tagesschau

ԲԱՑԱՌԻԿ Լրտեսող ծրագրակազմ

ԻՆՉՊԵՍ Է «ՊԵԳԱՍ»-Ը ԳՏՆՈՒՄ ԲՋՋԱՅԻՆ ՀԵՌԱԽՈՍԸ

Կարգավիճակ ՝ 18.07.2021, ժամը 18:01

Իսրայելական NSO ընկերության «Պեգաս» ծրագրակազմը հսկողության ամենահզոր գործիքներից մեկն է աշխարհում: Ծրագիրը կարող է գաղտնի տեղադրվել բջջային հեռախոսների վրա՝ առանց զոհի՝ այդ մասին ինչ-որ բան կռահելու:

Քրիստիան Բաարս, Ֆլորիան Ֆլեյդ և Գեորգ Մասկոլոն, NDR / WDR

Մի անգամ հարցազրույցում իսրայելական NSO ընկերության ղեկավար Շալև Հուլիոն բացատրեց այսպես, որ ընտրել են «Պեգաս» անունը, որովհետև ծրագրակազմը տրոյական ձի է, և այն էլ թևերով, որը ուղիղ թռչում է դեպի բջջային հեռախոս: Ֆիզիկական ոչ մի միջամտություն սարքին անհրաժեշտ չէ: Լրտեսության ծրագիրը կարող է տեղադրվել հեռակա, ծածուկ՝ առանց թիրախային անձի կողմից նկատվելու, և նույնիսկ զոհի կողմից առանց որևէ բան անելու:

«Խուսափեք ավելորդ ռիսկերից. Դուք չպետք է ամեն պահի թիրախի կամ սարքի մոտ մնաք », - ասվում էր NSO-ի գրքույկում մի քանի տարի առաջ: Տրոյական թևավոր «Պեգաս»-ը ընկերության գնայուն ապրանքն է: Ամբողջ աշխարհի գաղտնի ծառայությունները և ոստիկանական վարչություններն օգտագործում են այդ ծրագիրը՝ դրանով նպատակային անձանց համակողմանի և աննկատելիորեն հետախուզելու համար:

Բացառիկ 18.07.2021
Տրոյական «Պեգաս»
Ինչպես են ավտորիտար պետությունները լրտեսում իրենց հակառակորդներին
Ըստ երևույթին, ամբողջ աշխարհի լրագրողները, ակտիվիստներն ու քաղաքական գործիչները հզոր լրտեսական ծրագրակազմի թիրախ էին:

Եթե հարձակվողներին հաջողվել է «Պեգաս»-ն ածել օտար բջջային հեռախոսի վրա, ապա նրանք սարքի նկատմամբ ունեն լիակատար վերահսկողություն: Նրանք կարող են պատճենել բջջային հեռախոսի բոլոր տվյալները կամ, օրինակ, գաղտնի ակտիվացնել խոսափողը կամ տեսախցիկը և նույնիսկ կարդալ կոդավորված հաղորդագրություններ: Սակայն, վիճահարույց ծրագրակազմի հանրաճանաչության հիմնական պատճառը, ամենայն հավանականությամբ, այն փաստն է, որ «Պեգաս»-ը կարող է համեմատաբար հեշտությամբ գտնել բջջային հեռախոսը, և դա դժվար թե խոչընդոտվի:

«Այս տեսակի հարձակումներին դիմակայելու ոչ մի արդյունավետ միջոց չկա օգտագործողի համար», - ասում է “Amnesty International”-ի SS անվտանգության փորձագետ Կլաուդիո Գուարնիերին: NSO-ն իր հաճախորդներին առաջարկում է տարբեր միջոցներ, թե ինչպես կարող են թիրախային անձանց բջջային հեռախոսները վարակվել. կախված սարքի տեսակից կամ գործառնական համակարգից՝ դրանք կարող են քիչ թե շատ ժամանակատար լինել:

