Следчы камітэт Рэспублікі Беларусь звяртае ўвагу на з'яўленне і распаўсюджванне новага спосабу махлярства ў сетцы Інтэрнэт

Аналіз крымінагеннай абстаноўкі і практыкі дзейнасці следчых падраздзяленняў сведчыць аб з'яўленні і распаўсюджванні на тэрыторыі рэспублікі новага спосабу махлярства.

Механізм яго здзяйснення складаецца ў падмене банкаўскіх рэквізітаў замежных контрагентаў (Італія, КНР, Польшча, ПАР і іншыя) пры ажыццяўленні аплаты за пастаўку тавараў.

Так, пасля ўзгаднення істотных умоў кантракту з замежным партнёрам, а ў асобных выпадках і яго падпісання на электронную пошту арганізацыі (прадпрыемства) зламыснікамі накіроўваецца паведамленне нібыта ад імя супрацоўніка замежнага контрагента аб змене рэквізітаў абслуговага банка і неабходнасці пералічэння грашовых сродкаў на новы рахунак (напрыклад, па прычыне выплаты значнага падатку ў мінулым банку, перавышэння ліміту на рахунку, правядзення ў дачыненні да прадпрыемства дзяржаўнага аўдыту).

Пры гэтым адрас электроннай пошты махляроў мае істотнае падабенства з рэальным, што часцяком застаецца незаўважаным (напрыклад, e***@chainlon-com.pw замест e***@chainlon.com.tw). Наступная перапіска ужо ажыццяўляецца з кіберзлачынцамі.

Рэалізацыя падобнай схемы крадзяжу магчымая з дапамогай атрымання несанкцыянаванага доступу да электроннай пошты аднаго з бакоў здзелкі. У гэтай сувязі зламыснікі валодаюць інфармацыяй аб прадмеце, умовах дагавора і могуць весці перапіску, не выклікаючы падазрэнняў (у выпадку неабходнасці імі накіроўваюцца дадатковае пагадненне, рахунак-праформа (инвойс) са зменены мі рэквізітамі банкаўскага рахунку і кантактнымі данымі прадстаўнікоў фірмы шляхам іх « накладання » на падрыхтаваныя раней і захаваныя ў паведамленнях дакументы). Пры гэтым лісты рэальнага контрагента аўтаматычна перанакіроўваюцца ў папку «Спам ».

Акрамя таго, маюцца адваротныя выпадкі, калі ад імя беларускіх суб'ектаў гаспадарання шляхам кампраметацыі іх карпаратыўнай пошты на адрас замежных партнёраў таксама накіроўваліся лісты, рахункі-праформы са зменены мі банкаўскімі рэквізітамі. У выніку грашовыя сродкі, належачыя беларускім прадпрыемствам за выраблену (пастаўленую) прадукцыю, пераводзіліся на рахункі махляроў.

Неабходна адзначыць, што ў рамках расследавання названай катэгорыі крымінальных спраў устаноўлены факты выкарыстання супрацоўнікамі суб'ектаў гаспадарання карпаратыўнай пошты на хатніх камп’ютарах, пры рэгістрацыі ў сацыяльных сетках, асабістай электроннай пошты ў службовых мэтах, а таксама невыкананнем нават мінімальных патрабаванняў да яе абароны (адсутнасць рэзервовага адрасу электроннай пошты, прывязкі да нумара мабільнага тэлефона, ўстаноўкі пароля, які можа быць падабраны адмысловым праграмным забеспячэннем на працягу адной секунды). У шэрагу арганізацый доступ да электроннай пошты мела значная колькасць работнікаў, не звязаных з працэдурай закупкі таварна-матэрыяльных каштоўнасцяў, яго выкарыстанне ажыццяўлялася адначасова з некалькіх

камп’ютараў, а для ўваходу не патрабавалася ўвядзенне пароля (аўтаматычнае захаванне ў браўзэры).

У якасці мер, накіраваных на папярэджанне названых ашуканскіх дзеянняў, могуць разглядацца наступныя:

выключэнне ў дзейнасці арганізацый выкарыстання бясплатных паштовых сэрвісаў, а таксама прыняцце дадатковых мер аховы карпаратыўнай электроннай пошты (падключэнне двухфакторнай аўтэнтыфікацыі, выкананне патрабаванняў да складанасці пароля і перыядычнасці яго змены, антывіруснае праграмнае забеспячэнне);

пастаянны маніторынг карпаратыўнай электроннай пошты адміністратарам на прадмет несанкцыянаванага доступу (праверка гісторыі уваходаў у акаўнт, IP-адрасоў доступаў, настроек пераадрасацыі);

абмежаванне і кантроль доступу да камп’ютара і электроннай пошты, якія выкарыстоўваюцца пры вядзенні дзелавой перапіскі з замежнымі контрагентамі;

праверка правільнасці адрасу электроннай пошты контрагента пры атрыманні і адпраўцы паведамленняў, а таксама падтрыманне кантакту з яго прадстаўніком і ўзгадненне ключавых пытанняў дадаткова пры дапамозе іншых сродкаў сувязі (тэлефонных перамоваў, выкарыстання факсімільнай сувязі, мессенджэраў);

правядзенне навучальных заняткаў з супрацоўнікамі па бяспечнай працы ў сетцы інтэрнэт і выкарыстанні электроннай пошты.
