РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ

ПРЕПОРУКЕ ЗА ПРЕВЕНТИВНУ ЗАШТИТУ ОД РАНСОМВЕРА

Рансомвер је врста злонамерног софтвера или малвера, који је осмишљен тако да ускраћује приступ ИКТ систему или подацима док откупнина не буде плаћена. Рансомвер се обично шири путем фишинг порука електронске поште или ненамерно посећујући заражене интернет странице.

Рансомвер може имати велике последице како за индивидуалне кориснике, тако и за компаније. Сваки корисник који чува важне податке на рачунару или мрежи је у ризику, укључујући јавни и приватни сектор, као и друге субјекте који представљају критичну инфраструктуру. Опоравак може бити тежак процес, који у одређеним случајевима захтева и коришћење услуга стручних лица да би се откључале инфициране датотеке, а неке жртве најчешће плаћају откупнину, у нади да ће добити одговарајуће кључеве за откључавање инфицираних датотека.

Међутим, не постоји гаранција да ће се плаћањем откупнине добити наведени кључеви.

Национални ЦЕРТ препоручује следеће мере предострожности како би заштитили кориснике од претњи рансомвером:

- Потребно је да корисници редовно ажурирају оперативни систем, као и софтвер и антивирусна решења, најновијим верзијама на уређајима. Апликације и оперативни системи са застарелим верзијама су мета већине напада. Редовно крпљење рањивог софтвера је неопходно да би се спречила злоупотреба откривене рањивости. Размислите о коришћењу централизованог система управљања закрпама (енг. *centralized patch management system*).
- Креирање резервних копија на дневном нивоу или чешће, уколико за то постоји потреба. Детаљније о томе како креирати резервну копију података, можете погледати на страници Публикације брошуру под називом Креирање резервних копија - Backup. Враћање података из сигурне резервне копије је најбржи начин да се поврати приступ подацима.
- Корисници не треба да кликну на линкове или отварају прилоге који стижу са непознатих и сумњивих мејл адреса.
- Не остављајте личне податке када одговарате на имејл пошту, нежељени телефонски позив или текстуалну поруку. Фишинг нападачи ће покушати да преваре запослене и инсталирају злонамерни софтвер, али се могу и лажно представити тврдећи да су из ИТ-а. Обавезно се обратите свом ИТ одељењу уколико примите сумњиве поруке или позиве упућене вама или колегама.
- Користите антивирусни софтвер и *firewall* познатих и одобрених компанија. Одржавање *firewall*-а и ажурирање антивирусног софтвера су критични. Подесите антивирусне и анти-малвер програме да редовно скенирање раде аутоматски.

- Придржавајте се сигурне праксе приликом коришћења Интернета. *Exploit kits* који се налазе на компромитованим веб сајтовима се обично користе за ширење злонамерног софтвера.
- Ако путујете, претходно обавестите ИТ одељење, посебно ако ћете користити јавне приступне тачке за бежични интернет (Wi-Fi). Обавезно користите поуздану виртуелну приватну мрежу (VPN) када приступате јавној Wi-Fi мрежи.

Поред наведеног, Национални ЦЕРТ такође препоручује да компаније примењују следеће најбоље праксе:

- Спровести програм подизања свести и обуке. Будући да су крајњи корисници мета нападача запослени и појединци треба да се упознају са претњама од рансомвера, као и са начином на који се испоручује и шири кроз мрежу.
- Привилеговане налоге користите на принципу "least privilege" (најмање привилегије): корисницима не би требало додељивати администраторски налог осим ако за то не постоји изузетна потреба. Они корисници који поседују администраторске налоге треба да их користе само онда када је то потребно. Приликом инсталације и покретања апликација, корисницима треба увести рестриктивне мере, односно применити поменути принцип "least privilege" за све системе и сервисе. Овакав приступ може помоћи код превенције покретања малвера или свести на минимум ширење истог путем мреже.
- Користите одобрене и проверене апликације са тзв. whitelisting-а, које омогућавају системима да извршавају познате програме, дозвољене безбедносним политикама.
- Потребно је користити спам филтере, јер на тај начин онемогућавате да фишинг мејлови стигну до крајњих корисника, као и потврду долазне имејл поште користећи технологије попут *Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC)* и *DomainKeys Identified Mail (DKIM)* како бисте спречили подметање поште (*email spoofing*).
- Радите скенирање долазне и одлазне имејл поште како бисте открили потенцијалне претње и фајлове који садрже малициозни садржај и на тај начин спречили да дође до крајњих корисника. Користите скенирање и филтрирање садржаја на серверима имејл поште. Долазне имејлове треба скенирати на постојеће претње и блокирати све врсте прилога који могу представљати претњу.
- Конфигуришите *firewall* тако да блокира приступ познатим малициозним IP адресама.
- Конфигуришите контроле приступа - укључујући дозволе за дељење фајлова, директоријума и мреже – користећи принцип "*least privilege*". Ако корисник треба само да чита одређене фајлове, не би требало да има приступ уписа у тим фајловима, директоријумима или дељеним серверима.
- Онемогућите макро скрипте из датотека које се преносе путем електронске поште. Размислите о употреби *Office Viewer* софтвера за отварање *Microsoft Office* датотека које се преносе путем електронске поште уместо потпуне апликације.
- Примените *Software Restriction Policies (SRP)* или друге контроле да бисте спречили извршавање програма са уобичајених локација које захтева рансомвер, као што су привремени фолдери (*temporary folders*) који подржавају популарни интернет претраживачи или програме који служе за компресију/декомпресију, укључујући фолдер *AppData/LocalAppData*.

- Размислите о искључивању *Remote Desktop protocol*-а (*RDP*), ако се не користи.
- Извршне оперативне програме или специфичне програме издвојте у виртуелно окружење.
- Извршите поделу базирану на основу организационе структуре и примените физичко и логичко раздвајање мреже и приступ подацима за различите организационе јединице.
- Редовно правите резервне копије података. Проверите интегритет тих резервних копија и тестирајте процес враћања података, да бисте били сигурни да све фунцкионише на одговарајући начин.
- Спровести годишњи тест интегритета система (*penetration test*) и процену рањивости система (*vulnerability assessment*).
- Обезбедите резервне копије. Уверите се да резервне копије нису констатно повезане са рачунарима и мрежом за које се праве резервне копије. Примери за безбедно чување резервних копија су: облак (*cloud*) или физичко чување резервних копија ван мреже (*offline*). Неки случајеви рансомвера могу закључати резервне копије које се чувају у облаку, када системи непрестано праве резервне копије у реалном времену, познато као константна/упорна синхронизација (*persistent synchronization*). Резервне копије су кључне за опоравак система од рансомвера и као одговор на претњу. Ако је систем компромитован, резервна копија може бити најбољи начин да се поврате критични подаци.

Уколико се рансомвер напад успешно изведе, Национални ЦЕРТ препоручује да:

- Не плаћате откупнину, јер тиме охрабрујете и финансирате злонамерне нападаче. Чак и ако је откупнина плаћена, нема гаранције да ћете повратити приступ својим подацима, јер често кључеви које добијете за узврат, делимично или уопште неће откључати инфициране датотеке, односно фајлове.
- Пријавите инцидент надлежним органима како би вам помогли у решавању инцидента, јер постоји могућност да је исти тип инцидента пријављен од стране других лица, па је могуће да постоји декрипциони кључ којим можете откључати ваше податке. Како можете пријавити инцидент, погледајте на страници Публикације брошуру под називом Упутство за пријаву инцидента.

Извор:

CISA: https://www.us-cert.gov/Ransomware
FBI: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view