2025

ՀԱՅԱՍՏԱՆ. ԹՎԱՅԻՆ ՍՊԱՌՆԱԼԻՔՆԵՐԻ ՀԱՄԱՊԱՏԿԵՐԸ

CyberHUB-AM-ի տարեկան զեկույց

Երևան 2025

Media Diversity Institute

CyberHUB-AM

Բովանդակություն

01

Ամփոփ տեղեկություններ

2025-ը վճռորոշ շրջադարձային տարի էր Հայաստանի թվային անվտանգության ոլորտում: Դեպի Եվրոպական միություն և Միացյալ Նահանգներ ռազմավարական շրջադարձի արագացմանը զուգընթաց (որի ընթացքում երկիրն անջատվում է Ռուսաստանից ժառանգած անվտանգության համակարգերից)՝ Հայաստանի թվային տիրույթը դարձել է հիբրիդային պատերազմների, պատժիչ ազդանշանային գործողությունների և հետախուզական տվյալների հավաքագրման հիմնական թատերաբեմ:

CyberHUB-AM-ի պատրաստած սույն զեկույցում փաստագրվել և վերլուծության են ենթարկվել 2025 թվականի ընթացքում Հայաստանում արձանագրված հիմնական կիբեռսպառնալիքները: Առանցքային թեման «հիբրիդային և տեղեկատվական շրջափակումն» է՝ շարունակական բազմավեկտոր արշավ, որն իրականացվում է թե՛ պետությունների հետ սերտ կապեր ունեցող չարագործների, թե՛ հանցավոր խմբավորումների կողմից՝ օգտագործելով Հայաստանի աշխարհաքաղաքական անցումային փուլը և 2026 թվականի գալիք խորհրդարանական ընտրությունները:

Հիմնական եզրակացություններ

- Պետական հովանավորությամբ գործող սպառնալիքի դերակատարները, մասնավորապես՝ բարձր վտանգ պարունակող մշտական սպառնալիքի (անգլ.՝ Advanced persistent threat, APT) ռուսական խմբերը, ինչպիսիք են APT28-ը (Fancy Bear) և Mandiant-ի բացահայտած UNC5792 խումբը, ուժեղացրել են թիրախային գործողությունները հայկական քաղաքացիական հասարակության, պետական հաստատությունների և անկախ լրատվամիջոցների դեմ: Այս արշավներում ավանդական էլեկտրոնային փոստի միջոցով իրականացվող հարձակումների փոխարեն գնալով ավելի շատ են օգտագործվում գաղտնագրված հաղորդակցման հարթակները՝ Signal-ը, WhatsApp-ը և Telegram-ը:

- Զգալիորեն փոխվել է վարձու լրտեսող ծրագրերի (mercenary spyware) գործունեությունը. 2020-2023 թվականներին Հայաստանում լայնորեն արձանագրված Pegasus-ով վարակման դեպքերը, որոնք վերագրվում էին ադրբեջանական օպերատորներին, 2025 թվականին հասել են զրոյի, ինչը ենթադրում է, որ, հավանաբար, անցում է կատարվել վերահսկման այլընտրանքային գործիքակազմի:

- Նկատելիորեն աճել են Հայաստանի բանկային ոլորտը թիրախավորող ֆինանսական կիբեռհանցագործությունները: Դա պայմանավորված է Android-ի համար ստեղծված բանկային տրոյական ծրագրերով և վնասարար հավելվածներով, որոնք կիրառվում են՝ օգտվելով այն հանգամանքից, որ տնտեսությունն արագ թվայնացվում է, մինչդեռ բնակչության շրջանում կիբեռհիգիենայի մակարդակը մնում է ցածր:
- Քաղաքացիական հասարակությունը և անկախ լրատվամիջոցները շարունակում են մնալ առավել թիրախավորված ոլորտները: 2025 թվականին արձանագրվել է առնվազն ութ նշանակալի միջադեպ, այդ թվում՝ թիրախավորված ֆիշինգի (spearphishing) արշավներ, որոնց ընթացքում չարագործները ներկայացել են իբրև ԵՄ երկրների դեսպաններ, նախարարներ և Ազգային անվտանգության ծառայության աշխատակիցներ:
- Հայաստանն արձագանքել է օրենսդրական և ինստիտուցիոնալ ծանրակշիռ բարեփոխումներով, որոնց թվում են 2025 թվականին «Կիբեռանվտանգության մասին» օրենքի ընդունումը (ուժի մեջ է մտնելու 2026 թվականից), Հայաստանի տեղեկատվական համակարգերի գործակալության (ՀՏՀԳ) շրջանակներում Հայաստանի համակարգչային միջադեպերի արձագանքման ազգային թիմի (AM-CERT) գործարկումը և հանրային կրթական նախաձեռնությունների ընդլայնումը, ինչպիսին երեխաների առցանց անվտանգության «ԿիբեռՉատ» (CyberChat) հարթակն է:

Առաջ նայելով՝ ակնկալվում է, որ 2026 թվականի ընտրությունների մոտենալուն զուգընթաց կաճի նաև արտաքին միջամտության գործողությունների ինտենսիվությունը: Միայն տեխնիկական պաշտպանության միջոցները բավարար չեն այնպիսի չարագործների դեմ, որոնք հարմարվում են իրական ժամանակում և օգտագործում անվտանգության խաթարման մարդկային գործոնը: Անհրաժեշտ է ձևավորել միասնական ազգային մոտեցում, որը կմեկտեղի կարևորագույն ենթակառուցվածքների, ոլորտում մասնագիտացած քաղաքացիական հասարակության պաշտպանությունը և թվային գրագիտության ընդլայնումը:

02 Ներածություն

Նպատակը և ընդգրկումը

«Հայաստան. թվային սպառնալիքների համապատկերը 2025» զեկույցը ներկայացնում է 2025 թվականի ընթացքում Հայաստանի վրա ազդեցություն թողած կիբեռսպառնալիքների միջավայրի համապարփակ վերլուծություն: Զեկույցը կազմել է CyberHUB-AM-ը, որը Հայաստանի քաղաքացիական հասարակության և անկախ լրատվամիջոցների համար համակարգչային արտակարգ իրավիճակների արձագանքման թիմ է (անգլ.՝ Computer Emergency Response Team, CERT):

Զեկույցը նախատեսված է հետևյալ շահագրգիռ լսարանների համար. ռազմավարական ամփոփ պատկեր ստանալու ձգտող քաղաքականություն մշակողներ և պետական պաշտոնյաներ, անվտանգության ոլորտի մասնագետներ, որոնց անհրաժեշտ են տեխնիկական ցուցիչներ և հարձակման օրինաչափությունների վերլուծություններ, արձանագրված արշավների հիմնական թիրախներ հանդիսացող քաղաքացիական հասարակության կազմակերպություններ (ՔՀԿ) և լրատվամիջոցներ, ինչպես նաև միջազգային գործընկերներ և դոնորներ, որոնք աջակցում են Հայաստանի ժողովրդավարական և թվային զարգացմանը:

Վերլուծությունը հիմնված է 2025 թվականի ընթացքում CyberHUB-AM-ի հավաքած և մշակած միջադեպերի վրա՝ լրացված բաց աղբյուրներից ստացված հետախուզական տվյալներով, գործընկեր կազմակերպությունների (այդ թվում՝ Mandiant-ի, Google Threat Intelligence-ի և Volexity-ի) սպառնալիքների վերաբերյալ հետախուզական տվյալներով, ինչպես նաև՝ ՀՏՀԳ-ի և Հայաստանի կառավարության հրապարակային հաշվետվություններով: 5-րդ բաժնում ներկայացված պրակտիկ օրինակները վերցված են այն միջադեպերից, որոնցով անմիջականորեն զբաղվել է CyberHUB-AM-ը, կամ որի մասին ահազանգել են CyberHUB-AM-ին: Հարձակման ցուցիչները (անգլ.՝ Indicators of Compromise, IOC) զեկույցում ամբողջապես ներկայացված են վնասազերծված տարբերակով:

03 Ռազմավարական համատեքստը

3.1 Հայաստանի աշխարհաքաղաքական շրջադարձը

Հայաստանի 2025 թվականի կիբեռանվտանգության միջավայրը հնարավոր չէ դիտարկել երկրի ավելի լայն աշխարհաքաղաքական վերափոխումից դուրս: Հայաստանը շարժվում է որոշիչ ռազմավարական շրջադարձի ճանապարհով՝ ձգտելով ավելի սերտ ինտեգրման Եվրամիության և Միացյալ Նահանգների հետ, միաժամանակ հաղթահարելով տարարձայնությունները՝ կապված Ռուսաստանի գլխավորությամբ գործող ավանդական անվտանգության համակարգերից, այդ թվում՝ Հավաքական անվտանգության պայմանագրի կազմակերպությունից (ՀԱՊԿ) անջատվելու հետ: Այս վերադասավորումը, որն արագացել է այն բանից հետո, երբ 2023 թվականին Լեռնային Ղարաբաղում Ադրբեջանի հարձակման ժամանակ Ռուսաստանը չաջակցեց Հայաստանին, Հայաստանի թվային տիրույթը դարձրել է պատժիչ ազդանշանային գործողությունների և հիբրիդային ճնշումների հիմնական թատերաբեմ:

2025 թվականը հատկապես բարձր ռիսկայնությամբ տարի է դարձել՝ պայմանավորված երեք կառուցվածքային գործոններով: Առաջին. ԵՄ - ՀՀ հարաբերությունների պաշտոնական խորացումը (ներառյալ ԵՄ-ՀՀ գործընկերության համաձայնագրում գրանցված առաջընթացը) արտաքին հակառակորդների համար դառնում է ինտեգրման գործընթացի մասնակիցներին, մասնավորապես՝ ՔՀԿ-ներին և պետական պաշտոնյաներին վնասելու և վերահսկելու շարժառիթ: Երկրորդ. 2026 թվականի խորհրդարանական ընտրությունները մեծ արժեք ունեցող և առանձնահատուկ նշանակության թիրախ են արտաքին միջամտության գործողությունների համար, որոնց նպատակը հայաստանյան քաղաքականության արդյունքների վրա ազդելը և ժողովրդավարական ինստիտուտները վարկաբեկելն է: Երրորդ. Հայաստանի տնտեսության և հանրային ծառայությունների արագ թվայնացումը, չնայած զարգացման դրական գործոն լինելուն, առաջ է անցել բնակչության կիբեռհիրազեկվածության և կազմակերպությունների ներքին անվտանգության հասունության մակարդակից:

3.2 Հիբրիդային շրջափակման շրջանակը

2025 թվականի թվային սպառնալիքների միջավայրի գերակա թեման CyberHUB-AM-ը բնութագրում է իբրև «հիբրիդային շրջափակում»: Ի տարբերություն 2020 և 2023 թվականների զինված առճակատումների, որոնց ժամանակ կիբեռգործողությունները ծառայում էին որպես ռազմական գործողությունների մարտավարական աջակցություն, ներկայիս ագրեսիան ռազմավարական է, շարունակական և ոչ զինված: Սահմանին ակտիվ ռազմական գործողությունների բացակայությունը թվային ոլորտում խաղաղության չի հանգեցրել: Փոխարենը՝ հակամարտությունը տեղափոխվել է կիբեռտարածք, որտեղ այն կարող է իրականացվել գերազանցապես անանուն, ավելի քիչ ծախսերով և տևական ընթացքով:

Հիբրիդային շրջափակումն իրականացվում է միաժամանակ երկու ճակատով: Պետական հովանավորությամբ գործող դերակատարները՝ բարձր վտանգ պարունակող կայուն սպառնալիքի (անգլ.՝ Advanced persistent threat, APT) կատարելագործված խմբերը, որոնք կապված են ռուսական և, հնարավոր է, այլ օտարերկրյա հետախուզական ծառայությունների հետ, իրականացնում են թիրախային վերահսկողություն, մուտքային տվյալների հափշտակություններ և ազդեցության գործողություններ այն անձանց նկատմամբ, որոնք կարող են ազդել Հայաստանի ժողովրդավարական և աշխարհաքաղաքական ուղեգծի վրա: Հանցավոր նպատակներով կազմակերպված կիբեռհանցագործ խմբերը, որոնցից որոշները, ենթադրաբար, գործում են պետության լռելյայն հանդուրժողականության պայմաններում, օգտվում են Հայաստանի ընդլայնվող թվային տնտեսությունից և նոր թվայնացած սպառողների ֆինանսական անփորձությունից:

3.3 Սպառնալիքների դերակատարների շրջանակը

2025 թվականին հայկական թիրախների դեմ ակտիվ սպառնալիքի հիմնական կատեգորիաներն են՝

- **Ռուսաստանի պետական կառույցների հետ ասոցացվող բարձր վտանգ պարունակող կայուն սպառնալիքի (անգլ.՝ Advanced persistent threat, APT) խմբեր.** Ռուսաստանի Գլխավոր հետախուզական վարչությանը (ռուս.՝ ГРУ) վերագրվող APT28 (Fancy Bear) խումբը, որն իբրև ազդանշանային գործողություն՝ թիրախավորել է կառավարական ենթակառուցվածքները: UNC5792 խումբը, որը ժամանակին մեծ ճշգրտությամբ նույնականացրել է Mandiant-ը, և հաստատել է նաև Google Threat Intelligence-ը, Signal հավելվածի միջոցով շարունակական թիրախավորված ֆիշինգի (spearphishing) արշավներ է իրականացրել քաղաքացիական հասարակության և ընտրական ինստիտուտների դեմ:
- **Ադրբեջանական հետախուզական գործողություններ.** ադրբեջանական հետախուզական ծառայությունները, որոնք 2020-2023 թվականներին հայկական թիրախների դեմ Pegasus լրտեսող ծրագրի հիմնական կիրառողներն էին, 2025 թվականին, կարծես ժամանակավորապես, դադարեցրել են այս կարողության կիրառումը կամ փոխարինել են այն: Հաշվետու ժամանակահատվածում Pegasus-ով վարակման դեպքեր չեն հայտնաբերվել, ինչը ենթադրում է, որ կամ տեղի է ունեցել մատակարարի փոփոխություն, կամ անցում է կատարվել տվյալների հավաքագրման նվազ հայտնաբերելի մեթոդների:
- **Միջազգային կիբեռհանցագործություն.** Հանցավոր խմբերը, որոնք ենթադրաբար գործում են Արևելյան Եվրոպայից և Կենտրոնական Ասիայից, թիրախավորում են Հայաստանի ֆինանսական ոլորտի օգտատերերին Android-ի համար ստեղծված բանկային տրոյական ծրագրերով, որոնց թվում է Ajina.Banker ծրագրերի ընտանիքը: Այս խմբերն օգտվում են վճարումների արագ տեմպերով ընթացող թվայնացումից և բջջային սարքերի անվտանգության անբավարար մակարդակից:
- **Սոցիալական ինժեներիայի չնույնականացված օպերատորներ.** WhatsApp-ի և Viber-ի միջոցով հայ լրագրողներին և քաղաքացիական հասարակության ներկայացուցիչներին թիրախավորող խարդախության բազմաստիճան գործողություններ, որոնց ժամանակ իրականացվել է գործընկերների, ինչպես նաև Ազգային անվտանգության ծառայության կեղծ աշխատակիցների նմանակում, և որոնք մատնանշում են պետական ռեսուրսների ներգրավում, ինչը, սակայն, պաշտոնապես չի հաստատվել:

04 Սպառնալիքների համապատկերի վերլուծություն

4.1 Պետական հովանավորությամբ իրականացվող գործողություններ և լրտեսող ծրագրեր

2025 թվականին Հայաստանի դեմ պետական հովանավորությամբ իրականացվող կիբեռգործողությունները փոխել են իրենց մոտեցումը. կոպիտ ներխուժման մարտավարությանը փոխարինելու են եկել խիստ թիրախային սոցիալական ինժեներիայի արշավները: Կառավարական ցանցերի փոխարեն, չարագործները նախընտրում են թիրախավորել ազդեցիկ անհատների՝ քաղաքացիական հասարակության առաջնորդների, լրագրողների, պետական պաշտոնյաների և ընտրական հանձնաժողովների աշխատակիցների անհատական սարքերը և օգտահաշիվները:

Լրտեսող ծրագրերի տիրույթում ամենանշանակալի զարգացումը Pegasus-ով վարակման հաստատված դեպքերի լիակատար անհետացումն է. 2020-2023 թվականներին հայկական թիրախների՝ Pegasus-ով վարակման բազմաթիվ դեպքեր են արձանագրվել: Սա ամենայն հավանականությամբ չի նշանակում, որ հակառակորդի հետաքրքրությունը նվազել է, այլ ավելի շուտ ենթադրում է, որ տեղի է ունեցել կարողությունների փոփոխություն: Իբրև հնարավոր բացատրություն կարելի է նշել հետևյալը. անցում է կատարվել լրտեսող ծրագրերի նոր կոմերցիոն մատակարարի, որը դեռևս չի նույնականացվել առկա հայտնաբերման մեթոդներով, ավելացել են ավելի քիչ թվային հետք թողնող, զրո խոցելիությամբ գործողությունների կիրառման դեպքերը, կամ ռազմավարական անցում է կատարվել դեպի հասանելիության ձեռքբերում՝ հիմնված սոցիալական ինժեներիայի վրա, որն ավելի էժան է և դժվար հայտնաբերվող:

Միևնույն ժամանակ, արձանագրվել է APT28-ի (Fancy Bear) գործունեությունը՝ ուղղված Հայաստանի կառավարական ենթակառուցվածքների դեմ, ինչը համապատասխանում է այն օրինաչափություններին, որոնք նկատվել են Արևմուտքի հետ մերձենալ ձգտող հետխորհրդային այլ պետություններում ևս: Այս գործողությունների նպատակը, կարծես, ոչ այնքան անմիջապես տվյալների հափշտակությունն է, որքան, ավելի շատ ռազմավարական ուղերձ փոխանցելը՝ իբրև ճնշման գործիք ցուցադրելով կարևորագույն համակարգեր ներթափանցելու կարողությունը:

4.2 Թիրախավորված ֆիշինգ և սոցիալական ինժեներիա

Թիրախավորված ֆիշինգը (կոնկրետ ազդեցիկ անձանց նկատմամբ անհատականացված խայծերի կիրառմամբ նպատակային ֆիշինգային գրոհները, անգլ.՝ spearphishing) 2025 թվականի հարձակման ամենատարածված մեթոդն է: Մարտավարության առումով, սակայն, առանցքային փոփոխություն է տեղի ունեցել. չարագործները հիմնականում հրաժարվել են էլեկտրոնային փոստից՝ անցնելով գաղտնագրված հաղորդակցման հարթակներ, մասնավորապես՝ Signal: Նման փոփոխությունը մի շարք նպատակների է ծառայում. Signal-ի ծայրից ծայր գաղտնագրումը (անգլ.՝ end-to-end encryption) սահմանափակում է հայտնաբերման հնարավորությունը, հարթակը համարվում է անվտանգ և վստահելի, ինչը նվազեցնում է հաղորդագրություն ստացողների կասկածամտությունը, իսկ զրույցի ձևաչափը հնարավորություն է տալիս իրական ժամանակում կիրառել սոցիալական ինժեներիայի հնարքներ, մի բան, որը հնարավոր չէ կրկնել էլեկտրոնային փոստի դեպքում:

Արձանագրված ութ միջադեպերը ցույց են տալիս, որ գործում է հարձակման հստակ մեթոդաբանություն. հարձակում գործողները նախ հետախուզում են թիրախների մասնագիտական կապերը և ինստիտուցիոնալ պատկանելությունը, այնուհետև ստեղծում են վստահություն ներշնչող կեղծ կերպարներ (ԵՄ դեսպաններ, նախարարության պաշտոնյաներ, լրագրողներ), կապ են հաստատում Signal կամ WhatsApp հավելվածների միջոցով և օգտագործում ձևավորված կեղծ վստահությունը՝ վնասակար հղումներ ուղարկելու կամ նույնականացման տվյալներ ստանալու համար: Մի քանի միջադեպերի ուսումնասիրությունը ցույց է տալիս, որ չարագործները դրսևորել են իրական ժամանակում հարմարվելու ունակություն. երբ սկզբնական URL-ը հայտնաբերվում է կամ լրանում է դրա ժամկետը, փոխարինող URL-ները տրամադրվում են րոպեների ընթացքում՝ փաստելով, որ գործողությունը ղեկավարում են իրական մարդիկ, այլ ոչ թե ավտոմատացված համակարգերը:

Առանձնահատուկ վտանգավոր դեպք է Microsoft 365 OAuth սիմվոլի հափշտակությունը: Գաղտնաբառը ֆիշինգի միջոցով ստանալու փոխարեն, հարձակում գործողները զոհերին են ուղղորդում Microsoft-ի իրական մուտքի գործընթացով, ապա վերջիններիս հրահանգում պատճենել ստացված նույնականացման սիմվոլը (authentication token) և այն Signal-ի միջոցով հետ ուղարկել հարձակման հեղինակներին: Այս մեթոդը շրջանցում է բազմաստիճան վավերացումը և հարձակման հեղինակներին թույլ է տալիս իրենց ձեռքի տակ եղած սարքերը միացնել զոհի Microsoft Entra ID-ին՝ ապահովելով կազմակերպության ռեսուրսներին երկարաժամկետ, թվացյալ օրինական մուտք:

4.3 Ֆինանսական կիբեռհանցագործություններ և չարամիտ ծրագրեր

Հայաստանի ֆինանսական ոլորտը և նրա սպառողները բախվել են Android օպերացիոն համակարգով աշխատող սարքերը թիրախավորվող չարամիտ ծրագրերի կիրառմամբ արշավների աճի: Ajina.Banker չարամիտ ծրագրերի ընտանիքը, որը տարածվում է Telegram ալիքներով՝ օրինական բանկային կամ պետական ծառայություններ մատուցող հավելվածների անվան տակ, ունակ է որսալ SMS-ով ուղարկվող մեկանգամյա գաղտնաբառերը, հավաքագրել բանկային մուտքի տվյալները և հափշտակել կոնտակտային տեղեկությունները: Այս չարամիտ ծրագիրը նույնպես օգտվում է ֆինանսական ծառայությունների արագ թվայնացումից, որը Հայաստանի տնտեսական զարգացման օրակարգի շարժիչ ուժն է:

2025 թվականի մեկ այլ դեպքում արձանագրվել է ArmScan.apk-ի տարածումը. սա gov-am.sbs դոմեյնում տեղակայված չարամիտ Android հավելված է, որը ներկայանում է իբրև կառավարության կողմից տրամադրվող աջակցության (հետվճարների) հավելված: Չարագործները մանրակրկիտ կառուցել են սոցիալական ինժեներիայի պատմություն, իբրև թե օգտատերերը կարող են տվյալ ծրագրով սկանավորել ՀԴՄ կտրոնները և ստանալ պետական հետվճարներ՝ այդպիսով օգտվելով պետական աջակցության ծրագրերի վերաբերյալ հանրության մեջ ձևավորված սպասումներից: Հավելվածը որակվել է որպես Trojan/Dropper, այսինքն՝ այն կարող է ծառայել և՛ որպես անմիջապես տվյալների հավաքագրման գործիք, և՛ որպես լրացուցիչ վնասարար ծրագրերի տեղադրման մեխանիզմ:

Այս արշավները խոսում են միտումնավոր թիրախավորման ռազմավարության մասին. հանցավոր խմբերը Հայաստանի բանկային ոլորտը դիտարկում են իբրև «շահավետ թիրախ»՝ թվային վճարումների արագ աճի և տարածման, սպառողների շրջանում անվտանգության վերաբերյալ համեմատաբար ցածր մակարդակի իրազեկվածության և ֆինանսական կազմակերպություններում բջջային սարքերի սպառնալիքների հայտնաբերման ենթակառուցվածքներում առկա բացերի պատճառով:

4.4 DDoS հարձակումներ և կայքերի բովանդակության աղավաղում

«Բաշխված ծառայությունների ժխտում» (անգլ.՝ Distributed Denial-of-Service, DDoS) տեսակի հարձակումները և կայքերի բովանդակության աղավաղումները (անգլ.՝ Defacement), լինելով ոչ այնքան առաջադեմ հարձակումների տեսակ, շարունակում են հանդես գալ որպես քաղաքական ուղերձների փոխանցման և աշխատանքի խաթարման գործիքներ: Նմանօրինակ հարձակումները սովորաբար ակտիվանում են աշխարհաքաղաքական լարվածության սրացման ժամանակահատվածներում և օգտագործվում են հարձակողական

կարողությունների ցուցադրման, թվային ծառայությունների նկատմամբ հանրային վստահության խաթարման և լրատվամիջոցների այնպիսի լուսաբանման ապահովման համար, որը մեծացնում է հակառակորդի գործողությունների հոգեբանական ազդեցությունը:

2025 թվականի սպառնալիքների համատեքստում DDoS հարձակումները լավագույնս կարելի է պատկերել որպես ավելի լայն հիբրիդային շրջափակման ռազմավարության մի մաս. դրանք քիչ ծախսատար, աչքի ընկնող գործողություններ են, որոնք ոչ թե հանդես գալիս որպես առանձին արշավներ, այլ ուղեկցում են ավելի առաջադեմ և նպատակային գործողություններին : Հայաստանի կառավարության և հայկական լրատվամիջոցների կայքերը բովանդակության աղավաղման հարձակումների թիրախ են դարձել: Այդ գործողությունները վերագրվում են քաղաքական շարժառիթներով գործող խմբերի, որոնք կասկածելի կապեր ունեն պետությունների հետ:

4.5 Տեղեկատվական բնույթի գործողություններ և ապատեղեկատվություն

Հայաստանի՝ ԵՄ ինտեգրման գործընթացի արագացման և 2026 թվականի գալիք ընտրությունների ֆոնին ակտիվացել են հայկական լսարանին միտված ապատեղեկատվության և ազդեցության գործողությունները: Այս արշավներն իրականացվում են սոցիալական ցանցերով, Telegram ալիքներով և զանազան կայքերով, որոնց արտադրած բովանդակությունն ուղղված է կառավարության արևմտյան կողմնորոշման նկատմամբ հանրային վստահությունը խաթարելուն, քաղաքական պառակտումները խորացնելուն և ժողովրդավարական բարեփոխումների ջատագով քաղաքացիական հասարակության կազմակերպություններին վարկաբեկելուն:

Սույն զեկույցում ներկայացված միջադեպերը, որոնք առնչվում են տեխնիկական հարձակումներին և սոցիալական ինժեներիային, երկու նպատակի են ծառայում. բացի իրենց հիմնական նպատակից (մուտքային տվյալների հափշտակություն կամ սարքերի կոտրում), դրանք նաև հետախուզական տեղեկությունների հավաքագրման գործողություններ են: Կոտրված ՀԿ-ների հաշիվներից, լրագրողների գրագրություններից և քաղաքացիական հասարակության առաջնորդների սարքերից հավաքագրված տվյալներն անմիջականորեն օգտագործվում են հետագա ազդեցության գործողությունները պլանավորելու և դրանց թիրախավորումը կատարելագործելու նպատակով:

2025 թվականի առանցքային արձանագրումներից մեկն այն է, որ միտումնավոր թիրախավորվել է Հայաստանի հասարակական կյանքի վստահելիությունը. հանդես գալով ԵՄ դիվանագետների, նախարարության պաշտոնյաների և հարգված գործընկեր լրագրողների անունից՝ չարագործները ձգտում են ոչ միայն վնասել կոնկրետ թիրախների, այլև խաթարել քաղաքացիական խմբերի համագործակցությունը և անկախ լրատվամիջոցների արդյունավետ գործունեությունը հնարավոր դարձնող հասարակական վստահությունը:

05 Պրակտիկ օրինակներ

Ստորև բերված պրակտիկ օրինակները ներկայացնում են կիբեռանվտանգության ոլորտի 2025 թվականին արձանագրված ութ նշանակալի միջադեպեր, որոնք առնչվում են Հայաստանի քաղաքացիական հասարակությանը, լրատվամիջոցներին և պետական կառույցներին: Դեպքերը դասակարգված են՝ ըստ հարձակման տեսակի: Հարձակման բոլոր ցուցիչները (անգլ.՝ Indicators of Compromise, IOC) ներկայացված են վնասազերծված տարբերակով:

5.1 Թիրախային ֆիշինգ գաղտնագրված հաղորդակցման հարթակներով

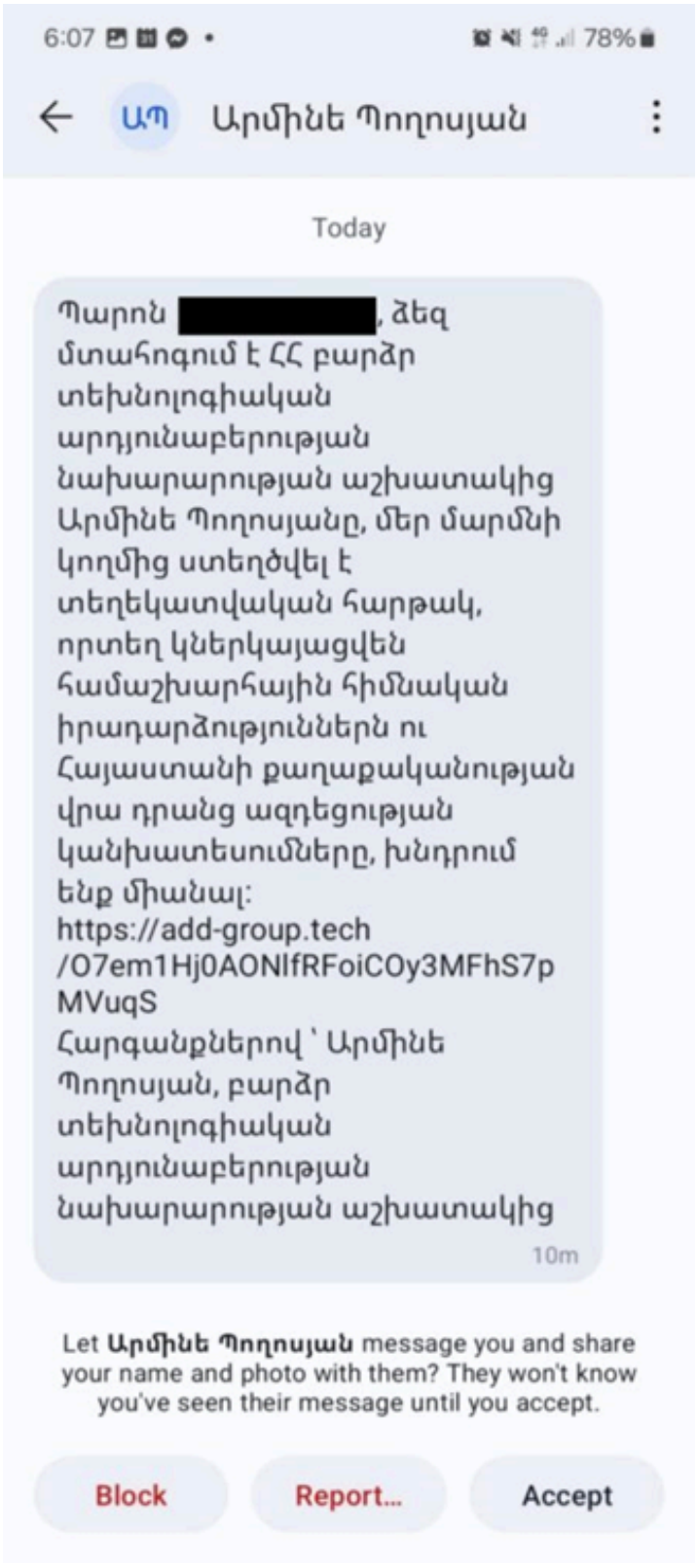
Միջադեպ 5.1.1. UNC5792-ի արշավ Signal-ում. նախարարության անունից ներկայանալու փորձ

2025 թվականի մարտ-ապրիլ

Թիրախ՝ քաղաքացիական հասարակության կազմակերպություններ, Կենտրոնական ընտրական հանձնաժողով

2025 թվականի մարտի սկզբին CyberHUB-AM-ը բացահայտել է թիրախավորված ֆիշինգի շարունակական արշավ, որն ուղղված էր ընդդեմ Հայաստանի քաղհասարակության, պետական կազմակերպությունների ու անհատների: Արշավը վերագրվել է բարձր վտանգ պարունակող կայուն սպառնալիքի (անգլ.՝ Advanced persistent threat, APT) UNC5792 խմբին, որը նախկինում բացահայտել էր Mandiant-ը և հաստատել նաև Google Threat Intelligence-ը:

Հարձակում գործողները ներկայացել են հորինված «Արմինե Պողոսյան» անվամբ, որն իբրև թե Հայաստանի բարձր տեխնոլոգիական արդյունաբերության նախարարության աշխատակից է, և օգտագործելով Signal-ը՝ հասցեատերերին հրավիրել են իբրև թե աշխարհաքաղաքական վերլուծություններ տրամադրող «տեղեկատվական հարթակ»: Սա քաղհասարակության վերլուծաբանների և ՀԿ-ների աշխատակիցների մասնագիտական հետաքրքրություններին համապատասխանեցված, հատուկ մշակված խայծ էր:



Signal-ի միջոցով UNC5792-ի ուղարկած ֆիշինգային հաղորդագրության էկրանանկար, 2025թ. մարտ:

Թիրախի նկարագիր

- ՀԿ, որն ակտիվ է օրենսդրական բարեփոխումների և ընտրությունների մշտադիտարկման ոլորտում
- Անվտանգության հարցերով վերլուծաբան, որը զբաղվում է երկրի քաղաքականության և քաղաքական գործընթացների վերլուծությամբ
- Հայաստանի Կենտրոնական ընտրական հանձնաժողովի աշխատակազմ

Հիմնական մարտավարություն

- Հարձակումն իրականացվել է բացառապես Signal հարթակի միջոցով՝ շրջանցելով էլ. փոստի անվտանգության համակարգերը:
- Կիրառված վնասակար հղումները ժամանակավոր բնույթ են կրել. հայտնաբերվելուց հետո սկզբնական add-group.tech դոմեյնը փոխարինվել է group-add.com-ով:
- Օպերատորի ակտիվ ներգրավվածություն իրական ժամանակում. սկզբնական URL-ի ժամկետի լրանալուց հետո րոպեների ընթացքում տրամադրվել է փոխարինող ակտիվ վնասակար հղում:
- Օգտագործվել են երեք դոմեյններ՝ add-group.tech, group-add.com, signal-groups-add.com: VirusTotal-ը բոլոր 3 դոմեյնները գնահատել է որպես խիստ վնասակար:

Ցուցիչի տեսակը	Ցուցիչի տվյալը	Նկարագիրը
Դոմեյն	add-group[.]tech	Սկզբնական դոմեյն
Դոմեյն	group-add[.]com	Հայտանաբերումից հետո կիրառված նոր դոմեյն
Դոմեյն	signal-groups-add[.]com	հարձակման երրորդ փուլում օգտագործված դոմեյն
URL	hxxps[://]add-group[.]tech/O7em1Hj0AONIfRFoIC0y3MFhS7pMVUqS	սկզբնական ֆիշինգային URL
URL	hxxps[://]group-add[.]com/kPDOT4Wr7PrKmkQtK6LrhFxmmo6LA7EE	փոխարինող ֆիշինգային URL

Միջադեպ 5.1.2. Signal-ի միջոցով ԵՄ դեսպանի անունից հանդես գալու դեպքը

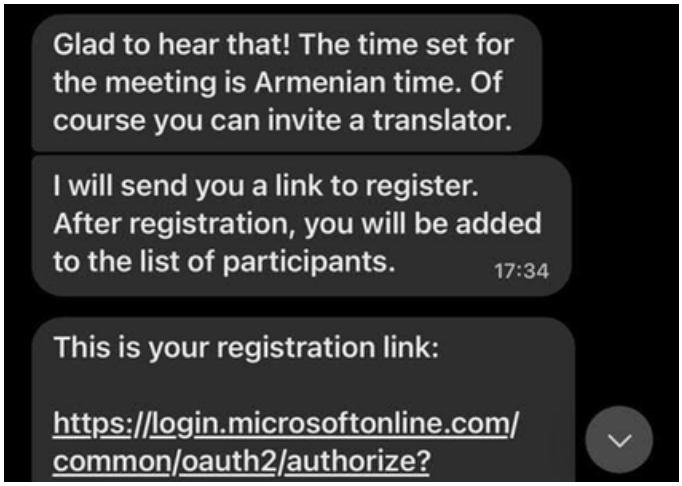
2025թ. ապրիլի 8
Թիրախ՝ քաղաքացիական հասարակության կազմակերպություններ (տասնյակ ՀԿ-ներ)

2025 թվականի ապրիլի 8-ին հայտնաբերվել է լավ մշակված թիրախային ֆիշինգի (անգլ.՝ spearphishing) արշավ, որի նշանակետում հայաստանյան տասնյակ ՀԿ-ներ են եղել: Հարձակման հեղինակները հաղորդագրությունն ուղարկել են Հայաստանում ԵՄ պատվիրակության ղեկավար, դեսպան Վասիլիս Մարագոսի անունից՝ կապ հաստատելով Signal մեսենջերի միջոցով: Հայաստանում ԵՄ պատվիրակությունն անմիջապես տեղեկացվել է միջադեպի մասին և հաստատել, որ իր համակարգերը չեն կոտրվել:

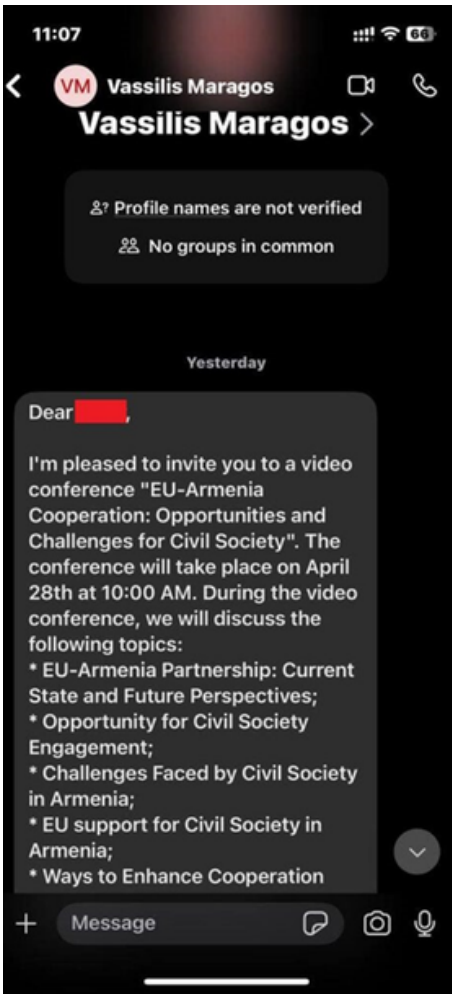
Ֆիշինգային հաղորդագրությունը՝ քողարկված իբրև Microsoft Teams հարթակին միանալու հղում, հասցեատերերին հրավիրում էր «ԵՄ-Հայաստան համագործակցություն. հնարավորություններ և մարտահրավերներ քաղաքացիական հասարակության համար» խորագրով տեսակոնֆերանսի: Հարձակման ժամանակ օգտագործվել է մուտքային տվյալների հափշտակության նորարարական մեթոդ:

Հարձակման մեթոդ.
Microsoft Entra ID համակարգում սարքի գրանցում

Զոհերին կեղծ մուտքի էջ ուղղորդելու փոխարեն, հարձակում գործողները նրանց առաջարկուն էին Microsoft-ի իրական էջ: Նույնականացումը հաջողությամբ անցնելուց հետո զոհի զննարկիչը ստեղծում էր Microsoft-ի վավերացման նշան: Չարագործը, Signal-ի միջոցով կապ հաստատելով, զոհին հրահանգում էր պատճենել և տեղադրել այդ նշանը՝ այդպիսով մեկնարկելով Microsoft Entra ID համակարգին սարքի միացման գործընթացը և հարձակման հեղինակի սարքը գրանցելով զոհի հաշվին:



Entra ID համակարգին սարքի միացման հարձակման ընթացքի իլյուստրացիա:



ԵՄ դեսպանի անունից ուղարկված ֆիշինգային հաղորդագրության էկրանանկար, 2025թ. ապրիլ:

CyberHUB-AM-ը հաստատել է առնվազն մեկ դեպք, երբ հարձակում գործողներին հաջողվել է տիրանալ մի հայտնի հասարակական կազմակերպության ղեկավարին պատկանող հաշվի: Ուսումնասիրությամբ պարզ է դարձել, որ նույնականացման փորձերը եղել են երեք IP հասցեներից, որոնք բոլորն էլ պատկանում էին ռուսական ամպային սերվերի պրովայդեր Biterika Group ՍՊԸ-ին:

Microsoft Authentica...	Failure	50053	95.182.124.124	Zelenograd, Moskva,...
Microsoft Azure CLI	Failure	50053	2605:6400:8583:2bef...	New York, New York,...
Microsoft Authentica...	Failure	50053	46.8.213.90	Zelenograd, Moskva,...

Մատյանի գրանցումները, որոնք ցույց են տալիս Microsoft Azure CLI-ի միջոցով մուտքի փորձերը հարձակում գործողների կողմից կառավարվող ռուսական ռեսուրսներից:

Այն բանից հետո, երբ միջադեպի արձագանքման թիմը խափանեց առաջին հարձակումը, չարագործները զոհի հետ կապը վերսկսեցին Signal-ի միջոցով և փորձեցին կրկնել գործողությունները՝ դա պայմանավորելով տեխնիկական խափանումով: Նման համառությունը բնորոշ է UNC5792 խմբի TTP-ներին (անգլ.՝ Tactics, Techniques, and Procedures, մարտավարություն, տեխնիկա և ընթացակարգեր) և ռուսական սպառնալիքի դերակատարների վարքագծին, որը մանրամասն նկարագրված է Veloxity-ի 2025 թվականի ապրիլին հրապարակած «Ֆիշինգ հանուն կոդերի. ռուսական չարագործների թիրախում Microsoft 365 OAuth-ի աշխատանքային պրոցեսներն են» զեկույցում:

Ցուցիչի տեսակը	Ցուցիչի տվյալը	Նկարագիրը
IP հասցե	95[.]182[.]124[.]124	Հարձակում գործողների կողմից օգտագործվող գործիքակազմ՝ Biterika Group ՍՊԸ (Ռուսաստան)
IP հասցե	46[.]8[.]213[.]90	Հարձակում գործողների կողմից օգտագործվող գործիքակազմ՝ Biterika Group ՍՊԸ (Ռուսաստան)
IP հասցե	188[.]130[.]142[.]95	Հարձակում գործողների կողմից օգտագործվող գործիքակազմ՝ Biterika Group ՍՊԸ (Ռուսաստան)

Միջադեպ 5.1.3. Signal-ի հաշվին տիրանալու արշավ

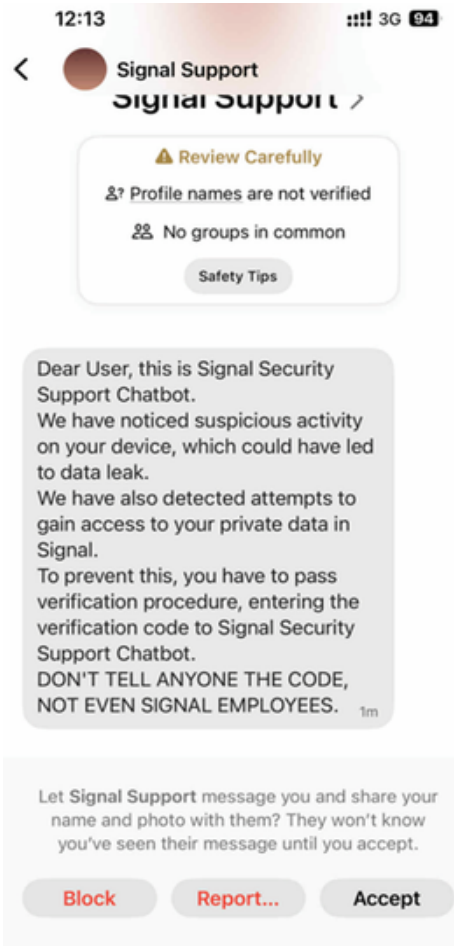
2025թ. սեպտեմբերի 23

Թիրախ՝ Signal հավելվածի հայաստանյան օգտատերեր

Չարագործները ֆիշինգային արշավ են իրականացրել Signal-ում՝ նպատակ ունենալով իբրև «Signal Support» («Signal-ի աջակցման ծառայություն») ներկայանալու միջոցով տիրանալու օգտատերերի հաշիվներին: Հարձակման հիմքում Signal ապրանքանիշի նկատմամբ սոցիալական վստահությունն է. թիրախավորվել են այն օգտատերերը, որոնք չէին միացրել հարթակի «Գրանցման արգելքը» (Registration Lock):

Հարձակման քայլերի հաջորդականությունը

1. Թիրախը Signal հարթակում «Signal Support» անունով գրանցված անհայտ համարից ստանում է անսպասելի հաղորդագրություն, որտեղ նշվում է, թե տվյալ հաշվի վրա արձանագրվել է կասկածելի ակտիվություն:
2. Միևնույն ժամանակ, չարագործը թիրախի հեռախոսահամարով Signal-ի գրանցման գործընթաց է սկսում իր ձեռքի տակ եղած սարքի վրա: Սրա արդյունքում Signal-ի համակարգը թիրախի սարքին է ուղարկում մեկանգամյա օգտագործման վեցանիշ վավեր կոդ (One time password, OTP):
3. Չարագործը թիրախից պահանջում է ուղարկել OTP կոդը՝ «ինքնությունը հաստատելու համար»:
4. Եթե տուժողը կատարում է այդ պահանջը, իսկ գրանցման արգելքն անջատված է, չարագործը հաշիվը հաջողությամբ վերագրանցում է իր սարքում:



Signal Support-ի կեղծ հաղորդագրության էկրանանկար

Անհրաժեշտ պաշտպանության միջոցներ

Այս հարձակումն ամբողջովին չեզոքացվում է, երբ միացվում է Signal-ի «Գրանցման արգելքը» (Signal Settings > Account > Registration Lock): Եթե այն միացված է, հեռախոսահամարը նոր համարին վերագրանցելու համար պահանջվում է օգտատիրոջ կողմից ստեղծված PIN կոդ, ինչը բավարար չէ, որ մեկանգամյա օգտագործման վավեր կոդ ունեցող չարագործը զավթի տվյալ հաշիվը:

5.2 Էլեկտրոնային նամակների և մի քանի հարթակների կիրառմամբ ֆիշինգ

Միջադեպ 5.2.1. Հայաստանյան ՀԿ-ի դեմ թիրախավորված ֆիշինգ՝ վարչապետի անվան օգտագործմամբ

2025թ. մայիսի 28-29
Թիրախ՝ Հայաստանյան ՀԿ (CyberHUB-AM-ի գործընկեր)

2025 թվականի մայիսի 28-ին CyberHUB-AM-ը բացահայտել է լավ մշակված, բարդ ֆիշինգային հարձակում, որի թիրախում եղել է իր գործընկեր ՀԿ-ներից մեկը: Հարձակման հեղինակներն ուղարկել են ֆիշինգային նամակ՝ PDF փաստաթղթի հղումով, որը քողարկված էր իբրև վարչապետի աշխատակազմի ղեկավարի պաշտոնական հրավեր (ֆայլի անվան մեջ օգտագործելով ՎԱՀԱԳՆ ԽԱՉԱՏՐՅԱՆ/ VAHAGN KHACHATRYAN անունը), ինչը վկայում է թիրախի նախնական հետազոտության մասին:

Dear Sir

Please find your formal invitation from the Republic of Armenia's Office of the Prime Minister attached.

VAHAGNKHACHATRYAN0-INVITATION-SCANDOC.PDF

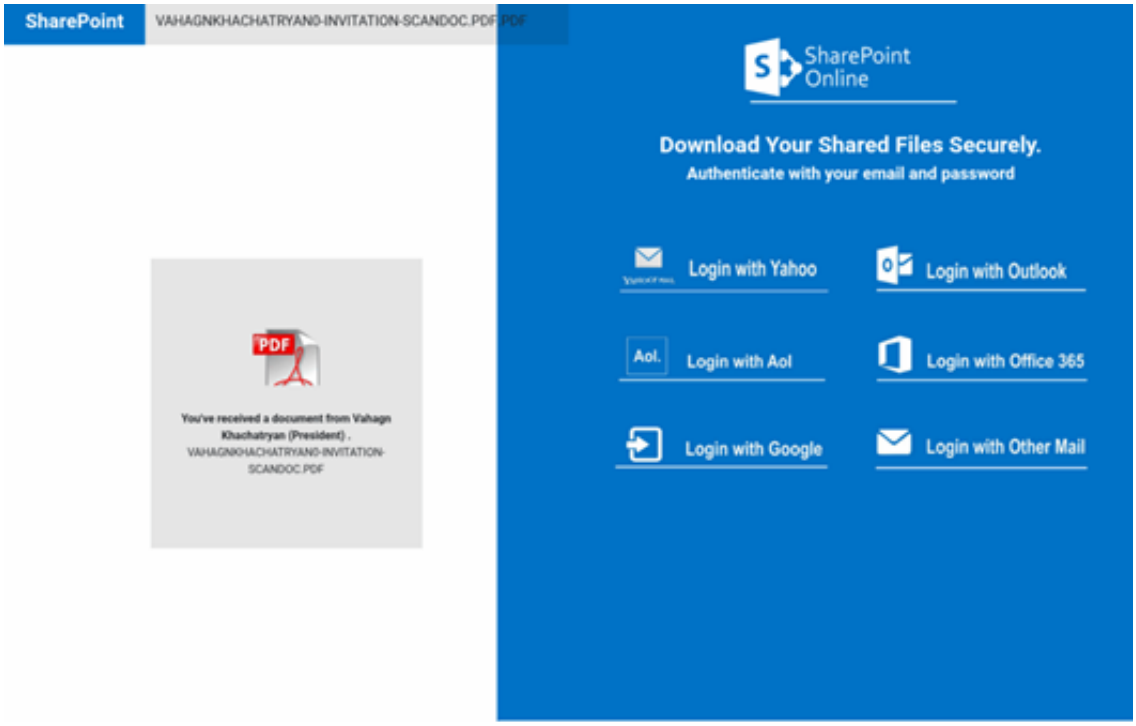
Regards

Arayik Harutyunyan

Chief of Staff (Armenia)
Address: Republic Square, Government House 1, 0010 Yerevan, Republic of Armenia
chief0fstaff@gov.am
Tel:(+374 60) 372109
Mobile:(+374 96) 030000

Վարչապետի աշխատակազմի ղեկավարի անունից ուղարկված ֆիշինգային էլեկտրոնային նամակի էկրանանկար, 2025թ. մայիս:

Վերաուղղորդման շղթայում օգտագործվել է Snip.ly հղումների համառոտիչը՝ քողարկելու համար իրական բովանդակության նմանությամբ ստեղծված GitHub Pages-ի asw910.github.io վնասակար կայքը: Էջում տեղակայված JavaScript-ը (jquery.min.js) կատարել է մուտքային տվյալների հավաքագրում և, օգտագործելով POST հարցումները, հափշտակված տվյալները փոխանցել է WordPress-ի կոտրված կայք:



ՀԿ-ին թիրախավորող տվյալների հավաքագրման ֆիշինգային էջի էկրանանկար

MITRE ATT&CK-ի քարտեզագրումը

- T1566.001 - ֆիշինգային նամակ՝ կցված ֆայլով
- T1584 - ենթակառուցվածքի վնասում (GitHub Pages, WordPress)
- T1204.002 - օգտագործողից կողմից գործարկում. վնասաբեր ֆայլի բացում
- T1056.001 - մուտքագրվող տվյալների հավաքագրում կեղծ հավատարմագրերի ձևի միջոցով
- T1071.001 - կիրառական մակարդակի արձանագրություններ՝ վեբ արձանագրություններ

Ցուցիչի տեսակը	Ցուցիչի տվյալը	Նկարագիրը
URL	hxxps[://]snip[.]ly/l9xqzf	Սկզբնական վերաուղղորդման URL
Դոմեյն	asw910[.]github[.]io	GitHub Pages-ում վնասաբեր ֆայլի հոսթ
URL	hxxps[://]wbbuffetchurrascobh[.]com[.]br/wp-admin/email[.]php	Մուտքային տվյալների հափշտակման վերջնակետ

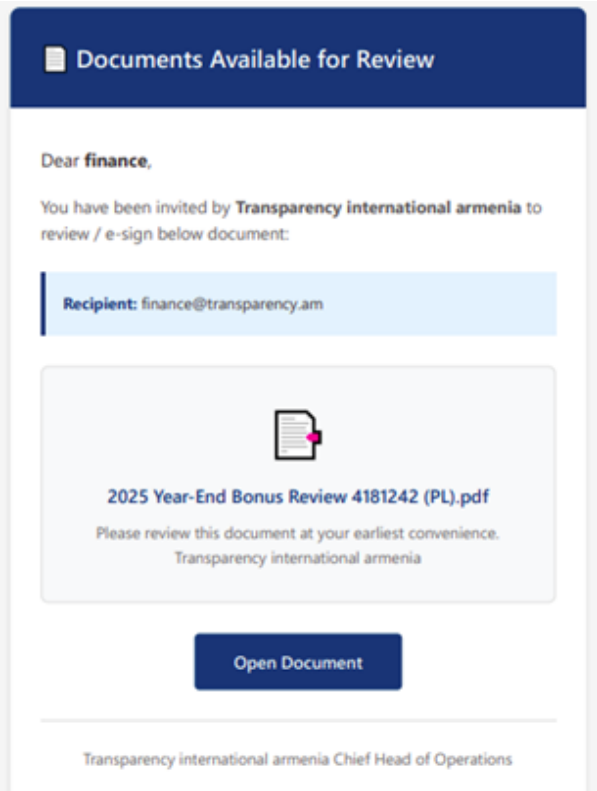
Միջադեպ 5.2.2. PDF → Google Maps → AWS ենթակառուցվածք ֆիշինգային շղթա

2025թ. դեկտեմբերի 18

Թիրախ՝ «Թրանսփարենսի Ինթերնեշնլ Հայաստան»

«Թրանսփարենսի Ինթերնեշնլ Հայաստան» հակակոռուպցիոն կենտրոնը հայտնվել է ֆիշինգային արշավի թիրախում: Կիրառվել է հղումների սկանավորման գործիքներից խուսափելու համար նախատեսված բազմաստիճան վերաուղղորդման շղթա: Հարձակումը սկսվել է medinex[.]in (հնդկական բժշկական ընկերություն է, որն առնչություն չունի թիրախի հետ) դոմեյնից ուղարկված «Documents Available for Review» («Դիտարկման համար ներկայացված փաստաթղթեր») թեմայով էլեկտրոնային նամակներով, որտեղ օգտագործվել է կեղծ հղման ID՝ պաշտոնականի տպավորություն թողնելու համար:

Էլեկտրոնային նամակը պարունակում էր կից PDF ֆայլ՝ կենտրոնում աչքի զարնող «Open Document» կոճակով: Մկնիկը հղման վրա պահելիս այն ցույց էր տալիս Google Իսպանիա (maps.google.es), սակայն սեղմելիս իրականում վերաուղղորդում էր դեպի վնասակար AWS S3 պահոց: Իբրև քողարկող շերտ այս վստահելի Google URL-ի կիրառումը հատուկ նախատեսված է էլեկտրոնային փոստի անվտանգության գործիքները շրջանցելու և մոլորեցնելու համար այն հասցեատերերին, որոնք հղումները սեղմելուց առաջ դրանց վրա պարզապես պահում են մկնիկը:



Ներդրված վերաուղղորդման կոճակով վնասակար PDF ֆայլի էկրանանկար, 2026թ. փետրվար:

Կասկածելի նշաններ

- Ընդհանրական ողջույն («Dear finance»)՝ զուգակցված հրատապության զգացում առաջացնող լեզվի հետ:
- PDF ֆայլը մեկ պատկեր է՝ կոճակով. օրինական փաստաթղթերն այդ ձևաչափով չեն լինում:
- Ուղարկողի դոմեյնը (medinex.in բժշկական պարագաների մատակարար, Հնդկաստան) տրամաբանական կապ չունի բովանդակության հետ:
- Տեսանելի URL-ը տարբերվում է վերաուղղորդման իրական հասցեից:

Ցուցիչի տեսակը	Ցուցիչի տվյալը	Նկարագիրը
Դոմեյն	medinex[.]in	Ուղարկողի դոմեյն՝ հնդկական բժշկական մատակարար
URL	hxxps[://]maps[.]google[.]es/url?q=[redirect]	Google Maps-ով քողարկված URL
URL	hxxps[://]bombapratclfnbjsmlkd58493849indexhtml[.]s3-website-us-east-1[.]amazonaws[.]com	Իրական վնասակար հասցե (AWS S3)

5.3 Սոցիալական ինժեներիա և ֆինանսական խարդախություն

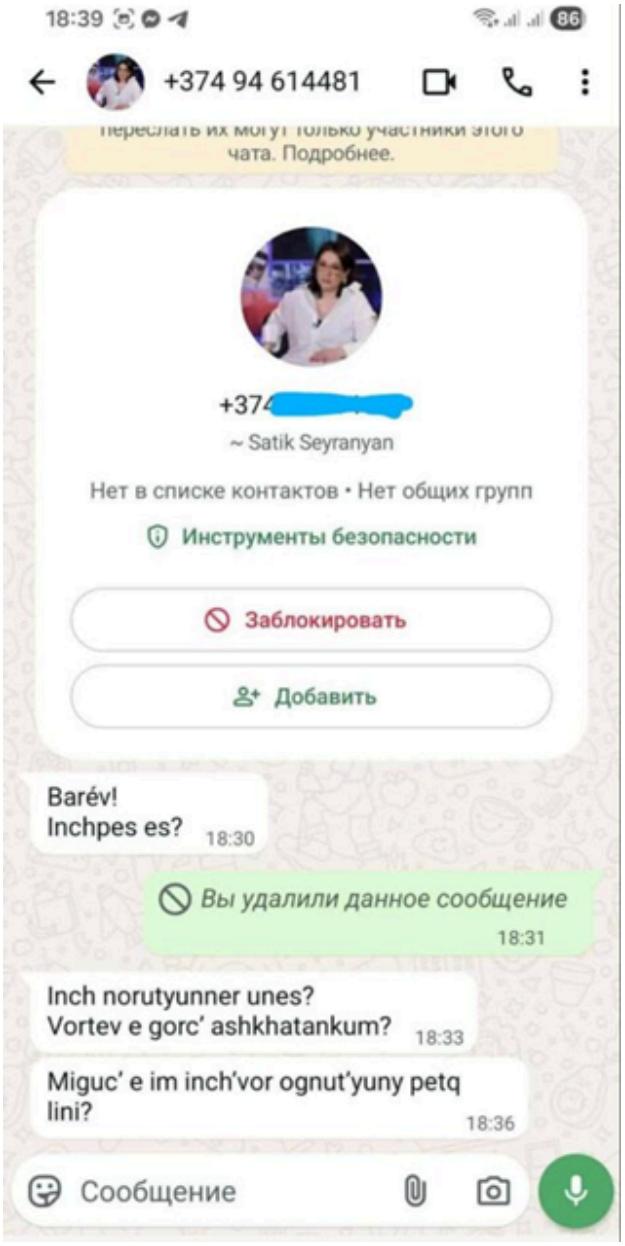
Միջադեպ 5.3.1. WhatsApp-ով բազմաստիճան խաբեություն՝ ԱԱԾ-ի կեղծ անվան կիրառմամբ

2025 թվականի հոկտեմբեր-նոյեմբեր

Թիրախ՝ հայաստանյան լրագրողներ և քաղաքացիական հասարակության ներկայացուցիչներ

2025 թվականի հոկտեմբերի վերջին, խիստ կատարելագործված բազմաստիճան սոցիալական ինժեներիայի գործողությամբ թիրախավորվել են հայկական լրատվամիջոցների և քաղաքացիական հասարակության ներկայացուցիչներ: Գործողությունը առանձնանում է մարդկային ռեսուրսների ներգրավմամբ, արհեստական բանականության օգնությամբ թարգմանության կիրառմամբ, ինչպես նաև իր հավանական երկու նպատակներով՝ ֆինանսական խարդախություն և հետախուզական տվյալների հավաքագրում կամ ճնշում գործադրելու փորձ:

Հարձակման ժամանակ կոտրված հայկական հեռախոսահամարներն օգտագործվել են թիրախին քաջ ծանոթ գործընկերների անունով կեղծ WhatsApp հաշիվներ ստեղծելու համար: «168 ժամ» լրատվամիջոցի խմբագիրը հրապարակավ հայտարարել է, որ իր անունն օգտագործվել է այլ լրագրողներին թիրախավորող կեղծ հաշիվներում:



«168 ժամ»-ի խմբագրի անունից հանդես եկող կեղծ WhatsApp հաշվի էկրանանկար:

Էկրանանկար, որը ցույց է տալիս ենթադրաբար արհեստական բանականության թարգմանության սխալը. ռուսերեն մեկ բառ մնացել է չթարգմանված՝ բացահայտելով ոչ լեզվակրի հանգամանքը:

Հարձակման քայլերի հաջորդականություն

1. Զեղծարարը, ներկայանալով ոլորտի ծանոթ մասնագետի անունից, WhatsApp-ում կապ է հաստատում թիրախի հետ՝ նշելով, որ փոխել է հեռախոսահամարը:
2. Անհատական զրույցի միջոցով կապ հաստատելուց հետո (թիրախի մասնագիտական շրջանակի ուսումնասիրության շնորհիվ), զեղծարարը հայտնում է, թե իբր թիրախը անարդար կերպով մեղադրվում է ադրբեջանական հանցավոր եկամուտների հետ կապված ֆինանսական հանցագործությունների համար:
3. Խաբեբան նշում է, թե իբր այդ գործով զբաղվում է Հայաստանի ազգային անվտանգության ծառայությունը (ԱԱԾ)՝ խնդրելով, որ թիրախը համագործակցի քննության հետ:
4. Թիրախին է զանգահարում մի երկրորդ անձ: Ներկայանալով որպես ԱԱԾ աշխատակից և խոսելով ռուսերեն՝ նա հայտնում է, որ սա Հայաստանի և Ադրբեջանի իրավապահների համատեղ գործողություն է:
5. Կեղծ ԱԱԾ աշխատակիցը թիրախին հորդորում է փոխանցել իր անձնական բանկային հաշվի միջոցները «ԱԱԾ անվտանգ հաշվին»՝ իբր դրանք հանցավոր աղբյուրներից ստացված եկամուտներից առանձնացնելու նպատակով:

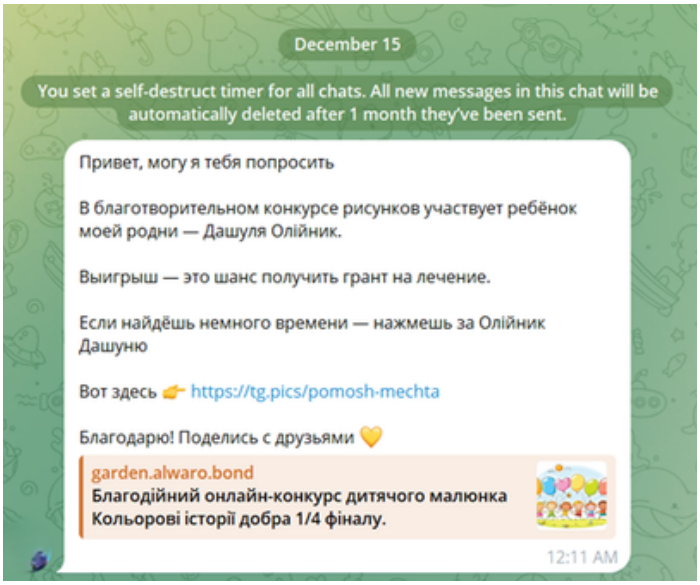
Բոլոր թիրախավորված անձինք կամ ինքնուրույն, կամ CyberHUB-AM-ի կողմից նախազգուշացվելուց հետո հասկացել են, որ դա խարդախություն է, և որևէ գումար չեն փոխանցել:

CyberHUB-AM-ի թիմի կարծիքով ֆինանսական հափշտակությունից զատ, հնարավոր է, գործողությունը նպատակ է ունեցել հավաքելու հետախուզական տվյալներ՝ քաղաքացիական հասարակության և մեդիա ոլորտի ազդեցիկ գործիչների վրա ապագայում ճնշման լծակներ ձեռք բերելու համար: Գործողությանը նախորդող ուսումնասիրությունների և մարդկային ռեսուրսների ներգրավման մակարդակը բնորոշ է Ռուսաստանին հետ կապված COLDRIVER (հայտնի է նաև որպես Star Blizzard, UNC4057 կամ Callisto) սպառնալիքի խմբին: Արշավի ընթացքում WhatsApp-ի կիրառումը և գործընկերների անունից հանդես գալը վկայում են, որ խումբը ռազմավարական անցում է կատարել դեպի բջջային հաղորդակցման հարթակներ և վստահության կառուցման երկարաժամկետ մարտավարության՝ նախատեսված ինստիտուցիոնալ անվտանգային համակարգերը շրջանցելու համար:

Միջադեպ 5.3.2. Telegram-յան «Քվեարկեք իմ ազգականի օգտին» հաշվին տիրանալու արշավ

2025թ. դեկտեմբեր
Թիրախ՝ Հայաստանում Telegram-ի օգտատերեր

2025 թվականի դեկտեմբերին արձանագրված սոցիալական ինժեներիայի կիրառմամբ ամենատարածված հարձակումներից մեկը հենվում է հուզական մանիպուլյացիայի և ծանոթ հասցեների նկատմամբ վստահության վրա: Հարձակման սկզբում թիրախը իր ծանոթներից մեկին պատկանող կոտրված Telegram հաշվից ստանում է հաղորդագրություն, որում խնդրանք է՝ օգնելու «բարեգործական մրցույթում երեխայի օգտին» քվեարկությամբ:



«Քվեարկեք իմ ազգականի օգտին» խնդրանքով առաջին հաղորդագրության էկրանանկար, 2025թ. դեկտեմբեր:

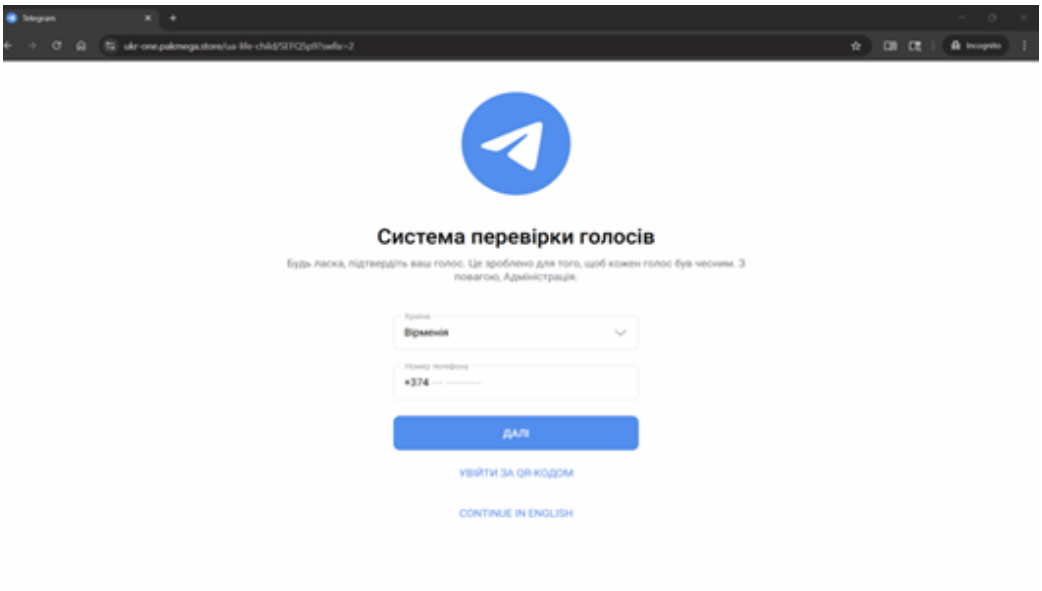
Հարձակման մեխանիզմ

- Հաղորդագրությունը պարունակում է հղում, որը, թվում է, առնչվում է Telegram-ին (օրինակ՝ tg[.]pics/pomosh-mechta), սակայն իրականում բազմաթիվ շղթաներով անցնելով վերաուղղորդում է դեպի քվեարկության կեղծ էջ:
- Կեղծ էջը, հնարավորինս հավաստի թվալու նպատակով, պրոֆեսիոնալ ձևավորում ունի՝ երեխաների նկարներով, ժամանակի հետհաշվարկով և հովանավորների լոգոներով:
- Կայքը ցուցաբերում է ըստ իրավիճակի գործելու կարողություն. ավտոմատ վերլուծական համակարգերով (VirusTotal, URLScan) մուտք գործելիս այն օգտատիրոջը վերաուղղորդում է դեպի անվնաս բովանդակություն (օրինակ՝ TikTok): Իրական բջջային զննարկչից մուտք գործելու դեպքում հայտնվում է հարձակման բովանդակությունը:
- «Քվեարկել» կոճակը սեղմելով՝ բացվում է «վավերացման» էջ, որը պահանջում է թիրախի հեռախոսահամարը, իսկ ֆոնային ռեժիմում աննկատելիորեն սկսում է Telegram իրական մուտքի գործընթաց, որի արդյունքում օգտատերը իր սարքին ստանում է մեկանգամյա օգտագործման OTP կոդ:
- Էջը զոհին հրահանգում է մուտքագրել ստացված կոդը՝ «վավերացում» անցնելու համար, ինչի արդյունքում կիբեռհանցագործը ստանում է լիարժեք հասանելիություն նրա հաշվին:

Պրոֆեսիոնալ ձևավորմամբ կեղծ բարեգործական մրցույթի էջի էկրանանկար:

Հարձակման կանխում

- Երբեք մի՛ մուտքագրեք Telegram-ի մուտքի կոդերը որևէ այլ կայքում. այս կոդերը նախատեսված են միայն Telegram հավելվածի ներսում օգտագործման համար:
- Միացրեք երկփուլային վավերացումը Telegram-ի կարգավորումներում:
- Նմանօրինակ հաղորդագրություններ ստանալու դեպքում, ստուգման նպատակով կապվեք ուղարկողի հետ այլ հարթակում. նրա Telegram հաշիվը, ամենայն հավանականությամբ կոտրված է:



Telegram-ի հաշվին տիրանալու գործընթացը սկսող «վավերացման» էջի էկրանանկար:

5.4 Չարամիտ ծրագրեր և խարդախ հավելվածներ

Միջադեպ 5.4.1: ArmScan.apk. կառավարության անունից տարածվող կեղծ «քեշբեք» հավելված

2025թ. դեկտեմբերի 16

Թիրախ՝ Հայաստանում սմարթֆոնների օգտատերեր

ArmScan.apk անունով վնասակար Android հավելվածը տարածվել է gov-am.sbs դոմեյնից՝ ներկայանալով իբրև կառավարության կողմից տրամադրվող ֆինանսական գործիք: Կեղծ կայքը, շահարկելով պետական աջակցության ծրագրերի վերաբերյալ հանրության շրջանում ձևավորված սպասումները, նշում էր, թե օգտատերերը կարող են տվյալ ծրագրով սկանավորել ՀԴՄ կտրոնները և ստանալ պետական հետվճարներ: Դոմեյնի WHOIS գրանցման տվյալները ցույց են տալիս, որ այն կապված է Մալայզիայի հետ, սակայն չի առնչվում որևէ պետական կառույցի:

VirusTotal-ը հավելվածը համարել է վնասակար (նախնական հայտնաբերման պահին ցածր աստիճանի վտանգավորությամբ): Մի շարք հակավիրուսային համակարգեր այն որակել են իբրև Trojan/Dropper, այսինքն՝ այն կարող է և՛ սարքից տվյալներ հավաքագրել, և՛ ներբեռնել լրացուցիչ վնասակար, այդ թվում ենթադրաբար բանկային տվյալներ հափշտակող ծրագրեր:

Օգտատերերի պաշտպանության ուղեցույց

- Ներբեռնեք և տեղադրեք հավելվածներ միայն պաշտոնական Google Play Store-ից:
- Ստուգեք պետական ծառայությունների մասին տեղեկությունները gov.am դոմեյնում գրանցված պաշտոնական կայքերում:
- Մեծ կասկածանքով վերաբերվեք առաջարկվող քեշբեքների կամ սուբսիդիաների հավելվածների գովազդներին:
- Երբեք մի՛ մուտքագրեք բանկային տվյալները կամ անհատական նույնականացման համարները ոչ պաշտոնական հարթակներով տարածվող հավելվածներում:
- Անջատեք «Տեղադրում անհայտ աղբյուրներից» («Install from Unknown Sources») գործառույթը Android կարգավորումներում:

Ցուցիչի տեսակը	Ցուցիչի տվյալը	Նկարագիրը
Դոմեյն	gov-am[.]sbs	Վնասակար կայք, որը ներկայանում է Հայաստանի կառավարության անունից
Ֆայլ	ArmScan[.]apk	Վնասակար Android հավելված (Trojan/Dropper)
Hash (SHA256)	ece1d80a3d0d8fea0d635d6acf432f75d15355bcc8cab62a0089a6a72b909a90	ArmScan.apk

06

Հայաստանի պաշտպանական կարողությունների ընդհանուր վիճակը

Սրվող սպառնալիքների ֆոնին՝ Հայաստանը 2025 թվականին էականորեն վերանայել է կիբեռանվտանգության կառավարման իր համակարգը: Արձագանքման միջոցառումների թվում են օրենսդրական բարեփոխումները, ինստիտուցիոնալ զարգացումը, քաղաքացիական հասարակության կարողությունների զարգացումը և հանրության կրթությունը:

6.1 Օրենք կիբեռանվտանգության մասին

Հայաստանի նոր պաշտպանական մոտեցման անկյունաքարը 2025 թվականին «Կիբեռանվտանգության մասին» համապարփակ օրենքի ընդունումն է: 2026 թվականին ամբողջությամբ ուժի մեջ մտնող օրենսդրությունը ներդնում է առանցքային կարգավորող մեխանիզմներ, որոնք նախկինում բացակայում էին Հայաստանի իրավական շրջանակից:

Առանցքային դրույթ	Նկարագիր	Ռազմավարական ազդեցություն
Կենսական նշանակության ոլորտներ	Սահմանում է ոլորտները, որոնք ունեն առանցքային նշանակություն բնակչության բնականոն գործունեության, տնտեսական ակտիվության, պետական անվտանգության, հանրային առողջության և անվտանգության կամ շրջակա միջավայրի պահպանման, Հայաստանի Հանրապետության կենսական նշանակության այլ շահերի պաշտպանության համար:	Սահմանում է այն ոլորտները, որոնց շրջանակներում կիբեռանվտանգության պահանջները կիրառվում են տեղեկատվական համակարգերի նկատմամբ, ներառյալ կիբեռմիջադեպերի հայտնաբերման, դրանց մասին ծանուցման, կանխարգելման և լուծման, վերահսկողության, ինչպես նաև կիբեռանվտանգության աուդիտի հետ կապված պարտավորությունները:

Առանցքային դրույթ	Նկարագիր	Ռազմավարական ազդեցություն
Կրիտիկական տեղեկատվական ենթակառուցվածքներ	Սահմանում է նույնականացման իրավական չափանիշներ էներգետիկայի, ֆինանսական ծառայությունների և հեռահաղորդակցության ոլորտներում կրիտիկական տեղեկատվական ենթակառուցվածքները:	Պահանջում է օպերատորներից ներդնել կիբեռանվտանգության պահանջներ և անցնել կիբեռանվտանգության աուդիտներ՝ հիմնվելով կիրառելի միջազգային կամ ազգային ստանդարտների վրա:
Միջադեպերի մասին ծանուցում	Սահմանում է պարտադիր ժամկետներ պետական և մասնավոր կառույցների համար՝ խախտումների մասին ազգային համակարգչային արտակարգ իրավիճակների արձագանքման թիմին (CERT) հայտնելու համար:	Բարելավում է ազգային մակարդակում սպառնալիքների տեսանելիությունը և ապահովում է արագ միջոլորտային արձագանք:
Ստանդարտացում	Ներկայացնում է կիբեռանվտանգության կառավարման և անվտանգության պահանջներ կենսական նշանակության ոլորտներում և առանցքային տեղեկատվական ենթակառուցվածքներում գործող տեղեկատվական համակարգերի համար: Նախատեսում է կիբեռանվտանգության ազգային ստանդարտների մշակում, ինչպես նաև տարբեր ոլորտների համար կիրառելի միջազգային ստանդարտների սահմանում:	Ստեղծում է կիբեռռիսկերի կառավարման, միջադեպերին արձագանքման, մշտադիտարկման և կիբեռանվտանգության աուդիտների միասնական ազգային համակարգ: Նպաստում է արևմտյան գործընկերների հետ ավելի խորը համագործակցությանը և բարելավում ներդրումային միջավայրը:
Կարգավորող մարմին	Նախատեսվում է ստեղծել անկախ պետական մարմին՝ պաշտոնական վերահսկողության և իրավակիրառական լիազորություններով:	Կենտրոնացնում է կառավարումը՝ նվազեցնելով նախարարությունների միջև պատասխանատվության կիսումը:

6.2 Բարեփոխումներ անձնական տվյալների պաշտպանության ոլորտում

2025 թվականին Հայաստանը նախաձեռնել է բարեփոխումներ՝ միտված անձնական տվյալների պաշտպանության (ԱՏՊ) վերահսկող մարմինը լիովին անկախ և ավելի լավ ռեսուրսներով հագեցած կառույցի վերափոխելուն: Չնայած նախևառաջ տվյալների պաշտպանության նախաձեռնություն լինելուն՝ այն նաև հզորացնում է կիբեռանվտանգությունը՝ հաշվի առնելով, որ Հայաստանի ԱՏՊ օրենքը կիրառվում է բոլոր ոլորտներում և սահմանում անձնական տվյալների պաշտպանության երաշխիքներ, այդ թվում՝ «Կիբեռանվտանգության մասին» օրենքով չնախատեսված ոլորտներում:

Այս բարեփոխման շնորհիվ զգալիորեն բարելավվում են ԱՏՊ մարմնի ինստիտուցիոնալ կարողությունները: Ներկայիս մարմինն ունի սահմանափակ անձնակազմ և ռեսուրսներ, ինչը նվազեցնում է պետական և մասնավոր հատվածներում տվյալների մշակման նրա վերահսկողական կարողությունները: Անկախության ամրապնդումը և կարողությունների հզորացումը կնպաստեն լավարկելու հիմնական պարտականությունների կատարումը, ներառյալ՝ տվյալների անվտանգության խախտումների պարտադիր բացահայտումը: Բարեփոխման սկիզբը դրվել է 2025 թվականի օգոստոսին՝ ԵՄ կողմից ֆինանսավորվող մեկամյա ծրագրի շնորհիվ, որի հիմնական նպատակն էր պատրաստել օրենսդրական փոփոխություններ՝ ԱՏՊ մարմնի լիակատար անկախությունն ապահովելու համար:

Այս նախաձեռնությունը քաղաքական աջակցություն է ստացել 2025 թվականի հոկտեմբերի 31-ին՝ վարչապետի գլխավորությամբ անցկացված խորհրդակցության ժամանակ, որտեղ ներկայացվել են նոր անկախ ԱՏՊ մարմնի հայեցակարգը և դրա իրականացման քայլերը: 2025 թվականի նոյեմբերի 5-ին Եվրոպական հանձնաժողովը ներկայացրել է Հայաստան-ԵՄ մուտքի արտոնագրերի ազատականացման գործողությունների ծրագիրը, որը սահմանում է անձնական տվյալների պաշտպանության չափորոշիչները: Դրանց թվում են անկախ վերահսկող մարմնի ստեղծումը, ԱՏՊ օրենսդրության կիրառումը բոլոր ոլորտներում և պետական կառույցների համար ուսուցման ծրագրերի և ուղեցույցների մշակումը: Ակնկալվում է, որ այս միջոցառումները կհզորացնեն Հայաստանի կառավարման համակարգը՝ նպաստելով ավելի դիմակայուն թվային և կիբեռանվտանգության միջավայրի ձևավորմանը:

6.3 Ինստիտուցիոնալ զարգացում. ՀՏՀԳ և AM-CERT

2022 թվականին հիմնադրված և 2025 թվականի օրենսդրությամբ զգալի լիազորություններով օժտված Հայաստանի տեղեկատվական համակարգերի գործակալությունը (ՀՏՀԳ), որն առաջիկայում նախատեսվում է վերափոխել անկախ պետական կարգավորող մարմնի (հանձնաժողովի), գործում է իբրև երկրի կիբեռպաշտպանության համակարգի գործառնական կենտրոն:
2025 թվականի հիմնական իրադարձությունների թվում են.

- AM-CERT-ի գործառնականացում. ՀՏՀԳ-ի ներքո գործող համակարգչային միջադեպերի արձագանքման Հայաստանի ազգային թիմը (AM-CERT) 2025 թվականի հոկտեմբերին Միջազգային հեռահաղորդակցության միության (International Telecommunication Union, ITU) հետ համագործակցությամբ մասնակցել է միջազգային կիբեռվարժանքների: Այդ վարժանքների ընթացքում ստուգվել է կարևորագույն ենթակառուցվածքների վրա սիմուլյացված APT հարձակումներին արձագանքելու երկրների պատրաստվածությունը:
- Ոլորտային պաշտպանություն. Հայաստանի կենտրոնական բանկը շարունակում է պահպանել ֆինանսական կառույցների համար կայացած ոլորտային CSIRT (Computer Security Incident Response Team, համակարգչային միջադեպերի արձագանքման ազգային թիմ)՝ բանկային հատվածի կազմակերպությունների համար ապահովելով միջադեպերի մասնագիտացված արձագանք:
- Թվային նույնականացում («ԵսԵՄ»). ՀՏՀԳ-ն ղեկավարում է «ԵսԵՄ» թվային ինքնության նախագիծը, որն ապահովում է պետական ծառայություններից անվտանգ օգտվելու մեկ միասնական նույնականացման համակարգ: Այս հարթակը հարձակումներից պաշտպանելը գերակա խնդիր է, քանզի դրա խափանումը կարող է ազդել միաժամանակ բազմաթիվ հանրային ծառայությունների վրա:

6.4 Քաղաքացիական հասարակություն. CyberHUB-AM-ի դերը

CyberHUB-AM-ը ամրապնդել է իր դիրքերը որպես Հայաստանի քաղաքացիական հասարակության և անկախ լրատվամիջոցների փաստացի CERT: 2025 թվականին CyberHUB-AM-ը պատշաճ արձագանք է ցուցաբերել ՀԿ-ների և ակտիվիստների մասնակցությամբ միջադեպերին՝ վեր հանելով լրտեսող ծրագրերով նպատակային հարձակումներ և կատարելագործված թիրախային ֆիշինգի արշավներ: 5-րդ բաժնում ներկայացված ութ դեպքերը բացահայտվել, վերլուծվել կամ արձագանք են ստացել CyberHUB-AM թիմի կողմից:

Քաղաքացիական հասարակության պաշտպանությանը միտված այս անվտանգային ներուժը, պետական կառույցների հետ մեկտեղ, նրանց լրացնող և անփոխարինելի դեր է կատարում. չարագործները միտումնավոր թիրախավորում են այն կազմակերպությունները, որոնք ունեն քաղաքական նշանակություն, ֆինանսական ռեսուրսների սակավություն և դուրս են կառավարության կիբեռանվտանգության մարմինների ծածկույթից: CyberHUB-AM-ը, այս կազմակերպություններին տեխնիկական փորձաքննություն, միջադեպերի արագ արձագանք և թվային անվտանգության նպատակային ուսուցում ապահովելով, լրացնում է Հայաստանի ընդհանուր պաշտպանական համակարգում առկա կառուցվածքային բացը:

6.5 Կրթություն և հանրային իրազեկում

- «ԿիբեռԱմիս» արշավ. ՀՀ բարձր տեխնոլոգիական արդյունաբերության նախարարության և ՀՏՀԳ-ի համատեղ ազգային իրազեկման նախաձեռնություն, որը ներառել է աշխատաժողովներ և սեմինարներ ամբողջ Հայաստանում, 2025 թվականի ընթացքում:
- Դպրոցական թվային անվտանգության ծրագիր. ՅՈՒՆԻՍԵՖ-ի և կրթական ՀԿ-ների գործընկերությամբ իրականացվող ծրագիր՝ միտված թվային անվտանգության ուսումնական ծրագրերը հանրակրթական դպրոցներում ներդնելուն: Նախաձեռնության անմիջական նպատակը սոցիալական ինժեներիայի կիրառմամբ արշավներում մարդկային գործոնի խոցելիությունները նվազեցնելն է:
- «ԿիբեռՉատ» հարթակ (chat.cyberhub.am). CyberHUB-AM-ի նախաձեռնած և ՅՈՒՆԻՍԵՖ-ի ու Միացյալ Թագավորության դեսպանատան աջակցությամբ իրականացվող այս թվային օգնության հարթակը երեխաներին և դեռահասներին հնարավորություն է տալիս հաղորդելու կիբեռհարձակումների և առցանց սպառնալիքների մասին: Սա Հայաստանում երիտասարդների առցանց անվտանգության համար նախատեսված առաջին նման հարթակն է:

Եզրակացություններ և ռազմավարական հեռանկար

07

7.1 Հիբրիդային շրջափակումը շարունակվում է

Այս զեկույցում ներկայացված փաստերը հաստատում են, որ Հայաստանը բախվում է շարունակական, բազմավեկտոր կիբեռարշավի, որն իրականացվում է քաղաքական դրդապատճառներով՝ պրոֆեսիոնալ և գնալով կատարելագործվող մեթոդներով: «Հիբրիդային շրջափակում» կոնցեպտը ճշգրտորեն բնութագրում է իրավիճակը. հակամարտությունը ֆիզիկական դաշտից տեղափոխվել է թվային տիրույթ, որտեղ այն իրականացվում է ավելի մեծ անանունության պայմաններում, ավելի քիչ ծախսերով և ոչ թե դրվագային, այլ շարունակական ինտենսիվությամբ:

Իբրև հարձակման հիմնական ուղղություն էլեկտրոնային փոստից հաղորդակցման գաղտնագրված հարթակներին անցումը 2025 թվականի ամենակարևոր մարտավարական փոփոխությունն է: Սա նպատակային արձագանք է կազմակերպությունների՝ էլ-փոստի անվտանգության բարելավմանը և արտացոլում է ավելի խորը ռազմավարական պատկերացում: Ամենաարժեքավոր թիրախները՝ քաղաքացիական հասարակության առաջնորդները, լրագրողները, պետական պաշտոնյաները, որպես իրենց հաղորդակցման հիմնական միջոցներ, զգայուն թեմաներով մասնագիտական աշխատանքում օգտագործում են Signal և WhatsApp: Անվտանգություն ապահովողները պետք է հարմարվեն այս փոփոխություններին:

7.2 2026-ի ընտրությունների ռիսկի պատուհանը

CyberHUB-AM-ի գնահատմամբ՝ մեծ է հավանականությունը, որ Հայաստանի 2026 թվականի գալիք խորհրդարանական ընտրություններին ընդառաջ կաճեն արտաքին միջամտության գործողությունների հաճախականությունն ու ինտենսիվությունը: 2025 թվականին արձանագրված արշավները դրա նախնական դիրքավորման փուլն են՝ ենթակառուցվածքների ստեղծում, ազդեցիկ թիրախների հայտնաբերում, սոցիալական ինժեներիայի մեթոդների փորձարկում և հետագա գործողություններում կիրառելու նպատակով տվյալների հավաքագրում և կազմակերպություններ մուտքի ապահովում:

Ընտրությունների հետ կապված սպառնալիքները, հավանաբար, կդրսևորվեն մի քանի ուղղություններով միաժամանակ՝ ընտրական ենթակառուցվածքների և կառավարության կոմունիկացիաների դեմ տեխնիկական հարձակումներ, հասարակության պառակտվածությունը խորացնելու և արդար ընտրությունների նկատմամբ վստահությունը խաթարելու համար նախատեսված ազդեցության գործողություններ, թեկնածուների, կուսակցական գործիչների և դիտորդների թիրախավորված հետապնդում և վարկաբեկում, ինչպես նաև ֆինանսական խարդախություններ՝ միտված ընտրություններում դիտորդությամբ զբաղվող քաղաքացիական հասարակության կազմակերպություններին վարկաբեկելուն:

7.3 Առաջարկություններ շահագրգիռ կողմերին

Կառավարությանը և կարգավորող մարմիններին

- Արագացնել «Կիբեռանվտանգության մասին» 2025 թվականին ընդունված օրենքի կիրառումը, մասնավորապես՝ միջադեպերի մասին հաղորդելու պարտադիր պահանջների մասով, մինչև 2026 թվականի սահմանված ժամկետը:
- Ստեղծել նախընտրական կիբեռանվտանգության հատուկ աշխատանքային խումբ, որը կհամակարգի AM-CERT-ի, իրավապահ մարմինների և Կենտրոնական ընտրական հանձնաժողովի աշխատանքը:
- Ընդլայնել տեղեկությունների փոխանակման մեխանիզմները ԵՄ կիբեռանվտանգության կառույցների (European Union Agency for Cybersecurity (ENISA) և գործընկեր երկրների CERT-երի հետ՝ օգտագործելով ԵՄ-ին Հայաստանի ինտեգրման գործընթացը:
- Պետական մարմիններում պարտադիր դարձնել Microsoft 365 անվտանգության բազային կարգավորումների կիրառումը, ներառյալ Entra ID Conditional Access-ը և սարքերի գրանցման քաղաքականությունները:

Քաղաքացիական հասարակության կազմակերպություններին և անկախ լրատվամիջոցներին

- Միացնել Signal-ի «Գրանցման արգելքը» (Registration Lock) և Telegram-ի երկփուլային վավերացումը կազմակերպության բոլոր հաշիվներում՝ առանց բացառության:
- Սահմանել ստուգման ներքին կանոններ՝ հղումներ սեղմելու, տվյալներ տրամադրելու կամ գումար փոխանցելու ցանկացած հարցման համար՝ անկախ աղբյուրի ակնհայտությունից:
- Կապվել CyberHUB-AM-ին՝ կազմակերպության թվային անվտանգության գնահատման և թիրախային ուսուցման համար, հատկապես ընտրություններին ընդառաջ:
- Պաշտոնյաներից, դիվանագետներից կամ անվտանգության ծառայությունների աշխատակիցների մեսենջերներով ստացված ցանկացած անսպասելի հաղորդագրություն համարել պոտենցիալ խարդախություն, մինչև դրանք չստուգվեն այլ հարթակներով:

Բիզնեսներին

- Այն կազմակերպությունները, որոնք ընդգրկված են «Կիբեռանվտանգության մասին» օրենքի շրջանակում, պետք է պատրաստվեն օրենքի պահանջները կատարելուն (անկախ այն հանգամանքից, որ պաշտոնական պարտավորությունները ուժի մեջ են մտնելու ավելի ուշ), ինչպես նաև միջոցներ և ֆինանսավորում հատկացնեն կիբեռանվտանգության միջոցառումների համար:

- «Կիբեռանվտանգության մասին» օրենքի շրջանակից դուրս գտնվող կազմակերպությունները, անգամ պաշտոնական պարտավորության բացակայության պարագայում, կարող են կամավոր հիմունքներով կիրառել կիբեռանվտանգության համապատասխան միջոցառումները:
- Բոլոր բիզնեսներին

- Օգտագործել անվտանգ հաղորդակցման հարթակներ և միացնել երկփուլային վավերացումը բոլոր կորպորատիվ հաշիվներում:
- Ինչպես ներքին, այնպես էլ արտաքին մասնագետների ներգրավմամբ պարբերաբար անցկացնել կիբեռանվտանգության աուդիտներ:
- Դիմել CyberHUB-AM-ին՝ աջակցություն ստանալու համար այնպիսի հարցերում, ինչպիսիք են թվային անվտանգության գնահատումը, ուսուցումը և խորհրդատվությունը՝ կազմակերպության դիմակայունությունը հզորացնելու համար:
- Եվ այլն...

Լայն հասարակությանը

- Երբեք չփոխանցել SMS-ով ստացված մեկանգամյա օգտագործման կոդերը (OTP) կամ վավերացման կոդերը որևէ երրորդ կողմի որևէ հարթակում:
- Հավելվածներ տեղադրել միայն պաշտոնական հավելվածների հարթակներից, խիստ կասկածանքով վերաբերվել կառավարության աջակցություն, հետվճարներ կամ ֆինանսական օգուտներ գովազդող հավելվածներին:
- Միացնել երկփուլային վավերացումը բոլոր բանկային և ֆինանսական հավելվածներում:
- Ֆիշինգի կամ խարդախության փորձերի կասկածի մասին հայտնել CyberHUB-AM-ին (cyberhub.am), իսկ ֆինանսական խարդախության դեպքում՝ համապատասխան բանկի անվտանգության թիմին:

7.4 Ամփոփում

Հայաստանի ժողովրդավարական ինստիտուտների անվտանգությունը ներկայումս չի կարող ապահովվել միայն տեխնիկական միջոցներով. անհրաժեշտ է միասնական մոտեցում: Չարագործները ցույց են տվել, որ ունակ են իրական ժամանակում հարմարվելու պաշտպանական միջոցառումներին, մի խոցված թիրախից անցնելու մյուսին և շահագործելու սոցիալական և ինստիտուցիոնալ վստահությունը, որի վրա է հիմնված հասարակական կյանքը: Այս սպառնալիքին դիմակայելու համար անհրաժեշտ են ոչ միայն ավելի ուժեղ ենթակառուցվածքներ և ավելի լավ տեխնոլոգիաներ, այլև հասարակության մեջ թվային զգոնության մշակույթ, ինչպես նաև կայուն, բավարար ռեսուրսներով ապահովված քաղաքացիական հասարակության անվտանգության հատված, որն ունակ է պաշտպանելու նրանց, ում պետությունը չի կարող հասնել:

CyberHUB-AM-ը հանձնառու է մնում այս ուղղությամբ և կոչ է անում պետական մարմիններին, միջազգային գործընկերներին և մասնավոր հատվածին՝ ճանաչել այդ հանձնառությունը և աջակցել այն առանցքային դերին, որը Հայաստանի ժողովրդավարական դիմակայունության մեջ ունի քաղաքացիական հասարակության կիբեռանվտանգությունը:

Հավելված Ա.
Հարձակման ցուցիչները՝ մեկ տեղում

Սույն զեկույցում ներկայացված հարձակման բոլոր ցուցիչները բերված են ստորև՝ համախմբված տեսքով: Բոլոր տվյալները ներկայացված են վնասազերծված տարբերակով:

Միջադեպ	Տեսակ	Ցուցիչ	Նշումներ
5.1.1 UNC5792	Դոմեյն	add-group[.]tech	Սկզբնական դոմեյն
5.1.1 UNC5792	Դոմեյն	group-add[.]com	Հայտանբերումից հետո կիրառված նոր դոմեյն
5.1.1 UNC5792	Դոմեյն	signal-groups-add[.]com	Երրորդ փուլում օգտագործված դոմեյն
5.1.2 ԵՄ Դեսպան	IP հասցե	95[.]182[.]124[.]124	Biterika Group ՍՊԸ (Ռուսաստան)
5.1.2 ԵՄ դեսպան	IP հասցե	46[.]8[.]213[.]90	Biterika Group ՍՊԸ (Ռուսաստան)
5.1.2 ԵՄ դեսպան	IP հասցե	188[.]130[.]142[.]95	Biterika Group LLC (Ռուսաստան)
5.2.1 Razer	Դոմեյն	razer-us[.]com	Կեղծ դոմեյն (գրանցված 2024թ. դեկտեմբերի12-ին)
5.2.1 Razer	IP հասցե	198[.]54[.]127[.]77	Փոստային սերվեր
5.2.1 Razer	IP հասցե	198[.]54[.]118[.]220	Հոսթինգի սերվեր

Միջադեպ	Տեսակ	Ցուցիչ	Նշումներ
5.2.1 Razer	SHA256	693cc086...736bce4	msimg32.dll
5.2.1 Razer	SHA256	08c7fb60...10f7a2	Վնասակար .exe
5.2.2 ՀԿ-ի ֆիշինգ	Դոմեյն	snip[.]ly	URL համառոտիչի կիրառում
5.2.2 ՀԿ-ի ֆիշինգ	Դոմեյն	asw910[.]github[.]io	GitHub Pages-ում վնասաբեր ֆայլի հոսթ
5.2.2 ՀԿ-ի ֆիշինգ	URL	hxxps[://]wbbuffetchurrascobh[.]com[.]br/wp-admin/email[.]php	Մուտքային տվյալների հափշտակման վերջնակետ
5.2.3 ԹԻՀԿ	Դոմեյն	medinex[.]in	Ուղարկողի դոմեյն
5.2.3 ԹԻՀԿ	Դոմեյն	amazonaws[.]com (S3)	Վնասակար վերջնակետ
5.4.1 ArmScan	Դոմեյն	gov-am[.]sbs	Կեղծ պետական աջակցության կայք
5.4.1 ArmScan	SHA256	ece1d80a3d0d8fea0d635d6acf432f75d15355bcc8cab62a0089a6a72b909a90	ArmScan.apk

Հավելված Բ. Հղումներ

- Հայաստան. Թվային սպառնալիքների համապատկերը 2024, CyberHUB-AM. https://cyberhub.am/hy/blog/2025/06/26/armenia-cybersecurity-threat-landscape-2024/
- Spear Phishing in Armenia: Inside a Persistent Campaign by UNC5792 — CyberHUB-AM: https://cyberhub.am/en/blog/2025/05/31/spear-phishing-in-armenia-inside-a-persistent-campaign-by-unc5792/
- 2026-ին Հայաստանում սպասվող կիբեռանվտանգության սպառնալիքները , Media.am. https://media.am/hy/critique/2025/12/18/44372/
- New Android Malware 'Ajina.Banker' — The Hacker News: https://thehackernews.com/2024/09/new-android-malware-ajinabanker-steals.html
- Building the Architecture of Cybersecurity: Armenia's Institutional Turn — EVN Report: https://evnreport.com/politics/building-the-architecture-of-cybersecurity-armenias-institutional-turn/
- «Կիբեռանվտանգության մասին» օրենք, ARLIS. https://www.arlis.am/hy/acts/218672/latest
- Միջազգային կիբեռվարժանքներ Հայաստանում, ՀՏՀԳ. https://isaa.am/en/articles/international-cyberdrill-in-armenia-strengthening-resilience
- «ԵսԵՄ» թվային նույնականացման ազգային հարթակ, ՀՏՀԳ. https://isaa.am/armenia%E2%80%99s-digital-id-solution
- «ԿիբեռԱմիս 2025» նախաձեռնության մեկնարկը Հայաստանում, ՀՏՀԳ. https://isaa.am/articles/%D5%B6%D5%B8%D6%80%D5%B8%D6%82%D5%A9%D5%B5%D5%B8%D6%82%D5%B6%D5%B6%D5%A5%D6%80/launch-of-cyber-month-2025-in-armenia
- Երեխաների առցանց անվտանգության ապահովմանն ուղղված նոր համագործակցություն, ՅՈՒՆԻՍԵՖ. https://www.unicef.org/armenia/en/press-releases/new-partnership-advance-childrens-online-safety-armenia
- Phishing for Codes: Russian Threat Actors Target Microsoft 365 OAuth Workflows — Volexity: https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/
- Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication — Volexity: https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/