Բազմակողմանի
տեղեկատվության ինստիտուտ

PEGASUS.
ԻՆՉՊԵ՞Ս ԵՆ ԹԻՐԱԽԱՎՈՐԵԼ ՀԱՅԱՍՏԱՆԸ

Զեկույց

Սարգիս Հարությունյան

ԵՐԵՎԱՆ
2024

PEGASUS.
ԻՆՉՊԵ՞Ս ԵՆ ԹԻՐԱԽԱՎՈՐԵԼ ՀԱՅԱՍՏԱՆԸ

Զեկույց

Սարգիս Հարությունյան

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

Նախաբան 4

Pegasus-ի մասշտաբները 5

Թիրախում Հայաստանն է 7

Մեկնարկը տրվել է առնվազն 2020 թվականի հուլիսին 7

Առաջնային թիրախը Հայաստանի ղեկավարությունն էր 8

Ի՞նչ թվերի մասին է խոսքը 9

Ձեզ հետևում է Bozbash-ը 10

Դիտարկումներ 12

Նախաբան

Կիբեռանվտանգության ոլորտում հայաստանցի մասնագետների գնահատմամբ, 2020 թվականից ամռանից մինչև 2023-ի աշուն Pegasus լրտեսող ծրագրի միջոցով Հայաստանում թիրախավորվել է մի քանի հարյուր անձ՝ պետական, քաղաքական, տնտեսական, հանրային գործիչներ, քաղհասարակության ներկայացուցիչներ և լրագրողներ:

Թիրախների շարքում են Հանրապետության առաջին երեք դեմքերը՝ երկրի նախագահ Վահագն Խաչատուրյանը, վարչապետ Նիկոլ Փաշինյանը, Ազգային ժողովի նախագահ Ալեն Սիմոնյանը, նրանց ընտանիքների անդամները[1] [2] [3]:

Access Now-ի, CyberHUB-AM-ի, Տորոնտոյի համալսարանի Munk School of Global Affairs-ի (the Citizen Lab), Amnesty International-ի անվտանգության լաբորատորիայի և թվային անվտանգության գծով հետազոտող Ռուբեն Մուրադյանի համատեղ հետաքննության արդյունքում 2023 թվականի մայիսին հայտնի դարձավ 12 դեպքերի մասին, երբ Apple-ի զգուշացնող ծանուցումներ ստացողների iPhone-ները փորձաքննության ենթարկեցին, և հետազոտողները պարզեցին, որ նրանք թիրախավորվել են Pegasus լրտեսող ծրագրի կողմից: Այդ գրոհները համընկել են Լեռնային Ղարաբաղի և Հայաստանի դեմ Ադրբեջանի նախաձեռնած 44-օրյա պատերազմի և դրան հաջորդած ռազմական գործողությունների հետ՝ փաստորեն, դառնալով պատերազմի ժամանակ մասնավոր լրտեսող ծրագրերի կիրառման առաջին հանրահայտ դեպքը[4]:

Այս զեկույցի նպատակն է լայն հանրությանը, որոշում կայացնողներին ներկայացնել համակարգված տեղեկատվություն Հայաստանում Pegasus լրտեսող ծրագրի կիրառության մասին:

---

1 Armenian Cabinet member, opposition MP among possible Pegasus spyware targets. Armenpress. Published November 25, 2021. Accessed June 18, 2024. https://armenpress.am/en/article/1069104

2 Apple նոր մեյլեր ա ուղարկում: Pegasus... - Samvel Martirosyan. Facebook.com. Published 2023. Accessed June 18, 2024. https://www.facebook.com/samvel/posts/pfbid02mb9FeTTK1SHB3g3K3f6Ctm8c1S2pQRQC6GnbaPUdNkVfuLwQJ5jAg1mdYA8Qa46Yl

3 Արտակ Խուլյան. Փաշինյանը կտրականապես հերքում է կառավարության կողմից լրտեսական ծրագիր օգտագործելու մասին տեղեկությունը. “Ազատ Եվրոպա/Ազատություն” ռադիոկայան. Published March 15, 2023. Accessed June 18, 2024. https://www.azatutyun.am/a/32319719.html

4 Spyware in warfare: Access Now documents first-time use of Pegasus tech in Azerbaijan-Armenia conflict - Access Now. Access Now. Published May 25, 2023. Accessed June 18, 2024. https://www.accessnow.org/press-release/spyware-warfare-pegasus-in-azerbaijan-armenia-conflict/

Pegasus-ի մասշտաբները

Pegasus-ը լրտեսող ծրագիր է, որը թողարկում և վաճառում է իսրայելական NSO Group ընկերությունը: Pegasus-ն օգտագործում է բջջային սարքերի անվտանգային խոցելիությունը՝ չթույլատրված մուտք գործելու համար: Ընդ որում, հաճախ այդ ընթացքում օգտատիրոջ որևէ գործողություն չի պահանջվում: Թիրախի սմարթֆոնում ներկառուցվելուց հետո, Pegasus-ը հարձակվողին թույլ է տալիս մուտք ունենալ օգտատիրոջ գաղտնաբառեր, կոնտակտներ, օրացույց, տեքստային հաղորդագրություններ, զանգեր, անգամ՝ միացնել հեռախոսի տեսախցիկը և խոսափողը՝ սարքի մոտակայքում առկա իրավիճակը արձանագրելու համար:

Թեև լրտեսող ծրագրի կիրառման իրական մասշտաբների մասին տվյալները հայտնի չեն, սակայն անցած տարիներին Pegasus-ի վերաբերյալ հրապարակված մի շարք փորձագիտական և լրագրողական զեկույցներն ու հետաքննությունները թույլ են տալիս որոշակի դատողություններ անել այդ մասին:

2016 թվականի զեկույցում the Citizen Lab-ը առաջին անգամ անդրադարձավ Pegasus-ին՝ մանրամասնելով, որ այն օգտագործվել է՝ Արաբական Միացյալ Էմիրություններում գործող մարդու իրավունքների պաշտպան Ահմեդ Մանսուրին թիրախավորելու համար[5]:

2018 թվականին հրապարակված the Citizen Lab-ի մեկ այլ զեկույցի համաձայն, NSO Group-ի լրտեսող ծրագիրը կիրառվում էր աշխարհի 45 երկրներում: Հետխորհրդային երկրներից նշված էին միայն կենտրոնասիական չորս երկրները՝ Ղազախստան, Ղրղզստան, Ուզբեկստան ու Տաջիկստան[6]:

Երեք տարի անց՝ 2021 թվականի հուլիսին, ֆրանսիական Forbidden Stories-ի համակարգմամբ Le Monde, The Guradian, Süddeutsche Zeitung, The Washington Post և այլ պարբերականներում գրեթե միաժամանակ լույս տեսած հրապարակումների համաձայն, Pegasus կիրառող երկրների թիվն անցնում էր 50-ից[7]: Լրագրողների ձեռքին էր հայտնվել մոտ 50 հազար հեռախոսահամար՝ Pegasus-ի թիրախներ աշխարհի տարբեր երկրներից: Այս զեկույցում արդեն հիշատակվում էր նաև Ադրբեջանը[8]:

Զեկույցը փաստում էր՝ տարբեր պետություններում Pegasus-ով թիրախավորվել են առնվազն 3 նախագահներ, 10 վարչապետներ, 1 թագավոր, ավելի քան 600 պետական բարձրաստիճան պաշտոնյաներ և քաղաքական ազդեցիկ գործիչներ, միջազգային գործարար հանրությունում կշիռ ունեցող 65 ղեկավարներ, 85 հեղինակավոր իրավապաշտպաններ և 189 հայտնի լրագրողներ[9]:

---

5 https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

6 Marczak B. HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries - The Citizen Lab. The Citizen Lab. Published September 18, 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/. Accessed May 20, 2024

7 About The Pegasus Project | Forbidden Stories. Forbiddenstories.org. Published 2021. 2024. https://forbiddenstories.org/about-the-pegasus-project/. Accessed May 20

8 About The Pegasus Project | Forbidden Stories. Forbiddenstories.org. Published 2021. Accessed May 20, 2024. https://forbiddenstories.org/about-the-pegasus-project/

9 Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. Carnegieendowment.org. Published 2023. https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en. Accessed May 20, 2024

NSO Group-ի ֆինանսական տվյալները ևս կարևոր ցուցիչ են: Հայտնի է, որ 2014 թվականին ընկերության եկամուտը կազմել է 40 միլիոն դոլար[10] և այդ ժամանակ այն ուներ մոտ 50 աշխատակից[11]: 2018 թվականի տարեկան եկամուտը գրեթե վեց անգամ շատ էր՝ 250 միլիոն դոլար[12], իսկ աշխատակիցների քանակը 2019 թվականին հասել էր 700-ի[13]:

Թե ինչ արժե Pegasus կիրառելը՝ հրապարակային պաշտոնական տեղեկություններ չկան: Ոլորտի մասնագետները սա օրինաչափ են համարում, որովհետև խոսքը գաղտնի, փակ պայմանավորվածությունների, գործողությունների մասին է, ուստի գինն էլ գործարքային է՝ յուրաքանչյուր դեպքում առանձին պայմանավորվածություններ ու թվեր են:

2016 թվականի սեպտեմբերին The New York Times-ը գրեց, թե, օրինակ, 10 հատ iPhone վարակելը արժե 650 հազար դոլար՝ գումարած ևս կես միլիոն դոլար՝ լրտեսող ծրագրի աշխատանքը ապահովող և հատուկ ձեզ համար ստեղծվող ենթակառուցվածքի հիմնման համար[14]:

Հայտնի է նաև, որ, օրինակ, 2012 թվականին Մեքսիկայի կառավարության հետ NSO Group-ի գործարքը կազմել է 20 միլիոն դոլար[15], իսկ 2017 թվականին Սաուդյան Արաբիայի հետ՝ 55 միլիոն դոլար[16]:

[10] Brewster T. Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text. Forbes. Published August 30, 2016. https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=6ae2815e3997. Accessed May 20, 2024

[11] Davies V. Who are NSO Group, the company being sued by Apple? Cybermagazine.com. Published November 25, 2021. https://cybermagazine.com/cyber-security/who-are-nso-group-company-being-sued-apple. Accessed May 20, 2024.

[12] NSO founders, management buy stake in firm from Francisco Partners. Timesofisrael.com. Published 2019. https://www.timesofisrael.com/nso-founders-management-buy-stake-in-firm-from-francisco-partners/. Accessed May 20, 2024.

[13] The Battle for the World's Most Powerful Cyberweapon (Published 2022). The New York Times. https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html. Published 2024. Accessed May 21, 2024.

[14] How Spy Tech Firms Let Governments See Everything on a Smartphone (Published 2016). The New York Times. https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html. Published 2024. Accessed May 21, 2024.

[15] Who are NSO Group, the company being sued by Apple? Cybermagazine.com. Published November 25, 2021. https://cybermagazine.com/cyber-security/who-are-nso-group-company-being-sued-apple. Accessed May 21, 2024.

[16] The Battle for the World's Most Powerful Cyberweapon (Published 2022). The New York Times. https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html. Published 2024. Accessed May 21, 2024.

Թիրախում Հայաստանն է

Հայաստանյան օգտատերերը Apple-ի ծանուցումները սկսեցին ստանալ 2021 թվականի նոյեմբերից[17]: Ըստ Apple-ի, այդ ծանուցումների նպատակն էր «տեղեկացնել և օգնել այն օգտատերերին, որոնք հնարավոր է անհատապես թիրախավորվել են շահադիտական լրտեսող ծրագրերի հարձակումների կողմից»[18]: Սակայն Apple-ի ծանուցումներում հստակեցված չեն հարձակվողները կամ ինչ տեխնոլոգիա է կիրառվել, ինչը բացահայտելու համար լրացուցիչ վերլուծության կարիք կա[19]:

Այլ կերպ ասած, Apple-ի ծանուցումները կարող են նշանակել, որ կիրառվել է Pegasus, Predator, Candiru կամ ցանկացած այլ լրտեսող ծրագիր: Սա նաև նշանակում է, որ Հայաստանում Pegasus-ի կիրառման ճշգրիտ շրջանակը հնարավոր չէ որոշել՝ սոսկ այն հիմքով, թե քանի մարդ է ստացել Apple-ի ծանուցումը: NSO-ի հաճախորդների ամբողջական ծավալը նույնպես անհայտ է՝ նաև այն պատճառով, որ պատվիրատուների գործունեության բնույթը գաղտնի է: Այնուամենայնիվ, կիբեռանվտանգության հայաստանցի մասնագետների գնահատմամբ, Pegasus-ի միջոցով հարձակման ենթարկված անձանց թիվը կարող է հասնել հարյուրների:

