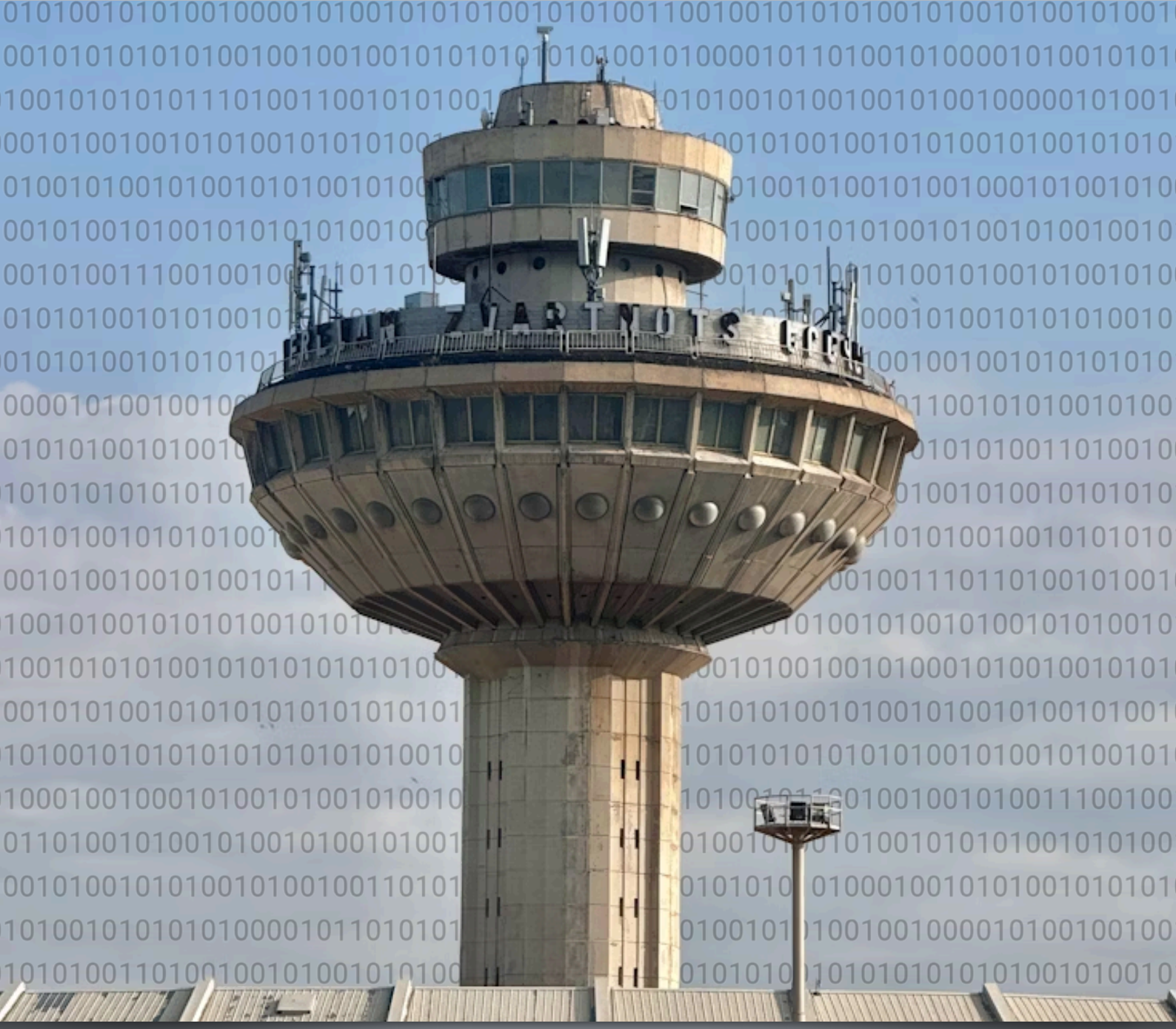


Լուսանկարը՝ Միկա Հովսեփյանի | Նկարազարդումը՝ ԲՏԻ-ի կողմից | Զվարթնոց միջազգային օդանավակայան, Երևան, Հայաստան

ՀԱՅԱՍՏԱՆ. ԹՎԱՅԻՆ ՍՊԱՌՆԱԼԻՔՆԵՐԻ ՀԱՄԱՊԱՏԿԵՐԸ 2024

Media Diversity Institute

CyberHUB

© mdi.am | cyberhub.am | 2025

Spyware Accountability Initiative

Բովանդակություն

3 Ներածություն

5 Ընդհանուր տեղեկություններ

5 Աշխարհաքաղաքական զարգացումները և կիբեռանվտանգության մարտահրավերները

7 Կիբեռանվտանգության տեղական նախաձեռնություններ

8 Մեդիագրագիտություն և պայքար ապատեղեկատվության դեմ

10 Սպառնալիքների զեկույց

10 Վարձու լրտեսող ծրագրեր

11 Ֆիշինգ

12 DDoS հարձակումներ

14 Կայքերի կոտրման դեպքեր

15 Դեպքերի ուսումնասիրություն

16 Հայկական ՀԿ-ների դեմ թիրախավորված հարձակման ժամանակ ներկայացել են իբրև ԵՄ պատվիրակություն

18 Թիրախավորված ֆիշինգը (անգլ.՝ spear phishing) Հայաստանում. UNC5792-ի շարունակական արշավի մանրամասները

19 Պատճենահենության (Pastejacking) հարձակումները Հայաստանում. կիբեռանվտանգության աճող սպառնալիք

23 Ֆիշինգի և վնասակար ծրագրի տարածում Razer-ի կեղծ հովանավորչական առաջարկի միջոցով

25 Թիրախավորված ֆիշինգային հարձակում հայկական ՀԿ-ի վրա

30 Ամփոփում

Հայաստանի թվային անվտանգության միջավայրը 2024 թվականին բախվել է զգալի մարտահրավերների, որոնք հիմնականում պայմանավորված էին աշխարհաքաղաքական լարվածությամբ և գերզարգացած կիբեռսպառնալիքներով: Դեպի Եվրամիություն և Միացյալ Նահանգներ երկրի ռազմավարական շրջադարձը և Ռուսաստանից կախվածության նվազումը, ըստ երևույթին, ուժեղացրել են առկա կիբեռանվտանգային ռիսկերը:

Սպառնալիքի շրջանակն ընդգրկում է թիրախավորված հարձակումներ բազմաթիվ ոլորտների՝ պետական կառույցների, լրատվամիջոցների և քաղաքացիական հասարակության խմբերի վրա: Հատկապես մտահոգիչ է դարձել պետական հովանավորությամբ գործող կիբեռլրտեսությունը. Հայաստան-Ադրբեջան հակամարտության ընթացքում արձանագրվել են լրտեսող նորագույն ծրագրերի կիրառման դեպքեր: Հայաստանի թվային ենթակառուցվածքների վրա այս շարունակական հարձակումներն անվտանգության վերաբերյալ լուրջ մտահոգություններ են առաջացրել:

Խոշոր տեխնոլոգիական ընկերությունները և կիբեռանվտանգության հարցերով մասնագիտացված կազմակերպությունները փաստագրել են այս սպառնալիքները՝ ընդգծելով զգայուն տեղեկությունների ու կարևորագույն համակարգերի պաշտպանության համար անհրաժեշտ անվտանգության ուժեղացված միջոցների ներդրման հրատապությունը:

Սույն զեկույցում ներկայացված են թարմացված տվյալներ Հայաստանի առջև ծառացած հիմնական կիբեռսպառնալիքների՝ վարձու լրտեսող ծրագրերի (mercenary spyware), ֆիշինգի, DDoS հարձակումների, կայքերը կոտրելու դեպքերի, հեռակառավարվող տրոյական ծրագրերի (Remote Access Trojans, RAT) և ինսայդերական վտանգների վերաբերյալ: Զեկույցում ներառված են կիբեռհանցագործությունների, այդ թվում պետական հովանավորությամբ կատարված հարձակումների նշանակալի դեպքերը, միտումները, ինչպես նաև Հայաստանի իշխանությունների և կիբեռանվտանգության մասնագիտացված կազմակերպությունների արձագանքը: Զեկույցի նպատակն է կիբեռանվտանգության ոլորտի մասնագետներին, քաղաքականություն մշակողներին և լրագրողներին ներկայացնել տվյալների վրա հիմնված վերլուծություն՝ Հայաստանի կիբեռդիմակայունության և 2024 թվականին ի հայտ եկած ռիսկերի վերաբերյալ:

«Հայաստանի թվային սպառնալիքների համապատկերը 2024» վերլուծությունը նախորդ տարեկան զեկույցի հերթական լրամշակված տարբերակն է, որում մանրամասնորեն ներկայացված է կիբեռանվտանգության վիճակը Հայաստանի Հանրապետությունում:

Բովանդակություն

5 **Ընդհանուր տեղեկություններ**

5 Աշխարհաքաղաքական զարգացումները և կիբեռանվտանգության մարտահրավերները

7 Կիբեռանվտանգության տեղական նախաձեռնություններ

8 Մեդիագրագիտություն և պայքար ապատեղեկատվության դեմ

Աշխարհաքաղաքական զարգացումները և կիբեռանվտանգության մարտահրավերները

Հայաստանի կիբեռանվտանգության լանդշաֆտը չի կարող տարանջատվել նրա աշխարհաքաղաքական համատեքստից. Հայաստանի և Ադրբեջանի միջև տասնամյակներ ձգվող հակամարտությունը հաճախ իր արտացոլումն է գտել նաև կիբեռտարածությունում: Լեռնային Ղարաբաղի և Հայաստանի դեմ Ադրբեջանի 2020 և 2023 թվականների ռազմական գործողություններին նախորդել են Հայաստանի պետական կառույցների վրա ծանր կիբեռհարձակումները, ներառյալ վնասարար ծրագրերի կիրառմամբ ֆիշինգը:

Այս իրադարձությունները ցույց են տալիս, թե հաճախ ինչպես են համակարգված կիբեռհարձակումները նախորդում ռազմական գործողություններին կամ իրականացվում դրանց զուգահեռ: Հայկական թիրախները եղել են նաև տարածաշրջանային և համաշխարհային կիբեռտերությունների ուշադրության կենտրոնում:

Հատկանշական է, որ հակամարտության ինտենսիվ փուլերում հայ պաշտոնյաների և ակտիվիստների դեմ գործադրվել է **NSO Group-ի Pegasus լրտեսող ծրագիրը**, ինչը միջազգային հակամարտությունում Pegasus-ի կիրառման առաջին հաստատված դեպքն էր: Պոտենցիալ թիրախները Apple-ից ծանուցումներ են ստացել նաև 2024 թվականին, ինչը սովորաբար ակնհայտ նշան է, որ լրտեսող ծրագրերի կիրառմամբ հարձակումները շարունակվում են: Ռազմական ոլորտում գործընկերների հետ համագործակցությունը հզորացրել է Ադրբեջանի կիբեռկարողությունները: Դրան նպաստել են նաև տրամադրված իսրայելական տեխնոլոգիաները, որոնք համալրել են Ադրբեջանի կիբեռզինանոցը:

Միևնույն ժամանակ, արտաքուստ դաշնակից պետությունները լրտեսություն են իրականացրել Հայաստանում. Ռուսաստանի պետական կառույցների հովանավորությամբ գործող տարբեր խմբեր (այդ թվում՝ Գլխավոր հետախուզական վարչության (ռուս.՝ ГРУ) հետ ասոցացվող **APT28 (Fancy Bear)** խումբը և Անվտանգության դաշնային ծառայության (ռուս.՝ ФСБ) հետ ասոցացվող **Turla-ն**) ակտիվություն են դրսևորել՝

թիրախավորված ֆիշինգի (անգլ.՝ spear phishing) և այլ մարտավարությունների կիրառմամբ նշանառելով հայկական պետական կառույցները:

2024 թվականի հունվարին Anonymous Russia հաքերային խումբը «Բաշխված ծառայությունների ժխտում» (անգլ.՝ Distributed Denial-of-Service, DDoS) տեսակի հարձակումներ է իրականացրել Հայաստանի պետական կայքերի, բանկերի և հեռահաղորդակցության ընկերությունների վրա, ենթադրաբար՝ ի պատասխան արևմտյան երկրների հետ Հայաստանի աճող կապերի:

Այնուհետև, 2024 թվականի մարտին, Ռուսաստանի հետ կապեր ունեցող Anonymous Sudan խումբը ստանձնեց հայկական խոշոր բջջային օպերատոր Team Telecom-ի վրա կիբեռհարձակման պատասխանատվությունը:

Այս միջադեպերն ընդգծում են, որ հայկական թվային ենթակառուցվածքների թիրախավորման գործում գնալով աճում է Ռուսաստանի հետ կապեր ունեցող հաքերային խմբերի ներգրավվածությունը:

Բացի այդ, 2024 թվականի հունիսին Հայաստանի կառավարական կայքերի վրա DDoS հարձակում ձեռնարկեց Ռուսաստանի ժողովրդական կիբեռբանակը (անգլ.՝ People's Cyber Army of Russia): Դա համընկավ Երևանի և Մոսկվայի միջև դիվանագիտական լարվածության ժամանակաշրջանի հետ:

Զուգահեռաբար, Հայաստանը հետամուտ է եղել Եվրամիության և Միացյալ Նահանգների հետ հարաբերությունների առաջխաղացմանը: 2025 թվականի հունվարին ստորագրվեց Հայաստանի Հանրապետության և Ամերիկայի Միացյալ Նահանգների միջև ռազմավարական գործընկերության մասին կանոնադրությունը, որի նպատակն է զարգացնել երկկողմ հարաբերությունները տարբեր ոլորտներում, ներառյալ պաշտպանությունը և կիբեռանվտանգությունը: Այս գործընկերությունը հեշտացնում է Հայաստանի հասանելիությունն ԱՄՆ տեխնոլոգիական փորձին, մասնավորապես՝ միջուկային ոլորտի արդիականացման և արհեստական բանականության կարողությունների զարգացման գործում:

Հայաստանի ներսում շարունակական քաղաքական անկայունությունը, որն էլ ավելի է սրվել 2020 թվականի Լեռնային Ղարաբաղի պատերազմով և դրան հաջորդած սահմանային լարվածությամբ, պարարտ հող է ստեղծել լրատվամիջոցներին և ընդդիմադիր գործիչներին թիրախավորող կիբեռհարձակումների համար: Այս միտումն ի ցույց է դնում այն փաստը, որ տարբեր դերակատարներ ավելի են ուժեղացրել տեղեկատվական լանդշաֆտը մանիպուլացնելու և վերահսկելու փորձերը, ինչը հիբրիդային պատերազմում գնալով ավելի տարածված մարտավարություն է դառնում: Վերջերս կատարված վերլուծություններն ընդգծում են հանրային դիսկուրսի վրա ազդելու և հանրային ինստիտուտները քայքայելու նպատակով ապատեղեկատվության և թիրախավորված կիբեռարշավների կիրառման աճը:

Կիբեռանվտանգության տեղական նախաձեռնություններ

Այս զարգացումների ֆոնին Հայաստանն ակտիվ աշխատանք է տարել՝ բարելավելու իր կիբեռանվտանգության կարողությունները՝ իբրև ավելի լայն թվային փոխակերպման գործընթացի մաս: Կառավարությունն ընդունել է Թվայնացման ռազմավարություն, որում շեշտը դրվում է նորարարական տեխնոլոգիաների, էլեկտրոնային կառավարման և կիբեռանվտանգության ինտեգրման վրա: Ստեղծվել են համակարգչային արտակարգ իրավիճակների արձագանքման բազմաթիվ թիմեր (անգլ.՝ Computer Emergency Response Team, CERT), ինչպես նաև շարունակվում է կիբեռանվտանգության մասին օրենսդրության մշակումը:

2024 թվականի մարտին Հայաստանը հայտարարեց տեղեկատվության պաշտպանությունն ամրապնդելու և անվտանգ ծրագրային լուծումներ մշակելու նպատակով Տեղեկատվական անվտանգության և գաղտնագրության ազգային կենտրոն ստեղծելու մասին:

Սրանից զատ, կիբեռդիմակայունության բարձրացման նպատակով 2024 թվականի դեկտեմբերին Հայաստանը Հեռահաղորդակցության միջազգային միության (International Telecommunication Union, ITU) հետ համատեղ անցկացրեց ազգային կիբեռանվտանգության իր առաջին վարժանքը: Միջոցառմանը մասնակցեցին կարևորագույն ենթակառուցվածքների ավելի քան 150 ներկայացուցիչներ՝

կենտրոնանալով կիբեռսպառնալիքներից պաշտպանվելու միջոցների հզորացման վրա:

Սրան զուգահեռ, կիբեռհանցագործությունների աճող դեպքերի դեմ պայքարելու նպատակով նախաձեռնվել են օրենսդրական աշխատանքներ: Առաջարկվող օրենքներից մեկը նպատակ ունի պաշտպանելու թվային ենթակառուցվածքները, ներառյալ էլեկտրոնային առևտրի հարթակները և կապի ծառայությունները՝ դրանք զինելով կիբեռսպառնալիքների դեմ պայքարի համապարփակ իրավական մեխանիզմներով: Այս նախաձեռնությունն ուղիղ արձագանք է կիբեռհանցագործությունների զգալի աճին, որը կրկնապատկվել է 2021-2023 թվականների ընթացքում:

Կարողություններին և համակարգմանն առնչվող մարտահրավերները, սակայն, պահպանվում են: 2023 թվականի վերջին Հայաստանի Հաշվեքննիչ պալատը հայտարարեց, որ ծրագրված Կիբեռանվտանգության ազգային կենտրոնը դեռևս չի հիմնադրվել, և որ պետական կառույցներում կիբեռպաշտպանության մակարդակը դեռ թույլ է՝ առանց կանոնավոր վարժանքների կամ ռեալ ժամանակում իրականացվող մոնիտորինգի: Ըստ Հաշվեքննիչ պալատի նախագահի՝ Հայաստանը կիբեռանվտանգության համաշխարհային ինդեքսներով 193 երկրների մեջ զբաղեցնում է միայն 93-րդ տեղը, ինչը փաստում է, որ երկիրը բարելավման զգալի տեղ ունի: Հայաստանի 2024 թվականի թվային անվտանգության համապատկերը կարելի է բնորոշել որպես սպառնալիքների ենթակայության բարձր մակարդակի և դեռևս հասունացման փուլում գտնվող պաշտպանական միջոցների խառնուրդ:

Մեդիագրագիտություն և պայքար ապատեղեկատվության դեմ

Ընդունելով տեղեկատվական պատերազմների դերը ազգային անվտանգության խաթարման գործում՝ Հայաստանը ներդրել է ապատեղեկատվության դեմ պայքարի ռազմավարություններ: 2023 թվականի դեկտեմբերին կառավարությունը ներկայացրել է Ապատեղեկատվության դեմ պայքարի 2024-2026 թվականների հայեցակարգը և գործողությունների պլանը՝ նպատակ ունենալով հզորացնելու կարողությունները ինչպես պետական, այնպես էլ մասնավոր

հատվածներում և բարձրացնելու քաղաքացիների մեդիագրագիտությունը: Այս միջոցները միտված են բնակչությանը զինելու անհրաժեշտ գիտելիքներով՝ քննադատաբար գնահատելու տեղեկատվության աղբյուրները՝ դրանով իսկ մեղմելով կեղծ լուրերի և արտաքին քարոզչության ազդեցությունը:

Հաջորդիվ

10 Սպառնալիքների զեկույց

10 Վարձու լրտեսող ծրագրեր

11 Ֆիշինգ

12 DDoS հարձակումներ

14 Կայքերի կոտրման դեպքեր

Վարձու լրտեսող ծրագրեր

Վարձու լրտեսող ծրագրերի կամ կոմերցիոն լրտեսող ծրագրերի կիրառումը Հայաստանում լուրջ մտահոգություններ է առաջացրել հատկապես ազգային անվտանգության և անձնական տվյալների գաղտնիության համատեքստում:

Վարձու լրտեսող ծրագրերը մասնավոր ընկերությունների կողմից մշակված ծրագրեր են, որոնք (հաճախ ծածուկ) վաճառվում են կառավարություններին կամ այլ կառույցներին, որպեսզի վերջիններս վերահսկեն օգտատերերին և արտագրեն թիրախավորված անձանց սարքերի տվյալները: Այս կարգի լրտեսող ծրագրերը հայտնի են իրենց խիստ զարգացած հնարավորություններով. դրանք կարող են ձայնագրել ստեղնաշարով հավաքած ցանկացած տեքստ, էկրանապատկերներ անել, հետևել անձի գտնվելու վայրին և նույնիսկ ակտիվացնել միկրոֆոնները և տեսախցիկները՝ առանց օգտատիրոջ իմացության:

Ըստ տարբեր տեղեկությունների՝ Հայաստանում վարձու լրտեսող ծրագրերն օգտագործվել են հետախուզական տվյալների հավաքագրման և հետաքրքրություն ներկայացնող պրոցեսները վերահսկելու համար: Այդպիսի լրտեսող ծրագրերի ներդրումը նման է երկսայրի սրի. թեև այն իշխանություններին տրամադրում է կիբեռսպառնալիքներին և հանցավոր գործողություններին դիմակայելու առաջադեմ գործիքներ, սակայն միևնույն ժամանակ առաջ է բերում էթիկական և իրավական հարցեր՝ կապված վերահսկման և գաղտնիության իրավունքի հետ: Լրտեսող ծրագրերի՝ ոչ ըստ իրենց բուն նպատակի կիրառման դեպքերը, երբ դրանք օգտագործվելեն քաղաքական հակառակորդներին, լրագրողներին կամ ակտիվիստներին թիրախավորելու համար, հանրային դժգոհություններ ենառաջացրել, և ավելի մեծ թափանցիկության և վերահսկողության պահանջներ են դրվել:

Հայաստանում վարձու լրտեսող ծրագրերի թվի աճն առաջին պլան է բերում կարգավորող ազդու համակարգերի և կիբեռանվտանգության միջոցառումների հրատապ անհրաժեշտությունը: Կառավարությունը պետք է հավասարակշռի այս հզոր գործիքների առավելությունները դրանց չարաշահման հնարավորության նկատմամբ՝ երաշխավորելով կոմերցիոն լրտեսող ծրագրերի օգտագործումն օրենքի շրջանակներում և հարգանքը մարդու իրավունքների նկատմամբ:

Բացի այդ, հանրային իրազեկման և մեդիագրագիտության արշավներն էական նշանակություն ունեն քաղաքացիներին լրտեսող ծրագրերի հետ կապված ռիսկերի մասին իրազեկելու և անձնական տվյալների պաշտպանության նկատմամբ զգոնությունը խթանելու հարցում: Հայաստանի ընթացիկ թվային վերափոխմանը զուգընթաց՝ վարձու լրտեսող ծրագրերի առաջ բերած մարտահրավերներին դիմակայելը կարևոր նշանակություն կունենա ինչպես ազգային անվտանգության, այնպես էլ անձնական ազատությունների պաշտպանության համար:

Ֆիշինգ

Վերջին տարիներին Հայաստանում ֆիշինգային հարձակումների անհանգստացնող աճ է արձանագրվել, ինչը մեծ սպառնալիք է դարձել ինչպես անհատների, այնպես էլ կազմակերպությունների համար: Ֆիշինգը կիբեռհանցագործության այն տեսակն է, երբ հարձակում գործողները քողարկվում են իբրև վստահելի կազմակերպություններ՝ զոհերին մոլորեցնելով այնպես, որ վերջիններս իրենց տրամադրեն անձնական զգայուն տեղեկություններ: Այն շարունակում է կատարելագործվել հնարամտության և ազդեցիկության առումով: Էլեկտրոնային փոստի, սոցիալական մեդիայի հաղորդագրությունների կամ կեղծ կայքերի միջոցով տեղի ունեցող այս հարձակումների նպատակն է զոհերին մոլորեցնելով ստիպել բացահայտել իրենց գաղտնաբառերը, ֆինանսական տվյալները կամ անձնական տեղեկությունները: Ֆիշինգի աճը հատկապես մտահոգիչ է՝ հաշվի առնելով Հայաստանում շարունակվող թվային փոխակերպումը և կապի, առևտրի և կառավարման առցանց ծառայություններից աճող կախվածությունը:

Հայաստանում ֆիշինգային հարձակումների հետևանքները բազմազան են և իրենց ազդեցությունն են թողնում բազմաթիվ ոլորտների և բնակչության տարբեր շերտերի վրա: Ձեռնարկությունների դեպքում ֆիշինգային հմուտ հարձակումը կարող է հանգեցնել ֆինանսական կորուստների, գաղտնի տեղեկությունների արտահոսքի և հեղինակության անկման: Պետական կառույցները նույնպես խոցելի են, իսկ հնարավոր խաթարումները սպառնում են ազգային անվտանգությանը և հանրային վստահությանը: Անհատական մակարդակում զոհերը կարող են բախվել անձնական տվյալների հափշտակման, բանկային հաշիվների դատարկմանև հոգեբանական սթրեսի: Չնայած կիբեռանվտանգության հզորացմանն ուղղված ջանքերին, որոնց թվում են օրենսդրական միջոցառումները և

տեխնոլոգիական առաջընթացը, ֆիշինգի շարունակական դեպքերն ընդգծում են մշտական զգոնության և թվային ուսուցման անհրաժեշտությունը: Քաղաքացիները և կազմակերպությունները պետք է զինված լինեն գիտելիքներով, որպեսզի տարբերեն նման սպառնալիքները և արդյունավետ կերպով արձագանքեն դրանց:

Ֆիշինգային հարձակումների ազդեցությունը մեղմելու նպատակով Հայաստանը ձեռնամուխ է եղել մի քանի նախաձեռնությունների, որոնք ուղղված են կիբեռդիմակայունության ամրապնդմանը: Հանրային իրազեկման արշավներն առանցքային նշանակություն ունեն քաղաքացիներին ֆիշերների մարտավարությանը ծանոթացնելու և առցանց տիրույթում անվտանգ գործելու համար: Բացի այդ, ձեռնարկությունների և պետական աշխատողների համար կիբեռանվտանգության ուսուցման ծրագրերը նպաստում են պրոակտիվ պաշտպանության ստեղծմանը՝ ընդդեմ ֆիշինգի փորձերի: Անվտանգության վստահելի կանոնակարգերի ներդրումը, ինչպիսիք են բազմաստիճան վավերացումը և համակարգի կանոնավոր թարմացումները, ավելի են ուժեղացնում պաշտպանությունայս խաբեբայական հարձակումներից: Հաշվի առնելով սեփական կիբեռանվտանգության միջավայրն ամրապնդելու Հայաստանի ձգտումը՝ տեխնոլոգիական, կրթական և օրենսդրական ռազմավարություններ ներառող համաձայնեցված գործողություններն առանցքային դեր ունեն սեփական թվային տիրույթը ֆիշինգի անողոք սպառնալիքից պաշտպանելու հարցում:

DDoS հարձակումներ

«Բաշխված ծառայությունների ժխտում» (անգլ.՝ Distributed Denial-of-Service, DDoS) տեսակի հարձակումները կիբեռանվտանգության լուրջ սպառնալիք են դարձել Հայաստանում՝ ազդելով տարբեր ոլորտների և հաստատությունների վրա: Այս հարձակումների իմաստն այն է, որ ինտերնետ տրաֆիկով հեղեղում են թիրախի առցանց ծառայությունները՝ դրանք անհասանելի դարձնելով իրական օգտատերերի համար: DDoS հարձակումների հեղինակները հաճախ օգտագործում են վարակված համակարգիչների ցանցեր (հայտնի իբրև բոտնետ)՝ գեներացնելու համար այն հսկայածավալ տրաֆիկը, որն անհրաժեշտ է ծառայությունը խաթարելու համար: Հայաստանյան բազմաթիվ ընկերություններ, պետական կառույցներ և նույնիսկ կարևորագույն ենթակառուցվածքներ

այս քայքայիչ հարձակումների զոհ են դարձել, ինչը վերստին փաստում է կիբեռանվտանգության ուժեղացված միջոցառումների հրատապ անհրաժեշտությունը:

DDoS հարձակումների հետևանքները Հայաստանում բազմաշերտ են. դրանք ազդում են ինչպես պետական, այնպես էլ մասնավոր հատվածի վրա: Ձեռնարկությունների դեպքում՝ հաջող DDoS հարձակումը կարող է հանգեցնել զգալի ֆինանսական կորուստների՝ պայմանավորված ծառայության ժամանակավոր անհասանելիությամբ, արտադրողականության նվազմամբ և հեղինակության հնարավոր անկմամբ: Խաթարվել կարող են նաև պետական հաստատությունների կայքերը՝ խոչընդոտելով հանրության հասանելիությանը առանցքային ծառայություններին և հանգեցնելով թվային կառավարման նկատմամբ վստահության կորստի: Ավելին, ազդեցությունը այնպիսի կարևորագույն ենթակառուցվածքների վրա, ինչպիսիք են էներգետիկան և առողջապահական համակարգերը, կարող է լրջագույն հետևանքներ ունենալ ազգային և հանրային անվտանգության համար: DDoS հարձակումների հաճախականության աճը և դրանց առավել կատարելագործված լինելն ի ցույց են դնում Հայաստանի թվային լանդշաֆտը պաշտպանելու համար վստահելի և համակարգված արձագանքի անհրաժեշտությունը:

Երկրի կիբեռպաշտպանության հզորացման և DDoS հարձակումների հետևանքները մեղմելու նպատակով Հայաստանում տարբեր նախաձեռնություններ են մեկնարկել: Ներդրումները կիբեռանվտանգության այնպիսի առաջադեմ տեխնոլոգիաներում, ինչպիսիք են ներխուժումների հայտնաբերման համակարգերը և հակա-DDoS լուծումները, կարևոր նշանակություն ունեն այս սպառնալիքները վերհանելու և չեզոքացնելու համար: Միջազգային գործընկերների և կիբեռանվտանգությամբ զբաղվող կազմակերպությունների հետ համագործակցությունը կարող է DDoS հարձակումներին դիմակայելու Հայաստանի կարողությունները հզորացնելու արժեքավոր գիտելիքներ և ռեսուրսներ տրամադրել: Սրան գումարած՝ դիմակայուն թվային էկոհամակարգ կառուցելու համար կարևոր է նաև քաղաքացիների և կազմակերպությունների շրջանում կիբեռանվտանգության իրազեկման մշակույթի խթանումը: Հայաստանի թվային փոխակերպման շարունակվող գործընթացի համատեքստում DDoS հարձակումների հետևանքով առաջացած մարտահրավերներին դիմակայելը վճռորոշ նշանակություն կունենա երկրի առցանց ծառայությունների կայունությունն ու անվտանգությունն ապահովելու համար:

Կայքերի կոտրման դեպքեր

Կայքերի կոտրման և բովանդակության աղավաղման (անգլ.՝ defacement) դեպքերը Հայաստանում կիբեռանվտանգության լուրջև շարունակական վտանգ են ներկայացնում՝ ազդելով տարբեր կառույցների, այդ թվում՝ քաղաքացիական հասարակության կազմակերպությունների (ՔՀԿ) և լրատվամիջոցների վրա: Այս հարձակումները հաճախ իրականացվում են այնպիսի վեբ հավելվածների խոցելիությունների կիրառմամբ, ինչպիսիք են WordPress-ի՝ այդօրինակ բովանդակության կառավարման համակարգերում հնացած խրվակները (plugin): Այս միջամտությունների հետևանքը, հաջողությամբ պսակվելու դեպքում, կարող է լինել այն, որ հարձակում գործողները ձեռք կբերեն կառավարման հասանելիություն, վեբկայքի այցելուներին կվերաուղղորդեն դեպի վնասակար կայքեր կամ կաղավաղեն կայքի բովանդակությունը քարոզչական կամ խնդրահարույց գրություններով:

Կայքերը կոտրելու դեպքերի ազդեցությունը հաճախ դուրս է գալիս զուտ դրանց խափանման բուն սահմաններից՝ պատճառելով նաև հնարավոր ֆինանսական կորուստներ, վնասելով հեղինակությանը և հանգեցնելով հանրային վստահության կորստի: Հայտնի միջադեպերի շարքում են հնացած ծրագրային ապահովմամբ աշխատող հոսթինգ պրովայդերներին կոտրելու դեպքերը (որոնք հանգեցրել են վեբկայքերի համատարած կոտրումների), ինչպես նաև օտարերկրյա (մասնավորապես Ադրբեջանից և Թուրքիայից) հաքերային խմբերի կողմից կանոնավոր թիրախավորումները: Շարունակվող այս սպառնալիքների ֆոնին ակնհայտ է դառնում անվտանգության մշտական միջոցառումների խիստ անհրաժեշտությունը:

Հայաստանի թվային համակարգերն այս տարածված կիբեռհարձակումներից պաշտպանելուն ուղղված գործողությունների թվում են ծրագրային ապահովման կանոնավոր թարմացումները, խոցելիությունների արդյունավետ կառավարումը և առցանց տիրույթում անվտանգ աշխատելու վերաբերյալ աշխատակիցների վերապատրաստումները:

Ստորև ներկայացված պրակտիկ օրինակները լույս են սփռում հայաստանյան ՔՀԿ-ների, մասնավորապես մարդու իրավունքներով զբաղվող կազմակերպությունների դեմ լավ մշակված արշավների վրա: Մենք արձանագրել ենք ռուսական շարունակական թիրախային հարձակումների (անգլ.՝ Advanced Persistent Threat, APT) ակտիվության աճ, որոնց ժամանակ կիրառվել են քաղաքացիական հասարակության կազմակերպությունների վրա հարձակվելու և դրանց թվային անվտանգությունը խաթարելու նոր մարտավարություններ: Ուսումնասիրելով այդ դեպքերը՝ կազմակերպությունները և կիբեռանվտանգության թիմերը կարող են ճանաչել զարգացող մեթոդները, բարելավել իրենց պաշտպանական մեխանիզմները և խթանել գլոբալ համագործակցությունը՝ կիբեռհանցագործությունների դեմ արդյունավետ պայքարելու նպատակով:

Այս բաժնում

15 **Դեպքերի ուսումնասիրություն**

16 Հայկական ՀԿ-ների դեմ թիրախավորված հարձակման ժամանակ ներկայացել են իբրև ԵՄ պատվիրակություն

18 Թիրախավորված ֆիշինգը (անգլ.՝ spear phishing) Հայաստանում. UNC5792-ի շարունակական արշավի մանրամասները

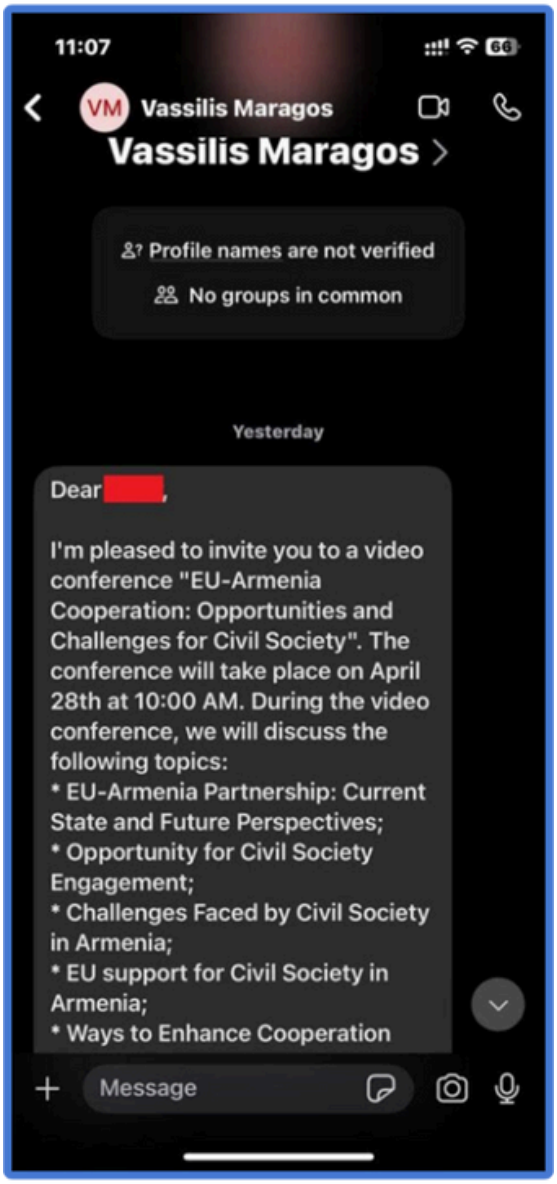
19 Պատճենահենության (Pastejacking) հարձակումները Հայաստանում. կիբեռանվտանգության աճող սպառնալիք

23 Ֆիշինգի և վնասակար ծրագրի տարածում Razer-ի կեղծ հովանավորչական առաջարկի միջոցով

25 Թիրախավորված ֆիշինգային հարձակում հայկական ՀԿ-ի վրա

Հայկական ՀԿ-ների դեմ թիրախավորված հարձակման ժամանակ ներկայացել են իբրև ԵՄ պատվիրակություն

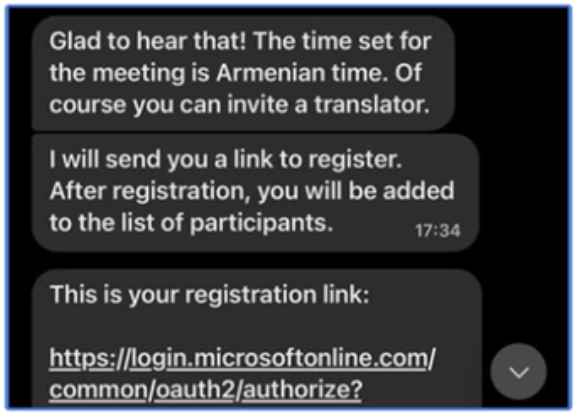
2025 թվականի ապրիլի 8-ին հայտնաբերվել է լավ մշակված թիրախային ֆիշինգի (անգլ.՝ spear phishing) արշավ, որի նշանակետում հայաստանյան տասնյակ ՀԿ-ներ են եղել: Հարձակման հեղինակները հաղորդագրությունն ուղարկել են Հայաստանում ԵՄ պատվիրակության ղեկավար, դեսպան Վասիլիս Մարագոսի անունից՝ Signal մեսենջերի միջոցով: Ֆիշինգային հաղորդագրությունը՝ քողարկված իբրև «ԵՄ-Հայաստան համագործակցություն. հնարավորություններ և մարտահրավերներ քաղաքացիական հասարակության համար» խորագրով տեսակոնֆերանսի հրավեր, նպատակ ուներ մոլորեցնելու հասցեատերերին այնպես, որ վերջիններս հավատային, թե հրավիրված են իրական միջոցառման: Հաղորդագրության մեջ նշվում էր, որ տեսակոնֆերանսը տեղի կունենա ապրիլի 28-ին, ժամը 10:00-ին, Microsoft Teams Video հարթակում: Հավանական զոհերին առաջարկվել է տալ մասնակցության համաձայնություն, որից հետո իբր կիրականացվեր նրանց գրանցումը:



Ֆիշինգի այս գործողության հիմքում վնասակար մի URL էր՝ քողարկված իբրև Microsoft Teams-ի հանդիպման հղում: Հաղորդագրությունը պարունակում էր հղում **Microsoft-ի թվացյալ վստահելի էջին**: Այն պահին, երբ թիրախավորված անհատը հաջողությամբ մուտք գործեր, գործողությունը կշարունակվեր զննարկիչի առանձին պատուհանում, որը պարունակում է **Microsoft-ի վավերացման նշան**: Չարագործների համար վճռորոշ քայլն այնուհետև թիրախավորված անձին ուղղորդելն էր, որ

վերջինս **պատճենի և տեղադրի այդ նոր հղումը (որը պարունակում է վավերացման նշան) և այն Signal-ի միջոցով հետ ուղարկի հարձակման հեղինակներին**: Այդ գործողությամբ կտրվեր **զոհի հաշվին Microsoft Entra ID սարքի միացման գործընթացի** մեկնարկը:

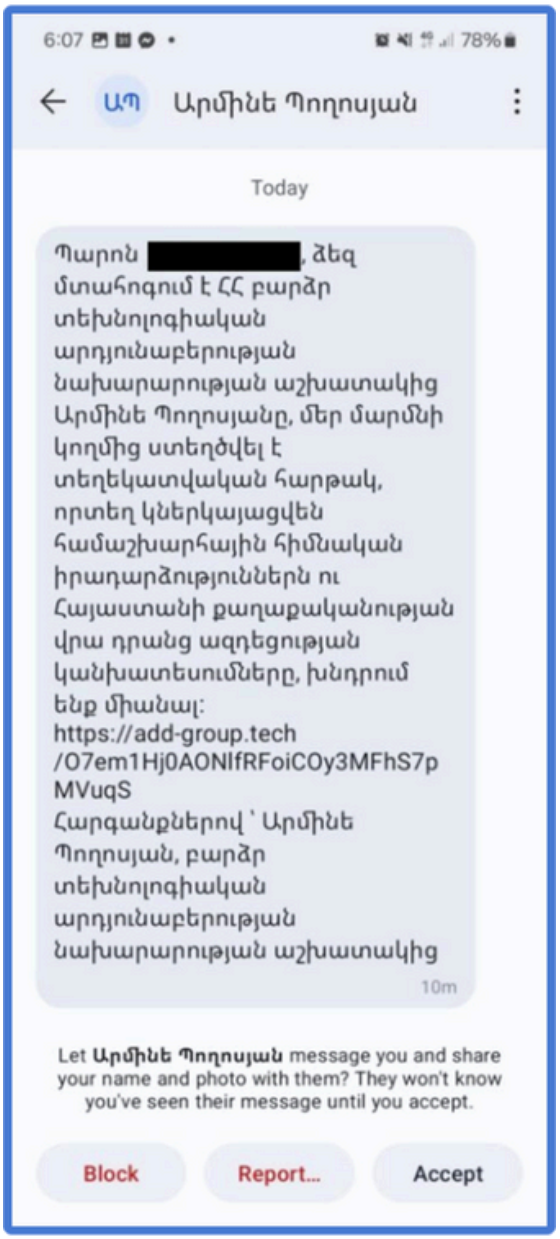
Հարձակում գործողներին հաջողվել էր տիրանալ առնվազն մեկ հաշվի, որը պատկանում էր մի հայտնի հասարակական կազմակերպության ղեկավարի: CyberHUB-AM թիմը, ՔՀԿ-ի SS մենեջերի հետ համագործակցելով, արձագանքել էր միջադեպին: Այդ աշխատանքի ընթացքում նրանք նկատել էին, թե ինչպես են հարձակում գործողները հաջողությամբ ներթափանցում ՔՀԿ ղեկավարի Microsoft Entra ID և փորձում մուտք գործել այնտեղ **Microsoft Azure CLI-ի** միջոցով: Մուտքի փորձերը եղել էին 95.182.124.124, 46.8.213.90, 188.130.142.95 IP հասցեներից, որոնք բոլորն էլ, ինչպես պարզվեց, պատկանում էին ամպային սերվերի պրովայդեր **Biterika Group ՓԲԸ-ին, որը գտնվում է Ռուսաստանում**:



Այն բանից հետո, երբ միջադեպի արձագանքման թիմը խափանեց առաջին հարձակումը, չարագործները լուրջ համառություն ցուցաբերեցին: Նրանք վերսկսեցին կապը Signal-ի միջոցով՝ տրամադրելով մեկ այլ հղում և զոհին ուղղորդելով կրկնել բոլոր վերոբերյալ քայլերը: Հարձակման հեղինակներից մեկի հաղորդագրությունում նշվում էր. «Ես պարզեցի, Դուք ամեն ինչ ճիշտ եք արել, բայց ինչ-ինչ պատճառներով գրանցումը չի ստացվել: Դուք ստիպված կլինեք նորից նույն բանն անել, և SS մասնագետը կկարգավորի խնդիրը». սրանով փորձ էր արվում կրկին ներգրավել զոհին և վերականգնել մուտքը:

Veloxity-ի զեկույցների հետ կապը. Այս միջադեպը սերտորեն փոխկապակցված է շարունակական թիրախային հարձակումների (անգլ.՝ Advanced Persistent Threat, APT) գործողությունների ու մեթոդների հետ, որոնք մանրամասն նկարագրված են Veloxity-ի վերջին զեկույցներում, մասնավորապես «Ֆիշինգ հանուն կոդերի. ռուսական չարագործների թիրախում Microsoft 365 OAuth-ի աշխատանքային պրոցեսներն են» (ապրիլի 22, 2025թ.) և «Տարբեր ռուս չարագործների թիրախում Microsoft-ի սարքերի կոդի վավերացումն է» (փետրվարի 13, 2025թ.):

Թիրախավորված ֆիշինգը (անգլ.՝ spear phishing) Հայաստանում. UNC5792-ի շարունակական արշավի մանրամասները



2025 թվականի մարտի սկզբին CyberHUB-AM-ը բացահայտել է նպատակային թիրախավորված ֆիշինգի արշավ՝ ուղղված Հայաստանի քաղհասարակության, պետական կառույցների և անհատների դեմ: Արշավը պարունակում էր հարձակման ցուցիչներ (անգլ.՝ indicators of compromise, IOCs), որոնք համապատասխանում էին շարունակական թիրախային հարձակումների (անգլ.՝ Advanced Persistent Threat, APT) գործողություններին և վերագրվում էին **UNC5792** խմբին, որը նախկինում բացահայտել էր Mandiant-ը:

Հարձակում գործողները ներկայացել էին հորինված «Արմինե Պողոսյան» անվամբ, որն իբրև թե Հայաստանի բարձր տեխնոլոգիական արդյունաբերության նախարարության «աշխատակից» է, և օգտագործելով Signal-ը՝ հասցեատերերին հաղորդագրությամբ հրավիրել էին համաշխարհային և հայաստանյան քաղաքական իրադարձություններին նվիրված մտացածին «տեղեկատվական հարթակ»: Հարձակման հիմքում չափազանց վնասակար, ժամանակավոր URL-ներ էին եղել (սկզբում add-group.tech-ում, այնուհետև տեղափոխվել էին group-add.com), որոնք նախատեսված են թիրախները կոտրելու համար: Ուշագրավ է, որ չարագործները դրսևորել էին իրական ժամանակում հարմարվելու ունակություն. անմիջապես այն բանից հետո, երբ իմացել էին, որ սկզբնական URL-ի ժամկետը լրացել է, վնասակար նոր ակտիվ հղում էին

տրամադրել մեկ այլ դոմեյնում:

Ֆիշինգի այս փորձն իրականացվել էր **Signal** մեսենջերի միջոցով, ինչը էլ-փոստի վրա հիմնված ավանդական վեկտորներից շեղում է և արտացոլում է անցումը դեպի անվտանգ, գաղտնագրված հարթակներ սոցիալական ինժեներիայի գործողությունների համար:

Ֆիշինգի գործիքակազմում կիբեռանվտանգության մասնագետները վերհանել են երեք դոմեյններ՝ add-group.tech, group-add.com, signal-groups-add.com: VirusTotal-ը բոլոր երեք դոմեյնները գնահատել է որպես խիստ վնասակար: Այս կարծիքը հաստատել են Mandiant-ի և Google Threat Intelligence-ի հետախուզական տվյալները: Բոլոր 3 դոմեյնները Mandiant-ը վերագրել է UNC5792-ին:

Հատկանշական է, որ այս URL-ները ժամանակավոր բնույթ են կրել: CyberHUB-AM-ի՝ վերահսկվող միջավայրում հղումները վերլուծելու փորձերը ցույց են տվել, որ սկզբնական URL-ի գործողության ժամկետն արդեն սպառվել է, ինչը վկայում է, որ չարագործն օգտագործել է կարճատև հասանելիության համար նախատեսված գործիքակազմ՝ նվազեցնելով պաշտպանվող կողմի արձագանքման հնարավորությունները:

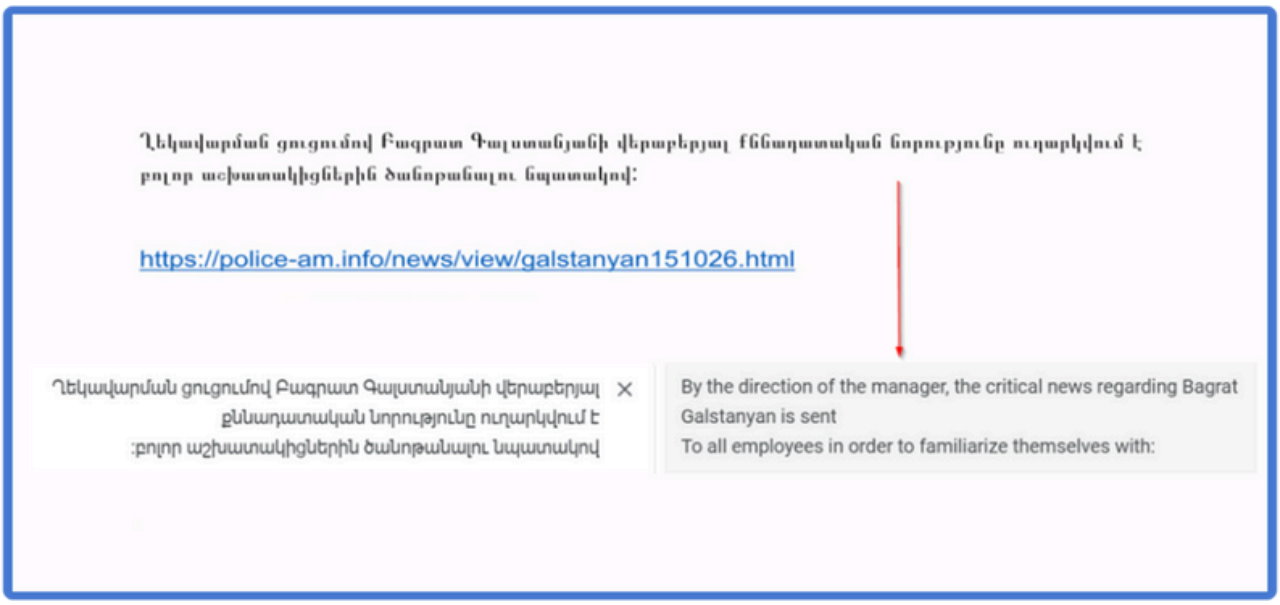
Միջադեպը ցույց է տվել նաև հարձակում գործողների՝ **իրական ժամանակում հարմարվելու ունակությունը**: Երբ թիրախավորված օգտատերը, դեպքով զբաղվող մասնագետների հսկողության ներքո, հարձակվող կողմին տեղեկացրել է, որ սկզբնական հղման ժամկետը սպառվել է, անմիջապես տրամադրվել է **նոր, գործող URL**: Այս վարքագիծը հաստատում է, որ հարձակում գործողներն ակտիվորեն հետևել են հաղորդակցությանը և ճկուն կերպով կառավարել ֆիշինգի գործիքակազմը:

Պատճենահենության (Pastejacking) հարձակումները Հայաստանում. կիբեռանվտանգության աճող սպառնալիք

30 հոկտեմբերի, 2024թ. | Անվտանգության մասնագետ Սայմոն Քենինը փաստագրել է կիբեռհարձակման նոր տեսակ (հայտնի իբրև Pastejacking՝ պատճենահենություն), որի թիրախում Հայաստանն է: Հարձակման ժամանակ օգտագործվել է նախորդ ամիսներին երկրում ընդդիմության

բողոքի ակցիաների համատեքստը և Հայ Առաքելական եկեղեցու սպասավոր Բագրատ արքեպիսկոպոս Գալստանյանի անունը:

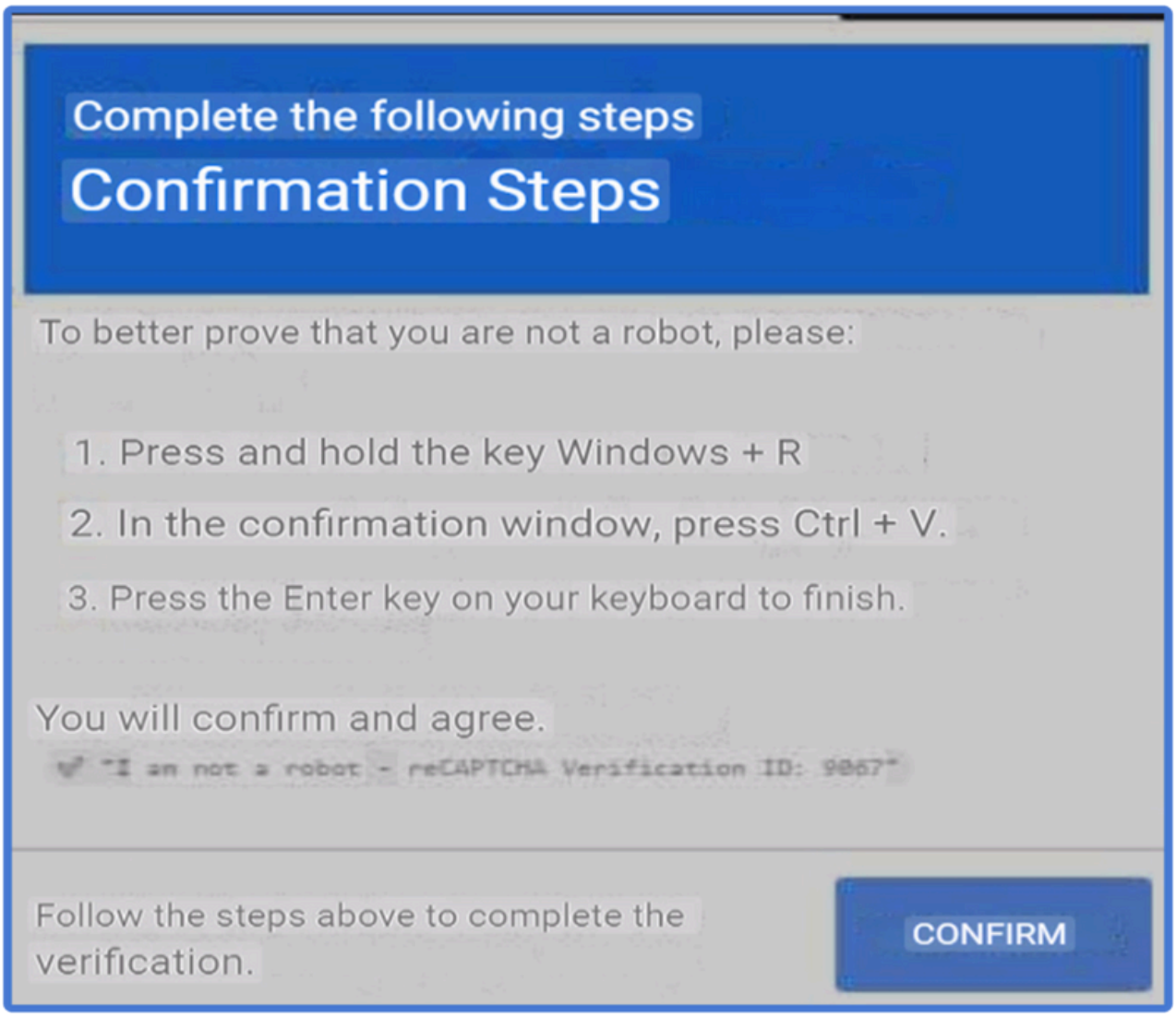
Հետազոտողը հայտնաբերել է MS Word ֆորմատի հայերեն փաստաթուղթ, որի ներքևի հատվածում հետևյալ հղումն է՝



Հայաստան. անվտանգության մասնագետ Սայմոն Քենինի բլոգային գրառման էկրանապատկերը, Երևան, *30*-ը հոկտեմբերի, *2024*թ.:

Հղումը տանում է դեպի դոմեյնային տիրույթ, որը նման է Հայաստանի ոստիկանության պաշտոնական դոմեյնային տիրույթին: Դոմեյնը գրանցվել է 2024 թվականի հոկտեմբերի 7-ին և ներկայում կասեցված է, ըստ երևույթին՝ որպես ֆիշինգային կայք մակնշվելու հետևանքով: VirusTotal-ում պահպանվել են որոշ մանրամասներ, այդ թվում՝ որոշակի տեքստ, որը քաղված է կայքից, երբ այն դեռ գործում էր, և հստակ ցույց է տալիս Հայաստանի ոստիկանությանը վերաբերող բանալի բառեր:

Սայմոնի բլոգային գրառման մեջ հավելյալ հետաքրքիր մանրամասներ էլ կան: Ըստ մասնագետի՝ հղումը բացելու դեպքում օգտատիրոջը ցուցադրվում է անվտանգության ստուգման հայերեն սեղմակ՝ captcha, որը սեղմելու դեպքում օգտատերը տեսնում է բուն պատճենահենային հարձակման պատուհանը:



Հայաստան. էկրանապատկեր անվտանգության մասնագետ Սայմոն Քենինի բլոգային գրառումից, Երևան, 30-ը հոկտեմբերի, 2024թ.:

Հարձակմանն առնչվող հավելյալ մանրամասների համար հետևեք այս հղմանը՝ https://k3yp0d.blogspot.com/2024/10/something-phishy-is-happening-in-armenia.html?lr=1730206198313:

Ստորև կներկայացնենք, թե ինչ է ենթադրում նմանօրինակ հարձակումը, և ինչպես պաշտպանվել դրանից:

Ի՞նչ է պատճենահենությունը

Պատճենահենությունը (անգլ.՝ Pastejacking) կիբեռհարձակման տեխնիկա է, որի ժամանակ հարձակում գործողները կիրառում են օգտատերերի սարքի օպերացիոն հիշողությունում պատճենված բովանդակությունը: Երբ

օգտատերը պատճենում է տեքստը վնասակար վեբկայքից, տվյալ բովանդակությունը փոխարինվում է այլ բանով, հաճախ՝ վնասակար: Սա կարող է ոչ կանխամտածված հետևանքներ ունենալ, երբ օգտատերը բովանդակությունը տեղադրում է այլ հարթակում, ասենք՝ տերմինալում կամ փաստաթղթում:

Օրինակ՝ օգտատերը կարող է որևէ կայքից պատճենել թվացյալ անվնաս URL կամ հրաման, սակայն այլ հարթակում տեղադրելուց հետո բովանդակությունը փոխվի վնասակար հրամանի կատարման կամ նրան վերաուղղորդի դեպի ֆիշինգային կայք: Սա կարող է հանգեցնել չարտոնված մուտքի, տվյալների արտահոսքի կամ վնասարար ծրագրերի տեղադրման:

Ինչպես է աշխատում պատճենահենությունը

1. **Պահնակի (clipboard) մանիպուլյացիա**. հարձակում գործողներն օգտագործում են JavaScript՝ փոփոխելու պահնակի բովանդակությունը, երբ օգտատերը պատճենում է տեքստը վեբ էջից: Այս սկրիպտը կարող է պատճենված տեքստը փոխարինել վնասակար հրամաններով կամ հղումներով:
2. **Վնասակար հրամանների կատարում**. երբ օգտատերը փոփոխված բովանդակությունը տեղադրում է տերմինալի կամ հրամանի տողում, կատարվում է վնասակար հրամանը, որը կարող է վտանգել համակարգի աշխատանքը:
3. **Ֆիշինգ և վերաուղղորդում**. պահնակի փոփոխված բովանդակությունը կարող է նաև օգտատերերին վերաուղղորդել դեպի ֆիշինգային կայքեր, որտեղ չարագործները կարող են հափշտակել զգայուն տեղեկություններ, օրինակ՝ մուտքային տվյալները:

Խորհուրդներ պատճենահենությունից պաշտպանվելու համար

- **Զգույշ եղեք որևէ բան պատճենելիս.** խուսափեք անվստահելի կայքերից տեքստ պատճենելուց: Եթե ձեզ անհրաժեշտ է պատճենել տեքստը, նախքան այն որևէ այլ հարթակում տեղադրելը ստուգեք դրա բովանդակությունը:
- **Վերստին ստուգեք տեղադրվող բովանդակությունը**. միշտ կրկնակի ստուգեք ձեր տեղադրած բովանդակությունը, հատկապես զգայուն միջավայրերում, ինչպիսիք են տերմինալները կամ հրամանների տողերը:

- **Կրթեք և վերապատրաստեք**. աշխատակիցների շրջանում բարձրացրեք պատճենահենության մասին իրազեկվածությունը և կազմակերպեք անվտանգ զննարկման թրեյնինգներ:

Այս պաշտպանիչ միջոցներն աչալրջորեն կիրառելով՝ դուք կարող եք զգալիորեն նվազեցնել պատճենահենության հարձակումների զոհ դառնալու ռիսկը:

Ֆիշինգ և վնասարար ծրագրի տարածում Razer-ի կեղծ հովանավորչական առաջարկի միջոցով

Ամսաթիվ՝ 18 դեկտեմբերի, 2024թ
Թիրախ՝ Նարեկ Կիրակոսյան, հայ լրագրող
Սպառնալիքի մակարդակ՝ բարձր (1-ին աստիճան)
Արձանագրող կազմակերպություն՝ CyberHUB-AM

Համառոտ նկարագիր
Հայ հայտնի լրագրող Նարեկ Կիրակոսյանը 2024 թվականի դեկտեմբերի 18-ին բարդ ֆիշինգային հարձակման է ենթարկվել: Չարագործները ներկայացել են իբրև խաղային սարքավորումներ արտադրող հեղինակավոր Razer Inc. ընկերություն, որպեսզի կեղծ հովանավորչական առաջարկի միջոցով չարամիտ ծրագիր տարածեն:

Հարձակման մանրամասները
- **Ֆիշինգային էլեկտրոնային նամակ**. հարձակում գործողները contact@razer-us.com էլեկտրոնային հասցեից ուղարկել են նամակ, որում մանրամասնորեն ներկայացված էր հովանավորչության առաջարկը՝ ինչպես նաև ենթադրյալ համագործակցության օրինակների հղումներ և մեդիայի համար նախատեսված նյութերի փաթեթ:
- **Վնասակար հղումներ**. Էլեկտրոնային նամակում առկա էր համառոտված URL (https://bit.ly/RazerPromoKit), որը տանում էր դեպի Dropbox-ում տեղակայված վնասակար արխիվ:
- **Չարամիտ ծրագիր**. արխիվը պարունակում էր երկու վնասակար ֆայլ՝
  - msimg32.dll (SHA256: 693cc086089277f083b680ed822d988c2ea80483bd40caff202adccaa736bce4)

- Razer – Contract and payment terms for partners on YouTube URL version.exe (SHA256: 08c7fb6067acc8ac207d28ab616c9ea5bc0d394956455d6a3eecb73f8010f7a2)

Հարձակման ցուցիչներ (անգլ.՝ Indicators of Compromise, IOCs)

- **էլեկտրոնային փոստի հասցե**՝ contact@razer-us.com
- **էլեկտրոնային նամակի հասցեատեր**՝ narek.journalist@gmail.com
- **Կեղծ դոմեյն**՝ razer-us.com (գրանցվել է 2024 թվականի դեկտեմբերի 12-ին)
- **էլ-փոստի սերվերի IP**՝ 198.54.127.77
- **Հոսթինգ սերվերի IP**՝ 198.54.118.220
- **Վնասակար ֆայլերի անուններ**՝
  - msimg32.dll
  - Razer – Contract and payment terms for partners on YouTube URL version.exe (MD5: 4864a55cff27f686023456a22371e790)
- **Ֆայլերի հեշեր**՝
  - msimg32.dll (MD5: 0d61f3fe33123d0fdc20a7db2c969c4f)
  - Razer – Contract and payment terms for partners on YouTube URL version.exe (MD5: 4864a55cff27f686023456a22371e790)
- **VirusTotal վերլուծության հղումներ**՝
  - msimg32.dll
  - Razer – Contract and payment terms for partners on YouTube URL version.exe

Վերլուծություն

Հարձակում գործողները սոցիալական ինժեներիայի մեթոդների օգտագործմամբ ստեղծել են համոզիչ ֆիշինգային էլ-նամակ՝ չարաշահելով լրագրողի՝ հնարավոր հովանավորչական գործարքի հանդեպ հետաքրքրությունը: Իրական Razer դոմեյնին շատ նման կեղծ դոմեյնի կիրառումը ավելի համոզիչ է դարձրել «առաջարկը»: Վնասակար ֆայլերի ընդգրկումը՝ քողարկված իբրև վստահելի փաստաթղթեր, միտված է եղել կոտրելու թիրախի համակարգը՝ հենց դրանք ներբեռնվեին և մեկնարկ ստանային:

Խորհուրդներ

- **էլ-փոստի անվտանգություն**. ներդրեք էլ-փոստի զտման և ֆիշինգի հայտնաբերման առաջադեմ մեխանիզմներ:

- **Օգտատերերի իրազեկում**. Պարբերաբար դասընթացներ անցկացրեք ֆիշինգի փորձերը ճանաչելու և էլ-նամակների իսկությունը ստուգելու վերաբերյալ:
- **Ցանցային անվտանգություն**. մշտադիտարկեք ցանցի կասկածելի գործողությունների տրաֆիկը և արգելափակեք մուտքը դեպի հայտնի վնասակար դոմեյններ և IP հասցեներ:
- **Սարքերի պաշտպանություն**. համոզվեք, որ առկա են հակավիրուսային և վնասարար ծրագրերի դեմ ուղղված վստահելի միջոցներ՝ սպառնալիքները հայտնաբերելու և մեղմելու համար:

Թիրախավորված ֆիշինգային հարձակում հայկական ՀԿ-ի վրա

2025 թվականի մայիսի 28-ին CyberHUB-AM-ը բացահայտել է լավ մշակված, բարդ ֆիշինգային հարձակում, որի թիրախում եղել է իր գործընկեր ՀԿ-ներից մեկը:

Dear Sir

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

VAHAGNKHACHATRYAN0-INVITATION-SCANDOC.PDF

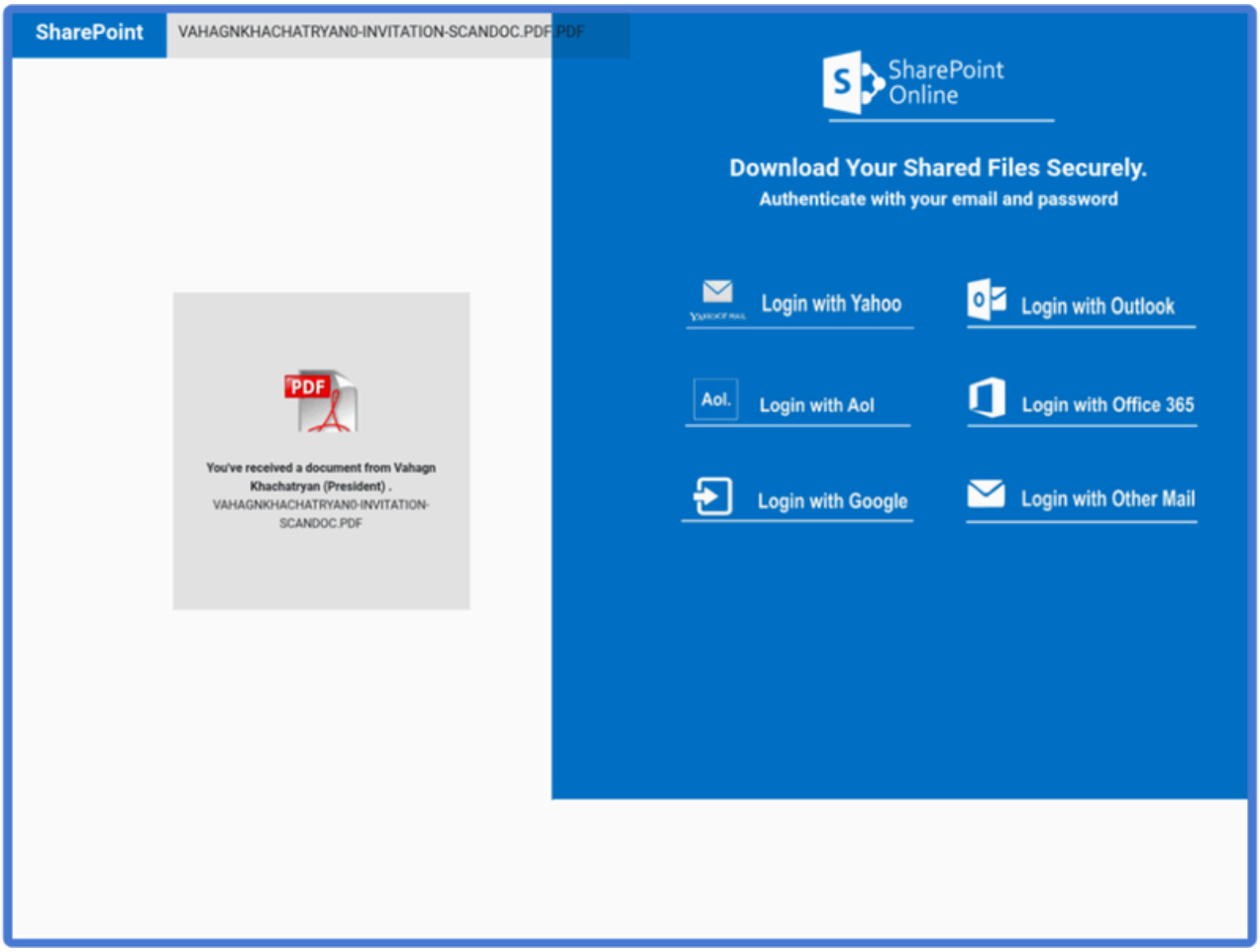
Regards

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

Հարձակման հեղինակներն ուղարկել են ֆիշինգային նամակ՝ PDF փաստաթղթի հղումով, որը քողարկված էր իբրև պաշտոնական փաստաթուղթ՝ VAHAGNKHACHATRYAN0-INVITATION-SCANDOC.PDF:

Այսպիսով, https://snip.ly/l9xqzf URL հղումը վերահասցեավորվել է վնասակար GitHub Pages կայքին (https://asw910.github.io/ar.mernia.github.io/index.html), որը ստեղծվել է օրինական բովանդակությունը նմանակելու նպատակով: Էջում ներկառուցված JavaScript-ը (jquery.min.js) ակտիվացրել էր գաղտնաբառերի հավաքագրման գործընթաց և մուտքային տվյալները փոխանցել կոտրված սերվերին հետևյալ հասցեով՝ hxxps[://]wbbuffetchurrascobh[.]com[.]br/wp-admin/email[.]php:



Թիրախ

Հարձակումը հստակ ուղղված է եղել քաղաքացիական հասարակության դեմ՝ մասնավորապես հայաստանյան ՀԿ-ի, ինչը վկայում է շահերի պաշտպանության, տարածաշրջանային քաղաքականության և իրավապաշտպան գործունեությամբ զբաղվող կազմակերպություններին նկատմամբ հարձակվողների ռազմավարական հետաքրքրության մասին:

Մարտավարություն, մեթոդներև ընթացակարգեր (Tactics, Techniques, and Procedures, TTPs)

Հետախուզություն

- **Թիրախի պրոֆիլավորում**. ֆիշինգային խայծի դերում օգտագործվել է Հայաստանի նախագահ Վահագն Խաչատուրյանի անունը (VAHAGN KHACHATRYAN), այն ստացվել է ՀՀ վարչապետի աշխատակազմի ղեկավարի անունից, ինչը վկայում է նախնական ուսումնասիրության կամ չարագործների մոտ որոշակի տվյալների առկայության մասին:

Ռեսուրսների մշակում

- **Ենթակառուցվածքի օգտագործում՝**
  - GitHub-ի (նոր գրանցված) օգտատիրոջ՝ asw910-իմոտ GitHub Pages-ում տեղադրվել է վնասաբեր ֆայլը:
  - Վերահղման շղթայում օգտագործվել է Snip.ly-ն՝ վերջնական վնասակար հասցեն քողարկելու նպատակով:

Առաքում

- **Ֆիշինգային նամակ**. ուղարկվել է սովորական էլեկտրոնային փոստի միջոցով: Այն պարունակել է սոցիալական ինժեներիայի մեխանիզմներով պատրաստված հղում՝ հետաքրքրասիրությունն ու հրատապությունը խթանելու համար՝ մղելով գործողության, որը բնորոշ է «spear phishing»-ի տեխնիկային:

Հասանելիություն մուտքային տվյալներին

- **Մուտքային տվյալների հավաքագրում**. GitHub-ի էջում տեղակայված վնասակար JavaScript-ը հավաքել է մուտքագրված տվյալները և, օգտագործելով POST հարցումները, դրանք փոխանցել է WordPress-ի կոտրված կայք:

Քողարկում

- **Կոդի քողարկում**. ֆիշինգային կոդը քողարկվել է որպես սովորական JavaScript գրադարան (jquery.min.js)՝ հայտնաբերվելուց խուսափելու համար:

MITER ATT&CK քարտեզագրում

- T1566.001 – ֆիշինգային նամակ՝ կցված ֆայլով

- T1584 – ենթակառուցվածքի վնասում
- T1204.002 – օգտագտատիրոջ կողմից գործարկում. վնասաբեր ֆայլի բացում
- T1056.001 – մուտքային տվյալների գրանցում՝ Keylogging կեղծ հավատարմագրերի ձևի միջոցով
- T1071.001 – կիրառական մակարդակի արձանագրություններ՝ վեբ արձանագրություններ

Քաղված դասեր

1. **Հեղինակավոր հարթակի չարամիտ օգտագործում -** GitHub-ում վնասակար բովանդակության տեղադրումը և հղումների համառոտման հանրահայտ Snip.ly ծառայության կիրառումը ցույց են տալիս, թե ինչպես են հարձակում գործողներն օգտվում վստահելի ծառայություններից՝ սեղմումների տոկոսային հարաբերակցությունը մեծացնելու և զտիչները շրջանցելու համար:
2. **Քաղաքացիական հասարակության դեմ թիրախային հարձակումներ** - Սա պատահական հարձակում չէր. այն արտացոլում է քաղաքական դրդապատճառներով պայմանավորված հարձակումների աճող միտումները, որտեղ թիրախում ՀԿ-ները, լրագրողները և ակտիվիստներն են, ինչը համապատասխանում է տարածաշրջանային սպառնալիքների վերաբերյալ զեկույցներում նկարագրված մոդելներին և դեպքերին:
3. **Մուտքային տվյալների հավաքագրում POST-ի միջոցով** - Այս տարածված, բայց արդյունավետ տեխնիկան ընդգծում է POST-ից դուրս եկող անոմալիաների տրաֆիկի ստուգման կարևորությունը, հատկապես դեպի օտարերկրյա դոմեյններ կամ չճանաչված հասցեներ:
4. **Պաշտպանական բացեր** - URL-ի զտման բացակայությունը կամ օգտատերերի իրազեկվածության պակասը հանգեցրել է նրան, որ զոհը սեղմել է վնասակար հղման վրա: Կազմակերպությունները պետք է առաջնահերթություն դարձնեն համապարփակ անվտանգությունը, ներառյալ վերջնակետի պաշտպանությունը և DNS (անգլ.՝ Domain Name System՝ Դոմեյնային անունների համակարգ) ֆիլտրացիան:

Խորհուրդներ

- Կիրառել SPF, DKIM, DMARC մեխանիզմներ՝ ուղարկողի իսկությունը ստուգելու և կեղծ նամակները հայտնաբերելու համար:
- Արգելափակել հղումը կարճացնող ծառայությունների հասանելիությունը՝ բացառությամբ հատուկ թույլատրվածների:

- Մշտապես վերահսկել GitHub-ի և այդօրինակ հարթակների համանման դոմեյնները, քանի որ դրանք հաճախ օգտագործվում են վնասաբեր բովանդակություն տարածելու համար:
- Կանոնավոր կերպով և պարբերաբար իրականացնել ֆիշինգային վարժանքներ, սիմուլյացիաներ և իրազեկման դասընթացներ, որպեսզի աշխատակիցները հնարավորինս կարողանան տարբերակել սպառնալիքները՝ հիմնված հարձակվողների կողմից կիրառվող ներկայիս մեթոդների վրա:

Սույն զեկույցը լույս է սփռում այն զարգացող մեթոդների վրա, որոնք հարձակում իրականացնողներն օգտագործում են հեղինակավոր ենթակառուցվածքները շահագործելու նպատակով, և ընդգծում է քաղաքացիական հասարակության համար սպառնալիքների աճը: Քննարկված միջադեպերն ու մոդելները մատնանշում են բարելավված պաշտպանական միջոցների, օգտատերերի իրազեկվածության բարձրացման և սպառնալիքների պրոակտիվ մոնիտորինգի հրատապ անհրաժեշտությունը: Առաջարկված խորհուրդներին հետևելով՝ կազմակերպությունները կարող են զգալիորեն ամրապնդել իրենց անվտանգային հնարավորություններն ընդդեմ թիրախային հարձակումների: