Cyber napadi na radiološke sustave - pregledni red

Viculin, Davor

SVEUČILIŠTE U SPLITU
Podružnica
SVEUČILIŠNI ODJEL ZDRAVSTVENIH STUDIJA
DIPLOMSKI SVEUČILIŠNI STUDIJ
RADIOLOŠKA TEHNOLOGIJA

Davor Viculin

CYBER NAPADI NA RADIOLOŠKE SUSTAVE - PREGLEDNI RAD

Diplomski rad

Split, 2024. godine

SVEUČILIŠTE U SPLITU

Podružnica

SVEUČILIŠNI ODJEL ZDRAVSTVENIH STUDIJA

DIPLOMSKI SVEUČILIŠNI STUDIJ

RADIOLOŠKA TEHNOLOGIJA

Davor Viculin

CYBER NAPADI NA RADIOLOŠKE SUSTAVE - PREGLEDNI RAD

CYBER ATTACKS ON RADIOLOGICAL SYSTEMS - REVIEW

Diplomski rad/Master's Thesis

Mentor:

Izv. prof. dr. sc. Frane Mihanović

Split, 2024. godine

ZAHVALA

Zahvaljujem se obitelji na podršci pri izradi ovog rada

SADRŽAJ

TEMELJNA DOKUMENTACIJSKA KARTICA

DIPLOMSKI RAD

Sveučilište u Splitu
Sveučilišni odjel zdravstvenih studija
Diplomski studij radiološke tehnologije

Znanstveno područje: Biomedicina i zdravstvo
Znanstveno polje: Kliničke medicinske znanosti

Mentor: Izv. prof. dr. sc. Frane Mihanović

CYBER NAPADI NA RADIOLOŠKE SUSTAVE - PREGLEDNI RAD

Davor Viculin, 661105

Sažetak:

Napretkom digitalnih tehnika snimanja (digitalni receptori slike, CT, MR) računala, računalni programi, računalne mreže i digitalne baze podataka su postali jedan od temelja suvremen radiologije. Radiološki odjel ima specifičan način rada te postoje standardi kao što su DICOM za medicinske slikovne zapise, PACS za arhiviranje i komunikaciju te HL7 za razmjenu informacija medicinskom sustavu. Kako radiologija postaje ekonomski zanimljiva grana, postaje meta za cyber napade. Ujedno, radiološki sustavi sadrže mnogo osobnih podataka koji mogu biti interesantni pojedincima. Razlozi za napade su često ostvarivanje financijske koristi, ali mogu biti i politički, ideološki ili osobni. Početak napada može biti fizički pristup radiološkim uređajima ili mrežni pristup, i same DICOM datoteke mogu biti početak napada. Napade dijelimo na one koji izravno utječu na pacijente i one koji imaju utjecaj na samu infrastrukturu. Najpoznatije vrste su denial-of-service, malware, kriptografički napadi i promjene na postavkama uređaja. Kod obrane od cyber napada bitno je osiguranje komunikacije elektroničkom poštom jer je česta kod malware napada a na računalima i uređajima održavati programe ažuriranima prema uputama proizvođača, osobito antivirusne i firewall programe. Informatička služba radiološkog odjela treba paziti na račune svih korisnika i provjeravati ovlasti sukladno radnim mjestima kako ne bi došlo do zlouporabe. Mreže moraju imati ograničenja pristupa te podijeljena prema radilištima i namjeni kako bi se otežali neželjeni pristupi. Web proxy zaštita ograničava pristup Internet lokacijama koje su potencijalno opasne. Osnove mreže odjela kao što su serveri potrebno je i fizički osigurati od pristupa, najbolje prostorijom koja se zaključava a nalazi se pod video nadzorom i alarmom. DICOM datoteke trebaju biti enkriptirane najsigurnijim dostupnim algoritmima. Kao odgovor na cyber napade potrebno je imati dogovorene postupke i takav sustav mora uvijek biti spreman. Poznati napadi na radiološke sustave su Kwampiris, Petja/NotPetya, Ryuk, Wannacry, Conti skupina i BianLian.

Ključne riječi: Cybernapadi, radiološki sustavi, sigurnost mreža

Rad sadrži: 55 stranica, 17 slika, 62 literaturnih referenci

Jezik izvornika: hrvatski

BASIC DOCUMENTATION CARD

MASTER THESIS

University of Split
University Department for Health Studies
Radiological technology

Scientific area: Biomedicine and health care
Scientific field: Clinical medical sciences

Supervisor: Izv. prof. dr. sc. Frane Mihanović

CYBER ATTACKS ON RADIOLOGICAL SYSTEMS - REVIEW

Davor Viculin, 661105

Summary:

One of the basis of today's radiological devices are computers and networks. The radiology department has a specific way of working, and there are standards such as DICOM for medical image records, PACS for archiving and communication, and HL7 for information exchange in the medical system. As radiology becomes an economically interesting branch, it becomes a target for cyber-attacks. At the same time, radiological systems contain a lot of personal data that may be of interest to individuals. The reasons for the attacks are often financial gain, but they can also be political, ideological or personal. The start of an attack can be physical access to radiological devices or network access. The DICOM files themselves can be the trigger of an attack. We divide attacks into those that directly affect patients, those that have an indirect impact, and those that affect the infrastructure itself. The most well-known types are Denial-Of-Service, malware, cryptographic attacks and making changes of device settings. When defending against cyber attacks, it is also important to secure communication by e-mail because it is common in malware attacks, and to keep programs on computers and devices updated according to the manufacturer's instructions, especially antivirus and firewall programs. The IT department of the radiology department should keep an eye on the accounts of all users and check the authorizations according to the workplaces so that there is no misuse. Networks must have access restrictions and division according to workplaces and purposes in order to make unwanted access difficult. Web proxy protection restricts access to Internet sites that are potentially dangerous. The basics of the department's network, such as servers, must also be physically secured from access, preferably with a room that can be locked and is under video surveillance and an alarm. DICOM files should be encrypted with the most secure algorithms available. In response to cyber-attacks, it is necessary to have agreed procedures and such a system must always be on standby. Known attacks on radiological systems are Kwampiris, Petja/NotPetya, Ryuk, Wannacry, Conti group and BianLian.

Keywords: cyberattacks, radiological systems, network security

Thesis contains: 55 pages, 17 figures, 62 references

Original in: Croatian

1. UVOD

Upotreba računala postala je sastavni dio moderne medicine. Od svog uvođenja u obliku bolničkih informatičkih sustava (BIS) oko 1970-e, digitalnih načina snimanja kao što su kompjuterizirana tomografija (CT) i magnetna rezonancija (MR) 70-ih i 80-ih godina te kasnije 80-ih i 90-ih godina kao sustava za arhiviranje slika i komunikaciju (PACS). Danas nam ta tehnologija omogućava elektroničku razmjenu kliničkih informacija između regija, nacija i kontinenata. Usporedno s razvojem računala i njihove primjene u medicini, stvorili su se novi izazovi, a jedna od tema koja postaje sve važnija za bolnice je kibernetička sigurnost (*cyber security*) kao odgovor na potencijalne *cyber* napade (kibernetičke napade) (1).

Posljednjih godina, hakeri su uspjeli kompromitirati većinu medicinskih uređaja, od pumpe za infuziju pa do rendgenskih uređaja. U jesen 2013., Mayo klinika zaposlila je skupinu hakera kako bi probali modificirati 40 različitih medicinskih uređaja. Nakon nekoliko tjedana tražeći sigurnosne propuste, kod svih uređaja uključujući i magnetsku rezonanciju i ultrazvuk, pronađene su slabe točke (2).

Koncept *hackiranja* i uporaba zlonamjernih programa kao alat za *cyber* napade javlja se ranih 1970-ih. Činjenica da je danas većina IT sustava u svijetu bar donekle povezana s internetom uzrokovala je dramatičan porast takvih incidenata koji se više ne pripisuju samo znatiželji pojedinaca nego i organiziranim kriminalnim skupinama (1).

Osobito velik problem stvara *ransomware*, koji je napravljen da šifrira (kriptira) određene bitne podatke te se za njihovo vraćanje pravom vlasniku traži otkupnina. Prema izvještaju Ministarstva pravosuđa SAD-a, 2016., u 2016. je bilo 4000 takvih napada, što je četverostruko više nego godinu ranije. Na zdravstveni sektor otpada oko 15% takvih napada što nije zanemarivo, a takva vrsta napada prema statistici iz 2017. je činila 50% *cyber* incidenata u bolnicama (3).

Političari diljem svijeta prepoznali su da je zdravstveni sustav dio kritične društvene infrastrukture koju treba zaštititi od svih napada pa tako i *cyber*. Primjerice, US National Infrastructure Protection Plan pruža plan zaštite pod nazivom Healthcare and Public Health Sector-Specific Plan (4), dok Europska Unija osnovala Agenciju za mrežnu informatičku sigurnost (EU Agency for Network and Information Security /ENISA) (5). *Cyber* napadi na bolničke sustave danas imaju višu dimenziju. Dok su takvi napadi nekad

bili prošireni i nasumični, danas su sve više orijentirani na konkretni sektor u zdravstvu, zavisno o uskim potrebama i interesima grupa iza njih. Radiološki uređaji zanimljivi su za napade jer su bitni dio svake zdravstvene ustanove, a njihova računalna razvijenost stvara mnogo mogućnosti za *cyber* napade.

2. CILJ RADA

Cilj ovog preglednog diplomskog rada je pokazati da *cyber* napadi na radiološke sustave nisu samo povremeni bezopasni incidenti već postaju rizični događaji. Prikazi do sad poznatih načina napada na sustave, tehnike obrane te primjena povrata podataka mogu biti korisni u svakodnevnom radu radiološkog odjela. Iskustva i savjeti iz drugih radioloških odjela i bolnice iz svijeta mogu pomoći da se njihove greške ne ponove drugima. Primjeri napada iz svijeta bi trebali motivirati na povećanje pažnje na *cyber* sigurnost u radiologiji.

3. IZVORI PODATAKA I METODE

Rad je napisan kao pregled dostupnih znanstvenih radova sa medicinskih baza podataka kao što su PubMed, uputa sa službenih stranica sigurnosnih agencija Europe i SAD-a koje su se odnosile na *cyber* sigurnost radioloških sustava. Korišteni su i radovi objavljeni u publikacijama radioloških društava raznih zemalja, a knjige su iz vlastite arhive stručne literature ili su njihovi dijelovi koji su bili korisni za ovaj rad dostupni besplatno. Podaci o *malware* napadima su iz izvještaja bolnica i lokalnih medija te objava samih *cyber* napadača.

4. RASPRAVA

4.1. OSNOVE RADIOLOŠKIH SUSTAVA

Radiološki odjel unutar bolničkog informatičkog sustava (BIS) zbog specifičnosti načina rada zahtjeva drugačiju i vlastitu mrežu, radiološki informacijski sustav (RIS), a s njim odgovarajuća računala i programe. Radiologija kao slikovna grana medicine mora biti spremna u svojem sustavu svakodnevno obraditi velike količine datoteka koje osim slikovnih zapisa sadrže i podatke o pacijentu, načinu izvođenja pretrage, korištenom uređaju te razne druge, zavisno koja pretraga je rađena. Veličina takvog skupa podataka za jednog pacijenta može biti i do 600 Mb, a ponekad i više (6).

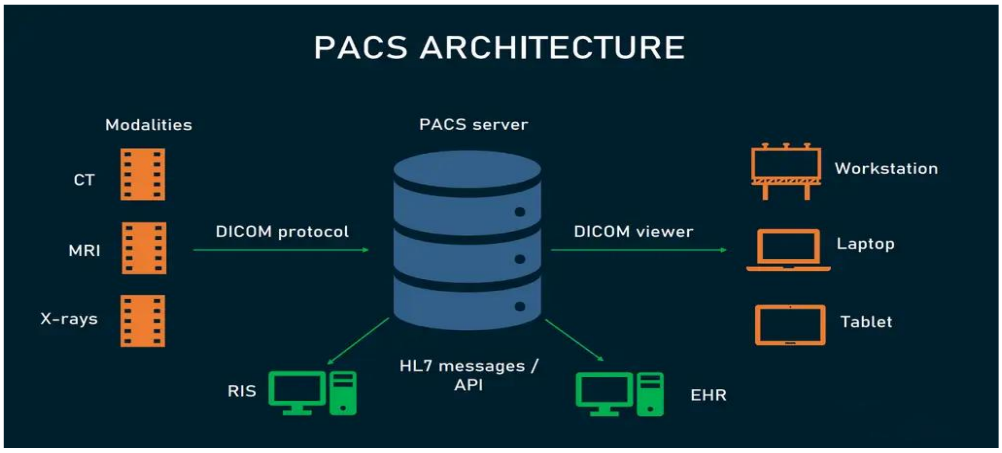
RIS zahtjeva mnogo mjesta za pohranu digitalnih podataka. Podaci svakog pojedinog pacijenta moraju se pohranjivati, svaki dan postoje novi zapisi za nove pacijente a podaci onih obrađenih moraju se čuvati još nekoliko godina što je i zakonska obaveza. Sve to utječe na njegovu brzinu, jer je njegova uloga da ubrza rad radiološkog odjela tako da svi podaci budu brzo i jednostavno dostupni na svim računalima povezanim u mrežu (Slika 1.).

Prilikom implementacije RIS-a treba obratiti pozornost i na standarde poput:

• DICOM (Digital Imaging and Communications in Medicine),

• PACS (Picture Archiving and Communication System)

• HL7 (Health Level Seven)



Slika 1. PACS arhitektura

Izvor: https://www.altexsoft.com/blog/pacs-vna/

4.1.1. DICOM

DICOM (Digital Imaging and Communications in Medicine) međunarodni je standard za medicinske slike i povezane informacije. Definira formate za medicinske slike koje se mogu razmjenjivati zajedno s pisanim podacima i potrebnom kvalitetom za kliničku upotrebu. On je implementiran u gotovo svaki radiološki i radioterapijski uređaj (rendgen, CT, MRI, ultrazvuk itd.), a sve više i u uređaje u drugim medicinskim domenama kao što su oftalmologija i stomatologija. Sa stotinama tisuća medicinskih uređaja za snimanje u upotrebi, DICOM je jedan od najraširenijih zdravstvenih standarda za slanje u svijetu. Trenutno postoje doslovno milijarde DICOM slika koje se koriste za kliničku skrb.

Od svog prvog objavljivanja 1993. godine, DICOM je revolucionirao praksu radiologije, zamijenivši rendgenski film s potpuno digitalnim načinom rada. Kao što je internet postao platforma za nove aplikacije i razmjenu informacija, DICOM je omogućio naprednu primjenu medicinskih prikaza koji su promijenili kliničku medicinu. Od odjela za hitni prijem i srčanih stanica do otkrivanja raka dojke, DICOM je standard koji čini medicinsku slikovnu obradu učinkovitom za liječnike i za pacijente.

DICOM je priznat od strane Međunarodne organizacije za standardizaciju kao standard ISO 12052. (7)

4.1.2. PACS

Sustav za arhiviranje i komunikaciju slika (PACS) je brzi, grafički, računalni mrežni sustav za pohranjivanje, oporavak i prikaz radioloških slika (ultrazvuk, rendgenski snimak, kompjutorizirana tomografija, pozitronska emisijska tomografija, endoskopija i magnetska rezonancija). To je tehnologija koja omogućuje ekonomičnu pohranu i praktičan pristup slikama iz više izvora, zamjenjujući konvencionalne filmove digitalnim slikama. Također povezuje očitanja različitih dijagnostičkih prikaza, čime se omogućuje istovremeno gledanje i slika i njihovih odgovarajućih nalaza. PACS rješava probleme povezane s konvencionalnim filmovima. Na primjer, filmovi su dostupni samo na jednom mjestu u isto vrijeme i često se povezuju s kašnjenjem u skrbi za pacijenta kada nisu odmah dostupni liječniku. Studije pacijenata mogu se pregledati s bilo kojeg računala spojenog na sustav.

Tipični PACS sastoji se od mreže razumne propusnosti, uređaja ili modaliteta za digitalnu sliku, softvera za arhiviranje/usmjeravanje, dijagnostičkih radnih stanica i općenito neke interakcije s bolničkim ili radiološkim informacijskim sustavom.

PACS ima četiri glavne namjene: upravljanje radiološkim radnim procesom, platforma za integraciju elektroničke slike (s bolničkim informacijskim sustavima, elektroničkim medicinskim zapisima i radiološkim informacijskim sustavima), daljinski pristup (pregledavanje i izvješćivanje izvan na različitim lokacijama, obrazovanje na daljinu i tele-dijagnostika) i zamjena tiskane kopije.

Prednosti PACS-a su: izravna ušteda troškova, smanjena potrošnja radiografskog filma, smanjeni troškovi rada, povećana integracija između odjela i ustanova, poboljšanja produktivnosti, bolja kvaliteta slike, simultano gledanje istih slika na više lokacija i smanjeno vrijeme tumačenja i priopćiti dijagnozu (8).

4.1.3. HL7

HL7 (Health Level 7) je sustav standarda za razmjenu, integraciju, dijeljenje i pronalaženje elektroničkih zdravstvenih informacija. Ovaj standard definira kako se informacije pakiraju i prenose s jedne strane na drugu, postavljajući jezik, strukturu i tipove podataka koji su potrebni za besprijekornu integraciju između sustava. HL7 standard služi za kliničku praksu i upravljanje, isporuku i evaluaciju zdravstvenih usluga, te se u svijetu najviše koristi (9).

4.2. RAZLOZI I NAČINI UPADA U RADIOLOŠKE SUSTAVE

Negativna popratna pojava širenja interneta je povećanje incidenata u *cyber* sigurnosti, primjerice računalni virusi, *ransomware* (traženje otkupnine za povrat pristupa podacima) ili krađa podataka o pacijentu. Dok su u prošlosti *cyber* napade najčešće uzrokovali radoznali amateri, danas se najviše pripisuju organiziranom kriminalu ili drugim organiziranim grupama. Sukladno tome, napadi na bolnice dobivaju novu dimenziju, jer nisu više slučajni nego se sve više usredotočuju na bolničke sustave koji postaju primarna meta.

