ՀԱՅԱՍՏԱՆ

Թվային սպառնալիքների լանդշաֆտ. քաղաքացիական հասարակություն և լրատվամիջոցներ

Internews
Local voices. Global change.

CyberHUB

Բովանդակություն

Ներածություն

Նախորդ տարվա ընթացքում հայաստանյան բազմաթիվ քաղաքական ու հասարակական գործիչներ թիրախավորվեցին Pegasus լրտեսող ծրագրի միջոցով: Մասնագետների համար ակնհայտ էին այդ գրոհների ու Ադրբեջանի իշխանությունների միջև կապերը, ինչը դարձավ միջազգային հակամարտության ընթացքում Pegasus-ի կիրառման առաջին արձանագրված դեպքը: Նախորդ տասնամյակների Հայաստան-Ադրբեջան լարված հարաբերությունները, չդարարող հակամարտությունը ամենևին էլ նորություն չեն:

Թեև Հայաստանում կիբեռսպառնալիքների պատկերը ներկայացնելիս լրատվամիջոցները կենտրոնանում են գլխավորապես լրտեսող ծրագրերի վրա, սակայն քաղաքացիական հասարակության (քաղհասարակության) ներկայացուցիչները բախվում են բազմաթիվ այլ թվային սպառնալիքների:

Այս զեկույցը պատրաստել է «Internews» կազմակերպության Համացանցի ազատության և դիմակայունության թիմը («Internet Freedom & Resilience Team»)՝ նպատակ ունենալով սպառնալիքների վերլուծության և միջադեպերին արձագանքելու տեղայնացված փորձի միջոցով ամրապնդել քաղհասարակության կազմակերպությունների, լրագրողների և իրավապաշտպանների կարողությունները՝ հայտնաբերել, վերլուծել և դիմազրավել թվային հարձակումները: Այս զեկույցում ամփոփ ներկայացված են Հայաստանի քաղհասարակության և լրագրողների առջև կանգնած սպառնալիքները, ինչպես նաև խորհուրդներ՝ թվային անվտանգության մասնագետներին, որոնք իրենց գործունեությամբ աջակցում են քաղհասարակությանն ու լրագրողական համայնքին:

Զեկույցը նաև ընդհանուր տեղեկություններ է տալիս կիբեռանվտանգությամբ զբաղվող հանրությանը, թե ինչ համատեքստում են ծագում հայաստանյան թվային սպառնալիքները, ինչը կօգնի մասնագետներին վերլուծել Հայաստանի քաղհասարակությանն և լրագրողական հանրությանը առնչվող միջադեպերը:

Ամփոփիչ մասում քննարկվել են ռիսկերը նվազեցնելու միջոցառումները, որոնք թվային անվտանգության մասնագետները կարող են առաջարկել տարբեր կազմակերպությունների, համայնքների և անհատների:

Զեկույցը պատրաստվել է «CyberHub-Am»-ի Համակարգչային արտակարգ իրավիճակների արձագանքման թիմի («Computer Emergency Response Team» / «CERT») հետ սերտ համագործակցությամբ, և նախատեսված է հայաստանյան քաղհասարակության՝ հասարակական կազմակերպությունների (ՀԿ), իրավապաշտպանների, ակտիվիստների, լրագրողների, լրատվամիջոցների համար:

«CyberHub-Am»-ը հայաստանյան քաղհասարակությանը թվային աջակցություն ցուցաբերող, թվային սպառնալիքներին արձագանքող կենտրոն է, որը, հարկ եղած դեպքում, ժողովում, վերլուծում և միջադեպերին առնչվող տվյալների ու ցուցիչների վերաբերյալ տեղեկություններն անանուն եղանակով փոխանցում է կիբեռանվտանգությամբ զբաղվող միջազգային համայնքին:

Այս զեկույցում նկարագրված սպառնալիքները, միտումները և օրինակները վեր են հանվել ռիսկային խմբերին թվային անվտանգության գծով աջակցության ցուցաբերման («Internews»-ի ու «CyberHub-AM»-ի կողմից), ուսումնասիրությունների և «Համացանցի ազատություն» («Internet Freedom») համայնքի վստահելի անդամների հետ զրույցների արդյունքում:

Զեկույցում մեկտեղված են թվային միջադեպերի արձագանքներին վերաբերող տվյալները և Հայաստանին բնորոշ թվային հարձակումները նկարագրող արձանագրումները:

Հոկտեմբեր 2023

Հեղինակներ՝ Մարտին Գրուտեն, Էշլի Ֆալեր, Մարկ Շաֆեր և Սքայլեր Սելիք

Սրբագրումը, ձևավորումը և էջադրումը՝ Սքայլեր Սելիքի

Թվային սպառնալիքների համայնապատկերը

Քաղաքական համատեքստը, քաղհասարակությունը և լրատվամիջոցները

ԽՍՀՄ-ից անկախանալուց ի վեր՝ Հայաստանը շարունակական հակամարտության մեջ է Ադրբեջանի հետ՝ անցնելով բազմաթիվ պատերազմների, զինված բախումների միջով: Հակամարտության պատճառը շրջանն է, որը հայերն անվանում են Արցախ, իսկ միջազգային հանրությունը՝ Լեռնային Ղարաբաղ: Ադրբեջանը վերջերս ներխուժեց Լեռնային Ղարաբաղ, ինչը հանգեցրեց տեղի հայ բնակչության զանգվածային արտագաղթին:[1]

2023 թվականի սեպտեմբերին Ադրբեջանը ներխուժեց Լեռնային Ղարաբաղ, և 24 ժամ անց տեղի հայկական ուժերը զիջեցին: Այդ ռազմական գործողությունից հետո, ավելի քան 100 հազար հայեր լքեցին տարածաշրջանը, ինչը հանգեցրեց մարդասիրական ընդգրկուն ճգնաժամի:

Լեռնային Ղարաբաղի առաջին պատերազմը 1988-1994 թվականներին էր, որն ավարտվեց Ռուսաստանի միջնորդած հրադադարով: Ըստ համաձայնագրի, Հայաստանը վերահսկում էր Լեռնային Ղարաբաղի տարածքի մեծ մասը: Անցած տասնամյակներում, սակայն, երկու երկրների միջև չմարող լարվածությունը թե՛ Հայաստանում, թե՛ Ադրբեջանում դիտվում էր տնտեսական խնդիրների գլխավոր պատճառ: 2020 թվականին Լեռնային Ղարաբաղի համար բռնկվեց նոր՝ լայնածավալ պատերազմ: Այն տևեց վեց շաբաթ՝ մինչ նոր զինադադարը, որը հայերի մեծամասնությունը պարտություն է համարում:

2023 թվականի հոկտեմբերին՝ այս զեկույցի պատրաստմանը զուգահեռ, Հայաստանում իրավիճակն արագորեն փոխվում էր: 2023 թվականի սեպտեմբերին Ադրբեջանը ներխուժեց Լեռնային Ղարաբաղ, և 24 ժամ անց տեղի հայկական ուժերը զիջեցին: Այդ ռազմական գործողությունից հետո, ավելի քան 100 հազար հայեր լքեցին տարածաշրջանը, ինչը հանգեցրեց մարդասիրական ընդգրկուն ճգնաժամի:[2] Այս զեկույցի պատրաստման ընթացքում պահպանվում էր մտավախությունը, թե Ադրբեջանը կշարունակի իր ագրեսիան՝ ներխուժելով Հայաստանի հարավ: Ադրբեջանի կառավարությունը, սակայն, բացառում է նման հեռանկարը: Բաքուն Երևանին կոչ է արել խաղաղ ճանապարհով միջանցք բացել, որը թույլ կտա Ադրբեջանին կապվել Նախիջևանի հետ: Նախկինում Ադրբեջանը սպառնում էր ուժով բացել այդ միջանցքը: Ադրբեջանի ձեռնարկած ռազմական գործողությունների հետևանքով ԱՄՆ պետքարտուղարությունը 2002 թվականից ի վեր առաջին անգամ հրաժարվեց երկարաձգել «Ազատության աջակցության ակտի» («Freedom Support Act») կիրառման կասեցումը: Այսինքն, այդ ակտը սկսեց գործել, ինչն էլ անհնար է դարձնում Վաշինգտոնի ռազմական աջակցությունը Ադրբեջանին:[3]

