Рансомвер као модел пружања услуга

(Ransomware-as-a-Service)

СРБ-ЦЕРТ

Рансомвер представља једну од најзаступљенијих интернет претњи. Статистички подаци Европске агенције за мрежну и информациону безбедност *(ENISA)** указују да је током 2022. године забележен пад броја изнуђених плаћања жртава рансомвер напада, док се у 2023. години поново бележи њихов пораст, баш као и пораст броја наплаћених изнуда. Узрок пораста је увођење тзв. "Дупле изнуде" као додатног облика изнуђивања. Уколико узмемо у обзир и чињеницу присуства вештачке интелигенције и могућности њене злоупотребе, то нам јасно може указати да ће рансомвер напад и даље бити у самом врху листе најзаступљенијих сајбер напада и да је примена превентивних мера једна од најбољих метода заштите од рансомвер напада.

Рансомвер (енг. *Ransomware*), је тип малвера (малициозни програмски код) који је усмерен на неовлашћено приступање информационим системима или уређају, са задатком да кориснику лимитира приступ, или да закључа одређене фајлове и датотеке и на тај начин у потпуности онемогући приступ нападнутом информационом систему или уређају. Крајњи циљ нападача је противправно стицање имовинске користи, али може бити злоупотребљен и за остваривање политичких, односно хактивистичких циљева. Након неовлашћеног приступа и закључавања фајлова или датотека, нападачи шаљу поруку која се појављује на монитору жртве која садржи инструкције за откуп декрипционих кључева (програмски код за откључавање), који би жртви требало да омогући поновни приступ инфицираним фајловима или датотекама.

Током свог развоја, рансомвер је представљао тип сајбер напада који је, пре свега, био усмерен на физичка лица, односно појединце. Разлог томе је био низак ниво сајбер културе појединца, која се најпре огледала у креирању само једне и често једноставне лозинке за приступ интернет налозима, као и неадекватна заштита уређаја у виду одсуства лиценцираних антивирусних софтвера. Малициозни програмски код за откључавање енкриптованих фајлова и датотека је често био лошег квалитета и није откључавао све инфициране датотеке. Са друге стране чест проблем је представљала и немогућност брзе реализације изнуде захтеване суме новца. То су била два основна изазова са којима су се суочавале жртве, али и нападачи приликом коришћења рансомвера.

Са унапређењем малициозног програмског кода, растао је и ниво софистицираности напада, што је хакерима омогућило да усмере своје нападе на мала и средња предузећа, а затим и на веће и боље заштићене системе. Онемогућавање рада великих система представља велики изазов како за конкретно правно лице, тако и за све оне који користе услуге или производе нападнуте организације.

Организовање сајбер напада на правна лица је нападачима омогућило и већу зараду, што је касније водило ка организовању већег броја хакера у „корпоративни модел пословања", као и развоја *RaaS (Ransomware-as-a-Service)* услуга.

RaaS услуге заправо представљају нови бизнис модел дизајниран од стране већих и озбиљнијих хакерских група које креирају одређени тип рансомвера и нуде га на продају

* https://www.enisa.europa.eu/publications/enisa-threat-landscape-²0²³

заинтересованим купцима, било да је реч о другим хакерским групама, било да говоримо о потенцијалним купцима који немају техничка знања, али из одређених интереса желе да покрену рансомвер напад на неки информациони систем. Хакерске групе своје RaaS услуге најчешће нуде заинтересованим купцима путем реклама на *Dark Web*-у. Купац се може одлучити за различити „пакет услуга" које су доступне у одговарајућем ценовном рангу - од једнократне услуге, па све до месечних или других одговарајућих модела „претплате".

У продужетку се налази кратак опис основних десет корака за извршавање Рансомвер напада:

1. анализа и одабир потенцијалне жртве,
2. анализа одбрамбених капацитета информационог система жртве,
3. уколико жртва има квалитетну заштиту система, приступа се анализи одбрамбених капацитета информационог система повезаних компанија са којима жртва има остварену пословну сарадњу, како би се упало преко тих система који имају слабију одбрану,
4. упад у систем жртве (најчешће то може бити помоћу фишинга, компромитације пословне кореспонденције – *BEC*, искоришћавања рањивости система који није ажуриран, или RDP приступа) који нападачима омогућава приступ информационом систему жртве,
5. копирање података из система жртве на систем нападача за потребе „Дупле изнуде",
6. анализа пословних процеса и података на основу преузетих информација из система жртве,
7. активирање одговарајућег рансомвер програмског кода који закључава датотеке на информационом систему жртве,
8. захтевање откупа декрипционих кључева у крипто валути,
9. претња јавним објављивањем прекопираних пословних и личних података путем медија („Дупла изнуда"),
10. достављање декрипционих кључева (у случајевима када жртва плати изнуђену суму новца).

Вођени „корпоративним моделом пословања" хакерске групе се данас углавном организују и раде у тимовима. Једна група ради анализу финансијских и пословних података приликом одабира жртве, док други тимови могу радити на анализи повезаних компанија у намери да злоупотребом ресурса повезане компаније омогуће нападачима лакши приступ систему крајње жртве рансомвер напада.

За потребе напада, хакери се најчешће одлучују за финишг напад, као улазни вектор, али то може бити и искоришћавање неке од рањивости информационог система жртве, као и злоупотреба RDP *(Remote Desktop Protocol)* приступа систему.

Након упада у систем жртве, хакери раде детаљну анализу пословних процеса и података, како би на основу те анализе могли да организују напад и дефинишу који је реални износ откупа који могу захтевати од жртве. Уовом кораку хакери такође преузимају одређену количину количину података из информационог система жртве и копирају их на своје системе.

Тако прикупљени подаци им служе за каснију претњу којом желе додатно да присиле жртву да плати износ откупа. Уколико би жртва одбила плаћање откупа, нападачи би запретили објављивањем прикупљених пословних и личних података целокупној јавности, путем медија, што представља тзв. „Дуплу изнуду".

Препорука Националног ЦЕРТ-а Републике Србије је да се откупни износ не плаћа, јер се на тај начин финансира криминално деловање хакерских група, при чему нема никаквих гаранција да ће жртва добити декрипционе кључеве, или да ће добијени кључеви у потпуности омогућити приступ и коришћење података који су били закључани рансомвером током напада. Са друге стране, уколико се плати откупни износ, хакерске групе се често опредељују да и у будућности понове напад на исту организацију или компанију, без обзира на поруку да ће, уколико им се први пут уплати тражени износ, заувек нестати из система те жртве и неће се више враћати.

Последице рансомвер напада могу имати веома негативан утицај на пословање, профит, али и репутацију организације или компаније, због чега је значај примене превентивних мера заштите у интересу свих запослених у једној организацији или компанији, као и повезаних пословних партнера са којима је остварена добра сарадња. Такође, значај примене превентивних мера се може односити и на све кориснике којима се нуде услуге одређене организације или компаније.

Превентивне мере, које се могу предузети у циљу заштите од рансомвер напада, су:

1. редовно ажурирање оперативних и апликативних софтвера, како би биле примењене све доступне закрпе за откривене рањивости,
2. сегментирање мреже којим се једна велика мрежа претвори у скуп мањих делова мреже, чиме се онемогућава брзо потенцијално ширење малвера по целокупној мрежи,
3. инсталација лиценцираног програма за заштиту рачунара од вируса и малвера,
4. редовно креирање резервних копија свих важних датотека и фајлова,
5. редовно тестирање резервних копија,
6. увођење и примена мултифакторске аутентификације као додатног слоја заштите,
7. контрола приступа информационом систему са удаљених локација,
8. континуиран рад на подизању свести запослених о безбедносним претњама, који се најпре огледа у:

    - креирању комплексних лозинки,
    - примена принципа: један налог – једна лозинка
    - коришћењу службених имејл налога искључиво у корпоративне сврхе,
    - избегавању клика на линк или отварање прилога у имејлу који стигне од непознатог пошиљаоца, јер се фишинг често користи као улазни вектор за рансомвер нападе,

- чувању личних или финансијских података, односно да их не треба делити путем: имејла, СМС или чет порука, телефонског позива или у директном разговору са непознатим особама,
- провери домена интернет страница које се посећују, имајући у виду да се на интернету налази велики број компромитованих интернет страница путем којих се шире малициозни садржаји.

Остале мере превенције, превасходно усмерене на пословне кориснике, можете погледати у нашој публикацији „Препоруке за заштиту од рансомвер напада”.