www.mdi.com

Media Diversity Institute

CyberHUB

ՀԱՅԱՍՏԱՆ. ԹՎԱՅԻՆ ՍՊԱՌՆԱԼԻՔՆԵՐԻ ՀԱՄԱՊԱՏԿԵՐԸ

2023

Լրտեսող ծրագրերի վերահսկման նախաձեռնություն

Հրապարակվել է՝ 2024թ.

www.cyberhub.am

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

03

ՆԵՐԱԾՈՒԹՅՈՒՆ

Թվային անվտանգության համատեքստում Հայաստանն աչքի է ընկել մի քանի պատճառներով. երկիրը ենթարկվել է այլ պետությունների կողմից հովանավորվող կիբերհարձակումների, այդ թվում՝ NSO Group-ի Pegasus լրտեսող ծրագրի միջոցով, որը կիրառվել է Լեռնային Ղարաբաղում, հայ-ադրբեջանական հակամարտության ժամանակ: Աշխարհաքաղաքական համապատկերը է՛լ ավելի է բարդանում համաշխարհային այնպիսի կիբերտերությունների ներգրավմամբ, ինչպիսիք են Ռուսաստանը, Իրանը և Իսրայելը, որը ծառայություններ է մատուցում Ադրբեջանին: Այս երկրները, ինչպես հայտնի է, ակտիվ գործունեություն են ծավալում Հայաստանի ներսում՝ գրգռելով առանց այն էլ լարված կիբերմիջավայրը:

Սույն զեկույցում ներկայացված են Հայաստանում քաղաքացիական հասարակության և լրագրողների առջև ծառացած սպառնալիքները, ինչպես նաև՝ արժեքավոր դիտարկումներ կիբեռանվտանգության փորձագետների համար: Խոշոր տեխնոլոգիական ընկերությունները, ինչպիսիք են Google-ը, Microsoft-ը, Meta-ն և Apple-ը, հրապարակել են զեկույցներ՝ մատնանշելով Հայաստանը թիրախավորած տարատեսակ կիբեռհարձակումներ: Այս զեկույցներն ընդգծում են, որ զգայուն տվյալների և ենթակառուցվածքների պաշտպանության համար անհրաժեշտ են կիբեռանվտանգության ուժեղացված հրատապ միջոցառումներ:

Բացի այդ, Հայաստանը, իբրև թվային վերափոխման իր նախաձեռնությունների բաղկացուցիչ, ընդունել է կառավարության հավանությանն արժանացած ռազմավարություն, որի առանցքում նորարարական տեխնոլոգիաները, կիբեռանվտանգությունը և էլեկտրոնային ծառայություններն են: Չնայած համակարգային թերություններին՝ երկիրն ընդունում է կիբեռանվտանգության կարևորությունը օրեցօր ավելի փոխկապակցվող աշխարհում:

Կիբեռհանցագործությունների սրընթաց աճը հրամայական է դարձրել Հայաստանի կիբեռանվտանգության մեխանիզմների հզորացումը և առցանց տիրությում աճող վտանգների մասին հանրային իրազեկվածության բարձրացումը: Շատ կիբեռհանցագործ խմբեր կիրառում են խիստ զարգացած մեթոդներ և թիրախավորում ինչպես անհատներին, այնպես էլ ձեռնարկություններին՝ օգտագործելով ֆիշինգ, դրամաշորթ վիրուսներ (անգլ.՝ ransomware) և այլ խափանող մարտավարություններ: Հաշվի առնելով նման զարգացումները՝ ազգային կիբեռանվտանգության համապարփակ միջոցառումների անհրաժեշտությունը գնալով ավելի օրախնդիր է դառնում ինչպես ներքին, այնպես էլ արտաքին կիբեռսպառնալիքներին հակազդելու համար:

Սույն զեկույցը պատրաստել է Բազմակողմանի տեղեկատվության ինստիտուտի **CyberHUB-AM** թիմը՝ Լրտեսող ծրագրերի վերահսկման նախաձեռնության (անգլ.՝ Spyware Accountability Initiative, SAI) աջակցությամբ:

CyberHUB-AM-ը Հայաստանի քաղաքացիական հասարակության՝ ՀԿ-ների, իրավապաշտպանների, ակտիվիստների, լրագրողների և անկախ լրատվամիջոցների համար SS աջակցման կենտրոն է և սպառնալիքների հետաքննության լաբորատորիա: Հայաստանյան վերոնշյալ խմբերի համար այն ծառայում է որպես կոնտակտային և աջակցման կենտրոն՝ հավաքելով, վերլուծելով և, անհրաժեշտության դեպքում, պատասխանատու և անանուն կերպով գլոբալ սպառնալիքների հետախուզությամբ զբաղվող համայնքին փոխանցելով միջադեպերի տվյալները և սպառնալիքների ցուցիչները:

Բազմակողմանի տեղեկատվության ինստիտուտ-Հայաստանը (ԲՏԻ-Հայաստան) շահույթ չհետապնդող, ոչ կառավարական կազմակերպություն է, որը փորձում է

օգտագործել ավանդական լրատվամիջոցների, սոցիալական մեդիայի և նոր տեխնոլոգիաների ընձեռած հնարավորությունները՝ մարդու իրավունքների պաշտպանության, ժողովրդավարական քաղաքացիական հասարակության կայացմանն աջակցելու, հասարակության անտեսված շերտերի ձայնը լսելի դարձնելու և սոցիալական բազմազանության տարբեր տեսակների կոլեկտիվ ընկալումն ուժեղացնելու համար: ԲՏԻ-Հայաստանը հիմնվել է 2006 թվականի ապրիլի 18-ին: 2018 թվականից ԲՏԻ-Հայաստանը սկսել է ավելի ակտիվորեն զբաղվել թվային անվտանգության, ապատեղեկատվության և ակնհայտ կեղծ տեղեկատվության բացահայտման տեխնոլոգիաներով՝ SS աուդիտի, ռիսկերի գնահատման, տրիաժի (աջակցության գերակայությունների որոշման) և անվտանգության հետ կապված միջադեպերի արձագանքման ծառայություններ մատուցելով հայկական տասնյակ ազդեցիկ իրավապաշտպան կազմակերպությունների, մեդիա ընկերությունների, ակտիվիստների, լրագրողների:

06

ԸՆԴՀԱՆՈՒՐ ՏԵՂԵԿՈՒԹՅՈՒՆՆԵՐ

Քաղաքական համատեքստը, քաղհասարակությունը և լրատվամիջոցները
Կիբեռանվտանգությունը Հայաստանում

Հայաստանը մշտապես տարբեր մակարդակների կիբեռսպառնալիքների ենթակա երկիր է: Աշխարհաքաղաքական իրավիճակը, Ադրբեջանի (որին ռազմական և քաղաքական աջակցություն է ցուցաբերում Թուրքիան) հետ շարունակվող ռազմական հակամարտությունը, Ռուսաստանի հետ վատթարացող հարաբերությունները և բազմաթիվ այլ գործոններ աշխարհի տարբեր պետությունների կողմից հովանավորվող հաքերային խմբերի համար հայկական կիբեռտարածքը դարձնում են դյուրին թիրախ: Այս սպառնալիքները գալիս են բազմաթիվ ուղղություններից՝ նպատակ ունենալով օգտվել Հայաստանի թվային ենթակառուցվածքների խոցելիությունից՝ լուրջ խնդիրներ առաջացնելով երկրի անվտանգության համար:

Հայաստանի թվային համապատկերում շարունակում է աճել նաև կիբեռհանցագործությունը: Որքան էլ տարօրինակ է, Ուկրաինա լայնամասշտաբ ներխուժման ծավալումը՝ զուգորդված Ռուսաստանից Հայաստան փախստականների զգալի ներհոսքի հետ, նպաստել է տարբեր տեսակի կիբեռխարդախությունների աճին: Ռուսաստանից և հետխորհրդային այլ երկրներից տեղափոխվող բնակչությանն ուղեկցել են թվային խարդախությունների և տարատեսակ խաբեբայական գործողությունների սխեմաները՝ ամրապնդվելով Հայաստանի առցանց միջավայրում:

Կիբեռհանցագործությունների սրընթաց աճը հրամայական է դարձրել Հայաստանի կիբեռանվտանգության մեխանիզմների հզորացումը և առցանց տիրությում աճող վտանգների մասին հանրային իրազեկվածության բարձրացումը: Շատ կիբեռհանցագործ խմբեր կիրառում են խիստ զարգացած մեթոդներ և թիրախավորում ինչպես անհատներին, այնպես էլ ձեռնարկություններին՝ օգտագործելով ֆիշինգ, դրամաշորթ վիրուսներ (անգլ.՝ ransomware) և այլ վնասարար մարտավարություններ: Հաշվի առնելով նման զարգացումները՝ ազգային

07

ԸՆԴՀԱՆՈՒՐ ՏԵՂԵԿՈՒԹՅՈՒՆՆԵՐ

Քաղաքական համատեքստը, քաղհասարակությունը և լրատվամիջոցները
Կիբեռանվտանգությունը Հայաստանում

Հայաստանը մշտապես տարբեր մակարդակների կիբեռսպառնալիքների ենթակա երկիր է: Աշխարհաքաղաքական իրավիճակը, Ադրբեջանի (որին ռազմական և քաղաքական աջակցություն է ցուցաբերում Թուրքիան) հետ շարունակվող ռազմական հակամարտությունը, Ռուսաստանի հետ վատթարացող հարաբերությունները և բազմաթիվ այլ գործոններ աշխարհի տարբեր պետությունների կողմից հովանավորվող հաքերային խմբերի համար հայկական կիբեռտարածքը դարձնում են դյուրին թիրախ: Այս սպառնալիքները գալիս են բազմաթիվ ուղղություններից՝ նպատակ ունենալով օգտվել Հայաստանի թվային ենթակառուցվածքների խոցելիությունից՝ լուրջ խնդիրներ առաջացնելով երկրի անվտանգության համար:

Հայաստանի թվային համապատկերում շարունակում է աճել նաև կիբեռհանցագործությունը: Որքան էլ տարօրինակ է, Ուկրաինա լայնամասշտաբ ներխուժման ծավալումը՝ զուգորդված Ռուսաստանից Հայաստան փախստականների զգալի ներհոսքի հետ, նպաստել է տարբեր տեսակի կիբեռխարդախությունների աճին: Ռուսաստանից և հետխորհրդային այլ երկրներից տեղափոխվող բնակչությանն ուղեկցել են թվային խարդախությունների և տարատեսակ խաբեբայական գործողությունների սխեմաները՝ ամրապնդվելով Հայաստանի առցանց միջավայրում:

Կիբեռհանցագործությունների սրընթաց աճը հրամայական է դարձրել Հայաստանի կիբեռանվտանգության մեխանիզմների հզորացումը և առցանց տիրությում աճող վտանգների մասին հանրային իրազեկվածության բարձրացումը: Շատ կիբեռհանցագործ խմբեր կիրառում են խիստ զարգացած մեթոդներ և թիրախավորում ինչպես անհատներին, այնպես էլ ձեռնարկություններին՝ օգտագործելով ֆիշինգ, դրամաշորթ վիրուսներ (անգլ.՝ ransomware) և այլ վնասարար մարտավարություններ: Հաշվի առնելով նման զարգացումները՝ ազգային

կիբեռանվտանգության համապարփակ միջոցառումների անհրաժեշտությունը գնալով ավելի օրախնդիր է դառնում ինչպես ներքին, այնպես էլ արտաքին կիբեռսպառնալիքներին հակազդելու համար:

Իր աշխարհաքաղաքական դիրքավորման պատճառով Հայաստանը կիբեռանվտանգության ոլորտի կառավարման հարցում յուրահատուկ մարտահրավերի առջև է կանգնած: Մշտական կոնֆլիկտային վիճակը, տարածաշրջանային լարվածությունը և փոփոխվող դաշինքները երկիրը դնում են խոցելի վիճակում ինչպես ֆիզիկական, այնպես էլ թվային առումով: Այս սպառնալիքներին հակազդելու նպատակով Հայաստանը պետք է համագործակցի միջազգային ասպարեզում՝ իր կիբեռպաշտպանությունը բարելավելու, առանցքային ենթակառուցվածքների անվտանգությունն ապահովելու և իր քաղաքացիներին կիբեռսպառնալիքների և հարձակումների աճող ալիքից պաշտպանելու համար:

Որպես Հայաստանի առջև ծառացած սպառնալիքի վառ օրինակ՝ կարելի է նշել 2023 թվականը, երբ Հայաստանը քաղաքական գործիչների, լրատվամիջոցների և քաղաքացիական հասարակության թիրախավորման նպատակով օգտագործվող Pegasus լրտեսող ծրագրի հայտնաբերմամբ դարձավ թվային անվտանգության առումով ամենաքննարկվող երկրներից մեկը: Լրտեսող ծրագիրը կապված է եղել Ադրբեջանի կառավարության հետ՝ ըստ էության իրենից ներկայացնելով առաջին դեպքը, երբ Pegasus-ը օգտագործվում էր միջազգային հակամարտությունների համատեքստում: Հայաստանի և Ադրբեջանի միջև շարունակվող հակամարտությունը երկար ժամանակ առանցքային է եղել երկու երկրների քաղաքականության համար և բազմիցս հանգեցրել է պատերազմների: Թեև լրատվամիջոցներն իրենց լուսաբանումներում կենտրոնացել են լրտեսող ծրագրերի վրա, սակայն Հայաստանում քաղաքացիական հասարակությունը բախվում է նաեւ թվային անվտանգության մի շարք այլ սպառնալիքների:

Քաղաքական համատեքստը, քաղհասարակությունը և լրատվամիջոցները

Եվրոպայի հետ ամուր հարաբերություններին զուգահեռ՝ Հայաստանը սերտորեն կապված է նաև Ռուսաստանի հետ: Ռուսերենը ամենատարածված օտար լեզուն է, և ռուսներն առանց վիզայի կարող են այցելել Հայաստան: Ռուսաստանը նաև ռազմական ներկայություն ունի Հայաստանում՝ Ռուսաստանի 102-րդ ռազմակայանը Գյումրիում և խաղաղապահ ուժերը հայ-ադրբեջանական սահմանին և Լեռնային Ղարաբաղում: Ռուսաստանի՝ 2022 թվականին Ուկրաինա ներխուժումից հետո մեծ թվով ռուս SS և տեխնոլոգիական աշխատողներ, ինչպես նաև Ռուսաստանի քաղաքացիական հասարակության ներկայացուցիչներ և լրագրողներ տեղափոխվել են Հայաստան: Չնայած այս կապերին՝ համաշխարհային ասպարեզում Հայաստանը դժվարին իրավիճակում է հայտնվել. 2022 թվականին Հայաստանը ձեռնպահ է քվեարկել ՄԱԿ-ի բանաձևին, որը Ռուսաստանից պահանջում էր դադարեցնել ռազմական գործողությունները և դուրս գալ Ուկրաինայի տարածքից:

Աշխարհաքաղաքական համապատկերի ընթացիկ փոփոխություններն էլ ավելի են բարդացրել Հայաստանի անվտանգության մարտահրավերները: Ադրբեջանի հետ շարունակվող հակամարտությունը, որի խորացմանը նպաստում է Թուրքիայի կողմից Ադրբեջանին ցուցաբերվող ռազմական և քաղաքական աջակցությունը, Հայաստանը խոցելի է դարձրել ինչպես ֆիզիկական, այնպես էլ թվային սպառնալիքների առումով: 2023 թվականին Հայաստանը քաղաքական գործիչների, լրատվամիջոցների և քաղաքացիական հասարակության թիրախավորման նպատակով օգտագործվող Pegasus լրտեսող ծրագրի հայտնաբերմամբ հայտնվեց թվային անվտանգությանն առնչվող քննարկումների առանցքում. սա միջազգային հակամարտությունում Pegasus-ի կիրառման առաջին

դեպքն էր: Այս իրադարձություններն ընդծում են այն փաստը, որ Հայաստանին անհրաժեշտ է հրատապ կերպով բարելավել իր կիբեռպաշտպանությունը և համագործակցել միջազգային ասպարեզում՝ ապահովելու համար իր թվային ենթակառուցվածքների անվտանգությունը և իր քաղաքացիներին պաշտպանելու անվտանգության բազմաշերտ սպառնալիքներից:

Հայաստանի քաղաքացիական հասարակությունը և լրատվամիջոցները հիմնականում ազատորեն գործելու հնարավորություն ունեն: Քաղաքացիական հասարակությունն ակտիվ մասնակցություն է ունեցել 2018 թվականի բողոքի ցույցերին, որոնք հանգեցրին իշխանափոխության:[1] 2021 թվականին խստացվեց զրպարտության և վիրավորանքի համար պատասխանատվությունը, ինչն օգտագործվում էր լրագրողներին պատասխանատվության ենթարկելու համար: Այնուամենայնիվ, ներքին և միջազգային բողոքի ալիքով պայմանավորված, 2022 թվականին խստացումը չեղարկվեց:[2] Խտրականության դեմ համապարփակ օրենքների բացակայությունը և էթնիկ փոքրամասնությունների և ԼԳԲՏՔ+ համայնքի հանդեպ խտրականությունն ավելի են խորացնում քաղաքացիական ազատությունների անկայուն վիճակը Հայաստանում:

Կիբեռանվտանգությունը Հայաստանում

Ըստ Հայաստանի ոստիկանության տվյալների՝ 2018 թվականին կիբեռհանցագործությունների 20-25% աճ է արձանագրվել: Կիբեռհանցագործության հիմնական տեսակը ֆինանսական ռեսուրսների հափշտակումն է, հատկապես՝ բանկային գործարքները և բանկային քարտերից գումարի հափշտակումը:[3] Հանցագործները բանկային տվյալները հափշտակելու նպատակով հաճախ կիրառում են սոցիալական ցանցերը: 2019 թվականին հայերից և հնդիկներից բաղկացած կազմակերպված հանցավոր խմբավորումը

տեխնիկական աջակցության խոշոր խարդախություն է իրականացրել՝ թիրախավորելով ԱՄՆ-ի և Կանադայի օգտատերերի:[4]

Երկրում լայն տարածում ունեն Telegram և WhatsApp մեսենջերները, որոնց օգտատերերը հաճախ խարդախությունների և հաքերային հարձակումների թիրախ են դառնում: Չարամիտ մղումներով հաղորդագրությունները հաճախ գրվում են ռուսերեն, և որոշ օգտատերեր կարող են Ռուսաստանի քաղաքացիներին թիրախավորող արշավների անուղղակի զոհ դառնալ:

2021 թվականին լրտեսող ծրագրերի մատակարար իսրայելական Candiru ընկերության ծրագրով թիրախավորված մարդկանց շարքում նշվում էին են նաև հայաստանցիներ: Այդ հարձակման ժամանակ կիրառվել են ծրագրային ապահովման՝ զրո օրվա խոցելիությունները (անգլ.՝ zero-day vulnerabilities), որոնք կիրառման պահին անհայտ էին ծրագրային ապահովում իրականացնող տուժած ընկերությանը:[5] Մոտավորապես նույն ժամանակ Google-ը հայտարարեց, որ Հայաստանում թիրախները ստացել են Google Chrome-ի՝ զրո օրվա խոցելիությունները օգտագործող հղումներով նամակներ:[6]

2022 թվականին հակառակորդի սպառնալիքների մասին զեկույցում Meta-ն հայտնել է վնասարար ծրագրերի (անգլ.՝ malware) և ֆիշինգի, ինչպես նաև կեղծ օգտահաշիվների և կայքերի կիրառմամբ ադրբեջանական գործողության մասին:[7] Հարձակումը, Ադրբեջանի ներսում շատերին թիրախավորելուց զատ, թիրախավորել է նաև Հայաստանում որոշ անհատների:

2023 թվականի սեպտեմբերին ESET-ը հայտնել էր ռուսական APT28 հաքերային խմբի կողմից Ուկրաինայի, Հայաստանի և Տաջիկստանի կառավարական հաստատությունների դեմ ուղղված թիրախավորված հարձակումների մասին: 2023

թվականի հունիսին ESET-ը հայտնաբերեց թիրախավորված ֆիշինգի (անգլ.՝ spear phishing) արշավների մի խումբ (այն անվանելով Operation RoundPress), որն օգտվում էր Roundcube-ում XSS խոցելիությունից: Օգտագործելով այս խոցելիությունը՝ հարձակում գործողներն ունակ են վնասակար JavaScript կոդը ներդնել տուժողի Roundcube վեբ փոստի սերվերում: Ներդրված կոդը ի վիճակի է հափշտակել նամակներ, հասցեագրքեր և ստեղծել վերահասցեավորման կանոններ՝ ստացվող նամակները հափշտակելու համար: Ըստ ESET-ի հեռաչափման տվյալների՝ Operation RoundPress-ի թիրախում Հայաստանի, Տաջիկստանի և Ուկրաինայի կառավարությունների աշխատակիցներն են եղել. [**աղբյուր**]

Հարկ է նշել, որ Հայաստանում գործում էին Ռուսաստանի պետական կառույցներին փոխկապակցված տարբեր խմբեր, այդ թվում՝ Անվտանգության դաշնային ծառայության (ռուս.՝ ՓՀԵ) հետ կապված Turla-ն և Գլխավոր հետախուզական վարչությանը (ռուս.՝ ԳՐՈՒ) վերագրվող Ember Bear խումբը. [**աղբյուր**]

Բազմաթիվ սպառնալիքներ բխում են Ադրբեջանի հետ փոխկապակցված խմբերից: Օրինակ՝ 2022 թվականի հոկտեմբերին ադրբեջանցի հաքերները տիրացել էին հնացած ծրագրային ապահովմամբ աշխատող հայկական մի հոսթինգ պրովայդերի՝ խափանելով դրա վրա գործող բոլոր կայքերը, որոնցից երկուսը տեղական հասարակական կազմակերպությունների կայքեր էին: Թուրքական խմբերը ևս հաճախ թիրախավորում են հայկական կայքերը:

Վարձու լրտեսող ծրագրեր

Վարձու լրտեսող ծրագրերը մասնավոր ընկերությունների կողմից մշակված օգտատերերին վերահսկելու խիստ զարգացած ծրագրեր են, որ վաճառվում են կառավարություններին կամ այլ կառույցներին, որոնք սովորաբար առնչություն ունեն իրավապահ մարմինների հետ: Ի տարբերություն պետության կողմից հովանավորվող ավանդական լրտեսող ծրագրերի՝ վարձու լրտեսող ծրագրերը օրինական կերպով վաճառվում են՝ հաճախ կիրառվելով թիրախավորելու համար կոնկրետ անձանց, ինչպիսիք են թմրանյութերի վաճառքով զբաղվողները, ահաբեկիչները, հանցագործները: *Citizenlab*-ի, *Amnesty International*-ի, *AccessNow*-ի, *Forbidden Stories*-ի և այլ կազմակերպությունների հետաքննությունները ցույց են տվել, որ վարձու լրտեսող ծրագրերը հաճախ կիրառվում են ոչ ըստ իրենց բուն նպատակի՝ թիրախավորելով նաև քաղաքական այլախոհների, լրագրողների, իրավապաշտպանների և այլ ճանաչված դեմքերի: Լրտեսող ծրագրերի այս տեսակը կարող է օգտվել սարքերի խոցելիությունից՝ անձնական տվյալներին, հաղորդակցություններին չարտոնված հասանելիություն ստանալու և անգամ սարքի տեսախցիկի և խոսափողի նկատմամբ վերահսկողություն ձեռք բերելու համար: Հայտնի օրինակներից է *NSO Group*-ի կողմից մշակված *Pegasus* լրտեսող ծրագիրը, որն օգտագործվել է բազմաթիվ աղմկահարույց դեպքերում՝ գաղտնի հսկողություն իրականացնելու համար:

Access Now-ի, CyberHUB-AM-ի, Citizen Lab-ի, Amnesty International-ի անվտանգության լաբորատորիայի և անկախ հետազոտող Ռուբեն Մուրադյանի համատեղ հետաքննությունը՝ հրապարակած 2023 թվականի մայիսին,[8] բացահայտել է Ադրբեջանի և Հայաստանի միջև հակամարտության ընթացքում Հայաստանի քաղաքացիական հասարակության դեմ NSO Group-ի Pegasus լրտեսող ծրագրի կիրառման դեպքեր: Հետաքննությունը պարզել է, որ առնվազն 12 անձ, այդ

թվում լրագրողներ, մարդու իրավունքների պաշտպաններ և ՄԱԿ-ի մեկ պաշտոնյա, 2020 թվականի հոկտեմբերից մինչև 2022 թվականի դեկտեմբերն ընկած ժամանակահատվածում Pegasus լրտեսող ծրագրի թիրախ են դարձել:
Լրտեսող ծրագրերով վարակման դեպքերը կապված են եղել Լեռնային Ղարաբաղի հակամարտության նշանակալից այնպիսի իրադարձությունների հետ, ինչպիսիք են 2020 թվականի պատերազմը, դրան հաջորդած խաղաղ բանակցությունները և Լաչինի միջանցքի շարունակվող շրջափակումը: Pegasus-ի զոհերի թվում են այնպիսի բարձրաստիճան դեմքեր, ինչպիսիք են Հայաստանի մարդու իրավունքների նախկին պաշտպան Քրիստինե Գրիգորյանը և Հայաստանի արտաքին գործերի նախարարության նախկին խոսնակ Աննա Նաղդալյանը:

Հետաքննությունը սկսվել է այն բանից հետո, երբ 2021 թվականի նոյեմբերին Apple-ը օգտատերերին ծանուցել է պետության կողմից հովանավորվող լրտեսող ծրագրերի կիրառմամբ հնարավոր թիրախավորման մասին: Դրանից հետո Հայաստանի քաղաքացիական հասարակության մի քանի ներկայացուցիչներ օգնության համար դիմել են CyberHUB-AM-ին և Access Now-ի թվային անվտանգության հարցերով աջակցման կենտրոնին: Փորձաքննությամբ հաստատվել են վարակման բազմաթիվ դեպքեր՝ ընդգծելով միջազգային այս հակամարտությունում Pegasus լրտեսող ծրագրի լայն կիրառման փաստը:

Վարձու լրտեսող ծրագրեր

Ֆիշինգը կիբեռհարձակման այն տեսակն է, երբ հարձակում գործողները ներկայանում են իբրև վստահելի կազմակերպություններ կամ անձինք՝ անհատներին այնպես մոլորեցնելով, որ վերջիններս իրենց տրամադրեն գաղտնի տեղեկություններ՝ գաղտնաբառեր, կրեդիտային քարտերի համարներ կամ անձնական տվյալներ: Այս հարձակումները

հաճախ տեղի են ունենում էլեկտրոնային փոստի, հաղորդագրությունների կամ կայքերի միջոցով, որոնք վստահելի աղբյուրի պատրանք են ստեղծում, սակայն իրականում խաբեբաներ են: Նպատակն է՝ զոհերին մոլորեցնելով ստիպել սեղմել չարամիտ հղումների վրա կամ ներբեռնել կցված վնասակար ֆայլերը, ինչը հանգեցնում է տվյալների արտահոսքի, ֆինանսական կորստի կամ անձնական տվյալների հափշտակման: Ֆիշինգը օգտվում է մարդու հոգեբանությունից՝ շտապողականության, շփոթմունքի, վախի կամ հետաքրքրասիրության զգացմունքների վրա ազդելու միջոցով թիրախներին դրդելով արագ, չմտածված գործողությունների:

2023 թվականի ընթացքում Հայաստանում մի քանի կազմակերպություններ ֆիշինգային հարձակումների զոհ են դարձել, ինչը վկայում է տարածաշրջանում կիբեռհանցագործությունների աճող սպառնալիքի մասին:

Գյումրու Կանանց իրավունքների տունը թիրախավորվել է ֆիշինգային արշավի կողմից, որը, վստահելի հաղորդակցության պատրանք ստեղծելով, նպատակ է ունեցել հափշտակելու զգայուն տեղեկություններ: Այս հարձակումը խաթարել է նրանց գործունեությունը՝ մտահոգություն առաջացնելով կազմակերպության կողմից պահվող անձնական տվյալների անվտանգության վերաբերյալ:

Նմանապես, «Պահապան» հիմնադրամը ենթարկվել է ֆիշինգային հարձակման Facebook-ում, որտեղ հարձակում գործողները, կեղծ հաղորդագրությունների օգտագործմամբ աշխատակիցներին մոլորեցնելով, նրանց ստիպել են հայտնել իրենց մուտքի տվյալները: Այս հարձակման հետևանքով չարագործները հիմնադրամի ֆեյսբուքյան էջ չարտոնված մուտքի հնարավորություն են ստացել, ինչը վտանգի տակ է դրել զգայուն տեղեկությունները և վնաս հասցրել կազմակերպության առցանց ներկայությանը:

Facebook-ում ֆիշինգային հարձակման է բախվել նաև Կանանց ռեսուրսային կենտրոնը, որի դեպքում կիբեռհանցագործները մոլորեցնող հաղորդագրություններ են ուղարկել կազմակերպության աշխատակիցներին՝ արդյունքում տիրանալով նրանց ֆեյսբուքյան օգտահաշվին: Այս միջադեպի հետևանքով ոչ միայն խաթարվել է կենտրոնի գործունեությունը սոցիալական ցանցում, այլև վտանգի տակ է դրվել կազմակերպության աջակիցների և շահառուների գաղտնիությունն ու անվտանգությունը:

Facebook-ում ֆիշինգային մեկ այլ հարձակման զոհ է դարձել «Շանթ» հեռուստաընկերությունը: Հարձակում գործողները բարդ սխեմա են կիրառել աշխատակիցներին մոլորեցնելու և ֆեյսբուքյան էջի իրենց մուտքի տվյալները տրամադրել ստիպելու համար, ինչի հետևանքով նրանք ժամանակավորապես կորցրել են վերահսկողությունը իրենց էջի նկատմամբ: Այս միջադեպն ի ցույց դրեց մեդիա կազմակերպությունների՝ կիբեռսպառնալիքների նկատմամբ խոցելիությունը և կիբեռանվտանգության վճռական միջոցառումների կարևորությունը:

Վերջին դեպքը «Բժիշկների միավորում» ՀԿ-ի վրա ֆիշինգային հարձակումն էր, որի հետևանքով նրանք կորցրել էին իրենց ֆեյսբուքյան էջ մուտք գործելու հնարավորությունը: Հարձակում գործողները կեղծ հաղորդագրություններ էին ուղարկել՝ պնդելով, որ դրանք Facebook-ի աջակցման թիմից են՝ այդպիսով ՀԿ-ի խաբված աշխատակիցներին ստիպելով հայտնել իրենց մուտքի տվյալները: Այս հարձակումը ոչ միայն ազդել է հասարակական կազմակերպության առցանց ներկայության վրա, այլև մտահոգություն է առաջացրել դրա անդամներին առնչվող զգայուն տեղեկությունների հնարավոր ոչ իրավաչափ օգտագործման վերաբերյալ:

DDoS հարձակումներ

«Բաշխված ծառայությունների ժխտում» (անգլ.՝ *Distributed Denial-of-Service, DDoS*) տեսակի հարձակումը թիրախավորված սերվերի, ծառայության կամ ցանցի բնականոն տրաֆիկը խաթարելու չարամիտ փորձ է՝ թիրախի ծանրաբեռնման կամ դրա շուրջ գտնվող ենթակառուցվածքները ինտերնետ տրաֆիկով հեղեղելու միջոցով: Այս գերծանրաբեռնվածությունն առաջացնում են բազմաթիվ վարակված համակարգերը (որոնց հաճախ անվանում են բոտնետ): Այն կարող է դրսևորվել տարբեր կերպ, օրինակ՝ մեծ ծավալի տրաֆիկ՝ նախատեսված թողունակությունը սպառելու համար, կամ վնասված տվյալներով փաթեթներ՝ միտված օգտվելու խոցելիություններից: *DDoS* հարձակման վերջնական նպատակը թիրախ հանդիսացող ռեսուրսը իրական օգտագործողների համար անհասանելի դարձնելն է:

«Բաշխված ծառայությունների ժխտում» (DDoS) տեսակի հարձակումները Հայաստանում գնալով ավելի լայն տարածում են ստանում հատկապես հայ-ադրբեջանական շարունակվող հակամարտության և ներքաղաքական պայքարի համատեքստում: Այս կիբեռհարձակումները հաճախ օգտագործվում են որպես տեղեկատվությունը ճնշելու և լրատվամիջոցների, քաղաքացիական հասարակության կազմակերպությունների և կառավարական հաստատությունների գործունեությունը խաթարելու գործիքներ: Հակամարտության նշանակալիությունը և դրա վիճելի բնույթը մեծացնում են այս հարձակումների հաճախականությունն ու ուժգնությունը՝ կիբեռանվտանգությունը դարձնելով կարևոր խնդիր բոլոր կողմերի համար:

2023 թ. հոկտեմբերի 24-ին և 25-ին հայկական հայտնի ընդդիմադիր Hraparak.am լրատվամիջոցը ենթարկվել է ագրեսիվ DDoS հարձակման: Հարձակումը սկսվել է հոկտեմբերի 24-ին, և կայքը 12 ժամվա ընթացքում

ստացել է 1,5 միլիարդ հարցում: Հետագայում չարագործները պարզել են ուժեղացման URL հասցեները և համապատասխանաբար վերահասցեագրել իրենց հարցումները:

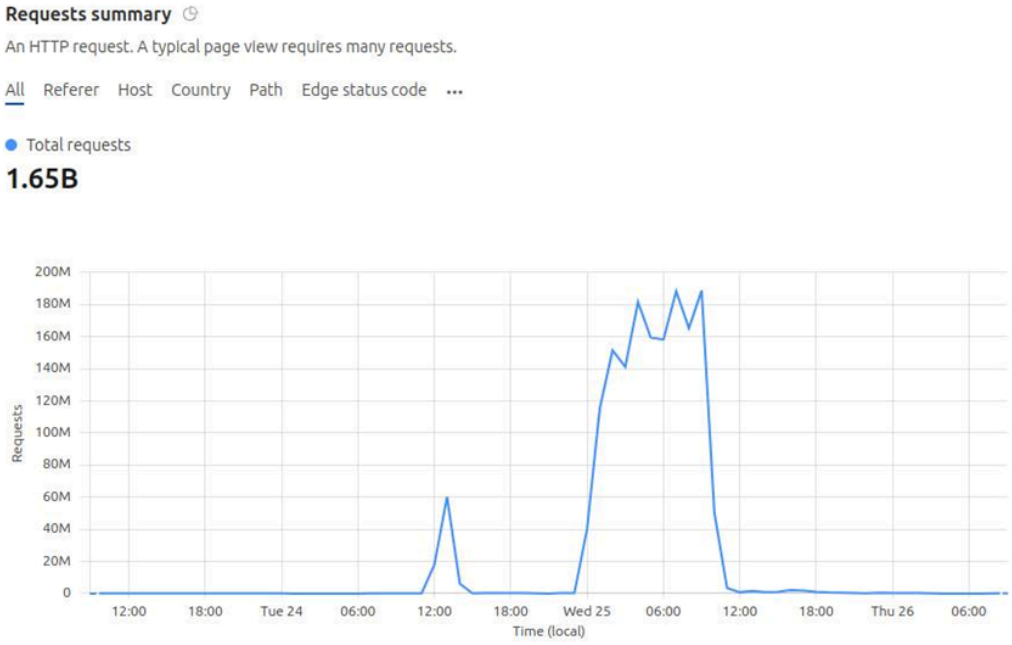
Հոկտեմբերի 25-ին՝ ժամը 12:40-ին, միջադեպին արձագանքել է Hexens կիբեռանվտանգության ընկերությունը: 25 րոպեի ընթացքում նրանց հաջողվել է վերականգնել կայքի գործունակությունը: Հարձակմանը ներգրավվել է մոտավորապես 20,000 հոսթ՝ հասնելով առավելագույնը վայրկյանում 200,000 հարցման, ինչը Hexens-ին հանդիպած երկրորդ ամենահզոր հարձակումն է:

Հարձակման հեղինակները դրսևորել են կատարելագործվածության բարձր մակարդակ՝ միջադեպին արձագանքելու ժամանակ չորս անգամ փոփոխելով իրենց մոտեցումը: Նրանք գտնում էին ուժեղացման նոր սարքեր՝ համապատասխանաբար հարմարեցնելով իրենց մեթոդները. օրինակ՝ երբ հարցումների սահմանափակիչը արգելափակեց GET հարցումները, նրանք անցան POST հարցումների:

Ըստ Hexens-ի թիմի՝ հարձակումների պատճառը Hraparak.am-ում մի քանի հոդվածների հրապարակումն է, որոնք կարելի է գտնել հետևյալ հղումներով՝

- https://hraparak.am/post/a7aa0f305f471a553d5f6ec19f6c0268
- https://hraparak.am/post/a9108423851caa624ce4e13462f59379
- https://hraparak.am/post/692c7a3185d50d4cf00f21e3e9b4f4ad
- https://hraparak.am/post/787a0eeab6959761f81b18bbb386f1e8
- https://hraparak.am/post/dc49dcd5dbae94bf57b70f64b13bfa5a

Ի պատասխան այս միջադեպի՝ Hexens-ն անկախ լրատվամիջոցներին առաջարկել է անվճար պաշտպանել DDoS հարձակումներից: Հատուկ շնորհակալություն ենք հայտնում DigiFence-ին այս նախաձեռնությանն աջակցելու համար:



Կայքերի կոտրման դեպքեր

2023 թվականի ընթացքում մի քանի ադրբեջանական հաքերային թիմեր (այդ թվում՝ իրեն հակահայկական կոչող մի մեծ խումբ) հայտնել են հարյուրավոր հայկական կայքերի բովանդակության աղավաղման (անգլ.՝ defacement) մասին: Այլ դեպքերից զատ, ինչպես հայտնի է, կոտրվել են մի քանի լրատվամիջոցների և ՔՀԿ-ների կայքեր, այդ թվում՝ news.am, yerkir.am, mamul.am, radiofama.am, transparency.am կայքերը: Հարձակումները հիմնականում տեղի են ունեցել Լեռնային Ղարաբաղի դեմ Ադրբեջանի ռազմական հարձակման օրերին:

2023 թվականի մայիսին կոտրվեց Հայաստանում խոցելի համայնքի պաշտպանությամբ զբաղվող մի կազմակերպության կայքը, որի պատճառով կայքից օգտվողներն ուղղորդվում էին դեպի այնպիսի կայքեր, որոնք ակնհայտորեն խաբեությամբ էին զբաղվում, և որոնց բովանդակությունը կապ չուներ սկզբնական

կայքի հետ: Քանի որ կազմակերպությունը պատրաստվում էր կարևոր զեկույց հրապարակել, «զգացվում էր», որ կայքը թիրախավորված է կոտրվել:

Միջադեպը հետաքննելու համար կազմակերպությունը դիմեց CyberHUB-AM-ին՝ համակարգչային արտակարգ իրավիճակների արձագանքման թիմին (անգլ.՝ Computer Emergency Response Team, CERT): CyberHUB-AM-ը աջակցում է Հայաստանի քաղհասարակությանը, ներառյալ՝ ՀԿ-ներին, իրավապաշտպաններին, ակտիվիստներին, լրագրողներին և անկախ լրատվամիջոցներին:

Տուժած կազմակերպության վեբկայքն աշխատում է բաց կոդով բովանդակության կառավարման հանրահայտ WordPress համակարգով, որը լայնորեն օգտագործում են ՀԿ-ները և քաղհասարակության կազմակերպությունները ողջ աշխարհում: Չարագործները հաճախ կարողանում են գտնել և օգտագործել WordPress-ի խոցելիությունները, մասնավորապես՝ նրա բազմաթիվ խրվակներում (plugin), որոնց միջոցով նրանք տիրանում են կայքերին՝ դրանք օգտագործելով չարամիտ նպատակներով կամ նենգափոխելով դրանց բովանդակությունը:

Հետաքննության ընթացքում CyberHUB-AM-ը վեբ սերվերում որոնել է ոչ վաղ անցյալում փոփոխված ֆայլերը և հայտնաբերել վերջերս ավելացված կամ փոփոխված տարբեր ֆայլեր, որոնք պատկանում էին posts-layouts անվամբ խրվակին: Նրանք նաև նկատել են wp-de-mouser-44 նոր օգտատեր, որը որպես ադմինիստրատոր ավելացվել է WordPress-ի օգտահաշվին, ինչ հաստատում էր, որ ինչ-որ այլ անձ մուտք է ունեցել հաշիվ:

Հետևելով այն հաջորդականությանը, որով օգտատերերը շարժվում էին կայք այցելելուց հետո, նշվել է, որ նրանց սկզբում ուղղորդում էին դեպի cdn[.]scriptsplatform[.]com: Այս դոմեյնն ընդամենը օրեր

առաջ էր գրանցվել՝ մայիսի 12-ին: Այս դոմեյնն իր հերթին օգտատերերին վերաուղղորդում էր խաբեությամբ զբաղվող մի որևէ կայք, ինչը նման վարակների դեպքում սովորական երևույթ է:

Կայքում ավելացված օգտատիրոջը որոնելու միջոցով պարզվեց, որ կան բազմաթիվ այլ կայքեր, որոնք նույն կերպ են կոտրվել: Արագ ստուգումը հաստատեց, որ այս կայքերը նույնպես ուղղորդում էին դեպի scriptsplatform[.]com դոմեյն: Հաշվի առնելով, որ տուժած մյուս կայքերը ո՛չ բովանդակությամբ, ո՛չ աշխարհագրորեն որևէ առնչություն չունեին կազմակերպության հետ, պարզ դարձավ, որ սա պատահական հարձակում էր:

Ստուգելով տեղադրած խրվակները՝ CyberHUB-AM-ի մասնագետները գտան Essential Addons for Elementor-ը, որը կայքերի ստեղծման հանրահայտ Elementor խրվակի ընդարձակ տարբերակն է (անգլ.՝ extension) է: Այդ խրվակում վերջերս խոցելիություն էր հայտնաբերվել, ինչից կարելի է ենթադրել, որ դա էր կայքը կոտրելու հավանական պատճառը: [9]

Կարճ ժամանակ անց, անվտանգությամբ զբաղվող Sucuri ընկերությունը վերլուծեց հենց այս խոցելիության միջոցով զանգվածային վարակների արշավը: Այդ զեկույցում տեղ գտած օգտահաշիվները կոտրելու ցուցիչները հաստատում էին, որ հայկական կազմակերպությունն այս արշավի զոհն է դարձել: [10]

Վարակված կայքի մաքրումը հեշտ գործընթաց էր՝ ի տարբերություն վեբկայքի կրկնակի վարակման հավանականությունը կանխարգելելու (թարմացնելով Essential Addons for Elementor խրվակը): Որոշ կախվածություններ թույլ չեն տվել կատարել այս թարմացումը՝ առանց կայքի հիմնական գործունակությունը խախտելու: Սա, ցավոք, բավականին տարածված երևույթ է՝ հատկապես

պատվերով պատրաստված կայքերի պարագայում: Սա վկայում է, որ նման կայք վարելը պահանջում է երկարաժամկետ սպասարկում:
Սակայն, ինչպես նշվում է CyberHUB-AM-ի՝ միջադեպի վերլուծական գրառման մեջ, «հայկական ընկերությունների մեծամասնությունն իրենց կայքերին վերաբերվում է ինչպես սառնարանի, որը կարելի է գնել, դնել խոհանոցում ու տարիներով մոռանալ դրա մասին»:[11]

Բարեբախտաբար, կազմակերպությունը նախատեսում էր դեպքից մի քանի շաբաթ անց գործարկել իր կայքի նոր տարբերակը, որը կլուծեր կախվածության հետ կապված խնդիրները: Մինչ այդ CyberHUB-AM-ը տեղադրեց վեբ հասանելիության պատնեշ (անգլ.՝ web access firewall, WAF)՝ հետագա սպառնալիքների ռիսկը մեղմելու համար: Կայքն այլևս չի կոտրվել:

Հեռակառավարվող տրոյական ծրագրեր (RAT)

Հեռակառավարվող տրոյական ծրագիրը *(անգլ.՝ Remote Access Trojan, RAT)* վնասարար ծրագրի տեսակ է, որի միջոցով հնարավորություն է ստեղծվում չարտոնված հեռահար մուտք գործել որևէ համակարգչային միավոր և վերահսկել կոտրված համակարգը: *RAT*-երը մի շարք վնասակար գործողությունների հնարավորություն են ստեղծում, որոնց թվում են տվյալների արտազատումը, հսկողությունը, համակարգի մանիպուլյացիան և վարակված սարքի օգտագործումը հետագա հարձակումների համար: Այս տրոյական ծրագրերը սովորաբար տարածվում են սոցիալական ինժեներիայի հնարքների, կցված վնասակար ֆայլերի կամ ավտոմատ ներբեռնումների միջոցով՝ զգալի վտանգ ներկայացնելով ինչպես անհատ օգտատերերի, այնպես էլ կազմակերպությունների անվտանգության համար:

2023 թվականի սկզբին հայկական երկու լրատվամիջոցների Google/YouTube օգտահաշիվները ենթարկվեցին կատարելագործված հարձակումների, որոնք միտված էին այդ հաշիվներին տիրանալուն:

Հունվար և մարտ ամիսներին տեղի ունեցած այս միջադեպերն իրականացվել են KMSauto ծրագրում (որը սովորաբար օգտագործվում է Microsoft Windows-ի և Office արտադրանքի անօրինական ակտիվացման համար) ներդրված Remote Access Trojan-ների (RAT) միջոցով:

RAT-երի ներդրումից հետո չարագործները վերահսկողություն են հաստատել լրատվամիջոցների օգտահաշիվների վրա: Նրանք փոխել են YouTube-ի օգտահաշվի լոգոները և անունները՝ դրանք վերափոխելով Tesla-ի կրիպտոարժույթների խարդախությունները խթանելու համար նախատեսված էջի: Այս գործողությունը ոչ միայն խաթարել է լրատվամիջոցների գործունեությունը, այլև նպատակ է ունեցել խաբելու լսարանին՝ խարդախ սխեմաներին մասնակից դարձնելու նպատակով:

Bitdefender-ի մանրակրկիտ վերլուծությունը[12] ընդգծում է, որ հեռարձակող ալիքների կոտրման (անգլ.՝ stream-jacking) պրակտիկան գնալով ընդարձակվում է: Նմանօրինակ հարձակումների դեպքում օրինական YouTube ալիքները կոտրվում են խարդախություններին վերաբերող բովանդակություն հեռարձակելու համար:

Մեկ այլ միջադեպ. սկսած 2022 թվականի վերջից՝ Check Point Research-ը բացահայտել է Հայաստանում գործող կազմակերպությունների դեմ ուղղված արշավ: Operation Silent Watch անունը ստացած այս արշավում կիրառվել է AutoIt-ի հիմքով OxtaRAT շրջանցող ծրագրի նոր տարբերակը, որը նախատեսված է հեռավար մուտքի և համակարգչի աշխատասեղանի հսկողության համար: Վնասարար ծրագիրը տարածվել է իբրև PDF ֆայլ՝ քողարկված ինքնուրույն բացվող արխիվի միջոցով, որը գործարկվելիս մի քանի ֆայլեր է տեղակայել՝ թիրախավորված համակարգը կոտրելու համար:

OxtaRAT շրջանցող ծրագիրը գործիք է, որն ունակ է արտազատել ֆայլեր, տեսաձայնագրել վեբ-

տեսախցիկներից և աշխատասեղաններից, TightVNC-ի միջոցով հեռակառավարում իրականացնել և տեղադրել վեբ-թաղանթներ: OxtaRAT-ի այս տարբերակը, նախորդ տարբերակների հետ համեմատած, աչքի էր ընկնում բարելավված օպերացիոն անվտանգությամբ և նոր գործառույթներով: Հարձակում գործողների թիրախում են հայտնվել Ադրբեջանի և Հայաստանի իրավապաշտպան կազմակերպություններ, այլախոհներ և անկախ ԶԼՄ-ներ: Սա հայկական թիրախների և կորպորատիվ միջավայրերի դեմ OxtaRAT-ի կիրառման արձանագրված առաջին դեպքն էր:

Check Point-ի մասնագետները, համագործակցելով CyberHUB-AM-ի թիմի հետ,[13] վերհանել են այս արշավի ողջ ծավալը: Նրանց ջանքերի շնորհիվ պարզվել է, որ վարակման շղթան սկիզբ է առել «Israeli_NGO_thanks_Artsakh_bank_for_the_support_of.scr» անունով ֆայլից, որը VirusTotal-ին է ներկայացվել Երևանի IP հասցեից: Այս ֆայլը կատարել է հրամաններ OxtaRAT վնասարար ծրագիրը ներդնելու համար՝ օգտագործելով իրավապաշտպան Ալեքսանդր Լապշինին առնչվող և իբրև խայծ կիրառվող մի PDF ֆայլ:

Հետաքննությունից պարզ դարձավ, որ չարագործներըհայտնաբերվելուց խուսափելու նպատակով օգտագործել են բազմաֆորմատ ֆայլեր (անգլ.՝ polyglot files)՝ միավորելով իրական JPEG և AutoIt A3X ձևաչափերը: OxtaRAT շրջանցող ծրագիրը պարունակում էր քողարկված AutoIt կոդի մոտավորապես 20,000 տող, ինչը տարբեր լրտեսող գործողությունների հնարավորություն էր ընձեռում: Այդ գործողությունների թվում էին լրացուցիչ կոդի գործարկումը, PHP վեբ-թաղանթների տեղադրումը և վարակված սարքերի հետախուզությունը:

Operation Silent Watch արշավը տարածաշրջանում շարունակվող կիբեռսպառնալիքների մասին վկայությունն է: Check Point Research-ի և CyberHUB-AM-ի

միջև համագործակցությունը կարևոր նշանակություն ունեցավ այս վնասարար ծրագիրը բացահայտելու և դրա ազդեցությունը մեղմելու համար: Նրանց եզրահանգումները հնարավորություն են տալիս պատկերացում կազմելու չարագործների մարտավարության, հնարքների և ընթացակարգերի մասին՝ բարելավելով հակամարտությունների գոտիներում կիբեռլրտեսության գործողությունների բացահայտումը:

Ինսայդերական հարձակումներ

Ինսայդերական հարձակումները կիբեռանվտանգության սպառնալիքներ են, որոնց հիմքում կազմակերպության ներսում գտնվող անձինք են, որոնք լիազորված մուտք ունեն դրա ցանցեր կամ համակարգեր: Այս սպառնալիքները կարող են միտումնավոր բնույթ կրել, օրինակ՝ երբ դժգոհ աշխատակիցը դիտավորյալ վնաս է պատճառում, կամ լինել ոչ միտումնավոր՝ անփութության կամ մարդկային սխալի հետևանքով: Ինսայդերական հարձակումները հատկապես վտանգավոր են, քանի որ դրանք օգտագործում են օրինական մուտքը, ինչը դժվարացնում է դրանց հայտնաբերումն ու կանխումը: Դրանք կարող են հանգեցնել տվյալների զգալի արտահոսքերի, ֆինանսական կորուստների և վնաս հասցնել կազմակերպության հեղինակությանը:

2023 թվականի ապրիլին հայկական մեդիա ընկերությունում նման ինսայդերական հարձակում է տեղի ունեցել. դժգոհ աշխատակիցը TeamViewer-ի միջոցով օգտվել է խմբագրություն հեռավար մուտքից՝ կազմակերպության YouTube ալիքին տիրանալու նպատակով: Աշխատակիցը, օգտվելով օրինական մուտքի հնարավորությունից, կարողացել է տիրանալ YouTube-ի օգտահաշվին, ինչը լուրջ խափանում է առաջացրել: Միջադեպի հետաքննության մեջ կարևոր դեր է ունեցել CyberHUB-ը՝ մանրակրկիտ հետևելով

հարձակման աղբյուրին և վերհանելով կիրառված մեթոդները: CyberHUB-ի թիմը նաև AccessNow-ի միջոցով համակարգել է իր գործողությունները YouTube-ի հետ՝ հաջողությամբ վերականգնելով օգտահաշվի նկատմամբ հեռուստաընկերության վերահսկողությունը: Այս միջադեպն ընդգծում է ներքին անվտանգության խիստ միջոցառումների և հեռահար մուտքի արձանագրությունների աչալուրջ մոնիտորինգի անհրաժեշտությունը:

Այսօրվա աշխարհում, որտեղ թվային սպառնալիքները գնալով ավելի են կատարելագործվում և դառնում պարբերական, Հայաստանը հայտնվել է բարդ և անընդհատ զարգացող սպառնալիքների միջավայրում: Ադրբեջանի հետ շարունակվող հակամարտությունը, ինչպես նաև Pegasus-ի նման նորագույն լրտեսող ծրագրերի կիրառումը ակնառու են դարձրել երկրի խոցելիությունը պետությունների կողմից հովանավորվող կիբեռհարձակումների նկատմամբ: Ֆիշինգային հարձակումները, վեբկայքեր կոտրելը և հեռակառավարվող տրոյական ծրագրերի (RAT) ներդրումը էլ ավելի ընդգծեցին լրատվամիջոցների, քաղաքացիական հասարակության կազմակերպությունների և կառավարական հաստատությունների թվային ենթակառուցվածքների խոցելիությունը:

Սույն զեկույցում ներկայացված միջադեպերը ընդգծում են Հայաստանի՝ կիբեռանվտանգության իր համակարգերն ամրապնդելու և միջադեպերին արձագանքելու կարողությունները հզորացնելու հրատապ անհրաժեշտությունը: Երկրի համար շատ կարևոր է համագործակցել միջազգային ասպարեզում և ներդրումներ կատարել սպառնալիքների հայտնաբերման և կանխարգելման նորագույն միջոցառումներում՝ կիբեռհարձակումների աճող սպառնալիքին դիմակայելու համար: Հավասարապես կարևոր են նաև կիբեռանվտանգության ռիսկերի մասին հանրային իրազեկվածության բարձրացումը և անվտանգ առցանց պրակտիկաների խթանումը՝ ավելի դիմակայուն թվային էկոհամակարգ կառուցելու համար:

Հիմնական եզրահանգումները ցույց են տալիս, որ ինչպես արտաքին, այնպես էլ ներքին դերակատարներն օգտվում են Հայաստանի համակարգերի խոցելիությունից՝ թիրախավորելով քաղաքացիական հասարակությանը, լրատվամիջոցներին և կառավարական հաստատություններին: Այս

սպառնալիքները ոչ միայն ռիսկի տակ են դնում կարևոր ենթակառուցվածքները, այլև խաթարում են վստահությունը թվային հարթակների նկատմամբ՝ վտանգելով մարդու իրավունքները: CyberHUB-AM-ի նման կազմակերպությունների կողմից ձեռնարկվող արձագանքման և համագործակցային միջոցառումները, միջազգային գործընկերներությունների հետ մեկտեղ, կարևոր նշանակություն ունեն այս ռիսկերը մեղմելու և երկրի կիբեռդիմակայունությունը հզորացնելու համար:

Քանի որ Հայաստանը այս միջավայրում շարունակում է բախվել մարտահրավերների, կառավարության, մասնավոր հատվածի և քաղաքացիական հասարակության համար հրամայական է՝ գործել միասին՝ ավելի ապահով և դիմակայուն թվային ապագա կառուցելու համար:

ԿՂԲՅՈՒՐԵՐ

1 "Freedom in the World 2023: Armenia." Freedom House. Վերջին մուտքը՝ 2023թ. հուլիս:

2 "Freedom in the World 2023: Armenia." Freedom House.

3 "Armenia police warn of growing cybercrime rate." Վերջին փոփոխությունը՝ 2018թ. հունիսի 12:

4 "Armenian police bust Yerevan-based cybercrime syndicate targeting U.S. users via tech support scam." Armenpress. Վերջին փոփոխությունը՝ 2019թ. մայիսի 1:

5 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.

6 Stone, Maddie and Clement Lecigne. "How we protect users from 0-day attacks." Google, Threat Analysis Group. July 14, 2021.

7 Nimmo, Ben, David Agranovich, and Nathaniel Gleicher. "Quarterly Adversarial Threat Report." Meta. April 2022.

8 "Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict." Amnesty International. Published May 25, 2023.Վերջին մուտքը՝ 2024թ. դեկտեմբերի 26:

9 Muhammad, Rafie. "Critical Privilege Escalation in Essential Addons for Elementor Plugin Affecting 1+ Million Sites." Patchstack. Վերջին փոփոխությունը՝ 2023թ. մայիսի 11:

10 Martin, Ben. "Vulnerability in Essential Addons for Elementor Leads to Mass Infection." SucriBlog. Վերջին փոփոխությունը՝ 2023թ. մայիսի 18:

11 "Hackers leverage vulnerability of Essential Addons plugin to exploit Armenian WordPress sites." CyberHUB. Վերջին փոփոխությունը՝ 2023թ. մայիսի 23:

12 "Armenia Country Threat Landscape Report" by CyberHUB 2023.docx. Sharepoint.com. Published 2023. Վերջին մուտքը՝ 2024թ. դեկտեմբերի 3:

13 "CyberHUB-AM. Իսրայելական Check Point Research-ը բացահայտել է ադրբեջանական կիբերհարձակումը հայաստանյան թիրախների դեմ" CyberHUB-AM. Published February 17, 2023. Accessed February 7, 2025.