HSBCnet
Malware Համակարգչային վնասակար ծրագիր

Ռիսկեր ձեր բիզնեսի համար.

- Տվյալների կորուստ
- ֆինանսական կորուստ
- Սարքավորումների վնաս
- Բիզնես գործունեության կաթվածահարում

Վնասակար համակարգչային ծրագիրը կոդավորված է՝ նպատակ ունենալով վնասելու իր թիրախին: Վնասելով մասնավոր և կորպորատիվ օգտատերերին՝ այն կարող է գողանալ տեղեկատվություն, վնասել տվյալներ, յուրացնել վեբ կայքի այցելությունների վերաբերյալ տեղեկատվություն և լրտեսել ինտերնետային գործունեությունը: Ինտերնետային բանկային ծառայության օգտատերերի ապօրինի վերաուղղորդումը դարձել է հաճախակի հանդիպող զեղծարարության ձև:

Ի՞նչ է համակարգչային վնասակար ծրագիրը
Համակարգչային վնասակար ծրագրերը կարող են թաքնվել բնականոն աշխատող ծրագրում (տրոյաններ) կամ տարածվել սարքերի միջև՝ առանց օգտատերի միջամտության (վորմս): Դրանք կարող են հատուկ ձևավորված լինել՝ շրջանցելու պաշտպանություն և կատարելու հատուկ առաջադրանքներ:

Մեկ անգամ անզգուշորեն ներդրվելուց հետո վնասակար ծրագիրը կարող է անտեսանելի բազմաթիվ գործողություններ կատարել: Այն կարող է լրտեսել վեբ կայքերի այցեր, ոչնչացնել տվյալներ կամ գուշակել գաղտնաբառեր: Հաճախակի դրանք օգտագործվում են հանցագործների կողմից՝ բիզնեսի կարևոր տեղեկատվության գաղտնագրման համար՝ ստիպելով կազմակերպությանը վճարել «փրկագին»: Ինտերնետային բանկային ծառայության օգտատերերը կարող են վերաուղղորդվել նաև դեպի կեղծ կայքեր, որտեղ գրանցվում են նրանց մուտքի տվյալները՝ ֆինանսական գողություն կատարելու նպատակով:

Վնասակար ծրագիրը սովորաբար ներբեռնվում է էլեկտրոնային նամակների միջոցով (ֆիշինգ), կամ կեղծ հղումներով: Վնասակար ծրագրերը և USB կրիչները կարող են նաև վնասել սմարթֆոններին և համակարգիչներին:

Վնասակար ծրագիրը կարող է ամիսներ շարունակ թաքնված մնալ մինչ ակտիվացումը:

Բիզնեսի անվտանգության խախտումների
համակարգչային վիրուսների, լրտեսող և վնասակար ծրագրերի հետևանք են:

68%-ը

Sources: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016; http://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics

Վնասակար ծրագրերի օրինակներ են՝

համակարգչային լրտեսումը
վիրուս-փրկագինը
տրոյանը
ստեղնաշարային վիրուսը

HSBC

Հակավիրուսային Թեստ Իսնտիտուտը

ամեն օր գրանցում

է 390,000

համակարգչային վնասակար ծրագրեր:

Sources: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016; http://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics

Ինչպես պաշտպանել ձեր բիզնեսը.

Ձեղծարարությունը կարող է ավելի համոզիչ թվալ, եթե զեղծարարները տեղեկատվություն ունենան ընկերության ղեկավարների և ֆինանսական դեպարտամենտի աշխատակիցների մասին, օրինակ՝ ընկերության կայքից:

- Կիրառեք ուժեղ արձագանքման, վերականգնման և պահուստային կրկնօրինակման գործընթացներ:
- Պարբերաբար, պլանավորված հիմունքներով գործարկեք արդի հակավիրուսային ծրագրեր Ձեր կազմակերպության բոլոր սարքերի վրա: Հաճախակի հակավիրուսային սկանավորումը կօգնի նվազագույնի հասցնել վնասակար հարձակումների ռիսկը:
- Ձեր համակարգիչները համապատասխանեցրեք ժամանակակից պահանջներին, սերվերները և փոխկապակցված սարքերը՝ հասանելի դառնալուն պես տեղադրելով անվտանգության արդի ծրագրերը:
- Համոզվեք, որ ձեր Ձեր անձնակազմը խուսափում է կասկածելի կայքերից, և չի ներբեռնում անվճար ծրագրեր/ հավելվածներ, չի գործարկում MS Office մակրոներն էլեկտրոնային փոստի հավելվածների վրա կամ օգտագործում USB քարտեր չստուգված աղբյուրներից:
- Կիրառեք հավելվածների whitelisting-ը (արգելափակելով ցանկացած համակարգչային ծրագիր, որը նախապես լիազորված չէ):
- Օգտագործեք տարբեր գաղտնաբառեր տարբեր բիզնես մուտքերի համար:

Եթե կասկածում եք, որ դուք դարձել եք զեղծարարության զոհ, դիմեք HSBC Ձեր ներկայացուցչին: