

Баспасөз хабарламасы

WhatsApp-ты бұзып кірусіз және ізсіз «үнсіз басып алу»

Қазақстан Республикасы Бас прокуратурасы Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің Қылмыстық қауіп-қатерлердің және қоғамдық қауіпсіздіктің тәуекелдерін болжау орталығы «WhatsApp» мессенджеріне қатысты жаңа киберқатер туралы ескертеді.

Шетелдік дереккөздердің мәліметіне сәйкес
(<https://infobezopasnost.ru/blog/news/kiberataka-ghostpairing-pozvolyaet-moshennikam-poluchit-polnyj-dostup-k-whatsapp-bez-vzloma-parolya/>,
<https://www.securitylab.ru/news/567291.php>, <https://securitymedia.org/news/list/ataka-ghostpairing-pozvolyaet-nezametno-zakhvatyvayut-akkaunty-whatsapp.html>) кибералаяқтар

«WhatsApp» akkaунттарын басып алудың жаңа қылмыстық схемасын қолдануда. Бұл әдіс «GhostPairing» деп аталады және парольдерді бұзуды, SIM-карталарды ауыстыруды немесе күрделі техникалық шабуылдарды қажет етпейді. Алаяқтар «WhatsApp»-қа заңды түрде, қосымша құрылғыларды байланыстыру функциясын пайдалану арқылы қол жеткізеді.

Сценарийі қарапайым: пайдаланушыға «Facebook» немесе «WhatsApp» атынан жасырынған хабарлама жіберіледі, ол «Facebook» пен «WhatsApp» интерфейсіні визуалды түрде қайталайтын жалған парақшаларға бағыттайды.

Контентке қолжетімділікті растау үшін фейк-парақша телефон нөмірі мен растау кодын енгізуді ұсынады, осыдан кейін зиянкес автоматты түрде жәбірленушінің akkaунтына сенімді құрылғы ретінде қосылып, «WhatsApp»-қа толық қол жеткізеді (хабарламаларды оқу, медиафайлдарды қарау, байланыстар тізімі, хабарлама жіберу, фотогалереяға қолжетімділік). Бұл ретте телефон әдеттегідей жұмыс істей береді және күдік тудырмайды.

«WhatsApp»-тың басып алуын анықтаудың жалғыз жолы - «Байланыстырылған құрылғылар» бөлімін қолмен тексеру. Кез келген белгісіз қосылу akkaунттың бұзылғанын көрсетеді және дереу жойылуы тиіс.

Сақ болыңыздар, киберқауіпсіздік талаптарын сақтаңыздар:

- белгісіз кіріс хабарламаларға, қоңырауларға және әр түрлі хабарландыруларға мұқият болыңыздар;
- «WhatsApp» кодын бөгде парақшаларға енгізбеңіздер, қосымшадан тыс жерде кодты сұрату - әрқашан алаяқтық;
- екі факторлы аутентификацияны пайдаланыңыздар;
- akkaунтыңыздың белсенділігін тұрақты түрде тексеріп отырыңыздар;
- қорғаныш бағдарламалық қамтамасыз етуді қолданыңыздар.

Бір қатенің құны - Сіздің жеке хат алмасуыңызды толық бақылау.