РЫЗЫКІ ЛІЧБАВАЙ ПРАСТОРЫ

ВІШЫНГ, ФІШЫНГ, АНЛАЙН-КРЭДЫТ

Ахвярамі інтэрнэт-злачынцаў становяцца не толькі простыя грамадзяне, але і тыя, хто мае глыбокія веды ў інфармацыйных тэхналогіях, кажа **Аляксандр ГРЫЦУК, начальнік упраўлення па супрацьдзеянні кіберзлачыннасці крымінальнай міліцыі УУС Мінаблвыканкама:**

— Адно з найбольш распаўсюджаных інтэрнэт-злачынстваў — вішынг — калі злачынцы тэлефануюць людзям, выдаюць сябе за супрацоўнікаў банкаў ці міліцыі і пад рознымі прычынамі выманьваюць у пацярпелых рэквізіты банкаўскіх рахункаў і картак. Адбываецца гэта праз айпі-тэлефанію ці месенджары: Viber і WhatsApp, у якіх можна падмяніць нумар і паставіць лагатып пазнавальных беларускіх банкаў. Называць рэквізіты не трэба, бо гэтыя звесткі і так ёсць у сапраўдных супрацоўнікаў банкаў і міліцыі.

Апошнім часам ахвярам актыўна прапануецца адкрыць крэдыт, каб з яго дапамогай нібыта пагасіць іншы, узяты на імя асобы, якой тэлефануюць. Пры гэтым чалавека запэўніваць, што робіцца гэта для таго, каб выкрыць няшчырых супрацоўнікаў банкаў.

Калі паступае такі званок, трэба спыніць размову, бо кібермахляры ўсё больш удасканальваюць майстэрства псіхалагічнага ўплыву. 90 % ахвяр адзначаюць, што ведалі пра падобную схему падману, і ўсё роўна трапіліся на вуду, падкрэсліў спецыяліст.

Падман, калі махлярская спасылка маскіруецца пад звычайную, якая нібыта вядзе на пэўны інтэрнэт-рэсурс, а насамрэч прыводзіць да махляра, атрымаў назву фішынг. У адрасе мяняецца літаральна адзін сімвал, і калі ахвяра пераходзіць па такой спасылцы і ўводзіць свае асабістыя даныя, яны трапляюць да злачынцаў.

— Найбольш часта такая схема сустракаецца на анлайн-пляцоўцы «Куфар», калі «прадавец» ці «пакупнік» прапануе ахвяры перайсці да стасункаў у інтэрнэт-месенджарах, — заўважыў Аляксандр Грыцук. — Махляр дасылае фішынгавую спасылку, якая нібыта павінна паскорыць працэс дастаўкі заказу. Ахвяра пераходзіць па ёй, указвае рэквізіты банкаўскай карткі і губляе грошы. Усе размовы весці трэба толькі на абароненай пляцоўцы, не пераходзячы па спасылках ад трэціх асоб.

(Заканчэнне. Пачатак на 1-й стар.)

ШАНТАЖ, ВЫМАГАННЕ, ПЕРАДАПЛАТА

Вельмі распаўсюджана махлярства сёння і ў сацыяльных сетках, калі прадавец патрабуе перадаплату за нейкі прадукт. Атрымаўшы грошы на электронны кашалёк ці картку, злачынца знікае з сацсеткі, часта разам са старонкай, канстатавалі эксперты.

Сацыяльныя сеткі — сапраўдная скарбонка персанальнай інфармацыі пра чалавека. Тут ёсць у тым ліку дамашні адрас, нумар тэлефона і нават дасыланыя адзін аднаму інтымныя фота. Пры гэтым людзі нячаста непакояцца аб абароне сваіх старонак і выкарыстоўваюць нескладаныя паролі. Калі акаўнт узломліваюць — усе звесткі і здымкі трапляюць да зламысніка, які пачынае шантаж.

— Гандаль бінарнымі апцыёнамі — амаль забытае, але цяпер ізноў актуальнае злачынства. Яго ахвяры вядуцца на яркую рэкламу і дзеля хуткага абагачэння наймаюць сабе лжэброкераў, якія замест грамадзян на біржы гандлююць бінарнымі апцыёнамі, — нагадаў начальнік упраўлення. — Схема ў тым, што лжэброкер гандлюе нібыта ад імя чалавека, у акаўнце якога паказваецца даволі вялікі прыбытак. Пасля махляр прапануе вывесці грошы на банкаўскую картку. Чалавек дае рэквізіты, аднак замест атрымання сумы губляе тую, што была на картцы. Другая схема — махляр раіць ахвяры адкрыць новы рахунак (ад тысячы долараў), каб перавесці «зароблены» даход у наяўнасць.

Людзі нячаста непакояцца аб абароне сваіх старонак і выкарыстоўваюць нескладаныя паролі. Калі акаўнт узломліваюць — усе звесткі і здымкі трапляюць да зламысніка, які пачынае шантаж.

Падмануты чалавек пачынае шукаць дапамогу і, здараецца, натыкаецца на лжэадвакатаў, якія працягваюць падманваць ахвяру, прапануючы адкрыць крыптакашалёк, каб яны маглі скласці іскавую заяву. І з гэтага рахунку таксама скрадваюць грошы. Перш чым спакушацца на вялікія сумы, трэба праверыць у інтэрнэце спісы лжэтрэйдынгавых кампаній ці звярнуцца на спецыялізаваны форум, параіў эксперт.

УЗЛОМ СЕРВЕРА, ПАДМЕНА Е-МЭЙЛУ

Да кіберпагроз адносяцца таксама атакі на прадпрыемствы і арганізацыі розных формаў уласнасці з мэтай зарабіць ці ў межах канкурэнтнай барацьбы. Гэта DDoS-атакі, узломліванне серверaў ці электроннай пошты, каб атрымаць аддалены доступ да файлаў кампаній. У Беларусі такія масавыя атакі на прадпрыемствы і ВНУ здарыліся напрыканцы 2020-га і пачатку 2021-га, нагадаў Аляксандр Грыцук:

— Калі зламыснік атрымлівае несанкцыянаваны доступ да файлаў і серверaў, ён шыфруе іх і патрабуе выкуп за дэшыфроўку. А калі бухгалтар арганізацыі яшчэ і не дастаў з камп'ютара банкаўскі лічбавы ключ, то кіберзлачынцы атрымліваюць доступ да фінансавых аперацый. Праз сістэму дакументаабароту яны фарміруюць ад імя прадпрыемства плацежку на пэўную суму і пераводзяць грошы на падстаўныя фірмы.

Яшчэ адзін спосаб кібермахлярства — падмена паштовай скрыні прадпрыемства, праз якую вядуцца перагаворы пра пастаўкі ці набыццё прадукцыі. Напрыканцы здзелкі, калі гаворка ідзе пра аплату, з падробленага е-мэйлу (які адрозніваецца літаральна на адзін сімвал) дасылаецца пісьмо з новымі плацежнымі рэквізітамі. Такая падмена часта застаецца незаўважанай, паколькі адрасы вельмі падобныя.

ГРУМІНГ, БУЛІНГ, СВАЦІНГ

Асобная кібернебяспека пагражае нашым дзецям, якія становяцца інтэрнэт-карыстальнікамі ў вельмі раннім узросце. У пошуках гульняў ці мульцікаў праз сецівa малыя могуць выпадкова трапіць на сайт з кантэнтам 18+. Каб абмежаваць дзяцей ад гэтага, бацькам трэба размаўляць з малымі і кантраляваць іх наведванне інтэрнэт-прасторы.

Малы можа трапіць у сітуацыю інтэрнэт-грумінгу, калі дарослы чалавек наладжвае даверлівыя стасункі з дзіцем, каб сексуальна задавальняцца, прыкідваючыся такім жа падлеткам. У выніку дзеці могуць дасылаць яму свае інтымныя фотаздымкі ці ўвогуле ўцягнуцца ў выраб порнаматэрыялаў.

Пагражае дзецям у інтэрнэце і кібербулінг — калі малога могуць цкаваць праз сацсеткі, анлайн-гульні, форумы. Робяць гэта, як правіла, знаёмыя і суседзі, якія ведаюць дзіця асабіста. Выклікае ў спецыялістаў боязь і магчымае

Кібермахляры ўсё больш удасканальваюць майстэрства псіхалагічнага ўплыву. 90 % ахвяр адзначаюць, што ведалі пра падобную схему падману, і ўсё роўна трапіліся на вуду.

аднаўленне груп смерці, накшталт сумна вядомага «сіняга кіта».

— Частыя перапады настрою дзіцяці, змена манеры выкарыстання гаджэтаў (малы можа пасярод ночы памкнуцца ў сеціва), памяншэнне колькасці сяброў у сацыяльнай сетцы, выдаленне акаўнту ўвогуле — найбольш яскравыя з'явы, якія сведчаць аб тым, што дзіця хутчэй за ўсё падвяргаецца інтэрнэт-булінгу, — акрэсліў спецыяліст. — Бацькі могуць і самі прагледзець старонкі свайго малога, выявіць, ці ёсць там абразлівыя словы.

Акрамя таго, што дзеці могуць пацярпець ад злачынцаў у інтэрнэце, іх саміх могуць уцягнуць у крымінальныя схемы. Занепакоенасць у спецыялістаў выклікае кіберзлачыннасць сярод падлеткаў, якіх спакушаюць абяцаннем лёгкіх грошай і выкарыстоўваюць у якасці закладчыкаў наркотыкаў ці асоб, якія абнаяўліваюць грошы.

Займаюцца малыя і свацінгам — заведама хлуслівым выклікам (з паведамленнем пра небяспеку) міліцыі ці аварыйных службаў на адрас іншага падлетка, з якім, магчыма, ён гуляе ў анлайн і хоча адцягнуць яго ўвагу такім чынам.

— За апошні час свацінг з забаўкі аматараў анлайн-гульняў ператварыўся ў масавую з'яву і вялікую праблему для праваахоўнікаў, — падзяліўся Аляксандр Грыцук. — Гэта дэарганізуе нармальную работу транспарту, спецслужбаў, устаноў і прадпрыемстваў, наносіць эканамічную шкоду. А паведамленне пра магчымы выбух ці падпал здольнае яшчэ і выклікаць паніку сярод насельніцтва. Між тым адказнасць для такіх «жартаўнікоў» наступае з 14 гадоў, таму вельмі важна навучыць дзіця лічбавай гігіене, а таксама прывіць яму правілы паводзін у інтэрнэце.

ПА ЛІЧБАВЫХ СЛЯДАХ...

Крымінальныя злачынствы ў сферы кіберпрасторы расследуюцца доўга. Гэта звязана з трансгранічнасцю дзейнасці крымінальных груп, фігуранты якіх часта знаходзяцца за межамі Беларусі, ахарактарызаваў сутнасць такіх спраў **Ігар ДАМАРАЦКІ, начальнік аддзела па расследаванні злачынстваў супраць інфармацыйнай бяспекі і незаконнага абароту наркотыкаў следчага ўпраўлення УСК па Мінскай вобласці:**

— Пры расследаванні падобных спраў абавязкова прысутнічае пэўная лічбавая інфармацыя: нумары тэлефонаў, электронныя пошты, кашалькі, спасылкі, якімі карысталіся зламыснікі для сваіх дзеянняў. Следчы камітэт распрацаваў аўтаматызаваную інфармацыйную сістэму «След», у якую ўносяцца ўсе выяўленыя лічбавыя сляды.

Большая частка кіберзлачынстваў адбываецца па артыкуле 212 Крымінальнага кодэкса (КК) «Крадзеж шляхам выкарыстання камп'ютарнай тэхнікі». Летась па ім было ўзбуджана звыш дзвюх тысяч спраў, а нанесеная беларусам шкода ацэнена ў больш як тры мільёны рублёў. Сёлета заведзена 577 спраў, з якіх 495 — па 212 артыкуле.

Перадаваць рэквізіты банкаўскіх картак праз інтэрнэт, аддаваць грошы на «ратаванне» сваякоў кур'ерам і верыць абяцанкам пра хуткі заробак нашых грамадзян вымушае недастатковая лічбавая адукацыя. Аднак калі ў жаданні падзарабіць чалавек перадае рэквізіты сваёй банкаўскай карткі для ўдзелу ў крымінальнай схеме, то ён становіцца саўдзельнікам злачынства. Згодна з артыкулам 222 КК, яму можа пагражаць да дзесяці гадоў зняволення.

Ірына СІДАРОК.

ШТО Ў СВЕЦЕ РОБІЦЦА

Эрдаган аб'явіў аб пачатку турэцкай ваеннай аперацыі ў Сірыі

Прэзідэнт Турцыі Рэджэп Таіп Эрдаган аб'явіў аб пачатку ваеннай аперацыі «Крыніца міру» ў Сірыі супраць тэрарыстаў, паведамляе РІА «Навіны» са спасылкай на Twitter кіраўніка дзяржавы.

Турэцкая армія нанесла авіяўдары па горадзе Рас-эль-Айн на паўночным захадзе правінцыі Хасекэ, таксама была атакавана вёска аль-Маджрафа каля горада і пазіцыі SDF у вёсках аль-Машрафа і Харбат аль-Банат.

«Нашы мэты — знішчыць тэрарыстычны калідор, які спрабуюць стварыць на нашых паўднёвых граніцах. Аперацыя «Крыніца міру» нейтралізуе тэрарыстычныя пагрозы ў адносінах да Турцыі і прывядзе да стварэння бяспечнай зоны, якая садзейнічае вяртанню сірыйскіх бежанцаў у свае дамы. Мы захаваем тэрытарыяльную цэласнасць Сірыі і вызвалім народ рэгіёна ад ціскоў тэрарыстаў», — гаворыцца ў паведамленні кіраўніка дзяржавы ў Twitter.

Затрыманы былы прэзідэнт Малдовы Ігар Дадон

Экс-прэзідэнта Малдовы Ігара Дадона затрымалі на 72 гадзіны ў рамках крымінальнай справы, распачатай па чатырох артыкулах Крымінальнага кодэкса, паведаміла прэс-сакратар генеральнай пракуратуры Мар'яна Керпек.

Антыкарупцыйная пракуратура краіны і супрацоўнікі Службы інфармацыі і бяспекі правялі вобыск у ягоным доме. Таксама праводзяцца вобыскі ў іншых месцах.

«Як толькі ў Малдове справы ідуць дрэнна, Дадона выклікаюць да пракурора, каб адцягнуць увагу насельніцтва ад надзённых праблем. Так было ў снежні мінулага года, калі тарыф на газ вырас у некалькі разоў. Цяпер, калі ў краіне новы скачок цэн, гэта хочуць паўтарыць», — пракаментаваў падзею сам экс-прэзідэнт у эфіры тэлеканала «НТБ-Малдова».

Ён дадаў, што не баіцца ніякіх мер, уцякаць з краіны не збіраецца і гатовы даць рашучы бой апанентам.

Тым часам намеснік старшыні Камітэта Дзярждумы па справах СНД Канстанцін Затулін у гутарцы з «Газетой.Ru» назваў затрыманне Ігара Дадона «палітычнымі рэпрэсіямі супраць апазіцыі» і спробай уцягнуць краіну ў падзеі ва Украіне.

ААН: рэкордныя 100 млн чалавек пакінулі дамы з-за канфліктаў па ўсім свеце

Колькасць людзей, вымушаных ратавацца ад узброеных канфліктаў, насілля, парушэнняў правоў чалавека і праследаванняў, упершыню за ўсю гісторыю назіранняў перавысіла адзнаку ў 100 млн, гэтаму таксама спрыялі баявыя дзеянні на тэрыторыі Украіны, паведамляе Euronews са спасылкай на Агенцтва ААН па справах бежанцаў.

«Гэта павінна паслужыць трывожным сігналам для вырашэння і прадухілення разбуральных канфліктаў, спынення праследаванняў і ліквідацыі асноўных прычын, якія вымушаюць нявінных людзей пакідаць свае дамы», — заявіў вярхоўны камісар ААН па справах бежанцаў Філіпа Грандзі.

Узброеныя канфлікты і крызісы ў Эфіопіі, Буркіна-Фасо, М'янме, Нігерыі, Афганістане і Конга таксама паўплывалі на рост бежанцаў. Колькасць людзей, якія пакінулі дамы, але засталіся ў межах сваіх краін, ацэньваецца ў 53,2 млн.

Раней стала вядома, што Польшча, якая прыняла рэкордную колькасць бежанцаў з Украіны, не мае ўрадавых праграм, каб падтрымліваць і рассяляць іх.