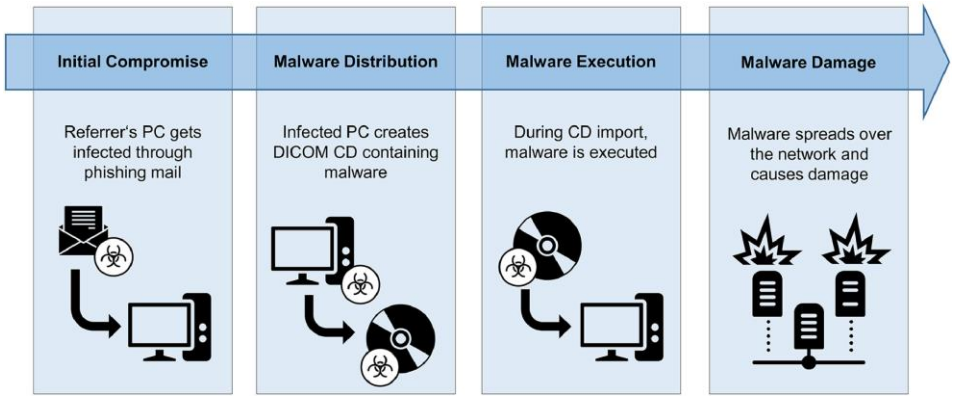
Najčešće razloge možemo podijeliti prema krajnjem cilju:

- Krađa podataka za financijsku korist, traženje otkupnine za kriptirane podatke ili njihova prodaja trećoj strani
- Špijunaža i napadi na državnoj razini, često potpomognuti od strane država kako bi dobili pristup radiološkim podacima u političke, ekonomske ili vojne svrhe (npr. zdravstveno stanje protivnika iz oporbe)
- Sabotaža i blokiranje, izazivanje kaosa i utjecaj na medicinske postupke iz ideoloških razloga ili u svrhu protesta
- Krađa identiteta, radiološke snimke i nalazi mogu sadržavati osobne podatke koji se mogu koristiti za razne prevare

4.2.1. Unos podataka o pacijentu sa prijenosnog medija

Pacijenti ponekad sami donose svoje podatke na medijima za pohranu u bolničku ustanovu kako bi terapijski ili dijagnostički postupak bio precizniji ili uopće moguć. Primjerice, kod kontrolnih radioloških postupaka bitna je usporedba sa starim nalazima i slikovnim zapisima. To može biti problem ukoliko dijagnostika nije rađena u istoj ustanovi te radiolog nema pristup starim podacima koje bi morao usporediti s novima. Jednako tako, prilikom reiradijacije u radioterapiji (ponovnog zračenja nekog područja ili novog polja zračenja u blizini tretiranog) potrebno je imati zapis svih prethodnih tretmana. Pacijent pritom donose svoj medij na kojem se mogu nalaziti zloćudni programi (*malware* ili virus). Ovakav scenarij započinje tako što se virus nalazi na računalu na kojem su se podaci snimali na CD ili USB. Tamo je mogao doći nepažljivim otvaranjem neželjenih i lažnih poveznica u elektroničkoj pošti i webu, pokretanjem zaraženih dokumenata ili piratskih programa. Virus se može dalje širiti tako što se ubacuje u svaku iduću datoteku koja se otvara ili mijenja na računalu. Većina sustava koji snimaju DICOM CD dodaju na medij i program za pregled snimaka koji radi na standardnim Windows sustavima, kako bi svaki korisnik mogao otvoriti zapis, u slučaju da DICOM radna stanica nije dostupna. Takvi CD-i po standardu imaju uključenu *autorun* funkciju, odnosno datoteku koju Windowsi sami pokreću čim računalo prepozna novi ubačeni medij u CD jedinicu, te datoteku u kojoj je spisak naredbi koje se pritom izvode. Tako se virus sa

prvog računala, preko DICOM CD-a može samostalno presnimiti na drugo računalo i to samim umetanjem medija bez potrebe da korisnik mora napraviti daljnju radnju (Slika 2.).



Slika 2. Unos malware-a sa prijenosnog medija

Izvor: https://www.sciencedirect.com/science/article/pii/S1076633220301719

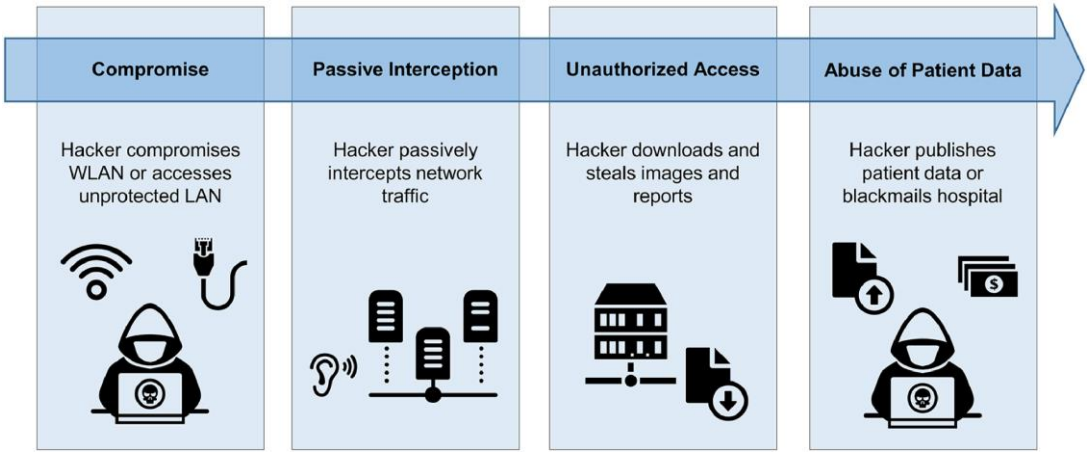
Zadnja faza napada je pokretanje samog virusa na novom računalu. Od ovog koraka su po definiciji zaštićene DICOM radne stanice, jer se ne pokreće preglednik nego program uzima gotove podatke s CD-a, pod pretpostavkom da radna stanica ima gotov preglednik u sebi te samo učitava slikovne zapise koji u ovom slučaju nisu zaraženi, odnosno dio napada. Pokretanje preglednika s virusom na drugim sustavima (npr. drugi uredski PC sa Windowsima na kojem se zapisi pregledavaju) aktivira virusni dio datoteka. Oni zatim mogu pokrenuti neke druge radnje ili se preko interneta spojiti na server pod kontrolom autora virusa te skinuti i pokrenuti druge programe. Time su stvoreni preduvjeti za razne tipove napada. Virus može presresti internet promet te poslati korisničko ime i šifru korisnika napadaču na server, može se dalje širiti mrežom kako bi obuhvatio još veći broj korisnika ili ono danas najčešće – *ransomware*. Takav tip napada zaključava/šifrira podatke korisnika i šalje mu poruku da mora platiti otkupninu kako bi mogao ponovno pristupiti svojim podacima (10).

U zadnje vrijeme pojavila se nova tehnika ovakvog napada, gdje napadač namjerno ostavlja USB, vanjski tvrdi disk ili CD na parkingu bolnice očekujući da će ga pronaći neki savjesni zaposlenik i spojiti ga na bolničko računalo kako bi provjerio tko je vlasnik (11).

U eksperimentu Ministarstva domovinske sigurnosti SAD-a, 60% njihovih zaposlenika koji su pronašli uređaj (USB, HD, CD) na parkiralištu, probali su provjeriti vlasnika na radnom mjestu. Ukoliko je na istom mediju postojala oznaka ustanove, udio se popeo na 90% (12).

4.2.2. Napad na mrežu

Osnova je napada na mrežu kad haker uspije pristupiti mrežnom sustavu bolnice. Prva je opcija ukoliko ima pristup nezaštićenom mrežnom priključku preko kabela. Druga je da uspije dešifrirati lozinku za bežični pristup (Slika 3.). Tijekom vremena otkrivene su slabosti svih mehanizma zaštite bežičnih mreža, od prvotne WEP (Wired Equivalent Privacy) do WPA2 (Wi-Fi Protected Access 2) koji se često i danas koristi. 2017. otkriven je uspješan oblik napada na WPA2 pod nazivom KRACK (Key Reinstallation Attacks) koji ponavljajući ključeve za provjeru spajanja omogućuju pristup bežičnoj mreži za koji napadač nema pristupnu lozinku (13).



Slika 3. Mrežni pristup u cyber napadu

Izvor: https://www.sciencedirect.com/science/article/pii/S1076633220301719

Nakon pristupa, pasivnim presretanjem podatkovnog prometa dolazi do podataka o strukturi mreže, sistema koji se koristi, korisničkih podataka i vrsti protokola. I DICOM i HL7 koji se koriste u radiološkim sustavima u osnovi šalju nezaštićene međusobne

poruke u tekstualnom formatu. To omogućuje potencijalnom napadaču sa pristupom mreži da pasivno presreće i analizira promet na mreži. Jedan od najpoznatijih programa za analizu protoka na mreži je Wireshark koji izričito podržava HL7 i DICOM protokole (14). Jedna od njegovih mogućnosti je i da pasivno ulovljene DICOM slike spremi kao DICOM datoteku, kao i imena pacijenata, demografske podatke i oznake pacijenata koji trenutno borave u bolnici.

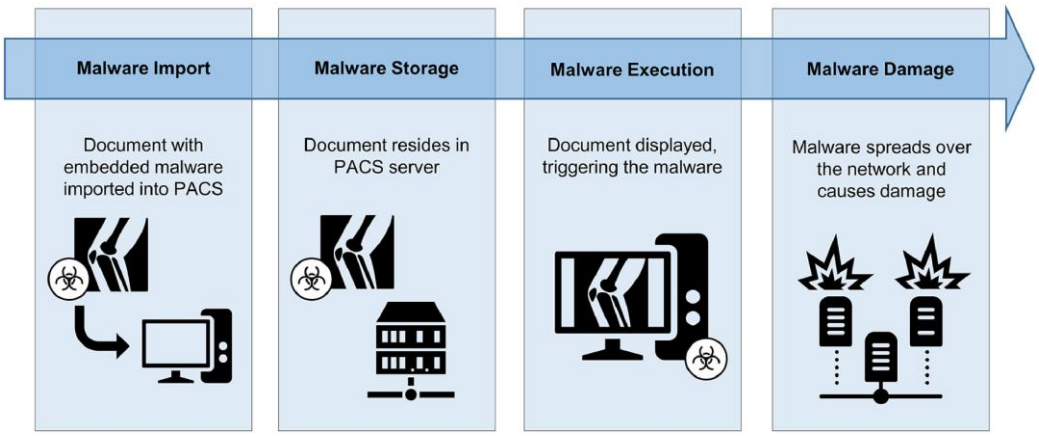
Zadnja faza ovakvog napada je pristup samoj mreži kako bi se skinuli slikovni zapisi i izvješća o pacijentima. Iako je ovo malo otežano jer DICOM C-MOVE protokol koji se često koristi zahtjeva od PACS-a zasebnu mrežu te samo računala na popisu imaju pristup PACS serverima, još uvijek je moguće prikupiti ostale podatke o pacijentu (10).

Nova metoda napada na mrežu je upotreba dronova. Ovakve bespilotne letjelice omogućavaju napadaču da pristupe blizu skoro svakoj bolničkoj mreži, a smatra se da je 10 metara dovoljno (15). U dva pokusa, dronovi su navođeni na teško dostupna mjesta iznad bolnica te se preko njih uspjelo neprimjetno spojiti na mrežu. Dronovi prvotno koriste metodu odjave, gdje su korisnici primorani odspojiti se sa bolničke mreže. Zatim dron postavi sebe kao pristupnu točku, te prevarom navede korisnike da se spoje na njegovu mrežu. Unošenjem korisničkih podataka na lažnu mrežu drona, napadači imaju korisničke podatke i pristup bolničkoj mreži. Dronovi također mogu poslužiti i za stvaranje komunikacijskog lanca između napadača i računala žrtve. Time se smanjuje mogućnost otkrivanja ili praćenja napadača (16).

4.2.3. Malware u DICOM formatu

Jednako kako se ponekad *malware* ubacuje u .docx (Microsoft Word) i .pdf (Portable Document Format) datoteke, koje prilikom otvaranja pokreću zlćudne skripte, postoji način da se to napravi i sa DICOM datotekama. To je mnogo kompliciranije od prethodnih načina jer zahtjeva detaljno znanje o manjkavostima programa korištenih u radiologiji, fizički pristup uređajima te detaljnu analizu radiološkog mrežnog sustava. S druge strane, moguća šteta od ovakvih napada je vrlo velika jer djeluju u PACS-u iza firewalla. *Malware* ubačen u DICOM slikovni zapis ili izvještaj u istom formatu ne aktivira se na uređaju gdje se importira u PACS mrežu nego na samu radnu stanicu ili server. Tek kasnije, kada radiolog, tehnolog ili drugi zaposlenik otvara dokument, *malware* se aktivira ili na dijagnostičkoj radnoj stanici ili na samom PACS serveru te se

tamo već nalazi iza firewall-a (Slika 4.). Aktivacijom na serveru, prisvaja pristup cijeloj PACS arhivi te može šifrirati ili prebrisati dijelove arhive kao primjerice dio *ransomware* napada. Postoje tri glavna načina kako se *malware* ubacuje u DICOM format (10).



Slika 4. Prikrivanje malware-a i DICOM format

Izvor: https://www.sciencedirect.com/science/article/pii/S1076633220301719

4.2.3.1. Zloupotreba uvoda u DICOM format

DICOM format datoteka je definiran da u prvih 128 *byte*-a ne sadrži ništa od DICOM standarda nego proizvoljne informacije. Tako je napravljeno kako bi DICOM objedinio dvije vrste informacija: jednu kao slikovni DICOM zapis a drugi kao valjani slikovni format s mogućnosti stavljanja oznaka. To otvara mogućnost da se umjesto proizvoljnih informacija u prvom dijelu DICOM-a može napraviti Windows program koji se može pokrenuti kao aplikacija. Prema izvješću i dokazu o konceptu istraživača informatičke sigurnosti Ortiza iz travnja 2019. godine, on je nazvao takve datoteke PE/DICOM, Windows prijenosne pokretačke datoteke ("*Portable Executable*" + DICOM) (10).

4.2.3.2. Malware pridodan u zatvoreni DICOM objekt

DICOM standard ne podržava samo pohranu i prijenos slika nego postoje i oblici za razne druge vrste informacija kao što su signal EKG-a, mjerenja ili izvještaji. Konkretno, današnji DICOM standard podržava dodavanje drugih tipova datoteka u

DICOM datoteku. To su primjerice .pdf (popularni vektorski format za tekst), HL7 -.cda (klinički dokumenti sa tekstualnim, slikovnim, zvučnim zapisom), .stl (3D pisači) i .obj koji se često koristi za 3D objekte i virtualnu stvarnost. Svaki taj zapis ima vlastite sigurnosne rupe. PDF format jako je kompleksan i podržava skripte koje se mogu pokrenuti, te je kao format u prošlosti već bio poznat kao sigurnosno rizičan. Postoje dva najpoznatija rizika, jedan je preko skripti uklopljenih u njega, a drugi preko zlođudno promijenjenih dokumenata koji namjerno prekomjerno opterećuju sustav te uzrokuju pogreške. NIST, američki Nacionalni Institut za znanost i tehnologiju u svojoj bazi podataka o sigurnosnim rupama trenutno navodi ukupno 1895 prijavljenih sigurnosnih propusta od kojih su 17 trenutno aktualna (17). Većina DICOM aplikacija nema vlastiti čitač .pdf datoteka već koriste gotova rješenja, a s njima preuzimaju i njihove sigurnosne propuste. Za .cda datoteke nema podataka da imaju propusta ali one mogu sadržavati u sebi i .pdf. Glavni rizik .stl datoteka za 3D ispis dokumentirali su Strum i sur. (10) gdje su zlođudnom manipulacijom .stl 3D pisači napravili predmet koji izvana izgleda ispravan, dok mu je unutarnja građa manjkava, što može biti pogubno kod izrade implantata ili pomagala u radioterapiji.

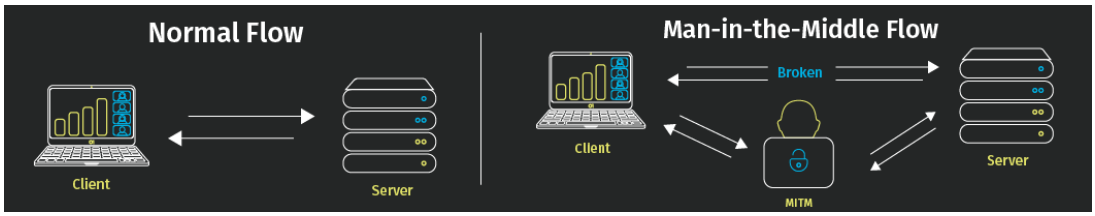
4.2.3.2. Malware baziran na izmjenama u sažimanju DICOM slika

DICOM standard podržava pohranu i prijenos komprimiranih slika i to na veliki broj načina, povratno i nepovratno. Kao slikovni format najčešće se radi od .jpeg datotekama, a kao video zapis .mpeg. Cijeli DICOM se može komprimirati na slični algoritam kao i kod .zip datoteka. Potencijalni napadač može napraviti zlođudnu komprimiranu DICOM datoteku koja će prilikom otpakiranja nakon nekoliko koraka pokrenuti zlođudnu skriptu. Jednostavnost ovakvog tipa napada prikazana je 2004. godine kada je u Windowsima otkrivena sigurnosna rupa pod nazivom CVE-2004-0200, preko koje svaka .jpeg datoteka predstavlja potencijalnu opasnost, a preko nje i svaki DICOM preglednik koji ju podržava (18). Drugi primjer je „Stagefright“ ranjivost, odnosno trema (eng.), prema bazi programa na Android operativnim sustavima. U ovom slučaju sami primitak datoteke je dovoljan da se aktivira zlođudna skripta, bez potrebe za otvaranjem (19).

