REVIEW PAPER (PREGLEDNI RAD)

Cyber attacks on radiological systems

Davor Viculin[1], **Frane Mihanović**[2]

[1]Department of radiotherapy and oncology, Clinic for tumors, University Clinical Hospital Center “Sestre Milosrdnice”, Croatia

[2]University Department of Health Studies, University of Split, Split, Croatia

Corresponding author: Davor Viculin, e-mail: davor.viculin@gmail.com

DOI: https://doi.org/10.55378/rv.48.2.1

Abstract

The base 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 are valuable. The reasons for the attacks are often financial gain, political, ideological or personal. The start of an attack can be physical access to radiological devices or network access. DICOM files 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. Well known types are Denial-Of-Service, malware, cryptographic attacks and making changes of device settings. When defending against cyber-attacks, it is important to secure communication by e-mail and to keep software updated. The IT department of the radiology department should observe accounts of all users and check the authorizations. Networks must have access restrictions according to workplaces and purposes to prevent unwanted access. Web proxy protection restricts access to Internet sites that are potentially dangerous. The basics of the department’s network, such as servers, must be physically secured from access. DICOM files should be encrypted with the most secure algorithms available. In response to cyber-attacks, it is necessary to have standard 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

Abbreviations and acronyms: AES (Advanced encryption standard), CD (Compact disc), CT (Computed tomography), DDOS (Distributed denial-of-service), DICOM (Digital Imaging and Communications in Medicine), HL7 (Health Level-7)MRI (Magnetic resonance imaging), PACS (Picture archiving and communication system), RIS (Radiology information system), RSA (Rivest–Shamir–Adleman), URL (Uniform resource locator), USB (Universal serial bus), WEP (Wired equivalent privacy), WPA2 (Wi-Fi protected access 2)

Introduction

Computers today have become an essential part of modern radiology. They allow us to send and receive medical imaging information around the world. With the development of computers and their application in radiology, new challenges have been created, and one of them is cyber security [1]. In recent years, hackers have been able to compromise most medical devices, from infusion pumps to X-ray machines. In the fall of 2013, the Mayo Clinic hired a group of hackers to try to modify 40 different medical devices. After several weeks of looking for security flaws, vulnerabilities were found in all devices, including MRI and ultrasound [2]. Most recent problem is ransomware, which is designed to encrypt data and request ransom. According to a report by the U.S. Department of Justice, in 2016, there were 4,000 such attacks, which is four times more than the year before. The healthcare sector accounts for about 15% of such attacks, which is not negligible, and this type of attack, according to statistics from 2017, accounted for 50% of cyber incidents in hospitals [3].

Cyber-attacks on hospital systems have become more popular today. While such attacks were once widespread and random, today they are oriented towards a specific sector in healthcare, depending on the needs and interests of the groups behind them. Radiological devices are targets because they are an essential part of every healthcare facility, and their infrastructure creates many opportunities for cyber-attacks.

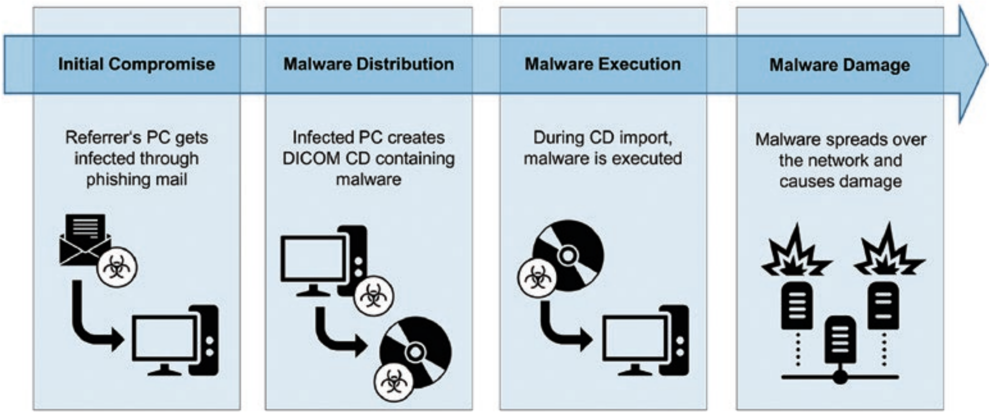

Initial Compromise
Referrer's PC gets infected through phishing mail
Malware Distribution
Infected PC creates DICOM CD containing malware
Malware Execution
During CD import, malware is executed
Malware Damage
Malware spreads over the network and causes damage

Figure 1. Entering malware from removable media
Source: https://www.sciencedirect.com/science/article/pii/S1076633220301719

Aim of the work

The aim of this review thesis is to show that cyber-attacks on radiological systems are not just occasional harmless incidents but a real threat. Presentations on theory of attacking systems, defense techniques and the application of data recovery can be useful in the daily work of the radiology department. Experience and advice from other radiology departments and hospitals around the world can help prevent repeating the same mistake. Examples of attacks from around the world should motivate us to increase attention to cyber security in radiology.

Discussion

Reason and methods

A negative side effect of wide Internet is the increase in cybersecurity incidents, such as computer viruses, *ransomware* (demanding a ransom to regain access to data) or the theft of patient data. While in the past, cyberattacks were most often caused by curious amateurs, today they are mostly work of organized crime groups. Accordingly, attacks on hospitals are no longer random, but increasingly focus on hospital systems that are becoming primary target.

The most common reasons are: stealing data for financial gain (ransom, selling data or scams), state-level espionage, gaining access to radiological data (political, economic or military purposes) and sabotage (blocking or influencing medical procedures).

Entering patient data from a removable medium

Patients bring their data on storage media to the hospital facility and their media can contain malware. Most systems that burn DICOM CDs add viewer that runs on standard Windows systems which have autorun function included. Malware from the first computer, via DICOM CD, can be copied to the second computer without the need for user action. (Figure 1). It can intercept Internet traffic and send the usernames and passwords to the attacker's device and spread further. [5]. Sometimes an attacker deliberately leaves a USB, external hard drive or CD in the parking lot of hospital expecting that some conscientious employee will find it and connect it to the hospital computer [6]. In an experiment by the US Department of Homeland Security, 60% of their employees who found a device in the parking lot, tried to check the owner at the workplace. If there was an institution label on the same medium, success was 90% [7].

Network Attack

Network attack is when a hacker manages to gain access to a hospital's network system. The first option is access to

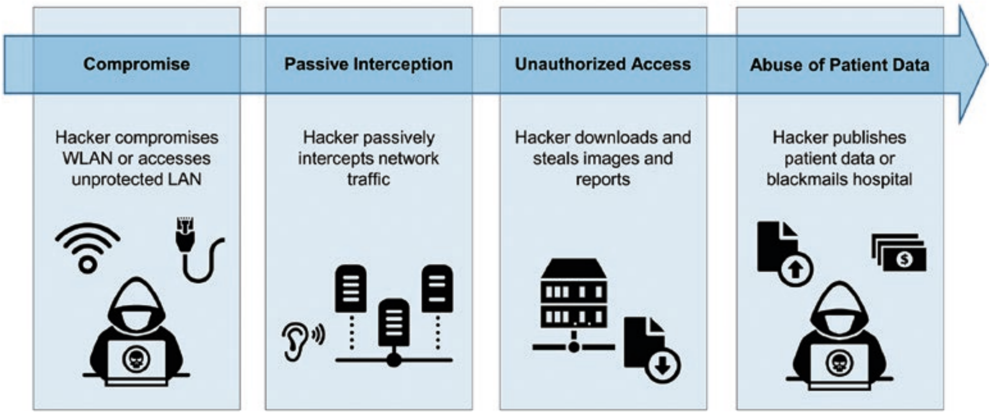

Compromise
Hacker compromises WLAN or accesses unprotected LAN
Passive Interception
Hacker passively intercepts network traffic
Unauthorized Access
Hacker downloads and steals images and reports
Abuse of Patient Data
Hacker publishes patient data or blackmails hospital

Figure 2. Network Access in a Cyber Attack
Source: https://www.sciencedirect.com/science/article/pii/S1076633220301719

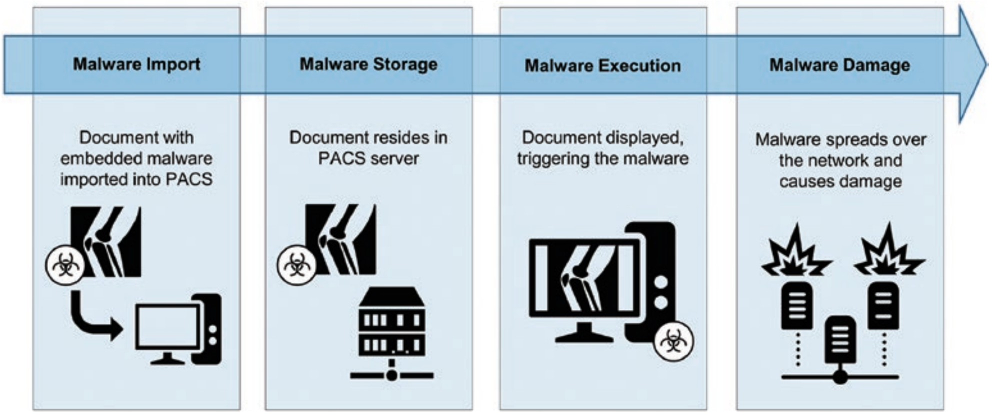

Malware Import
Document with embedded malware imported into PACS
Malware Storage
Document resides in PACS server
Malware Execution
Document displayed, triggering the malware
Malware Damage
Malware spreads over the network and causes damage

Figure 3. Malware cloaking and DICOM format
Source: https://www.sciencedirect.com/science/article/pii/S1076633220301719

an unprotected network connection via cable. The second is when he manages to decrypt the password for wireless access (Figure 2). Over time, weaknesses in all wireless network protection mechanisms have been discovered, from the original WEP to WPA2, which is used today. [8]. The final stage is downloading images and patient reports.

A new method of attacking the network is the use of drones. This allows the attacker to access any hospital network within 10 meters distance [9]. In two experiments, drones were guided to hard-to-reach places above hospitals and managed to connect. Drones initially use the logout method, where users are forced to disconnect from the hospital network and then set new fake access. [10].

Malware in DICOM format

Malware can be injected into DICOM files where it can operate in the PACS behind the firewall. Malware inserted into a DICOM image or report will not activate on the user device but on the workstation or server. (Figure 3). When activated, it can access the entire PACS archive. There are three main ways to inject malware into the DICOM format [5].