Կտտոցով և առանց կտտոցի

«Դասական» մեթոդը, որով «Պեգասը» մտնում է բջջային հեռախոս, աշխատում է կեղծ հաղորդագրության միջոցով: Թիրախային անձը դրդում է ստանում կտտացնել հղմանը կամ ֆայլին և, այդպիսով, անգիտակցաբար սկսում է ներբեռնումը, օրինակ՝ տեքստային հաղորդագրության կամ էլեկտրոնային նամակի միջոցով: Հենց որ կտտացնում են դրա վրա, տրոյականը տեղադրվում է: NSO-ն իր հաճախորդների տրամադրության տակ է դնում մի տեսակ շինարարական բլոկների հավաքածու, որով կեղծ էլեկտրոնային նամակները կամ տեքստային հաղորդագրությունները կարող են հնարավորինս ճշգրիտ և ճկուն կերպով մշակվել:

Այնուամենայնիվ, NSO ընկերությունը գտել է մեկ այլ, վախեցնող ճանապարհ, թե ինչպես «Պեգաս»-ը կարող է աննկատ տեղադրվել բջջային հեռախոսի վրա. ճանապարհ, որի դեմ զոհերը լրիվ անպաշտպան են: Կտտացնելու անհրաժեշտություն այլևս չկա: Բջջային հեռախոսը միայն պետք է միացված և ցանցին կապված լինի: Հարձակվողը ուղարկում է հաղորդագրություն, որը չի ցուցադրվում բջջային հեռախոսում: Դա սարքին ստիպում է բեռնել և տեղադրել լրտեսական ծրագրակազմը:

“Amnesty International”-ի անվտանգության փորձագետները մի քանի, նաև այժմեական այֆոններում գտան «Պեգաս» ծրագրակազմի հետքեր, որոնք, ըստ երևույթին, այս ճանապարհով էին հասել սարք: Նրանց վերլուծության համաձայն՝ լրտեսական ծրագիրը կարող է տեղադրվել հեռակա կարգով՝ օգտագործելով ինտերնետի վրա հիմնված iMessage ծառայությունը: Դրա համար NSO-ի հաճախորդները պետք է մուտքագրեն միայն թիրախային անձի հեռախոսահամարը: Այնուհետև սմարթֆոնը ավտոմատ կերպով ստանում է տվյալներ, որոնք ներբեռնված են ինտերնետից: Այս դեպքում դա տրոյական «Պեգաս»-ն է:

31.01.2021
Իսրայելական ծրագրակազմ
Հաքերային գործիքներ գաղտնալսման համար
Ամբողջ աշխարհում քննիչները կարող են «կոտրել» սմարթֆոնները՝ նաև հեռակա կարգով:

Օգտագործել են ծրագրակազմի թույլ տեղերը

“Amnesty International”-ի անվտանգության փորձագետները չկարողացան ստուգել՝ արդյո՞ք այս մեթոդը նման ձևով է գործում Android-ի սարքերում: Կազմակերպությունը Apple-ի ուշադրությունն է հրավիրել անվտանգության պակասին: Ընկերությունն անձամբ հարցմանն ի պատասխան տեղեկացրեց, որ գրոհի այս տեսակը չի սպառնում օգտագործողների ճնշող մեծամասնությանը: Բայց ինքը, իհարկե, հետևողականորեն աշխատում է բոլոր հաճախորդների անվտանգությունն ապահովելու ուղղությամբ:

Այնուամենայնիվ, պարզ է. ամբողջ աշխարհում հակերները մշտապես փորձում են համակարգերում նոր բացթողումներ գտնել, և դրանք մասամբ մեծ գումարով վաճառում են գաղտնի ծառայություններին կամ NSO-ի նման ընկերություններին: Այս մրցավազքում ամենից շատ հետ են մնում սարքերի արտադրողները:

Տորոնտոյի համալսարանի “Citizen Lab”-ի SS հետազոտողները նայել են, թե ինչպես են աշխատում «Պեգաս»-ի նախորդ տարբերակները: Նրանք հաստատեցին, որ գործարկման համակարգերում, ինչպիսիք են iOS-ը կամ Android-ը, ծրագիրն օգտագործում է ծրագրակազմի թույլ տեղերի շղթան, այսպես կոչված՝ շահագործումները: Դրանց մեջ էին նաև հակերների համար առանձնապես օգտակար թույլ տեղերը, այսպես կոչված՝ «զրոյական օրերի շահագործումները»: Այս դեպքում խոսքը վերաբերվում է անվտանգության բացերին, որոնք գրեթե անմիջապես, նախքան արտադրողները հակաքայլեր կձեռնարկեն, օգտագործվում են գրոհների համար: Ասում են, որ NSO-տրոյականի կողմից մասամբ հաջորդաբար կիրառվել են այդպիսի երեք «զրոյական օրեր»՝ հեռախոս մուտք ունենալու համար:

Բացառիկ 26.08.2016
«Պեգաս»-ով լրտեսության SS փորձագետ
«Այստեղ ոչ մի անտեղյակ չէր աշխատում»
«Պեգաս»-ը Apple-ի մղձավանջի անունն է: Լրտեսական ծրագրակազմը խիստ փորձության է ենթարկում օգտատերերի վստահությունը:

Տարբեր ճանապարհներ դեպի սմարտֆոններ

«Պեգաս» տրոյականով սարքերը վարակելու մեկ այլ միջոց է գործում WLAN ցանցի կամ տեղական բջջային ցանցի միջոցով: Դրա համար բջջային հեռախոսը պետք է մուտք գործի մանիպուլացված կայմ կամ երթուղիչ: Օրինակ՝ NSO ընկերությունը վաճառում է սարքեր, որոնք հավակնում են լինել բջջային կայմ՝ IMSI-Catcher: Դրանց ազդանշանն ավելի ուժեղ է, քան բոլոր հարակից կայմերինը, որի հետևանքով բջջային հեռախոսը կապվում է դրան: Այսպիսով, հարձակվողը միանում է, այսպես ասած, բջջային հեռախոսի և իսկական կայմի արանքում: Երբ այնուհետև օգտագործողը կայք է կանչում, ինչպես, օրինակ, Google-ի էջը, տվյալների հոսանքի ուղղությունը վայրկյանների ընթացքում փոխվում է դեպի NSO-ի սերվերներ: Վերահսկման ծրագրակազմը ցանցի միջոցով վերբեռնվում է բջջային հեռախոս:

Մեկ անգամ բջջային հեռախոսում տեղադրելով՝ «Պեգասը» միայն հսկողության միջոցառումներ չէ, որ կարող է իրականացնել կամ որոնել պահպանված տվյալներ: Հայտնապես ծրագրակազմը նաև ի վիճակի է ճնշել արտադրողի կողմից անվտանգության կարևոր թարմացումները, որոնցով, օրինակ, գործառնական համակարգում թույլ կետերը կարող են փակվել: Այսպես տրոյականը վստահեցնում է, որ կարող է երկար ժամանակ աշխատել բջջային հեռախոսի վրա:

Արտադրողը նշում է, որ իր տեխնոլոգիան վաճառում է միայն ստուգված պետական մարմիններին, և այն էլ՝ բացառապես ահաբեկչության և հանցավորության դեմ պայքարի նպատակով: Ինչպես հայտնում է NSO-ն, դրա համար «օրավուր» ծրագրակազմն օգտագործվում է ամբողջ աշխարհում, որ իրենք «կյանքեր փրկող առաքելություն» են իրականացնում:

Այս տեքստի հետազոտությանը մասնակցել է Հաննես Մունցինգերը:

Հրապարակվել է https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-smartphone-101.html կայքում