Zloćudni programi na osnovi promijenjenih komprimiranih DICOM datoteka mogu biti upotrjebljeni za napad na PACS servere. Kada DICOM radna stanica pokuša povući slike, može „pregovarati“ sa serverom da li se prijenos treba odviti sa komprimiranim ili nekomprimiranim datotekama. Ako radna stanica ne podržava komprimirane datoteke, zadatak servera je da ih otpakira, te se će se pokretanje zloćudnih skripti dogoditi na samom serveru.

4.2.4. Presretanje komunikacije

U ovom slučaju radi se u umetanju malog računala u vezu između samog radiološkog uređaja (npr. CT, MR…) i radne stanice, servera ili mreže općenito (Slika 5.). Naziva se i *man-in-the-middle* napad („čovjek u sredini sustava“). Ovakav način napada izgleda bezazleno osoblju jer današnja računala mogu biti jako mala a i takvi prostori sadrže puno veća računala i radne stanice. Glavni problem ovdje je što takav napad zahtjeva fizički pristup prostorima. Također potrebno je poznavanje sustava radiološkog odjela ili bolnice i pažljivu pripremu. Ubačeno računalo postavljeno od strane napadača neprimjetno presreće, analizira i prosljeđuje sve DICOM slike koje šalje radiološki uređaj. Pridodano „uljez“ računalo može otvoriti vlastitu bežičnu mrežu kako bi presretalo druge komunikacijske kanale, primjerice hvatalo korisnička imena i lozinke i omogućilo kontrolu na daljinu od strane napadača (10).



Slika 5. Presretanje mreže (Man-in-the-middle napad)

Izvor: https://www.veracode.com/security/man-middle-attack

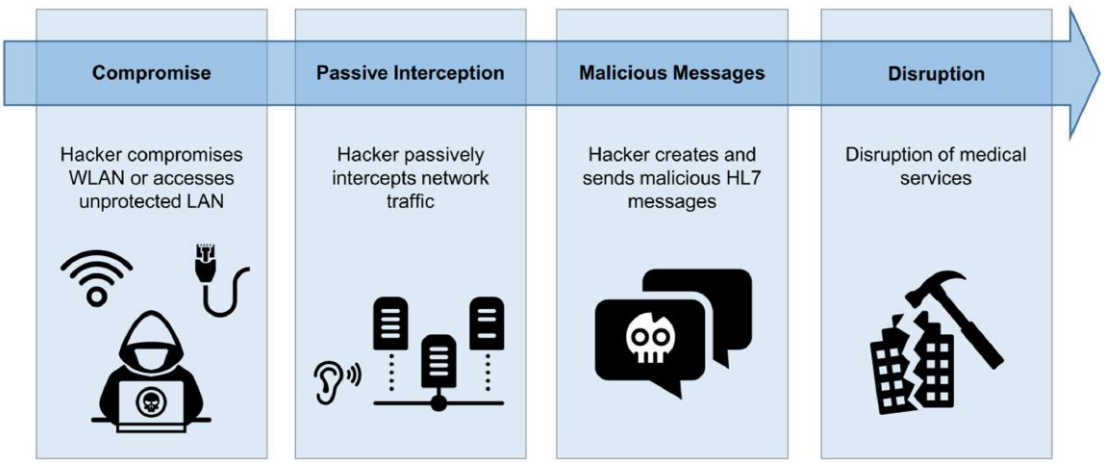
Man-in-the-middle napad koji se izvodi na sistemu cijelog radiološkog odjela mijenja podatkovne pakete, prikazuje lažne prikaze na ekranima te preuzima potpunu kontrolu. Pažljivi operater na radiološkom uređaju mogao bi primijetiti da se npr. strelica

miša pomiče neovisno o njegovom radu, što indicira uljeza na istim kontrolama. Napadač tako može napraviti postupke i izvršiti naredbe kojima se ošteti uređaj ili ozljeđuje pacijent. „Address resolution protocol“ oblik napada je jedan od popularnijih, gdje se promjenom MAC adrese uređaja i IP adrese u tablici koja služi za sigurnost komunikacije, podaci šalju na pogrešno računalo. Kod „*replay*“ napada, podaci se mijenjaju te se ponovno vraćaju u sustav kako bi napad ostao neprimjetan. Treća vrsta napada je slanje lažnih poruka, „*spoofing*“ na uređaj. Tako se operater može zavarati lažnom porukom na uređaju da je potrebna neka radnja, ili prikriti stvarnu potrebu za intervencijom (2).

4.2.5. Infiltracija mreže krivim HL7 porukama

Dok DICOM pokriva većinu komunikacije za rad u PACS okruženju, HL7 poruke često se koriste kako bi podaci bili dosljedni i u ostalim sustavima koji se koriste u bolnicama ili ustanovama, kao što su bolnički informacijski sustav (BIS), radiološki informacijski sustav (RIS) ili PACS. HL7 poruke koriste se kako bi najnoviji podaci o pacijentu bili dostupni u cijelom mrežnom sustavu. Pod tim se smatra i ažuriranje podataka nekog pacijenta, u slučaju promjene imena i prezimena, adrese, telefonskog broja ili spajanje dva pacijenta u jednog. To se događa u slučaju da je ista osoba upisana različito na odvojenim odjelima, što se događa zbog ljudske pogreške ili hitnog prijema kada zbog zdravstvenog stanja nije izvršena potpuna identifikacija već upisanog pacijenta.

Napadač pasivnim praćenjem HL7 podataka preko mreže, može doći do informacija o prijemu na odjel, uputnicama, dijagnozama i laboratorijskim nalazima (Slika 6.). Na jednak način, može dodavati ili mijenjati postojeće HL7 poruke. Razlog za ovo je pridobiti pristup mreži, preko nezaštićenog kabelskog ili bežičnog priključka (10).



Slika 6. Ubacivanje krivih HL7 poruka

Izvor: https://www.sciencedirect.com/science/article/pii/S1076633220301719

4.3. VRSTE NAPADA

Cyber napadi mogu ciljati radiološke sustave na tri nivoa. Primarna infiltracija odnosi se na napad koji ima izravan utjecaj na bolničke pacijente. Sekundarnim se smatra ako ima samo posredni utjecaj ali ne i direktan, te mogu biti vezani sa primarnim. Tercijarna infiltracija ima šire značenje, odnosi se na napad na infrastrukturu kao što su napajanja ili mreže (20).

Na svim nivoima, postoji neki općeniti slijed događaja. Potencijalni napadač prvo pokušava pristupiti bolničkoj mreži ili opremi, ako se radi o postavljanu među-uređaja. Kada dobije pristup, procjenjuje koje informacije i mogućnosti ima sa dobivenim ovlastima, te ih uspoređuje sa vlastitim namjerama. To je kritični korak kako bi pojedinac ili skupina uspjela u namjeri, a da pritom izbjegne otkrivanje osobnih podataka. Vrhunac napada je kada napadač zbog ranjivosti sustava osiguranja uspije u svojoj namjeri (21).

Radnje u zadnjem koraku mogu se podijeliti na aktivne i pasivne. Aktivnim se smatraju namjerno prodiranje u funkcije sustava, kao što je podešavanje ili zaustavljanje rada, te presretanje i promjena podataka prikupljenih preko radioloških uređaja. Pasivni napad znači pristup i prikupljanje medicinskih slikovnih zapisa i sličnih informacija (15).

4.3.1. Denial-of-service

Napad kojem je cilj zagušiti sva računala spojena u neku mrežu i tako im onesposobiti komunikaciju naziva se Denial-Of-Service napad (DoS). U slučaju kad je takav napad izveden od strane više računala (kako bi napad bio učinkovitiji) koja sinkronizirano šalju podatke kako bi umanjila resurse potrebne za rad mreže, kao što su procesor, memorija ili brzina mrežne izmjene podataka naziva se distribuirani DoS , DDoS. Smatra se da je ovo najjači oblik napada kojim se može onesposobiti mrežni rad. Tako se može utjecati na rad jednostavnih stranica, pa do mreža ustanova, gradova ili cijelih zemalja (22).

Kod radioloških mrežnih sustava, ovakav napad može (23):

- •Umanjiti učinkovitost mreže radiološke opreme
- •Uzrokovati kvarove na opremi
- •Zaustaviti rad mreže na radiološkom odjelu ili cijeloj bolnici

DDoS napad može poslati velik broj DICOM poruka kako bi opteretio server, što dovodi do prestanka rada. Drugi način je namjerno slanje oštećenih DICOM datoteka kako bi se otežao rad ili dovelo do pada sustava (24).

4.3.2. Malware – neovlašteni program umetnut u računalo

Izraz je nastao kao skraćenica „malicious software“, odnosno zlćudni software. M*alware* je pojam koji pokriva široki spektar potencijalno opasnih programa. Posebno je napravljen kako bi napadač pridobio pristup nekom računalu, preuzeo podatke i informacije te oštetio ciljani računalni sustav. *Malware* se smatra svaki program koji ima zlćudnu namjenu kao što su uzrokovanje kvara, onemogućavanje rada ili ograničavanje kontrole pravog vlasnika i pridobivanje kontrole od strane napadača. Najčešći oblici su virusi, crvi (šire se dupliciranjem po drugim računalima), *keyloggers* (prate korisnikovu upotrebu tipkovnice, redoslijed i tipke), trojanski konji (zlćudni program koji se prikrije kao bezopasan), *ransomware* (zaključava određene datoteke te za povrat vlasniku zahtjeva npr. otkupninu ili drugu uslugu) (25).

Prema izvješću NTT Data iz 2017. godine ("2017 Global Threat Intelligence Report“), u ukupnom broju *ransomware* napada u svim granama gospodarstva, zdravstvene organizacije su imale 15%, dok se u samom zdravstvu *ransomware* odnosio na 50% incidenata (26).

4.3.3. Kriptografički napad

Kriptografički napad izvodi se kako bi se otkrili podaci koji su sakriveni, odnosno dešifrirale informacije koje nisu namijenjene trećim osobama (21). Kriptografija je postupak šifriranja i dešifriranja informacija u kodove koje samo pošiljatelj i primalac mogu razumjeti (27). Način šifriranja prikriven je od drugih potencijalnih korisnika informacija i taj algoritam poznat je samo autoru kako bi se zadržala privatnost (28). Kod radioloških sustava, kriptografskim napadom smatramo kada pojedinac želi nadgledati, ukrasti, promijeniti, pobrisati ili oštetiti informacije o pacijentu ili njegove slikovne medicinske zapise (11).

Osim klasičnih napada na radiološke sustave kako bi se napadači okoristili podacima za traženje otkupnine ili prodaju na crnom tržištu, postoji mogućnost da pojedinac mijenja CT ili MR slikovne zapise. Dodavanjem ili oduzimanjem dokaza o bolesti na volumnim medicinskih snimkama, može se primjerice zaustaviti politički kandidat, sabotirati istraživanje, izvršiti prevara osiguranja ili čak usmrtiti (29).

Medicinski zapisi CT ili MR uređaja snažan su dokaz medicinskog stanja. Pacijenti se često liječe prema njihovim nalazima bez potrebe za dodatnim pretragama, osobito kod hitnih stanja. Neke dijagnoze se i ne mogu drukčije postaviti, poput primjerice ozljede meniskusa ili nekih tipova raka dojke. Napadač može dodati ili maknuti dokaze o aneurizmi, ugrušku, upali, tumora mozga ili ozljede kralježnice, čime može radikalno utjecati na tijek liječenja (29).

Drugi razlog su prevare osiguranja, gdje pojedinac može ostvariti osobnu dobit na temelju lažiranih nalaza. Ovdje nema rizika ozljede za druge a moguće je dobiti povlastice. Na primjer:

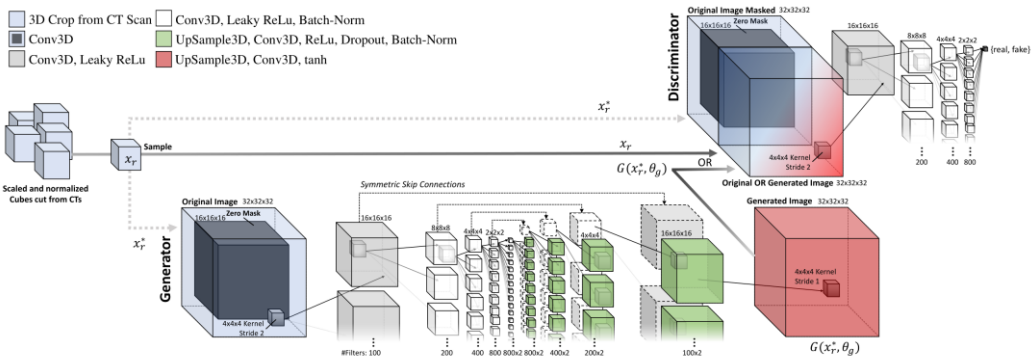
- Osoba ugovori životno ili neko drugo osiguranje
- Lažira prometnu nesreću ili drugi nesretni događaj

- Žali se na radnu nesposobnost ili drugu otegotnu okolnost
- Na CT ili MR zapis pridoda izljev krvi u mozak, frakturu kralješka…
- Sa nalazima ostvari dobit od osiguranja

Kod ciljanih napada, pacijent može biti namamljen na dijagnostički pregled dodajući termin u bolnički sustav, lažirajući poziv za nacionalni screening neke bolesti ili hakiranjem rutinskih laboratorijskih testova. Visoki PSA je indikacija za karcinom prostate te se radi MR abdomena, visoki tirotropin može biti indikacija za tumor mozga te se radi MR glave a metanefrin u urinu ukazuje na mogući tumor te se radi MR toraksa i abdomena (29).

Kako bi proces bio uspješan i anatomski realističan, slijede se koraci (Slika 7.) (28):

1. Određivanje mjesta na CT/MR zapisu gdje se dokaz treba dodati ili ukloniti
2. Izrezivanje „kocke“ sa te pozicije
3. Dodavanje/uklanjanje željenog objekta (znaka bolesti)
4. Popravljanje izmijenjene „kocke“ umjetnom inteligencijom
5. Provjera mjera kocke
6. Vraćanje izmijenjene kocke natrag u CT/MR zapis

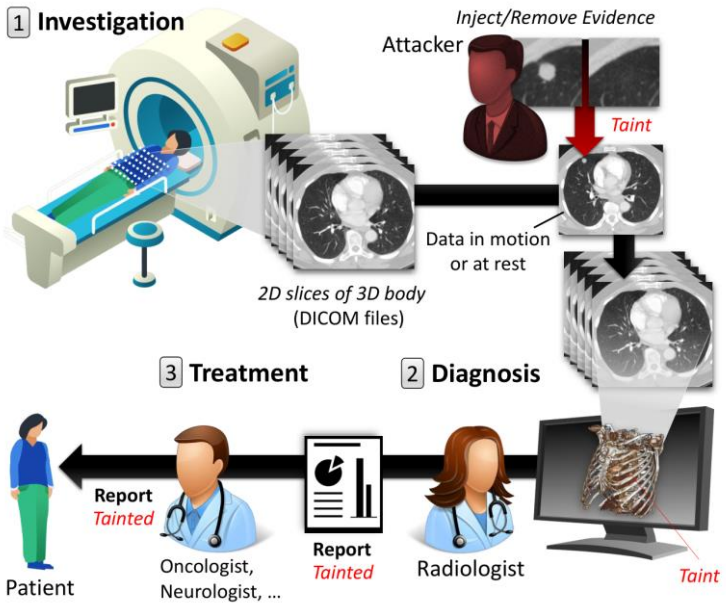


Slika 7. Prepravljanje CT zapisa

Izvor: https://www.researchgate.net/publication/330357848_CT-GAN_Malicious_Tampering_of_3D_Medical_Imagery_using_Deep_Learning

Istraživači sa izraelskih sveučilišta sa Odsjeka za informacijski sistemski inženjering (Sveučilište Ben-Gurin i Sveučilišni bolnički centar Soroka, Beer-Sheva) objavili su nekoliko radova na ovu temu koristeći navedeni algoritam. U tom istraživanju zaposlili su 3 radiologa i kao četvrtu opciju koristili umjetnu inteligenciju, kako bi pregledali snimke CT-a i odredili dijagnozu (Slika 8.)(28).

Kao snimke, korišteno je 70 računalno izmijenjenih snimki na kojima su dodani ili izbrisani znakovi karcinoma pluća i 30 nepromijenjenih. Radiolozi su na 99% naknadno promijenjenih snimki dijagnosticirali karcinom pluća. Na CT snimkama na kojima su računalno uklonjeni znakovi iste bolesti, 94% posto ih je proglašeno zdravima od strane radiologa. Nakon što su istraživači upoznali radiologe s pokusom i prezentirali da su neke snimke digitalno obrađene kako bi dodali i prikrili znakove bolesti, ponovili su pisanje nalaza. U ponovnom krugu očitanja, 60% snimaka sa dodanim znakovima bolesti i 87% sa uklonjenim bilo je pogrešno očitano. Isto tako, nakon što su isprobali najmoderniji sustav umjetne inteligencije koji je bio dostupan u vrijeme istraživanja a koristi se za automatiziranu *screening* metodu, sa naknadno izmijenjenim slikama imali su pogrešku od 100%, što dokazuje da je jako nepouzdan kod ovakvih vrsta napada (28).



Slika 8. Postupak izmjene na CT snimkama

Izvor: https://www.researchgate.net/publication/330357848_CT-GAN_Malicious_Tampering_of_3D_Medical_Imagery_using_Deep_Learning

4.3.4. Promjene na postavkama uređaja

Uređaji u radiologiji kao što su kompjuterizirana tomografija, magnetska rezonancija, PET-CT i u radioterapiji akceleratori, mogu biti upotrjebljeni kako bi se ozlijedio pacijent. Razlog je princip njihovog rada, jako ionizirajuće zračenje, gama zračenje ili jaki magnet. Do danas nema službenih izvještaja o takvim incidentima izazvanim *cyber* napadom na radiološke sustave u kojima je pacijent ozlijeđen ili smrtno stradao. Međutim, postoje nenamjerni incidenti koji nam pokazuju da u današnje vrijeme velike ovisnosti radioloških uređaja o mreži uvijek postoji mogućnost.

Dokumentirani incident pod nazivom Therac-25 iz 1985. godine pokazuje da su ovakvi scenariji mogući. Therac-25 bio je radioterapijski uređaj koji je u periodu od 1985. do 1987. uzrokovao nekoliko slučajeva prekomjernog ozračivanja pacijenata. Operativni sustav na ovom uređaju imao je opasan propust sa sigurnosnom sklopkom, koja je bila samo programska a ne i mehanička. Ovakav nedostatak u sustavu, kod kojeg prilikom radioterapije nekoliko dijelova programa istovremeno pokušava napraviti istu operaciju, doveo je to toga da sustav nije prekidao zračenje na vrijeme. Rezultat je bio prekomjerno ozračivanje pacijenata, neke i po stotinu puta više od planirane doze. Ozlijeđeno je bar 6 pacijenata, koji su zadobili ozbiljne radijacijske opekotine i paralizu različitih dijelova tijela (npr. ruke, noge, glasnice), oštećenja živaca crijeva i mokraćnog mjehura, dezorijentaciju, komu, pa i smrtni ishod. Ovo nije bio rezultat *cyber* napada ali pokazuje mogućnost i potencijalni rizik promjene načina rada uređaja koji koriste ionizirajuće zračenje. Danas su sustavi provjere i sigurnosti puno kvalitetniji ali kod svakog radiološkog (i radioterapijskog) uređaja postoje potencijalne opasnosti, osobito kad su svi uređaji danas mrežno povezani (30).

4.3.4.1. Općenite promjene postavki

Slikovni zapis pretrage često se algoritmom povezuje preko neke identifikacije (ime, prezime, datum rođenja i OIB) sa osobom koja je upisana u bolnički sustav, te se DICOM protokolom šalje u PACS. Promjenom postavki i ukidanjem sustava provjere o identifikaciji pacijenta, moguće je pridodati novi zapis o nekom drugom pacijentu iz baze podataka. Obrnuti slučaj bio bi da se neki drugi zapis pridoda trenutnom pacijentu.

Brizgalice za davanje kontrastnog sredstva često se upotrebljavaju u radiološkim pretragama kako bi se poboljšali slikovni prikazi. To je mehanički sistem spojen na krvožilni sustav kojim se upravlja posebnom kontrolnom jedinicom ili računalom. Promjenama u postavkama može se manipulirati količinom kontrasta koje se daje pacijentu. Problem kod ovakve namjerne greške (uzrokovane *cyber* napadom) je što dijagnostička vrijednost pretrage može biti smanjena zbog netočne količine kontrastnog sredstva, a i veće su mogućnosti nuspojava kod prekomjernih doza. Također, može doći i do oštećenja sustava brizgalice zbog pogrešne uporabe. (29)

Radiološki uređaji najčešće imaju primarni monitor koji tehnolozi koriste prilikom pretraga. Na njima se prikazuju svi podaci koji su bitni za radiološku pretragu, identifikaciju pacijenta, kontrole i postavke samog uređaja. Promjenom postavki od strane napadača mogu se prikriti bitne stavke ili prikazati pogrešne postavke, što može utjecati na pregled pacijenta.

Isključivanjem sustava alarmiranja može se onesposobiti mogućnost sustava da pravovremeno upozori operatera na opasnu radnju ili situaciju, te se time ne aktivira ručno/ automatsko zaustavljanje pretrage ili terapije što može uzrokovati ozljede ili fatalne posljedice. Na sličan način, napadač može podesiti sustav da stalno javlja lažne alarme. To mogu biti upozorenja za visoku temperaturu, požar, razinu kisika, otkucaje srca, krvni tlak, temperaturu prostorije u kojoj je uređaj te su senzori podešeni da na nekim vrijednostima sami isključuju uređaj ili na to upozoravaju operatera. Time najviše dovodi u opasnost pacijenta prilikom tretmana (intervencijska radiologija ili radioterapija). U nekim situacijama, može doći i to kvara uređaja. Kod ovakvog tipa napada, radi se o utjecaju na put između uređaja i senzora: onesposobljava ga, ometa alarme koji koriste radio-frekventnu komunikaciju ili blokiraju sami senzor.

Radiološki uređaji koriste više komponenti sa elektromotorima kao što su stol za pacijenta ili gentri (stativ), a u radioterapiji i kolimator snopa zračenja. Oni dobivaju naredbe iz kontrolne jedinice, računala. Napadač izmjenom postavki u računalu im može zadati neželjene pokrete kako bi izazvao sudar i tako oštetio uređaj. Ukoliko neki dio uređaja može doći u doticaj s pacijentom, posljedice mogu biti ozbiljne ozljede ili fatalne.

Povrat sustava uređaja na zadnje spremljene ili tvorničke postavke može dovesti do gubitka podataka o zadnjim pacijentima ako nisu poslani u PACS ili ručno namještenih

protokola za pregled pacijenata. Time se utječe na dostupnost uređaja za pacijente na određeni vremenski period dok se sustav ne dovede u prvobitno stanje (29).

4.3.4.2. Napadi specifični za kompjuteriziranu tomografiju

Jedan od specifičnih parametara kod dijagnostičkih pretraga CT-om su miliamper sekunde (mAs). Njima se mjeri proizvedena količina zračenja (mA) kroz protok vremena (s). Njegovim povećanjem, isporučuje se veća doza zračenja. Zloćudnom manipulacijom postavki ovog parametra od strane napadača, može doći do distorziranog ili nepoželjnog slikovnog zapisa, ali i prekomjernog ozračivanja što može biti rizik za pacijenta. Jednako tako, postoji i kV parametar, kojim se definira najveća energija fotona u x-zrakama. Doza zračenja na pacijenta je direktno proporcionalna kvadratu vrijednosti kV. Njegovim povećanjem, smanjuje se kontrast između kosti i mekih česti. Rezultat ovoga, kao i kod mijenjanja postavki mAs, je pogoršanje kvalitete slikovnog zapisa i moguća opasnost za pacijenta. Kombiniranjem ova dva parametra, mogu se uzrokovati ozbiljne radijacijske ozljede, a pravilnim doziranjem same promjene u postavkama ne moraju biti odmah uočljive. Dugoročno gledano, one mogu biti potencijalni rizik za razvoj tumorskih procesa, a do otkrivanja ovakvog problema može proći dosta vremena.

Promjenama postavki na sustavu za rekonstrukciju slika na samom CT uređaju može se utjecati na izgled snimke te time i dijagnoze pacijenata. Sličnom promjenom na drugoj komponenti ovog sustava mogu se napraviti i poremećaji na snimkama u smislu artefakata. Ta komponenta je obično standardni dio Windows operacijskog sustava ali se teže ažurira jer pokreće poseban program proizvođača uređaja. Rjeđe obnavljanje može značiti i veću ranjivost na napade. Na ovaj način se može utjecati samo na slike koje nisu još poslane u PACS, nego čekaju dodatnu obradu i slanje.

Cijeli skup postupaka za izvođenje CT pregleda definiran je u uređaju u datoteci sa postavkama. Ona se nalazi u glavnom računalu CT-a te je izuzetno bitna za normalan rad. Napadač može sa promjenama ulaznih i izlaznih naredbi na toj datoteci utjecati na ponašanje CT uređaja te tako utjecati na cijeli proces snimanja, od kvalitete snimke pa do mogućeg fizičkog oštećenja uređaja.

CT uređaj za pravilan rad mora biti kalibriran. Promjenom postavki, može se manipulirati vrijednostima za kalibraciju te natjerati uređaj da koristi parametre koji inače

ne bi zadovoljavali provjeru kvalitete. Takav postupak može oštetiti uređaj uništiti ga ili smanjiti upotrebljivost. Osim tehničkih problema, može utjecati na kvalitetu slikovnih prikaza i dovesti do prekomjernog zračenja pacijenta(29).

4.3.4.3.Specifični napada na magnetnu rezonanciju

Promjenama u konfiguracijskim datotekama uređaja za magnetnu rezonanciju može se napraviti jače magnetno polje od onog predviđenog za normalni rad. Preopterećenje magnetnih zavojnica može oštetiti prijemne zavojnice ili druge elektroničke komponente u blizini koje su osjetljive na magnetno polje. Na sličan način, napad se može usredotočiti na ometanje izlaznih snimaka. To može uključivati i ometanje radio-frekventnog signala. Ovakav napad može rezultirati velikim radio-frekventnim zračenjem koje može izazvati oštećenje uređaja i opekline kod pacijenata (30). Od svih ozljeda prilikom pretraga na magnetnoj rezonanci, takve opekline su najčešće (Slika 9.). Broj incidenata sa opeklinama povećava se usporedno sa pojačavanjem magnetskog polja uređaja, radiofrekvencija utječe na zagrijavanje. Mehanizam stvaranja ozljeda je zatvaranje vodljive petlje: strani objekt (elektrode, tetovaže, šminka, flaster) ili nabori kože (primjerice zakoljena jama) (31).

Slika 9. Primjer ozljede pojačavanja magnetnog polja MR-a

Izvor: https://mri-q.com/rf-burns.html

Specifičnost magnetske rezonancije je da koristi superprovodljive magnete, koji koriste tekući helij za održavanje niže temperature kako bi uređaj mogao nesmetano raditi. Napadač promjenom postavki može lažno aktivirati sigurnosni sustav za brzo hlađenje magneta („*quenching*“) koji se koristi ako dođe do požara ili curenja plina. Ako su uvjeti bili normalni i za takvim postupkom nije bilo potrebe, može doći do gušenja, hipotermije ili puknuća slušnog bubnjića pacijenta. Nadalje, može oštetiti uređaj, no i sama aktivacija *quenching*-a zahtjeva popravak koji traje nekoliko tjedana (30).

4.4. OBRANA RADIOLOŠKIH SUSTAVA OD CYBER NAPADA

4.4.1. Osiguranje komunikacije elektroničkom poštom

Neželjene poruke elektroničke pošte postali su standard kod pokušaja prevare. U jednom istraživanju pozivnica na radiološke kongrese i skupove, 73.3% od 45 sudionika radiologa, zaprimilo je pozivnice za nekakvo sudjelovanje u periodu od 2 tjedna, no 96% njih se nije uopće odnosilo na njihovu specijalnost (31).

Dva najčešća načina *phishinga* su izravno traženje podataka o nekom pacijentu ili ubacivanje *malware*-a kako bi se proširio dalje. Antispam i antivirusni programi su osnovna zaštita koja bi trebala biti u svakom sustavu unutar bolnice i radiološkog odjela na računalima koja imaju pristup vanjskoj mreži i na kojima se može otvoriti elektronička pošta. Time se provjerava svaka dolazna i odlazna pošta poznatih zloćudnih pošiljatelja ili uzorci takvog sadržaja. Uobičajeno je dodavanje [EXTERNAL] u dolaznu elektroničku poštu ako dolazi na službeni e-mail neke bolnice, kako bi primatelj uočio da dolazi izvan bolničke ili zdravstvene domene (32).

Pošta može sadržavati i osjetljive podatke o pacijentu, slikovne prikaze, dijagnoze, ili planove zračenja. Zato je bitno da poruke budu kriptirane (šifrirane). Može se aktivirati na način da se u predmet poruke npr. #encrypt ili #confidential, ili klijent za komunikaciju to može sam napraviti preko nekog drugog programa. Time se osigurava da neovisno o mjestu slanja poruke, sadržaj ostaje vidljiv samo pravom primatelju. Preporuke za obranu radioloških i bolničkih sustava od ovakvih napada su (32):

- Dodavanje gumba ili linka u e-mail klijente kojima korisnici mogu odmah prijaviti poruku sumnjivog pošiljatelja i sadržaja. Što je jednostavniji postupak

prijave, veća je šansa da će potencijalna opasnost biti prijavljena a time i otkrivena. Takav izvještaj odlazi informatičkoj službi koja poduzima daljnje korake

- Slanje lažnih poruka kako bi se ispitalo koliko će zaposlenika primijetiti i prijaviti lažne elektroničke poruke
- Upozoravanje svih korisnika na primijećene zloćudne e-mailove

4.4.2. Zadnje točke u radiološkim sustavima

Zadnje točke (endpoint) su računala i računalni uređaji (printeri, skeneri, druga medicinska oprema) preko kojih je moguć pristup mreži radiološkog odjela ili bolnice. Takvi uređaji nisu uvijek statični u bolničkom sustavu nego se ponekad omogućuje zaposlenicima rad od doma ili su neki programi prilagođeni za rad na laptopima. Primjerice, radiolog u dežurstvu može raditi od kuće, na računalu koje inače koristi privatno, i na kojem može već imati instaliran neki *malware* (33).

Periodičke nadogradnje sustava koje sadrže zakrpe za sigurnosne propuste za takva računala su česte te ih je potrebno redovno ažurirati. Problem su veći uređaji kao CT ili MR koji se koriste vlastitim radnim stanicama. Ponekad operativni sustav na njima nije jednostavno ažurirati ili nadogradnje više ne postoje, te je nemoguće tako poboljšati njihovu obranu od *malware*-a. Preporuka je takve sisteme zaštititi preko vatrozida (*firewall*-a) i to uvođenjem strožih pravila koji uređaji mogu s njim komunicirati (npr. dozvoliti ulaze samo za DICOM i HL7 protokole) (9).

Programe koji se koriste na radnim stanicama također treba redovno ažurirati, najbolje automatiziranim procesom kako se ne bi preskočila nadogradnja. Time se sprečava šteta koju mogu napraviti *bug*-ovi ili sigurnosni propusti. Među njima treba odrediti koji su bitni za rad a koji ne, te napravili listu dozvoljenih a uklonili nepotrebne. Operativni sustavi, programi i aplikacije imaju svoj rok trajanja, koji kad istekne proizvođač više ne podržava i ne održava njihovu sigurnost. Takve bi trebalo prestati koristiti, zamijeniti novom verzijom ili zatražiti dodatnu podršku proizvođača. Zadnja opcija bi trebala biti prihvaćanje rizika upotrebe, i to samo dok se ne nađe prihvatljivije rješenje (32).

Najbolja obrana su redovito ažurirani antivirusni programi, koji otkrivaju *malware* heuristikom (provjeravajući kod programa za sumnjive osobine) ili preko „potpisa“ (uzorak iz *malware* se uspoređuje s sumnjivim programom)(34).

Neki uređaji i radne stanice koriste i fizičku zaštitu, kako bi se spriječilo fizičko spajanje (USB, mrežni kabel). Takav način obrane je koristan ako se potencijalni napad planira tehnikom „man-in-the-middle“, spajanjem drugog računala na samu metu napada (35).

4.4.3. Organizacija pristupa

Radiološki odjeli moraju imati mogućnost jasne identifikacije svih korisnika i sustav praćenja njihovog pristupa podacima, aplikacijama, sustavima i uređajima. Korisnički podaci svakog zaposlenika odjela pomažu u njihovoj identifikaciji u digitalnom okruženju te im ograničavaju pristup i aktivnosti. Zato bi u svrhu sigurnosti svaki zaposlenik trebao imati vlastito korisničko ime i lozinku (koja bi trebala biti različita od one koju pojedinac koristi za druge privatne račune, e-mailove, forume ili aplikacije)(36). Primjerice, za pregled podataka u radiološkom sustavu potrebno se prijaviti, a svaka promjena podataka o pacijentu se dokumentira. Time se osigurava da ukoliko dođe do pogrešnih podataka bude vidljivo tko ih je prepravljao. Također, sprečava pregledavanje zapisa o pacijentima koji se rade iz privatnih potreba a ne profesionalnih.

Upotrebu računa koji dijeli više korisnika također treba izbjegavati. Ako postoji potreba za takvim načinom rada, svi korisnici trebaju biti educirani da se odjave prilikom završetka rada, najbolje porukom u samom programu ili i nekim podsjetnikom. Neki radiološki uređaji, radne stanice i pristupi bolničkoj mreži koji zahtijevaju ovakav način prijave, velika su sigurnosna prijetnja. Korisnik može ostaviti aktivnu prijavu koju može iskoristiti netko tko inače ne bi trebao imati pristup. Promjena lozinke je otežana jer veći broj korisnika mora biti obaviješteno. S druge strane, duljim korištenjem iste lozinke duže vremena povećava se šansa da pristup dobije netko tko ga ne bi trebao imati.

Pristup svakog korisnika treba biti prilagođen zahtjevima njegovog radnog mjesta. Osoba koja radi administraciju na radiološkom odjelu treba imat pristup demografskim podacima i uputnicama, ali ne i PACS-u, dok netko tko radi u dežurstvu na CT-u, MR-u ili klasičnom rendgenu mora imat pristup i podacima. Samo voditelji odjela trebaju imati

mogućnost izrada narudžbi (potrošnog materijala, ponuda za dodatnu opremu…). Jednako tako trebalo bi definirati koji računi se mogu koristiti na kojim računalima, uređajima i programima. Tako se smanjuje mogućnost krađe podataka ili nedozvoljenog ulaza korisnika ukoliko su nečiji podaci za prijavu ukradeni.

Ako zaposlenik mijenja radno mjesto ili odlazi u mirovinu, važno je izbrisati njegov račun kako prijašnji zaposlenici ne bi mogli doći do podataka o pacijentima i drugih osjetljivih informacija. To je važno za odjele koji koriste mrežne servere na koje se može pristupiti sa računala izvan odjela. Isto tako, prilikom mijenjanja radnog mjesta unutar odjela, treba prilagoditi dozvole koje račun ima sa novim odgovornostima zaposlenika. Vanjski suradnik radiološkog odjela, ako mora imati račun, ne mora imat pristup svim podacima koji su bitni za odjel. Povremeno je potrebno provjeriti koje su dozvole aktivne na kojim računima, kako ne bi došlo do zlouporabe. Korisnici se ponekad zaborave odjaviti s uređaja i programa koje koriste, stoga se u postavkama može namjestiti da uređaji sami odjave korisnika u slučaju neaktivnosti (36).

Kada se od zaposlenika zahtjeva da uvijek rade pod svojim računom i pravovremeno se odjavljuju s uređaja to postaje dodatna sigurnost PACS sustava. U prvom redu, svaka provjera autentičnosti zaposlenika stvara prepreku potencijalom uljezu da pristupi PACS arhivi. Time se omogućuje i ostavljanje pisanog traga koje radnje su poduzete sa kojeg računa, što je bitno prilikom istraživanja nedopuštenog pristupa podacima pacijenta (9).

4.4.4. Organizacija mreže

4.4.4.1. Vatrozid (firewall)

Uspješna metoda očuvanja sigurnosti mreže je upotreba vatrozida (firewall) kako bi se omogućio siguran rad unutar radiološkog odjela i pristup njemu izvana. Granice kako se mrežni promet smije odvijati trebaju biti dobro postavljene kako ne bi došlo do neželjenih pristupa mreži(32).

Vatrozidi u svojoj osnovi ograničavaju pristup radiološkoj mreži prema prethodno postavljenim uvjetima. Postoje 4 osnovne vrste (37):

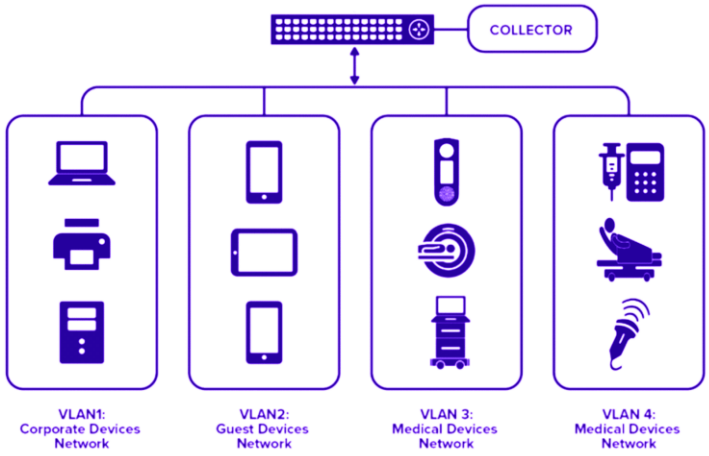
- Filter paketa, najstarija vrsta, najjeftinija ali i najmanje sigurna, uspoređuje svaki podatkovni paket u mreži sa postavljenim ograničenjima

- Provjera pristupa na razini mreže – ograničava komunikaciju između uređaja (radiološki uređaji, radne stanice, serveri, računala) bez provjere vrste podataka
- Provjera pristupa na razini aplikacija – ograničava komunikaciju aplikacija i mreže stvarajući međumrežu
- Višeslojni vatrozid - osigurava mrežu na 7 razina mrežne komunikacije

U radiologiji vatrozidi imaju osnovnu ulogu u održavanju sigurnosti, privatnosti informacija o pacijentu i čuvanju medicinskih slikovnih zapisa. Kao barijera između radiološke mreže i ostalih, kontrolirajući promet i pristup, preveniraju nedozvoljeni pristup podacima. Time brane sustav od *cyber* napada i *malware*-a. Kontrolom pristupa omogućuju da do podataka imaju pristup samo oni zaposlenici kojima je to bitno za obavljanje posla, dok štiti od drugih koji bi to mogli zloupotrijebiti.

4.4.4.2. Dioba mreže

Druga osnovna metoda ograničavanja *cyber* napada je dijeljenje mreže na sigurnosne zone (Slika 10.). Ove zone se dijele prema osjetljivosti podataka za koje se koriste (npr. mreža radioloških uređaja, radne stanice, sustav bolnice, pristup vanjskom internetu) ili standardna podjela (mreža za podatke, aplikacije, *middleware*…) (32).



Slika 10. Primjer diobe mreže radioloških uređaja i ostale bolničke mreže

Izvor: https://www.armis.com/blog/healthcare-network-segmentation-bridging-the-nac-gap/

Svaki segment se postavlja kao izolirani dio mreže. Administratori mogu staviti drukčiji način nadzora na svaki dio mreže te kontrolirati njihovu međusobnu komunikaciju. Ako se takva podjela dobro napravi, većina mrežnog prometa ostaje unutar namijenjenoga dijela mreže. Primjerice, slanje podataka sa CT-a ili MR-a na radnu stanicu ili PACS koje se odvija po posebnoj mreži na koju nema pristupa izvana, pozitivno utječe na nadzor mreže, sigurnost i brzinu. Time se sprečavaju i usporavaju neovlašteni ulazi i zloćudni *cyber* napadi na radiološke uređaje jer zahtijevaju izvođenje napada na više mreža što otežava cijeli postupak. Porastom broja segmenata povećava se i sigurnost mreže. Potrebno je pronaći dobar omjer diobe, jer prevelika segmentacija mreže dovodi do sporijeg rada, a premala utječe na sigurnost. Najčešći način segmentacije je VLAN (*Virtual Local Area Network*) kojim se fizička mreža dijeli na nove programski načinjene. Na VLAN mrežu se mogu primijeniti ACL (*Access Control List*) pravila, koja definiraju koji korisnik ima pristup kojoj VLAN mreži (zaposlenici na pojedinom radiološkom uređaju, cijeli radiološki odjel, pristup BIS-u…).

Cijela mreža radiološkog sustava može biti jako velika te time teška za organizaciju i sigurnost. Ako su svi radiološki uređaji i druga računalna infrastruktura spojeni zajedno, napadač koji dobije pristup jednoj točki, može pristupiti svim drugim uređajima na toj mreži. Segmentacijom se sprečavaju takvi razvoji događaja i stvaraju barijere, a ujedno se i osjetljivi podaci izoliraju od lakih upada u sustav (38).

Glavni cilj segmentiranja mreže na radiološkom odjelu je smanjenje i kontrola protoka podataka između radioloških uređaja sa svojom računalnom opremom i vanjskih mreža bez poteškoća u radu. Kako bi pridonijeli većoj sigurnosti od *cyber* napada na radiološke sustave treba pripaziti na:

- Zlouporabu – kada osoblje radiološkog odjela pokušava pristupiti vanjskoj mreži preko uređaja i računala, ili postavljanjem aplikacija koje koriste vanjsku mrežu
- Pogrešnim postavkama – za neke uređaje i računala potrebna je vanjska mreža kako bi se nadogradili, napadač može iskoristiti ovo i preusmjeriti protok podataka na lažni server i dohvat zloćudnih programa

- Potrebne vanjske veze – kod uređaja kojima je za rad potrebna stalna vanjska mreža, neovlašteni korisnici ju mogu iskoristiti za pristup povjerljivih dijelova mreže odjela
- Pristup dobavljača – radiološki uređaji ponekad trebaju pristup vanjskoj mreži kako bi se osigurala podrška servisa, slanje izvještaja ili nadogradnja, na takva spajanja na vanjske mreže treba obratiti posebnu pažnju
- Pred-instalirani programi – neka računala i radne stanice dolaze sa dodatnim programima koji se mogu pokušati spajati na vanjske mreže (npr. radne stanice sa Windows operativnim sustavom koji imaju pretpostavljene programe koji dolaze sa Windowsima a nisu potrebne za rad) (38).

4.4.4.3. Web proxy zaštita

Web *proxy* sustavi pružaju važnu zaštitu od *malware* napada na radiološke radne stanice. Većina *malware* i *phishing* napada su temeljeni na web-u, stoga sustav u slučaju pokušaja pristupu poznatim zlоćudnim stranicama javlja korisniku poruku da je ta radnja potencijalno opasna te je pristup uskraćen. Ako je sigurnosni sustav dobro postavljen, *web proxy* zaštitom umanjuje se mogućnost *cyber* napada na slijedeće načine (32):

- Blokiranje prema reputaciji – sigurnosni centri i organizacije objavljuju liste stranica koje sadrže zlоćudni sadržaj, te ih *proxy* serveri u svrhu zaštite koriste kako bi onemogućile otvaranje takvih web lokacija
- Blokiranje organizacija – pokušaji zlоćudnih napada upisuju se u posebnu listu kako se napad ne bi ponovio, a server prema postavkama odmah blokira pokušaje pristupa
- Blokiranje kategorije – moderni web *proxy* sustavi imaju pretpostavljene kategorije web stranica kojima se može ograničiti ili spriječiti pristup. Tako se mogu ukinuti stranice socijalnih mreža koje sadrže zlоćudne, sumnjive ili ilegalne sadržaje

4.4.4.4. Fizička zaštita mrežnih uređaja

Za neke *cyber* napade potreban je fizički pristup mrežnim uređajima, kako bi se spojili dodatni uređaji ili mijenjanjem postavki omogućio mrežni pristup napadačima. Zato je važno da serveri, *router*-i i drugi uređaji koji su potrebni za mrežni rad radiološkog odjela ne moraju biti na samom odjelu, nego smješteni na sigurnim i kontroliranim mjestima s ograničenim pristupom. Idealno je da takva mjesta imaju video nadzor i kontrolu pristupa (kartica, PIN, biometrijski sken). U slučaju provale treba postojati alarmni sustav koji će dojaviti neovlaštene ulaze dežurnoj službi za sigurnost. Da bio ovakav sustav dobro funkcionirao, potrebne su redovne kontrole sigurnosti prostora. Treba obratiti pažnju i na putove mrežnih kablova između prostorije servera i radiološkog odjela (32).

4.4.5. Zaštita podataka DICOM enkripcijom

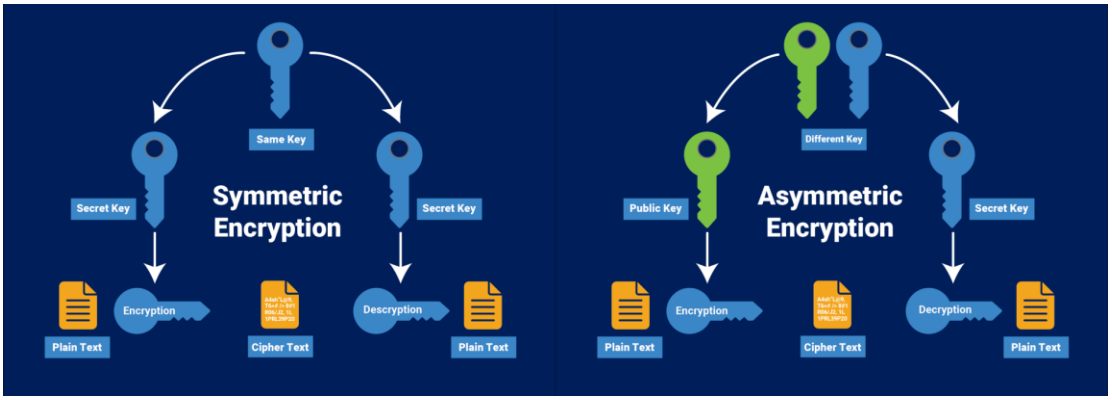
Zaštita podataka važno je područje interesa u obrani od *cyber* napada na radiološke sustave. Podaci o pacijentu i njihovi medicinski slikovni zapisi su osjetljiva tema. Stoga su strogo pravno regulirani od strane HIPPA (Health Insurance Portability and Accountability Act) u SAD-u ili nama bliži GDPR (General Data Protection Regulation) u Europskoj uniji. Svaki napad na radiološki mrežni sustav može imati za cilj krađu takvih podataka, a ukoliko je uspješan može snositi teške pravne posljedice.

Standard za spremanje i slanje medicinskih slikovnih prikaza sa rendgena, CT-a i MR-a je DICOM. Njegova enkripcija je osnovna sigurnosna mjera zaštite podataka koja podliježe GDPR-u i HIPPA-u. Za sveobuhvatnu sigurnost ona se mora nadopunjavati sa ostalim mjerama od *cyber* napada na radiološke sustave. Enkripcija DICOM-a štiti osjetljive informacijske i slikovne podatke o pacijentu. Sustav DICOM anonimizacije ima za zadatak prikrivanje osobnih podataka o pacijentu, dok DICOM enkripcija čuva privatnost prilikom slanja ili pohranjivanja. Anonimizacija je bitna za neotkrivanje identifikacijskih podataka, dok enkripcija obuhvaća ukupan skup kao bazu podataka. Obje tehnike imaju svoju funkciju u obrani od *cyber* napada jer imaju ulogu u prikrivanju osobnih podataka pacijenta koji se nalaze spremljeni sa slikovnim prikazom.

DICOM može koristiti napredne algoritme enkripcije kao što su AES (advanced Encryption Standard) ili RSA (Rivest-Shamir-Adleman) kako bi kriptirali podatke prije

slanja ili pohranjivanja. AES je standard za enkripciju DICOM-a, koristi simetrični algoritam koji sadrži isti ključ za enkripciju i dekripciju. On omogućava brze i efikasne operacije te je idealan za osiguravanje velikih količina podataka. Široko je prihvaćen i siguran enkripcijski algoritam koji podržava više opcija jačine. Nazivi AES-128, AES-192 i AES-256 označuju dužinu ključa za enkripciju u bitovima, te je tipična preporuka za najbolju sigurnost AES-256. RSA je asimetrični algoritam enkripcije koji koristi privatne i javne ključeve. Njegova uloga je kriptiranje AES ključa što se naziva hibridna enkripcija. RSA služi za razmjenu AES ključeva između dvije strane koje izmjenjuju DICOM datoteke (Slika 11.). Oba se koriste za enkripciju DICOM podataka, ali imaju drukčiju namjenu. AES je koristi za enkripciju aktualnih DICOM podataka zbog svoje efikasnosti i brzine, dok se RSA više koristi za sigurnu razmjenu podataka između ovlaštenih strana. Kombinacijom oba sustava imamo dostatno sigurnu enkripciju za izmjenu i pohranu. Općenito pravilo je da se za sigurnu AES zaštitu koristi generator brojeva za sigurnosni ključ željene duljine, primjerice AES-256 (39).

Enkripcija ima bitnu ulogu u zaštiti podataka koji su arhivirani, u procesu slanja i koji se trenutno koriste (mijenjaju, procesuiraju, brišu ili su otvoreni na nekoj radnoj stanici). Zato podaci uvijek trebaju biti enkriptirani, kada god prelaze preko radiološke ili vanjske mreže.



Slika 11. Razlika između AES (simetričnog) i i RSA (asimetričnog algoritma)

Izvor: https://dcmsys.com/project/dicom-encryption-anonymization/

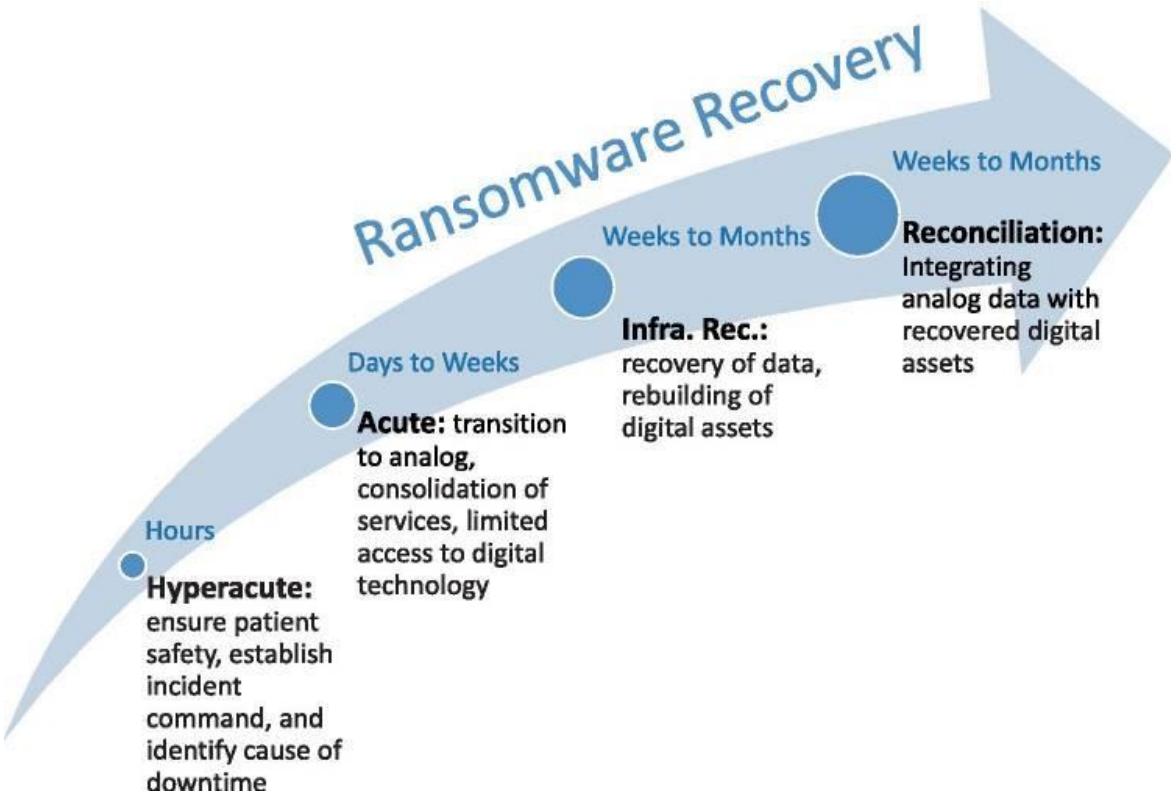
Kako bi obrana protiv *cyber* napada bila uspješnija, dobro je (39):

- Enkriptirati DICOM podatke sa generiranim ključem, simetrničnim ili asimetričnim
- Spremati enkriptirane DICOM podatke zajedno sa podacima za dekripciju, te te enkriptirati cijeli disk sa arhiviranim podacima. Ovime se ne mogu zaštiti podaci koji putuju ili su u uporabi nego samo oni spremljeni na uređaju
- Koristiti poseban server za podatke u uporabi Enkripcija podataka koji su u upotrebi je moguća ali vrlo nepraktična i zahtjevna za računala. Dijagnostičke aplikacije rade sporije ako moraju dekriptirati datoteke, stoga je najbolje rješenje posebno odvojeni server za aktualne podatke koji se koriste
- Kod slanja enkriptiranih DICOM podataka koristiti sigurnosne protokole za slanje poput TLS (Transport Layer Security) ili HTTPS (Hypertext Transfer Protocol Secure)
- Kod dekriptiranja podataka, paziti da ključ imaju samo ovlaštene strane

4.5. ODGOVOR I OPORAVAK OD CYBER NAPADA

U slučaju da *cyber* napad na radiološki sustav bude uspješan, odjel mora imati standardizirane procedure kao odgovor. Pod tim se smatra imati razrađene korake za otkrivanje napada koji su u postupku i zaobišli su sigurnosne prepreke, odgovor na njih dok nije napravljena prevelika šteta te oporavak i popravljanje učinjenog. Za uspješni odgovori i oporavak moraju postojati smjernice za odgovor na incident (Slika 12.). To je lista postupaka kojima se određuje kategorija i ozbiljnost incidenta, koji su sudionici uključeni te koje su njihove odgovornosti. Veliki bolnički sustavi pod koje spada i radiološki, imaju informatičke službe koje znaju kako se rješavaju problemi kod ozbiljnih incidenata (32).

Prema istraživanju (40), *ransomware cyber* napadi na radiološke sustave se mogu podijeliti u četiri faze, a za svaki postoje predviđeni koraci obrane i spašavanja podataka.



Slika 12. Prikaz vremenskih okvira oporavka od cyber napada. Vremena potrebna za faze ovise o veličini, složenosti i pripremljenosti radiološkog odjela

Izvor: https://pubmed.ncbi.nlm.nih.gov/34159418/

4.5.1. Hiperakutna (prva) faza

Često je teško je točno odrediti vrijeme napada, no možemo pretpostaviti vremenski okvir napada i prema tome dalje planirati. Najraniji znak je da su nekoliko informatičkih sustava unutar radiološkog odjela nedostupni. To uzrokuje nemogućnost pristupa svim podacima o pacijentima kao što su povijesti bolesti, PACS ili radiološki informacijski sustav. Unutarnja i vanjska mreža mogu biti onesposobljene, ili kao zaštitni mehanizam kako bi se spriječila veća šteta ili kao izravni utjecaj zloćudnog napada. Neki radiološki uređaji mogu biti onemogućeni u radu, dok drugi normalno rade ali ne mogu slikovne zapise slati dalje. Prvi sati napada i blokade sustava ne razlikuju se od kratkotrajnih problema na mreži. Zato dolazi do iznenadne neusklađenosti između ponude i potražnje radioloških usluga. Radiološke usluge se ne mogu u potpunosti izvršiti a pacijenti dolaze i dalje.

Odgovor na napad u ovoj fazi mora se usredotočiti na sigurnost pacijenta i sprječavanje daljnje štete. Obrada hitnih radioloških slučajeva treba se prebaciti na jednostavnije načine, ispis slika ili očitavanje na samom uređaju (iako ih većina nije predviđena za to zbog kvalitete slike). Za mogućnosti o preostalim sposobnostima i kapacitetima potrebna je procjena radiologa, tehnologa, sestara i ostalih djelatnika kako bi se razjasnilo koje radiološke obrade su trenutno moguće. Sve teleradiološki načini rada koji se koriste za hitne slučajeve ili intenzivnu njegu smatraju se nedostupnima te ih je potrebno zamijeniti očitanjima na odjelu. Kod fizički odvojenih radilišta koji šalju medicinske slikovne zapise u centralni sustav za očitanje, potrebno je ograničavanje usluga kako bi se smanjio broj lokacija za slanje zapisa a time i osiguralo bolju raspodjelu radiologa koji sada moraju biti na samom odjelu. Pacijenti koji zahtijevaju hitnu obradu prosljeđuju se na lokacije gdje je tražena pretraga moguća ili u drugu ustanovu koja nije imala *cyber* napad.

Bez pristupa bolničkom informacijskom sustavu i povijesti bolesti pacijenata potreban je privremeni dogovor za identifikaciju pacijenata te označavanje slikovnih zapisa. Iako su ovakvi koraci obično privremeni i koriste se samo na određenom uređaju kod kratkotrajnih prekida rada, duži prekidi zahtijevaju bolju razradu privremenog standarda.

4.5.2. Akutna (druga) faza

Nakon nekoliko dana od pada sustava, druga faza započinje s dovoljnom količinom podataka o šteti na radiološkom odjelu. Uz dobro isplaniran oporavak, neki dijelovi se u ovoj fazi mogu ponovno pustiti u rad. Ako su digitalni zapisi o pacijentima neoštećeni ili uspješno spašeni, iz sigurnosnih razloga dozvoljava im se ograničeni pristup za pregled preko web sučelja bez mogućnosti mijenjanja. Pretpostavlja se da su unutarnja mreža i neka računala još izvan uporabe iz sigurnosnih razloga ili potreba provjere. Radiološki odjel u ovom slučaju mora sam osmisliti alternativna rješenja kao što su mobilni Internet preko telefona, izravno mrežno ili USB spajanje uređaja ili korištenje računala koja nemaju pristup mreži.

Planiranje za drugu fazu bazira se na izravnijem tijeku rada radiološke obrade pacijenta, od samog naručivanja pacijenta do očitavanja i izdavanja nalaza. Pritom je

potrebno paziti da se podaci i slikovni zapisi pravilno spremaju kako bi se nakon dolaska mreže mogli ubaciti u redovni digitalni sustav. Posebno treba paziti na hitne ambulantne i bolničke slučajeve kako ne bi došlo do zabune. Unatoč novom principu „podataka u oblaku“, većina trenutne radiološke tehnologije kao što su PACS i RIS koriste unutarnju mrežu. Bezmrežno pregledavanje radioloških slikovnih zapisa može se omogućiti preko računala koja su spojena na monitore koji zadovoljavaju dijagnostičke kriterije a prijenos podataka se vrši preko CD/DVD-a. Zavisno o dostupnim računalima, spremnosti na povrat podataka i veličinu radiološkog odjela, moguće je postavljanje privremene mreže. U nju se povežu radiološki uređaji, privremeni PACS, radne stanice i druga računala. To zahtjeva posebno planiranje jer postoji mogućnost postojanja dvije baze zapisa, analogne (ispis rendgenskih snimaka i pisani nalazi) te digitalne (zapisi očitanja u računalu i CD/DVD/privremeni PACS), čime može doći do gubitka nekih podataka. Također, digitalni mediji napravljeni u ovoj fazi mogu sadržavati zloćudne programe. Prilikom izrade CD/DVD medija, ponekad se instaliraju i preglednici u kojima se nalazi *malware*. I same DICOM datoteke mogu biti izvor ponovne zaraze (23). Kao i . JPEG ili . TIFF formati, najsigurnije ih je otvarati preko drugih programa a ne pridodanih na medij, kako bi se smanjila mogućnost novih *cyber* incidenata. Prilikom prelaska u 3. fazu, potencijalno zaražena računala ne bi smjela biti spojena na novu mrežu.

4.5.3. Oporavak infrastrukture (treća faza)

U fazi 3 veća je pažnja na obnovi same računalne mreže nego na planiranje radioloških postupaka. Informatička služba koja radi na odjelu može početi s obnovom infrastrukture dok paralelno daje podršku trenutnom radu. Svaka od kritičnih baza podataka kao što su PACS, zapisi o pacijentima i bolnički računalni sustav mogu imati tri opcije razvoja događaja. Prva je da su baze podataka ostale neoštećene zahvaljujući nekoj od preventivnih mjera sigurnosti. To znači da su razlog za greške pristupa samo druga računala i povezanost, a ne problemi na samoj bazi podataka. Druga opcija je da je baza oštećena ali se može popraviti i vratiti u prvotno stanje preko sigurnosne kopije. U slučaju *ransomware*-a, kada je tražena otkupnina za povrat podatak, ovo vjerojatno znači da su ispunjeni zahtjevi hakera za novčanom naknadom. Zadnja opcija je da je baza podataka bespovratno izgubljena. Neke *cyber* terorističke skupine nemaju želju za materijalnom

koristi nego im je interes samo bespovratna šteta, iz najčešće ideoloških ili političkih razloga.

Da bi radiološki odjel mogao nastaviti s radom, informatička služba mora imati predviđene korake u slučaju nepredviđenih događaja u drugom i trećem slučaju grešaka na bazama podataka. Sigurnosna kopija na drugoj mreži ili nepovezanom serveru je najbolja opcija (41). Za pretpostaviti je da nijedan *antimalware* program ne može sa potpunom sigurnosti prepoznati sve zloćudne programe instalirane u sustav. Samo jedna neprepoznata opasnost može pokrenuti cijeli napad ponovno. Zato je preporuka da se, neovisno da li su podaci neoštećeni, spašeni ili izgubljeni, cijeli sustav ponovo postavlja na programski čistim uređajima.

4.5.4. Usklađivanje (četvrta faza)

Prve 3 faze usredotočene su na osiguravanje nastavka rada i pružanje sigurne skrbi za pacijenta. Zadnja faza ima za zadatak povezivanje podataka koji nisu uvedeni u digitalni radiološki sustav kako ne bi bili izgubljeni i mogli bi se koristiti za daljnje praćenje pacijenata. Uspjeh ove faze jako ovisi o dobroj organizaciji prikupljanja podataka iz prijašnjih faza. Kako je radiološki odjel radio neko vrijeme bez mrežne pohrane, moramo biti sigurni da su podaci pacijenata pravilno upareni. Za ovo trebaju biti posložene vrste radioloških pretraga sa podacima koji su bitni za radiološke tehnologe i radiologe. Radiološki slikovni zapisi sa CD/DVD-a, informacije o naručivanju, izvještaji i nalazi trebaju biti sigurno spremljeni kako bi bili lako dostupni za povrat u bazu podataka. To zahtjeva rad svih zaposlenika jer se slike trebaju ručno dodati u sustav a nalazi ponovno izdiktirati.

U zadnjoj fazi oporavak može biti puno duži nego što je potrebno kod standardnih kratkotrajnih prekida rada. Usklađivanje podataka i povrat informacija može potrajati i nekoliko mjeseci. Prema nekim iskustvima, najbolji način je obrada podataka prema datumima, počevši od trenutne situacije pa unatrag prema datumu pada sustava zbog napada. Prethodne analogne zapise kao što su ručno napisani nalazi treba uvesti u digitalni zapis. Kako je mreža u ovoj fazi u potpunosti osposobljen i omogućen je pristup svim starim podacima, nova očitanja se mogu razlikovati jer se više podataka sad može uzeti u obzir. Dok je usklađivanje podataka u tijeku, tehnolozi i radiolozi mogu imati

probleme u radu. Slikovni zapisi koji su trenutno potrebni mogu se nalaziti na PACS-u, na nekom mediju za pohranu, na oba ili nijednom ako su izgubljeni. Za nove radiološke obrade ponekad je potreban pristup starima koji se nalaze na više lokacija pohrane. Takvi novi sporedni zadaci ometaju normalan rad radiološkog odjela.

4.5.5. Redovita kontrola spremnosti (nulta faza)

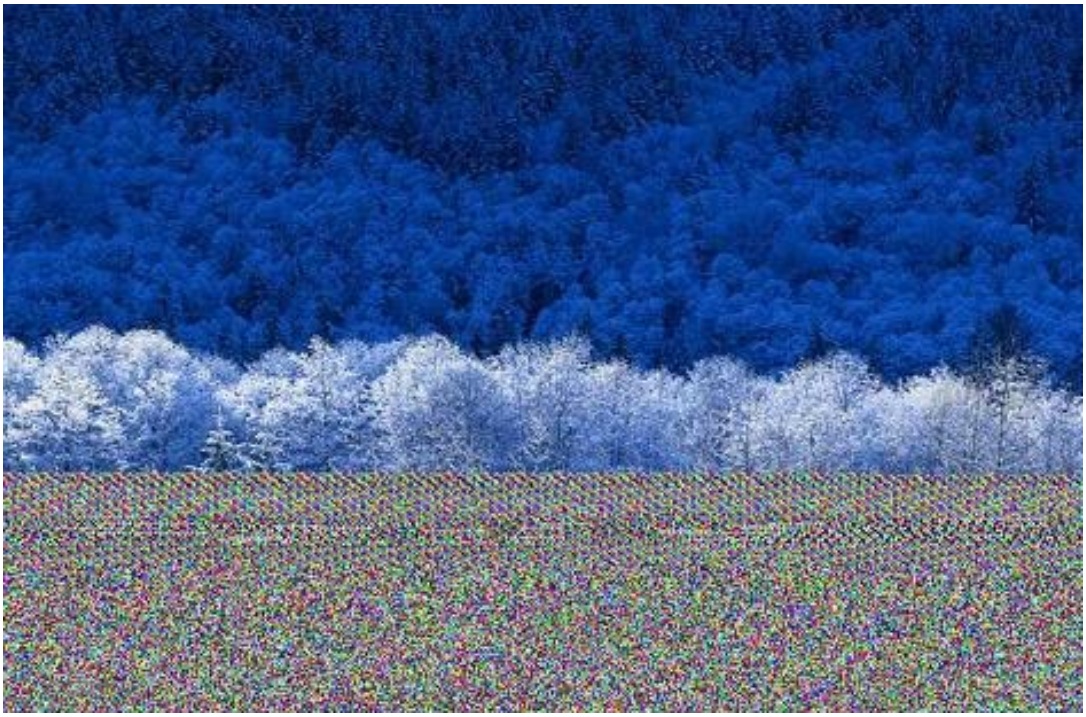
Cyber napadi se vjerojatno neće smanjiti s vremenom. Današnja literatura o organizaciji odjela preporuča da je *cyber* sigurnost informatičke infrastrukture uključi u standardne planove i proračune. Zato pripremljenost za *cyber* napade zahtijeva planiranje za obranu od neželjenih događaja. To uključuje i nadogradnju i održavanje takvih planova. Redovitu kontrolu spremnosti zato možemo smatrati kao fazom 0 kod *ransomware* i sličnih napada. Sva informatička infrastruktura i zaposlenici odjela mogu se smatrati kao potencijalno ranjivi a njihov sigurnosni rizik se može držati pod kontrolom ali nije potpuni uklonjiv. S druge strane jedan dan koji je na radiološkom odjelu protekao bez problema, drugi dan može započeti potpunim padom sistema. Stoga rutinski protokoli mogu zahtijevati izmjene kako bi se prilagodili trenutnoj situaciji.

4.6. POZNATI NAPADI NA RADIOLOŠKE SUSTAVE U SVIJETU

4.6.1. Orangeworm (Kwampiris)

U siječnju 2015. otkrivena je *cyber* skupina Orangeworm. Njihov *malware* pod nazivom Kwampirs pronađen je na sistemima velikih korporacija koje se bave zdravstvom u Americi, Aziji i Europi. Meta napada bili su davatelji zdravstvenih usluga, farmaceuti, informatička rješenja koja se koriste u zdravstvu i proizvođači računalne opreme. Pretpostavlja se da je razlog napada samo prikupljanje podataka iz sustava. Skupina je odabirala mete pažljivo i namjerno, dobro planirajući napade. Kwampirs je pronađen na sustavima za upravljanje suvremenim medicinskim uređajima u radiologiji, kao što su rendgen i magnetska rezonancija. Jedan od razloga lakog širenja je to što se na skupim radiološkim uređajima često koriste stariji operativni sustavi koji se rijetko nadograđuju te time nemaju sigurnosne zakrpe koje bi spriječile ovakve zloćudne *cyber*

programe. Drugi razlog je što se može prikriti u slikovne zapise (Slika 13.). Za takve zastarjele sustave dobro su opisani i svi sigurnosni propusti što puno olakšava rad *cyber* napadačima (42, 43).



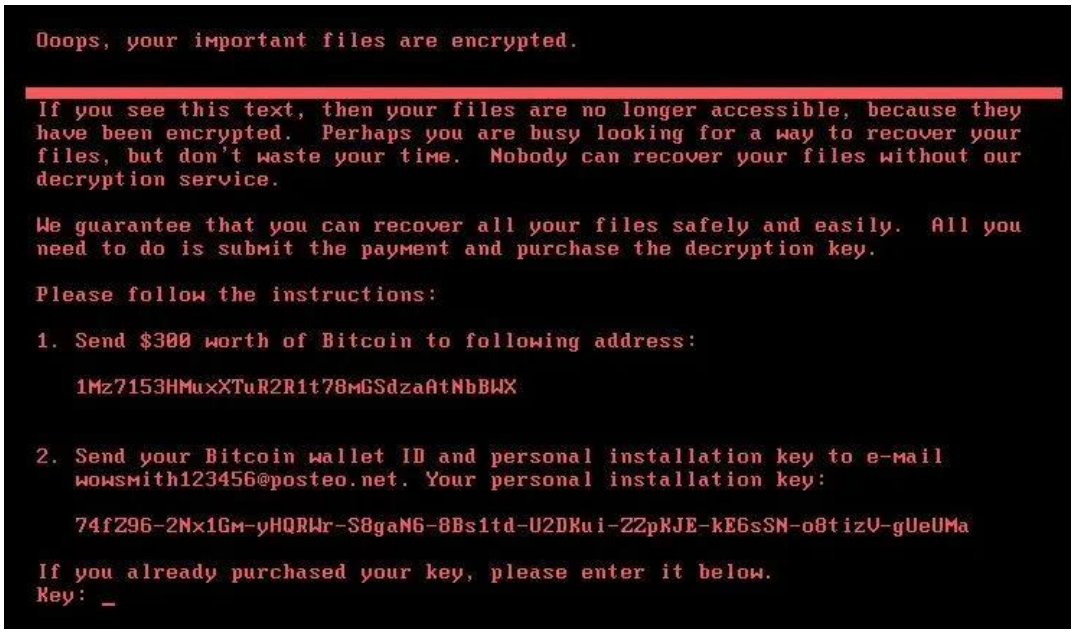
Slika 13. Primjer slikovnog prikaza koji sadrži Kwampir, izgleda kao greška u slici a zapravo je malware instalacija koja tako izbjegava antivirusne programe

Izvor: https://resources.cylera.com/hubfs/Cylera%20Labs/Cylera%20Labs%20Kwampirs%20Shamoon%20Technical%20Report.pdf

Kwampirs prvo analizira radiološki uređaj te šalje podatke autorima samo ako pronađeno odgovara određenim zahtjevima. Podaci koji su interesantni su slikovni zapisi, detalji o uređaju i računalnoj mreži. Tada se širi dalje, mijenjajući svoj zapis u sustavu kako bi izbjegao sigurnosne programe koji bi ga mogli prepoznati i zaustaviti. Posebna opasnost je što ujedno omogućava i upravljanje radiološkim uređajima na daljinu. Obično nema simptoma zaraze, jedino se može prepoznati prema zloćudnim datotekama i procesima koji rade u pozadini operativnog sustava (44).

4.6.2. Petya i NonPetya

Petya je vrsta *malware*-a koja se pojavila 2016. godine. Djeluje tako da zaključava datoteke i mape na računalu žrtve te zatim *cyber* napadači traže otkupninu kao bi omogućili pristup podacima. Za razliku od prijašnjih vrsta *malware*, Petya blokira cijeli tvrdi disk korisnika na način da blokira popis datoteka, bez kojeg on nije uporabljiv, a djeluje samo na Windows operativnom sustavu. Najčešće se širi preko poruka elektroničke pošte, kao .PDF datoteka koja sadrži linkove ili prikrivena aplikacija. 2017. godine pojavila se NotPetya, a ime je dobila prema sličnosti sa Petyom. U periodu od mjesec dana, ušla je u najmanje 2000 organizacija, a većina meta je bila u Ukrajni. Princip je da enkriptira cijeli tvrdi disk sa svim podacima, ne samo popis datoteka kao Petya (Slika 14.). Brzo se širi sustavom jer ne zahtjeva aktivnost korisnika računala(45).



Slika 14. Prikaz ekrana nakon napada NotPetya malwareom

Izvor: https://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/?sh=6eb2317f532e

Prvotna namjena je bila napad ruske hackerske skupine Sandworm na razne svjetske korporacije (Maersk, FedEx, Merck), prešla je i na bolničke sustave na svim kontinentima. Šteta je jedino nastajala na računalima koja koriste Windows platformu,

dok su ona računala i uređaji sa Linux sustavom bili pošteđeni. Primjerice, Heritage Valley Health System (Pennsylvania, SAD) navodi u izvješću da njihovi radiološki uređaji kao što su rendgen, CT ili MR nisu imali problema. Problem je bila radna stanica koja preuzima MR snimke, a radi na Windows sustavu. Kao takva, nije bila upotrebljiva a time ni MR uređaj. Druga bolnica, navodi primjer, kako nisu mogli pristupiti preoperativnim radiološkim snimkama pacijenata, se su morali odgoditi kirurške zahvate (46).

4.6.3. Ryuk Ransomware

Ryuk *ransomware* se privi puta pojavio 2018. godine kada je srušio računalne sustave mnogih ustanova kao što su škole, tvrtke, državne institucije ali medicinski centri. Cilja na visoko vrijedne mete unutar sustava, enkriptira ih te traži otkupninu za povrat pristupa. Širi se preko poruka elektroničke pošte koje sadrže lažne Microsoft Office Word dokumente. Otvaranjem dokumenata zapravo se pokreće *malware* koji omogućava napadačima da prisvoje kontrolu nad računalima, tako što im prosljeđuje administratorske račune (47).

2020. godine onesposobio je više od 250 centara najvećeg privatnog pružatelja zdravstvenih usluga, Universal Health Services, a oporavak je koštao oko 65 milijuna dolara. U izjavi su naveli da nemaju pristup podacima o pacijentima, kao ni slikovnim zapisima CT-a ili rendgena (48).

2021. godine Ryuk napad je izvršen na OrthoVirginia, najvećeg pružatelja usluga ortopedske medicine i terapije u državi Virginia, SAD. Enkriptirao je PACS na kojem su bili medicinski rendgenski zapisi ključni za ortopedsku kirurgiju. Uzrok napada je otvaranje zloćudne poveznice od strane jednog zaposlenika. Dio podataka su spasili gašenjem drugih servera a na kraju tvrde da nisu platili ni otkupninu (49).

4.6.4. Wannacry

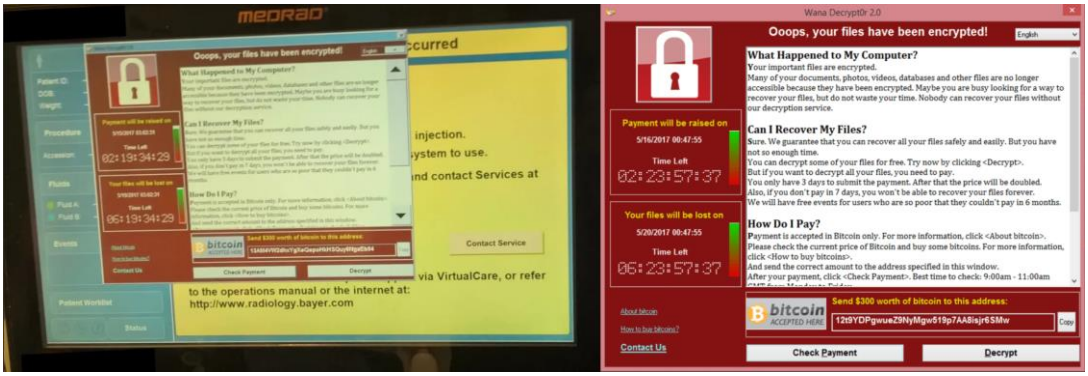
Globalni *ransomware* napad WannaCry započeo je 12.5.2017. godine na nekoliko kontinenata i organizacija. Iako nije bio direktno cilj napada, jedna od najvećih žrtava bio je engleski Nacionalni zdravstveni sustav. Oko 600 ustanova je pogođeno, od kojih su

izravno 34 bolnice potpuno ostale bez digitalnih sustava i medicinskih uređaja kao što su magnetska rezonancija. Neizravno je pogođeno 46 bolnica koje su radile ali otežano (50).

Autori odgovorni za napad iskoristili su sigurnosni propust u Windows operativnom sustavu koji se zvao EternalBlue te ga javno objavili. Microsoft je izdao sigurnosnu zakrpu skoro 2 mjeseca prije WannaCry napada. Problem je bio što mnoge organizacije nisu pravovremeno obnavljale sustave novim zakrpama (51).

Veliki proizvođači intervencijske i dijagnostičke radiološke opreme, BD (Becton, Dickinson and Company) i Siemens izdali su preporuke korisnicima svoje opreme te zakrpe. Siemens je dao upute za 6 grupa svojih proizvoda koji su uključivali CT i MR uređaje (52).

Jedan od pogođenih uređaja je bio i Bayerov injektor za kontraste (Slika 15.) koji se koriste kod radioloških pretraga, kao i neki konvencionalni rentgenski uređaji (53).



Slika 15. Snimka ekrana sa pogođenog Bayerovog injektora (lijevo), snimka same poruke na drugom uređaju (desno)

Izvor: https://www.forbes.com/sites/thomasbrewster/2017/08/03/wannacry-hackers-use-shapeshift-to-launder-bitcoin/?sh=220060323d0d

https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation

Unatoč globalnom širenju, WannaCry je usporen u napredovanju slučajno. Unutar njegovog koda, istraživači *cyber* sigurnosti otkrili su poveznicu na web stranicu. *Malware* se širio samo ako se nije mogao spojiti na navedeni URL. Kupnjom domene i otvaranjem stranice, prestalo je i širenje, odnosno aktivirao se „kill-switch“. Time se nije zaustavilo djelovanje *malware*-a na već instaliranim uređajima (54).

4.6.5. Conti Ransomware

Conti grupa jedna je od najvećih *cyber* kriminalnih skupina na svijetu, a poznati su po agresivnim taktikama i napadima velikih razmjera. Njihove prve verzije *malware*-a pojavile su se početkom 2020. te su postali jedna od najaktivnijih takvih skupina. Pristup mrežama osiguravali su lažnim elektroničkim porukama, iskorištavanjem pristupa računalima na daljinu ili kupovinom pristupa mreži od drugih skupina.

2021. Irski zdravstveni sustav morao je privremeno isključiti svoju mrežu zbog Conti napada. To je izazvalo probleme cijeloj zdravstvenoj infrastrukturi, a ograničilo je pristup svim dijagnostičkim zapisima. Conti je priznao da je imao pristup mreži 2 tjedna, u kojima su preuzeli 700 GB podataka a za otkupninu su tražili skoro 20 milijuna dolara (55).

U izvještaju objavljenom u Irish Medical Journal pod nazivom „The Impact of the Cyberattack on Radiology Systems in Ireland“ navode kako su iz sigurnosnih razloga nakon napada isključili nacionalni sustav pohrane medicinskih slikovnih zapisa, što je utjecalo na dostupnost radioloških usluga na razini cijele države. Ujedno je ugašen i RIS, te su se nalazi slikovnih prikaza pisali ručno te nosili na druge odjele. Očitanja radioloških pretraga obavljala se na samim uređajima sva međusobna komunikacija obavljala se preko osobnih telefona.

Oporavak od štete iznosio je oko 100 milijuna eura, dok pravni troškovi nisu objavljeni. Ukradeno je oko 113.000 privatnih podataka pacijenata i zaposlenika (56,57).

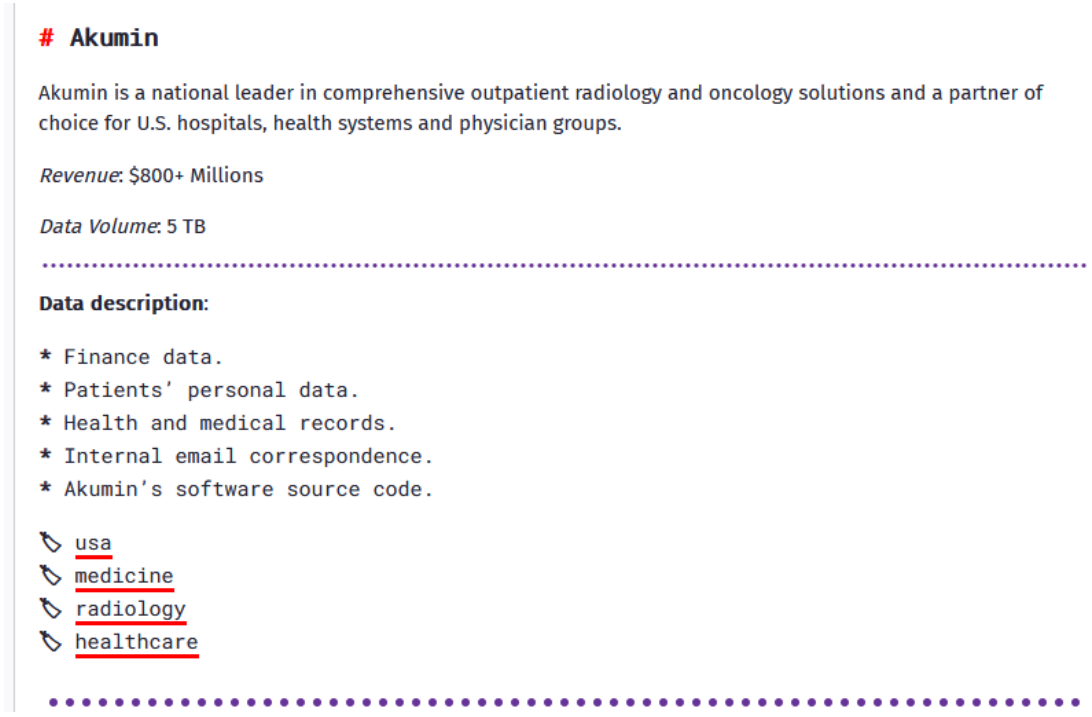
4.6.6. BianLian Ransomware

BianLian je *ransomware* kriminalna *cyber* grupa koja je napadala kritične infrastrukture organizacije SAD-a od 2022. Grupa je dobivala pristup mreži žrtava preko upravljanja računalima na daljinu, koristeći besplatne skripte drugih autora te preuzimala podatke preko FTP-a (file transfer protocol). Iznudom su tražili novčanu naknadu, prijeteći da će javno objaviti podatke ukoliko ih se ne isplati. Prvotno su imali pristup dvostruke iznude, gdje su nakon što sebi presnime podatke enkriptirali ih na računalu žrtve, no od 2023. su prešli na samo presnimavanje (58).

U rujnu 2023. BianLian napao je Akumin, drugu najveću zdravstvenu kompaniju sa Floride koja se bavi radiološkim i onkološkim zdravstvenim uslugama u oko 1000

bolnica na području 48 država SAD-a. Prvi znakovi napada pojavili su se 11.10.2023. te su preventivno pogasili radiološke centre na 50 mjesta. Prema istrazi, napadači su uspjeli pristupiti serverima sa osobnim podacima pacijenata (59).

Prikupili su oko 5 TB medicinskih zapisa, slikovnih podataka dijagnostičkih postupaka te preslike putovnica (Slika 16.). To sve je uzrokovalo odgađanje na stotine pacijenata. Mjesec dana kasnije, 10.11., službeno su objavili da su uspjeli spasiti većinu arhiviranih podataka te na nastavljaju s radom. Početkom prosinca ponovno su napadnuti od iste *cyber* skupine (60).

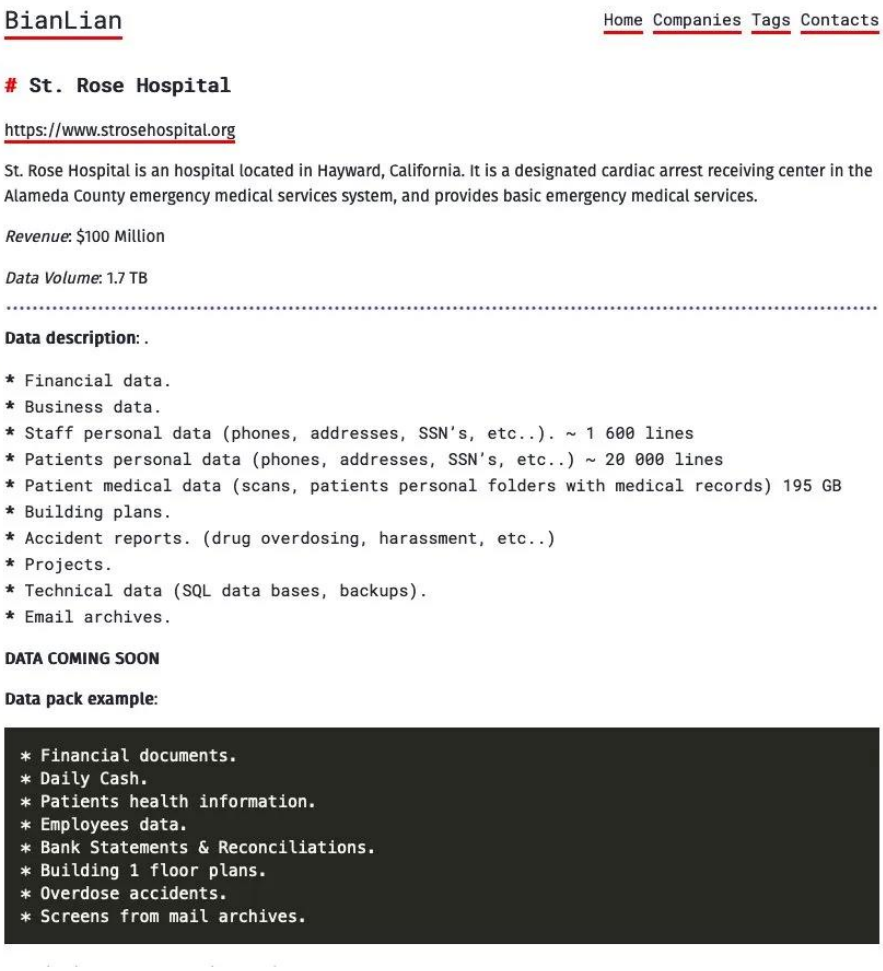


Slika 16. Objava BianLian grupe na svojoj internet stranici na kojoj su prikazali količinu i koje podatke su preuzeli

Izvor: https://twitter.com/H4ckManac/status/1731992794137338295

Ovaj put podaci nisu kriptirani nego samo preuzeti, a napad je uzrokovao prekid u radu odjela za nuklearnu medicinu i dijagnostičku radiologiju u trajanju od 2 tjedna (61).

St. Rose Hospital u Kaliforniji je također bila žrtva napada. Prema vlastitim tvrdnjama, imali su pristup na 1.7 TB podataka osoblju i pacijentima. (Slika 17.).



Slika 17. Objava grupe BrianLian o svom napadu na St. Rose Hospital

Izvor: https://thecyberexpress.com/bianlian-ransomware-st-rose-hospital-as-victim/

Preuzeli su 195 GB od svih podataka kojima su mogli pristupiti, te su tvrdili da će ih objaviti javno ukoliko se ne ispune zahtjevi (62).

5. ZAKLJUČAK

Cyber napadi na radiološke sustave dosta su zanemarena tema što se vidi iz dostupnosti literature i obrađenosti u člancima. Veliki broj radova je nastao nakon nekog napada, te su autori dokumentirali i analizirali propuste nakon što je šteta već učinjena. To dovodi to zaključka da se o tome ne vodi briga dok ne postane problem i bude prekasno. U svijetu je sve više primjera velikih novčanih izdvajanja za oporavak sustava, isplata otkupnina ali i odšteta pacijentima koji nisu na vrijeme dobili traženu radiološku dijagnostičku pretragu ili su im osobni i medicinski podaci postali javni. Nepažnja jednog korisnika koji otvori zloćudni email ili spoji zaraženi prijenosni medij može dovesti do kolapsa cijelog odjela, a i šire. Stoga je za obranu od *cyber* napada bitno da svaki zaposlenik radiološkog odjela bude upoznat sa osnovama brige za sigurnost odjelnog mrežnog sustava. To podrazumijeva opreznost kod samog načina rada na računalu i uređaju, prepoznavanje simptoma *malware*-a i protokola za poduzimanje koraka obrane. Na odgovornosti informatičke službe je pravovremeno ažuriranje svih računalnih sustava, a ovlaštenih servisa uređaja njihovih računalnih sustava.

Jedan od osnovnih odjela svih bolnica je radiološki odjel, gdje počinje najveći dio dijagnostike i odlučuje se o nastavku liječenja. A osnova njegovog rada su računala i mreže bez kojih radiologija postaje spora ili čak neupotrebljiva. Kada radiološki odjel zbog problema sa računalnom infrastrukturom prestane s radom, to ima poguban utjecaj na cijeli bolnički sustav, od hitnog prijema do odgađanja operacija, čime se ugrožavaju životi pacijenata. Pridavanjem veće pažnje na napade na radiološke sustave i obranu od njih, možemo spriječiti ili barem umanjiti njihov utjecaj na rad zdravstvenih sustava, pokazati brigu i spriječiti štetu za pacijente.

6. LITERATURA

1. Europol, Iocta, Internet Organised Crime Threat Assessment : 2018. Europol; 2018. Dostupno na: doi/10.2813/858843

2. Ayala L. Cybersecurity for Hospitals and Healthcare Facilities [Internet]. Apress; 2016. Available from: http://dx.doi.org/10.1007/978-1-4842-2155-6

3. U.S. Department of Homeland Security. National Infrastructure Protection Plan – Healthcare and Public Health Sector-Specific Plan 2015. Capitol Heights: Cybersecurity and Infrastructure Security Agency; 2015 [pristupljeno 04.04.2024.] Dostupno na: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf

4. European Union Agency for Cybersecurity, Smart hospitals : security and resilience for smart health service and infrastructures. European Network and Information Security Agency; 2016. Dostupno na: doi/10.2824/28801

5. Babić RR, Milošević Z, Đinđić B, Stanković Babić G. Radiološki informacioni sistem. Acta medica Medianae. 2012;51(4):39-46.

6. DICOM. [Internet]. Arlington: Medical Imaging & Technology Alliance; 2020. About DICOM Overview. [pristupljeno 04.04.2024.] Dostupno na: https://www.dicomstandard.org/about

7. Imaging Technology News [Internet]. New Jersey: Imaging Technology News; 2018 PACS definition. [pristupljeno 04.04.2024.] Dostupno na: https://www.itnonline.com/content/pacs-definition

8. HL7 International [Internet]. Hl7.org. Ann Arbor: HL7 International; 2016 Introduction to HL7 Standards. [pristupljeno 04.04.2024.] Dostupno na: https://www.hl7.org/implement/standards/index.cfm?ref=nav

9. Eichelberg M, Kleber K, Kämmerer M. Cybersecurity Challenges for PACS and Medical Imaging. Acad Radiol. 2020 Aug;27(8):1126-1139. doi: 10.1016/j.acra.2020.03.026. Epub 2020 May 15. PMID: 32418786.

10. Bhuyan SS, Kabir U, Escareno JM, Ector K, Palakodeti S, Wyant D, et al. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. J Med Syst. (2020) 44:98. doi: 10.1007/s10916-019-1507-y

11. Sterling B. The dropped drive hack [Internet]. Wired. 2011 [pristupljeno 04.04.2024.] Dostupno na: https://www.wired.com/2011/06/the-dropped-drive-hack/

12. Vanhoef, M, Piessens, FRelease the Kraken: New KRACKs in the 802.11 Standard. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security 2018 (pp. 299–314). Association for Computing Machinery. Dostupno na: https://doi.org/10.1145/3243734.3243807

13. Wireshark [Internet]. Wireshark; 2024. Wireshark - display filter reference: Index. [pristupljeno 04.04.2024.] Dostupno na: https://www.wireshark.org/docs/dfref//

14. Martignani C. Cybersecurity in cardiac implantable electronic devices. Expert Rev Med Devices. (2019) 16:437–44. doi: 10.1080/17434440.2019.1614440

15. Sethuraman SC, Vijayakumar V, Walczak S. Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles. J Med Syst. 2019 Dec 14;44(1):29. doi: 10.1007/s10916-019-1489-9. PMID: 31838588.

16. The National Vulnerability Database [Internet] Gaithersburg: National Institute of Standards and Technology; 2024. National Institute of Standards and Technology NVD-results [pristupljeno 04.04.2024.] Dostupno na: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=adobe+reader&search_type=all&isCpeNameSearch=false

17. IBM Security. X-Force Vulnerability Report: Microsoft Windows JPEG buffer overflow CVE-2004-0200 Vulnerability Report [Internet]. 2004. [pristupljeno 04.04.2024.] Dostupno na: https://exchange.xforce.ibmcloud.com/vulnerabilities/16304

18. Be'er H. NorthBit technical repor: Metaphor: a (real) reallife Stagefright exploit. [Internet]. 2016. [pristupljeno 04.04.2024.] Dostupno na: https://www.exploit-db.com/download/39527

19. Spanakis, E, Bonomi, S, Sfakianakis, S, Santucci, G, Lenti, S, Sorella, M, Tanasache, F, Palleschi, A, Ciccotelli, C, Sakkalis, V, Magalini, SCyber-attacks and threats for healthcare – a multi-layer thread analysis. In 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC) 2020 (pp. 5705-5708)

20. Langer SG. Cyber-Security Issues in Healthcare Information Technology. J Digit Imaging. 2017 Feb;30(1):117-125. doi: 10.1007/s10278-016-9913-x. PMID: 27730416; PMCID: PMC5267602.

21. Bhattacharyya DK, Kalita J.K. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance [Internet]. Chapman and Hall/CRC; 2016. Dostupno na: http://dx.doi.org/10.1201/b20614.

22. Moses V, Korah I. Lack of security of networked medical equipment in radiology. AJR Am J Roentgenol. 2015 Feb;204(2):343-53. doi: 10.2214/AJR.14.12882. PMID: 25615757.

23. Desjardins B, Mirsky Y, Ortiz MP, Glozman Z, Tarbox L, Horn R, Horii SC. DICOM Images Have Been Hacked! Now What? AJR Am J Roentgenol. 2020 Apr;214(4):727-735. doi: 10.2214/AJR.19.21958. Epub 2019 Nov 26. PMID: 31770023.

24. Nguyen TN. Certified ethical hacker v. 10 online course: a case study. InProceedings of the 10th International Conference on E-Education, E-Business, E-Management and E-Learning 2019 Jan 10 (pp. 168-173). https://doi.org/10.1145/3306500.3306547

25. NTT Security. 2017 Global Threat Intelligence Report (GTIR). [Internet] 2017 [pristupljeno 04.04.2024.] Dostupno na: https://www.astrid-online.it/static/upload/2017/2017_gtir_ntt_security_04252017.pdf

26. Encyclopædia britannica [Internet]. Chicago (IL): Encyclopædia Britannica Inc. Encyclopedia Britannica. 2024 Cryptography Dostupno na: https://www.britannica.com/topic/cryptography

27. Cho, A. (2014). Quantum spy games. Science, 343, 482–283. DOI: https://doi.org/10.1126/science.343.6170.482

28. Mirsky Y, Mahler T, Shelef I, Elovici Y. CT-GAN: Malicious tampering of 3D medical imagery using deep learning. In Proceedings of the 28th USENIX Security Symposium. USENIX Association. 2019. p. 461-478. (Proceedings of the 28th USENIX Security Symposium).

29. Mahler T, Elovici Y, Shahar Y. A new methodology for information security risk assessment for medical devices and its evaluation. arXiv preprint arXiv:2002.06938. 2020 Feb 17.

30. Tang M, Yamamoto T. Progress in Understanding Radiofrequency Heating and Burn Injuries for Safer MR Imaging. Magn Reson Med Sci. 2023 Jan 1;22(1):7-25. doi: 10.2463/mrms.rev.2021-0047. Epub 2022 Feb 26. PMID: 35228437; PMCID: PMC9849420.

31. Radmard M, Ansari G, Mirza-Aghazadeh-Attari M, Taratuta E, Butler R, Colucci PG, Yousem DM, Khan M. Unsolicited Invitations to Scientific Meetings: Radiologists' Experience. Curr Probl Diagn Radiol. 2023 Nov-Dec;52(6):534-539. doi: 10.1067/j.cpradiol.2023.06.018. Epub 2023 Jul 2. PMID: 37442705.

32. Healthcare and Public Health Sector Coordinating Council (HSCC). Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations. [Internet]. Washington, D.C.; The U.S. Department of Health & Human Services; 2023. https://405d.hhs.gov/Documents/tech-vol2-508.pdf

33. Recht MP. Work From Home in Academic Radiology Departments: Advantages, Disadvantages and Strategies for the Future. Acad Radiol. 2023 Apr;30(4):585-589. doi: 10.1016/j.acra.2022.11.019. Epub 2022 Dec 26. PMID: 36577604; PMCID: PMC9791330.

34. Kaspersky. [Internet]. Massachusetts: Kaspersky; 2023. What is heuristic analysis? 2023 [pristupljeno 05.04.2024.] Dostupno na: https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis mm

35. Wang Z, Ma P, Zou X, Zhang J, Yang T. Security of medical cyber-physical systems: an empirical study on imaging devices. InIEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) 2020 Jul 6 (pp. 997-1002). IEEE..

36. Healthcare and Public Health Sector Coordinating Council (HSCC). Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations. [Internet]. Washington, D.C.; The U.S. Department of Health & Human Services; 2023, [pristupljeno 05.04.2024.] Dostupno na: https://405d.hhs.gov/Documents/tech-vol1-508.pdf

37. IBM documentation. Introduction to firewall support. [Internet]. Ibm.com. 2024. [pristupljeno 05.04.2024.] Dostupno na: https://www.ibm.com/docs/en/db2/11.5?topic=security-firewall-support

38. Cynerio. [Internet]. Cynerio. Network Segmentation for Hospitals: Challenges and Technology Solutions. 2020. [pristupljeno 05.04.2024.] Dostupno na: https://assets-global.website-files.com/5d2dbce8358ee9004d1c7eb6/5e9c6c1d5fc32360da6a4943_Segmentation%20Whitepaper.pdf

39. Dicom Systems. [Internet]. DICOM encryption and anonymization 2020, [pristupljeno 05.04.2024.] Dostupno na: https://dcmsys.com/project/dicom-encryption-anonymization/

40. Chen PH, Bodak R, Gandhi NS. Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. J Digit Imaging. 2021 Jun;34(3):731-740. doi: 10.1007/s10278-021-00466-x. Epub 2021 Jun 22. PMID: 34159418; PMCID: PMC8218969.

41. Cybersecurity and Infrastructure Security Agency CISA. [Internet]. Ransomware activity targeting the healthcare and public health sector. 2020. [pristupljeno 05.04.2024.] Dostupno na: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a

42. Threat hunter team. Symantec Enterprise Blogs [Internet]. New Orangeworm attack group targets the healthcare sector in the US, Europe, and Asia. 2018. [pristupljeno 05.04.2024.] Dostupno na: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

43. Seals T. Orangeworm mounts espionage campaign against healthcare [Internet]. Threatpost. 2018 [pristupljeno 05.04.2024.] Dostupno na: https://threatpost.com/orangeworm-mounts-espionage-campaign-against-healthcare/131381/

44. Kiguolis L. Kwampirs malware Removal Guide. 2SPYWARE [Internet]. 2017 [pristupljeno 05.04.2024.] Dostupno na: https://www.2-spyware.com/remove-kwampirs-malware.html

45. Cloudflare. [Internet] What are Petya and NotPetya?. Cloudflare Learning Security. 2024 [pristupljeno 05.04.2024.] Dostupno na: https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/

46. Greenberg A. How the worst cyberattack in history hit American hospitals [Internet]. Slate. 2019 [pristupljeno 06.04.2024.] Dostupno na: https://slate.com/technology/2019/11/sandworm-andy-greenberg-excerpt-notpetya-hospitals.html

47. Burdova C. What is Ryuk ransomware? [Internet]. What Is Ryuk Ransomware? Avast; 2022 [pristupljeno 06.04.2024.] Dostupno na: https://www.avast.com/c-ryuk-ransomware

48. Bajak F, Alonso-Zaldivar R. Suspected ransomware attack hobbles major hospital chain's U.S. facilities [Internet]. PBS NewsHour. 2020, [pristupljeno 06.04.2024.] Dostupno na: https://www.pbs.org/newshour/nation/suspected-ransomware-attack-hobbles-major-hospital-chains-u-s-facilities

49. Gillin P. Lessons from a ransomware attack: How one healthcare CIO helped her company recover [Internet]. SiliconANGLE. 2023 [pristupljeno 06.04.2024.] Dostupno

na: https://siliconangle.com/2023/09/08/lessons-ransomware-attack-one-healthcare-cios-company-recovered/

50. National Audit Office. [Internet]. Investigation: WannaCry cyber-attack and the NHS London: National Audit Office; 2018 [pristupljeno 06.04.2024.] Dostupno na: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

51. Kaspersky. [Internet]. Kaspersky Cyber Security Solutions for Home and Business. What is WannaCry ransomware? 2024 [pristupljeno 06.04.2024.] Dostupno na: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

52. Fierce Biotech. [Internet]. Taylor NB. WannaCry ransomware infected Bayer U.S. medical devices 2017 [pristupljeno 06.04.2024.] Dostupno na: https://www.fiercebiotech.com/medtech/wannacry-ransomware-infected-bayer-u-s-medical-devices

53. Pearson D. MRI contrast injector among devices attacked by WannaCry in U.S [Internet]. Health Imaging. 2017 [pristupljeno 06.04.2024.] Dostupno na: https://healthimaging.com/topics/health-it/enterprise-imaging/mri-contrast-injector-among-devices-attacked-wannacry-us

54. Woollaston-Webber V. WannaCry ransomware: what is it and how to protect yourself [Internet]. WIRED. 2017 [pristupljeno 06.04.2024.] Dostupno na: https://www.wired.co.uk/article/wannacry-ransomware-virus-patch

55. Flashpoint. [Internet]. Flashpoint Intel Team. Conti Ransomware: The History Behind One of the World's Most Aggressive RaaS Groups 2022 [pristupljeno 06.04.2024.] Dostupno na: https://flashpoint.io/blog/history-of-conti-ransomware/

56. Anderson T, Torreggiani WC. The impact of the cyberattack on radiology systems in Ireland. Irish Medical Journal. 2021;114(5):347.

57. Warner M. Responding to a ransomware attack in radiology [Internet]. Everything Rad. Carestream Health; 2023 [pristupljeno 06.04.2024.] Dostupno na:

https://www.carestream.com/blog/2023/06/28/responding-to-ransomware-attack-in-radiology/

58. Cybersecurity and Infrastructure Security Agency. [Internet]. #StopRansomware: BianLian Ransomware Group. Cybersecurity and Infrastructure Security Agency. 2023 [pristupljeno 06.04.2024.] Dostupno na: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a

59. Goodman CK. Patients desperate for imaging services, worried about health information, after Akumin shuts down due to ransomware attack [Internet]. Sun Sentinel. 2023 [pristupljeno 06.04.2024.] Dostupno na: https://www.sun-sentinel.com/2023/10/24/patients-desperate-for-imaging-services-worried-about-health-information-after-akumin-shuts-down-due-to-ransomware-attack/

60. De Felice MA. Akumin undergoes two cyber attacks in less than a month: thousands of PHI and PII data still in the hands of BlackSuit and BianLian. [Internet]. SuspectFile 2023 [pristupljeno 06.04.2024.] Dostupno na: https://www.suspectfile.com/akumin-undergoes-two-cyber-attacks-in-less-than-a-month-thousands-of-phi-and-pii-data-still-in-the-hands-of-blacksuit-and-bianlian/

61. De Felice MA. Akumin Case: BianLian Publishes Initial Proof Data on Their Blog. [Internet]. SuspectFile 2023 [pristupljeno 06.04.2024.] Dostupno na: https://www.suspectfile.com/akumin-case-bianlian-publishes-initial-proof-data-on-their-blog/

62. Pandagle V. BianLian ransomware lists St. Rose Hospital as victim, claims access to 1.7TB data [Internet]. The Cyber Express. 2023 [pristupljeno 06.04.2024.] Dostupno na: https://thecyberexpress.com/bianlian-ransomware-st-rose-hospital-as-victim/

7. ŽIVOTOPIS

OSOBNI PODACI

Ime i prezime: Davor Viculin

Datum i mjesto rođenja: 30.4.1985. god, Zagreb

Državljanstvo: Hrvatsko

Adresa: Bele Bartoka 18, Zagreb

Mobitel: 091/ 539 7129

E-mail: davor.viculin@gmail.com

OBRAZOVANJE I OSPOSOBLJAVANJE:

1992. – 2000. Osnovna škola „Nikola Tesla“, Zagreb

2000. - 2004. Gimnazija „Lucijan Vranjanin“, Zagreb

2004. - 2006. Prirodoslovno-matematički fakultet u Zagrebu

Smjer: Istraživački studij fizike (nezavršeni studij)

2006. – 2010. Zdravstveno veleučilište u Zagrebu

Smjer: Studij radiološke tehnologije

2021. – 2024. Sveučilišni odjel zdravstvenih studija Split

Diplomski sveučilišni studij

Smjer: Radiološka tehnologija

RADNO ISKUSTVO:

2011. – 2012. Pripravnički staž:

Dom zdravlja Zagreb Istok, Radiološka ambulanta Peščenica

Klinika za tumore, Služba za dijagnostičku i intervencijsku radiologiju

2014. - 2015. Klinički bolnički centar Sestre Milosrdnice, Zagreb

Zavod za onkologiju i radioterapiju

2015. - Klinika za tumore, Zagreb, Zavod za radioterapiju i internističku onkologiju

ZNANJA I VJEŠTINE

Engleski jezik – aktivno u govoru i pismu

Rad na računalu - ECDL diploma (European Computer Driving Licence), Osnovni (sedam ECDL-ispita)