Եվրոպայի հետ հարաբերությունների խորացմանը զուգահեռ՝ Հայաստանը սերտ կապեր ունի Ռուսաստանի հետ: Ռուսերենը ամենից տարածված օտար լեզուն է երկրում, և ռուսաստանցիները վիզայի կարիք չունեն՝ Հայաստան այցելելու համար: Հայտնի է, որ

Ռուսաստանը ռազմակայան ունի Հայաստանում. ռուսական 102-րդ ռազմակայանը տեղակայված է Գյումրիում և Ռուսաստանի զինված ուժերի հարավային ռազմական օկրուգի հրամանատարության ներքո է: Ռուսաստանը նաև խաղաղապահ ուժեր ունի հայ-ադրբեջանական սահմանին և Լեռնային Ղարաբաղում, թեև այդ ուժը զգալիորեն կրճատվել են՝ Ուկրաինա ռուսական լայնամասշտաբ ռազմական ներխուժման պատճառով:

Կիևի դեմ Կրեմլի սանձազերծած պատերազմից հետո, տեղեկատվական տեխնոլոգիաների (ՏՏ) ռուսաստանցի շատ մասնագետներ, Ռուսաստանի քաղհասարակության որոշ ներկայացուցիչներ և լրագրողներ տեղափոխվեցին Հայաստան:[4]

2022 թվականին Հայաստանը ձեռնպահ քվեարկեց ՄԱԿ-ի բանաձևին, որը պահանջում էր Ռուսաստանից դադարեցնել ռազմական գործողությունները Ուկրաինայում և դուրս բերել իր զորքերը այդ երկրից:[5]

Լեռնային Ղարաբաղ Ադրբեջանի ներխուժման ժամանակ Ռուսաստանի անգործությունը անորոշություն է առաջացրել ռուս-հայկական հարաբերություններում: Ի հավելումն՝ Հայաստանը աջակցություն չստացավ Հավաքական անվտանգության պայմանագրի կազմակերպությունից (ՀԱՊԿ), որին անդամակցում է, և այդ հանգամանքը Երևանում հարցեր առաջացրեց, թե որքանով է արդյունավետ մնալ Մոսկվայի ղեկավարած ռազմական այդ դաշինքի անդամ:

2023 թվականի հոկտեմբերին Հայաստանը վավերացրեց Հռոմի ստատուտը՝ միանալով Միջազգային քրեական դատարանին: Ռուսաստանը վճռականորեն դեմ է արտահայտվեց այդ քայլին. հայտնի է, որ դատարանը հրահանգ է իջեցրել ձերբակալել նախագահ Վլադիմիր Պուտինին:[6]

Ընդհանոր առմամբ, հայաստանյան քաղհասարակությունն ու լրատվամիջոցները ազատորեն են գործում: Այնուամենայնիվ, նախորդ տարիներին նկատվել է սահմանափակումների աճ, իսկ տարածաշրջանային զարգացումներին զուգահեռ՝ իրավիճակը կարող է փոխվել:

Հատկանշական էր հայաստանյան քաղհասարակության ակտիվ դերակատարումը 2018 թվականի բողոքի ակցիաներին, որոնք երկրում հանգեցրին իշխանափոխության:[7] 2021 թվականին Հայաստանի իշխանությունները նախաձեռնեցին զրպարտության մասին օրենսդրության խստացում, որը կարող էր ուղղվել լրագրողների դեմ, սակայն ներքին ու միջազգային դիմադրության շնորհիվ՝ հաջորդ տարի հրաժարվեցին այդ գաղափարից:[8] Ըստ «Լրագրողներ առանց սահմանների» («Reporters Without Borders») կազմակերպության, Հայաստանի կառավարությունը բավարար չափով չի պաշտպանում մամուլի ազատությունը, նշվում է, որ լրագրողների նկատմամբ բռնությունները հաճախ անպատիժ են մնում:[9]

Հաճախակի են դարձել խոսքի ազատության և քաղհասարակության առջև ծառացած սպառնալիքները՝ վտանգելով հատկապես խոցելի խմբերը:

Համեմատաբար վերջերս մի քրեական հետապնդում թույլ տվեց խոսել խոսքի ազատության և քաղհասարակության առջև ծառացած մարտահրավերբների մասին, և ուշադրության կենտրոնում էր հայաստանյան էթնիկ փոքրամասնություններից մեկը՝ եզդիական համայնքը:

Իշխանությունները ձերբակալել են Հայաստանում Մարդու իրավունքների եզդիական կենտրոնի ղեկավար Սաշիկ Սուլթանյանին՝ նրան մեղադրելով ատելության խոսք տարածելու և բռնություն հրահրելու մեջ:[10]

Հայաստանը չունի խտրականության դեմ պայքարի հատուկ օրենք, և ոլորտի հետազոտողները մտավախություն ունեն, որ այս դեպքը կարող է բացասական ազդեցություն ունենալ խոսքի ազատության վրա:[11]

> ***Համախակի են դարձել խոսքի ազատության և քաղհասարակության առջև ծառացած սպառնալիքները՝ վտանգելով հատկապես խոցելի խմբերը:***

Հայաստանի ԼԳԲՏՔ+ համայնքը նույնպես բախվում է խտրականության, ինչն ազդում է համայնքի կազմակերպությունների արդյունավետության վրա:[12] Քվիր համայնքի շահերը ներկայացնող կազմակերպությունները՝ «Փինք» և «Իրավունքի կողմ» ՀԿ-ները առերեսվել են ահաբեկումների ու սպառնալիքների՝ երկրում առկա դատական այնպիսի համակարգի պայմաններում, որը փաստացի չի արձագանքում հոմոֆոբ բռնությանը:[13] Չնայած սպառնալիքներին, ԼԳԲՏՔ+ կազմակերպությունները շարունակում են իրենց գործունեությունը՝ համագործակցելով լրատվամիջոցների ու կառավարության հետ և աջակցություն տրամադրելով հայաստանյան քվիր համայնքին:[14]

Կիբեռանվտանգությունը Հայաստանում

Թեև Հայաստանը համացանցին միացել է 1994 թվականին՝ .am դոմեյնի ներդրմամբ, սակայն մոտ 2010 թվականին համացանցի օգտագործումը երկրում համատարած դարձավ:[15]

Հավանաբար, Ռուսաստանի հետ սերտ հարաբերություններն են նպաստել ֆինանսական շահ հետապնդող հաքերների ազատ գործունեությանը Հայաստանում: Ըստ «Verizon»-ի, 2013 թվականին Հայաստանը բազմաթիվ նման հաքերների էր «հյուրընկալել»:[16] Մեծածավալ սփամ ուղարկող «Bredolab» բոտնետի ենթադրյալ հեղինակը՝ հայկական ծագմամբ մի ռուսաստանցի, 2012 թվականին չորս տարվա ազատազրկման դատապարտվեց Հայաստանում:[17]

Ըստ Հայաստանի ոստիկանության տվյալների, 2016-2018 թվականներին կիբեռհանցագործությունների 20-25% աճ է արձանագրվել: Երկրում կիբեռհանցագործության հիմնական տեսակը դրամական միջոցների հափշտակումն է, և ամենից տարածված եղանակներից է բանկային քարտերից գումար գողանալը: Բանկային տվյալները հափշտակելու նպատակով՝ հարձակվողները սոցցանցերի միջոցով թիրախավորում են քաղաքացիներին՝ երբեմն նմանակելով նրանց հարազատներին:[18] 2019 թվականին հայերից և հնդիկներից բաղկացած կազմակերպված հանցավոր խմբավորումը ԱՄՆ-ի և Կանադայի օգտատերերին թիրախավորող խոշոր խարդախության տեխնիկական աջակցությունն էր իրականացրել:[19]

