Смернице за превенцију и отпорност на **рансомвер нападе**

Децембар 2025.

СРБ-ЦЕРТ

РАТЕЛ

САДРЖАЈ

УВОД

Рансомвер напади остају једна од најдеструктивнијих сајбер претњи на глобалном нивоу, а сектори критичне инфраструктуре попут финансијског, енергетског и телекомуникацијског све чешће су мета нападача. Иако нису део критичне инфраструктуре, мала и средња предузећа као и појединци подједнако су угрожени овим нападима, али са несразмерно мањим капацитетима за одбрану од њих. Током 2024. и почетком 2025. године, број инцидената повезаних са рансомвером нагло је порастао по учесталости и софистицираности, узрокујући озбиљну оперативну и финансијску штету широм планете. Злонамерни актери прилагодили су своје тактике - од начина на који продиру у ИКТ системе до начина на који уцењују жртве.

У циљу сагледавања реалних претњи у тексту смо презентовали најновије статистике и трендове са жељом да укажемо на потребу за сагледавањем реалне опасности и одабиром адекватних контрола за превенцију и отпорност на рансомер нападе.

У документу анализирамо актуелне претње и наводимо конкретне препоруке за превенцију рансомвер напада и подизање сајбер отпорности ИКТ система са идејом и циљем да организацијама помогнемо да ојачају своју сајбер одбрану од рансомвер напада, примењујући слојевите контроле и најбоље праксе усклађене са провереним стандардима који се баве овом проблематиком.

О ПРОЈЕКТУ

Овај документ израђен је у оквиру пројекта "Подршка ЕУ изградњи капацитета за сајбер безбедност Западног Балкана" и у партнерству са Националним ЦЕРТ-ом.

Пројекат "Подршка ЕУ изградњи капацитета за сајбер безбедност Западног Балкана" (пројекат "Сајбер Балкан") финансиран је од стране Европске Уније, а за циљ има побољшање отпорности корисника IPA III програма на Западном Балкану у складу са правним тековинама ЕУ и најбољим праксама. Пројекат "Сајбер Балкан" реализују Академија за е-управу (eGA, Естонија), Центар за међународну правну сарадњу (CILC, Холандија) и Национална агенција за сајбер и информациону безбедност (NÚKIB, Чешка Република), уз стручну подршку националних ЦЕРТ тимова Естоније, Летоније и Словеније.

ГЛОБАЛНИ ПРЕГЛЕД ПРЕТЊИ ОД РАНСОМВЕРА

Најважније карактеристике

Нагли пораст учесталости напада

Последњих година бележе се рекорди по обиму рансомвер активности. Анализе у индустрији указују на драстично повећање како фреквенције тако и размера напада - критични сектори као што су здравство, финансије, телекомуникације били су посебно на удару. Већина извора чије податке смо обрађивали у наставку текста указује на значајно увећане финансијске губитке и све већу ефикасност актуелних рансомвер напада.

Крађа података и „вишеструке изнуде“

Већина рансомвер инцидената, поред енкриптовања, сада укључује крађу података пошто нападачи користе украдене осетљиве податке за уцену жртава (тзв. дупла изнуда). У просеку 60% рансомвер напада забележених 2023. године укључивали су потврђену или потенцијалну крађу података. Нападачи објављују украдене податке на тзв. leak сајтовима како би извршили притисак на жртве - обим објава на овим сајтовима скочио је за 75% током 2023. у односу на претходну годину, са преко 4.500 база података жртава постављених јавно. Ова тактика повећава вероватноћу да ће организације платити, под претњом да ће поверљиви подаци (базе података клијената, интелектуална својина итд.) бити јавно објављени или продати ако се захтеви за откуп не испуне. Многе криминалне групе отишле су корак даље, ка такозваној трострукој изнуди, која додаје и трећи слој принуде - на пример, извођење DDoS напада или претњу да ће директно контактирати клијенте, партнере или регулаторе жртве уколико откупнина не буде плаћена. Забележени су и случајеви да неке рансомвер групе прескачу енкрипцију у потпуности ослањајући се искључиво на крађу података: примера ради, група Clop је злоупотребила zero-day рањивости у софтверу за дељење фајлова како би украла податке и уцењивала жртве претњом објављивања, чак и без коришћења самог малвера за шифровање. Ове нове шеме изнуда представљају претњу чак и организацијама са поузданим резервним копијама које и даље могу трпети значајне последице у случају компромитације њихових података.

Утицај на критичне секторе

Рансомвер напади настављају да се сврставају у водеће претње, како глобално тако и регионално укључујући Европу. Извештај ENISA о претњама за 2023. показује да је рансомвер био претња број 1 у ЕУ, чинећи 34% инцидената, док је нагли пораст DDoS (Distributed Denial of Service) напада почетком 2024. године променио поредак па су у извештајима из 2024. и 2025. године рансомвер и упади у систем оцењени као друга по реду претња по заступљености. Последице напада на критичну инфраструктуру показале су се тешким: на пример, напади на индустријске и комуналне организације проузроковали су прекиде у операцијама, а напади на финансијске институције и пружаоце телекомуникационих услуга испоставили су се не само као оперативне претње већ и као претње ка поверењу јавности у услуге које користе. Посматрано по секторима, рансомвер актери нису превише бирали жртве - ENISA је у свом извештају из 2025. године забележила да су производња (14,9%) и дигитална инфраструктура и сервиси

(10,3%) били најпогођенији сектори у ЕУ. Значајно је да су и владини органи и финансијске услуге често присутни у извештајима о рансомвер инцидентима. Мотивација је јасна: критични сектори представљају уносне мете (организације са значајним приходима или осетљивим подацима) и пружају потенцијал за изузетан притисак (ометање основних услуга). Примера ради, напади рансомвера на енергетски сектор расли су за 80% из године у годину, привлачећи нападаче приликама за реализацију значајних оперативних сметњи услед споријег времена опоравка у тој индустрији. У целини, протекле године су потврдиле да ниједан сектор није поштеђен - од глобалних банака до регионалних комуналних предузећа и телекомуникационих оператера, рансомвер групе настављају да циљају организације где би застој или губитак података нанели највећу штету, како би повећали изгледе за исплату откупнине.

Најактивније рансомвер групе

Akira - Ова група се брзо развија и модификује технике напада у циљу повећања ефикасности и прилагођења циљаном систему, користећи посебно развијене малвере за Windows и Linux окружења. Акира најчешће таргетира мала и средња предузећа, али изводи нападе и на велике организације. Њихове жртве најчешће припадају секторима производње, образовања, информационих технологија, здравства, финансија, пољопривреде и производње хране. Примењују широку лепезу техника у свим фазама напада (од иницијалног приступа до утицаја). Примењују и модел Ransomware-as-a-Service (RaaS).

ALPHV / BlackCat - Веома иновативан, BlackCat (такође познат и под именом ALPHV) је активан од 2021. године и користи рансомвер заснован на Rust[1]-у. Примењује модел троструке изнуде са DDoS нападима и другим претњама како би појачао притисак на жртве. Познат је по циљању правног, здравственог и малопродајног сектора. Након полицијске операције спроведене 2023. године активности ове групе значајно су смањене.

Clop - Ова група (позната и као Cl0p) специјализована за крађу података путем рансомвер напада примећена је 2019. године. У 2025. години имали су неколико великих рансомвер кампања. Као примарни вектор напада користе zero-day рањивости, а најпознатији су по коришћењу до тада непознате рањивости у MOVEit трансферу. Циљају углавном академски сектор, финансије и пружаоце софтверских услуга у Северној Америци, Европи и Аустралији.

LockBit - LockBit је први пут примећен крајем 2019. године, а 2022. године били су према броју жртава најактивнија рансомвер група и RaaS провајдер на свету.

Капацитети ове групе значајно су умањени након што је у великој међународној полицијској операцији "Кронос" у фебруару 2024. године онеспособљена примарна платформа, заплењено више од 30 сервера и ухапшено пар чланове ове групе[2]. И поред тога, LockBit остаје једна од најопаснијих рансомвер група, позната по брзом шифровању, RaaS моделу и сталној еволуцији. Често циљају владине агенције, транспортне мреже и здравствене системе.

Medusa - Први пут су примећени 2021. године. Група циља јавне институције и секторе попут едукације и здравства. За иницијални упад обично користе незакрпљене познате рањивости, али и процурелe информације о систему. Примењују дуплу изнуду и RaaS модел.

1 Програмски језик који пружа могућности компајлирања кода за примену у различитим оперативним системима

2 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

NoEscape - Релативно новија група (из 2023. године) која напада хибридна и клауд окружења. Примењују RaaS модел и сарађују са другим рансомвер групама. Примењују методу троструке изнуде уз објављивање података на свом TOR блогу. Жртве су већином из јавног, енергетског и здравственог сектора из Европе и САД.

RansomHub - Нова (први пут примећена 2024. године) и брзо растућа група осумњичена за регрутовање бивших подружница ALPHV групе. RansomHub је био укључен у нападе на здравствени сектор, академски сектор и институције локалне самоуправе. Најчешће циљају велике организације са великим захтевима за откуп. Примењују RaaS модел и у 2025. години су били међу најактивнијим групама.

Rhysida - Први пут су примећени 2023. године и постоје и данас, али са варијацијама у активностима. Примењују дуплу изнуду и RaaS модел. Познати су по томе што повећавају своју видљивост контактирањем новинара и објављивањем цурења података. Жртве Rhysida групе укључују болнице, невладине организације и субјекте локалне самоуправе, често са великим утицајем на јавност.

Royal / BlackSuit - Селективна и затворена рансомвер група, позната по прилагођеним енкрпторима и ефикасним нападима на представнике критичне инфраструктуре (углавном финансије и здравство), органа за спровођење закона и владиних система. Примењују дуплу изнуду, али не примењују RaaS модел. Активни су од 2022. године, а неки истраживачи повезују их са бившим члановима групе Conti.

Play / Playcrypt - Play је први пут примећен 2022. године, да би већ 2024. године постао једна од најактивнијих рансомвер група. Примењују модел двоструке изнуде, а карактеристично за ову групу је да након ексфилтрације и енкрипције фајлова не остављају поруку са захтевом за плаћање откупа, него имејл адресу из .de домена са инструкцијама за комуникацију. Примењују и метод додатног притиска тако што неодлучне жртве контактирају телефоном претећи да ће објавити украдене податке. Њихове жртве су већином организације које припадају критичној инфраструктури и пословни субјекти у Европи, Северној и Јужној Америци.

SafePay - Први пут примећена у другој половини 2024. године, ова група је током 2025. године била једна од најактивнијих и најопаснијих. Користе модификован LockBit рансомвер, а због ефикасности напада претпоставља се да су прилично искусни па неки истраживачи наводе могућност да су у овој групи бивши чланови LockBit и ALPHV група. Карактеристика ове групе је да изводе веома динамичне нападе са стриктним периодом од највише 24 сата између иницијалног приступа и енкрипције података на нападнутом систему, укључујући ексфилтрацију података, након чега примењују модел дупле изнуде.

Qilin - Имали су интензиван раст од првог забележеног напада 2022. године до данас. Примењују метод дупле изнуде, а познати су случајеви када су вршили додатне притиске пријавом регулатору или контактирањем клијената. Најчешће циљају здравствени и финансијски сектор, а жртве су најчешће из САД. Примењују RaaS модел.

INC Ransom - Ова група је релативно новија (примећена 2023. године). Познати су по софистицираним циљаним нападима на корпоративне мреже. Примењују дуплу изнуду и RaaS модел. Најчешће мете су им у секторима здравства, едукације, технологије и јавне управе, а више од половине жртава је из САД, Канаде и Немачке.

DragonForce / Cartel - Ова група је први пут детектована 2023. године. Примењују RaaS модел и отворени су за сарадњу са другим групама, нудећи напредне технике укључујући BYOVD (Bring Your Own Vulnerable Driver). Нису посебно оријентисани на одређене секторе, а у 2025. години забележен је раст њихових активности.

BlackBasta - Примећени су 2022. године, а постоји могућност да је група настала од бивших чланова групе Conti. Примењују дуплу изнуду и RaaS модел. Жртве припадају различитим секторима (углавном производња, грађевинарство, здравсто и јавна управа), већином из САД и Европе. До 2024. били су међу најактивнијим групама, након чега се бележи смањење активности.

Conti - Ова група више не постоји, али је сматрана за једну од најсофистицираних рансомвер група, а технике, тактике и процедуре (TTP) које су примењивали и даље су у употреби. Група се распала 2022. године након интерног цурења података. Сматра се да су бивши чланови ове групе сада у другим тренутно активим групама као што су Akira, BlackBasta, BlackSuit и Royal.

Извори: Swiss Cyber Institute[3] и CISA[4]

СТАТИСТИКА РАСНОМВЕРА НАПАДА У СВЕТУ И ЕУ

Рансомвер, као један од најопаснијих типова сајбер напада, заступљен је у готово свим статистичким публикацијама из области сајбер безбедности и анализиран је у мањој или већој мери. Посебна специфичност везана за статистику рансомвер напада је што стварни ефекти могу бити обрађени само у случају да организација која је жртва напада те податке учини доступним. Да је нека организација била жртва рансомвер напада не мора никада постати јавно познато ако је напад био малог обима након чега су подаци успешно враћени из бекапа, ако нападачи нису урадили ексфилтрацију података или ако су уредно доставили кључ за декрипцију након што је организација платила откуп. Ако је и познато да је организација претрпела рансомвер напад, често се не објављују стварне последице напада и колико је података трајно изгубљено. Чак и ако нападачи објаве информације о успешном нападу и део преузетих података на свом leak сајту, не може се са сигурношћу знати шта се десило са осталим украденим подацима и да ли је након тога организација платила откуп.

Све ове непознанице чине статистичке податке о рансомвер нападима релативно поузданим, али се може сматрати да успешно показују статистичке трендове.

У нашем прегледу статистике фокусирали смо се на неколико публикација:

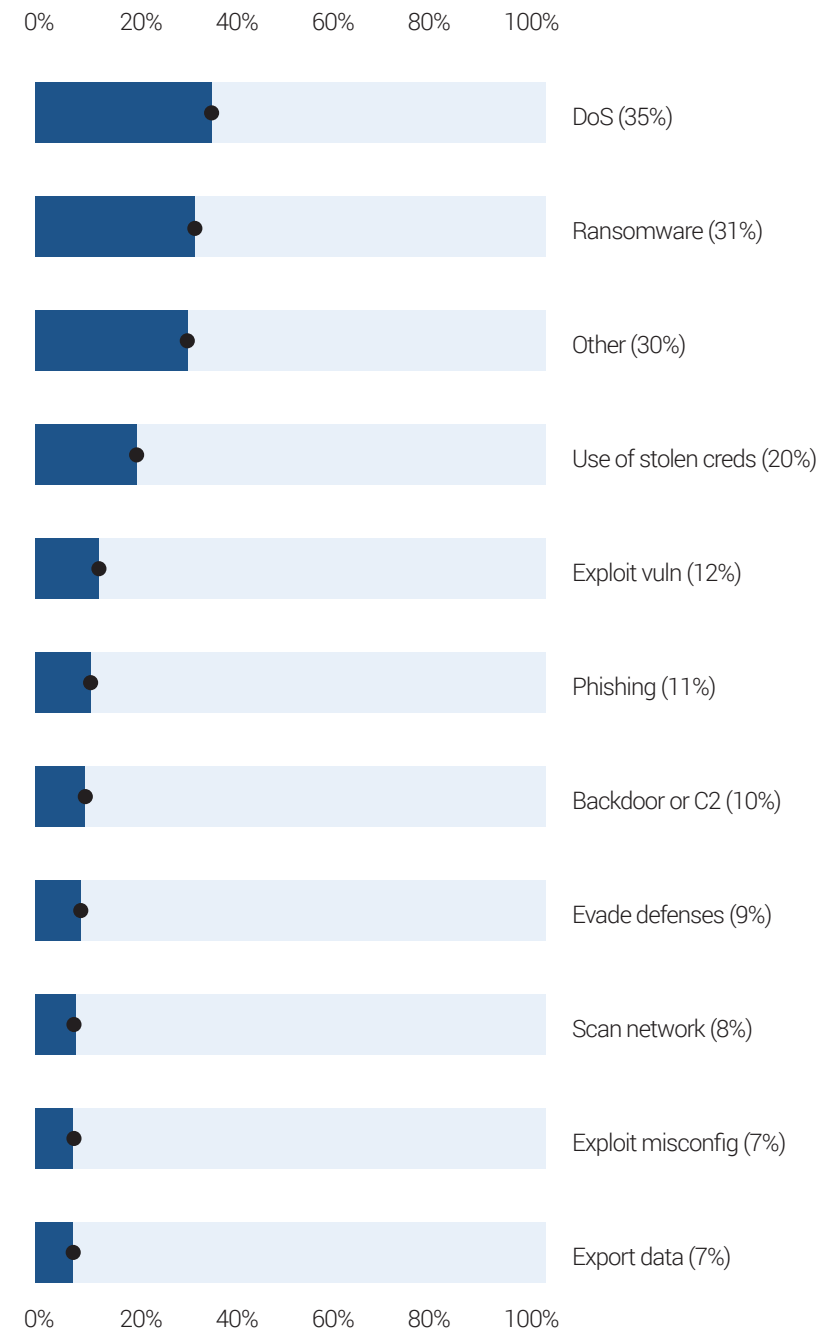
- ENISA Threat Landscape (ETL), коју годишње објављује Агенција ЕУ за сајбер безбедност,

- Data Breach Investigations Report (DBIR), коју годишње објављује компанија Verizon,

-годишњи извештаји Националног ЦЕРТ-а Републике Србије о статистичким подацима о свим инцидентима у ИКТ системима од посебног значаја.

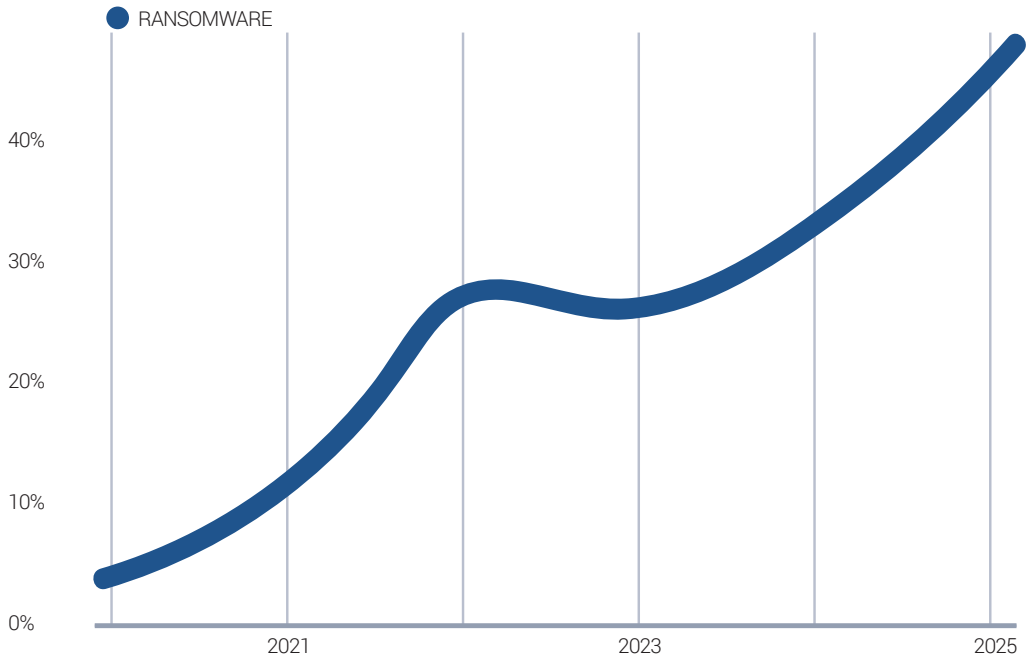
3 https://swisscyberinstitute.com/blog/10-most-notorious-ransomware-groups-2025/
4 https://www.cisa.gov/stopransomware/stopransomware

Према подацима које је у својој публикацији објавила компанија Verizon, базираним на анализи 22052 сајбер инцидента од којих су 12195 упади у систем са потврђеном крађом података, приметан је тренд раста броја рансомвер напада у последњих неколико година. Анализе су показале да је рансомвер као компонента у 2025. години био присутан у чак 31% инцидената, што представља велико повећање у односу на 14% претходне године. Оваква учесталост поставила је рансомвер нападе на друго место по бројности, одмах иза DoS напада.



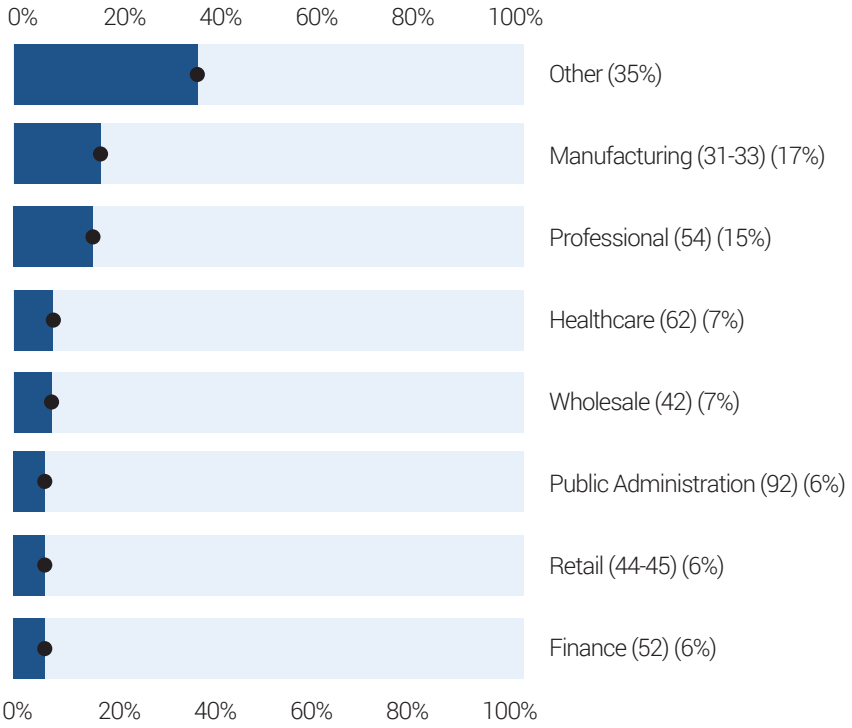
Слика 1: идентификоване компоненте у сајбер инцидентима (извор: Verizon 2025 DBIR)

Посматрајући одвојено упаде у ИКТ систем, у 2025. години рансомвер компонента забележена је у чак 44% случајева, што је такође значајно повећање у односу на 32% претходне године. Приликом анализе напада уочена је значајна разлика у односу на величину субјекта – у већим организацијама, рансомвер је био компонента у 39% упада, док су мала и средња предузећа имала упаде повезане са рансомвером у 88% случајева.



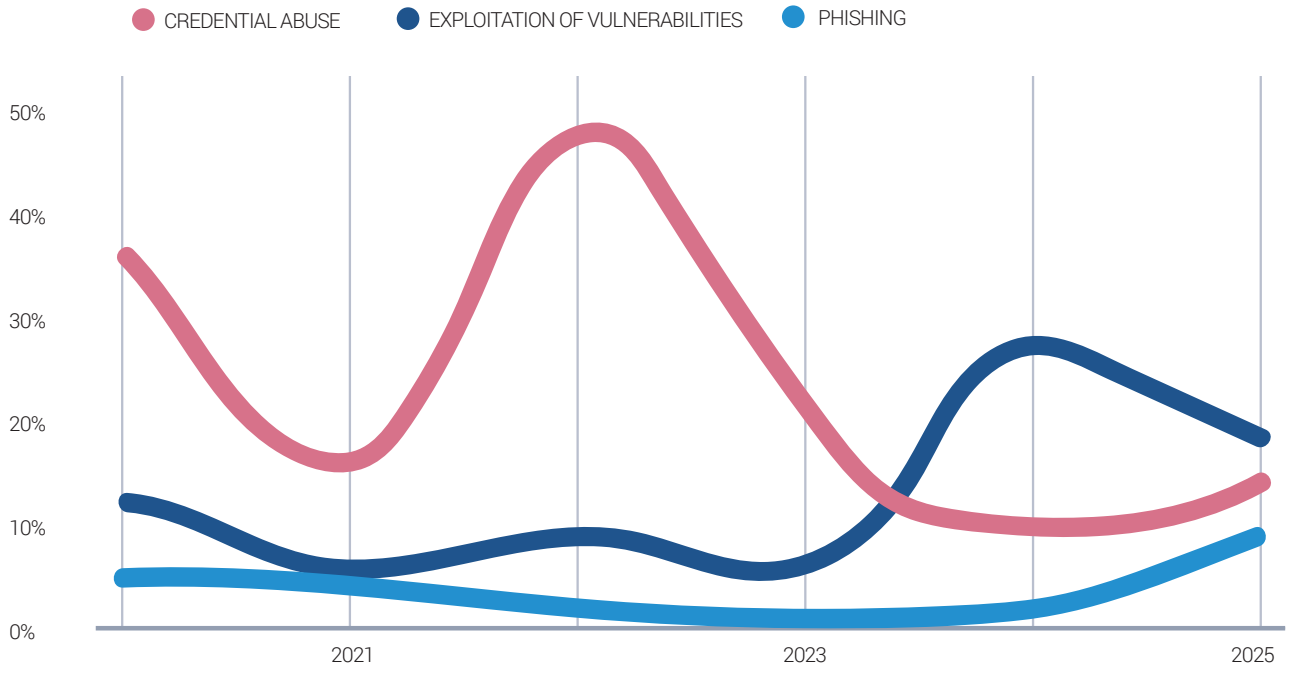
Слика 2: рансомвер компонента у укупном броју упада у ИКТ систем (извор: Verizon 2025 DBIR)

Рансомвер напади не заобилазе ни један сектор. Ипак, у нешто већем проценту забележени су напади на производњу и професионалне сервисе.



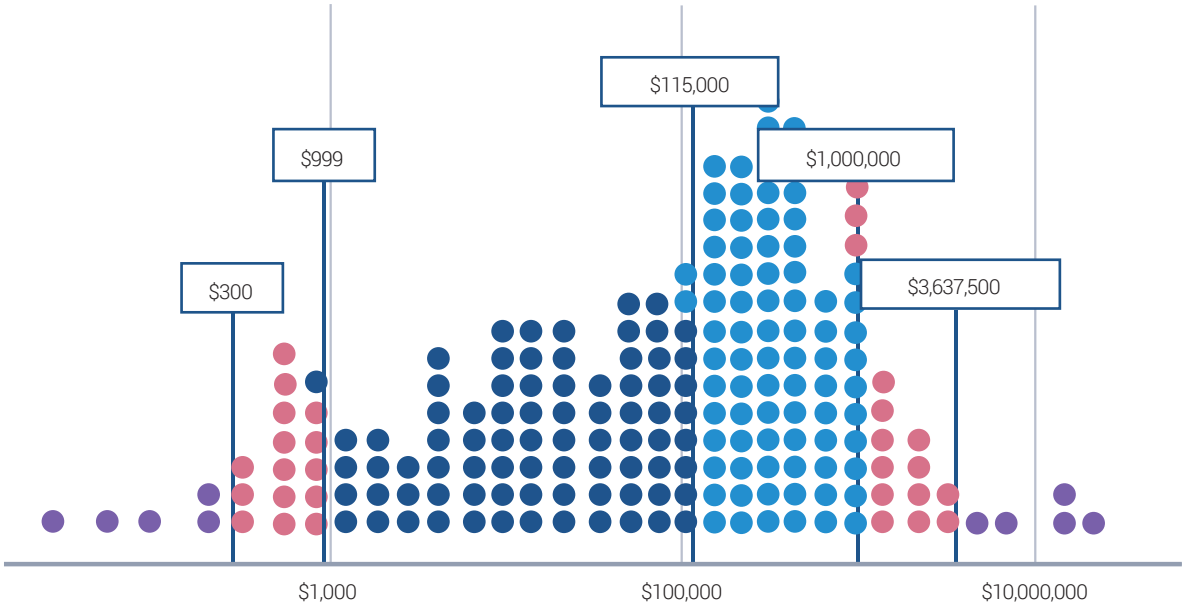
Слика 3: сектори погођени рансомвер нападима (извор: Verizon 2025 DBIR)

У последњих пар година приметан је пораст процентуалног удела експлоатације рањивости као иницијалног вектора напада уз смањење удела злоупотребе креденцијала. Ипак, људски фактор остаје свеукупно доминантан за омогућавање приступа нападачима.



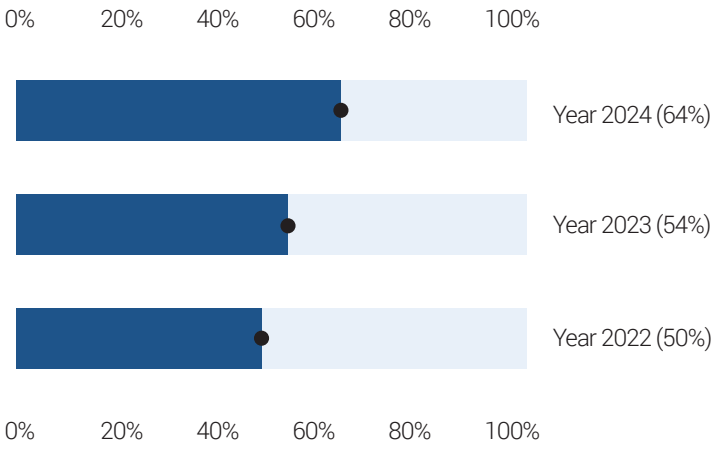
Слика 4: иницијални вектор приступа за рансомвер нападе (извор: Verizon 2025 DBIR)

У публикацији Verizon 2025 DBIR приказани су и резултати анализе откупа плаћених након рансомвер напада. Подаци за 2024. годину показују велике разлике у износима плаћених откупа, а средња вредност исплаћене откупнине била је 115.000 долара (што је мање од 150.000 долара колика је била средња вредност исплаћене откупнине 2023. године, али знатно више од 73.500 долара из 2022. године).



Слика 5: плаћени откупи (извор: Verizon 2025 DBIR)

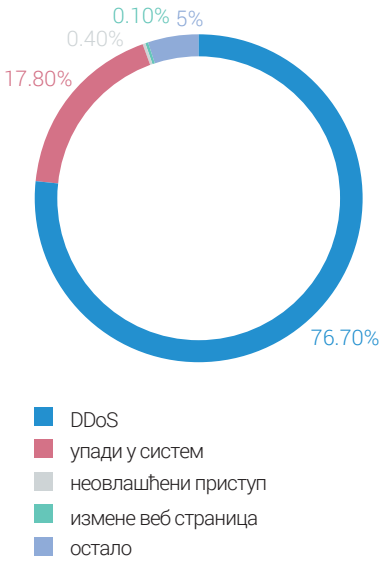
Ипак, и поред значајног повећања броја напада, приметно је и да се повећава проценат организација које одбијају да плате откуп. Ово може бити последица боље припремљености оргаизација на овакве врсте напада, али и других фактора (на пример, већег неповерења према обећањима нападача).



Слика 6: проценат организација које су одбиле да плате откуп (извор: Verizon 2025 DBIR)

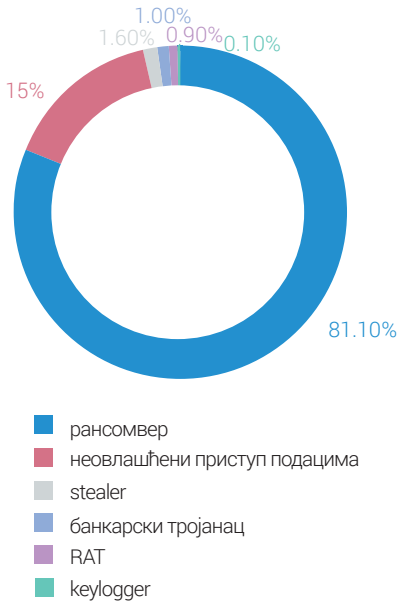
У публикацији ENISA Threat Landscape Report статистички су обрађени извештаји о инцидентима у земљама чланицама и институцијама ЕУ. Према овим извештајима, упади у систем били су друга најзаступљенија категорија напада, а рансомвер компонента идентификована је као најприсутнија у овој категорији напада (треба имати у виду да је рансомвер компонента заступљена и у мањем броју DDoS напада).

Најчешћа мета у 2025. години био је јавни сектор на који се односи чак 38,2% свих анализираних напада. Ово је велико повећање у односу на 2024. годину када је јавни сектор био мета у 19% случајева. Највећи утицај на оволико повећање имао је значајан раст броја DDoS напада и то баш на јавни сектор у ЕУ, чинећи да овај тип напада буде свеукупно доминантан са 76,7% од свих забележених напада[5].



Слика 7: заступљеност најчешћих категорија напада (извор: ETL 2025)

5 Занимљиво је да велика већина DDoS напада потиче од хактивиста, док су криминалне групе ретко изводиле овакве нападе и то углавном у сврху повећања притиска након рансомвер напада

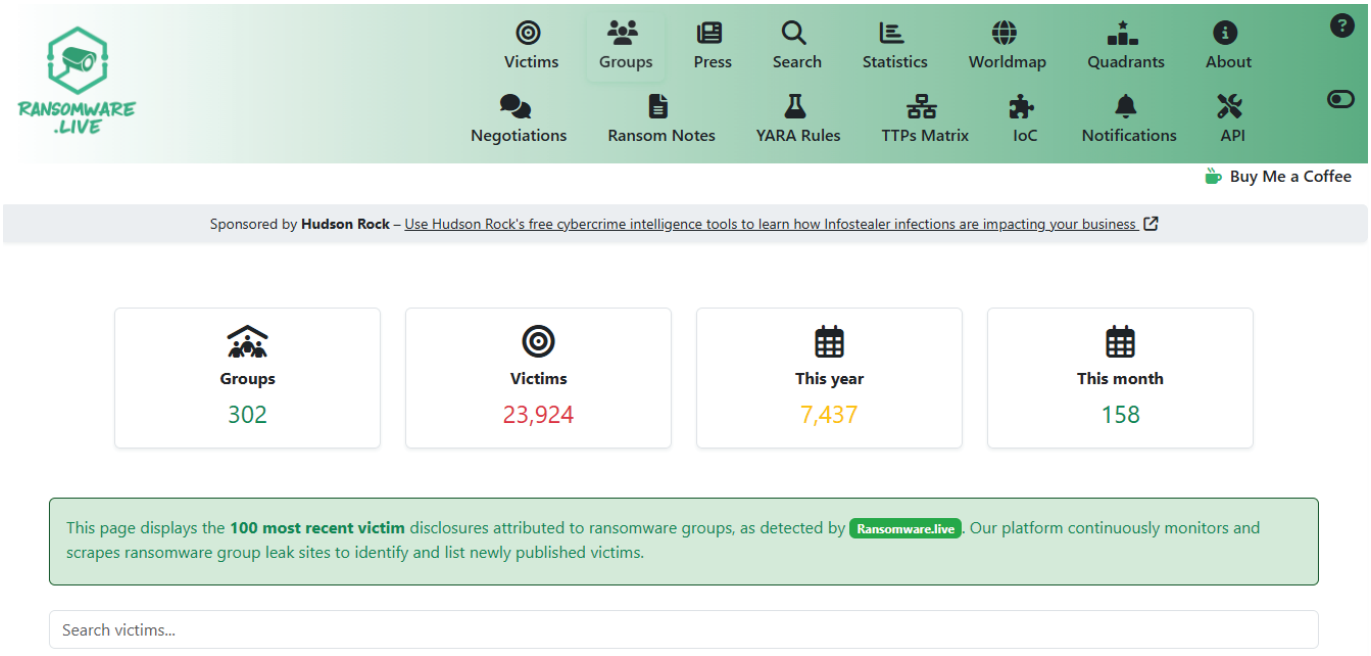


Слика 8: заступљеност категорија напада који спадају у сајбер криминал (извор: ETL 2025)

Рансомвер напади су са преко 81% најзаступљенији од категорија напада који спадају у сајбер криминал. У 2025. години идентификоване су 82 различите варијанте рансомвера, а доминантни су Akira, SafePay, Qilin, Play, Cl0p и INC Ransom. Рансомвер LockBit, који је био доста заступљен претходних година, идентификован је у веома малом броју напада 2025. године.

УВИД У РАНСОМВЕР ГРУПЕ И ЖРТВЕ

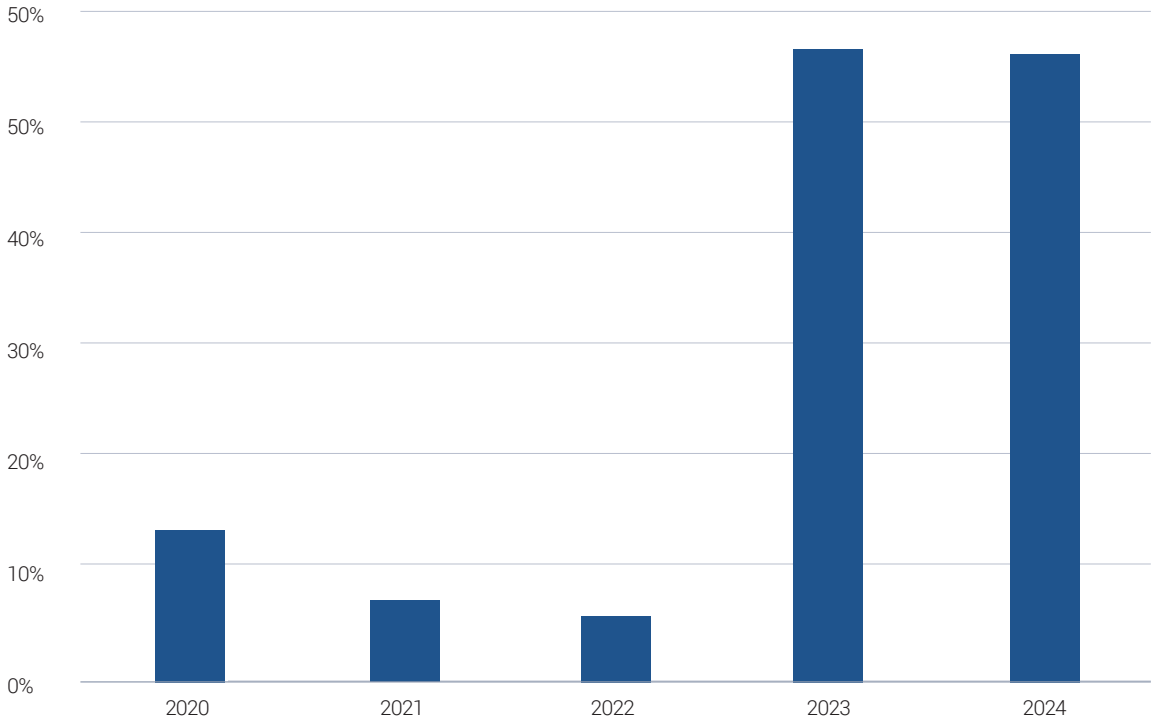
Сајт ransomware.live (приватни пројекат Julien Mousqueton) даје тренутни увид у жртве различитих рансомвер група, географску распрострањеност жртава, детаље трагова које остављају различите групе и др.



Слика 5: плаћени откупи (извор: Verizon 2025 DBIR)

СТАТИСТИКА РАСНОМВЕРА НАПАДА У РС

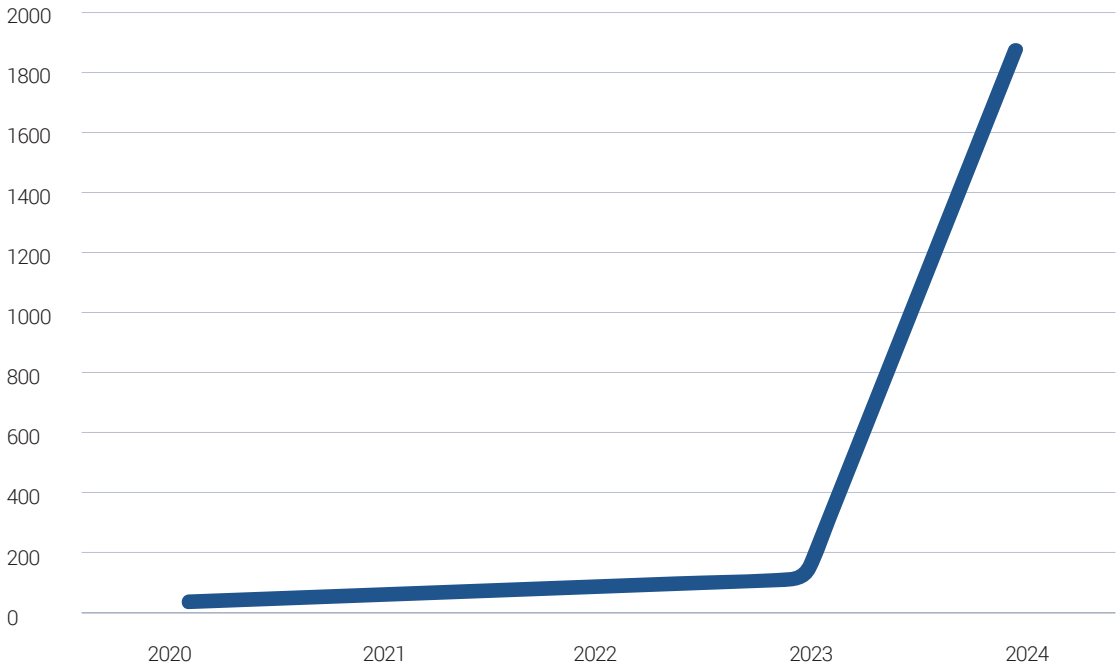
У складу са Законом о информационој безбедности, ИКТ системи од посебног значаја[6] имају обавезу да Националном ЦЕРТ-у доставе податке о свим инцидентима у ИКТ системима од посебног значаја за претходну годину, а Национални ЦЕРТ има обавезу да извештај о статистичким подацима о свим инцидентима јавно објави. Према подацима из ових извештаја, који се објављују једном годишње, може се приметити огроман пораст броја пријављених инцидената од 2023. године, за шта је директан узрок повећање пријављених инцидената у групи неовлашћено прикупљање података.



Слика 10: број пријављених инцидената у ИКТ системима од посебног значаја (извор: Национални ЦЕРТ)

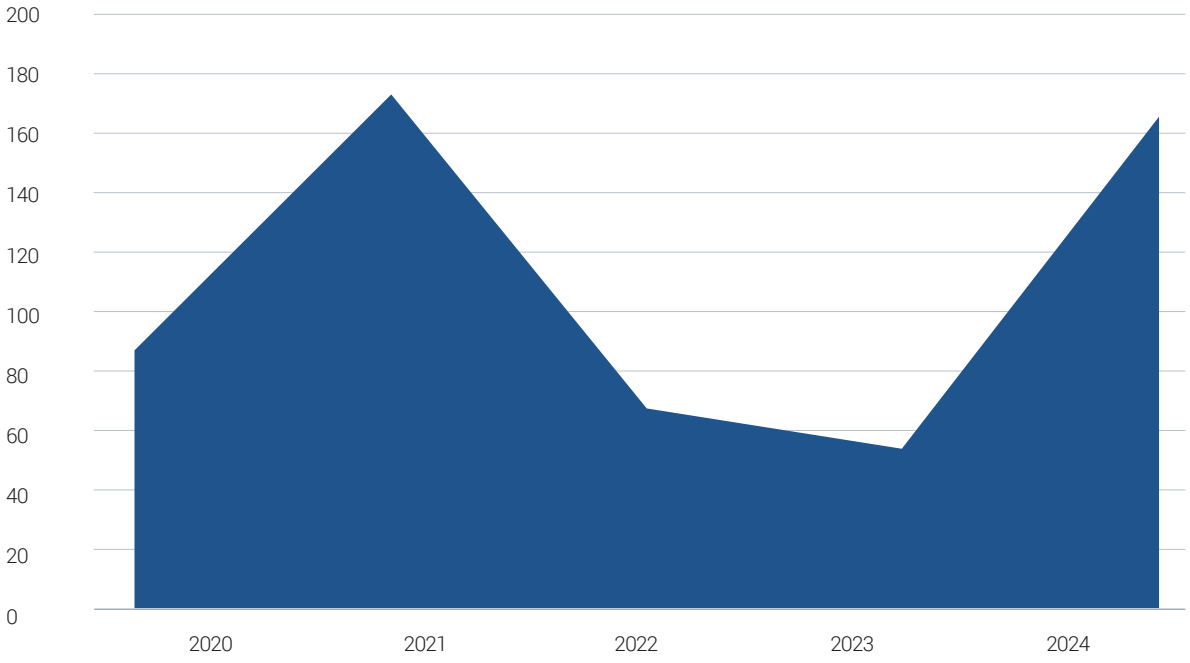
Највећи број пријављених инцидената у групи неовлашћено прикупљање података спада у категорију скенирања портова, док је број инцидената у категорији компромитовања или цурења података (data breaches) занемарљив у односу на укупан број инцидената у овој групи. Ипак, подаци показују да је у 2024. години дошло до великог раста броја инцидената који спадају у категорију компромитовање или цурење података.

6 ИКТ системи од посебног значаја су ИКТ системи који су од кључног значаја за одржавање критичних друштвених и економских активности чији би прекид или поремећај у пружању услуга имао или могао да има значајан утицај на јавну безбедност, јавно здравље, функционисање других сектора или би створио односно могао да створи значајан системски ризик (члан 5. Закона о информационој безбедности)



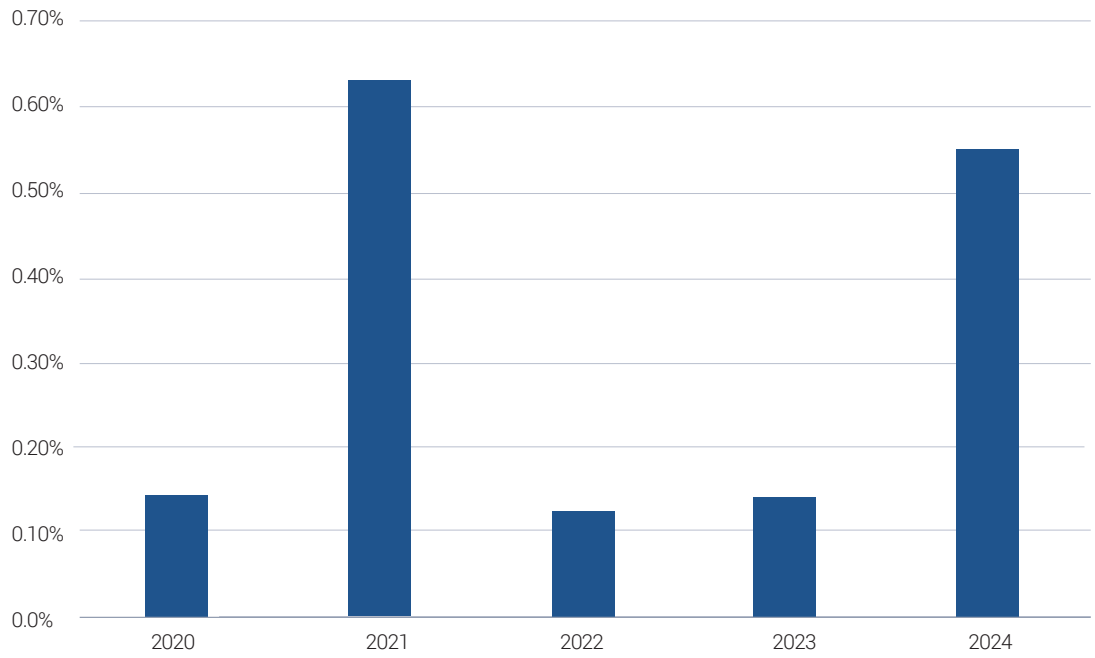
Слика 11: број пријављених инцидената у категорији компромитовање или цурење података (извор: Национални ЦЕРТ)

Када је реч о пријављеним рансомвер нападима, постоје значајне разлике по годинама и са доступним подацима није могуће утврдити јасан тренд, али последње године (2024.) забележено је повећање броја напада у овој категорији од чак три пута у односу на претходну годину. Ипак, треба напоменути да рансомвери сваке године имају удео мањи од 1% у односу на укупан број пријављених малвера.



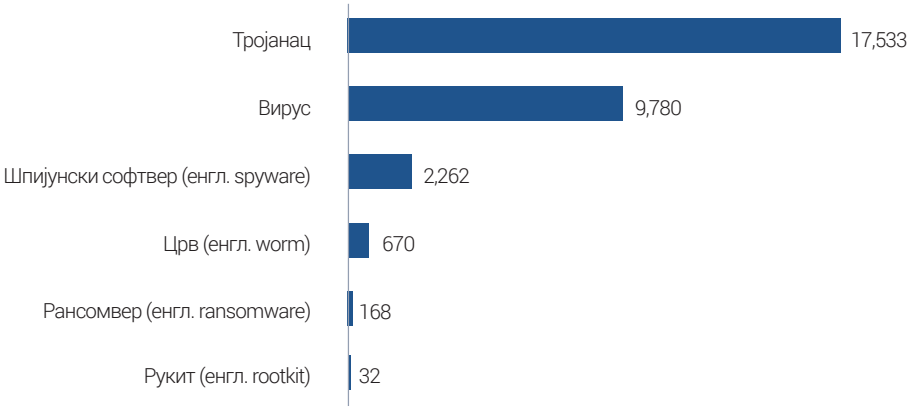
Слика 12: број пријављених рансомвера (извор: Национални ЦЕРТ)

Највећи број пријављених инцидената у групи неовлашћено прикупљање података спада у категорију скенирања портова, док је број инцидената у категорији компромитовања или цурења података (data breaches) занемарљив у односу на укупан број инцидената у овој групи. Ипак, подаци показују да је у 2024. години дошло до великог раста броја инцидената који спадају у категорију компромитовање или цурење података.



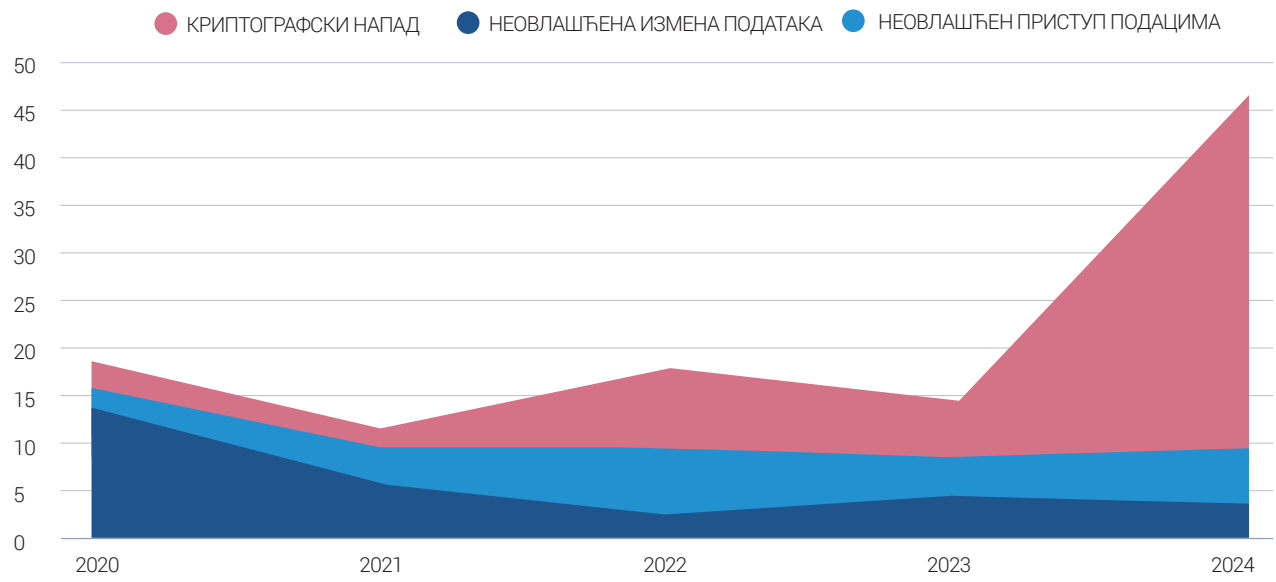
Слика 13: удео рансомвера у укупном броју пријављених малвера (извор: Национални ЦЕРТ)

Према подацима Националног ЦЕРТ-а у оквиру групе инцидената „Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. malware)", током извештајног периода регистровано је укупно 30.445 случајева. Највећи број инцидената односи се на тројанце (17.533) и вирусе (9.780), док су шпијунски софтвер (2.262) и црви (670) мање заступљени. Рансомвер (168) и руткит (32) чине најмањи део укупног броја, али представљају висок ризик по безбедност и интегритет система.



Слика 14: регистровани малвери (извор: Национални ЦЕРТ)

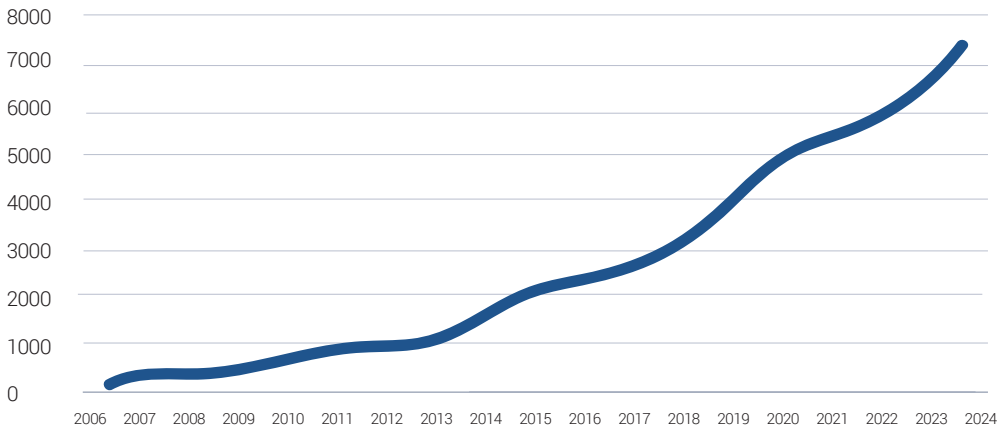
Последице рансомвер напада могу спадати у групу угрожавање безбедности података, у коју су сврстани инциденти категорија неовлашћен приступ подацима, неовлашћена измена или брисање података и криптографски напад. Достављени подаци показују да и у овој групи инцидената постоји приметан раст последњих година.



Слика 15: инциденти у групи угрожавање безбедности података по категоријама (извор: Национални ЦЕРТ)

Националном ЦЕРТ-у Републике Србије пријављено је пет рансомвер напада у прва три квартала 2025. године и четири у току 2024. године. Нападачи су користили SMOK рансомвер, Crypto 24, DragonForce рансомвер Cartel, Medusa Locker и Rapid1 рансомвере. У већини случајева се десило да антивирусни софтвер није детектовао напад, док је квалитетан бекап у већини случајева омогућио да се пословање настави (business continuity) без већих последица по институцију која је доживела напад.

У складу са светским трендовима, и у Србији се константно бележи повећање броја кривичних дела из области високотехнолошког криминала. Према подацима Посебног одељења за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду, у 2024. години заведено је 7198 предмета из ове области што представља повећање од 10,31% у односу на претходну годину.



Слика 16: пораст броја предмета по годинама (извор: Програм борбе против високотехнолошког криминала за период 2026-2030)

Слика 17: захтеви тужилаштва према МУП у 2024. години (извор: МУП Р. Србије)

Служба за борбу против високотехнолошког криминала током 2024. године примила је 2467 захтева за прикупљање обавештења, што представља повећање од око 22% у односу на 2023. годину и чак око 59% у односу на 2022. годину.

Из домена кривичних дела против безбедности рачунарских података, најбројнија категорија су неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података, а затим следе рачунарска саботажа и рачунарска превара. Рансомвер није заступљен као посебна категорија, али је у Програму борбе против високотехнолошког криминала за период 2026-2030[7] препознат као изузетно опасан, са трендом повећања броја и софистицираности и све веће присутности ексфилтрације података и двоструке изнуде.

АНАЛИЗЕ РАСНОМВЕР НАПАДА

Модерни рансомвер напади одвијају се кроз више фаза у којима нападачи прво продру у мрежу, затим шире свој приступ (ескалирају привилегије и крећу се латерално кроз систем) са циљем идентификације и ексфилтрације података, да би се на крају окренули процесу енкрипције као припреме за даље изнуде. Упркос појачаним акцијама органа гоњења - почетком 2024. године спроведено је више глобалних акција против рансомвер група (укључујући операције против доминантног LockBit-a и BlackCat-a) - уцене путем рансомвера достигле су рекордан ниво.

Уобичајени почетни вектори упада

Нападачи најпре траже начин да остваре иницијални упад у циљану организацију. У наставку су описани најчешћи вектори почетног компромитовања ИКТ система.

Фишинг и социјални инжењеринг

Слање убедљивих фишинг мејлова са злонамерним прилозима или линковима и друге облике обмане корисника (нпр. телефоном или SMS-ом) ради крађе креденцијала. Ово остаје традиционални метод напада у коме се жртве наводе да саме "отворе врата" нападачима.

Компромитовани или процурели креденцијали

Коришћење украдених лозинки и налога (нпр. купљених од група специјализованих за продају украдених креденцијала, познатих под заједничким називом Initial Access Brokers) за легитимно пријављивање на систем. Рансомвер групе често купују од ових специјализованих група већ успостављене приступе у ИКТ системима жртава. Такође, слабе лозинке на изложеним сервисима (Remote Desktop Protocol, VPN и сл.) омогућавају нападачима да се директно улогују.

7 https://www.mup.gov.rs/wps/wcm/connect/e59cd9f7-203e-4ccc-b2f5-d0488e3407b5/cirprogram+borbe+protiv+visokotehnoloskog+kriminal-a+za+period+2026+–+2030+sa+akcionim+planom+2026+–+2028.pdf?MOD=AJPERES&CVID=pD8FumC

Експлоатација рањивости (укључујући zero-day рањивости)

Све више напада почиње искоришћавањем познатих безбедносних пропуста у интернет-експонираним системима организације. У 2023. и 2024. години уочен је тренд да рањивости престижу фишинг као водећи узрок иницијалног упада. Примери обухватају рањивости VPN уређаја (нпр. Fortinet SSL VPN, Citrix ADC), имејл сервера (Microsoft Exchange) и алата за трансфер фајлова. Рансомвер групе ефикасно користе zero-day пропусте у широко коришћеним софтверима како би постигле масовни продор - нпр. Cl0p је 2023. искористио zero-day у MoveIt софтверу за пренос датотека, притом проваливши у стотине организација из којих су успели да украду осетљиве податке пре него што су у последњој фази напада активирали рансомвер софтвер за енкрипцију.

Напади на ланац снабдевања

На мети нападача све више су и посредници - провајдери ИТ услуга или софтверски добављачи - како би се преко њих компромитовало више жртава одједном. Овај метод је ређи од горенаведених, али има разоран домино-ефекат у случају успеха.

Искоришћавање постојећих жртава

Неке нападачке групе преузимају наставак напада на мреже које су већ угрожене од стране других злонамерних актера. Куповином приступа од криминалних посредника (гореспоменутих Initial Access Brokers), они прескачу почетно хаковање и директно настављају са злоупотребом већ компромитованог ИКТ система жртве.

Латерално кретање и ескалација привилегија

Након што остваре почетни приступ, нападачи настоје да прошире своје присуство у мрежи жртве. Циљ латералног кретања је преузимање контроле над што више критичних система, укључујући домен контролере и сервере са осетљивим подацима, како би финални удар (шифровање и изнуда) имао максималан ефекат. Технике латералног кретања (ширења са једног компромитованог система на други) обично су тесно испреплетане са техникама ескалације привилегија (стицања виших нивоа овлашћења, нпр. администраторских). Неке од најзаступљенијих тактика укључују:

Крађа креденцијала и злоупотреба легитимних налога

Нападачи издвајају приступне податке (лозинке, хешеве) са компромитованих машина помоћу алата као што је Mimikatz (очитавање меморије процеса LSASS) или пресретањем keylogger-има. Украдени валидни налози се затим користе за ширење приступа на друге системе у домену.

Коришћење регуларних алата (Living off the Land)

Масовно коришћење легитимних администраторских алата и сервиса оперативног система ради неупадљивог кретања кроз мрежу. Уобичајено се злоупотребљавају Windows алати попут PowerShell-a, WMI команди и сродних скрипти, јер њихово покретање не изазива сумњу као што би је изазвао потпуно страни извршни фајл. Нападачи преко командне линије извршавају команде за скенирање мреже, кретање и припрему терена за енкрипцију, маскирајући се иза уобичајених администраторских активности.

Коришћење легитимних алата за даљинско администрирање

Осим системских алата, често се инсталирају и злоупотребљавају комерцијални алати за даљински приступ и менаџмент, попут TeamViewer, AnyDesk, Atera, Splashtop и сл. Они омогућавају нападачима даљински надзор и контролу над више машина одједном, понекад чак и преко легитимних VPN конекција жртве.

Коришћење алата за командно-контролни (C2) упад и кретање

Многе групе након иницијалног упада у систем жртве инсталирају сопствене малвер алате ради поузданије контроле и кретања. На пример, широко је раширена употреба Cobalt Strike beacon-а који омогућава даљинско извршавање команди, keylogging, ексфилтрацију података и сл. Такви оквири за напад дају нападачима флексибилност да инсталирају додатне модуле (нпр. рансомвер) на више машина истовремено.

Експлоатација унутрашњих рањивости

Ако су почетно ушли на један сервер, нападачи ће затим тражити рањивости у остатку инфраструктуре. Честа мета су неажурирани сервери и сервиси у локалној мрежи - на пример, старији Windows сервери, VMware ESXi хипервизори, NAS уређаји, менаџмент системи као што је Zoho ManageEngine и др. Искоришћавањем локалних пропуста нападачи могу добити приступ администраторским привилегијама или другим сегментима мреже који иницијално нису били доступни.

Кретање преко Remote Desktop-а и дељених ресура

Традиционално, након крађе администраторских креденцијала, нападачи се повезују на друге машине путем RDP-а (пун интерактивни приступ) или извршавају команде на даљину кроз алате попут PsExec (Microsoft Sysinternals) и WMIC. Ово им омогућава да ручно или аутоматизовано дистрибуирају рансомвер на више система у домену. На пример, група Play је позната по томе да након крађе домен администраторских привилегија дистрибуира извршне фајлове рансомвера преко Group Policy објеката на све рачунаре у домену, чиме оркестрира симултано покретање енкриптовања широм мреже.

Деактивација безбедносних механизама

У припреми завршне фазе, многи нападачи покушавају да онемогуће сигурносни софтвер и бекап системе. То укључује гашење антивирус програма, деинсталацију или онемогућавање EDR агената, брисање логова, па чак и уништавање shadow copies (Windows VSS) да би се онемогућило враћање система на претходно стање. На пример, LockBit и слични рансомвери имају скрипте које аутоматски гасе услуге за бекаповање, антивирусе и бришу резервне копије пре покретања шифровања.

Комбинацијом наведених техника, нападачи настоје да се крећу „испод радара“ кроз мрежу жртве, постепено преузимајући контролу над кључним системима. Коначни циљ је да пре фазе енкрипције имају максималну контролу - нпр. да поседују домен администраторске креденцијале и да су позиционирани на свим серверима на којима се налазе критични подаци.

Фазе изнуђивања и технике притиска

Када је инфраструктура жртве довољно компромитована, почиње завршна фаза напада - изнуђивање откупнине. Савремени напад готово увек укључује двоструко изнуђивање: пре него што се активира рансомвер (енкрипција фајлова), нападачи неауторизовано преузимају осетљиве податке из мреже жртве. Такви подаци служе као додатан елемент за уцену - ако жртва одбије да плати откуп, криминалци прете да ће украдене информације објавити или продати. Већина водећих група води своје веб сајтове на darknet-у (тзв. Leak Site) где објављују имена жртава које су одбиле да плате откупнину као и узорке њихових поверљивих података како би их додатно уценили.

Након ексфилтрације, покреће се малвер који енкриптује фајлове по читавој мрежи - ово је класична уцена закључавањем података. Рансомвер обично оставља упутство (откупни захтев) са информацијом како да жртва ступи у контакт са нападачима и уплати откупнину у криптовалути у замену за кључ за дешифровање. Време је у овом процесу веома битан фактор - нападачи често прете да ће после истека неког рока објавити све украдене податке или уништити кључ.

Последњих година, неке групе су отишле и корак даље у ескалацији притиска, прелазећи на троструко изнуђивање. Поред шифровања и претњи објавом података, додаје се још један вид принуде - на пример, покретање Distributed Denial-of-Service (DDoS) напада на јавне сервисе жртве или директно контактирање њених клијената, партнера и медија са обавештењем о хаковању. Група LockBit 3.0 била је пионир ове тактике у 2022/2023. години, комбинујући шифровање, крађу података и DDoS напад како би појачала притисак на велике компаније да плате откуп. Слично томе, забележено је да неки актери телефоном или имејлом директно уцењују руководиоце жртве или њене партнере, не би ли изнудили плаћање.

Након иницијалног напада, следи фаза преговора (уколико жртва одлучи да преговара). Комуникација се одвија преко анонимних канала (нпр. преко TOR chat портала које група постави, или преко енкриптованих имејл адреса). Нападачи обично демонстрирају дешифровање мањег фајла као „доказ исправности“ кључа и траже суму која зависи од процене платежне моћи жртве (нпр. процурели финансијски извештаји, величина компаније итд.).

СТРАТЕШКА ОДБРАНА ОД РАНСОМВЕРА

Да би се ефективно спречили и ублажили рансомвер напади, организације би требало да усвоје слојевиту стратегију одбране ИКТ система која покрива све релевантне захтеве - од основне сајбер хигијене до напредне детекције претњи и одговора на инциденте. Уместо ад-хок мера, ослањање на проверене оквире за сајбер безбедност гарантује свеобухватни приступ. Конкретно, поред 37 мера које прописује Закон о информационој безбедности (СГ РС 91/25), усклађивање са смерницама светски признатих организација препорука је за адекватну заштиту ваших ИКТ система. Смернице које доноси организација NIST, Cybersecurity Framework (CSF), нуде добро познату структуру базирану на елементима за организовање контрола (Идентификација, Заштита, Детекција, Одговор и Опоравак), а коју смо искористили за дефинисање смерница у овом документу. Поред овог документа препоруке смо ускладили и са смерницама за рансомвер (NISTIR 8374) које је објавила иста организација које усклађују циљеве превенције и ублажавања последица рансомвер напада са функцијама CSF оквира. Такође, одличан извор савета и конкретних препорука можете пронаћи у документу Центра за интернет безбедност (Critical Security Controls v8 CIS) који дефинише приоретизован сет најбољих пракси за одбрану од сајбер напада а на чије ћемо се савете такође осврtати у наставку документа.

Поред горенаведенога, смернице и прописи специфични за поједине секторе све више захтевају од организација да имплементирају наведене најбоље праксе. На пример, Директива NIS2 ЕУ (Directive (EU) 2022/2555) налаже да „есенцијални и важни субјекти" у критичним секторима (енергетика, транспорт, финансије, здравство, телекомуникације итд.) усвоје низ мера за управљање ИКТ ризицима - укључујући руковање инцидентима, планове континуитета пословања, безбедност ланца снабдевања, енкрипцију и контролу приступа. Национални органи и CERT-ови такође редовно објављују смернице фокусиране на рансомвер, које упућују на сличне превентивне мере.

У Републици Србији је у октобру 2025. године усвојен нови Закон о информационој безбедности који између осталог доноси нове контролне мере, предвиђа формирање Канцеларије за информациону безбедност и дефинише нове обавезе за операторе ИКТ система од посебног значаја. Са друге стране, неки сектори попут финансијског су већ одавно уређени посебним прописима (нпр. Одлука НБС о минималним стандардима за управљање информационо-комуникационим системима финансијских институција) који прате светске трендове и нову регулативу попут Digital Operational Resilience Act (DORA).

Идентификација - познавање својих средстава, рањивости и ризика

Функција идентификације усмерена је на успостављање видљивости над окружењем и креирање свести о сопственом профилу ризика. Кључне мере у фази идентификације ради заштите од рансомвера обухватају:

Инвентар имовине (хардвер и софтвер)

Одржавајте ажурирани попис свих система, уређаја и апликација на вашој мрежи. Тај инвентар треба да садржи детаље попут верзија софтвера и нивоа закрпа. Свеобухватно управљање средствима представља темељ, јер вам омогућава да брзо утврдите који системи могу бити погођени новом рансомвер претњом или који захтевају хитно инсталирање закрпа због одређене рањивости. NISTIR 8374 публикација наглашава да детаљан хардверски инвентар помаже опоравак (знајући шта све треба обновити

након напада), а да софтверски инвентари помажу да се прецизира који системи могу имати рањивост коју би рансомвер могао да искористи. У пракси, користите алате за аутоматско праћење уређаја и апликација и класификујте системе према критичности (како бисте могли приоритизовати заштиту и резервне копије за најважнија средства).

Идентификација критичних података и највреднијих средстава („crown jewels“)

Одредите који су подаци, апликације и услуге од пресудног значаја за ваше пословање или би вашој организацији била нанета највећа штета ако би били мета рансомвер напада или подаци процурели у јавност. То могу бити базе података корисника, системи за финансијске трансакције, индустријски контролни системи (ICS) итд. Креирањем дијаграма токова података и зависности (NIST ID.AM-3) можете разумети где би напад рансомвера нанео највише штете по вашу организацију.

Процена ризика и информације о претњама

Спроводите редовне процене ризика које обухватају сценарије рансомвер напада - на пример: какав би био утицај да је наша кључна база података шифрована и недоступна? Процените не само последице по ИКТ системе, већ и утицај на континуитет пословања. Будите информисани о актуелним тактикама рансомвер група које циљају ваш сектор (извештаји о информација о претњама (threat intelligence reports) или ISAC платформе за размену информација могу ово пружити). За потребе ИКТ система од посебног значаја Национални ЦЕРТ је успоставио MISP платформу за размену информација о претњама, за коју можете затражити приступ уколико припадате категорији ИКТ система од посебног значаја. Многи рансомвер напади користе познате слабости (незакрпљене сервере, погрешне конфигурације итд.), па спроводите проактивне провере рањивости како бисте идентификовали те пропусте. Размотрите коришћење алата или оквира за самопроцену спремности на рансомвер - на пример, организције CISA и MS-ISAC пружају алате за самопроцену, а NISTIR 8374 профил може се користити да измерите ваше тренутно стање у односу на жељено циљно стање. Уколико припадате ИКТ системима од посебног значаја можете затражити приступ Платформи за пружање раних упозорења Националног ЦЕРТ-а на којој можете пронаћи информације о потенцијалним рањивостима у вашој инфраструктури (напомена: Платформа је тренутно у изради).

Ланац снабдевања и треће стране - идентификација

Идентификујете своје повезаности са трећим странама - који добављачи или партнери имају приступ вашој мрежи или рукују вашим подацима. Недавни напади преко софтверског ланца снабдевања (попут злонамерних ажурирања или експлоатације у широко коришћеним софтверским библиотекама) указују на потребу организација да воде евиденцију о критичним добављачима и сервисима. У тај инвентар укључите кључне клауд сервисе и SaaS (Software as a Service) апликације. Ова идентификација биће основа за контролу приступа трећих страна и њиховог надзора.

Фаза идентификације поставља основу: идентификовали сте шта је изложено ризику и где су слабе тачке које треба ојачати. Након овог корака, потребно је спровести циљане контроле заштите.

Заштита - слојевити заштитни механизми за спречавање инцидената

Функција заштите обухвата широк опсег мера које спречавају да рансомвер уђе у систем и прошири се. Главне области овог сегмента заштите укључују:

Безбедно управљање идентитетом и приступом

Контрола приступа је од највеће важности, јер рансомвер често злоупотребљава слабе креденцијале или преобимна овлашћења. Уведите мултифакторску аутентификацију (MFA) за све кориснике - нарочито за даљински приступ (VPN, RDP, веб мејл, клауд апликације) и за налоге са повећаним привилегијама. Примена ових савета помаже да се смањи ризик од украдених лозинки - чак и ако нападачи прибаве креденцијале, не могу се пријавити без другог фактора. Примените MFA где год је изводљиво. Упознајте се са различитим типовима MFA и како и где се могу применити. Поред тога, практикујте начело најмањих потребних овлашћења (least privilege) за корисничке и сервисне налоге: корисници треба да имају минимум права неопходних за радно место, а администраторске привилегије треба строго ограничити. Један од такође битних савета је и коришћење стандардних (не-администраторских) налога за свакодневни рад, а употребу администраторских налога само када је то неопходно, уз обавезну примену MFA за те налоге. Редовно ревидирајте привилеговане налоге и уклоните или спустите ниво овлашћења онима који нису апсолутно потребни. Имплементација хигијене лозинки - као што су сложеност, политике ротирања лозинки и прагови за закључавање налога - такође је важна. На пример, уведите привремена или трајна закључавања налога након неколико неуспелих покушаја пријаве, како бисте спречили аутоматизоване brute-force нападе. Многи пробоји укључују ситуацију да нападачи успешно погађају или разбијају слабе лозинке; политике закључавања налога (уз надзор тих догађаја) могу бити очигледан знак покушаја компромитовања налога. Размотрите специјализовану заштиту за најосетљивије налоге у виду решења за Privileged Access Management (PAM) која захтевају „sign-out/check-out“ приступ администраторским креденцијалима, примењују снимање сесија и ограничавају употребу таквих налога на одређене радне станице. На крају, обезбедите правилно управљање корисничким сесијама и креденцијалима - одмах деактивирајте некоришћене налоге (нарочито оне бивших запослених), захтевајте јединствене креденцијале за администраторске активности (без дељења налога) и уведите заштите против напада типа pass-the-hash и крађе сесија (нпр. омогућите заштиту LSASS процеса на Windows-у да онемогућите екстракцију хешева). Смањењем броја доступних привилегованих налога и осигуравањем процедуре пријављивања значајно смањујете шансе да актери рансомвер напада остваре приступ или ескалирају привилегије у вашем систему.

Сегментација мреже и Zero Trust архитектура

Имајући у виду чињеницу да се рансомвер унутар мрежа обично шири латерално, тражећи file сервере, резервне копије и контролере домена, правилна архитектура мреже може ограничити ово ширење. Сегментирајте своје мреже у зоне (према пословној функцији или осетљивости) и ограничите непотребну комуникацију између њих. На пример, корисничке корпоративне мреже треба одвојити од data-центар мрежа; OT/SCADA мреже у продукцијском сегменту требало би да буду изоловане од IT мрежа уз строге контроле приступа; развојна/тест окружења изолована од продукције, итд. Користите интерне filewall уређаје или VLAN функционалности да спроведете сегментацију - дозволите само саобраћај који је нужан за пословање. У пракси, то може значити примену степенасте

архитектуре у којој компромитована радна станица запосленог путем фишинг напада не може директно да приступи критичним серверима а да притом не прође кроз додатне безбедносне контроле. Препорука је доследна примена начела Zero Trust широм интерних система (никада не претпостављати да је интерни саобраћај поуздан) и сегментацију унутрашњих мрежа „где год је могуће" ради спречавања ширења малвера. Zero Trust архитектура подиже лествицу у циљу безбедности система, захтевајући континуирану аутентификацију и ауторизацију за било какво латерално кретање у мрежи. Имплементација Zero Trust-а је процес који се одвија у фазама, али започињање са мерама као што су микросегментација мреже, софтверски дефинисани периметри и строге политике приступа засноване на идентитету у великој мери ће ограничити слободу кретања нападача у случају продора у ваш систем. Као део сегментације, учините безбедним сервис за даљинско администрирање као што је Remote Desktop Protocol (RDP) - пошто је RDP чест алат за латерално кретање и често почетни вектор компромитовања, ограничите његову употребу. Ако је могуће, онемогућите RDP на радним станицама и серверима на којима није неопходан или барем осигурајте да RDP портови нису отворени према интернету. Уколико се RDP мора користити интерно или преко VPN-а, захтевајте јаку аутентификацију на њему и помно га надзирите. Такође је препорука да редовно спроводите ревизију свих система који користе RDP и на основу резултата обављате затварање некоришћених RDP портова, захтевање MFA и логовање приступа за RDP, као и ограничавање броја покушаја пријаве. Слично томе, ажурирајте и обезбедите VPN-ове и друге удаљене приступне тачке - држите их ажурним како бисте избегли познате методе напада и размотрите увођење контроле мрежног приступа како бисте осигурали да се на ваш ИКТ систем могу повезати само проверени уређаји.

Безбедно конфигурисање система и контрола апликација

Нарочито битан заштитни слој подразумева безбедну конфигурацију (hardening) ваших система и уређаја како бисте смањили шансе да се рансомвер изврши или прошири. Циљ је обезбедити да су сви крајњи уређаји (сервери, радне станице) и мрежни уређаји конфигурисани безбедно, у складу са референтним стандардима и најбољом праксом. Редовно ажурирајте ваше системе како бисте отклонили рањивости (ово је један од елементарних захтева, због чињенице да су незакрпљени системи најчешће прва мета рансомвера). Дајте приоритет критичним закрпама за оперативне системе, VPN уређаје, базе података, као и за било који софтвер изложен интернету. Многи рансомвер напади искористили су познате, незакрпљене CVE рањивости - благовремено ажурирање нарочито сервера и апликација окренутих ка интернету је од суштинског значаја. Размотрите омогућавање аутоматског ажурирања за програме на корисничким уређајима где год је то изводљиво и користите централизован систем за управљање ажурирањем како бисте пратили и спроводили ажурирања. Поред ажурирања, примените безбедне конфигурације система (hardening): онемогућите непотребне сервисе и портове (нпр. ако SMB или RDP нису потребни на неком уређају, искључите их или блокирајте), уклоните подразумеване налоге или подразумеване лозинке, и осигурајте безбедне конфигурације за контролере домена, виртуелизационе хостове, итд. Користите firewall на хостовима да ограничите долазни приступ сваком уређају само на оно што је неопходно.

Једна од најефикаснијих мера безбедног конфигурисања јесте дозвола извршавања само одобрених апликација (whitelisting). Препорука је конфигурисање система тако да могу да се покрећу само унапред одобрене апликације уз адекватно одржавање листе дозвољеног софтвера. Ово може спречити покретање непознатих рансомвер извршних фајлова или скрипти уопште. Имплементација whitelisting-а може бити изазов у

динамичним окружењима, али почетак на критичним серверима или радним станицама (где су листе апликација предефинисане) може донети велике користи по безбедност система. Чак и у корисничким окружењима, технологије попут Microsoft AppLocker-a или Windows Defender Application Control (WDAC), или независна решења за беле листе, могу спречити неауторизоване извршне датотеке, макрое или библиотеке да се покрену. Контрола уређаја за блокирање непознатих USB дискова или ограничавање извршавања из директоријума у које корисници могу писати (попут temp фолдера) коришћењем Software Restriction Policies (SRP) је још једна доказано ефикасна техника (Национални ЦЕРТ Србије специфично саветује употребу SRP-а да се спречи извршавање рансомвера из уобичајених фолдера попут привремених директоријума и AppData).

Обезбеђење конфигурације пословних апликација такође је важно - на пример, ако користите Microsoft Office, подесите поставке да се макрои подразумевано онемогуће (јер многи рансомвер напади и даље почињу злоупотребом Office макроа). Генерална препорука је искључивање или прецизно ограничавање Office макроа за кориснике уз коришћење „protected view" режима за све документе преузете из имејлова. Ако су макрои неопходни у вашем пословању, размислите о захтеву дигиталног потписивања кода или специфичним листама одобрених аутора макроа. Такође, безбедно конфигуришите веб прегледаче (онемогућите непотребне додатке у оквиру њихове конфигурације) и обезбедите да PDF читачи и други уобичајени алати буду ажурни како бисте смањили ризик од експлоатације.

Доследна безбедна конфигурација помаже смањењу ризика и умањује могућности експлоатације ваших система за нападаче. Сваки сервис који искључите, сваки непотребан администраторски приступ који укинете, сваки софтвер који деинсталирате - смањује шансе да се рансомвер напад реализује или ескалира свој утицај.

Безбедносна решења за радне станице и системе за електронску пошту

Као додатни заштитни слој, примените софтвер за детекцију извршавања малициозног кода као заштиту на свим рачунарима у систему. Савремени алати за детекцију и одговор на нападе (EDR) иду даље од традиционалног антивируса, користећи бихејвиоралну анализу за хватање сумњивих активности (као што су масовно екриповање фајлова, креирање рансомвер откупних порука, заустављање сервиса резервних копија итд.). Обезбедите да су антивирус/EDR инсталирани на свим серверима и радним станицама и да се редовно ажурирају са најновијим сигнатурама. Препорука је коришћење софтвера за детекцију малвера у сваком тренутку, уз подешавање аутоматског скенирања свих долазних фајлова (као што су прилози имејлова и USB дискови). Конфигуришите свој безбедносни софтвер да блокира или бар упозори при покретању непознатих програма. Искористите напредне функције попут режима заштите од рансомвера или детекције напредних претњи ако су доступне (неки AV/EDR добављачи имају специфичне хеуристике против рансомвера).

Безбедност електронске поште подједнако је битна: имплементирајте заштиту мејл сервера која обухвата филтрирање спама, детекцију фишинг порука и скенирање прилога и линкова. Многи фишинг имејлови могу бити филтрирани пре него што стигну до корисника. Користите sandbox за анализу прилога како бисте детектовали да ли прилози или линкови који се налазе у оквиру мејла показују понашање рансомвера када се отворе у виртуелном окружењу. Као што је раније поменуто, примените протоколе за аутентификацију електронске поште (SPF, DKIM, DMARC) како бисте спречили spoofing - DMARC је посебно истакнут као примарна одбрана против рансомвера, јер спречава да лажни имејлови који изгледају као да су од поузданих пошиљалаца уопште стигну до корисника. Комбинацијом филтрирања спама са аутентификацијом електронске поште значајно смањујете шансу да фишинг поруке стигну до крајњих корисника.

Једна од основних контрола у данашње време је и мера контроле веб саобраћаја: за ове потребе користите DNS филтрирање и друга подешавања firewall уређаја да блокирате приступ познатим злонамерним доменима или фишинг страницама. Многе рансомвер инфекције и даље се ослањају на комуникацију са командно-контролним серверима (C2C) или преузимање payload-а са одређених URL-ова - блокирање познатих лоших домена (нпр. путем ажурних информација о актуелним сајбер претњама или коришћењем услуга DNS филтрирања) може превентивно спречити нападе. Савет у овом случају је и блокирање одлазног саобраћаја ка познатим злонамерним IP-адресама и доменима у склопу мрежне одбране. За крајње кориснике, размотрите опцију додавања безбедносних додатака у прегледаче или примену других решења која спречавају приступ новорегистрованим доменима или упозоравају кориснике на потенцијалне фишинг сајтове.

Сигурносне праксе за електронску пошту и корисничке налоге

Још једна битна превентивна мера је спровођење политика за коришћење електронске поште које смањују ризично понашање корисника. На пример, аутоматски уклоните или деактивирајте Office макрое и HTML садржај из долазних имејлова кад год је то могуће. Поставите упозоравајуће банере за имејлове који стижу споља како бисте подсетили кориснике да буду опрезни (нарочито ако имејл изгледа као да долази од познатог контакта, а у ствари је послат са спољне адресе - то може смањити ризике од покушаја лажног представљања). Такође, едукујте кориснике да не користе службене имејл адресе за личне налоге и пријаве, како бисте смањили ризик од credential stuffing напада (јер компромитација личних налога може нападачима открити њихову лозинку коју такође користе на службеном налогу).

Детекција - рано откривање и праћење аномалија

Пошто ниједна одбрана није 100% непробојна, организације морају успоставити системе детекције како би у што ранијој фази напада уочиле знакове малициозног софтвера или активности које му претходе. Један од примарних циљева одбране је идентификовати знакове компромитовања (индикаторе компромиса - IoCs, или сумњиво понашање) пре или тачно у тренутку када нападачи покушају да активирају рансомвер, тако да одбрамбене активности буду што ефикасније и са примарним циљем спречавања шире инфекције. ИКТ системи од посебног значаја могу затражити приступ платформи за дељење информација о претњама Националног ЦЕРТ-а где се могу пронаћи индикатори компромитовања актуелних напада који се дешавају у свету (напомена: платформа је у тренутку писања овог документа још увек у припреми).

Централизовано логовање и SIEM

Осигурајте да се логови из читавог окружења (логови са радних станица, сервера, Active Directory-a, firewall-a, VPN-a итд.) прикупљају и агрегирају у систем за управљање безбедносним информацијама и догађајима (SIEM) или сличну платформу за логовање. Нападачи који изводе рансомвер често остављају трагове - на пример, бројни неуспели покушаји пријаве (brute-force), креирање нових административних налога, неуобичајени процеси који се покрећу на хостовима, употреба специјализованих алата попут Mimikatz-a, или неочекивани обрасци приступа дељеним фолдерима. Централизованим прикупљањем логова можете извршити корелацију догађаја и подесити аутоматска упозорења за сумњиве обрасце.

Пример ове контроле је надгледање Windows Event логова за догађаје попут успешних пријава на систем са необичних изворних IP адреса или у чудно доба дана, неуспешних пријава што може указивати на brute-force покушаје, додавања корисника у администраторску групу или масовне измене фајлова. Такође, савет је да пратите антивирусне логове (ако AV детектује и блокира малвер, истражите у што ранијој фази - како бисте детектовали напад у почетном стадијуму). Многе организације не успевају да благовремено открију упад у систем јер нису ефикасно анализирале своје логове. Кључна препорука у склопу ове контроле је коришћење потенцијала и могућности SIEM уређаја за анализу и детекцију случајева специфичних за тактике рансомвер напада (TTPs - tactics, techniques, procedures). Неки јавно доступни ресурси (попут Sigma правила или методологија у складу са MITRE ATT&CK дефиницијама) могу помоћи у креирању правила детекције за познате рансомвер нападе.

Надзор EDR алата

Ако користите EDR или агенте за праћење радних станица и сервера, искористите њихове могућности упозоравања и трагања за претњама („threat hunting“). EDR решења често детектују сумњиве низове активности (попут покретања процеса који брише Volume Shadow Copies - што је један у низу очекиваних корака током рансомвер напада). Савет је да подесите ваш EDR да алармира на радње као што су извршење команди vssadmin delete shadows, wbadmin delete backup или bcdedit (често коришћених за онемогућавање опција опоравка) - то су црвене заставице које указују на покушај рансомвер напада. Такође, користите EDR за праћење тзв. „living-off-the-land“ бинарних алата (LOLBins). На пример, ако се powershell.exe или wmic.exe користе за преузимање фајлова или кодирање команди, или ако rundll32.exe покреће необичне скрипте - подигните узбуну. Континуирано ажурирајте логику детекције како се откривају нове технике рансомвер напада (нпр. неки рансомвери покрећу Windows у Safe Mode да би заобишли безбедносне алате - то може оставити траг у EDR логовима у виду одређених измена регистра и рестартовања система).

Детекција аномалија у мрежном саобраћају

Разместите системе за детекцију упада (IDS) или превенцију упада (IPS) на кључним тачкама мреже како бисте детектовали познати злонамерни саобраћај. На пример, ако интерни хост одједном почне да се повезује на познати рансомвер командно-контролни сервер или TOR нод (на Dark Web-у), IDS са ажурираним информацијама о претњама (фидовима) могао би то препознати као почетак напада и подићи аларм (или чак блокирати ако је IPS у питању). Помно пратите одлазни саобраћај - многи рансомвери ће покушати да комуницирају са спољним сервером (ради преузимања кључева за шифровање или извлачења података). Неуобичајене промене у одлазном саобраћају

или везе ка неуобичајеним земљама/доменима треба истражити. Поред тога, надзор унутрашњег саобраћаја може помоћи; на пример, коришћење алата који успоставља базну линију нормалне комуникације између сервера и означава одступања могло би открити рансомвер који скенира мрежу или пребацује податке на неки неочекивани хост. Коришћење „honey pot" ресурса такође је валидна техника детекције: нпр. направите лажни дељени диск или мамац-фајл (назван на пример „финансијски_изводи.xlsx" или слично) и пратите да ли му ико приступа – пошто легитимни корисници то не би радили, такав приступ би могао указивати да малвер претражује мрежне дискове у потрази за фајловима за шифровање.

Праћење интегритета фајлова и понашања система

Имплементирајте праћење интегритета фајлова (File Integrity Monitoring) на критичним директоријумима (посебно онима који чувају важне податке или конфигурације). Ако се велики број фајлова промени у кратком року (нпр. њихов садржај се замени и евентуално екстензија промени - што је обележје шифровања), то је знак за узбуну. У многим случајевима корисници су успели да уоче ране фазе шифровања приметивши изненадну појаву преименовања фајлова. Иако је у том тренутку рансомвер већ започео активност, детекција на почетку циклуса шифровања (можда и само на једном file-серверу) могла би омогућити брз одговор (попут изолације тог хоста са мреже) пре него што се прошири на друге. Модерни сензори засновани на анализи обрасца понашања могу аутоматски зауставити процесе или „замрзнути" систем када их детектују - размислите о њиховој имплементацији посебно за ваше фајл-сервере.

Threat hunting и ручни преглед аномалија

Не ослањајте се искључиво на аутоматске аларме - укључите проактивно „ловљење претњи" у ваше редовне активности. То у пракси значи периодично претраживање система и логова у потрази за знацима присуства нападача који можда до сада нису изазвали аутоматска упозорења. На пример, тражите процесе који обично нису активни или се покрећу из необичних директоријума, трагајте за неправилностима попут корисничког налога који се логовао на више машина којима никада пре није приступао, или за присуством познатих злонамерних алата (попут Cobalt Strike „beacon" или алата за откривање лозинки) на системима. Обучите аналитичаре о уобичајеним техникама рансомвер напада (MITRE ATT&CK оквир може помоћи, нпр. како групе онемогућавају безбедно логовање, које фајлове/скрипте користе). Чак и просто прегледање ко је у администраторским групама или да ли су инсталирани нови сервиси на вашим рачунарима може открити да ли је нападач креирао „backdoor" приступ. Имајући у виду да многи рансомвер напади укључују „dwell time" (нападачи могу провести дане или недеље у мрежи пре лансирања рансомвера), ефикасно ловљење претњи може их детектовати и елимисати током тог периода.

Пријаве корисника и „canary" фајлови

Подстичите културу у којој запослени одмах пријављују сумњиве појаве - нпр. ако радна станица изненада падне и покаже чудну поруку, или фајлови постану недоступни, корисници треба да знају да одмах алармирају службу задужену за информациону безбедност. Ране пријаве од стране корисника понекад су први траг рансомвер напада у току (нпр. неко види поруку „ваши фајлови су шифровани" која се појавила). Такође можете користити „мамац" фајлове (фајлове којима нико не би легитимно приступао) уз аларме, као што је већ поменуто, или лажне налоге чија би употреба одмах указала на компромитовање.

Сумирано, функција Детекције односи се на брзу идентификацију инцидента. Национални CERT-ови такође позивају организације да прате своје логове и подесе аларме за потребе детекције упада. Брза детекција напада омогућава брзу реакцију и одговор на инцидент што представља следећи слој одбране који обрађујемо у наставку овог документа.

Одговор - план за инциденте и сузбијање напада

Када је рансомвер инцидент (или покушај инцидента) детектован, од пресудне је важности поседовати добро осмишљен и увежбан план одговора на инциденте како би се претња обуздала и смањила штета. Функција Одговор (Respond) обухвата припрему процедура за одговор на инциденте и способност ефикасне координације и комуникације током самог инцидента. Кључне препоруке су:

Успоставите план одговора на инциденте специфичан за рансомвер

Иако је свеобухватан план одговора на сајбер инциденте неопходан, рансомвер доноси јединствене изазове (нпр. потреба за брзом изолацијом система, одлуке о плаћању откупнине или не, укључивање полиције, руковање цурењем података/изнудама). Организације треба или да имају посебан „playbook“ за рансомвер, или да обезбеде да постојећи план за одговор на инцидент детаљно покрива рансомвер сценарије. План треба да дефинише улоге и одговорности - ко је менаџер инцидента, ко обавештава руководство, ко контактира органе реда или осигуравајућу кућу, правни тим итд. - као и овлашћења за доношење кључних одлука (нпр. да ли разматрати плаћање откупнине у крајњој нужди, што је одлука која обично укључује највише руководство и правни тим). NIST препоручује поседовање плана за опоравак од инцидента са дефинисаним улогама и стратегијама доношења одлука, потенцијално као део ширег плана континуитета пословања. У плану идентификујте ваше критичне сервисе и приоритизујте њихово враћање. План треба да обухвати техничке кораке (попут процедура тријаже, мера сузбијања попут сегментације мреже или гашења одређених сервиса, као и кораке за отклањање претње као што су брисање или реинсталација машина), као и кораке комуникације.

Припремите процедуре комуникације и листе контаката које ћете користити за време инцидента

Унапред саставите ажурирани списак свих страна које би могле бити укључене током рансомвер напада. Овај списак треба да укључује унутрашње контакте (ИТ тимове, руководство, PR, правни тим итд.) и кључне спољне контакте: локалну полицију или јединице за сајбер криминал, Национални ЦЕРТ Србије, вашег осигуравача за сајбер ризике или унапред ангажовану фирму за одговор на инциденте, регулаторе за заштиту података о личности (ако су лични подаци укључени и уколико постоји обавеза пријаве), и евентуално индустријске регулаторе специфичне за ваш сектор. Организацијама се саветује да унапред успоставе контакт листе са свим релевантним организацијама које је неопходно контактирати у случају инцидента (видети Прилог 2.). Такође планирајте методе комуникације ван уобичајених канала - претпоставите да у рансомвер нападу ваш корпоративни имејл или chat систем можда неће бити доступни или би могли бити надгледани од стране нападача. Обезбедите алтернативна средства (приватни телефони, спољне имејл адресе, итд.) за координацију одговора ако буде потребно. Организујте „tabletop“ вежбе да симулирате рансомвер напад и тестирате да ли план комуникације функционише.

Стратегије за сузбијање ефеката напада

Оног тренутка када се посумња или детектује рансомвер, брза изолација је критична за ограничавање ширења. Ово може подразумевати изолацију погођених хостова из мреже (нпр. искључење рачунара или сервера са мреже на нивоу мрежне опреме), искључивање одређених услуга или сегмената мреже, па чак и превентивно искључивање непогођених система ако су под ризиком. Једна ефективна тактика је унапред дефинисати и увежбати коришћење „прекидача за гашење" - на пример, имати процедуре да се муњевито блокира сав одлазни саобраћај или деактивирају одређени налози на нивоу целе организације ако се рансомвер шири. Иако су ово екстремне мере, у условима муњевитог ширења рансомвера што пре прекинете контролу и ширење од стране нападача, то ћете спасити већи део свог окружења. Ако су погођени само делови система, изолујте их и немојте их поново прикључивати на мрежу док се не обави форензика (искључивање машине током шифровања може понекад сачувати делове фајлова у меморији - консултујте стручњаке за одговор на инциденте о најбољој пракси у вашој ситуацији). Ако детектујете упад у ранијој фази (нпр. пре него што шифровање почне, али видите изношење података или активности нападача), и даље реагујте одлучно да сузбијете претњу - блокирајте приступ нападача мрежи (укидањем њихових VPN сесија, онемогућавањем компромитованих налога итд.) и, ако треба, искључите привремено свој интернет линк док не сагледате обим нарушавања (имајте у виду да ово може пореметити пословање, али исто то чини и широко распрострањен рансомвер – ово је тешка одлука коју план реаговања на инциденте треба да разради).

Неутралисање и уклањање претње

Када је претња сузбијена, фокусирајте се на њено уклањање - идентификујте све инстанце малвера, алате или „backdoor" које је нападач инсталирао и уклоните их. То ће вероватно значити форматирање и обнову компромитованих система са чистих резервних копија, јер се машинама зараженим рансомвером не може у потпуности веровати чак и ако се фајлови на њима дешифрују. Планирајте процедуре за сигурно брисање и поновно инсталирање. Имајте на уму да рансомвер често прати и други малвер (крадљивци креденцијала итд.), тако да је неопходно темељно „чешљање" кроз мрежу. Искористите индикаторе из напада (хешеве фајлова, измене у регистру, IP адресе нападача) да претражите остатак мреже за било какве трагове. Често је препоручљиво ангажовати професионалне тимове за одговор на инциденте или форензичаре у овој фази ради темељности (многе полисе сајбер осигурања покривају ову услугу).

Комуникација и извештавање

Током и након инцидента, савет је да опрезно управљајте комуникацијама. У интерној комуникацији неопходно је да држите руководство и по потреби запослене информисаним, како бисте одржали транспарентност без изазивања панике. У екстерној комуникацији, ако су подаци украдени или је дошло до прекида услуга, можда имате законску обавезу да обавестите кориснике или надлежне органе у одређеним роковима, на пример, GDPR захтева да се нарушавање безбедности личних података пријави у року од 72 сата ако утиче на приватност лица. У Републици Србији заштита физичких лица у вези са обрадом података о личности регулисана је Законом о заштити података о личности, који повреду података о личности дефинише као повреду безбедности података о личности која доводи до случајног или незаконитог уништења, губитка, измене, неовлашћеног откривања или приступа подацима о личности који су пренесени, похрањени или на други начин обрађивани. Према истом Закону, руковалац је дужан да о повреди података о личности која може да произведе ризик по права и слободе физичких лица обавести Повереника за заштиту података о личности без непотребног

одлагања, или, ако је то могуће, у року од 72 часа од сазнања за повреду. Ако руковалац не поступи у року од 72 часа од сазнања за повреду, дужан је да образложи разлоге због којих није поступио у том року. Обрађивач је дужан да, после сазнања за повреду података о личности, без непотребног одлагања обавести руковаоца о тој повреди. Руковалац је дужан да документује сваку повреду података о личности, укључујући и чињенице о повреди, њеним последицама и предузетим мерама за њихово отклањање. Припремите шаблоне саопштења за разне сценарије (обавештење о прекиду услуге, обавештење о цурењу података итд.). И као што је напоменуто, координишите се са релевантним државним органима, који могу пружити смернице, а у појединим случајевима могу имати кључеве за дешифровање или друге информације ако је група напада позната (на пример, пројекат NoMoreRansom или FBI поседују кључеве за неке варијанте рансомвера). Већина влада подстиче пријављивање рансомвер инцидената; у неким јурисдикцијама, непријављивање може имати регулаторне последице, па се свакако консултујте са правним саветником.

Одлука о плаћању откупнине

План одговора на инциденте (IR план) треба да укључи оквир за разматрање плаћања откупнине. Званичне смернице саветују избегавање плаћања откупнина - нема гаранције да ћете повратити податке, плаћањем финансирате криминал, а у неким случајевима плаћањем можете прекршити закон што вама или вашој организацији може створити додатне проблеме. Идеално је да се организације припреме да не плате тражени откуп и да се за ту одлуку обезбеде ослањањем на своје резервне копије и отпорност система. Међутим, реалност може бити сложена ако су животи у питању (нпр. у болници) или уколико резервних копија уопште нема, што је нажалост чест случај. Ако размишљате о плаћању, обавезно се консултујте са правним тимом у вези одредби Закона о спречавању прања новца и финансирања тероризма и дискретно укључите релевантне државне органе. Неке државе иду ка томе да обавезују пријављивање плаћања откупнина, или чак да их забране у одређеним околностима. Ове одлуке су на крају пословне, али треба да буду вођене етиком, правним разматрањима и вероватноћом опоравка података. Поседовање сајбер осигурања које покрива рансомвер може пружити неку помоћ (осигуравач често обезбеђује преговараче или менаџере инцидента), али имајте на уму да су и осигуравајуће компаније обавезане прописима (не могу, на пример, посредовати у плаћању санкционисаном субјекту). Укратко, укључите у ваш IR план и протокол за руковање комуникацијом са нападачима - чак и ако ће његова намена бити само да купите време - то може бити корисно. Ако ипак ступите у контакт са нападачима (често путем TOR chat портала који обезбеде), радите то пажљиво и пожељно под вођством искусних преговарача или органа безбедности.

Укључите се у размену информација

Након сузбијања инцидента, поделите шта можете о индикаторима или методама напада са својим колегама из сектора или кроз платформе за размену информација о претњама. Ово може помоћи другима да ојачају своју одбрану и доприноси колективној безбедности. Многи национални CERT-ови прихватају добровољно достављање узорака рансомвер малвера или индикатора компромитације како би креирали упозорења за друге ентитете. На пример, Национални ЦЕРТ Србије охрабрује организације да пријаве инциденте и поделе техничке детаље напада, чиме заједница стиче вредне увиде у актуелне претње.

ENISA је такође објавила основни сет препорука које треба да примене појединци и организације који постану жртве рансомвера:

• контактирање националних органа за сајбер безбедност или органа за спровођење закона;

• одбијање плаћања откупнине и одбијање преговарања са актерима претње;

• стављање погођених система у карантин уз искључивање погођених система из мреже како би се обуздала инфекција и спречило ширење рансомвера;

• посета сајту „No More Ransom Project" на којем се могу наћи декриптори за многе варијанте рансомвера (видети Прилог 3.);

• закључавање приступа резервним системима док се инфекција не уклони.

У Републици Србији надлежност за поступање у предметима кривичних дела против безбедности рачунарских података и других кривичних дела која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала има Више јавно тужилаштво у Београду за територију Републике Србије, односно посебно одељење за борбу против високотехнолошког криминала (Посебно тужилаштво за високотехнолошки криминал) образовано у Вишем јавном тужилаштву.

Законом о информационој безбедности прописано је да Национални ЦЕРТ, између осталог, прикупља и размењује информације о претњама, рањивостима, избегнутим инцидентима и инцидентима и пружа подршку, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, пружа рана упозорења, узбуне и најаве и информише релевантна лица о претњама, рањивостима и инцидентима, као и да реагује без одлагања по пријављеним или на други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и по пријавама физичких и правних лица, тако што пружа савете и препоруке на основу расположивих информација о инцидентима и предузима друге потребне мере из своје надлежности на основу добијених сазнања.

Добро изведен одговор може значајно смањити време и трошкове опоравка. Организације које се припреме и увежбају (кроз симулације и вежбе) реагују много ефикасније када се заиста суоче са инцидентом. Цитирајући г. Бенџамина Френклина који је једном приликом изјавио „Ако заборавите да планирате, припремите се за неуспех" желимо да укажемо да су рансомвер инциденти кризе које стварају висок притисак на учеснике па је самим тим постојање познатог и увежбаног плана којег тим може да се држи у стресној ситуацији веома битно за излазак из кризе са што мањим последицама.

Опоравак - стратегије резервних копија и враћање система

Функција Опоравак представља сигурносну опцију - упркос најбољим напорима у превенцији, ако рансомвер ипак успе да шифрује или уништи податке, робусне могућности опоравка осигуравају да ваша организација може обновити рад без плаћања откупа. Резервне копије података (бекап) су стуб опоравка од рансомвера. Међутим, нису све резервне копије једнаке; нападачи циљано нападају и саме системе за бекап како би онемогућили опоравак. Стога је неопходна добро осмишљена, поуздана и проверена стратегија креирања резервних копија:

Примените правило 3-2-1 за бекап

Широко се препоручује да имате најмање три копије критичних података (продукциони подаци + бар две резервне копије), на две различите врсте медија, са најмање једном копијом смештеном ван главне локације или офлајн. Овај принцип „3-2-1" штити од разних сценарија отказа. На пример, један бекап може бити на другом физичком медијуму (трака или друго складиште) од примарног, а један може бити ван локације (географски одвојен или у клауду) или у потпуности офлајн (није стално повезан на мрежу). Офлајн копија је кључна за рансомвер - резервне копије којима рансомвер може да приступи (попут мрежно повезаног бекап сервера који је увек укључен) могу бити шифроване заједно са свим осталим. Нападачи често покушавају да обришу или шифрују Windows Volume Shadow Copies, мрежне бекап дискове или повезане уређаје за складиштење. Обезбеђивањем да постоји бар једна офлајн копија (нпр. бекап на траци који се чува ван мреже, или периодични бекап који се по копирању података дисконектује) осигуравате да постоји бар једна нетакнута копија коју нападачи не могу уништити. Многе организације сада имплементирају неизменљиве резервне копије или WORM складиште (Write-Once-Read-Many) у ту сврху - бекап системи где се, једном написани, подаци не могу мењати или брисати одређени временски период. На пример, клауд складишта или бекап уређаји са функцијом неизменљивости могу држати бекап снимке „закључаним" против измене. Неки користе и air-gap бекап - физички изоловано складиште на које се подаци пренесу, па се уређај одвоји од мреже. И air-gap и неизменљива складишта пружају јаке гаранције да чак и ако нападач добије администраторска права на домен, не може једноставно обрисати све ваше резервне копије.

Редовност бекапа и опсег покривених података

Обављајте честе бекапе свих критичних система и података. Учесталост треба да буде усклађена са вашим циљевима тачке опоравка (RPO) - максимално прихватљив губитак података који можете толерисати. Многе организације раде дневне инкременталне бекапе (или чак чешће, нпр. снимање стања на сваки сат за критичне базе података) и недељне пуне бекапе. Минимум би био да циљате на дневне бекапе кључних података, тако да чак и ако будете погођени рансомвер нападом, изгубите мање од 24 сата података. За неке податке (нпр. финансијске трансакције) оправдано је и континуирано реплицирање на бекап системе. Примарни циљ је да су сви важни фајлови, копије виртуелних машина, конфигурације и апликациони подаци укључени у план бекапа. Лако се превиде ствари попут конфигурација мрежне опреме, које, ако се изгубе, могу успорити опоравак. Експортујте конфигурације рутера, свичева, firewall-ова и чувајте и њих (познати су случајеви да рансомвер напади понекад бришу или закључавају чак и мрежну опрему).

Обезбедите своје резервне копије

Третирајте безбедност бекап система исто као и продукције. Уведите контроле приступа и сегментацију мреже за делове ИКТ система где се држе резервне копије - на пример, бекапи треба да се смештају у мрежној зони која није директно доступна са других корисничких мрежа. Користите наменске сервисне налоге за бекап софтвер који нису Domain Admin (да ограничите кретање нападача према бекапима). Шифрујте бекап податке у мировању и у транзиту, тако да ако нападачи и украду бекап фајлове, не могу да читају осетљиве податке (ово је корисно при сценарију изнуде путем цурења података: ако су ваши бекапи шифровани, чак и ако их нападачи украду ради изнуде, бескорисни су без кључа). Осигурајте да су кључеви за декрипцију бекапа безбедно ускладиштени (идеално управљани кроз интерни систем за управљање кључевима). Такође, одржавајте интегритет бекапа - користите контролне суме или софтвер за бекап који верификује бекапе како бисте били сигурни да нису неприметно оштећени или делимично шифровани.

Рутинско тестирање бекапа (вежбе враћања)

Бекап вреди онолико колико и ваша способност да га успешно вратите! Спроводите редовне тестове враћања (restore) како бисте потврдили да бекапи функционишу и да се подаци могу успешно повратити. Ово укључује симулацију рансомвер сценарија: одаберите насумично одређен фајл или систем, покушајте да га вратите из бекапа и измерите колико времена треба и да ли су подаци нетакнути. Многе организације су тек у кризи откриле да њихови бекапи нису исправни или су били непотпуни - тестирање помаже да се та непријатна изненађења избегну. Тестирање треба да обухвати и сценарио потпуног опоравка окружења: нпр. извежбајте ситуацију да је читав сервер или data центар изгубљен и проверите колико брзо можете обновити систем из бекапа. Ово може открити проблеме у процесу бекапа (попут недостајућих ажурирања или конфигурационих фајлова). Чувајте документоване процедуре за враћање, и уверите се да је више чланова тима обучено за њих (у случају напада, не желите да само једна особа зна како да спроведе опоравак). Не заборавите да документујете и увежбате поновну изградњу система „од нуле“ ако је потребно (поседовање референтних “златних” копија система или инфраструктурних скрипти за аутоматизовану инсталацију може драстично убрзати опоравак).

Чувајте offline копије критичног софтвера и кључева

Поред самих података, обезбедите да имате приступ инсталационим медијима или копијама за сав критичан софтвер (инсталације оперативних система, инсталације апликација) у случају да морате да обновите системе од нуле. Такође, бекапујете лиценцне кључеве, конфигурационе фајлове и документацију одвојено. На пример, ако вам мрежа не ради, веома је корисно имати offline копије конфигурација мрежне опреме или бекап Active Directory домен контролера. Неке организације држе „jump bag“ или offline архиву која садржи за пословање најбитнији софтвер и системске копије, ажуриране периодично, који се могу употребити у сценарију опоравка када мрежа можда није доступна.

Отпорност и планови континуитета

Изван техничког опоравка, имајте спремне процедуре за континуитет пословања најважнијих операција. Ово укључује да знате како бисте наставили пружање основних услуга ако су ИКТ системи недоступни - на пример, могу ли се одређени процеси привремено обављати ручно (на папиру)? Имате ли алтернативне методе комуникације (попут хитних телефонских конференција ако је имејл недоступан)? За индустријска окружења, постоје ли ручне опције за управљање постројењем ако SCADA системи откажу? Ови планови осигуравају безбедност и минимум оперативности док се ИТ системи обнављају. Функција Recover у NIST CSF наглашава одржавање планова за отпорност управо из ових разлога. Редовно ажурирајте и увежбавајте ове планове континуитета пословања заједно са вашим вежбама тестирања бекапа.

Укључите кључне заинтересоване стране у планирање опоравка

Опоравак од рансомвер напада није искључиво ИТ задатак; координација са пословним руководиоцима је важна за одређивање приоритета (који системи се прво враћају) и разумевање утицаја. У случају раширеног енкриптовања, мораћете да одредите шта се враћа и којим редоследом - ти приоритети треба да буду унапред утврђени уз потврду и сагласност менаџмента. Често су системи који су оријентисани према клијентима или они који генеришу приход највиши приоритет, док интерни системи могу сачекати. Укључивањем руководилаца у процес планирања опоравка обезбеђујете да технички

тим разуме пословне императиве - на пример, руководиоци могу нагласити да је враћање услуге за клијенте критично у првих 24 сата, чак и ако интерни сервиси морају да трпе.

Примењивањем робусних процеса бекапа и опоравка, организација знатно побољшава своју отпорност на рансомвер - способност да кажу „Чак и ако будемо погођени, можемо да обновимо податке уз минималан губитак и застој, и нема потребе да плаћамо нападачима.“ Многе националне смернице истичу бекапе као појединачно најважнију одбрану: на пример, Национални ЦЕРТ Србије наводи да је враћање из сигурне резервне копије најбржи начин да се поврати приступ подацима након рансомвер напада. Посебну пажњу обратите на ваше податке у клауду и начине на које сте их интегрисали у вашу бекап стратегију. Квалитетно уређен бекап, комбинован са превентивним контролама за заштиту тих бекапа, у суштини одузима главну полугу моћи рансомвер актера (барем у погледу аспекта енкрипције ваших података - процурели подаци остају посебан ризик).

ЗАКЉУЧАК

Сајт ransomware.live (приватни пројекат Julien Mousqueton) даје тренутни увид у жртве различитих рансомвер група, географску распрострањеност жртава, детаље трагова које остављају различите групе и др. Рансомвер напади представљају значајну претњу организацијама широм света, посебно онима које управљају критичном инфраструктуром у јавном сектору и секторима финансија, енергетике и телекомуникација, али и мањим субјектима као што су мала и средња предузећа. Тренд претњи у периоду 2024-2025. обележен је све софистицираније активностима нападача - од Ransomware-as-a-Service (RaaS) група које експлоатишу украдене креденцијале и zero-day рањивости, до употребе двоструке/троструке изнуде па чак и техника потпомогнутих вештачком интелигенцијом - што све захтева промишљене и добро припремљене одбрамбене механизме. У овим смерницама навели смо различите препоруке, базиране на најновијим подацима о претњама мапираних на признате стандарде и препоруке из домена сајбер безбедности, у циљу помоћи организацијама у постизању боље отпорности и способности за превенцију и одговор на рансомвер инциденте.

Истовремено, постизање отпорности је последња тактика у одбрани. Она се постиже улагањем у поуздану стратегију бекапа (сигурну, офлајн, тестирану) тако да, чак и ако нападачи закључају ваше системе, не могу да вам трајно онемогуће приступ до ваших података. Једнако важна је и пракса успостављања и тестирања планова одговора на инциденте, како би ваш тим могао брзо и ефикасно реаговати чим се упад у систем детектује - са примарним циљем да пресечете даље ширење нападача, обавестите релевантне стране и отпочнете опоравак по утврђеном плану.

За критичне секторе, ове праксе се морају додатно прилагодити њиховим окружењима - финансијске институције морају одржавати на високом нивоу заштиту података и обезбедити усклађеност са прописима, пружаоци услуга снабдевања енергијом морају осигурати своје ОТ мреже и системе безбедности, а телекомуникациони оператори обезбедити доступност мреже и податке о корисницима. У свим секторима, сарадња и размена информација (са колегама, преко ISAC-ова, CERT-ова, и органа за спровођење закона) делује као додатан сегмент заштите: дељењем обавештајних података о претњама и научених лекција, организације колективно смањују ризик за све. Рансомвер напади јесу распрострањени и све софистицираније, али свакако нису несавладива препрека за наше одбрамбене системе.

Чињеница да многи рансомвер напади и даље експлоатишу познате слабости (незакрпљене системе, слабу хигијену лозиники, недостатак адекватних изолација мрежа) представља подједнако и претњу и прилику - решавањем ових проблема, организације могу спречити већину будућих напада и тиме подићи степен безбедности своје организације.

Као посебно битно издвајамо чињеницу да руководиоци и менаџери информационе и сајбер безбедности треба да проверавају спремност одговора на рансомвер нападе као пословни приоритет процењујући ризике које ови типови напада са собом носе. Већина нових директива и законских регулатива препознаје одговорност за сајбер безбедност у топ менаџменту који у крајњој инстанци и носи одговорност за пословање читаве организације.

Препоруке у овом извештају - изведене из смерница Националног ЦЕРТ-а Републике Србије, препорука релевантних светских организација NIST, CIS, ENISA и CISA и анализе стварних инцидената дате су са циљем прављења јасних смерница за систематско унапређење „имунитета“ ваше организације као одговора на потенцијалне рансомвер нападе. Њихова примена захтева одређене инвестиције и напор, али трошак превенције је по досадашњим искуствима знатно мањи у поређењу са негативним потенцијалом који собом носи рансомвер инцидент (финансијски губици, регулаторне казне због цурења података, застоји у пословању, нарушен углед и др.). Увођењем наведених контрола заштите, организације могу драстично смањити вероватноћу да постану жртва рансомвера, тј. осигурати да, ако до напада и дође, могу да га преброде са минималним утицајем на пословање. У светлу стално еволуирајућих претњи из сајбер домена адекватне мере заштите и сајбер отпорност свакако представљају најбоље елементе за одбрану од постојећих и будућих претњи по ваше ИКТ системе.

С поштовањем,

Тим eGA консултаната у партнерству са Националним ЦЕРТ-ом Републике Србије

Београд, децембар 2025. године

РЕФЕРЕНЦЕ

1. Закон о информационој безбедности (“Службени гласник РС”, бр. 91/2025) https://www.paragraf.rs/propisi/zakon-o-informacionoj-bezbednosti-2025.html

2. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 директива)

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

3. TRM Labs – “Ransomware in 2024: Latest Trends, Mounting Threats, and the GovernmentResponse,”октобар2024. https://www.trmlabs.com/resources/blog/ransomware-in-2024latest-trends-mounting-threats-and-the-government-response

4. Cybersecurity Dive – “CVE exploits, stolen credentials fueled рансомвер surge in 2023,”јун2024. https://www.cybersecuritydive.com/news/exploits-credentialsfuel-ransomware-surge/717943/

5. BleepingComputer (Lawrence Abrams) – “Ransomware gangs switching to new intermittent encryption tactic,” септембар 2022. https://www.bleepingcomputer.com/news/ security/ransomware-gangs-switching-to-new-intermittent-encryption-tactic

6. CISA/FBI (Заједнички водич) – #StopRansomware Guide (ажуриран у мају 2023). (Доступно на: https://www.cisa.gov/stopransomware/ransomware-guide)

7. NIST IR 8374 – "Ransomware Risk Management: A Cybersecurity Framework Profile," октобар 2021. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf

8. Institute for Security & Technology (IST) – "Blueprint for рансомвер Defense (ver.2),"август2022. https://securityandtechnology.org/wp-content/uploads/2022/08/IST-Blueprint-for-Ransomware-Defense.pdf

9. ENISA – Threat Landscape 2024 (кључни налази о рансомвер претњама у Европи). (Доступно у PDF формату: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf)

10. ENISA – Threat Landscape 2025 (кључни налази о рансомвер претњама у Европи). (Доступно у PDF формату: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf)

11. The NIST Cybersecurity Framework 2.0, фебруар 2024., https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

12. CIS Critical Security Controls Version 8, мај 2021., https://www.cisecurity.org/controls/v8

13. CIS Critical Security Controls Version 8.1, март 2024., https://www.cisecurity.org/controls/v8-1

14. Национални ЦЕРТ Републике Србије – "Preporuke za preventivnu zaštitu od ransomvera" (препоруке за превентивну заштиту), 2023.

https://www.cert.rs/files/shares/Preporuke%20za%20preventivnu%20za%C5%A1titu%20od%20ransomware%20napada%20lat.pdf

15. Trustwave SpiderLabs – "Ransomware Attacks Against the Energy and Utilities Sector Up 80%," јануар 2025. https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/trustwave-spiderlabs-ransomware-attacks-against-the-energy-and-utilities-sector-up-80percent

16. Rapid7 – "The 2024 рансомвер Landscape: Looking back on another painful year,"јануар2025.(Аутор:ChristiaanBeek) https://www.rapid7.com/blog/post/2025/01/27/the-2024ransomware-landscape-looking-back-on-another-painful-year/

17. dmarcian – "DMARC: Foundational рансомвер Defense," октобар 2023. https://dmarcian.com/ransomware/

18. Национални ЦЕРТ Републике Србије – "Заштита налога коришћењем двофакторске аутентификације" https://cert.rs/files/shares/2FA%20cert.pdf

ПРИЛОГ 1. КАНАЛИ КОМУНИКАЦИЈА У СЛУЧАЈУ РАНСОМВЕР ИНЦИДЕНТА

Најбоље праксе и смернице које се тичу информационе безбедности и континуитета пословања упућују организације/компаније да успоставе, документују и редовно практикују симулације инцидентних ситуација како би у случају реалног инцидента били што ефикаснији у одговору на инцидент.

Једна од битних ставки у споменутој документацији је и матрица комуникације у којој се наводе прецизни кораци о поступку и начину комуницирања у случају инцидента. Како у оквиру само организације/компаније (оперативни центар, надређени руководилац, топ менаџмент и др.) тако и ка екстерним контактима (клијенти, пружаоци услуга, државни органи и др.).

У табели у наставку наводимо најбитније екстерне контакте за територију Републике Србије.

Назив институције	Мејл	Телефон	Сајт
Национални ЦЕРТ	info@cert.rs	062/20-20-30	www.cert.rs
Посебно тужилаштво за високотехнолошки криминал	vtk@vtk.jt.rs vtk@beograd.vtk.jt.rs	011/745-1233	https://www.beograd.vtk.jt.rs/
Министарство унутрашњих послова - Служба за борбу против високотехнолошког криминала	vtk@mup.gov.rs	011/306-2000	https://www.mup.gov.rs/wps/portal/sr/gradjani/saveti/Visokotehnoloski%20kriminal/
Повереник за информације од јавног значаја и заштиту података о личности	office@poverenik.rs	011/340-8900	https://www.poverenik.rs

Табела 1: Листа екстерних контаката у случају инцидента

ПРИЛОГ 2. МЕРЕ ЗАШТИТЕ ИКТ СИСТЕМА

Зановљени Закон о информационој безбедности ("СГ РС", бр. 91/2025) објављен 23. октобра 2025. године прописује 37 мера заштите ИКТ система којима се обезбеђује превенција од настанка инцидента, односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

У табели у наставку наведене су прописане мере и њихова улога у процесу превенције и одговора на рансомвер инцидент

Претрага	Тип контрола	Практични примери активности
1) Успостављање организационе структуре, са утврђеним пословима, знањима, компетенцијама, искуством и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система	Организационе	Израда дијаграма, дефинисање описа послова, именовање CISO-а, усвајање политика и процедура, формирање тима за безбедност, израда матрице одговорности
2) Прикупљање података о претњама по информациону безбедност ИКТ система	Техничке / организационе	Имплементација SIEM система, праћење извештаја CERT-а, коришћење threat intelligence сервиса, редовно анализирање логова, чланство у безбедносним заједницама
3) Постизање безбедности рада на даљину и употребе мобилних уређаја	Техничке	Набавка и имплементација VPN решења, MDM система, политика за BYOD, мултифакторска аутентикација за приступ на даљину, шифровање мобилних уређаја
4) Обука корисника и менаџера, континуирано образовање	Образовне / организационе	Организација редовних обука, фишинг симулације, e-learning платформе, израда водича и постера, тестови знања, специјализоване радионице за ИТ особље

5) Обезбеђивање довољно ресурса за адекватно управљање информационом безбедношћу	Организационе	Планирање и обезбеђивање буџета за безбедност, запошљавање стручњака, набавка софтвера и хардвера за заштиту, outsourcing одређених безбедносних функција
6) Заштита од ризика при променама посла или престанка радног ангажовања	Организационе / процедуралне	Процедуре за деактивацију налога, повраћај опреме, опозив приступних права, излазни интервју, ажурирање инвентара приступа
7) Идентификовање информационих добара и одређивање одговорности за њихову заштиту	Организационе	Инвентаризација ИТ ресурса, додела власника података, вођење регистра информационих добара, редовно ажурирање инвентара
8) Класификација података према значају и управљање ризицима	Организационе / процедуралне	Дефинисање нивоа поверљивости (јавно, интерно, поверљиво), означавање докумената, процена ризика, израда матрице ризика
9) Заштита носача података	Техничке / физичке	Коришћење сефова за физичко чување, шифровање USB уређаја, забрана коришћења личних USB-ова, уништавање старих носача података
10) Ограничење приступа подацима и средствима за обраду података	Техничке	Имплементација ACL-а, RBAC система, сегментација мреже, додела права приступа по принципу најмањих привилегија
11) Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему	Техничке	Коришћење аутентикације (лозинке, картице, токени), ауторизације, логовања приступа, ревизија приступних права
12) Утврђивање одговорности корисника за заштиту средстава за аутентификацију	Организационе / техничке	Едукација о лозинкама, политика за коришћење токена, мониторинг злоупотреба, потписивање изјава о одговорности
13) Употреба криптографских контрола и других техника за заштиту података	Техничке	Имплементација енкрипције података у транзиту и мировању, дигитални сертификати, PKI инфраструктура, коришћење HSM уређаја
14) Мере заштите ради спречавања отицања података	Техничке	DLP системи, мониторинг мрежног саобраћаја, блокирање USB портова, политика забране слања поверљивих података ван организације
15) Физичка заштита објеката, простора, зона	Физичке / техничке	Видео надзор, контрола приступа (картице, биометрија), алармни системи, физичко обезбеђење, закључавање сервер соба

16) Заштита од губитка, оштећења, крађе или угрожавања имовине ИКТ система	Физичке / техничке	Осигурање опреме, бекап решења, физичка заштита сервера, коришћење UPS-а, мониторинг температуре и влаге
17) Обезбеђивање исправног и безбедног функционисања средстава за обраду података	Техничке	Редовно одржавање, мониторинг система, patch management, аутоматизовани алати за надзор перформанси
18) Процедуре и мере заштите при коришћењу клауд услуга	Техничке / процедуралне	Уговарање SLA са клауд провајдером, енкрипција података у клауду, контрола приступа, процена безбедности клауд провајдера, двофакторска аутентикација
19) Праћење ИКТ система ради откривања рањивости и претњи	Техничке	Набавка SIEM система, редовно скенирање на познате рањивости, пенетрациони тестови, коришћење алата за детекцију аномалија
20) Ограничење приступа веб презентацијама које могу нарушити безбедност	Техничке	Веб филтери, блокирање ризичних сајтова, праћење приступа, едукација корисника о фишинг претњама
21) Заштита података и средстава од злонамерног софтвера	Техничке	Антивирус софтвер, EDR решења, редовно ажурирање дефиниција, sandboxing, едукација корисника
22) Редовно прављење резервних копија података, софтвера и система	Техничке / процедуралне	Аутоматизовани бекап системи, тестирање повраћаја података, бекап на удаљене локације, вођење евиденције о бекапима
23) Чување података о догађајима значајним за безбедност ИКТ система	Техничке / процедуралне	Логовање догађаја, SIEM анализа, чување логова на сигурној локацији, аутоматизована анализа логова
24) Обезбеђивање интегритета софтвера и оперативних система	Техничке	Patch management, хеш провера, мониторинг промена, коришћење integrity check алата
25) Заштита од злоупотребе техничких безбедносних слабости ИКТ система	Техничке	Редовно ажурирање софтвера, пенетрациони тестови, едукација администратора, коришћење vulnerability management алата
26) Заштита ИКТ система у ревизијском испитивању	Техничке / процедуралне	Дефинисање процедура за тестирање, мониторинг током ревизије, ограничавање приступа тест окружењу, бекап пре тестирања

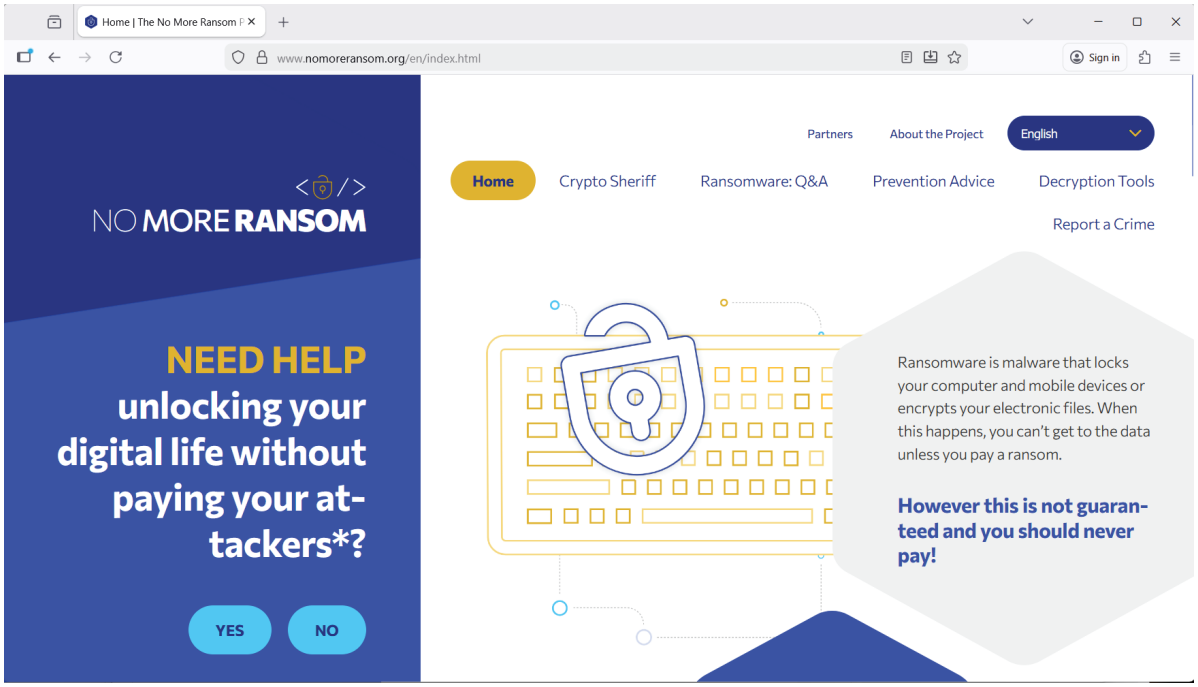
27) Заштита података у комуникационим мрежама	Техничке	Шифровање комуникације, firewall, сегментација мреже, IDS / IPS системи
28) Безбедност података у преносу унутар и ван оператора ИКТ система	Техничке	VPN, енкрипција, политика за размену података, коришћење сигурних канала за екстерну комуникацију
29) Испуњење захтева за информациону безбедност у свим фазама животног циклуса ИКТ система	Процедуралне / организационе	Дефинисање процедура за развој, тестирање, имплементацију и повлачење система, вођење документације о променама
30) Заштита података коришћених за тестирање ИКТ система	Техничке / процедуралне	Анонимизација тестних података, контрола приступа тестном окружењу, брисање тестних података након завршетка тестирања
31) Процедуре за чување и брисање информација у ИКТ системима	Процедуралне	Дефинисање политика data retention-а, аутоматизација брисања података, вођење евиденције о брисању
32) Заштита средстава оператора ИКТ система доступних пружаоцима услуга	Техничке / организационе	Ограничавање приступа екстерним партнерима, мониторинг активности, уговарање безбедносних захтева са партнерима
33) Одржавање уговореног нивоа информационе безбедности и услуга	Организационе / процедуралне	Праћење SLA, ревизија уговора, извештавање о безбедности, спровођење периодичних провера усклађености
34) Превенција и реаговање на безбедносне инциденте, размена информација, мере санације	Управљање инцидентима / процедуралне	Израда incident response плана, формирање тима за инциденте, вежбе симулације, комуникација са ЦЕРТ-ом, вођење евиденције о инцидентима
35) Мере континуитета пословања у ванредним околностима	Континуитет пословања	Креирање плана континуитета, резервне локације, тестирање опоравка, уговарање DR (disaster recovery) услуге
36) Усвајање докумената за проверу адекватности мера заштите	Организационе / процедуралне	Редовна ревизија политика, израда извештаја о усклађености, спровођење интерних и екстерних провера
37) Употреба мултифакторске аутентикације, безбедне комуникације у хитним случајевима	Техничке	Набавка и имплементација MFA решења, коришћење сигурних комуникационих канала (нпр. шифровани телефони), обука запослених за хитне процедуре

Табела 2: Мере заштите прописане Законом о информационој безбедности са улогама у превенцији и отпорности на рансомвер нападе

ПРИЛОГ 3. СЕРВИСИ ЗА САМОПОМОЋ

Пројекат "No more ransom" резултат је иницијативе Националне јединице за високотехнолошки криминал полиције у Холандији, Европоловог Европског центра за сајбер криминал и компанија Kaspersky и McAfee са циљем подршке жртвама рансомвера и враћању шифрованих података без плаћања откупнине криминалцима.

На овом сајту можете бесплатно добити кључеве за декрипцију неких од најпознатијих крипто алгоритама.



Слика 18: Изглед сајта
https://www.nomoreransom.org