БЫЦЬ ПІЛЬНЫМІ ЗАЎСЁДЫ

(Заканчэнне. Пачатак на 1-й стар.)

Асноўным застаецца вішынг — званкі патэнцыяльным пацярпелым ад прадстаўнікоў альбо банкаўскіх устаноў, альбо ад імя супрацоўнікаў праваахоўных органаў. Што характэрна гэтаму віду злачынстваў? У ходзе размовы на патэнцыяльнага пацярпелага ўздзейнічаюць, каб ён у самы кароткі час здзейсніў нейкае няправільнае дзеянне, прыняў няправільнае рашэнне: перадаў трэцяй асобе рэквізіт доступу ад свайго мабільнага банкінгу, усталяваў дадатак аддаленага доступу на мабільную прыладу і гэтак далей.

«Вопыт процідзеяння фроду паказвае, што ашуканцы пастаянна адсочваюць меры, якія прымаюцца ў дачыненні да іх, і вынаходзяць новыя спосабы супрацьпраўных дзеянняў. Таму кожны з карыстальнікаў паслуг электрасувязі павінен клапаціцца пра сваю бяспеку і праяўляць пільнасць».

Падстаў для такіх дзеянняў таксама можа быць шмат: гэта і падазроная актыўнасць на банкаўскім рахунку, здзяйсненне пераводу грошай у адрас невядомай асобы і нібыта афармленне крэдыту з выкарыстаннем пашпартных даных патэнцыяльнага пацярпелага. «Даходзіць да таго, што пад такім эмацыянальным уздзеяннем некаторыя пацярпелыя нават прадаюць маёмасць, якая ёсць у іх дома, і нават нерухомасць. У гэтым выпадку неабходна памятаць, што ніколі супрацоўнікі міліцыі, іншых праваахоўных органаў, банкаўскіх устаноў не будуць тэлефанаваць на мабільныя тэлефоны, тым больш на месенджары, і ўдакладняць нейкую інфармацыю, звязаную з грашыма і банкаўскімі рахункамі», — распавёў Дзмітрый Стасюлевіч.

Ён адзначыў, што вяртаецца такі спосаб здзяйснення злачынстваў, як «Алё, мама!». Рэгіструюцца нячаста, але ўсё ж такі такія злачынствы ёсць. Гэта званкі патэнцыяльным пацярпелым ад свайго, якія нібыта трапілі ў дарожна-транспартнае здарэнне. Пры гэтым неабходна перадаць грошы менавіта кур'еру для вырашэння таго ці іншага пытання.

Дэкларавання праз... кур'ера

Таксама ў канцы мінулага года пачалі рэгістравацца злачынствы, падставай у якіх гучыць неабходнасць задэкларавать усе грашовыя сродкі, якія маюцца дома. Потым прапануецца перадаць іх так званаму кур'еру, супрацоўніку праваахоўных органаў або прыйсці ў банкаўскую ўстанову і пакласці іх на рахунак для таго, каб было відаць, якая колькасць грашовых сродкаў ёсць, нібыта каб іх не выкралі. Аднак трэба разумець, што самамэта ў зламыснікаў заўсёды адна — гэта выкраданне грошай. У ведамстве нагадалі, што супрацоўнікі міліцыі не маюць зносіны з людзьмі ў месенджарах, а таксама не дасылаюць туды фота сваіх пасведчанняў.

«Актуальнай праблемай застаюцца і фішынгавыя спасылкі. Гэта спасылкі на падробленыя сайты, якія па сваім знешнім інтэрфейсе нагадваюць легітымны сайт, як правіла, банкаўскай установы, Белпошты, службы дастаўкі і гэтак далей», — праінфармаваў начальнік упраўлення.

Фішынгавая спасылка можа з'явіцца ў якасці рэкламнай пры выкарыстанні аднаго з інтэрнэт-пошукавікаў. Яе можна атрымаць і ў асабістай перапісцы са зламыснікам, напрыклад, пры продажы якога-небудзь тавару, дапусцім, у сацыяльных сетках. У гэтых выпадках праваахоўнікі рэкамендуюць звяртаць увагу на даменнае імя наведвальнага сайта.

Пакупнікі таннай «халявы»

Начальнік упраўлення па супрацьдзеянні кіберзлачыннасці адзначыў, што застаюцца праблемай у нас гандлёвыя пляцоўкі, на якіх купляюць і прадаюць тавары. Некаторыя людзі, зацікавіўшыся нізкай цаной тавараў, даюць невядомым перадаплату, чакаючы, што праз 2—3 тыдні гэты тавар усё ж такі прыйдзе, але ён не прыходзіць. «Рэкамендацыя: не набываць тавары з якой-небудзь перадаплатай і дастаўкай. Можна купіць тавар, аплаціўшы яго пры атрыманні, гэта засцеражэ вас і вашы грошы», — раіць Дзмітрый Стасюлевіч.

«Белтэлекам» працуе толькі з сігнальным трафікам, змест размоў спецыялістам недаступны, таму дакладна ўстанавіць, ці здзяйсняецца выклік ашуканцамі, мы не можам».

На яшчэ адзін від махлярства трапляюцца ахвотныя хутка разбагацець. «Часта ў апошні час выкарыстоўваюцца сайты, якія ўяўляюць сабой нібыта крыптабіржы і біржы ў цэлым. Звязваючыся з пацярпелымі, ашуканцы абяцаюць вельмі вялікі прыбытак. Для гэтага неабходна толькі перавадзіць грошы і папаўняць рахунак. Пры гэтым за кожным пацярпелым замацоўваецца так званы менеджар, які будзе падказваць, як гандляваць і што рабіць. Аднак усё гэта, зразумелая справа, у выніку аказваецца выкрутам махляроў.

Людзі губляюць усе грошы, бо перавадзяць іх не ў нейкі асабісты кабінет на рахунак біржы. Часам зламыснікі пераконваюць пацярпелых ва ўзнікненні цяжкасцяў з пералічэннем грошай, вырашыць якія можна, яшчэ раз папоўніўшы рахунак. Для гэтага некаторыя пацярпелыя нават бралі крэдыты», — праінфармаваў начальнік упраўлення.

Яшчэ адзін распаўсюджаны від махлярства — званкі ад нібыта супрацоўнікаў праваахоўных органаў і просьбы ад іх прыняць удзел у спецаперацыі па выяўленні зламыснікаў у банкаўскай сферы. «У гэтых выпадках людзей вымушаюць у тым ліку браць крэдыты. Гэта адзін з прыкладаў. На самай справе спосабы мяняюцца пастаянна.

Чаму не заўсёды можна вылічыць махляроў?

Як паведаміў **начальнік сектара аналізу і кантролю трафіку службы бяспекі «Белтэлекама» Павел ДАВІДОВІЧ,** іх спецыялісты штодня сутыкаюцца з рознымі відамі супрацьпраўнай дзейнасці і актыўна змагаюцца з махлярствам. Супрацьзаконныя дзеянні ў сетках электрасувязі з мэтай атрымання нелегальнага даходу можна падзяліць на два віды. Гэта здзяйсненне аперацый, якія парушаюць устаноўлены парадак пропуску трафіку, і выкарыстанне паслуг «Белтэлекама» для атрымання асабістай інфармацыі карыстальнікаў, напрыклад лагінаў, пароляў, рэквізітаў банкаўскіх картак або матэрыяльных сродкаў, зразумела, падманным шляхам.

З першым выглядам махлярства людзі сутыкаюцца, калі міжнародны выклік паступае ад нібыта знаёмага чалавека, але з невядомага або замежнага нумара альбо калі ў непрацоўны час абанент атрымлівае вялікую колькасць званкоў ад якой-небудзь дзяржаўнай арганізацыі. Другі від махлярства на дадзены момант уяўляе найбольшую пагрозу. Грамадзян падманваюць з дапамогай SMS або электронных паштовых паведамленняў са спасылкамі на шкоднасныя (фэйкавыя) інтэрнэт-рэсурсы або званкоў, як тэлефонных, так і ў месенджарах Viber, WhatsApp і іншых.

Сапраўдныя крыніцы свайго падключэння да сеткі агульнага карыстання аферысты хаваюць. Гэта значыць, IP-адрасы, акаўнты, нумары тэлефонаў, якія бачыць чалавек на прыладзе, рознымі спосабамі падмяняюцца на іншыя, якія не належаць злачынцам.

— Для процідзеяння гэтаму віду махлярства спецыялісты «Белтэлекама» ў рамках дадзеных ім правоў праводзяць аналіз сігнальнага тэлефоннага трафіку і выяўляюць тэлефонныя выклікі, якія могуць з'яўляцца ашуканскімі. Падкрэслю, што «Белтэлекам» працуе толькі з сігнальным трафікам, змест размоў спецыялістам недаступны, таму дакладна ўстанавіць, ці здзяйсняецца выклік ашуканцамі, мы не можам, — паведаміў Павел Давідовіч.

Аналіз статыстыкі парадку праходжання ашуканскіх тэлефонных выклікаў паказвае, што ўсе яны паступаюць з-за мяжы, з нумароў, якія належаць замежным аператарам сувязі, устанавіць якія па наяўнай у сетцы «Белтэлекама» інфармацыі тэхнічна немагчыма. На падставе атрыманых звестак работнікі кампаніі прыходзяць да наступнай высновы: першапачаткова ашуканцы не валодаюць поўнай інфармацыяй аб абаненце, якому яны тэлефануюць. Злачынцы ажыццяўляюць веерны абзвон тэлефонных нумароў пэўнага рэгіёна краіны ў аўтаматычным рэжыме (напрыклад з дапамогай ботаў), затым — адрасны, гэта значыць, звязваюцца з тымі людзьмі, якія ў гэты час, цалкам магчыма, знаходзяцца дома і здымуць трубку.

Многія абаненты самі перарываюць тэлефонную размову, паколькі вылічаюць махляра, частка з іх паведамляе аб выкліку ў праваахоўныя органы або ў службу тэхнічнай падтрымкі. Астатніх карыстальнікаў аферыстам атрымліваецца падмануць.

— Наш вопыт процідзеяння фроду паказвае, што ашуканцы пастаянна адсочваюць меры, якія прымаюцца ў дачыненні да іх, і вынаходзяць новыя спосабы супрацьпраўных дзеянняў. Таму кожны з карыстальнікаў паслуг электрасувязі павінен клапаціцца пра сваю бяспеку і праяўляць пільнасць, — адзначыў спецыяліст. Улічваючы маштабы праблемы, работнікі «Белтэлекама» працуюць над яе ліквідацыяй ва ўзаемадзеянні з іншымі беларускімі і замежнымі аператарамі сувязі, праваахоўнымі органамі і міжнароднымі арганізацыямі.

РУП «Белпошта» яшчэ раз нагадвае, што азнаёміцца з інфармацыяй аб аказанні паслуг паштовай сувязі можна на афіцыяльным сайце belpost.by. У выпадку ўзнікнення праблемных пытанняў звяртайцеся ў кантакт-цэнтр прадпрыемства па нумары 154.

Рэкамендацыі для абанентаў:

— Сачыце за станам інфармацыйнай бяспекі гаджэтаў, сродкаў вылічальнай тэхнікі і іншага праграмна-тэхнічнага забеспячэння, у тым ліку офісных аўтаматычных тэлефонных станцый.

— Не пераходзьце па спасылках з SMS або электронных лістоў, паведамленняў месенджараў, калі вы іх не запытвалі.

— Не спампоўвайце праграмныя дадаткі з неправерaных крыніц, нават калі ў якасці адпраўніка паказаны вядомы вам кантакт (яго маглі ўзламаць).

— Не паведамляйце нікому па тэлефоне персанальныя даныя, уключаючы рэквізіты банкаўскіх картак, коды аўтарызацыі і гэтак далей.

— Не ператэлефаноўвайце, калі высвечваецца неадказны выклік. Вас могуць перанакіраваць на іншы нумар прэміум-класа, і чым даўжэй вы застаняцеся на лініі, тым больш адчувальным апынецца ўдар па кашальку.

— Калі вам паступае тэлефонны выклік з-за мяжы ад знаёмага абанента, але з нумара, які яму не належыць, то неабходна паведаміць пра гэта чалавеку і парэкамендаваць яму звярнуцца да аператара сувязі з прычыны неналежнага аказання паслугі.

Крыптавалюта — гэта рызыка, без неабходных ведаў — двайная

Начальнік аддзела па аналізе практыкі і метадычнага забеспячэння папярэдняга расследавання УСК па горадзе Мінску Пётр МІКУЛА адзначыў, што крыптавалюта як спосаб заробку — рызыка. Гэта, па сутнасці, прадпрымальніцкая дзейнасць. Няхай яна такой не прызнаецца ў адпаведнасці з заканадаўствам, але па сваёй сутнасці гэта дзейнасць, накіраваная, як у нас напісана ў Грамадзянскім кодэксе, на атрыманне прыбытку на свой страх і рызыку. А што датычыцца захоўвання, то, зноў жа, памятаем пра тое, што ў любы момант такая лічбавая валюта можа перастаць каштаваць наогул, упэўнены спецыяліст.

Калі мы гаворым пра самыя вядомыя і самыя дарагія крыптавалюты, такія коіны, як біткоін, этэрыум, доджкоін, гэта ўсё ж такі свайго роду прадпрымальніцкая рызыка, прычым значная. І гэта свайго роду фінансавыя піраміды, бо ўсім нам вядома, што яны валодаюць вельмі высокай ступенню валацільнасці. І зарабіць у дадзеным выпадку можна толькі на скачках курса. Але іх немагчыма спрагназаваць, імі немагчыма кіраваць, лічыць наш эксперт.

На яшчэ адзін від махлярства трапляюцца ахвотныя хутка разбагацець. «Часта ў апошні час выкарыстоўваюцца сайты, якія ўяўляюць сабой нібыта крыптабіржы і біржы ў цэлым. Звязваючыся з пацярпелымі, ашуканцы абяцаюць вельмі вялікі прыбытак. Для гэтага неабходна толькі перавадзіць грошы і папаўняць рахунак. Пры гэтым за кожным пацярпелым замацоўваецца так званы менеджар, які будзе падказваць, як гандляваць і што рабіць».

Так, ёсць пэўныя маркеры, якія сведчаць аб тым, што ў хуткім часе гэты курс можа значна павялічыцца або значна ўпасці. Але ніхто гэтым не кіруе. Таму казаць пра тое, што гэта добры спосаб зберажэння, не даводзіцца, бо, набыўшы сёння некалькі біткоінаў за тысячы долараў, заўтра яны могуць не каштаваць ужо нічога або каштаваць некалькі долараў.

Акрамя таго, існуюць незаконныя крыптаабменнікі. Яны паступаюць наступным чынам: прадаюць «крыпту» за наяўныя грошы. Гэта значыць, яны дазваляюць ашуканцам, рознага роду зламыснікам свой злачынны даход канвертаваць у крыптавалюту. А ўжо якім чынам яны далей будуць распараджацца, ніхто гэтага ніколі не даведаецца. Таму трэба разумець, што празрыстай, законнай можа быць дзейнасць толькі з легальнымі, афіцыяльнымі крыптабіржамі. Але трэба памятаць пра фішынгавыя спасылкі і старанна, уважліва правяраць тыя сайты, дзе мы ўводзім якую-небудзь плацежную інфармацыю.

І абавязкова, што датычыцца крыптабірж і крыптаабменнікоў, у кожнага з іх ёсць тысячы, дзясяткі тысяч водгукаў. Гэта абавязкова трэба правяраць, бо інакш мы можам страціць усе свае плацежныя даныя. А следам — і грошы.

Сяргей КУРКАЧ.