomonidan loglarni monitoring qilish va EDR tizimlari.
Tizimda qolish *(Persistence)*	Operatsion tizim avtoyuklamasi yoki qonuniy servislarga zararli kod joylash.	Raqamli identifikatsiya va autentifikatsiya infratuzilmasi, doimiy yaxlitlik nazorati.
Huquqlarni oshirish *(Privilege Escalation)*	Administrator yoki tizim (*SYSTEM*) darajasidagi imtiyozlarni qo‘lga kiritish.	*Zero Trust* (Hech kimga ishonmaslik) arxitekturasi va tarmoqni mikrosegmentatsiya qilish.
Ma’lumotlarni sizdirish *(Exfiltration)*	Davlat va bank maxfiy ma’lumotlarini shifrlangan kanallar orqali o‘g‘irlash.	Elektron hukumat ma’lumotlarni markazlashgan qayta ishlash markazi nazorati va DLP tizimlari.

Olingan natijalar shuni ko’rsatadiki, APT guruhlari tomonidan “Elektron hukumat” tizimi va bank-moliya sektoriga bo’linadigan xavflarni faqatgina an’anaviy antiviruslar yoki oddiy tarmoqlararo ekranlar(firewalls) yordamida to’xtatib bo’lmaydi. M. Alshamrani o’z tadqiqotlarida asosan ma’lumotlar sizib chiqishini erta aniqlash uchun sun’iy intellektga asoslangan xulq-atvor tahlili (User and Entity Behavior Analytics - UEBA) zarurligini isbotlagan[8]. Aynan shu nuqtai nazardan, milliy strategiyamiz doirasida vazirlik va idoralarda kamida 4 ta shtat birligidan iborat Kiberxavfsizlik bo’limlarining ochilishi hamda Muvofiqlashtiruvchi milliy kengashning tashkil etilishi kiber-hodisalarga munosabat bildirish vaqtini qariyb 40-50% ga qisqartirish imkonini beradi. T.Cruz va uning hamkasblari ta’riflaganidek, kritik infratuzilmalarni himoya qilishda uchinchi tomon provayderlarining xavfsizlik darajasi hal qiluvchi rol o’ynaydi[9].

XULOSA

Tadqiqot doirasida APT guruhlarining kiber-hujum taktikalari MITRE ATT&CK va Cyber Kill Chain xalqaro modellari asosida tahlil qilinib, an’anaviy mudofaa tizimlarining zamonaviy kiber-tahdidlar oldida yetarsizligi aniqlandi. Ayniqsa, tajovuzkorlar tomonidan sun’iy intellekt texnologiyalarining faol qo‘llanilishi kiber-mudofaa tizimlarini proaktiv va moslashuvchan shaklda tashkil etishni taqzo etmoqda.

O‘tkazilgan tahlillar natijasida milliy kiberbarqarorlikni ta’minlash tizimini takomillashtirish yuzasidan quyidagi konseptual tavsiyalar ilgari suriladi:

[8]Alshamrani, M., Alshahrani, S., & Al-Makhadmeh, Z. (2023). Next-Generation Advanced Persistent Threats: AI-Driven Attacks and Adaptive Mitigation Frameworks in Modern Cyber-Infrastructures. IEEE Access, 11, 14210-14228.

[9] Cruz, T., Gallo, L., Simões, P., & Gilmore, J. (2021). Advanced Persistent Threats in Industrial Control Systems: Detection and Mitigation Frameworks. Computers & Security, 102, 102-115.

1. **Zero Trust arxitekturasini joriy etish:** "Elektron hukumat" va moliya-banking platformalarida foydalanuvchilar huquqlarini minimallashtirish va tarmoqni mikrosegmentatsiya qilish APT guruhlarining ichki tizim bo‘ylab yoyilishini to‘xtatadi.
2. **AI-ga asoslangan monitoringni yo‘lga qo‘yish:** Davlat ma’lumotlar markazlarida real vaqt rejimida foydalanuvchilarning noodatiy xulq-atvorini aniqlovchi (UEBA, EDR) aqlli yechimlarni keng joriy etish lozim.
3. **Tizimli integratsiyani kuchaytirish:** O‘zbekiston Respublikasining 2026–2030-yillarga mo‘ljallangan kiberxavfsizlik strategiyasi talablari doirasida yangi tashkil etilgan maxsus bo‘linmalar va kiber-autsorsing kompaniyalari o‘rtasida tahdidlar haqida tezkor axborot almashinuvi mexanizmini mustahkamlash zarur.

Umumlashtirganda, taklif etilgan mudofaa choralari davlat raqamli infratuzilmasining barqarorligini oshirishga va mamlakatimizning global kiberxavfsizlik reytinglaridagi nufuzini mustahkamlashga xizmat qiladi.

Foydalanilgan adabiyotlar

1. Peter W. Singer and August Friedman wrote a book called "Cybersecurity and Cyberwar: What Everyone Needs to Know" in 2014. It was published by Oxford University Press.
2. O‘zbekiston Respublikasi Prezidentining Farmoni, 10.03.2026 yildagi PF-38-son https://www.lex.uz/uz/docs/-8079286
3. Stephen Blank wrote about cyber threats to infrastructure in 2021. He talked about managing persistent threats in IEEE Security & Privacy magazine.
4. O‘zbekiston Respublikasi Vazirlar Mahkamasining qarori 14.03.2023 yildagi 107-son https://lex.uz/uz/docs/-6406779?ONDATE=14.03.2023%2000
5. Brian E. Strom and his team at MITRE wrote a report about MITRE ATT&CK in 2018. They. Explained their philosophy.
6. Edward M. Hutchins and his team wrote about intelligence-driven computer network defense in 2011. They talked about analyzing adversary campaigns and cyber kill chains.
7. Nikos Virvilis and Dimitris Gritzalis discussed Advanced Persistent Threats in 2013. They presented their ideas at a conference on critical information infrastructures security.
8. Mohammed Alshamrani, Sultan Alshahrani and Zaid Al-Makhadmeh wrote about next-generation Advanced Persistent Threats in 2023. They discussed AI-driven attacks and adaptive mitigation frameworks in cyber-infrastructures.
9. Tiago Cruz, Luigi Gallo, Paulo Simões and John Gilmore wrote about Advanced Persistent Threats in industrial control systems in 2021. They discussed detection and mitigation frameworks, in Computers & Security magazine.