Հանրահայտ «Telegram» և «WhatsApp» մեսենջերների հայաստանյան օգտատերերը հաճախ են հայտնվում տարաբնույթ խարդախությունների և հաքերային հարձակումների թիրախում: Ըստ «CyberHub-AM»-ի, հանցավոր նպատակներով հաղորդագրությունները հաճախ գրվում են

ռուսերեն: Որոշ օգտատերեր կարող են Ռուսաստանի քաղաքացիներին թիրախավորող արշավների անուղղակի զոհ դառնալ:

Քանի որ «Telegram»-ը և «WhatsApp»-ը կապված են օգտատիրոջ հեռախոսահամարին, յուրաքանչյուր ոք, ով կարող է ստանալ այդ համարին հասցեագրված «SMS» հաղորդագրությունը, նաև կարող է տիրանալ «Telegram»-ի, «WhatsApp»-ի տվյալ օգտահաշվին, եթե, իհարկե, կիրառված չէ լրացուցիչ պաշտպանություն՝ օրինակ, այդ հավելվածներում ևս օգտագործվող գաղտնաբառ: Թեև նման գրոհները երբեմն իրականացվում են, այսպես կոչված, սոցիալական ինժեներիայի օգտագործմամբ, սակայն օգտահաշիվներին հափշտակությունը հաճախ է տեղի ունենում առանց որևէ շարժառիթի:

Քիչ չեն նաև դեպքերը, երբ մարդիկ, որոնք չեն օգտվում, օրինակ, «WhatsApp»-ից, հայտնում են, որ իրենց հեռախոսահամարներն օգտագործվել են «WhatsApp»-ի օգտահաշիվ ստեղծելու համար: Այս ամենը թույլ է տալիս ենթադրել, որ հարձակվողները մուտք ունեն կա՛մ հեռահաղորդակցական ընկերություն, որը ստանում է հեռախոսահամարի գոյությունը հաստատող «SMS» հաղորդագրությունը, կա՛մ այն հարթակներ, որոնք օգտագործվում են դրանք ուղարկելու համար:

Վերջին տարիներին Հայաստանում արձանագրվել են պետության կողմից հովանավորվող թվային հարձակումների դեպքեր: 2019 թվականին Ռուսաստանի հետ առնչություն ունեցող «Turla» խումբը «ջրելատեղ» («watering hole») տեսակի հարձակման[i] միջոցով «կոտրեց» հայաստանյան չորս կարևոր կայքեր, որոնցից երկուսը պատկանում էին կառավարությանը: Գրոհը արձանագրել է կիբեռանվտանգությամբ զբաղվող «ESET» ընկերությունը:[20] Խմբավորման նախկին գործունեությունից և «կոտրված» կայքերից դատելով՝ «Turla»-ն, հավանաբար, ցանկանում էր թիրախավորել քաղաքական գործիչների և պետական պաշտոնյաների:

2021 թվականին լրտեսող ծրագրերի արտադրությամբ զբաղվող իսրայելական «Candiru» ընկերության ծրագրով թիրախավորվեցին նաև հայաստանցիներ՝ լայնամասշտաբ արշավի շրջանակում: Հարձակումներն իրականացվել էին օգտագործելով «Microsoft»-ի[21] ծրագրային ապահովման մեջ առկա, այսպես կոչված «զրո օրվա խոցելիությունը»:[ii] Թիրախում էին քաղաքական գործիչներ, իրավապաշտպաններ և լրագրողներ: Մոտավորապես նույն ժամանակ «Google»-ը հայտարարեց, որ Հայաստանում թիրախները ստացել են «Google Chrome»-ի՝ «զրո օրվա խոցելիությունն» օգտագործող հղումներով նամակներ:[22]

[i] «Ջրելատեղ» («watering hole») տեսակի թվային գրոհի ժամանակ հարձակում գործողները «կոտրում» և վնասակար ծրագրով վարակում են այն կայքը, որն, ամենայն հավանականությամբ, այցելում են թիրախավորված խմբի ներկայացուցիչները: Այդկերպ, հարձակումը տեղի է ունենում առանց թիրախների հետ ուղղակի գործ ունենալու: Ինչո՞ւ «ջրելատեղ», որովհետև հաքերները նման գրոհները նմանեցնում են այն իրավիճակին, երբ, օրինակ, այծեղջյուրը եկել է որևէ լճի մոտ ծարավը հագեցնելու, և կոկորդիլոսը գրոհում է:

[ii] «Զրո օրվա խոցելիությունները» («zero-day vulnerabilities») նրանք են, որոնք հայտնաբերվում ու օգտագործվում են նույն օրը և որոնք մինչ այդ հայտնի չէին տվյալ ծրագիրը մշակողին, արտադրողին, ուստի վերջիններս զրո օր ունեին այն շտկելու համար: Հայտնի դառնալուց հետո, խոցելիությունն այլևս չի կոչվում «զրո օրվա», այլ անվանվում է այն օրերի թվով, ինչ հայտնի է, օրինակ՝ «մեկ օրվա խոցելիություն», «երկու օրվա խոցելիություն» և այլն:

2022 թվականին թվային սպառնալիքների մասին իր զեկույցում «Meta»-ն հայտնեց Ադրբեջանի [կառավարության] իրականացրած թվային հարձակումների մասին՝ վնասակար ծրագրերի (malware), ֆիշինգի (phishing), կեղծ օգտահաշիվների ու կայքերի կիրառմամբ:[23] Թեև այդ գրոհները առավելապես Ադրբեջանի ներսում էին, սակայն թիրախավորել էին նաև Հայաստանում գտնվող որոշ մարդկանց:

Քաղհասարակության և լրատվամիջոցների կիբեռանվտանգության վիճակը

Թեև հայաստանյան քաղհասարակության և լրատվական դաշտի ներկայացուցիչները ենթարկվում են թվային այն բոլոր հարձակումներին, որոնց զոհ են դառնում մյուս հայաստանցիները, սակայն իրենց գործունեության բնույթով պայմանավորված նրանք նաև առանձնահատուկ սպառնալիքների առջև են: Լինում են նաև չթիրախավորված թվային գրոհներ, որոնք երբեմն ավելի մեծ վնաս են պատճառում: Ուստի, քաղհասարակության ներկայացուցչի համար երբեմն պարզ չէ՝ հարձակումը թիրախավորվա՞ծ էր, թե՞ ոչ: Նրանց «Telegram»-ի, «WhatsApp»-ի և սոցմեդիայի օգտահաշիվները հաճախ են հայտնվում հարձակվողների թիրախում, կայքերը «կոտրվում» են՝ դառնալով «DdoS» գրոհների զոհ: Թե կայքը «կոտրելու» միջոցով ՀԿ-ի համար ինչպես են լուրջ խնդիր ստեղծել, նկարագրված է օրինակների բաժնում:

> ***Քաղհասարակության ներկայացուցչի համար երբեմն պարզ չէ՝ հարձակումը թիրախավորվա՞ծ էր, թե՞ ոչ: Նրանց «Telegram»-ի, «WhatsApp»-ի և սոցմեդիայի օգտահաշիվները հաճախ են հայտնվում հարձակվողների թիրախում, կայքերը «կոտրվում» են՝ դառնալով «DdoS» գրոհների զոհ:***

Ինչպես ողջ աշխարհում, այնպես էլ Հայաստանում լրատվամիջոցների և քաղհասարակության ներկայացուցիչների ռեսուրսները սահմանափակ են՝ դիմագրավելու թվային սպառնալիքներին: Նրանց թվային անվտանգության վրա պարբերաբար ազդում են իրենց իսկ որոշումները, օրինակ՝ հնացած ծրագրերի օգտագործումը. «կոտրված», չարտոնագրված ծրագրերի ներբեռնումը համացանցից՝ պաշտոնական տարբերակը գնելու փոխարեն: Վերջին երևույթն այնքան տարածված է, որ հայտնի են դեպքեր, երբ կազմակերպությունները, ունենալով պաշտոնական, արտոնագրված ծրագրեր, այդուհանդերձ ներբեռնել են դրանց «կոտրած» տարբերակը:[24]

Կազմակերպություններից մեկը, որ օգտագործում էր նման՝ «կոտրված» ծրագիր, թվային գրոհի էր ենթարկվել: «Կոտրված» ծրագիրը հարձակվողներին հնարավորություն էր տվել կազմակերպության ներքին ցանցում հաքերային «keylogger» ծրագիր տեղադրել, որի միջոցով էլ չարագործները տիրացել էին ՀԿ-ի «Google» օգտահաշվին: Ցանցում վնասակար ծրագրի առկայության մասին «Google»-ի նախազգուշացումից հետո միայն «keylogger»-ը հայտնաբերվեց:

Մեկ այլ ՀԿ մի քանի հազար ԱՄՆ դոլար էր կորցրել՝ կորպորատիվ էլ.-փոստի վրա հարձակման («business email compromise», «BEC») հետևանքով, որի միջոցով «կոտրվել» էր կազմակերպության «Yahoo»-ի օգտահաշիվը: Հաքերները, օգտագործելով օգտահաշիվը և

սոցիալական ինժեներիայի հնարքները, իրենց արդեն իսկ հասանելի էլ.-փոստի հասցեից նամակ են ուղարկել դոնոր-կազմակերպությանը՝ համոզելով գումար փոխանցել հարձակվողների ստեղծած բանկային հաշվին: Չնայած այս խարդախությունն իր մասշտաբով զիջում է «BEC»-ի կիրառմամբ այլ դեպքերին, սակայն ՀԿ-ն տուժել էր թվային այդ գրոհից:[25]

> ***Ադրբեջանի իշխանությունները ձեռք են բերել «Pegasus»-ը և օգտագործել այդ լրտեսական ծրագիրը՝ թիրախավորելու տեղացի ակտիվիստներին և լրագրողներին՝ ցուցադրելով միաժամանակ ծրագիրը Հայաստանում աշխատեցնելու իրենց կարողությունը:***

Հայաստանում իրականացված թվային գրոհներից շատերի հետքը տանում է դեպի հարևան Ադրբեջան: Օրինակ, 2022 թվականի հոկտեմբերին ադրբեջանցի հաքերները տիրացել էին հնացած և խոցելի ծրագրային ապահովմամբ աշխատող հայկական մի հոսթինգ պրովայդերի: Արդյունքում՝ այդ հոսթինգի վրա առկա բոլոր կայքերը «կոտրվել» էին: Թեև հարձակումն ուղղակի հասցեատեր չուներ, կայքերից երկուսը պատկանում էին հայաստանյան ՀԿ-ների:[26] Թուրքական հաքերային խմբերը ևս պարբերաբար թիրախավորել են հայկական կայքերը:

Ի հավելումն վերը հիշատակված, տեխնիկապես նվազ բարդություն ներկայացնող գրոհների, որոնց պատճառը նաև թվային անբավարար հիգիենան է ու սոցիալական ինժեներիայի կիրառումը, որոշ հայտնի հայաստանցիներ, այդ թվում՝ քաղհասարակության ներկայացուցիչներ, լրագրողներ, թիրախավորվել են նաև լրտեսող նորագույն ծրագրերի՝ «Predator»-ի և «Pegasus»-ի միջոցով:

2021 թվականի դեկտեմբերին «Meta»-ն[27] ու «Citizen Lab»-ը[28] համատեղ առաջին անգամ հայտնեցին Հյուսիսային Մակեդոնիայում գտնվող «Cytrox» ընկերության մշակած «Predator» լրտեսող ծրագրի մասին: Նշվում էր, որ «Cytrox»-ի որոշ պատվիրատուներ գտնվում են Հայաստանում: Այնուհետև, «CyberHub-AM»-ը հաստատեց, որ «հայաստանյան քաղաքական և մեդիա թիրախներին» պատկանող մի քանի սարքեր վարակված են եղել «Predator»-ով, և սա թույլ է տալիս կասկածել, որ այդ հարձակումների հետևում կանգնած են տեղական անվտանգության ծառայությունները:[29]

«Telegram»-ի «կոտրված» օգտահաշիվներն օգտագործվել էին «Predator»-ի տեղադրումն ապահովող հղումներ տարածելու համար: Այս մարտավարությունը գալիս է բացատրելու, թե ինչու էր անհրաժեշտ «առևանգել» ոմանց օգտահաշիվները՝ այդ թվում «Telegram»-ում (վերը անդրադարձանք): Ուշագրավ հնարք է. այսինքն, ցածր կամ միջին ռիսկայնության գոտում գտնվող մարդկանց օգտահաշիվները, սովորաբար, ավելի դյուրին է «կոտրել», քան բարձր ռիսկայնության գոտում գտնվող անձանց, և իրական թիրախները քիչ կասկածանքով կբացեն իրենց ծանոթ, բայց «կոտրված» օգտահաշիվներից եկած հաղորդագրությունները՝ դառնալով թվային հարձակման զոհ:

«Pegasus» լրտեսող ծրագիրը, որը մշակել և վաճառում է Իսրայելում գործող «NSO Group»-ը, իր տեսակի մեջ ամենահայտնին է: Այն բազմաթիվ լրատվական նյութերի, փաստաթղթերի, նույնիսկ գրքերի թեմա է դարձել: Դեռ 2016 թվականին Մեքսիկայում և ԱՄԷ-ում հայտնաբերված «Pegasus»-ի՝ Հայաստանում օգտագործման առաջին ապացույցներն ի հայտ եկան 2021-ի

նոյեմբերին: Այդ ժամանակ «Apple»-ից ծանուցումներ ստացվեցին, որ պետությունները գործողություն են իրականացնում «iPhone»-ի որոշ օգտատերերի դեմ: Թեև սկզբնական շրջանում մեղադրանքներ էին հնչում Հայաստանի իշխանությունների հասցեին, սակայն փաստերը ցույց տվեցին, որ Հայաստանում «Pegasus»-ի կիրառման հետևում կանգնած են Ադրբեջանի իշխանությունները:[30]

2023 թվականին «CyberHub-AM»-ը՝ արտերկրի գործընկերների հետ, «Pegasus»-ի կիրառման դեպք բացահայտեց, որը տեղի էր ունեցել ղարաբաղյան երկրորդ պատերազմի ժամանակ՝ 2020 թվականին, և այդ հանգամանքը միայն ամրապնդեց կասկածները, թե գրոհի հետևում Ադրբեջանի իշխանություններն են:[31] Հայտնի է նաև, որ Ադրբեջանը ձեռք է բերել «Pegasus» ծրագիրը և այն կիրառել երկրի ներսում՝ թիրախավորելու ադրբեջանցի ակտիվիստներին ու լրագրողներին:[32] Միաժամանակ, այն կիրառվել է Հայաստանում: Հայաստանցի մի լրագրողի դեմ «Pegasus»-ի օգտագործման դեպքի նկարագրությունը օրինակների բաժնում է:

Ռիսկերը նվազեցնող միջոցառումներ

Օգտահաշվի անվտանգությունը կարևոր է յուրաքանչյուրի, հատկապես՝ քաղհասարակության և լրատվամիջոցների ներկայացուցիչների համար:

Երկփուլային վավերացման համակարգը (two-factor authentication) պարտադիր է. այն նվազեցնում է հատկապես թույլ գաղտնաբառերի օգտագործման դեպքում առաջացող խոցելիությունները: Թեև երկփուլային վավերացման համակարգի առկայությունն, ամեն դեպքում, ավելի լավ է, քան բացակայությունը, սակայն առկա են բազմաթիվ փաստեր, որ «SMS»-ի միջոցով վավերացումն անցնող գործընթացը Հայաստանում բավականաչափ անվտանգ չէ, հատկապես բարձր ռիսկային գոտում գտնվող օգտատերերի համար: Որպես օրինակ կարելի է ծանոթանալ «CyberHub-AM»-ի այս հրապարակմանը: Երկփուլային վավերացման հավելվածի օգտագործումն ավելի ապահով է, քան «SMS» ստանալու տարբերակը, իսկ ընդհանրապես՝ առավել ապահովը կոդերի գեներատոր սարքի (hardware token) օգտագործումն է:

Որոշ մեսենջերներ՝ «Telegram»-ը, «WhatsApp»-ը, «Signal»-ը, հաշվի ակտիվացման համար հեռախոսահամար են պահանջում, և ունեն երկփուլային վավերացման իրենց համակարգը: Այսինքն, պահանջում են հավելյալ գաղտնաբառ: Նման կերպ ապահովվում է լրացուցիչ պաշտպանություն, երբ որևէ մեկը ապօրինաբար հասանելիություն ստանա ձեր հեռախոսահամարին ուղղվող «SMS»-ներին: Երբ մեսենջերների երկփուլային վավերացման համակարգը միացված է, հավելվածը («Telegram», «WhatsApp», «Signal») պարբերաբար կխնդրի օգտատիրոջը մուտքագրել իր գաղտնաբառը՝ երաշխավորելով, որ հաղորդագրությունները հասանելի չեն երրորդ անձին: Ինչպես ասացինք, սա կարող է կանխել «SMS»-ները ճանկելու միջոցով օգտահաշիվներին տիրանալը, ինչը տարածված երևույթ է Հայաստանում:

Անհրաժեշտ է պարբերաբար թարմացնել սմարթֆոնների, նոութբուքերի ծրագրային ապահովումները և կիրառել անվտանգության շտկումները, երբ դրանք այլևս հասանելի են: Ծրագրերը պետք է ձեռք բերվեն միայն պաշտոնական աղբյուրներից, ինչը շատ դեպքերում վճարովի է: ՀԿ-ները չպետք է զերծ մնան այս հարցը դոնորների քննարկելուց կամ փնտրեն

անվճար այլընտրանքներ՝ բաց կոդով ծրագրեր, որոնք անվճար են կամ սեփականատերերի կողմից կարող են էժան տրամադրվել որոշ ՀԿ-ների:

Սովորաբար աղրբեջանցի, հազվադեպ նաև՝ թուրք հաքերները թիրախավորում են հայաստանյան քաղհասարակության կազմակերպությունների կայքերը «DdoS» գրոհներով, կամ «կոտրելով» կայքը՝ աղավաղում, փոխում են դրա բովանդակությունը (defacement): Եթե նման հարձակումների սպառնալիք կա, պետք է կանխարգելիչ միջոցներ ձեռնարկվեն՝ օգտվելով «DdoS» գրոհների վտանգը նվազեցնող ծառայություններից՝ «Cloudflare», «Project Shield»: Կայքի բովանդակության կառավարման համակարգը և խրվակները (plugin) մշտապես թարմ վիճակում պահելուց զատ, անհրաժեշտ է ընտրել հոսթինգի այնպիսի պրովայդեր, որն իր համակարգերում հետևողականորեն կիրառում է անվտանգության շտկումները:

Կայքերում և նոութբուքերում, սմարթֆոններում կուտակված տվյալների կանոնավոր կրկնօրինակումը (backup) թույլ է տալիս օգտատերերին վերականգնել դրանք ջնջվելուց հետո: Հոսթինգի պրովայդերները կամ տվյալ սարքը արտադրողները երբեմն ավտոմատ կերպով ներդնում են կրկնօրինակման գործառույթը, ինչն ամենահարմար տարբերակն է: Եթե չկա նման բան, ապա լավագույն լուծումը շաբաթը կամ առնվազն ամիսը մեկ կրկնօրինակներ ստեղծելն է, համոզվել, որ դրանք ապահով պահեստավորված են՝ նման կերպ կանխելով տվյալների անվերադարձ կորուստը:

Առաջատար լրտեսող ծրագրերը՝ «Pegasus»-ը, «Predator»-ը, սովորաբար օգտագործում են «զրո օրվա խոցելիությունները»: «Pegasus»-ը նաև հաճախ դիմում է, այսպես կոչված, օգտատիրոջ կողմից զրո միջամտության միջոցով վարակման տարբերակին (zero-click infections), երբ թիրախը որևէ գործողություն չի կատարել՝ չի բացել որևէ հաղորդագրություն, չի անցել որևէ հղումով, սակայն, միևնույն է, իր սարքը (սմարթֆոն, նոութբուք և այլն) վարակվել է: Սա նշանակում է, որ անգամ բոլոր հնարավոր թարմացումներն ունեցող սարքը կարող է վարակվել, և օգտատերը չի կարողանա դեմն առնել՝ կիրառելով վերը նշված կանխարգելիչ քայլերը: Նման վտանգի առջև գտնվողները պետք է հաշի առնեն սա:

Հատկապես ռիսկային բարձ գոտում գտնվող անձանց խորհուրդ է տրվում մեսենջերներում միացնել հաղորդագրությունները որոշ ժամանակ անց ավտոմատ ջնջող տարբերակը: Սա կարող է նվազեցնել վնասը, երբ ապագայում տվյալ օգտահաշիվը «կոտրվի»: Աշխատանքային ու անձնական շփումների համար նախատեսված սարքերի տարանջատումը (compartmentalization), իսկ բարձր ռիսկային գոտում անձանց պարագայում ևս մեկ՝ երրորդ սարքի կիրառումը նույնպես նվազեցնում է հնարավոր վնասի չափը, թեև այս ամենը լրացուցիչ ծախսեր ու անհարմարություններ են:

Սմարթֆոնների ծրագրերը թարմ վիճակում պահելուց զատ, օրինակ, «iPhone»-ների պարագայում կանոնավոր վերագործարկումը (restart) (օրական մեկ անգամ) և մեկուսացման ռեժիմի (lockdown mode) միացումը (այս պարագայում գործ կունենաք որոշ ծառայությունների սահմանափակման հետ) նույնպես նվազեցնում են «կոտրվելու» հավանականությունը:

Ավելի քիչ է հայտնի «Android» համակարգը թիրախավորող լրտեսական ծրագրերի մասին, թեև այն չի նշանակում, որ «Android» օգտագործողների առջև կանգնած խնդիրները սակավ են:

Հայտնի է, որ թանկարժեք «Android» սարքերն ավելի անվտանգ են և, սովորաբար, նրանց ավելի արագ են հասանելի դառնում խոցելիություններից պաշտպանող անվտանգային շտկումները: Հավանական է, որ «Android»-ով աշխատող սարքի կանոնավոր վերագործարկումը կարող է նվազեցնել «կոտրվելու» ռիսկը, քանի որ լրտեսող ծրագրերը վերագործարկումից հետո սովորաբար չեն պահպանվում:[iii] Թեպետ «Android»-ի դեպքում հարկ է գիտակցել, որ վերագործարկումը կարող է նաև հեռացնել վարակվածության ապացույցները: Ոմանց սա կարող է մտահոգել:

[iii] Այդպես է iPhone-ի համար նախատեսված բոլոր հայտնի և, հավանաբար, Android-ի համար նախատեսված այլ լրտեսող ծրագրերի դեպքում, հատկապես այն տեսակների պարագայում, որոնք «արմատներ են գցում» սարքում:

Օրինակներ

«WordPress»-ի խոցելի խրվակի միջոցով «կոտրված» կայքը

Հայաստանում փոքրամասնությունների իրավունքների պաշտպանությամբ զբաղվող մի կազմակերպության կայքը 2023 թվականի մայիսին «կոտրվեց», և կայքի այցելուներն ուղղորդվում էին դեպի այնպիսի կայքեր, որոնք ակնհայտորեն խաբեությամբ էին զբաղվում, և որոնց բովանդակությունը կապ չուներ կազմակերպության կայքի հետ: Կազմակերպությունը պատրաստվում էր կարևոր զեկույց հրապարակել, և նրանք «զգում էին», որ կայքը միտումնավոր է «կոտրվել»:

Միջադեպը հետաքննելու համար կազմակերպությունը դիմեց «CyberHub-AM»-ին՝ Համակարգչային արտակարգ իրավիճակների արձագանքման թիմին:

Թիրախավորված կազմակերպության կայքն աշխատում էր բովանդակության կառավարման և բաց կոդով աշխատող հանրահայտ «WordPress» համակարգով, որից, սովորաբար, օգտվում են բազմաթիվ երկրների ՀԿ-ներ: Չարագործները հաճախ կարողանում են գտնել և օգտագործել «WordPress»-ի խոցելիությունները: Մասնավորապես, այդ հարցում նրանց օգնում են բազմաթիվ խրվակներ, որոնց միջոցով նրանք տիրանում են կայքերին՝ օգտագործելով դրանք չարամիտ նպատակներով կամ փոխելով կայքերի բովանդակությունը:

Հետազոտության ընթացքում «CyberHub-AM»-ի թիմը ուշադրություն դարձրեց վեբ սերվերում ոչ վաղ անցյալում փոփոխված ֆայլերին և հայտնաբերեց վերջերս ավելացված կամ փոփոխված տարբեր ֆայլեր, որոնք պատկանում էին «posts-layouts» անվամբ խրվակին: Հայտնաբերվեց նաև «de-mouser-44» անունով նոր ադմինիստրատոր-օգտատեր (admin user), ինչն ապացույցն էր, ոչ արտաքին դերակատարը մուտք է ստացել օգտահաշվին:

Վերլուծելով հաջորդականությունը, ըստ որի շարժվում էին կայքի այցելուները, «CyberHub-AM»-ը պարզեց, որ նրանց սկզբում ուղղորդում էին դեպի «cdn[.]scriptsplatform[.]com»: «scriptsplatform[.]com» դոմեյնն ընդամենը օրեր առաջ էր գրանցվել՝ մայիսի 12-ին: Իր հերթին՝ այդ դոմեյնն օգտատերերին վերաուղղորդում էր խաբեությամբ զբաղվող այլ կայք, ինչը նման պարագաներում սովորական մարտավարություն է:

Որոնելով կայքում «հայտնված» նոր օգտատիրոջը՝ «CyberHub-AM»-ը պարզեց, որ կան բազմաթիվ այլ կայքեր, որոնք նույն կերպ են «կոտրվել»: Ստուգումը հաստատեց, որ այդ կայքերը նույնպես ուղղորդում էին դեպի «scriptsplatform[.]com» դոմեյն: Հաշվի առնելով, որ տուժած մյուս կայքերը որևէ առնչություն չունեին կազմակերպության հետ՝ ո՛չ բովանդակությամբ, ո՛չ աշխարհագրորեն, «CyberHub-AM»-ը եզրակացրեց, որ կազմակերպության դեմ հարձակումը պատահական էր:

Ստուգելով «WordPress»-ի օգտահաշվում կազմակերպության տեղադրած խրվակները՝ «CyberHub-AM»-ի մասնագետները գտան «Essential Addons for Elementor»-ը, որը կայքերի ստեղծման հանրահայտ «Elementor» խրվակի ընդարձակ տարբերակն է (extension) է: Այդ

խրվակում վերջերս խոցելիություն էր հայտնաբերվել, ինչից կարելի էր ենթադրել, որ դա էր կայքը «կոտրելու» հավանական պատճառը:[33]

Կիբեռնվտանգությամբ զբաղվող «Sucuri» ընկերությունը որոշ ժամանակ անց վերլուծեց հենց այս խոցելիության միջոցով տեղ գտած զանգվածային վարակումների արշավը: Այս զեկույցում նկարագրված նշանները հաստատում են, որ հայաստանյան կազմակերպությունը ևս այդ արշավի զոհն էր:[34]

«CyberHub-AM»-ը հեռացրեց է կեղծ՝ «posts-layout» խրվակով թղթապանակը՝ վնասակար «init.php», «job.php» ֆայլերով, ինչպես նաև որոշ քողարկված վեբ-թաղանթներ (webshells): Թեև «CyberHub-AM»-ը դյուրությամբ վերացրեց վարակը, կայքի կրկնակի վարակումը կանխարգելելուն ուղղված քայլերը նույնքան հեշտ չէին: Որոշ կախվածությունների պատճառով չհաջողվեց թարմացնել «Elementor» խրվակի առանցքային ընդարձակումները՝ այնպես վերացնել խոցելիությունը, որ կայքի հիմնական գործառույթը չխախտվի:

Առանց հիմնական գործառույթը խախտելու՝ թարմացումներ իրականացնելու անկարողությունը, ցավոք, տարածված երևույթ է՝ հատկապես պատվերով պատրաստված կայքերի պարագայում: Սա վկայում է, որ նման կայք վարելը պահանջում է անդադար սպասարկում: Ըստ «CyberHub-AM»-ի վերլուծական գրառման, «հայաստանյան ընկերությունների մեծամասնությունն իրենց կայքերին վերաբերում է ինչպես սառնարանի, որը կարելի է գնել, դնել խոհանոցում ու տարիներով մոռանալ այդ մասին»:[35]

Բարեբախտաբար, կազմակերպությունը նախատեսում էր գործարկել իր կայքի նոր տարբերակը՝ դեպքից մի քանի շաբաթ անց, որը նաև կլուծեր նման կախվածության խնդիրը: Մինչ այդ՝ «CyberHub-AM»-ը տեղադրեց վեբ հասանելիության պատնեշ (web access firewall, WAF)՝ հնարավոր նոր թիրախավորման ռիսկը նվազեցնելու համար: Կայքն այլևս չի «կոտրվել»:

«Pegasus» լրտեսող ծրագրի միջոցով լրագրողի «կոտրված» հեռախոսը

2022 թվականի նոյեմբերի 10-ին Աստղիկ Բեդևյանը նամակ ստացավ «Apple»-ից, թե «պետության կողմից հովանավորվող հարձակվողները, հնարավոր է, թիրախավորում են [իր] «iPhone-ը»»:[36] Նա՝ նման ահազանգ ստացած մի քանի հայաստանցիներից մեկն էր:

Բեդևյանը «Ազատ Եվրոպա/Ազատություն» ռադիոկայանի հայկական ծառայության լրագրող է: 2020 թվականին լուսաբանել է Լեռնային Ղարաբաղի հակամարտությունը, իսկ 2021-ին՝ Հայաստանում կայացած արտահերթ խորհրդարանական ընտրությունները, որոնք մեծապես կենտրոնացած էին այդ հարցի վրա:[37]

Թեև «Apple»-ի ծանուցման մեջ նշված չէր, որ լրագրողի «iPhone»-ը վարակվել է, Աստղիկը լրջորեն վերաբերվեց նախազգուշացմանը՝ ստուգման համար հեռախոսը հանձնելով «CyberHub-AM»-ին: Հետևելով «CyberHUB-AM»-ի խորհրդին՝ «Ազատություն» ռադիոկայանի երևանյան բյուրոյի աշխատակիցների սմարթֆոնները ստուգվեցին «Amnesty Tech»-ի կողմից: Մանրազնին փորձաքննության ենթարկելով հեռախոսները՝ «Amnesty Tech»-ը հաստատեց

«Pegasus»-ի կիրառումը, որը տեղի է ունեցել 2021 թվականին՝ մոտավորապես հայաստանյան խորհրդարանական ընտրությունների ժամանակ: «Կոտրվել» էր նաև Բեդնյանի գործընկեր՝ «Ազատություն» ռադիոկայանի լրագրող Կարլեն Ասլանյանի հեռախոսը:

Հայաստանում «Pegasus»-ի կիրառման մասին առաջին փաստը արձանագրվել է 2021 թվականին, երբ լրտեսող ծրագիրը հայտնաբերվեց իշխանական և ընդդիմադիր հանրահայտ մի քանի գործիչների սարքերում:

Հարձակում գործողները «Pegasus»-ի միջոցով վարակել էին Արցախի Հանրապետության նախկին օմբուդսմենի, նախարարություններից մեկի խոսնակի, մի գիտնականի հեռախոսները:[38] Հետագայում պարզվեց, որ վարակված են եղել նաև մի հեռուստալրագրողի ու մի հանրաճանաչ իրավապաշտպանի սարքերը: Թիրախավորված այլ անձինք նախընտրեցին անանուն մնալ:

Թեպետ «Pegasus»-ը մշակած իսրայելական «NSO Group» ընկերությունը ծրագիրը վաճառում է միայն կառավարություններին, հնարավոր չէ հաստատապես ասել, թե ով է այս արշավի հետևում կանգնածը: Հայաստանում «Pegasus»-ի կիրառման մասին իր զեկույցում, սակայն, «Amnesty International»-ը վկայակոչում է մեծածավալ անուղղակի ապացույցներ, ըստ որոնց գրոհների հետքերը տանում են Ադրբեջան:[39] Ավելի վաղ «Citizen Lab»-ն էր տեղեկացրել, որ Ադրբեջանում գոյություն ունի «Pegasus»-ի կառավարման երկու կենտրոն՝ մեկը կենտրոնացած է երկրի ներսում առկա թիրախների ուղղությամբ, մյուսը՝ Հայաստանի դեմ:[40]

«Pegasus»-ով թիրախավորվելը լուրջ ազդեցություն է թողել Աստղիկ Բեդնյանի վրա, քանի որ հեռախոսում առկա էին նաև անձնական տվյալներ, այդ թվում՝ իր երեխաների մասին, որոնք, ամենայն հավանականությամբ, հասանելի են դարձել օտար պետությանը: «Զգում եմ, որ կոպիտ կերպով ներխուժել են իմ անձնական կյանք»,- ասել է նա «Access Now»-ին:[41]

«Pegasus»-ի վերաբերյալ վերլուծությունները, փաստագրումները հաճախ անտեսում են, որ այդ ծրագրով վարակված սարք ունենալը ավելի ծանր հետևանքներ է առաջացնում կանանց և խոցելի խմբերի դեպքում: Օրինակ, Ադրբեջանում իշխանությունների հասցեին սուր քննադատությամբ աչքի ընկնող մի գործչի կնոջ անձնական տվյալները՝ անունը, լուսանկարները և հեռախոսահամարը, հրապարակվել էին սոցիալական ցանցերում և էսկորտ ծառայություններ մատուցող կայքում: Իշխանամետ մամուլն օգտագործեց այդ արտահոսքը՝ նրա դեմ արշավ սկսելու համար: Թեև տեղի ունեցածն ակնհայտ կապ չուներ «Pegasus»-ի հետ, սակայն փաստերը վկայում են, որ այդ տեղեկությունները հափշտակվել էին կնոջ սմարթֆոնից:[42]

Լրացուցիչ ընթերցանության նյութեր

Քաղհասարակության կազմակերպությունները և լրագրողները հաճախ են բախվում նորագույն թվային խնդիրների՝ չունենալով դրանք հայտնաբերելու, վերլուծելու և կանխելու կարողություններ: Քաղհասարակության և լրատվամիջոցների առջև ծառացած նման սպառնալիքների վերլուծությունն է թույլ տալիս թվային անվտանգության մասնագետներին առավել արդյունավետ հակաքայլեր առաջարկել գործընկեր կազմակերպություններին՝ ձևավորելով նման ռիսկերը, սպառնալիքները նվազեցնող պատասխաններ, որոնք կարող են ընկալելի ու կիրառելի լինել քաղհասարակության և լրագրողական հանրության համար:

Թվային նման սպառնալիքների մասին տեղեկություններ տրամադրելու համար՝ «Internews»-ն ու գործընկերները հեղինակել են «Թվային սպառնալիքների համաշխարհային միտումները. քաղհասարակություն և լրատվամիջոցներ» զեկույցը, ինչպես նաև Բրազիլիայում, Մեքսիկայում, Սերբիայում և Ուկրաինայում թվային սպառնալիքների համայնապատկերների մասին հրապարակումները, որոնք հասանելի են «Internews»-ի կայքում:

Երախտիքի խոսք

2021 թվականից «Internews»-ն աշխատում է թվային սպառնալիքներով զբաղվող յոթ լաբորատորիաների հետ (Threat Labs. տեղական կազմակերպություններ, որոնք ունեն տեխնիկական կարողություններ և համապատասխան գործիքակազմ՝ վնասարար ծրագրերը վերլուծելու, թվային հարձակումների միտումների, ծագող սպառնալիքների և հակազդեցությունների մասին տեղեկություններ տրամադրելու համար)՝ արձագանքելու միջադեպերին, որոնք ազդում են ողջ աշխարհում քաղհասարակության և լրատվամիջոցների, լրագրողների թվային անվտանգության վրա: Միջադեպերին արձագանքելու միջոցով հավաքված տվյալները օգնել են մշակել ռիսկային գոտում գտնվողների համար սպառնալիքները նվազեցնող քայլեր:

«Internews»-ն իր երախտագիտությունն է հայտնում թվային սպառնալիքներով զբաղվող լաբորատորիաների համայնքին, որն աշխատել է մեզ հետ այս նախագծի վրա: Նրանք հանձնառու են օգնել կարիքավորներին և երաշխավորելու, որ քաղհասարակության, լրատվամիջոցների իրենց գործընկերները կկարողանան անվտանգ ու արդյունավետ կատարել իրենց աշխատանքը: Ընդհանուր առմամբ, այս ծրագրի աջակցությամբ՝ թվային սպառնալիքներով զբաղվող լաբորատորիաները արձագանքել են նմանատիպ ավելի քան 200 միջադեպեր և հրապարակել են կրթական ավելի 60 ուղեցույցներ:

Հատուկ շնորհակալություն ենք հայտնում «CyberHub-AM»-ին՝ այս զեկույցում նկարագրված օրինակների փաստագրման և հրապարակման համար, ինչպես նաև այս զեկույցի վերաբերյալ արժեքավոր նկատառումներ ներկայացնելու համար: Զեկույցն իրականություն չէր դառնա առանց Յանա Ղահրամանյանի, Սամվել Մարտիրոսյանի և Արթուր Պապյանի աջակցության:

Ծանոթագրություններ

[1] "Explainer: What is Nagorno-Karabakh and why are tensions rising?" *Al Jazeera.* April 24, 2023. https://www.aljazeera.com/news/2023/4/24/explainer-what-is-nagorno-karabakh-why-are-tensions-rising

[2] Ertl, Michael. "Nagorno-Karabakh: Conflict between Azerbaijan and Armenians explained." BBC News. September 28, 2023

[3] Bazail-Emil, Eric and Gabriel Gavin. "Blinken warned lawmakers Azerbaijan may invade Armenia in coming weeks." Politico. October 13, 2023. https://www.politico.com/news/2023/10/13/blinken-warned-lawmakers-azerbaijan-may-invade-armenia-in-coming-weeks-00121500

[4] Amiryan, Tigran and Anna Sokolova. "Relocated Russian Democracy - A View from Armenia." Heinrich Böll Stiftung. June 1, 2022. https://ge.boell.org/en/2022/06/01/relocated-russian-democracy-view-armenia

[5] Tatikyan, Sossi. "The Context Behind Armenia's UN Vote on Ukraine." *EVN Report*. March 3, 2022. https://evnreport.com/politics/the-context-behind-armenias-un-vote-on-ukraine/

[6] Atasuntsev, Alexander. "Long-Standing Ties Between Armenia and Russia Are Fraying Fast." Carnegie Endowment for International Peace. October 13, 2023. https://carnegieendowment.org/politika/90768

[7] "Freedom in the World 2023: Armenia." Freedom House. վերջին մուտքը՝ 2023թ. հուլիս https://freedomhouse.org/country/armenia/freedom-world/2023

[8] Նույն տեղում

[9] "Armenia." Reporters Without Borders. վերջին մուտքը՝ 2023թ. հուլիս. https://rsf.org/en/country/armenia.

[10] "Armenia must drop 'intimidating' criminal charges against minority rights activist – UN experts." United Nations, OHCHR Press Release. August 10, 2021. https://www.ohchr.org/en/press-releases/2021/08/armenia-must-drop-intimidating-criminal-charges-against-minority-rights

[11] Chilingaryan, Anahit. "High Stakes for Armenian Democracy in Rights Defender's Trial." Human Rights Watch. June 21, 2022. https://www.hrw.org/news/2022/06/21/high-stakes-armenian-democracy-rights-defenders-trial

[12] "Public opinion toward LGBT people in Yerevan, Gyumri and Vanadzor cities." We and Our Rights. 2011. https://issuu.com/pinkarmenia/docs/lgbtsurveyen/9?e=3748946/2746746

[13] "LGBT activist Mamikon Hovespyan announced as equality award winner for 2017." Equal Rights Trust. July 25, 2017. https://www.equalrightstrust.org/news/lgbt-activist-mamikon-hovespyan-announced-equality-award-winner-2017; Pilishvili, Catherine. "Another Change to Address Homophobic Violence in Armenia." Human Rights Watch. August 28, 2020. https://www.hrw.org/news/2020/08/28/another-chance-address-homophobic-violence-armenia

[14] "LGBT activist Mamikon Hovespyan announced as equality award winner for 2017," Equal Rights Trust.

[15] Papyan, Artur. "Internet penetration rate has declined in Armenia in 2020 according to ITU." *The Armenian Observer Blog*. October 16, 2020. https://ditord.com/2020/10/internet-penetration-rate-has-declined-in-armenia-in-2020/

[16] Ranum, Marcus J. "FUDwatch: Armenia." Tenable. May 3, 2013. https://www.tenable.com/blog/fudwatch-armenia

[17] "Russian spam mastermind jailed for creating botnet." *BBC*. May 24, 2012. https://www.bbc.com/news/technology-18189987

[18] “Armenia police warn of growing cybercrime rate.” *Armenpress*. վերջին փոփոխությունը՝ 2018թ. հունիսի 12. https://armenpress.am/eng/news/937066/

[19] “Armenian police bust Yerevan-based cybercrime syndicate targeting U.S. users via tech support scam.” *Armenpress*. վերջին փոփոխությունը՝ 2019թ. մայիսի 1. https://armenpress.am/eng/news/973297.html

[20] Faou, Matthieu. “Tracking Turla: New backdoor delivered via Armenian watering holes.” We Live Security, ESET Research. March 12, 2020. https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/

[21] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert. “Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus.” The Citizen Lab. July 15, 2021. https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

[22] Stone, Maddie and Clement Lecigne. “How we protect users from 0-day attacks.” Google, Threat Analysis Group. July 14, 2021. https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/

[23] Nimmo, Ben, David Agranovich, and Nathaniel Gleicher. “Quarterly Adversarial Threat Report.” Meta. April 2022. https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf

[24] Տեղեկությունը՝ CyberHub-AM-ի

[25] Միջադեպի արձագանքի վերաբերյալ տեղեկությունը՝ CyberHub-AM-ի

[26] Միջադեպի արձագանքի վերաբերյալ տեղեկությունը՝ CyberHub-AM-ի

[27] Dvilyanski, Mike, David Agranovich, and Nathaniel Gleicher. “Threat Report on the Surveillance-for-Hire Industry.” Meta. December 16, 2021. https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

[28] Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert. “Pegasus vs. Predator: Dissident’s Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware.” The Citizen Lab. December 16, 2021. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

[29] “Review of Attacks Against Armenian Telegram Users in Recent Months.” CyberHUB. վերջին փոփոխությունը՝ 2022թ. օգոստոսի 26. https://cyberhub.am/en/blog/2022/08/26/review-of-attacks-against-armenian-telegram-users-in-recent-months/

[30] “Arsen Babayan: How authorities infect victims’ phones with Pegasus spyware.” *Panorama*. Վերջին փոփոխությունը՝ 2021թ. նոյեմբերի 27. https://www.panorama.am/en/news/2021/11/27/Arsen-Babayan/2604970

[31] Krapiva, Natalia, and Giulio. “Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict.” Access Now. May 25, 2023. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/

[32] RFE/RL. “Azerbaijan Suspected Of Spying On Reporters, Activists By Using Software To Access Phones.” RadioFreeEurope RadioLiberty. վերջին փոփոխությունը՝ 2021թ. հուլիսի 18. https://www.rferl.org/a/azerbaijan-pegasus-spying-nso/31365076.html

[33] Muhammad, Rafie. “Critical Privilege Escalation in Essential Addons for Elementor Plugin Affecting 1+ Million Sites.” Patchstack. վերջին փոփոխությունը՝ 2023թ. մայիսի 11. https://patchstack.com/articles/critical-privilege-escalation-in-essential-addons-for-elementor-plugin-affecting-1-million-sites/

[34] Martin, Ben. “Vulnerability in Essential Addons for Elementor Leads to Mass Infection.” *SucriBlog*. վերջին փոփոխությունը՝ 2023թ. մայիսի 18. https://blog.sucuri.net/2023/05/vulnerability-in-essential-addons-for-elementor-leads-to-mass-infection.html

[35] “Hackers leverage vulnerability of Essential Addons plugin to exploit Armenian WordPress sites.” CyberHUB. վերջին փոփոխությունը 2023թ. մայիսի 23. https://cyberhub.am/en/blog/2023/05/23/hackers-leverage-vulnerability-of-the-essential-addons-plugin-to-exploit-armenian-wordpress-sites/

[36] "Armenia: Azerbaijan Hacks Armenian Journalist Astghik Bedevyan’s Phone During War.” Coalition For Women in Journalism. May 29, 2023. https://www.womeninjournalism.org/threats-all/armenia-azerbaijan-hacks-armenian-journalist-astghik-bedevyans-phone-during-war

[37] “Armenia PM Pashinyan’s Civil Contract claims victory in snap poll.” *Al Jazeera.* June 21, 2021. https://www.aljazeera.com/news/2021/6/21/armenia-nikol-pashinyan-claims-victory-in-snap-polls

[38] Krapiva, Natalia, and Giulio. “Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict.” Access Now. May 25, 2023. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/

[39] “Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict.” Amnesty International. May 25, 2023. https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/

[40] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Nicola Lawford, and Ron Deibert. “Armenia-Azerbaijan conflict: Pegasus infections – Technical Brief [1].” The Citizen Lab. May 25, 2023. https://citizenlab.ca/2023/05/cr1-armenia-pegasus/

[41] Krapiva, “Hacking in a war zone: Pegasus spyware in Azerbaijan-Armenia conflict.”

[42] Patrucic, Miranda and Kelly Bloss. “Life in Azerbaijan’s Digital Autocracy: ‘They Want to be in Control of Everything.’” Organized Crime and Corruption Reporting Project. July 18, 2021. https://www.occrp.org/en/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything