athena dynamics

DICOM: A Ticking Cybersecurity Time-Bomb In The Healthcare Industry

Author: Nyan Tun Zaw, CISSP, CISO & Regional Senior Vice President for Business Development at Athena Dynamics
Advisory Editor: Ken Soh, Group CIO, BH Global and CEO, Athena Dynamics
Copyright © Nov 2017 All Rights Reserved Athena Dynamics Pte Ltd

---

Current Cyber Security Landscapes in Healthcare Industry

WannaCry. NotPetya. In the past few years, all these malware names became familiar not just to security professionals but also to the public due to their alarmingly fast proliferation, high destructive power and extensive media coverage. Recently, in May 2017, a massive WannaCry ransomware outbreak has shut down 16 hospitals across the UK, freezing systems and encrypting extremely critical information such as patient records, which means that a huge amount of clinical and surgery appointments were cancelled since the doctors cannot access even the most basic patient medical records. 1 Imagine there is a patient urgently needing a surgery but the doctors could not proceed or delay in saving this patient's life just because all the previous medical records of the patient were encrypted by the ransomware and not accessible. The result would be devastating.

DICOM: A Ticking Time Bomb

In healthcare institutions, one of the most common file types being shared around is DICOM file. DICOM is a very specialized file format created about 24 years ago specifically for the healthcare industry. It holds all the sensitive information about a patient name, age, ID, date of birth, weight, etc., attached to the relevant medical images such as X-Ray, CT Scan, MRI etc, which helps the doctors in doing the diagnosis efficiently via digital conduits and devices. However, due to the amount of data it needs to contain, the structure of a DICOM file is vaguely similar to that of an archive file where it is essentially a container holding multiple files inside.

What makes it most alarming is that DICOM today has been deployed globally as the mainstream conduits for storage of digital medical images in most hospitals and healthcare establishments. Due to the highly specialized purpose of this file format, such vulnerability is not in the consideration of mainstream cyber protection tools.

The current state of affair poses a serious security concern because malicious software like ransomware can effortlessly be transported via DICOM file by disguising as a legitimate digital object. Healthcare institutions typically use portable media devices such as USB flash drives or DVDs to transfer and share the DICOM files. The problem is, in most cases, these innocent-looking portable media devices, which were brought over by the patients themselves, can be the main source of a ransomware outbreak.

A Scenario Based Attack via DICOM

Imagine this scenario. A patient did an MRI scan overseas and this overseas hospital gave him the MRI scan files in a DICOM format using a DVD disc. What he did not know was that this overseas hospital's network had been infected and there is a ransomware spreading around, even in the DICOM file inside the DVD they gave him.

Now he is back to his own country and decided to do a follow up with a local doctor so he passed the DVD to him. The unsuspecting local doctor just inserts the DVD inside his computer, opens up the file, and malicious attack could then find its way in. The ransomware inside the DICOM file infects the doctor's computer first, from which it continues to infect the hospital's Picture Archiving and Communication System (PACS). Once the ransomware is inside the PACS system, it is just a matter of time before it proliferates to the whole hospital network and encrypting everything, essentially bringing down the entire system, shutting down all the operations and compromising the sensitive patient information.

The proliferated impact of DICOM infection would potentially be much more devastating than what ransomware has done to the healthcare sector thus far. This is because such vulnerability is relatively unknown, and the impact would not just affect the IT systems, but also the OT (Operational Technology) platforms such as the PACS and other related medical devices. The degree of damages could hence be the health and life of patients in the hospital.

The Traditional Measures Are Not Longer Effective

To be fair, as a security feature, DICOM files are typically encrypted and hashed but it is usually not enough to protect from the attacker attaching a hidden malware to a legitimate DICOM image file or a DICOM viewer application, which is triggered when the doctor opens up to see the medical images. Certainly, comparing the hash of the original DICOM file against the hash of the DICOM file the doctor received will expose any tampering done to the file. However, there are three main problems with this approach:

1. It is tedious and counter-productive to compare the hashes of every single image files with the original hashes before opening the file
2. Even if this hash-comparing process is done automatically with the help of an application or script, there is still a good chance that the original hash might be tampered even before going through this process if the computers connected to the MRI or X-ray scan machines already have some backdoors

3. Most importantly, after comparing the hashes, what happens next if it is different from the original? The doctor may ask the patient to get a legitimate copy again and come back since it can be potentially life-threatening if the patient's X-ray images or MRI images in the DICOM file are tampered and the diagnosis went wrong. However, what if it is a critical patient who needs the medical attention right away based on these X-ray images in the DICOM file?

Hence, the main objective here should NOT be based on finding out what is wrong with the file, but rather, on making sure that whatever DICOM files the doctors receive are clean and legitimate so that they can stop worrying about whether they will bring down the whole hospital system and instead, focus on the more important thing: saving lives.

The Challenge Today Facing DICOM

Now the next challenge here is how can we make sure that these DICOM files are clean? Traditionally, the common belief is that we can just scan them using detection tools such as anti-virus or sand-boxes. While it is true that using detection-based tools can give protection to a certain extent, the main underlying issue lies in the fact that "detecting nothing malicious" does not mean that it is safe, in consideration of today's advanced cyber threat landscapes. Detection tools, whether it is signature or non-signature based, work on the same principle to employ the most advanced technology to detect the "bad guy" in a bid to remove them. Unfortunately, while this may work a couple of years ago, it is no longer effective today. This is because advanced threats are not straightforwardly detectable in the first place. With literally hundreds and thousands of new advanced malwares being developed everyday by highly-funded cyber criminals around the world, it is simply impractical and impossible to detect them. This means that applications are bound to miss out on certain new threats every now and then. If that is the case, how can we make sure that all the files are 100% clean?

The Solution with CDR/CDNR Non-Detection Centric Strategy

In view of the challenges mentioned, we need to move on to a non-detection centric technology named "CDNR". It is an acronym for Content Deconstruction Neutralization and Reconstruction, also commonly known as CDR (Content Disarm and Reconstruction) in the security industry. CDNR is a nondetection based file-cleansing technique where every file is deconstructed and stripped down to the bare minimum components, neutralized or sanitized using a different number of algorithms and techniques and then usually reconstructed back to the original file format, without affecting much on the original legitimate contents. A good CDNR solution can rebuild the file so perfectly that it is barely noticeable to the users.
Sanitizing a DICOM file with CDNR technique would mean that even if there is any malicious content or ransomware hidden inside the DICOM file, all these components will be wiped out and only the sanitized content will reach the user. However, the sanitization and rebuilding process in CDNR needs to be done very precisely in a smart and delicate way because these DICOM image files are naturally much more sensitive to changes than a normal image file

since a slight change in the image content can result in a drastically wrong diagnosis.

Conclusion: Military Grade CDR/CDNR for DICOM Protection

In summary, as much as being an extremely useful file type for healthcare industry, the world has come to a juncture that DICOM is a file type that needs to be handled with extreme care. The file can literally be a trojan horse for malwares and viruses to compromise the healthcare sector. Since healthcare is one of the most sensitive industries where the patients' lives are at risk, hospitals and clinics would need to step up their cybersecurity game and go extra miles to make sure that they are always protected and safe.

One last word of caution is that, while CDR/CDNR is a fast-emerging technology that comes to notice by the industry only recently, it is important to source for one has strong track records in protection of state-level critical info infra-structures. This is in view that there are many tools that claimed to have CDR/CDNR technologies but they are probably just a recent development with very thin layer of actual CDR/CDNR operations. The healthcare sector needs a military grade CDR/CDNR technology to protect its files, especially the DICOM file which could affect patient's health and lives directly.

Source: https://athenadynamics.com/event/dicom-unknown-vulnerability-cyber-attacks-global-healthcare-industry/

Disclaimer: The outcome of general best practices introduced in this material may vary due to environmental and contextual parameters. Neither BH Global Corporation Ltd, Athena Dynamics Pte Ltd nor the writers are responsible for any direct or indirect implications/impacts to the readers due to the adoption of these practices.

Not for Distribution. No part of this presentation materials may be distributed/reproduced without the writers' expressed consent.