

Абайлаңыз, цифрлық алдау: алаяқтар жасанды интеллекттің мүмкіндіктерін қалай пайдаланады

Осыдан бірнеше жыл бұрын жасанды интеллект алыс болашақтың үрдісі болып көрінген. Бүгінгі күні ол бізге мәтін жазуға, бейнелер жасауға, құжаттар аударуға және ақпарат іздеуге көмектеседі. Алайда, өмірімізге жаңа технологиялардың енуімен қатар, олардың мүмкіндіктерін тек әзірлеушілер мен бизнес қана емес, алаяқтар да пайдалануға тырысады.

ChatGPT-ға сену алаяқтардың мүддесіне қызмет еткен кезде

Егер бұрын қаскүнемдер адамды сендіретін хаттар дайындау, жалған сайттар жасау немесе телефон соққан кезде түрлі «аңыз» әңгімелер таңдауға апта бойы уақыттарын жұмсаса, ендігі жерде бұл міндеттердің көбін нейрожелілердің көмегімен бірнеше минуттың ішінде шешуге болады. Нәтижесінде алдау схемалары сенімді бола түседі, ал оларды тану күннен күнге қиындай түседі.

Киберқауіпсіздік мамандарының жақында анықтаған оқиғасы қылмыскерлердің қаншалықты айлакеш бола алатындарын көрсетеді. Push Security зерттеушілері зиянды бағдарламалық қамтылым таратудың жаңа схемасын тапты. Қаскүнемдер ChatGPT-дің ортақ сілтемелер функциясын пайдаланып, сервис жұмысында орын алған ақаулықтар туралы хабарламалары бар жалған беттерді орналастыра бастады. Пайдаланушы ChatGPT-дің таныс доменін көріп, ештеңеден күдіктенбеген. Содан кейін оған проблеманы шешу үшін «OpenAI ресми қосымшасын» көшіріп алу ұсынады. Іс жүзінде бағдарлама ретінде зиянды бағдарламалық қамтылым таратылған.

Схема қарапайым психологиялық тетікке негізделген. Адамдардың басым көпшілігі белгілі сервистерді қауіпсіз деп есептейді. Адам таныс логотипті немесе сайттың мекенжайын көргенде, оның қырағылығы төмендейді. Алаяқтар осыны пайдаланды.

Мұндай шабуылдар сервистің өзін бұзуды талап етпейтінімен қауіпті. Алаяқтар пайдаланушылардың танымал брендке деген сенімін пайдаланып, оны әлеуметтік инженерия құралына айналдырады.

Бастық жалған болып шықты...

Жасанды интеллекттің көмегімен белсенді дамып келе жатқан тағы бір бағыт — жалған дауыстар немесе бейнелер (дипфейк) жасау. Бүгінгі күні қаскүнемдерге жасанды интеллект арқылы адамның цифрлық көшірмесін жасау үшін ашық дереккөздерден бірнеше аудио- немесе бейнежазбалардың болғаны жеткілікті. Мұндай технологиялар алаяқтық қоңыраулар мен бейне хабарламаларды барынша шынайы ете отырып, дауысты, бет әлпетті және қарым-қатынас әдісін қолдан жасауға мүмкіндік береді.

Осындай схемалар қазірдің өзінде бүкіл әлем бойынша компаниялардың миллиондаған шығындарының себебіне айналды. Жасанды интеллект технологияларын қолдана отырып, алаяқтар басшының дауысы мен сыртқы келбетінің цифрлық көшірмесін жасайды, содан кейін қаржы бөлімшелерінің қызметкерлеріне телефон немесе бейнебайланыс арқылы хабарласады. Шұғыл мәселе деген сылтаумен олар ақша аударуды, шот төлеуді немесе басқа қаржылық операция жасауды сұрайды. Мұндай жалған хабарламалардың жоғары шынайылығының арқасында алаяқтық қоңыраулар мен бейнехабарламалар тіпті тәжірибелі мамандардың өзінде күдік туғызбауы мүмкін.

Қарапайым азаматтар үшін тәуекелдер ең алдымен туыстарының, достарының немесе таныстарының дауысы мен бейнесін қолданумен байланысты. Алаяқтар бейнеқоңырауды немесе дауыстық хабарламаны қолдан жасап, орын алған апат, құқық қорғау органдарына ұсталуды, денсаулығына байланысты проблемалар немесе шұғыл қаржылық көмекті қажет ететін басқа да төтенше жағдай туралы хабарлауы мүмкін.

Сарапшылар заманауи технологиялар барған сайын шынайы аудио және бейнехабарларды жасауға мүмкіндік беретінін атап өтеді. Нәтижесінде жалған дауысты немесе бейнені тану қиындай түседі. Сонымен қатар, бірқатар зерттеулердің нәтижелері адамдардың жинақталып жасалған материалдарды шынайы материалдардан ажыратуға тырысқанда жиі қателесетінін көрсетіп отыр.

Ешқашан болмаған әңгімелесу

Еңбек нарығы да қиын жағдайға тап болды.

Соңғы жылдары киберқауіпсіздік мамандары жасанды интеллект арқылы құрылған алаяқтық бос жұмыс орындарының өсуін тіркеп отыр. Нейрожелілер лауазымдардың шынайы сипаттамаларын, компаниялардың сайттарын және рекрутерлер атынан хат алмасуды жылдам жасауға мүмкіндік береді. Ізденушіге онлайн-әңгімелесуден өту, сауалнамалар толтыру немесе қашықтан жұмыс істеуге арналған бағдарламалық қамтылымды орнату ұсынылады. Нәтижесінде алаяқтар дербес деректерді алады немесе жәбірленушінің құрылғысын зиянды бағдарламалармен жұқтырады.

Кейде схема одан да күрделі болады. Жұмыс берушілердің атын жамылып, қылмыскерлер бірқатар әңгімелесу жүргізеді, үміткердің түйіндемесін зерделеп, сенімді қарым-қатынас орнатады. Осыдан кейін ғана оған тест тапсырмасына немесе зиянды болып табылатын арнайы бағдарламаға сілтеме жібереді.

Қайшылықты жағдай, бірақ жасанды интеллект басқа жағынан да қолданылады. Кейбір алаяқтар компанияға жұмысқа орналасу үшін толығымен ойдан шығарылған үміткерлерді жасайды. Олар фотосуреттерді, түйіндемелерді жасайды және дипфейктер арқылы бейне-әңгімелесуге қатысады. Олардың мақсаты корпоративтік жүйелер мен деректерге қол жеткізу болуы мүмкін.

Неліктен жасанды интеллект алаяқтарды қауіпті етеді

Қылмыскерлер үшін жасанды интеллекттің басты артықшылығы – ауқымының кеңдігі. Егер бұрын алаяқ күніне ондаған хат дайындай алатын болса, қазір нейрожелі бірнеше минут ішінде мыңдаған жеке хабарламалар жасай алады. Егер бұрын жалған мәтіндерде қателер көп болса, бүгінде олар мінсіз көрінеді. Егер бұрын дауысты қолдан жасау күрделі жабдықты қажет етсе, енді мұндай сервистер қолжетімді және арзанырақ болуда.

Жылдамдық ерекше қауіп төндіреді. Егер бұрын алаяқтық науқан бірнеше аптада дайындалса, қазір қаскүнемдер атышулы оқиғаларға дереу ден қояды. Танымал сервисте іркіліс болды, жаңа төлемдер туралы жаңалық пайда болды, банк қағидалары өзгерді – бірнеше сағаттан кейін жасанды интеллектінің көмегімен құрылған ондаған жалған сайттар, хабарлар мен жарнама сипатындағы хабарландырулар пайда болуы мүмкін.

Шын мәнінде ЖИ алаяқтық әрекетке кіру шегін төмендетеді. Ауқымды схеманы іске қосу үшін бағдарламалау, дизайн немесе копирайтинг саласындағы терең білімнің болуы міндетті емес. Көптеген тапсырмалар автоматтандырылады, яғни алаяқтық операциялар қаскүнемдердің кең ауқымы үшін арзанырақ, жылдамырақ және қолжетімді болады.

Сондықтан киберқауіпсіздік жөніндегі мамандар шабуылдың негізгі объектісі компьютер немесе смартфон емес, адам екендігі туралы жиі айтады. Жасанды интеллект алаяқтарға бұрынғыдан да сенімді сценарийлер жасауға көмектеседі, алайда сілтеме арқылы өтуге, бағдарламаны орнатуға немесе ақша аударуға қатысты түпкілікті шешімді әлі де пайдаланушы қабылдайды. Сол үшін орынды пайымдау мен цифрлық сауаттылық ЖИ-дің қарқынды даму дәуірінде де ең сенімді қорғаныс болып қала береді.

ЖИ негізіндегі сервистерді қалай қауіпсіз пайдалануға болады?

Негізінде, жасанды интеллект қауіпті емес. Көптеген тәуекел алаяқтар адамдардың жаңа технологияларға деген сенімін пайдаланатын уақытта туындайды. Сондықтан ЖИ сервистерімен жұмыс істеген кезде бірнеше қарапайым қағидалы сақтаған жөн: қосымшаларды әзірлеушілердің ресми сайттарынан және қосымшалардың ресми дүкендерінен ғана жүктеңіз; сервистердің таныс атаулары көрсетілген жағдайдың өзінде күдікті сілтемелерге өтпеңіз; дереккөзі аз ғана күмән тудырған жағдайдың өзінде бағдарламаларды орнатпаңыз; шұғыл проблемалар, бұғаттау немесе шұғыл әрекет ету қажеттілігі туралы кез келген хабарға мұқият қараңыз; егер сізге туысыңыз немесе басшыңыз шұғыл түрде ақша аудару туралы өтінішпен қоңырау соқса, оған басқа байланыс арнасы арқылы хабарласыңыз; жеке деректеріңізді, растау кодтары мен банктік ақпаратты чат-боттар мен белгісіз сайттар арқылы жібермеңіз; бос жұмыс орындары мен жұмыс

берушілерді мұқият тексеріңіз, әсіресе мәселе қашықтан жұмыс істеу туралы болатын болса; маңызды аккаунттар үшін екі факторлы аутентификацияны пайдаланыңыз.

Жасанды интеллект біздің күнделікті өміріміздің бір бөлігіне айналып кетті және болашақта бұдан да үлкен рөл ойнайтын болады. Сондықтан қазіргі уақытта жаңа технологияларды пайдалануды үйреніп қана қоймай, сондай-ақ алаяқтардың оларды қалай пайдалануы мүмкін екенін де түсіну қажет.

Цифрлық сауаттылық бейтаныс адамдарға есік ашпау немесе бөтен адамдарға банк картасының деректемелерін хабарламау керектігі сияқты қажетті әдетке айналып келеді.

Материал www.fingramota.kz сайтының көмегімен дайындалды.