Hospitals Are Vulnerable to Ransomware Attacks

For
José R. Sánchez
President & CEO
Norwegian American Hospital
Formal Analytical & Unsolicited Recommendation Report

By

Eonshik Kim

December 18, 2017

Executive Summary

I. *Problem*

Hospitals are a popular target to Ransomware attacks from hackers. However, the hospitals are vulnerable to those attacks.

II. *Possible Solutions*

- install the software that blocks the advertisement on the internet.
- Buy an anti-virus software.
- Upgrade the operating system.

III. *Criteria for Evaluating solutions*

- Feasibility
- Cost
- Time required to implement solution
- Potential to resolve the problem(Sustainability)

IV. *Final Recommendation*

I would recommend considering an upgrade the operating system and install the software that blocks the advertisement on the internet to reduce the possibility of Ransomware attacks.

Introduction

What is Ransomware?

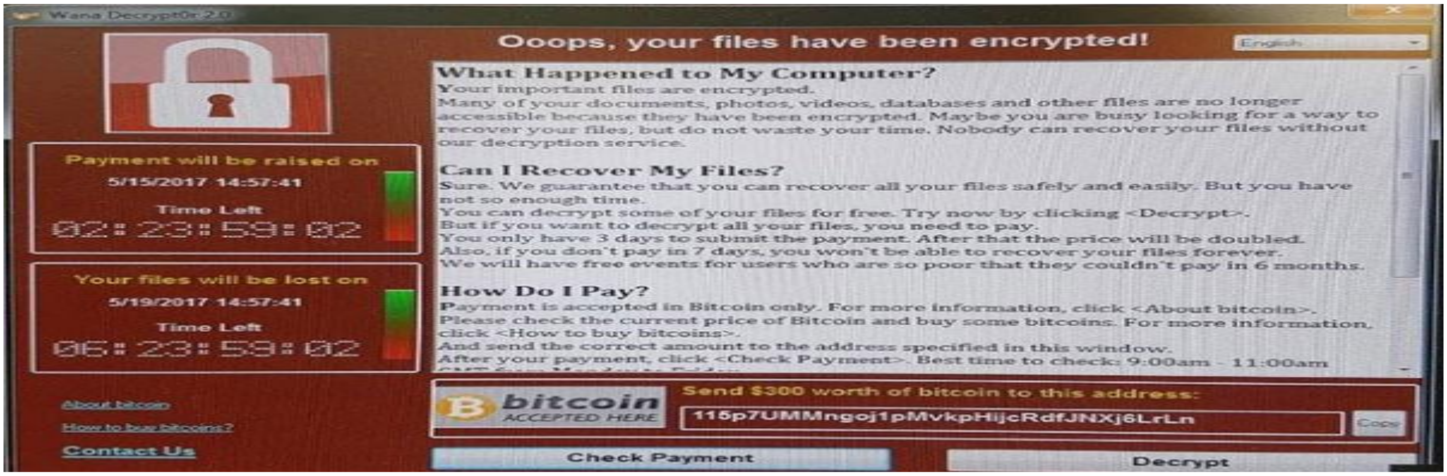
According to Zetter Kim, Ransomware is malware (malicious software) that locks your keyboard or computer to prevent you from accessing your data until you pay a ransom, usually demanded in Bitcoin (digital currency). It is an acronym which is combined ransom and software. Another meaning is to take hold of your data until you pay money. It is also difficult to track hackers since they use Bitcoin.

Why is Ransomware dangerous?

Unlike other malware, Ransomware is more powerful. Usual malware could infect your computer when you download suspicious software. Ransomware could infect your computer not only from malicious software but also from the network. Therefore, it means that even the user doesn’t have to download anything. There is still a possibility to infect the computer.

“Wanna cry” Ransomware attack on May 12, 2017

Most people are aware of that it is dangerous to download suspicious software from the internet. However, they are not many aware that Ransomware could infect from the network system. There are lots of different kinds of Ransomware. “Wanna cry” is one of Ransomware. However, it can massively damage all the computers around the world. According to Tyler Durden, the Wanna Cry attack in 2017 was the worst-ever recorded Ransomware attack. It struck over 57,000 users worldwide. Hackers hacked the powerful hacking tool from NSA and modified it to their own version.



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 14:57:41
Time Left
02:23:59:02

Your files will be lost on
5/19/2017 14:57:41
Time Left
06:23:59:02

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

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

The users who were infected with this attack got the message pop up message like above picture when they turned on their computers. The message said: “your important files are encrypted, so you have to pay to recover your files by bitcoin and the price will go up on and on every hour”. Lots of people got panicked when they saw this message and they ended up paying their money. According to Durden, the infections were reported in the UK, US, China, Russia, Spain, Italy, Vietnam, Taiwan, and others. This attack infected over nine million computers in nearly 200 countries. This attack was aimed at the weak spots of security from outdated operating systems.

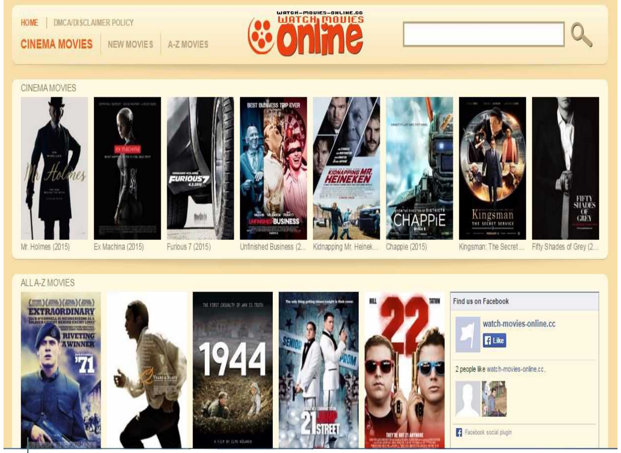
Why are hospitals so vulnerable to Ransomware attack?

Hospitals were one of the popular targets since the most operating systems in the hospital are outdated. “The National Audit Office (NAO) said that 19,500 medical appointments were canceled, computers at 600 GP surgeries were locked and five hospitals had to divert ambulances elsewhere. According to Selena Larson, many people don't realize that healthcare hardware -- like MRI machines, ventilators, and some types of microscopes -- are actually computers. If those systems are down, it directly affects the health of patients. Especially, the patients who are in critical states might die because of Ransomware attacks. Also, the registration system is a computer too. Most workers in the hospital don’t have enough education for cybersecurity. If the workers realize that their registration systems are down. Then, they would get embarrassed and they might end up paying money for hackers.

Data Section

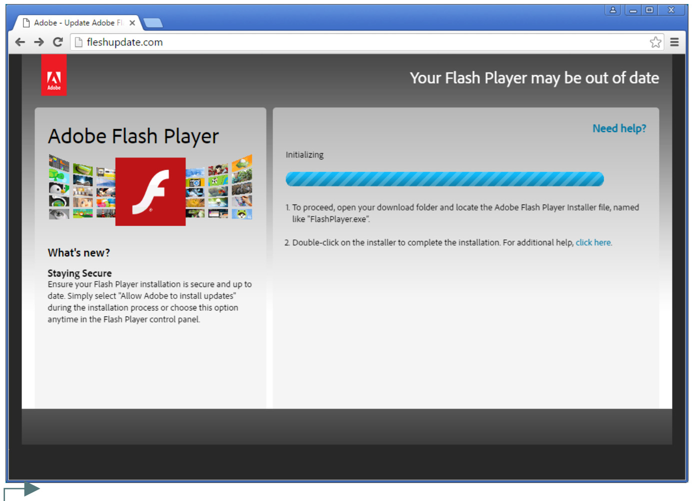
Process of Ransomware attacks

There are lots of processes to Ransomware attacks since there are numerous kinds of Ransomware. This is one of the popular process that Ransomware might infect the user's computer with.