File format in the first 128 *bytes* contains nothing of the DICOM standard but arbitrary information. This can be a place for malware insertion. [5]. Today's DICOM standard supports adding other file types to a DICOM file which have their own security holes. DICOM can be compressed, so attacker can create a file that, when unpacked, will run a malicious script [11].

Interception of communication

Hacker installs small computer into the connection between the radiological device itself (e.g. CT, MRI...) and the workstation, server or network in general (Figure 4). It is also called *a man-in-the-middle* attack. This requires physical access [5]. It can change data packets, display false displays on screens and take full control [2].

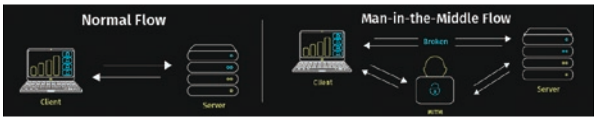


Figure 4. Man-in-the-middle attack
Source: https://www.veracode.com/security/man-middle-attack

Network Infiltration with Wrong HL7 Messages

By passively monitoring HL7 data over the network, the attacker can obtain patient data. (Figure 5). In the same way, it can add or modify existing HL7 messages. [5].

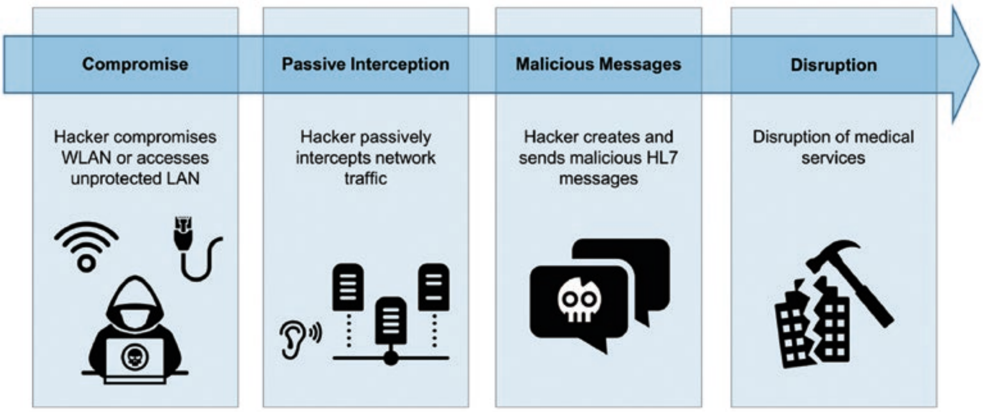

Compromise
Hacker compromises WLAN or accesses unprotected LAN
Passive Interception
Hacker passively intercepts network traffic
Malicious Messages
Hacker creates and sends malicious HL7 messages
Disruption
Disruption of medical services

Figure 5. Inserting Wrong HL7 Messages
Source: https://www.sciencedirect.com/science/article/pii/S1076633220301719

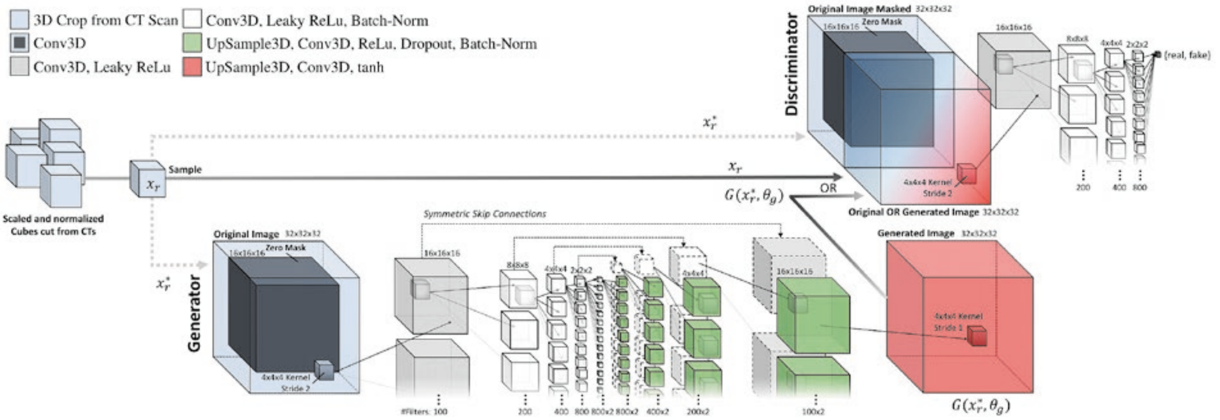


Figure 6. Rewriting CT Scans
Source: https://www.researchgate.net/publication/330357848_CT-GAN_Malicious_Tampering_of_3D_Medical_Imagery_using_Deep_Learning

Types of attack

Cyberattacks can target radiological systems at three levels. Primary infiltration that has a direct impact on hospital patients. Indirect influence is considered secondary. Tertiary infiltration refers to an attack on infrastructure such as power supplies or networks [12].

A potential attacker first tries to access the hospital network or equipment, then he evaluates what information and possibilities he has and compares them with intentions. The peak of an attack is when the attacker succeeds in his intention [13].

Actions in the last step can be divided into active (adjusting or stopping operation, and intercepting/changing data collected through radiological devices) and passive (accessing and collecting medical imaging records). [9].

Denial-of-service

An attack that aims to block all computers connected to a network and disable their communication by overflow is called a Distributed Denial-Of-Service (DDoS) attack. [14]. DDoS attack can send a large number of DICOM messages to overflow the server or send corrupted DICOM files to cause system crash [15].

Malware – an unauthorized program inserted into a computer

Malware (malicious software) can be any program that has a malicious purpose, such as causing a malfunction, disabling or limiting the control of the rightful owner and gaining control by the attacker [16].

According to the 2017 NTT Data ("2017 Global Threat Intelligence Report"), in the total number of *ransomware* attacks in all branches of the economy, healthcare organizations accounted for 15%, while in healthcare itself, *ransomware* accounted for 50% of incidents [17].

Cryptographic attack

A cryptographic attack is revealing data that has been hidden or decrypt information that is not intended for third parties [13]. Cryptography is the process of encrypting and decrypting information that only the sender and receiver can understand [18]. In radiology, there is a possibility of altering CT or MRI images. Adding or subtracting evidence of illness from medical images can stop a political candidate, sabotage research, commit insurance fraud, or even murder [20]. As insurance fraud, individuals can make personal gain based on falsified findings. Intention is getting undeserved benefits: life insurance, faking accident, incapacity to work or profit from insurance. In targeted attacks, a patient can be lured into a diagnostic examination by adding an appointment to the hospital system, faking a call for national screening or hacking routine laboratory tests. [20].

For the process to be successful and anatomically realistic, the following steps are followed (Figure 6). [19]:

1. Determining the location on the CT/MRI data where evidence should be added or removed
2. Cut out the "cube" from that position
3. Adding/removing the desired object (disease sign)
4. Fixing a modified "cube" with artificial intelligence
5. Checking the cube measurements
6. Inserting modified cube back to the CT/MRI data

Researchers from Israeli universities from the Department of Information Systems Engineering (Ben-Gurin University and Soroka University Hospital Center, Beer-Sheva) have published several papers on this topic. In this study, they hired three radiologists and used artificial intelligence to review CT scans and determine the diagnosis (Figure 7). [19].

As images, 70 computer-altered images were used in which signs of lung cancer were added or deleted, and 30 unchanged. Radiologists diagnosed lung cancer on 99% of subsequently altered images. On CT scans where signs of disease were removed by computer, 94% of them were declared healthy by radiologists. After the researchers introduced the radiologists to them, they repeated the examination. In this round, they incorrectly diagnosed 60% of the data with added signs of illness, and 87% with those removed. Also, after they used modern artificial intelligence for the automated *screening* method, they had a 100% error with the subsequently altered images, which

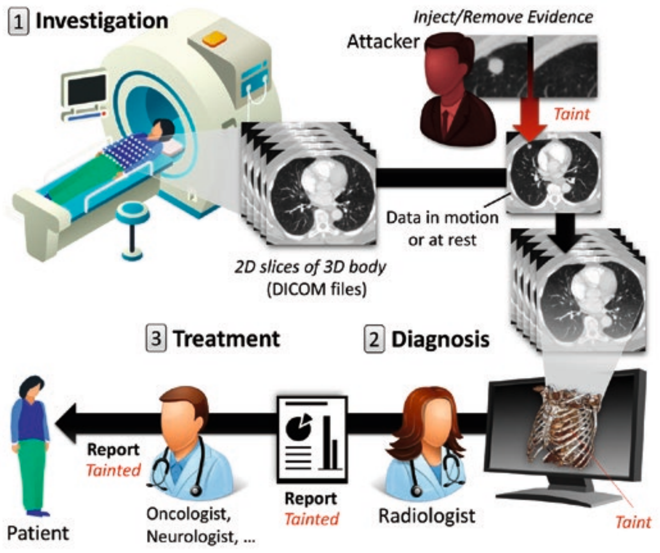


Figure 7. Modification procedure on CT scans
Source: https://www.researchgate.net/publication/330357848_CT-GAN_Malicious_Tampering_of_3D_Medical_Imagery_using_Deep_Learning

proves that it is very unreliable in these types of attacks (19).

Changes to device settings

Devices in radiology such as CT, MRI and radiotherapy accelerators, can be used to injure a patient by using their imaging methods. A documented incident from 1985 shows that similar scenarios are possible. Therac-25 was a radiotherapy device that had a defective safety switch which did not interrupt radiation on time. This was not a cyber attack, but it shows potential risk of changing settings. Today there are potential hazards with any radiological (and radiotherapy) device, especially now when all devices are networked [21]. Manipulation in contrast media injectors settings can change the amount of contrast given to the patient, reduce diagnostic value of examination or cause side effects with excessive doses and damage injector [20]. Radiological devices use multiple components with electric motors. By changing the settings on the control unit computer, an attacker can make unwanted movements in order to cause a collision and damage the device or injure the patient [20].

Specific parameters in diagnostic CT scans are mAs and kV. If these parameters are higher than supposed, it can cause radiation injuries. By changing CT settings, an attacker can influence the behavior of device and affect the imaging process or damage device. If calibration values are changed, device can be forced to use wrong parameters [20].

Changes in the configuration files of MRI device may produce a stronger magnetic field than intended which can damage the receiving coil. This may also include interference with the radio frequency signal that can cause damage to the device and burns in patients [21]. Another option is to falsely activate the magnet's rapid cooling ("*quenching*") security system, which is used if a fire or gas leak occurs. If there was no need for such a procedure, suffocation, hypothermia or rupture of the patient's eardrum may occur. Furthermore, it can damage the device [21].

DEFENSE OF RADIOLOGICAL SYSTEMS AGAINST CYBER ATTACKS

Securing communication by e-mail

In one study of invitations to radiology congresses and conferences, 73.3% of the 45 radiologist participants received invitations to participate in some way over a period of 2 weeks, but 96% of them were not related to their specialty at all [22].

Endpoints in radiological systems

The problem with larger devices such as CT or MRI that use their own workstations, so it is recommended to protect such systems through a firewall [4]. Some devices and workstations also use physical protection, to prevent connection (USB, network cable). This method of defense is useful if a potential attack is planned using the "man-in-the-middle" technique [24].

Organization of access

Radiology departments must identify all users and monitor their access to data, applications, systems and devices so it can restrict their access and activities if needed. [25]. Employees must work under their account and log out when done. This becomes an additional security of the PACS system [4].

Organization of the network

A successful method of maintaining network security is the use of firewall. In radiology, they play a fundamental role in security.

Another method of *cyber*-attacks security is segmentation into smaller ones. (Figure 8). These zones are di-

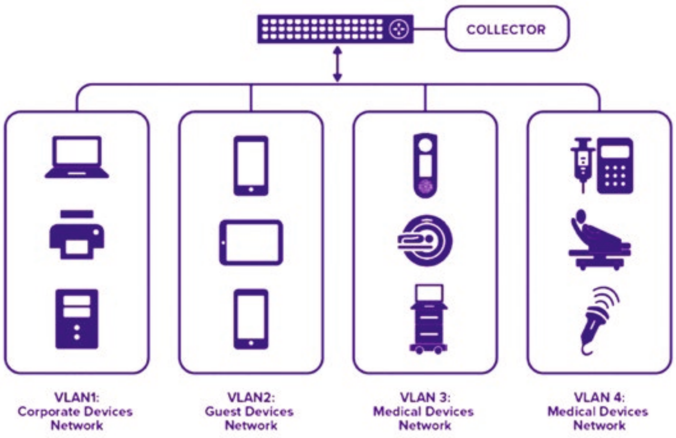


Figure 8. An example of the division of a network of radiological devices and other hospital networks
Source: https://www.armis.com/blog/healthcare-network-segmentation-bridging-the-nac-gap/

vided according to value of data [23]. Each segment is set up as an isolated part of the network. If all devices were connected, an attacker who gains access to one point can access all other devices on that network [26]. Web *proxy* systems provide important protection against *malware* attacks on radiological workstations. Most *malware* and *phishing* attacks are web-based, so they block access to known malicious sites (23). Some cyber-attacks require physical access to network devices so servers and routers should be located in safe places. Network cable paths between the server room and the radiology department can also be weak spot [23].

Data protection with DICOM encryption

DICOM can use advanced encryption algorithms AES or RSA to encrypt data. AES is a standard for DICOM encryption, it uses a symmetric algorithm with the same key for encryption and decryption. AES is used to encrypt current DICOM data due to its efficiency and speed, while RSA is more used for the secure data in transfer.

Cyber-attack response and recovery

The radiology department should detect attacks that bypassed security obstacles and responding against them and have guidelines for incident response (Figure 9). (23). According to research [27], Ransomware Cyber Attacks on radiological systems can be divided into four phases.

The earliest sign is that several IT systems within the radiology department are inaccessible. This causes the inability to access patient data in PACS or RIS. Networks must be disabled to prevent major damage and focus on patient safety and preventing further harm. The second phase begins with a sufficient amount of damage data in the radiology department. In phase three, attention is on network repair, and not on radiological procedures. Backing up to another network or unconnected server is the best option [28]. Antimalware programs probably can't identify all malware so entire system should be restored on software-clean devices.

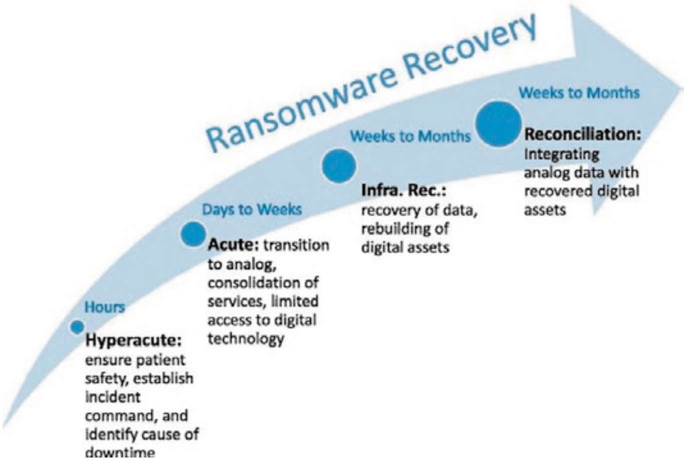

Ransomware Recovery
Hours
Hyperacute: ensure patient safety, establish incident command, and identify cause of downtime
Days to Weeks
Acute: transition to analog, consolidation of services, limited access to digital technology
Weeks to Months
Infra. Rec.: recovery of data, rebuilding of digital assets
Weeks to Months
Reconciliation: Integrating analog data with recovered digital assets

Figure 9. View cyber attack recovery timelines. The times required for the phases depend on the size, complexity and preparation of the radiology department
Source: https://pubmed.ncbi.nlm.nih.gov/34159418/

The first three phases focus on ensuring the continuation of work and providing safe care for the patient. The last phase is connecting data that has not been entered into the digital radiology. The success of this phase is highly dependent on the good organization of data collection from previous phases. *Cyberattacks* are unlikely to decrease over time so cybersecurity must be included in standard plans and budgets [27].

Attacks on radiological systems in the world

Orangeworm (Kwampiris)

In January 2015, the Orangeworm cyber group was discovered. Their malware, called Kwampirs, was found on the systems of large healthcare corporations in America, Asia and Europe. Kwampirs have been found on medical devices in radiology, such as X-rays and MRI. The problem was with devices that used older operating systems and were rarely upgraded. It could also be disguised in image records (Figure 10). For such outdated systems, all security vulnerabilities are well described, which makes them easy target (42, 43).

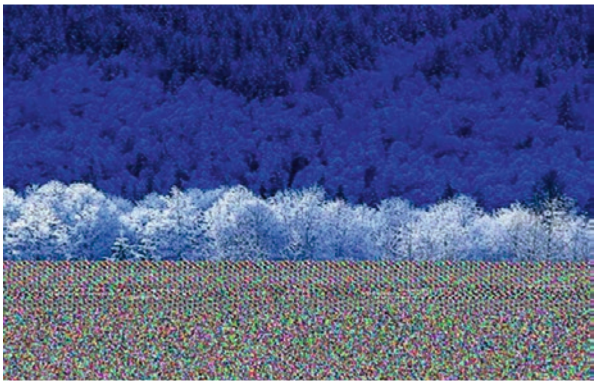
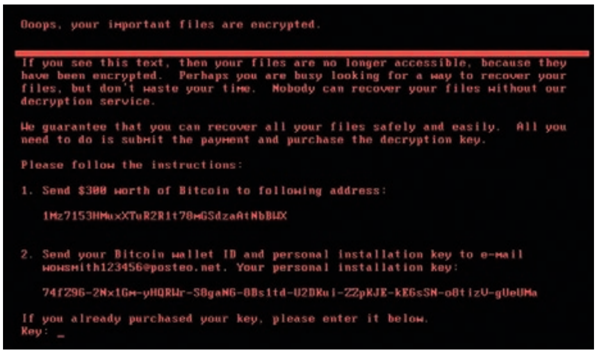


Figure 10. An example of an image that contains Kwampir, looks like an error in the image, but in fact it is a malware installation that thus avoids antivirus programs
Source: https://resources.cylera.com/hubfs/Cylera%20Labs/Cylera%20Labs%20Kwampirs%20Shamoon%20Technical%20Report.pdf

Kwampirs first analyzes the radiological device and sends the data to the authors only if it meets certain requirements. Interesting data are image records, details about the device and the computer network. It spreads further altering its record in the system to avoid security programs. It also allows remote control of radiological devices. It usually has no symptoms of infection [29].

Petya and NonPetya

Petya is a type of malware that appeared in 2016. It locks files and folders demand a ransom to retrieve them. Unlike previous types of malwares, Petya blocks the user's entire hard drive by blocking the file list and works only on Windows operating system. It spreads through e-mail messages as attachment or link. In 2017, NotPetya appeared. It encrypts the entire hard drive with all the data (Figure 11). It spreads rapidly because it does not require user activity.



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

Figure 11. Screenshot after NotPetya malware attack
Source: https://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/?sh=6eb2317f532e

The original purpose was to attack various global corporations, but it also spread to hospital systems on all continents. The damage was only caused on computers using the Windows platform, while Linux systems were spared. For example, the Heritage Valley Health System (Pennsylvania, USA) states in a report that their radiology devices such as X-rays, CT scans or MRIs had no problems. The problem were workstations that saved MRI images and runs on Windows. Another hospital could not access preoperative radiological images of patients so surgical procedures had to be postponed [30].

Ryuk Ransomware

The Ryuk *ransomware* first appeared in 2018 when it crashed the computer systems of many institutions such as schools, businesses, government institutions and medical centers. It targets high-value data, encrypts them, and demands a ransom to regain access. It spreads through e-mails with fake Microsoft Office Word documents. Opening documents triggers *malware* that allows attackers to take control of computer by getting administrator accounts [31].

In 2020, it disabled more than 250 centers of the largest private health care provider, Universal Health Services, and the recovery cost about $65 million. In a statement, they stated that they do not have access to patient data, as well as CT or X-ray images [32].

In 2021, Ryuk attacked OrthoVirginia, the largest provider of orthopedic medicine and therapy services in the state of Virginia, USA. It encrypted PACS, which contained medical X-ray records crucial for orthopedic surgery. They saved some data by shutting down servers, and in the end, they claim that they did not even pay the ransom [33].

Wannacry

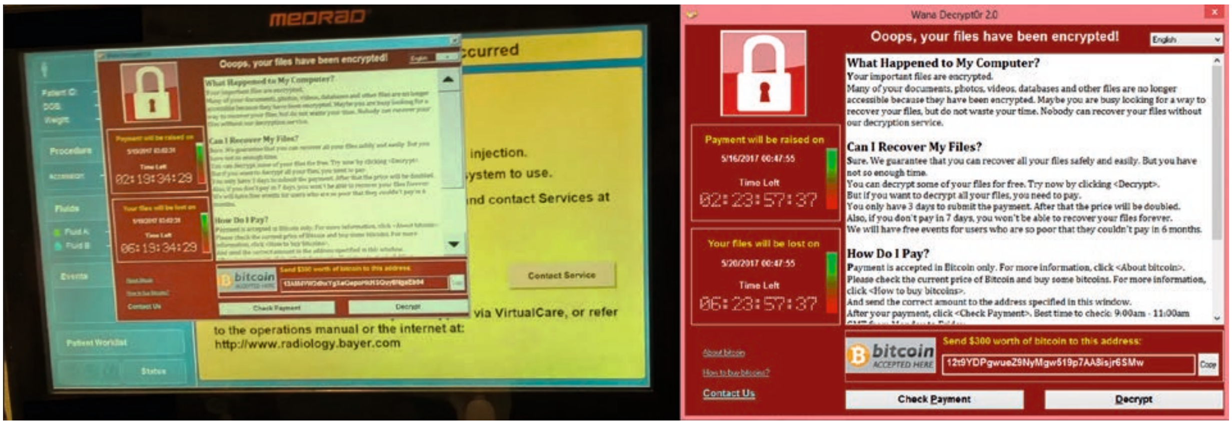
The global WannaCry ransomware attack began on May 12, 2017, on several continents and organizations. One of the biggest casualties was the English National Health Service. About 600 facilities were affected, of which 34 hospitals were completely left without medical devices. Indirectly, 46 hospitals were affected, but with difficulty [34]. The authors responsible for the attack took advantage of a security flaw in the Windows operating system called EternalBlue. Microsoft released the security patch almost two months before the WannaCry attack, but organizations did not update systems [35].

Major manufacturers of interventional and diagnostic radiological equipment, BD (Becton, Dickinson and Company) and Siemens have issued recommendations to users of their equipment and patches. Siemens provided guidance for 6 groups of its products which included CT and MRI machines [36]. One of the devices affected was Bayer contrast injector (Figure 12), which is used in radiology [37].

Despite its global spread, WannaCry has been slowed down by accident. Within its code, a link to a website was found. The malware only spreads if it could not connect to the specified URL. With the purchase of the domain, the "kill-switch" was activated. This did not stop the malware on devices where were already installed [38].

Conti Ransomware

The Conti Group is one of the largest and most active cybercriminal groups. Their first versions of *malware* appeared in early 2020. In 2021, the Irish health system had to temporarily shut down network due to the Conti attack. This caused problems for the entire healthcare infrastructure. Conti admitted that he had access to the network for



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

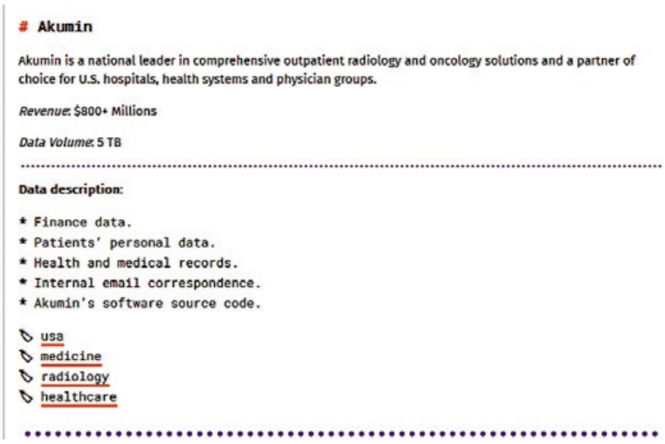
Figure 12. Screenshot from the affected Bayer injector (left), screenshot of the message itself on another device (right)
Source: https://www.forbes.com/sites/thomasbrewster/2017/08/03/wannacry-hackers-use-shapeshift-to-launder-bitcoin/?sh=220060323d0d
https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation

2 weeks, in which they downloaded 700 GB of data and demanded almost $20 million for ransom [39].

In a report published in the Irish Medical Journal entitled “The Impact of the Cyberattack on Radiology Systems in Ireland”, they state that for security reasons they turned off the national medical imaging storage system after the attack, which affected the availability of radiology services nationwide. Radiological examinations were taken on the devices themselves and all communication was done via personal phones. Recovery from the damage cost about 100 million euros, while legal costs were not disclosed. About 113,000 private data of patients and employees were stolen (56.57).

BianLian Ransomware

BianLian is a *ransomware* criminal *cyber* group that has been targeting critical infrastructures of the U.S. organization since 2022. The group gained access to the victims network through remote computer management. They demanded financial compensation by extortion, threatening to publish the data if not paid [40].



Akumin

Akumin is a national leader in comprehensive outpatient radiology and oncology solutions and a partner of choice for U.S. hospitals, health systems and physician groups.

Revenue: $800+ Millions

Data Volume: 5 TB

Data description:

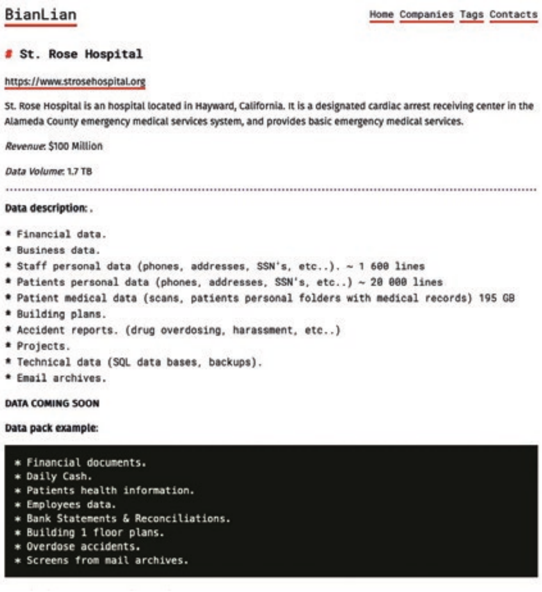
* Finance data.
* Patients' personal data.
* Health and medical records.
* Internal email correspondence.
* Akumin's software source code.

Figure 13. Publication of the BianLian Group on their website where they showed the quantity and what data they downloaded
Source: https://twitter.com/H4ckManac/status/1731992794137338295

In September 2023. BianLian attacked Akumin, Florida’s second-largest health care company that provides radiology and oncology health services to about 1,000 hospitals in 48 U.S. states. The first signs of the attack appeared on 11.10.2023 and preventively shut down radiology centers in 50 places. According to the investigation, the attackers were able to gain access to servers with the personal data of patients [41].

They collected about 5 TB of medical records, imaging data of diagnostic procedures and copies of passports (Figure 13).

At the beginning of December, they were attacked again by the same *cyber* group [42]. This time, the data was not encrypted, but only downloaded, and the attack caused a 2-week interruption in the work of the Department of Nuclear Medicine and Diagnostic Radiology [43].



St. Rose Hospital

https://www.strosehospital.org

St. Rose Hospital is an hospital located in Hayward, California. It is a designated cardiac arrest receiving center in the Alameda County emergency medical services system, and provides basic emergency medical services.

Revenue: $100 Million

Data Volume: 1.7 TB

Data description: .

* Financial data.
* Business data.
* Staff personal data (phones, addresses, SSN's, etc..). ~ 1 600 lines
* Patients personal data (phones, addresses, SSN's, etc..) ~ 20 000 lines
* Patient medical data (scans, patients personal folders with medical records) 195 GB
* Building plans.
* Accident reports. (drug overdosing, harassment, etc..)
* Projects.
* Technical data (SQL data bases, backups).
* Email archives.

DATA COMING SOON

Data pack example:

```
* Financial documents.
* Daily Cash.
* Patients health information.
* Employees data.
* Bank Statements & Reconciliations.
* Building 1 floor plans.
* Overdose accidents.
* Screens from mail archives.
```

Figure 14. BrianLian’s Statement on Her Attack on St. Rose Hospital
Source: https://thecyberexpress.com/bianlian-ransomware-st-rose-hospital-as-victim/

St. Rose Hospital in California was also the victim of the attack. According to their own claims, they had access to 1.7 TB of data to staff and patients. (Figure 14).

They downloaded 195 GB of data and claimed that they would publish it publicly [44].

Conclusion

Cyber-attacks on radiological systems are not receiving proper attention, which can be seen from the availability of literature and articles. A large number of papers were created after an attack, and the authors documented and analyzed cases after the damage had already been done. This leads to the conclusion that it is not interesting until it becomes a problem and it is too late. Worldwide there are more and more examples of financial allocations for the recovery of the system, payments of ransoms and compensation to patients who did not receive the required radiological diagnostic test on time or whose medical data became public. It is important that every employee of the radiology department is familiar with the basics of cyber security. That means recognizing the symptoms of malware and learning protocols for defense. It is the responsibility of IT service to update all computer systems on time, and the authorized healthcare manufactures their devices.

When the radiology department stops working, it has a devastating impact on the entire hospital system, from emergency admission to postponement of surgeries and other treatments. By paying more attention to attacks on radiological systems and cyber security in radiology, we can prevent or at least reduce their impact on the operation of health systems, show care and prevent harm to patients.

Cyber napadi na radiološke sustave

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

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. 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.
5. 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
6. 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/
7. 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
8. Wireshark [Internet]. Wireshark; 2024. Wireshark – display filter reference: Index. [pristupljeno 04.04.2024.] Dostupno na: https://www.wireshark.org/docs/dfref//
9. 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.
10. 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
11. 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
12. 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.
13. 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.
14. 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.
15. 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
16. 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
17. Encyclopædia britannica [Internet]. Chicago (IL): Encyclopædia Britannica Inc. Encyclopedia Britannica. 2024 Cryptography Dostupno na: https://www.britannica.com/topic/cryptography

18. Cho, A. (2014). Quantum spy games. Science, 343, 482–283. DOI: https://doi.org/10.1126/science.343.6170.482
19. 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).
20. 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.
21. 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.
22. 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.
23. 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
24. 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..
25. 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
26. 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
27. 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.
28. 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
29. Kiguolis L. Kwampirs malware Removal Guide. 2SPYWARE [Internet]. 2017 [pristupljeno 05.04.2024.] Dostupno na: https://www.2-spyware.com/remove-kwampirs-malware.html
30. 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
31. 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
32. 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
33. 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/
34. 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
35. 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
36. 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
37. 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
38. 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
39. 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/
40. 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
41. 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/
42. 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/
43. 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/
44. 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/