ЗАШТИТИТЕ СВОЈУ ФИРМУ И ЗАПОСЛЕНЕ

https://www.pexels.com/photo/email-blocks-on-gray-surface-1591062/

BUSINESS EMAIL COMPROMISE (BEC)

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ

СРБ-ЦЕРТ

ШТА ПРЕДСТАВЉА *BUSINESS EMAIL COMPROMISE (BEC)*?

Компромитовање пословне електронске поште (*Business email compromise - BEC*) је врста преваре у којој нападач има за циљ наношење штете компанији, користећи лажне имејл налоге те компаније.

BEC представља велики и растући проблем који може погодити различите типове организација, без обзира на њихову величину. *BEC* представља једну од најтежих финансијских превара на мрежи, која искоришћава чињеницу да се у свакодневном раду већина организација, за пословну комуникацију, ослања на електронску пошту. Овакав тип преваре је поједине организације изложио великим губицима, који се могу мерити у милијардама еура.

Компромитовање налога електронске поште (*Email account compromise - EAC*) или преузимање налога електронске поште је претња која се убрзано развија у ери пословања заснованој на cloudинфраструктури. *EAC* је често повезан са *BEC*-ом, јер се компромитовани налози користе у све већем броју превара у сајбер простору.

Велики изазов представља откривање и спречавање *BEC* и *EAC* типова напада, посебно са постојећим алатима, *endpoint* решењима и актуелним решењима која се користе за одбрану *cloud* платформи.

У *BEC* превари, злонамерни нападач се представља као неко коме прималац такве поруке треба да верује - обично као колега, шеф или компанија са којом, посредно или непосредно, сарађују. Злонамерни нападач шаље имејл поруку за коју се чини да долази од познатог извора који поставља легитиман захтев, као нпр. да изврши трансфер новца са једног на други рачун, преусмери платни списак, промени банкарске детаље за будућа плаћања и сл.

ВРСТЕ *BEC* ПРЕВАРА

Постоји неколико врста *BEC* превара:

Извршни директор (*chief executive officer - CEO*) превара: Овде се злонамени нападачи представљају као извршни директор или руководилац компаније и обично електронском поштом пошаљу захтев појединцу из сектора финансија, да се средства пребаце на рачун који контролише нападач.

Компромитован налог: Налог електронске поште запосленог је хакован и користи се за потраживање плаћања услуга и производа компанија са којом посматрана организација сарађује. Уплате се затим шаљу на лажне банковне рачуне у власништву нападача.

Лажна фактура: Нападачи обично циљају стране добављаче путем ове тактике. Злонамерни нападач се представља као да је добављач и захтева пребацивање средстава на лажне рачуне.

Лажно представљање адвоката: То је случај када се злонамерни нападач лажно представља као адвокат или законски заступник. Запослени на извршним позицијама су обично мета овакве врсте напада, јер не доведе у питање валидност оваквог захтева.

Крађа података: Ове врсте напада обично циљају запослене у људским ресурсима, где злонамерни нападачи покушавају да добију личне или осетљиве информације о појединцима унутар компаније, попут извршних директора и руководилаца. Ови подаци се могу искористити за будуће нападе, попут поменутог типа - Извршни директор.

НА КОЈИ НАЧИН ЗЛОНАМЕРНИ НАПАДАЧИ ИЗВРШАВАЈУ *BEC* ПРЕВАРЕ?

Могући су следеће технике извршавања *BEC* превара:

- **Подметање (*spoof*) имејл налога, веб сајта и домена.** Мале варијације на легитимним имејл адресама (нпр. petar.petrovic@primer.com насупрот petar.petrovc@primer.com), које заварају жртве да су имејл налози аутентични и наставе да комуницирају са злонамерним нападачем, мислећи да се комуникација одвија са легитимним пошиљаоцем. Још једна од техника лажног представљања је подметање (*spoofing*) домена и домена налик легитимним доменима. Ови напади су веома ефикасни јер је злоупотреба домена сложен проблем. Заустављање подметања домена довољно је тешко, а предвидети сваки потенцијални домен који личи на легитимни је још теже. Ова потешкоћа се само умножава са сваким доменом који користе спољни партнери, а који би могли да се користе у *BEC* нападима, са циљем да се злоупотреби поверење корисника. Више о овој теми можете погледати на линку.
- **Слање *spearphishing* имејл порука.** Имејл поруке изгледају као да су од поузданог пошиљаоца, како би се жртва преварила и открила поверљиве информације. Ове информације омогућавају злонамерним нападачима приступ рачунима компанија, календарима и подацима који им дају детаље потребне за спровођење *BEC* напада. Више о овој теми можете погледати на линку.
- **Коришћење малвера.** Уколико се покрене злонамерни софтвер у мрежи организације, нападач може добити приступ легитимним имејловима о наплатама и фактурама. Тако прикупљене информације се користе за постављање захтева или слање порука, како рачуновође или финансијски службеници не би довели у питање захтеве за плаћање. Злонамерни софтвер, такође омогућава злонамернимнападачима приступ подацима жртве, укључујући лозинке и информације о финансијским рачунима.

Ипак злонамерни софтвер се ретко користи у *BEC* нападима, јер се тада могу лакше открити и анализирати системима за одбрану од сајбер напада. *BEC* напади се најчешће ослањају на лажно представљање и друге технике социјалног инжењеринга да би се преварили корисници и ступили у интеракцију са нападачем. Ове нападе је тешко открити, због циљане природе напада и коришћења социјалног инжењеринга, а анализа и санирање оваквих напада је тежак процес који захтева много времена, али и новца.

Код *EAC* напада, злонамерни нападач добија контролу над легитимним налогом електронске поште, што му даље омогућава покретање *BEC* напада. Али у овим случајевима нападач не лажира да има приступ системима као и изабрана особа – већ заиста приступа тим ресурсима.

Пошто се *BEC* и *EAC* фокусирају на људске слабости, а не на рањивост система, потребно је да се одбрана усмери на обучавање корисника како да препознају потенцијалне претње и да се на тај начин спречи, открије и одговори на широк спектар *BEC* и *EAC* техника напада.

Фазе одвијања напада:

ФАЗА 1 - Циљане листе електронске поште

Нападачи почињу са израдом циљане листе имејлова. Уобичајене тактике укључују прикупљање података са *Linkedin* профила, проверавање кроз пословне базе података електронске поште или чак пролазак кроз разне веб странице у потрази за контакт подацима.

ФАЗА 2 – Извршавање напада

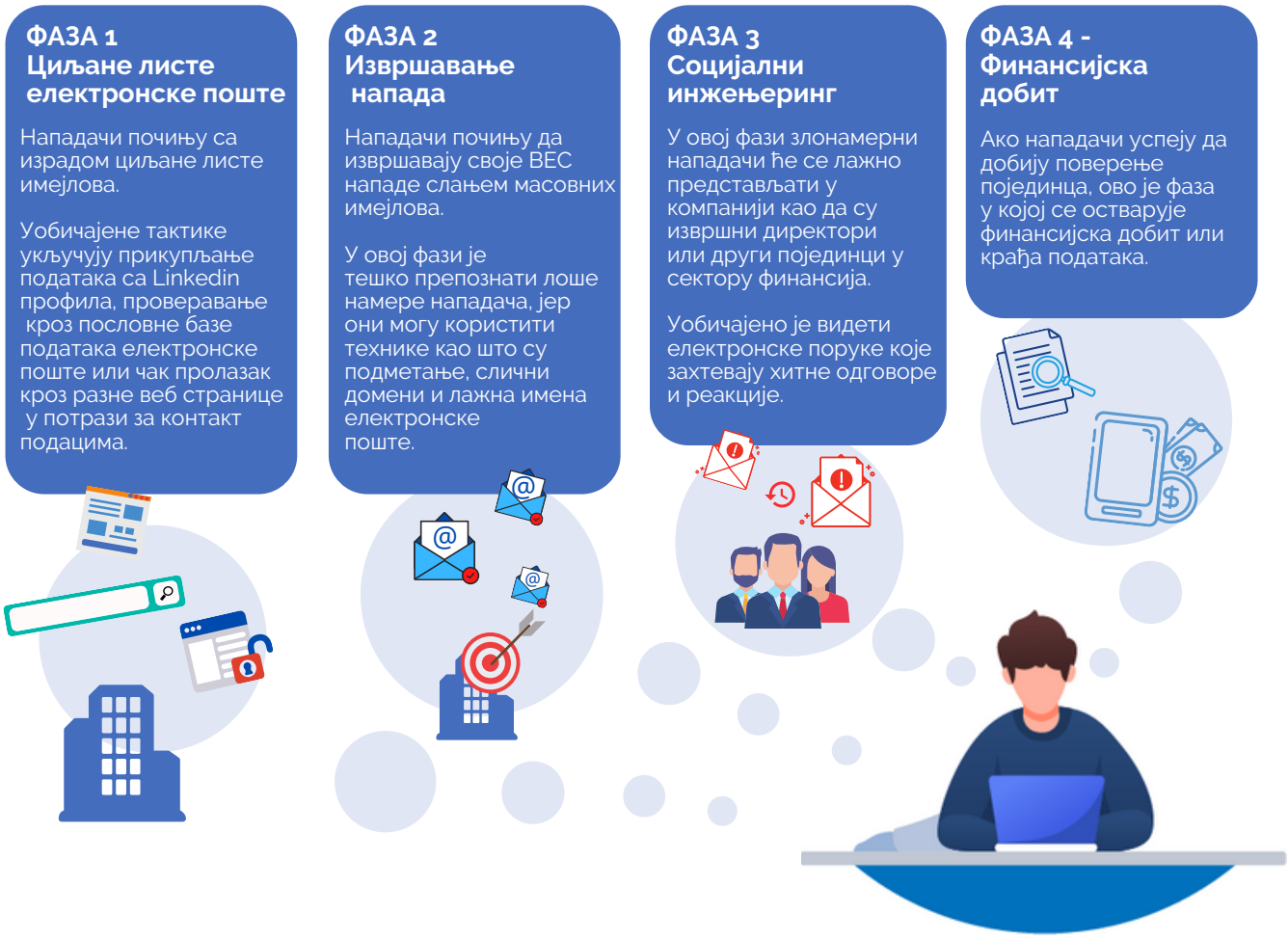
Нападачи почињу да извршавају своје *BEC* нападе слањем масовних имејлова. У овој фази је тешко препознати лоше намере нападача, јер они могу користити технике као што су подметање, слични домени и лажна имена електронске поште.

ФАЗА 3 - Социјални инжењеринг

У овој фази злонамерни нападачи ће се лажно представљати у компанији као да су извршни директори или други појединци у сектору финансија. Уобичајено је видети електронске поруке које захтевају хитне одговоре и реакције.

ФАЗА 4 - Финансијска добит

Ако нападачи успеју да добију поверење појединца, ово је фаза у којој се остварује финансијска добит или крађа података.



КАКО СЕ КОРИСНИЦИ МОГУ ЗАШТИТИТИ?

- Неопходно је пажљиво руковање информацијама које корисници објављују на интернету, најчешће на друштвеним мрежамама. Отвореним дељењем информација попут имена кућних љубимаца, школа које сте похађали, веза са члановима породице и рођендана, дајете злонамерном нападачу све потребне информације и могућност да открије вашу лозинку или одговори на ваша безбедносна питања.
- Треба водити рачуна о линковима или документима које корисник добије у оквиру електронске поште, или СМС-а, а посебну пажњу обратите на захтеве да ажурирате или проверите/промените информације о налогу. Додатно је пожељна провера телефонског број компаније у адресару организације (не треба користити онај број који нуди потенцијални нападач у мејлу), као и позив компанији, уколико се било шта учини сумњивим, како би се утврдило да ли је захтев легитиман.
- Пажљиво проверити адресу електронске поште, URL и правопис који се користи у било којој преписци. Нападачи користе мале разлике како би заварали око корисника и стекли поверење.
- Преузимање прилога представља додатни изазов којем треба приступити са више пажње. Не треба отварати прилоге електронске поште добијене од непознатог пошиљаоца.
- Администратор имејл система може подесити *Domain-Based Message Authentication*, *Reporting and Conformance Protocol* (*DMARC*) полису, која заједно са *Sender Policy Framework* (*SPF*) и *Domain Keys Identified Mail* (*DKIM*) механизмима значајно умањује ризик од пријема фишинг имејл порука. У наслове порука које нису послате са компанијског сервера може се додати реч “екстерно” што може олакшати процену да ли је реч о превари или не. Више о овим механизмима можете прочитати на линку.
- Подешавање двофакторске (или мултифакторске) аутентификације на било ком налогу представља додатни вид заштите и може значајно отежати злоупотребу налога.
- Пожељно је коришћење опције личне верификације захтева за плаћање и куповину или да корисник ступи у директан контакт са особом, како би се уверио да су примљени налози легитимни. Овај принцип треба применити посебно уколико дође до било какве промене броја рачуна или процедуре плаћања са особом која подноси захтев.
- Корисник треба да буде посебно обазрив уколико пошиљалац врши притисак да се брзо поступи.

Национални ЦЕРТ Републике Србије не промовише или фаворизује било који од коришћених јавних извора, међу којима су и комерцијални производи и услуге. Све препоруке, анализе и предлози дати су у циљу превенције и заштите од безбедносних ризика.

Извори:

- FBI: Business Email Compromise
- Proofpoint: Business email compromise (BEC)
- Dmarcian: https://dmarcian.com/basic-bec-defense/

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

#odbraniseznanjem

СРБ-ЦЕРТ