ФИШИНГ ВА УНИНГ УСУЛЛАРИ

Умид Жўрабоевич Кенжаев
Ўзбекистон Республикаси Жамоат хавфсизлиги
Университети Магистратураси тингловчиси, подполковник

Айдос Фархадович Жолдасов
Ўзбекистон Республикаси Жамоат хавфсизлиги
Университети Магистратураси тингловчиси, подполковник

АННОТАЦИЯ

Мақолада тажовузкорлар томонидан керакли маълумотларга кириш ёки фойдаланувчининг шахсий компьютерини зарарлаш учун фишингдан фойдаланиш муаммоси ўрганилади. Фишинг муаммоларини ҳисобга олсак, маълумотларнинг йўқолишида нафақат тажовузкорнинг ўзи, балки фойдаланувчининг ўзи ҳам айбдор эканлигини эслатиб ўтмаслик мумкин эмас, чунки у маълумотни ҳимоя қилишнинг барча усулларига риоя қилмаган бўлиб чиқади. Шунингдек мақолада фишер томонидан амалга оширилаётган киберҳужумлар таҳлил қилинади.

Калит сўзлар: фишинг, киберҳужум, фишинг усуллари, ахборот хавфсизлиги, интернет, кибермайдон.

ABSTRACT

The article explores the problem of phishing using hackers to gain access to the necessary information or damage the user's personal computer. Given the problems of phishing, it goes without saying that not only the attacker is to blame for the loss of data, but also the user, since it turns out that he did not follow all data protection methods. The article also analyzes cyber attacks carried out by phishers.

Keywords: phishing, cyberattack, phishing methods, information security, internet, cyberspace.

КИРИШ

Биринчи фишинг ҳужумлари ўтган асрнинг охирида пайдо бўлган ва ҳозирда, Google маълумотларига кўра, ҳар йили дунёда 12,4 миллионга яқин фойдаланувчи фишинг қурбонига айланади.

Кредит карта маълумотларига кириш имконини берувчи AOL ҳисобларининг ўғирланиши тўлов

процессорлари ва уларнинг фойдаланувчилари ҳам заиф эканлигини кўрсатди. Маълум бўлган биринчи уриниш 2001 йил июнь ойида электрон e-gold тўлов тизимига қилинган ҳужум бўлса, иккинчиси 11 сентябрь ҳужумларидан кўп ўтмай содир бўлган эди.[1]

Бу биринчи уринишлар фақат тажриба, имкониятлар синови эди. 2004 йилда эса фишинг компаниялар учун энг катта хавфга айланди ва ўшандан бери у доимий равишда ривожланиб, ўз салоҳиятини ошириб келмоқда. [2]

Анъанавий фишинг усуллари аста-секин ўтмишга айланиб бораётган бўлса-да, бу турдаги фирибгарлик ҳали ҳам жисмоний шахслар ва компаниялар учун жиддий хавф туғдиради.

АДАБИЁТЛАР ТАҲЛИЛИ ВА МЕТОДОЛОГИЯ

Фишинг (фишинг, яъни инглиз тилидаги балиқ овлаш сўзидан олинган бўлиб) - Интернетдаги фирибгарликнинг бир тури, унинг мақсади фойдаланувчи идентификация маълумотларини (банк карталари, ҳисоблар учун логин ва пароллар) олишдир.

Кўпинча фишинг - бу таниқли брендлар, банклар, тўлов тизимлари, почта хизматлари, ижтимоий тармоқлар номидан хатлар ва билдиришномаларни оммавий юбориш. Бундай хатлар, қоида тариқасида, логотип, хабар ва ташқи томондан ҳақиқийдан фарқ қилмайдиган сайтга тўғридан-тўғри ҳаволани ўз ичига олади. Ҳаволани босиш орқали сиз "хизмат" веб-сайтига ўтишингиз ва турли баҳоналар билан тегишли шаклларга махфий маълумотларни киритишингиз керак. Натижада фирибгарлар фойдаланувчи ҳисоблари ва банк ҳисобларига кириш ҳуқуқига ега бўладилар.

Фишинг 1996 йилда Usenet тармоғида alt.online-service.America-Online янгиликлар гуруҳида яратилган. Фишерлар ҳақида биринчи эслатма AOL медиа компанияси билан боғлиқ бўлиб, фирибгарлар ўзларини AOL ходимлари сифатида кўрсатиб, тезкор хабар алмашиш дастурлари орқали фойдаланувчилар билан боғланишган ва компания ходимлари номидан ҳисоб паролларини сўрашган. Ҳисобга кириш ҳуқуқига эга бўлгач, у спам юбориш учун ишлатилган.

2000-йилларнинг бошида фишинг тўлов тизимларига тарқалди ва 2006 йилда MySpace ижтимоий тармоғи фойдаланувчилари фишинг ҳужумига учради, бунинг натижасида рўйхатга олиш маълумотлари ўғирланди.

Фишинг ҳужумлари ҳам жисмоний, ҳам алоҳида компанияларни нишонга олиши мумкин. Фирибгарлар томонидан жисмоний шахсларга уюштирилган

ҳужумларнинг мақсади, қоида тариқасида, банк хизматлари, тўлов тизимлари, турли провайдерлар, ижтимоий тармоқлар ёки почта хизматлари фойдаланувчиларининг логинлари, пароллари ва ҳисоб рақамларига кириш ҳуқуқига эга бўлишдир. Бундан ташқари, фишинг ҳужумининг мақсади қурбоннинг компьютерига зарарли дастурларни ўрнатиш бўлиши мумкин.

Ҳамма фишерлар ўзлари кириш ҳуқуқига эга бўлган ҳисобларни пулга ўтказа олмайди. Ҳисоб-китобларни нақд қилиш амалий нуқтаи назардан қийин жараёндир. Қолаверса, нақд пул берган шахсни қўлга олиш ва жиноий гуруҳни жавобгарликка тортиш осонроқ. Шунинг учун, махфий маълумотларни олган баъзи фишерлар уни бошқа фирибгарларга ҳисоб варақлардан пул олишнинг яхши ўрнатилган схемаларидан фойдаланган ҳолда сотишади.

Фишинг ҳужумлари компанияларга қаратилган ҳолларда, кибержиноятчиларнинг мақсади баъзи бир ходимнинг ҳисоб маълумотларини олиш ва кейин компанияга ҳужумни кенгайтиришдир.

Фишингнинг асосий усуллари қуйидагилардан иборат:

Ижтимоий муҳандислик усули. Машҳур компанияларнинг вакиллари сифатида ўзини тутган фишерлар кўпинча олувчиларга ҳар қандай сабабга кўра шахсий маълумотларни зудлик билан ўтказишлари ёки янгилашлари кераклиги ҳақида хабар беришади. Бундай талаб маълумотларнинг йўқолиши, тизимнинг бузилиши ёки бошқа сабабларга кўра юзага келади. Инсон ҳар доим у учун муҳим воқеаларга муносабат билдиради. Фишинг ташкилотчилари фойдаланувчини огоҳлантириб, унинг дарҳол реакциясини қўзғатишга ҳаракат қилади. Мисол учун, "ҳисобингизга киришни тиклаш учун ..." сарлавҳали электрон почта эътиборни жалб қилиш ва одамни батафсил маълумот олиш учун ҳаволага киришга мажбур қилиш учун ҳисобланади.

Алдаш билан фишинг усули. Бу фишинг ҳужумининг энг кенг тарқалган тури. Ушбу усул ёрдамида тузилган хабарлар билан фирибгарлар бир неча соат ичида миллионлаб электрон почта манзилларига спам юбориши мумкин. Бундай ҳолда, фишер ташкилот номидан сохта электрон почта хабарини юбориб, ҳаволага риоя қилишни ва ҳисоб маълумотларини текширишни сўрайди.

Шахсий маълумотларни ўғирлаш учун ҳақиқий сайт доменига имкон қадар ўхшаш доменда жойлаштирилган махсус фишинг сайтлари яратилади. Бунинг учун фишерлар кичик матбаа хатолари ёки субдоменлари бўлган URL манзилларидан фойдаланиши мумкин. Фишинг сайти шунга ўхшаш дизайнда яратилган ва унга кирган фойдаланувчида шубҳа уйғотмаслиги керак.

Шуни таъкидлаш керакки, алдамчи фишинг фишерлар ишининг энг анъанавий усули ва шу билан бирга ҳужумлар ташкилотчилари учун энг кам хавфсиз ҳисобланади, шунинг учун сўнгги йилларда у аста-секин ўтмишга айланиб бормоқда.

“Гарпун фишинг” усули. "Гарпун" фишинг объектлари кенг фойдаланувчилар гуруҳлари эмас, балки аниқ одамлардир. Кўпинча, бу усул компаниянинг ҳимоясини енгиб ўтиш ва унга мақсадли ҳужум қилиш учун биринчи қадамдир. Бундай ҳолларда ҳужумчилар ижтимоий тармоқлар ва бошқа хизматлардан фойдаланган ҳолда ўз қурбонларини ўрганадилар ва шу тариқа хабарларни мослаштирадилар ва ишончлироқ ҳаракат қилишади.

"Кит овлаш" усули. Топ-менеджерлар ва бошқа муҳим шахсларнинг махфий маълумотларини овлаш "кит ови" деб аталади. Бундай ҳолда, фишерлар ҳисоб маълумотларини ўғирлаш учун тўғри вақт ва воситаларни топиш учун мақсадли қурбоннинг шахсий хусусиятларини аниқлашга кўп вақт сарфлашади.

Вирусларни юбориш усули. Шахс маълумотларни ўғирлашдан ташқари, фирибгарлар жисмоний шахсларга ёки шахслар гуруҳига зарар етказишни ҳам мақсад қилган. Фишинг электрон почтасидаги ҳавола босилганда, компъютерга зарарли вирусни юклаб олиш мумкин: кейлоггер, троян ёки жосуслик дастури.

Фарминг (деҳқончилик) усули. Бу фишингнинг янги тури. Ушбу усулдан фойдаланган ҳолда, фишерлар шахсий маълумотларни хат ва ҳавола орқали эмас, балки тўғридан-тўғри расмий веб-сайтда оладилар. Фармерлар DNS-сервердаги расмий сайтнинг рақамли манзилини сохта сайт манзилига ўзгартирадилар ва бунинг натижасида бехабар фойдаланувчи сохта сайтга йўналтирилади. Бундай фишинг анъанавий фишингга қараганда хавфлироқдир, чунки алмаштиришни кўришнинг иложи йўқ. Ebay аукциони, PayPal тўлов тизими ва таниқли жаҳон банклари аллақачон бундай ҳужумлардан азият чекмоқда.

Вишинг усули. Вишинг - маълумот олиш учун телефон алоқасидан фойдаланадиган фишинг усулидир. Хабарнома хатида "муаммо пайдо бўлган"ни ҳал қилиш учун қайта қўнғироқ қилиш учун телефон рақами кўрсатилган бўлади. Кейин, суҳбат давомида оператор ёки жавоб бериш машинаси фойдаланувчидан муаммони ҳал қилиш учун идентификация маълумотларини номлашни сўрайди.

Барча киберҳужумларнинг 91 фоизи фишинг электрон почта хабарлари бўлса, киберҳужумларнинг 70 фоизи фишинг ва хакерлик комбинациясидан фойдаланади.[3]

Умуман фишинг ҳақида 2011-2012-йиллардан бери бутун дунёда жиддий гапирилмоқда, бу ахборот хавфсизлиги компанияларининг оммавий ҳисоботларида акс эттирилган. [4]

Фишингдан қандай ҳимояланиш керак ? Бу соҳадаги ишларнинг бошланганига ҳали кўп вақт бўлгани йўқ.

2004-йил 26-январда АҚШ Федерал Савдо Комиссияси фишингда гумон қилинган шахсга қарши биринчи судга мурожаат қилди. Калифорниялик ўсмир судланувчига AOL сайтига ўхшаш веб-саҳифа яратиш ва кредит карта маълумотларини ўғирлаш айби қўйилган. Бошқа давлатлар ҳам шунга эргашиб, фишерларни қидириб, ҳибсга олишни бошладилар. Компаниялар ҳам фишингга қарши курашда қатнашмоқда. 2005 йил 31 март куни Microsoft АҚШнинг Ғарбий округ судига "Жон Доу"ни пароллар ва махфий маълумотларни олишда айблаб, 117 та даъво киритди. 2005 йил март ойида Microsoft ва Австралия ҳукумати ўртасида ҳуқуқни муҳофаза қилиш органлари ходимларини турли кибержиноятларга, жумладан, фишингга қарши курашишга ўргатиш бўйича ҳамкорлик бошланди.[5]

Фишинг усулини қўллаш орқали содир этилган жиноятларга жавобгарлик асосан Ўзбекистон Республикаси Жиноят кодексининг 168-моддаси (фирибгарлик) 2-қисми ва 169-моддаси (ўғирлик) 3-қисмларида белгилаб ўтилган. Бундан ташқари Жиноят кодексида XX[1] боби “Ахборот технологиялари соҳасидаги жиноятлар”га бағишланган.[6]

Ушбу турдаги жиноятларга белгиланган жавобгарлик турларини хорижий давлатлар кодекслари мисолида таҳлил қиладиган бўлсак, масалан Хитой Халқ Республикаси Жиноят кодексининг 287-моддасида “Компьютер техникасидан фойдаланган ҳолда ўзга маблағларни пора бериш ёки мақсадсиз фойдаланиш учун фирибгарлик йўли билан талон-тарож қилиш ёхуд эгаллаб олганлик ҳаракатлари учун жавобгарлик белгиланган. Компьютер техникаларидан фойдаланиб содир этилган шу каби жиноятлар учун жавобгарликни ушбу кодекснинг 285 ва 286-моддаларида кўриш мумкин. [7]

Австралия Жиноят кодексининг 10.7 боби “Компьютер жиноятчилиги” деб номланиб, боб ўз ичига компютер тизимига рухсатсиз кириш, ундан маълумотларни ўғирлаш, модификация қилиш, алоқани қасддан бузиш, маълумотларга зарар етказиш каби ҳаракатлар учун жиноий жавобгарлик белгиланган. [8]

Россия Федерациясининг Жиноят кодекси 272-моддаси “Компьютер ахборотларидан қонунга хилоф равишда фойдаланиш” ва 273-моддаларида “Зарарли келтирувчи

компьютер дастурларини яратиш, ишлатиш ёки тарқатиш”га жавобгарлик белгиланган. [9]

Бу каби жиноий ҳаракатлар (кибержиноят) учун жавобгарлик Германия ва Люксембург давлатлари қонунчилигида кўришимиз мумкин.[10]

Юқоридагилардан келиб чиққан ҳолда бизнинг фикримизча, сўнгги пайтларда фуқароларнинг пластик карталари ҳисобларидан пул маблағлари ўғрилик ва фирибгарлик йўли билан, хусусан тадқиқот доирасида ўрганаётган фишинг усулида содир этиш кўпайганини кузатиш мумкин. Бинобарин мазкур жиноий хатти-ҳаракатлар ахборот технологиялари билан узвий боғлиқ бўлиб, бу қилмишни XX[1] бобда, яъни Ахборот технологиялари соҳасидаги жиноятлар қаторида қайд этилмаганлиги, балки бу қилмиш учун жавобгарлик Жиноят кодексимизнинг X бобига, яъни “Ўзгалар мулкини талон-тарож қилиш” номли бобига мурожаат қилишга тўғри келмоқда.

Шу муносабат билан бу каби жиноятларни алоҳида бобда қайд этиш орқали тергов бўлинмаларини бу йўналишга эътиборини янада қаратган бўламиз, сабаби ҳозирда бизга маълумки бу каби жиноятларни тергов қилиш бўйича терговчи ва суриштирувчиларда Ахборот технологиялари сохасида кўникмалар етарлича шакилланмаган, тергов ва суриштирув тармоқларида мазкур жиноятларни тергов қилиш бўлинмаларини ташкил этиш, уларни илғор хорижий тажрибалар асосида малакаларини ошириб бориш мухим деб ҳисоблаймиз.

Юқоридагилардан келиб чиқиб мутахассислар, биринчи навбатда, хизмат фойдаланувчиларига фишингни мустақил равишда таниб олишни ўрганишни маслаҳат беришади.

Ҳисоб қайдномасини ёки шунга ўхшаш ҳар қандай сўровни “тасдиқлаш” сўралган электрон хатга жавобан экспертлар фойдаланувчиларга унинг ҳақиқийлигини текшириш учун хабар юборилган компания билан боғланишни маслаҳат беради. Шунингдек, ҳар қандай гиперҳаволалар ўрнига ташкилотингизнинг URL манзилини манзиллар қаторига ўзингиз киритишингизни тавсия қилади.

Деярли барча ҳақиқий хизмат хабарларида фишерлар учун мавжуд бўлмаган баъзи маълумотлар мавжуд, масалан, исм ёки ҳисоб рақамининг охирги рақамларини эслатиб ўтиш. Шу билан бирга, шахсий маълумотларга эга бўлмаган ҳар қандай хатлар шубҳа туғдириши керак.

Шуни ҳам унутмаслик керакки, фишинг сайтлари қалқиб чиқувчи ойналар орқасида яшириниши мумкин. Улар мақсадли реклама бўлиши мумкин. Вақти-вақти билан

фойдаланувчи ўзининг електрон почта манзилини "кириш" устунида кўради ва фақат пастки устунга паролни киритиш сўралади. Форумлар ва ижтимоий тармоқлардаги шарҳларда фишинг сайтига ҳаволани кўриш имконияти мавжуд. Ҳаволани сизга ҳисоби бузилган дўстингиз ёки танишингиз ҳам юбориши мумкин. Агар хат ёки ҳавола сизда шубҳа уйғоца, унга эргашмаслик яхшироқдир.

ХУЛОСА

Хулоса шуки, киберҳужумлар узоқ вақтдан бери ҳаётимизнинг бир қисми бўлиб келган. Фирибгарликдан ҳимоя қилиш молиявий, электрон тижорат ва бошқа хизматларни ривожлантирувчи корпорациялар ва стартаплар учун глобал вазифадир. Аммо фойдаланувчилар тажовузкорнинг илгагига тушиб қолмаслик учун оддий қадамларни унутмасликлари керак.

REFERENCES

1.GP4.3 — Growth and Fraud — Case #3 — Phishing (англ.) (30 декабря 2005). Дата обращения: 21 ноября 2008.
2. Kate Stoodley. In 2005, Organized Crime Will Back Phishers (англ.) (недоступная ссылка) (23 декабря 2004). Дата обращения: 21 ноября 2008. Архивировано 31 января 2011 года.
3.https://stealthmail.com/ru/statistics;
4.https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/ironport_targeted_phishing.pdf;
5. https://topuch.ru/prezentaciya-na-temu-fishing/index.html;
6. Ўзбекистон Республикаси Жиноят кодекси 1994 йил 22 сентябрь
7. Хитой Халқ Республикаси Жиноят кодекси
8. Австралия Жиноят кодекси
9. Россия Федерацияси Жиноят кодекси
10. https://ru.m/wikipedia.org.