Հայաստանում Pegasus լրտեսող ծրագրի՝ թվային քրեագիտության (digital forensic) միջոցով հաստատված միակ դեպքերը նկարագրված են Access Now-ի, the Citizen Lab-ի, CyberHUB-AM-ի և Ռուբեն Մուրադյանի 2023 թվականի համատեղ հետաքննության մեջ, որը փաստում է Pegasus-ի կիրառումը Հայաստանում քաղաքացիական հասարակության 12 ներկայացուցիչների նկատմամբ: Այդուհանդերձ, ցայսօր Հայաստանի իրավապահ մարմինների կողմից բացահայտումներ չեն եղել, թեև, ենթադրաբար, այդ առումով դիմումներ եղել են:

Բացը լրացնելու նպատակով՝ սույն զեկուցի պատրաստման ընթացքում նաև հենվել ենք կիբեռանվտանգության գծով հայաստանյան մասնագետների՝ CyberHUB-AM-ի համահիմնադիր Արթուր Պապյանի և SS անվտանգության գծով փորձագետ Ռուբեն Մուրադյանի հետ հարցազրույցների վրա: Երկու մասնագետներն էլ նախորդ տարիներին հետազոտել են Pegasus-ի բազմաթիվ վարակումներ:

Մեկնարկը տրվել է առնվազն 2020 թվականի հուլիսին

CyberHUB-AM-ի և Ռուբեն Մուրադյանի կողմից Հայաստանում Pegasus-ով վարակված սմարթֆոնների ուսումնասիրությունները ցույց տվեցին, որ հայաստանյան առաջին հաջող թիրախավորումներն արվել են առնվազն 2020 թվականի հուլիսին: Ժամանակահատվածը համընկավ տավուշյան մարտերին: Ինչպես հայտնի է, այդ տարվա հուլիսի 12-21-ը ռազմական գործողություններ ծավալվեցին Հայաստանի ու Ադրբեջանի զինված ուժերի միջև՝ Տավուշի մարզի ուղղությամբ:

Սա կարևոր առանձնահատկություն է, որովհետև հետագայում վարակումների մասին տեղեկությունները, Apple-ի ծանուցումները ուսումնասիրելիս՝ պարզ էր դառնում, որ հայաստանյան թիրախների դեմ Pegasus-ի կիրառումը հատկապես ակտիվ է եղել հայ-ադրբեջանական սրացումների՝ պատերազմի, սահմանային բախումների, հայ-

[17] https://support.apple.com/en-us/102174
[18] Նույն տեղում:
[19] Access Now's Digital Security Helpline and Apple threat notifications - Access Now. Access Now. Published May 2, 2024. Accessed July 3, 2024. https://www.accessnow.org/help/access-nows-digital-security-helpline-and-apple-threat-notifications/

ադրբեջանական առանցքային բանակցությունների, հայաստանյան ներքաղաքական լարվածության ժամանակաշրջանում, ինչն առաջին հիմքերից է կասկածելու, որ Հայաստանում, Հայաստանի դեմ ծավալվող կիբեռարշավների հետևում կանգնած են Ադրբեջանի իշխանությունները:

Գոյություն ուներ մեկ այլ պատճառ, թե Հայաստանում Pegasus-ը ինչու սկսվեց կիրառվել 2020 թվականի ամռանից: Ըստ տեղեկությունների, մինչ այդ Բաքվում աշխատում էին լրտեսող ծրագրեր մշակող ու վաճառող իտալական HackingTeam-ի[20] և իսրայելական Candiru[21] ընկերությունների հետ: Ընդհանրապես, Carnegie Endowment for International Peace-ի գնահատմամբ, Ադրբեջանի կառավարությունը սկսել է նման լրտեսող ծրագրեր կիրառել դեռ 2009 թվականից, և խոսքը, ըստ ամենայնի, վերաբերում է 2003 թվականին հիմնադրված HackingTeam-ի հետ համագործակցությանը[22]:

Հնարավոր է, Բաքվում գոհ չէին HackingTeam-ի և Candiru-ի հետ համագործացության արդյունքներից, և անցում է կատարվել Pegasus-ին, կամ NSO Group-ի ընձեռած հնարավորություններն ավելի լայն էին ու գրավիչ:

Առաջնային թիրախը Հայաստանի ղեկավարությունն էր

Հայաստանի վարչապետ Նիկոլ Փաշինյանը[23], Ազգային ժողովի նախագահ Ալեն Սիմոնյանը[24], երկրի նախագահ Վահագն Խաչատուրյանը[25] հրապարակավ հայտարարել են, որ ստացել են Apple-ի ծանուցումներ: Այս պահին թվային քրեագիտական որևէ վերլուծություն չունենք, որը կհստակեցներ, թե ինչ լրտեսող ծրագրի թիրախում են նրանք հայտնվել, կամ արդյո՞ք, ընդհանրապես, թիրախավորվել են:

CyberHUB-AM-ի ուսումնասիրության արդյունքում հաստատվել է, որ տարբեր նախկին և գործող պետական պաշտոնյաների, պատգամավորների, փորձագետների, քաղաքացիական հասարակության ներկայացուցիչների և լրագրողների ավելի քան երկու հարյուր iPhone-ներ ստացել են սպառնալիքների մասին Apple-ի ծանուցումները, ինչը արձանագրված ամենից բարձր թիվն է:

«Գիտենք, որ Pegasus-ով թիրախավորվելու մասին հայտարարել են Հայաստանի վարչապետ Նիկոլ Փաշինյանը, Ազգային ժողովի նախագահ Ալեն Սիմոնյանը, նախագահ Վահագն Խաչատուրյանը: Թիրախավորման մասին հայտարարել են ԱԱԾ նախկին

[20] Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses, https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

[21] So strategic relations with Azerbaijan became a family affair for Lieberman https://detaly.co.il/tak-strategicheskie-otnosheniya-s-azerbajdzhanom-stali-semejnym-delom-libermana/

[22] Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses, https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

[23] Արտակ Խուլյան. Փաշինյանը կտրականապես հերքում է կառավարության կողմից լրտեսական ծրագիր օգտագործելու մասին տեղեկությունը. “Ազատ Եվրոպա/Ազատություն” ռադիոկայան. Published March 15, 2023. Accessed July 2, 2024. https://www.azatutyun.am/a/32319719.html

[24] Apple նոր մեյլեր ա ուղարկում: Pegasus... - Samvel Martirosyan. Facebook.com. Published 2023. Accessed July 2, 2024. https://www.facebook.com/samvel/posts/pfbid02mKyGhkhYv57vGtpXCSBALNWSptorDkJiADceDCz3RDWgvt558pJ7JjNNTezEx2Eel

[25] Armenpress. Armenian Cabinet member, opposition MP among possible Pegasus spyware targets. Armenpress. Published November 25, 2021. Accessed July 2, 2024. https://armenpress.am/en/article/1069104

ղեկավար Արթուր Վանեցյանը[26], Պետական վերահսկողության ծառայության նախկին պետ Դավիթ Սանասարյանը[27], Մարդու իրավունքների նախկին պաշտպան Քրիստինե Գրիգորյանը: Այսինքն, մարդիկ, որոնց ի պաշտոնե հասանելի է եղել շատ զգայուն տեղեկատվություն[28]: Pegasus-ով վարակված լինելու մասին հայտարարել են նաև ընդդիմադիր գործիչներ Դավիթ Խաժակյանը, Ռուբեն Մելիքյանը, Սամվել Ֆարմանյանը»,- մեզ հետ զրուցում պատմեց Արթուր Պապյանը[29]:

Հաջորդ կարևոր հանգամանքն է, որ պետական մարմիններից թիրախավորումները հատկապես կենտրոնացած են եղել անվտանգային հարցերով զբաղվող կառույցների աշխատակիցների ուղղությամբ՝ Հայաստանի Անվտանգության խորհուրդ, Արտաքին գործերի ու Պաշտպանության նախարարություններ, Ազգային անվտանգության ծառայություն, Ոստիկանություն:

««Վարակվել» էր Հայաստանի Արտաքին գործերի նախարարության գրեթե ողջ անձնակազմը: Ծավալները շատ մեծ էին: Վարակում էին բոլորին, ով կարող էր որևէ տեղեկության տիրապետել Հայաստանի անվտանգային ու արտաքին քաղաքականությունների վերաբերյալ: Աննա Նաղդալյանի հեռախոսը, օրինակ, Pegasus-ով վարակել են 27 անգամ, որովհետև նրա սմարթֆոնի մարտկոցը լավը չէր, հեռախոսը հաճախ էր «նստում», ուստի ստիպված էին նորից վարակել այն, քանի որ iPhone-ների վերագործարկումից հետո հեռախոսը պետք է կրկին վարակել Pegasus-ով»,- փոխանցեց Ռուբեն Մուրադյանը:

Մուրադյանի խոսքերն ավելի ուշ հաստատում գտան the Citizen Lab-ի կողմից 2023 թվականի մայիսին հրապարակած Technical Brief զեկույցում[30], ուր մանրամասներ են թիրախավորման ընթացքում օգտագործված ենթակառուցվածքի և խոցելիությունների մասին:

Ի՞նչ թվերի մասին է խոսքը

Թե 2020 թվականի հուլիսից ի վեր որքան է կազմել Pegasus-ով թիրախավորված հայաստանյան օգտատերերի թիվը, թիրախավորումների քանի տոկոսն է հաջող եղել, նշել ենք, որ ցայսօր ստույգ թիվը հայտնի չէ՝ նաև նախորդ հատվածում նկարագրված պատճառներով:

Զուգահեռաբար՝ հայաստանյան թիրախավորումների քանակի մասին տակավին լայն շրջանառության մեջ է AccessNow-ի, Citizen Lab-ի, Amnesty International-ի, CyberHUB-AM-ի և Ռուբեն Մուրադյանի կողմից իրականացված հետազոտությունը, որտեղ նշվում

---

[26] Artur Vanetsyan - Այսօր Apple ընկերությունից նամակ ստացա, որն... Facebook.com. Published 2023. Accessed July 2, 2024. https://www.facebook.com/avav111/posts/pfbid0ho6NbY5QtJho24pCsfSEvvGX2TvCurfnKGr25Apd54VAUYdV7jqUeh8kyUUBaR4Hl

[27] Երեկ գիշեր ժամը 2-ին Apple-ի... - Davit Sanasaryan. Facebook.com. Published 2023. Accessed July 2, 2024. https://www.facebook.com/sanasaryan/posts/pfbid0HnLVguwbPUiB2fo948RqwBYz7mevJUpscbhqvLgMZJ1MWcRCXx3Duh4ExAiaCK8Yl

[28] Armenia spyware victims: Pegasus hacking in war. Access Now. Published November 27, 2023. Accessed July 2, 2024. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/

[29] Armenia spyware victims: Pegasus hacking in war. Access Now. Published November 27, 2023. Accessed July 2, 2024. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/

[30] Scott-Railton J. Armenia-Azerbaijan conflict: Pegasus infections - Technical Brief [1] - The Citizen Lab. The Citizen Lab. Published May 25, 2023. Accessed July 3, 2024. https://citizenlab.ca/2023/05/cr1-armenia-pegasus/

է, թե 2020-2021 թվականներին Pegasus-ով Հայաստանում հաջողությամբ թիրախավորվել են քաղաքացիական հասարակության 12 ներկայացուցիչ[31]:

Այս հետազոտության շրջանակում, առանց անուններ ներկայացնելու հայաստանցի մասնագետների ներկայացրած թվերը առնվանզ մեկ կարգ բարձր են: CyberHUB-AM-ի և Ռուբեն Մուրադյանի ներկայացրած տվյալների համաձայն, 2020 թվականից իրենց դիմել են Apple-ից ծանուցումներ ստացած առնվազն 200 անձինք:

Հարկ է նկատել, որ խոսք է գնում բացառապես iOS օպերացիոն համակարգի մասին, քանի որ Google-ը Pegasus-ով թիրախավորվելու մասին ծանուցումներ չի ուղարկում իր ստեղծած օպերացիոն համակարգի՝ Android-ի օգտատերերին: Ուստի, թիրախավորումների քանակը կարող է ավելի բարձր լինել:

Այս լրտեսական ծրագրի հետազոտմամբ անմիջականորեն զբաղվող հայաստանյան մասնագետները պնդում են, որ 2020 թվականի հուլիսից ի վեր Հայաստանում Pegasus-ով թիրախավորվել են մի քանի հարյուր սմարթֆոններ (Արթուր Պապյանի գնահատականն է), և թիրախավորվել են հայաստանյան պետական մարմինների, քաղաքական ուժերի անգամ, այսպես կոչված, շարքային աշխատակիցներ ու անդամներ, գործարար աշխարհի, քաղաքացիական հասարակության և լրատվամիջոցների բազմաթիվ ներկայացուցիչներ:

Հայաստանյան թիրախավորումների ուսումնասիրության առաջին ակնհայտ է հետևությունն այն է, որ նախորդ տարիներին կիբեռգրոհների քանակի աճը գրեթե միշտ զուգորդվել է հայ-ադրբեջանական հարաբերություններում ժամանակ առ ժամանակ ծագող սրացումների հետ՝ 2020 թվականի տավուշյան մարտեր, 44-օրյա պատերազմ, Բաքվի գործողությունները Լեռնային Ղարաբաղի դեմ, Հայաստան-Ադրբեջան սահմանային մարտեր, հայ-ադրբեջանական բանակցությունների առանցքային փուլեր, կամ հայաստանյան ներքաղաքական կարևոր զարգացումների, օրինակ՝ 2021 թվականի հունիսին կայացած արտահերթ խորհրդարանական ընտրությունների հետ:

Ձեզ հետևում է Bozbash-ը

Գրեթե միշտ՝ առաջին հարցը, որ տալիս է յուրաքանչյուր ոք, ով հայտնվում է այդպիսի կիբեռհարձակման թիրախում, թե ով է կանգնած նման գրոհի հետևում, որովհետև այդ հարցի պատասխանն է, որ կօգնի հասկանալ՝ ինչո՞ւ են նման քայլի դիմել, ինչո՞ւ է հենց ինքը թիրախավորվել, ի՞նչ տեղեկություն, տվյալներ են փնտրել, ինչո՞ւ հենց հիմա, ի՞նչ պետք է սպասել, ի պատասխան՝ ի՞նչ պետք է ձեռնարկել և այլն:

Սկզբնական շրջանում հատկապես հայաստանյան մասնագետների մոտ հարցեր կային, թե հաշվի առնելով ընդդիմադիր քաղաքական գործիչների թիրախավորումը[32]՝ արդյո՞ք Հայաստանի իշխանություններն են կանգնած երկրում Pegasus-ի կիրառման հետևում: Սակայն ժամանակ անց ի հայտ եկած վկայությունները հետքերը տարան հարևան Ադրբեջան: Մոտ մեկ տարի առաջ՝ 2023 թվականի մայիսին լույս տեսան Access Now-ի, the Citizen Lab-ի, Amnesty International-ի ներքո գործող Security Lab-ի, CyberHUB-AM-ի և փորձագետ Ռուբեն Մուրադյանի՝ ամիսներ տևած համատեղ հետաքննության

[31] Armenia-Azerbaijan conflict Pegasus infections - Technical Brief, https://citizenlab.ca/2023/05/cr1-armenia-pegasus/. Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict, https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/

[32] Ռուբեն Մուրադյանի ներկայացմամբ, Հայաստանի երկրորդ ու երրորդ նախագահների շրջապատը ներկայացնող անձանց Pegasus-ով թիրախավորման դեպքերը եղել են մի քանի տասնյակ:

արդյունքները, ուր մի քանի առանցքային տվյալներ հրապարակվեցին Pegasus-ի օգտագործմամբ հայաստանյան թիրախավորումների գործում Ադրբեջանի մասնակցության մասին[33]:

The Citizen Lab-ի հրապարկման համաձայն, Ադրբեջանում դեռ 2018 թվականի ավարտին կամ նույնիսկ ավելի շուտ հիմնվել է Pegasus-ի կառավարման առնվազն երկու կենտրոն (օպերատորներ), որոնց հետաքննության հեղինակաները կոչել են Yanar ու Bozbash: Եթե առաջինը պատասխանատու է եղել Ադրբեջանի ներսում գործառնության համար, ապա Bozbash-ի նպատակն է եղել Pegasus-ով թիրախավորումներն ինչպես Ադրբեջանում, այնպես էլ արտերկրում, ներառյալ՝ Հայաստանը[34]:

Հայտնի է, որ, օրինակ, Ադրբեջանում թիրախավորված են եղել ավելի քան հազար սմարթֆոններ[35]:

Հայաստանի դեմ Ադրբեջանի կառավարության կողմից Pegasus-ի կիրառման մասին հրապարակավ հայտարարեց ԱՄՆ-ն: Այս ապրիլին հրապարակված Միացյալ Նահանգների պետքարտուղարության զեկույցում՝ աշխարհում մարդու իրավունքների վիճակի մասին, նշված է, թե կան ցուցիչներ, որ 2020 թվականի հոկտեմբերից մինչև 2022 դեկտեմբեր Ադրբեջանի կառավարությունը ներգրավված է եղել Հայաստանում քաղաքական նկատառումներով իրականացվող լրտեսման գործում՝ կիրառելով Pegasus ծրագիրը[36]:

[33] Armenia-Azerbaijan conflict Pegasus infections - Technical Brief, https://citizenlab.ca/2023/05/cr1-armenia-pegasus/

[34] Scott-Railton J. Armenia-Azerbaijan conflict: Pegasus infections - Technical Brief [1] - The Citizen Lab. The Citizen Lab. Published May 25, 2023. Accessed July 3, 2024. https://citizenlab.ca/2023/05/cr1-armenia-pegasus/

[35] Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict. Amnesty International. Published May 25, 2023. https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/. Accessed May 21, 2024.

[36] 2023 Country Reports on Human Rights Practices: Azerbaijan, https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/azerbaijan/.

Դիտարկումներ

Տեսանելի հեռանկարում նման կարգի կիբեռգրոհների հաճախականությունը, ծավալները և խորությունը կարող են աճել, քանի որ մարդկանց կախվածությունը սմարթֆոններից ու այլ տիպի գաջեթներից շարունակաբար աճում է:

Այս փետրվարին Google-ի Threat Analysis Group-ի հրապարակած զեկույցում ներկայացվել են լրտեսական ծրագրեր մշակող և վաճառող մոտ 40 մասնավոր կազմակերպություններ (commercial surveillance vendors[37]:

Անշուշտ, զուգահեռաբար զարգանում են նաև նման կարգի կիբեռգրոհներից պաշտպանելու կարողությունները: Ծրագրային ապահովումներ և սմարթֆոններ արտադրող ընկերությունները (Apple, Google, WhatsApp, Signal), պետություններն ու իրավապաշտպան կազմակերպությունները շարունակաբար ընդլայնում են իրենց ներգրավածությունը նմանատիպ լրտեսող ծրագրերի դեմ պայքարում[38], սեղանին են դնում նոր գործիքներ[39]՝ նման ծրագրերի հայտնաբերման համար, սակայն պետք է գիտակցել կարևոր մեկ փաստ՝ ձեր սմարթֆոնը եղել և մնում է լավագույն լրտեսը՝ հենց ձեր դեմ:

[37] Buying Spying Insights into Commercial Surveillance Vendors. https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf

[38] Նորություն չէ, որ հատկապես բռնապետական երկրներում իրավապաշտպանները, քաղաքացիական հասարակության ներկայացուցիչները և լրագրողները կառավարությունների առաջնային թիրախներից են, և նման ծրագրերն օգտագործվում են նրանց լրտեսելու համար:

[39] 2021 թվականի հուլիսին Amnesty International-ը ներկայացրեց Mobile Verification Toolkit-ը (MVT), որը գործիք է iOS և Android օպերացիոն համակարգերի վրա հիմնված սմարթֆոններում նման լրտեսող ծրագրեր հայտնաբերելու համար (https://docs.mvt.re/en/latest/): iOS-ով գործող սարքերի համար առկա է նաև iMazing գործիքը (https://imazing.com/guides/detect-pegasus-and-other-spyware-on-iphone):

Բազմակողմանի տեղեկատվության ինստիտուտ

www.mdi.am