1. The user accesses an untrustworthy website like free movie streaming sites.

2. The user is redirected to a fake Adobe Flash website, and the website forces to download a player.



Your Flash Player may be out of date

Adobe Flash Player

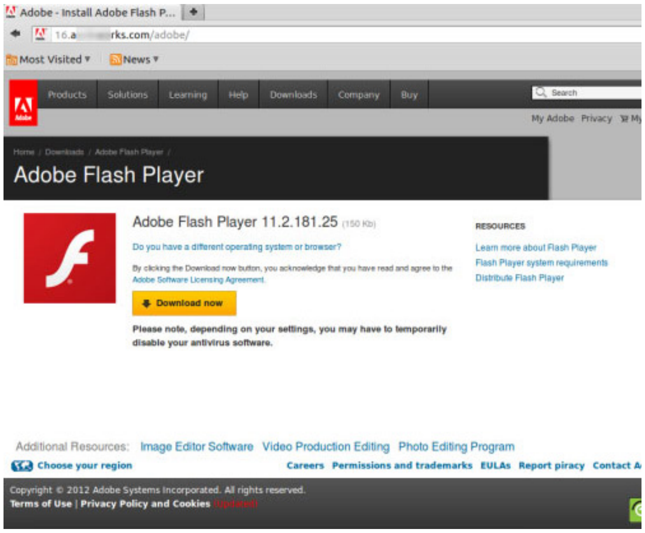
What's new?

Staying Secure
Ensure your Flash Player installation is secure and up to date. Simply select "Allow Adobe to install updates" during the installation process or choose this option anytime in the Flash Player control panel.

Need help?

Initializing

1. To proceed, open your download folder and locate the Adobe Flash Player Installer file, named like "FlashPlayer.exe".
2. Double-click on the installer to complete the installation. For additional help, click here.



Adobe Flash Player

Adobe Flash Player 11.2.181.25 (150 Kb)

Do you have a different operating system or browser?

By clicking the Download now button, you acknowledge that you have read and agree to the Adobe Software Licensing Agreement.

Please note, depending on your settings, you may have to temporarily disable your antivirus software.

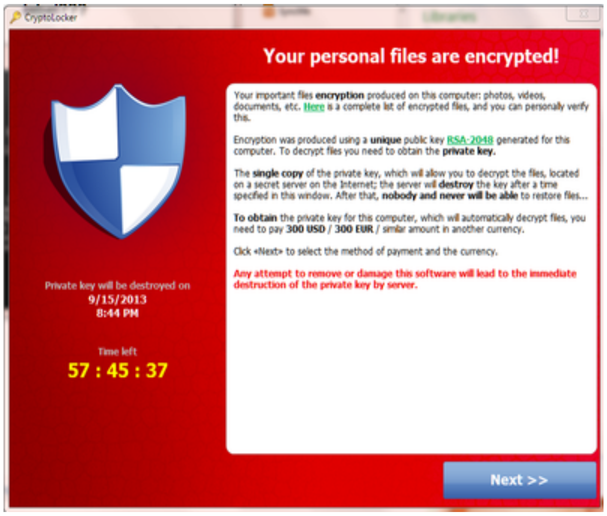
RESOURCES
Learn more about Flash Player
Flash Player system requirements
Distribute Flash Player

Additional Resources: Image Editor Software Video Production Editing Photo Editing Program

Careers Permissions and trademarks EULAs Report piracy Contact A

Copyright © 2012 Adobe Systems Incorporated. All rights reserved.
Terms of Use | Privacy Policy and Cookies (Updated)

3. The user prompts to download the fake Adobe Flash Player.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/15/2013
8:44 PM

Time left
57 : 45 : 37

4. Ransomware program runs as soon as the download is completed.

Possible Solutions

There are some possible solutions that might reduce Ransomware attacks: install the software that blocks the advertisement on the internet, buy an anti-virus software, and upgrade the operating system.

First Solution: install the software that blocks the advertisement on the internet.

Most Ransomware is infected from downloading malicious software from suspicious websites. Users can add an extension on their internet that can prevent 90% of advertisements. One of popular extension is called “Ad-Block”.

- Feasibility

Feasibility of this solution is high because it doesn’t require complex steps or expert knowledge to install ad-block extensions.

- Cost

Most ad-block extensions are free.

- Time required to implement solution

The extensions usually have small storages, it doesn’t take much time to install it. It approximately takes 5 minutes per computer.

- Potential to resolve the problem(Sustainability)

Sustainability is low. Blocking advertisement can’t completely reduce the Ransomware attacks because Ransomware also could infect a computer by the network system.

Second Solution: buy an anti-virus software

Buying an anti-virus software is a good solution to reduce Ransomware attacks. However, it’s important to buy the anti-virus software that has a function: Ransomware removal tool, and network monitoring tool.

- Feasibility

Feasibility of this solution is medium because this solution requires employees to know how to scan the virus.

- Cost

There is some cheap anti-virus software. However, they might not have functions for network monitoring and network monitoring tools. For those functions to require buying over $30 software. In addition, the software requires you pay every year.

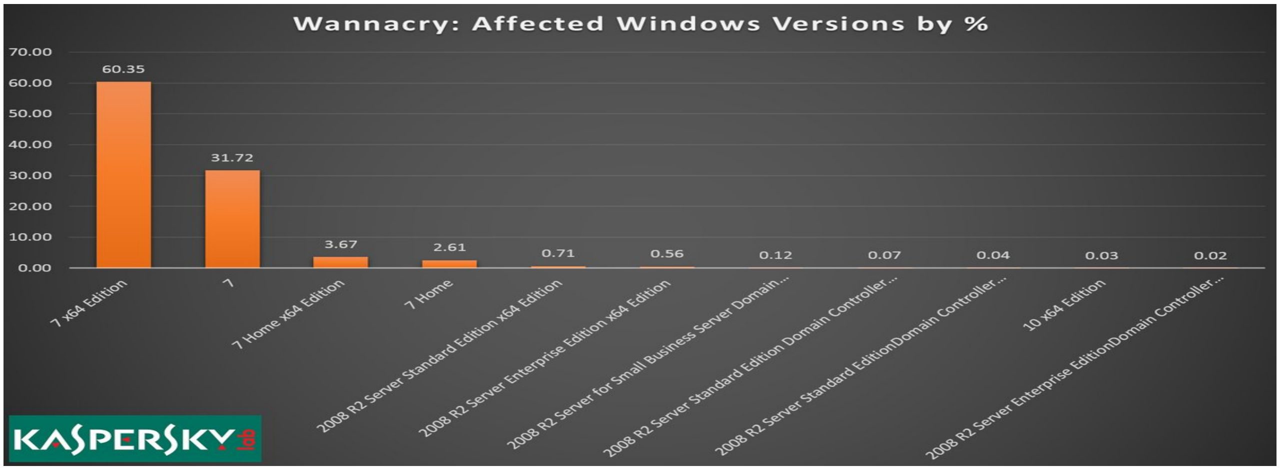
- Time required to implement solution

It would take a pretty long time to scan all computers. Anticipated time would be about a week.

- Potential to resolve the problem(Sustainability)

Sustainability is medium. Some outdated system might still be vulnerable even though anti-virus software is installed.

***Last solution:** upgrade operating system*



According to Kaspersky Lab, most victims of "Wanna Cry" attack were from window 7 which is the outdated operating system. In contrast, window 10 which is the latest operating system has only 0.03% victims. This chart shows how important it is to upgrade your operating system to the newest version.

- Feasibility

Feasibility of this solution is medium because this solution requires the employees to know how to upgrade their outdated operating systems.

- Cost

If I assume that the hospitals have Window 7 system. It would cost $119 to upgrade to window 10 for each computer.

- Time required to implement solution

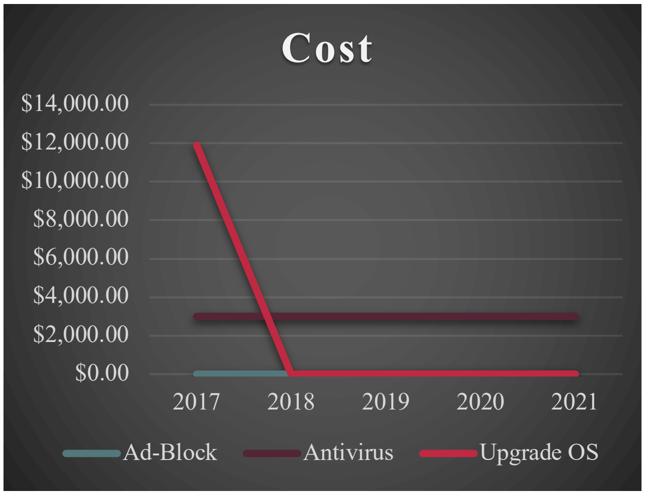
It would take a long time to upgrade all computers. Anticipated time would be about a month.

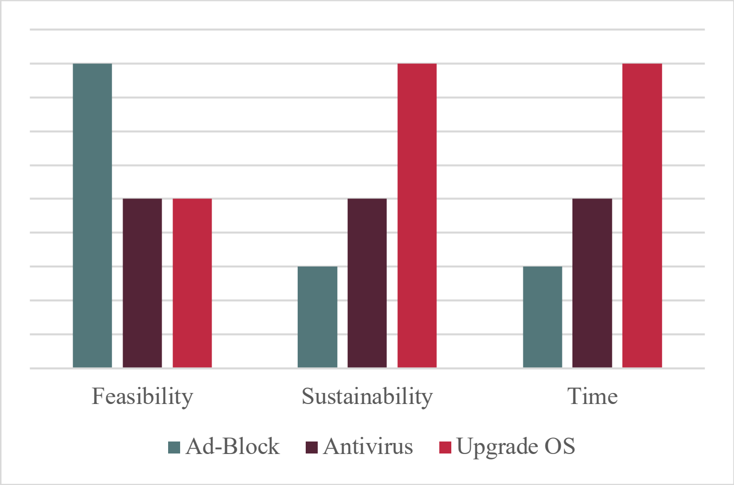
- Potential to resolve the problem(Sustainability)

Sustainability is high because window 10 has a more powerful security system than another numbering. Also, Microsoft offers a free security update to prevent Ransomware attacks.

Comparison charts

Assuming that the hospitals have 100 computers.





Potential cost to buy an antivirus: $15,000

Potential cost to upgrade operating system: $11,900

Feasibility: Ad-Block(high) > Antivirus(Medium) = Upgrade OS (Medium)

Sustainability: Upgrade OS(High) > Buying an antivirus(Medium) >Ad-block(Low)

Time: Ad-Block (One day) > Antivirus (1 week) > Upgrade OS (1 month)

Conclusion

I suggest 3 possible solutions to reduce Ransomware attacks for hospitals: install the software that blocks the advertisement on the internet, buy an anti-virus software, and upgrade the operating system. From the comparison, the potential cost of buying antivirus is higher than upgrade operating system of computers. Also, sustainability of upgrading operation system is higher than buying antivirus. Therefore, it’s more effective to choose solution 3 than solution 2. This solution would be most beneficial to hospitals because it reduces the cost of damage from Ransomware attacks.

Final Recommendation

I would recommend considering an upgrade the operating system and install the software that blocks the advertisement on the internet to reduce the possibility of Ransomware attacks.

Works cited

Cimpanu, Catalin. “Over 98% of All WannaCry Victims Were Using Windows 7.” BleepingComputer, BleepingComputer.com, 20 May 2017, www.bleepingcomputer.com/news/security/over-98-percent-of-all-wannacry-victims-were-using-windows-7/.

Cimpanu, Catalin. “Shoddy Ransomware Destroys User's Files.” Softpedia, 13 Jan. 2016, news.softpedia.com/news/shoddy-ransomware-destroys-the-user-s-files-498889.shtml.

Durden, Tyler. “"Worst-Ever Recorded" Ransomware Attack Strikes Over 57,000 Users Worldwide, Using NSA-Leaked Tools.” ZeroHedge, 11 May 2017, www.zerohedge.com/news/2017-05-12/massive-ransomware-attack-goes-global-huge.

Larson, Selena. “Why hospitals are so vulnerable to ransomware attacks.” CNNMoney, Cable News Network, money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/index.html.Violet Blue. “Hospital ransomware: A chilling wake-up call.” Engadget, 14 July 2016, www.engadget.com/2016/02/19/hospital-ransomware-a-chilling-wake-up-call/

Zetter, Kim. “What Is Ransomware? A Guide to the Global Cyberattack's Scary Method.” Wired, Conde Nast, 2 June 2017, www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/.

Zetter, Kim. “Why Hospitals Are the Perfect Targets for Ransomware.” Wired, Conde Nast, 3 June 2017, www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.