

Ծրագրային դիվերսիա

Ինչպես սթաքսնետը (stuxnet) խափանեց Իրանի ուրանի հարստացման գործընթացը

1. Վնասակար համակարգչային ծրագիր, ենթադրաբար մուտք է գործել համակարգչային համակարգ, որը սովորաբար կտրված է արտաքին աշխարհից՝ Նաթանզում ուրանի հարստացման հաստատություն, շարժական USB հիշողության միջոցով:
2. Վիրուսը ղեկավարվել է Դանիայի և Մալայզիայի սերվերներից երկու համացանցի հասցեների կողմից, որոնցից երկուսն էլ գրանցված են եղել կեղծ անուններով: Այս վիրուսը վարակել է աշխարհում 100,000 համակարգիչներ:
3. Ստաքսնետը տարածվում է համակարգի միջոցով մինչև այն գտնվում է Սլեմենս (Slemens) Քայլ 7 վերահսկողության ծրագրակազմ ունեցող համակարգիչներ, որոնք պատասխանատու են կարգավորելու ցենտրիֆուգայի (centrigues) ռոտացիոն արագությունը:
4. Համակարգչային որդը մաշում է ցենտրիֆուգայի (centrigues) ռոտացիոն արագությունը: Սա կարող է կործանել ցենտրիֆուգան (centrigues) և վնասել ուրանի հարստացումը:
5. Ստաքսնետի հարձակումը սկսել է 2009թ.-ի հունիսին: Այս տեսանկյունից, անսարք ցենտրիֆուգաների քանակը խիստ աճում է:

Պատկերի կողքին- Իրանի ցենտրիֆուգաները ուրանի հարստացման համար

In operation- աշխատել է

Out of operation- անսարք

Feb- Փետրվար

May-Մայիս

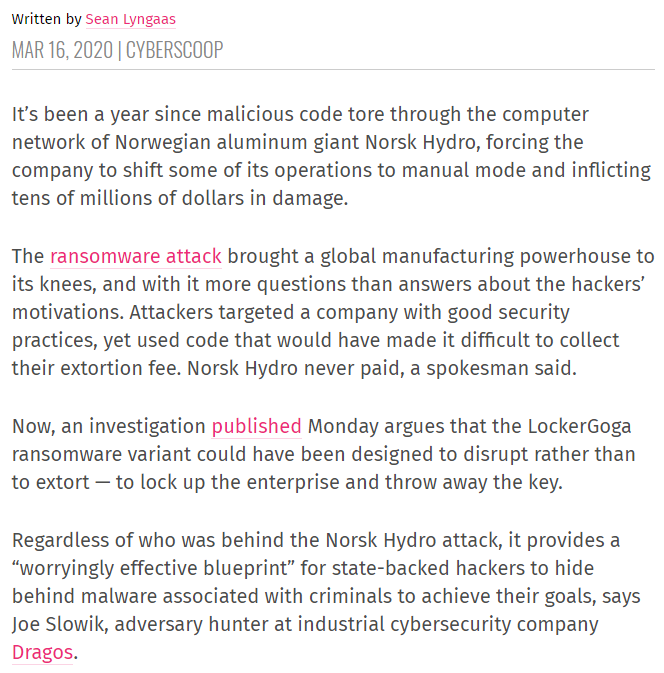
Aug-օգոստոս

Nov-Նոյեմբեր

Jan- Հունվար

Source- աղբյուր

Research-հետազոտություն



Արդեն շուրջ մեկ տարի է, ինչ վնասակար կոդը ճեղքել է Նորվեգական ալյումինի հսկայական Նորսկ հիդրոն (Norsk Hydro) համակարգչային ցանցի միջոցով` ստիպելով ընկերությանը փոխելու իր գործողություններից մի քանիսը՝ անցնելով ձեռքի ռեժիմի և պատճառելով տասնյակ միլիոնավոր դոլլարների վնաս: Շորթող վիրուսի հարձակումը բերել է համաշխարհային արտադրական էլեկտրակայանը ծնկների վրա և դրանով շատ ավելի հարցերի, քան պատասխանների՝ հակերների դրդապատճառի վերաբերյալ: Հարձակվողները թիրախավորել են լավ անվտանգության փորձ ունեցող ընկերությանը՝ օգտագործելով կոդ, որն անհնար կդարձներ հավաքելու իրենց գումարները: Նորսկ հիդրոն (Norsk Hydro) երբեք չվճարեց, ասել է խոսնակը:

Այժմ հետաքննիչը հրատարակել է, որ Monday-ն վիճարկում է, որ LockerGaga շորթող վիրուսի տեսակը կարող է նախագծված լինի խանգարելու, այլ ոչ կորզելու- փակելու ձեռնարկությունը և դեն նետելու բանալին:

Անկախ նրանից, թե ով էր կանգնած Norsk Hydro հարձակման ետևում, այն տրամադրում է «անհանգստացնող արդյունավետ նախագիծ» պետության աջակցություն ունեցող հակերների համար թաքնվելու վնասակար ծրագրերի ետևում, որն ասոցացվում է հանցագործների հետ՝ իրենց նպատակներին հասնելու համար, ասում է՝ Ջո Սլոուիկը, Դրագոս արդյունաբերական կիբեր անվտանգության ընկերության խորհրդատվական որսորդ: