ՀԱՅԱՍՏԱՆԻ ԴԵՄ ՀԱՔԵՐԱՅԻՆ ՀԱՐՁԱԿՈՒՄՆԵՐԻ ՄԱՍԻՆ

Սամվել Մարտիրոսյան[*]

Հայտնի է, որ Հայաստանի Հանրապետության, ինչպես նաև Սփյուռքի հայության դեմ բավական ակտիվ գործում են ադրբեջանական և թուրքական մի շարք հաքերային խմբավորումներ[1]: Մյուս կողմից՝ Հայաստանը թիրախավորում են այլ հաքերային խմբավորումներ, որոնք, ենթադրաբար, հովանավորվում կամ անմիջապես կառավարվում են տարբեր պետությունների հատուկ ծառայությունների կողմից:

Այսպես, Էդվարդ Սնոուդենի բացահայտումներից ելնելով՝ տեսնում ենք, որ Հայաստանի հանդեպ հետաքրքրությունը ԱՄՆ հատուկ ծառայությունների կողմից միջինից բարձր է: *NSA* բացահայտված համակարգերից մեկը, որը կոչվում է *Boundless Informant,* թույլ է տալիս քարտեզի վրա հետևել, թե որ երկրներից ինչ ակտիվությամբ է կորզվում տեղեկատվությունը ԱՄՆ այս հատուկ ծառայության կողմից էլեկտրոնային լրտեսության («շպիոնաժի») բոլոր հնարավոր միջոցներով: Սնոուդենի տրամադրած պատկերից երևում է, որ 2013թ. մարտի ընթացքում միայն ԱՄՆ տարածքից ստացվել է մոտ 3 միլիարդ տարբեր տիպի տեղեկատվություն: Երկրները ներկայացված են ըստ այդ ամսվա ընթացքում դրանց հանդեպ *NSA* համակարգի ակտիվության, կանաչ գույնը վկայում է ցածր ակտիվության մասին, կարմիրը՝ հակառակը: Տվյալ պատկերի վրա, օրինակ, Հայաստանը դեղին գույնի է՝ մոտավորապես Չինաստանի պես և Ռուսաստանից ավելի ակտիվ, ինչը խոսում է *NSA*-ի միջինից բարձր ակտիվության մասին[2] ինչն,

---

[*] «Նորավանք» ԳԿՀ Տեղեկատվական հետազոտությունների կենտրոնի փորձագետ:

[1] *Սամվել Մարտիրոսյան*, Ադրբեջանական հաքերները թիրախավորում են հայ օգտատերերին, http://www.noravank.am/arm/articles/detail.php?ELEMENT_ID=15580&sphrase_id=64438

[2] *Սամվել Մարտիրոսյան*, Սնոուդենի բացահայտումները. աշխարհին ամերիկյան և բրիտանական գաղտնալսման տակ, http://www.noravank.am/arm/articles/detail.php?ELEMENT_ID=12421&sphrase_id=64438

իհարկե, կարող է նորմայից բարձր լինել՝ պայմանավորված Հայաստանի ներքին իրավիճակով, որտեղ այդ ժամանակ ընտրություններ էին ընթանում (տե՛ս *Նկար 1*).

Նկար 1

Boundless Informant համակարգի տվյալների քարտեզն ըստ Էդվարդ Սնոուդենի կողմից բացահայտված փաստաթղթերի

Մյուս բացահայտումը նույնպես 2013թ. եղավ, և կրկին զուտ Հայաստանին չէր վերաբերում: Կասպերսկի լաբորատորիայում հայտնաբերեցին սուպերլրտեսական վիրուս, որն անվանվեց *Red October*: Այն ներմուծվում էր պետական և ոչ պետական կարևոր ենթակառուցվածքներ, կատարվում էին լայնածավալ կիբեռլրտեսական գործողություններ՝ գողանալով հնարավոր տիպի ամբողջ կարևոր տեղեկատվությունը, նույնիսկ վերականգնելով արդեն ջնջված ֆայլերը, որոնք կարող էին վիրուսի ստեղծողների համար հետաքրքիր լինել: Պարզվեց, որ ծրագիրը գաղտնի գործել է հինգ տարի և ոչ մի տեղ մինչև 2013թ. չի հայտնաբերվել: Հայաստանն ամենավարակված երկրների տասնյակի ցանկում էր, այստեղ Կասպերսկի լաբորատորիան հայնաբերել էր վարակման տասը դեպք[3]:

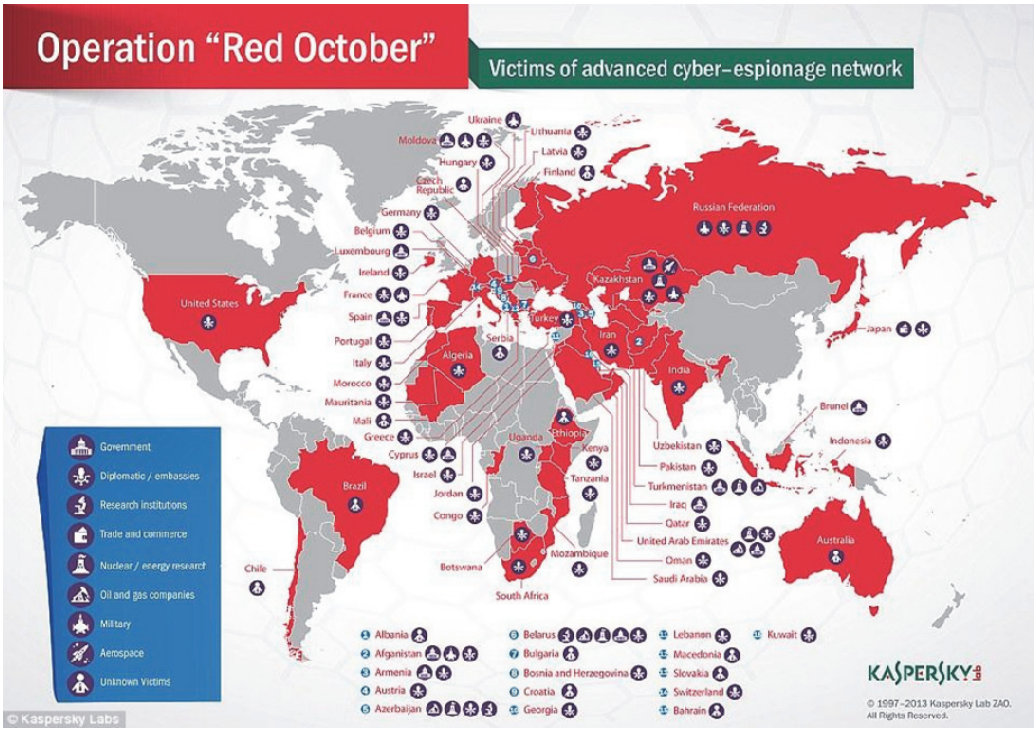
Այդպես էլ չհստակեցվեց, թե ով էր կանգնած *Red October*-ի հետևում: Անվտանգության մասնագետներն առնվազն գտել էին ծրագրի

[3] "Red October" Diplomatic Cyber Attacks Investigation, https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/#8

մեջ ռուսական հետքեր, սակայն դրանք կարող էին միտումնավոր թողած լինել կոդի մեջ, որպեսզի շեղեն ուշադրությունը: Ավելին, Ռուսաստանն այս հարձակման հիմնական թիրախն էր (տե՛ս *Նկար 2*): Ավելի հավանական է Չինաստանի հետքը: Օգտագործված տեխնիկաներում կան հատվածներ, որոնք հղում են անում մի շարք ծրագրերի վրա, որոնք օգտագործվել են Տիբեթի ակտիվիստների դեմ, և ենթադրաբար օգտագործվել են Չինաստանի հատուկ ծառայությունների կողմից:

Նկար 2

Red October ծրագրի թիրախներն
ըստ Կասպերսկի լաբորատորիայի



FireEye կազմակերպությունը, որը զբաղվում է տեղեկատվական անվտանգությամբ, 2014թ. *APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?* զեկույցում հայտնաբերել էր մի հաքերային խմբի լայնածավալ միջազգային ակտիվություն, որի թիրախներից մեկը

նաև հայաստանյան զինվորականներն էին[4]: Խոսքը *APT28* կամ *Fancy Bear* անվանումը կրող հաքերային խմբի մասին է, որը հիմա արդեն հայտնի է իր գործողություններով, որոնք, հավանաբար, ազդեցություն են ունեցել ԱՄՆ ընտրությունների ժամանակ: Տվյալ խումբը շատ մասնագետների կողմից համարվում է ռուսաստանյան պետական կիբեռխումբ, որը գործում է Կրեմլի շահերից ելնելով: Ըստ *FireEye*-ի ուսումնասիրության, *Fancy Bear* հաքերները ստեղծել էին կեղծ mail.rnil.am ֆիշինգային կայք, որը նմանակում էր Հայաստանի պաշտպանության նախարարության դոմեյնը՝ mil.am, և թույլ էր տալիս ֆիշինգային նամակների միջոցով թիրախավորել հայաստանյան զինվորականներին, նրանց դեմ իրականացնել կիբեռլրտեսական գործողություններ. «*o target members of the Armenian military by hosting a fake login page*»: Թե ինչ վնաս են հասցրել հաքերները Հայաստանին, հայտնի չէ:

2017թ. մայիսին *Citizen Lab* կազմակերպությունը նոր բացահայտումներ արեց *Fancy Bear* հաքերային խմբի նոր գործողությունների մասին: Այս անգամ նույնպես Հայաստանը հայտնվեց զոհերի ցանկում: *TAINTED LEAKS. Disinformation and Phishing With a Russian Nexus* զեկույցից հայտնի է դառնում, որ այս անգամ թիրախ են դարձել Հայաստանի կառավարության և բանակի ներկայացուցիչները[5]: Ըստ կազմակերպության տվյալների, Հայաստանը ֆիշինգային հարձակման հիմնական զոհ երկրներից մեկն էր, մոտ 3% ֆիշինգային հարձակումները բաժին են ընկնում հենց մեր հանրապետությանը: Մեր ունեցած տվյալներով՝ հայաստանյան զոհերի ցանկում կան բարձրաստիճան զինվորականներ, ինչպես նաև դիվանագետներ:

Տարեվերջին հայտնվեց *Associated Press*-ի «*Russia hackers pursued Putin foes, not just US Democrats*» զեկույցը[6], որում կրկին տեսնում ենք արդեն հարազատ դարձած *Fancy Bear* խմբին: Եվ նորից պարզ է դառնում, որ լայնածավալ կիբեռհարձակումների ցանկում, որոնք կատարվել են

[4] APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf, TAINTED LEAKS. Disinformation and Phishing With a Russian Nexus, https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

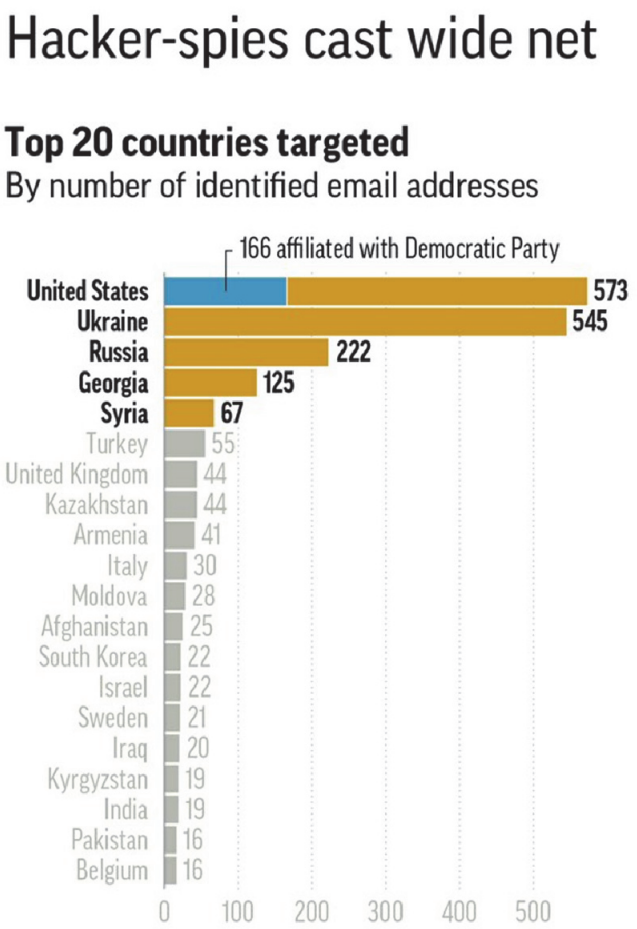
[5] TAINTED LEAKS. Disinformation and Phishing With a Russian Nexus, https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

[6] Russia hackers pursued Putin foes, not just US Democrats, https://www.apnews.com/3bca5267d4544508bb523fa0db462cb2

միանգամից բազմաթիվ պետությունների տարածքում, կան նաև հայաստանցիներ: Ըստ ներկայացված քանակական ցանկի, Հայաստանում եղել է 41 թիրախ (տե՛ս *Նկար 3*).

Նկար 3

Fancy Bear հաքերային խմբի հարձակման թիրախներն ըստ երկրների: Associated Press-ի տվյալներ



Սրանք պետական կիբեռլրտեսության այն մի քանի դեպքերն են, որոնց մասին տեղեկացված ենք: Հաշվի առնելով, թե վերջին տարիներին որքան արհեստավարժ է դարձել պետական հաքինգը, կարելի է եզրակացնել, որ Հայաստանի դեմ իրականացվող կիբեռգործողությունների մի մասը, գուցե՝ զգալի մասը, դեռ բացահայտված չէ: Հասկանալի է նաև, որ Հայաստանը հետաքրքրության թիրախ է գրեթե բոլոր խոշոր կիբեռհետախուզությունների համար: