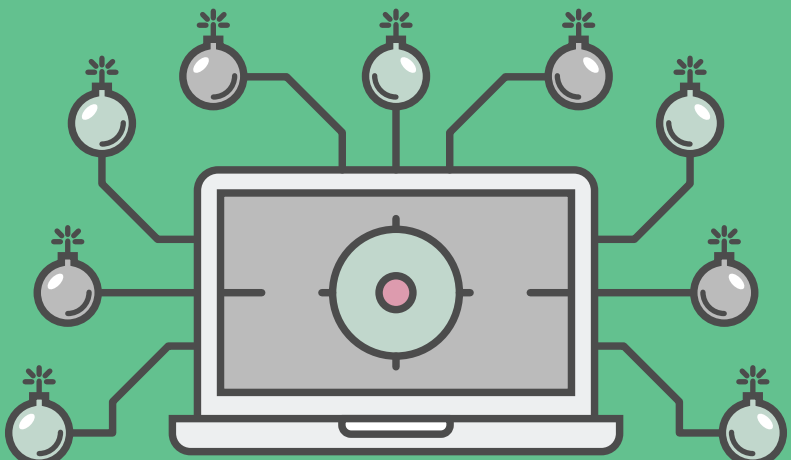
ВРСТЕ САЈБЕР НАПАДА



USAID
ОД АМЕРИЧКОГ НАРОДА

СРБ-ЦЕРТ

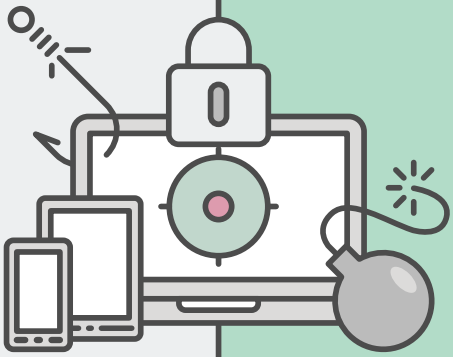
РАТЕЛ

oebs Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji

1. Шта су сајбер напади

Сајбер напади представљају врсту напада у коме је циљ злонамерно онемогућити рад рачунара или рачунарских мрежа, украсти податке или нападнути рачунар користити као полазну тачку за друге нападе. Сајбер криминалци користе разне методе за покретање напада, међу којима су најчешћи фишинг, рансомвер, дистрибуирано ускраћивање услуга (DDOS) и друге врсте малвера.

Број регистрованих случајева у области сајбер криминала у Републици Србији расте по годишњој стопи већој од 20%. Дигитализација свакодневних процеса у приватном и пословном деловању повећава и ризике у смислу сајбер безбедности. Од кључне важности је развити свест о потенцијалним опасностима и превентивном деловању. Погрешно би било у потпуности се ослонити на технолошка решења уз очекивање да ће се на тај начин осигурати комплетна заштита.



Да ли сте знали да се на сваких 39 секунди догоди по један сајбер напад? У порасту је проценат успешности сајбер напада, као и штета коју они проузрокују.
Нове технике сајбер напада су теже уочљиве и одвијају се као позадински процеси, због чега је важно развити безбедносне процедуре и правовремено реаговати.

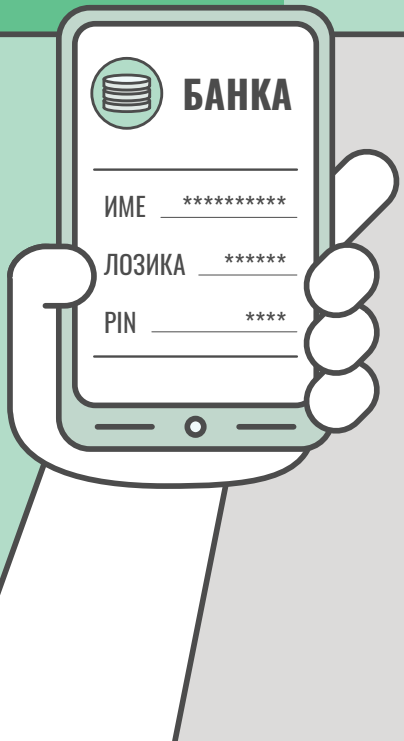
2. Фишинг

Фишинг (енг. phishing) је тип преваре где је циљ доћи до поверљивих података корисника, попут бројева банковних рачуна, лозинки налога на друштвеним мрежама или електорнској пошти. Жртва овог типа сајбер напада добија поруку путем електронске поште, друштвених мрежа, телефона или као СМС-а у којој се од ње захтева да посети линк или отвори документ и упише личне и поверљиве податке.

Пошто изглед тог документа или веб странице делују веродостојно и поуздано, као да су стигли од банке или неке друге институције, жртва попуњава формулар и тиме прослеђује своје податке нападачу.

Препорука је да приликом пријема мејла у коме се од вас захтева унос личних података, детаљно анализирате име и адресу пошиљаоца, као и садржај поруке. Често ћете на тај начин уочити да порука није стигла са званичне адресе банке или друге институције, а да текст поруке садржи правописне грешке.
Уколико посетите линк са формуларом за унос личних података, обавезно проверите URL адресу, јер и на тај начин можете закључити да је у питању покушај крађе података.

Друга врста фишинг напада реализује се кроз дистрибуцију докумената у оквиру електронске поруке. Када жртва отвори документ покренуће се процеси који доводе до инфицирања рачунарског система.



3. Малвер

Малвер је злонамерни софтвер који се, осим фишингом, дистрибуира и преко интернет страница које наводе корисника да инсталира нежељени софтвер. Најзаступљенији вид дистрибуције малвера је преко поруке електронске поште, у којој се од жртве захтева да отвори документ из прилога поруке. Након тога, најчешће се појављује обавештење да се кликне на дугме "Enable Content" чиме ће се покренути преузимање малвер садржаја са локације нападача. Тај софтвер ће омогућити покретање штетних процеса у оперативни систем рачунара жртве, и променити његово понашање на начин који одговара нападачу.

То може бити блокада антивируса и других безбедносних софтвера, регистровање свега што укуцате на тастатури, прављење снимака екрана или крађа датотека. Неки малвери врше "рударење" крипто валута користећи ресурсе рачунара жртве или обављају преглед рекламних банера у корист нападача.

Постоје и софистицираније типови малвера, код којих се одмах по отварању наизглед обичног документа извршавају злонамерни процеси, а малвер се шири и путем преносних уређаја (USB), мрежним приступом (жичним или бежичним приступом), преузимањем садржаја са сајтова и др.

Реч малвер је кованица састављена од почетних слогова енглеског термина Malicious Software. Најчешће врсте малвера су: рансомвер, вирус, тројанац, рат алати, веб шел, логичка бомба, црв, адвер, спајвер, килогер итд.

4. Рансомвер

Рансомвер је врста напада путем злонамерног софтвера (малвера) којим се преузима контрола над рачунаром и подацима жртве. Напад прати порука да је за откључавање рачунара и података потребно уплатити одређени износ (откупнину) у новцу или крипто валутама.

Овај тип напада је све распрострањенији и софистицираније због финансијске користи који криминалци остварују путем њега. Многи корисници сматрају да не представљају занимљиву мету за сајбер криминалце, што је погрешно. Осим напада који циљају одређеног корисника или организацију, постоје и масовни рансомвер напади који су усмерени ка најширем кругу корисника.

Жртве рансомвер напада одмах након добијања поруке треба да онемогуће даље ширење малвера кроз мрежу, тако што ће искључити све рачунаре и фунцкије попут Wi-Fi, NFC и Bluetooth. Након процене степена распрострањености малвера и изазване штете, потребно је пријавити случај Тужилаштву за високотехнолошки криминал и потражити помоћ стручњака за сајбер безбедност.

Препорука Националног ЦЕРТ-а је да се откупнина не плаћа, јер плаћање откупа није гаранција да ће корисник заиста добити кључ за откључавање података, а на овај начин се финансира сајбер криминал. Боља решења су редовно креирање заштитних копија (бекапа) или покушај да се изврши декрипција и откључавање фајлова.

5. Заштита од сајбер напада

Безбедносна решења која би гарантовала потпуну заштиту не постоје. Због тога је потребно развити свест о сајбер ризицима и стално унапређивати знања везана за њихово спречавање.

Честе жртве сајбер напада су компаније или институције које врше велика улагања у безбедност и имају приступ најсавременијим технологијама, што указује на то да сајбер криминалци могу располагати ресурсима и техникама који су "за корак испред".

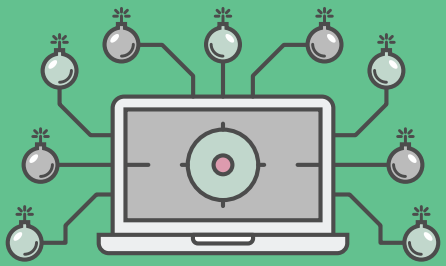
Зато је важна континуирана едукација индивидуалних корисника и запослених у компанијама и институцијама, као и успостављање безбедносних протокола који ће смањити могућност сајбер инцидента. Нажалост, ниједан протокол не може да поништи ризично и неодговорно понашање појединца.

Неке покушаје сајбер напада је врло лако уочити, јер се покрећу са очигледно непостојећих адреса електронске поште, садрже неразумљиве или језички неправилне поруке, воде на лажне сајтове чије се УРЛ адресе не подударају са називом институција. Насупрот њима, постоје софистициране технике које не изазивају сумњу, а засноване су на пресретању електронске комуникације жртве или крађи идентитета.

ОПШТЕ ПРЕПОРУКЕ ЗА ЗАШТИТУ ОД СВИХ ТИПОВА САЈБЕР НАПАДА:

1. Редовно ажурирање оперативног система и антивирусног софтвера
2. Редовно креирање резервних копија података (backup)
3. Креирање комплексних лозинки са најмање 9 алфа нумеричких знакова, укључујући и знакове
4. Коришћење различитих лозинки за налоге
5. Брисање сумњивих порука електронске поште или означавање као Spam/Junk
6. Хитно обавештавање банке у случају поделе/губитка података о банковном рачуну
7. Активирање антивируса и комплетно скенирање уређаја
8. Промена лозинке на свим налозима, у случају губитка једне лозинке

ВРСТЕ САЈБЕР НАПАДА



Регулаторна агенција за
електронске комуникације и
поштанске услуге (РАТЕЛ)

Палмотићева 2
11103 Београд
Република Србија

www.cert.rs

Ставови изречени у брошури припадају искључиво аутору и његовим сарадницима и не представљају нужно званичан став Мисије ОЕБС-а у Србији.

USAID
OD AMERIČKOG NARODA

СРБ-ЦЕРТ

РАТЕЛ

oebs Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji

Израда ове брошуре омогућена је уз подршку америчког народа путем Америчке агенције за међународни развој (USAiD).
За садржај брошуре одговорни су аутори и она не мора нужно да одражава ставове USAiD-а или Владе Сједињених Америчких Држава.