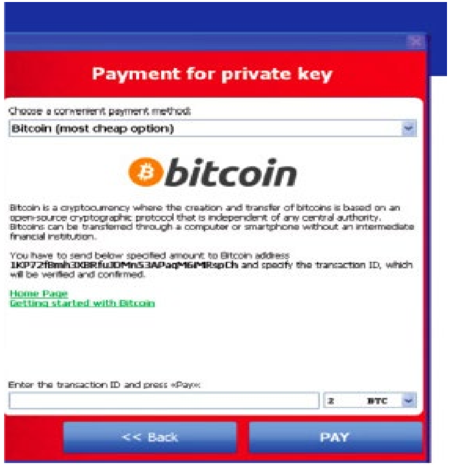
Ransomware and Hospitals

How criminals hijack records
(and what we can do about it)

Objectives

1. To bring BET technicians and managers up to speed on what is actually happening to hospitals and businesses worldwide
2. To give a breakdown on what a ransomware is, what it does, and how criminals are using it to make money.
3. To tell how cryptolockers are different from general ransomware. Describe viruses like WannaCry and their effects on medical equipment.
4. To give some common ways to prevent ransomware and cryptolockers from spreading.
5. To suggest a course of action and a plan to minimize risk by introducing a new risk assessment.



Payment for private key

Choose a convenient payment method:

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address **1KP72fBmh3XBRfuJDMn53APaqM6MRspCh** and specify the transaction ID, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

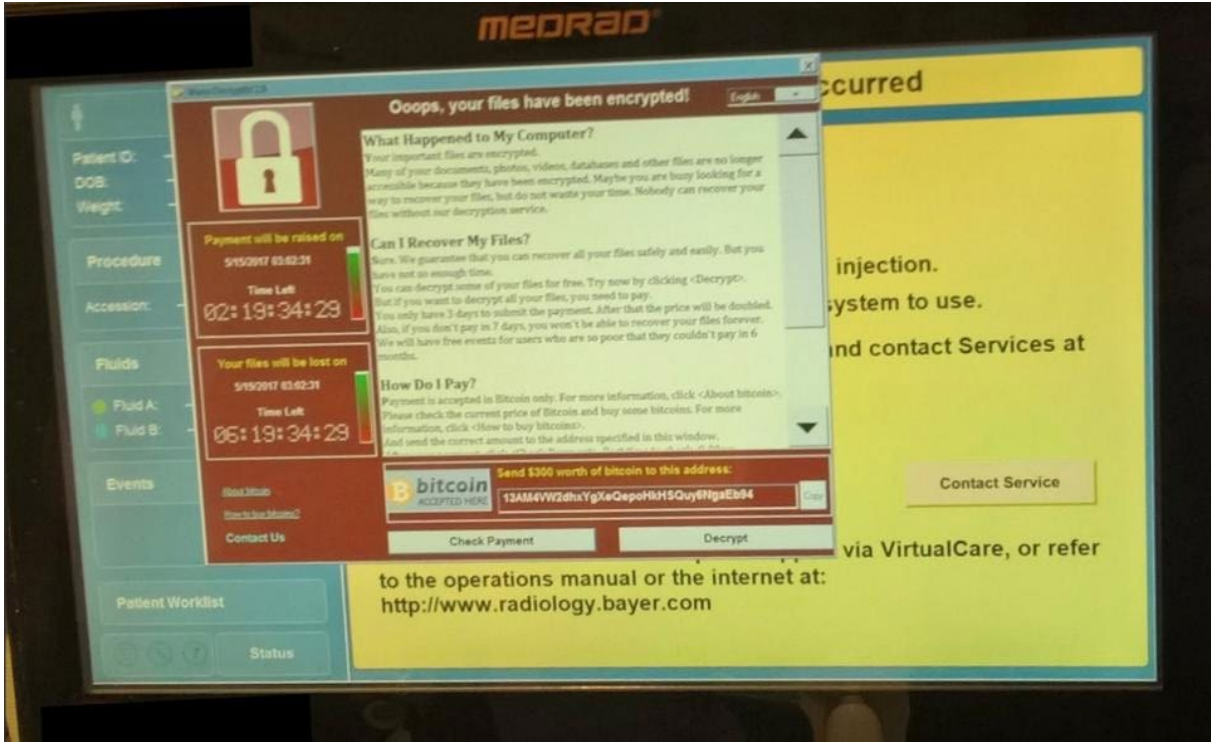
Enter the transaction ID and press «Pay»:

2 BTC

What is all the fuss about?

This is a recent article (5/17/17) from Forbes: [Wannacry ransomware hit real medical devices]

Bayer Medrad confirmed two reports from customers in the U.S. with devices hit by the ransomware. If a hospital's network is compromised, this may affect Windows-based medical devices connected to that network.



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 03:02:31
Time Left
02:19:34:29

Your files will be lost on
5/19/2017 03:02:31
Time Left
06:19:34:29

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.

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

ccurred

injection.

system to use.

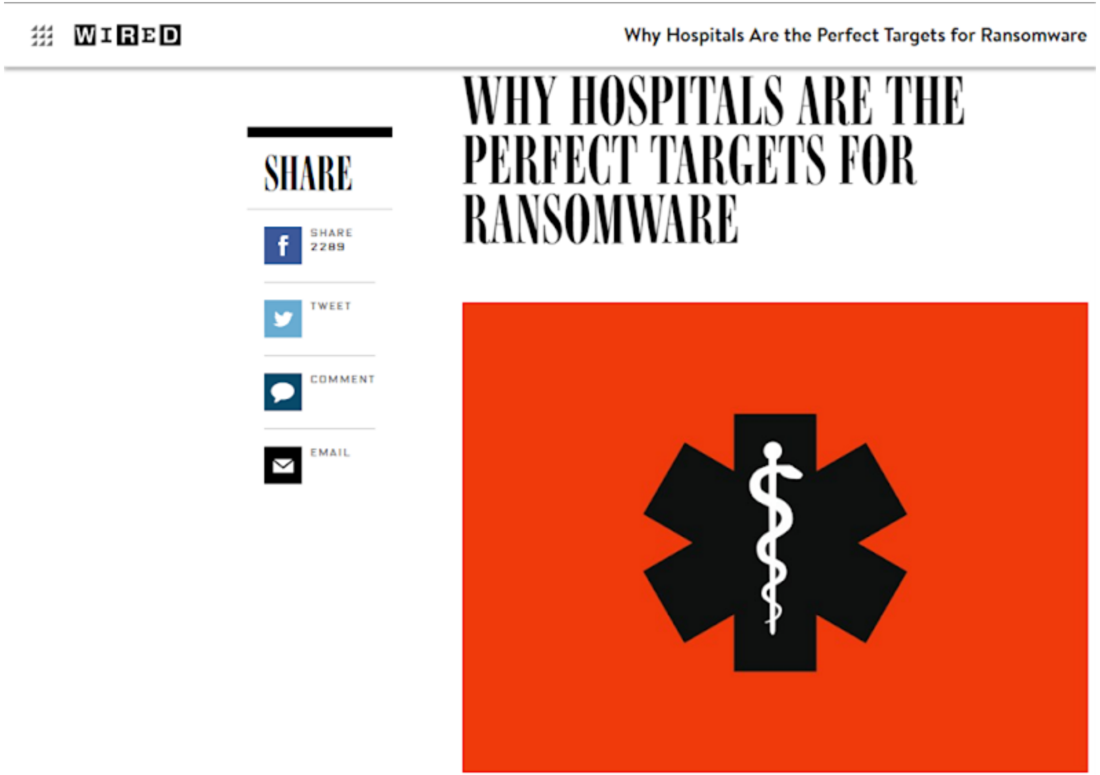
nd contact Services at

via VirtualCare, or refer to the operations manual or the internet at:
http://www.radiology.bayer.com

WIRED Magazine (magazine hackers may read)

One last article describing the possibilities of a cryptolocker. From WIRED magazine 3/30/16:

“The FBI estimated in 2014 that the extortionists behind the CryptoLocker strain of ransomware swindled some $27 million in just six months out of people whose data they took hostage.”

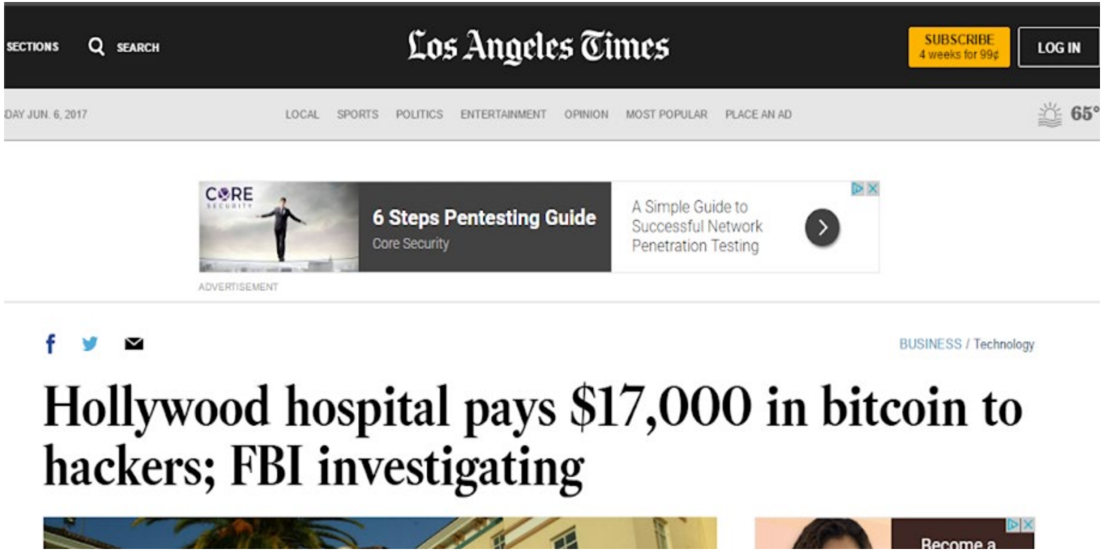


WIRED

Why Hospitals Are the Perfect Targets for Ransomware

WHY HOSPITALS ARE THE PERFECT TARGETS FOR RANSOMWARE

Here is a typical Ransomware attack:



Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

From the LA times (2/18/16) :

"Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin to a hacker who seized control of the hospital's computer systems and would give back access only when the money was paid, the hospital's chief executive said Wednesday."

Thankfully, this attack focused more on the operations computers than on medical devices or records.

What is ransomware?

A ransomware is any computer virus designed to prevent the user from accessing their data or computer system AND demanding money to restore the system to its previous operating state. These funds are usually exchanged in an internet currency called a bitcoin. It is untraceable.

There are usually 3 different types of ransomware:

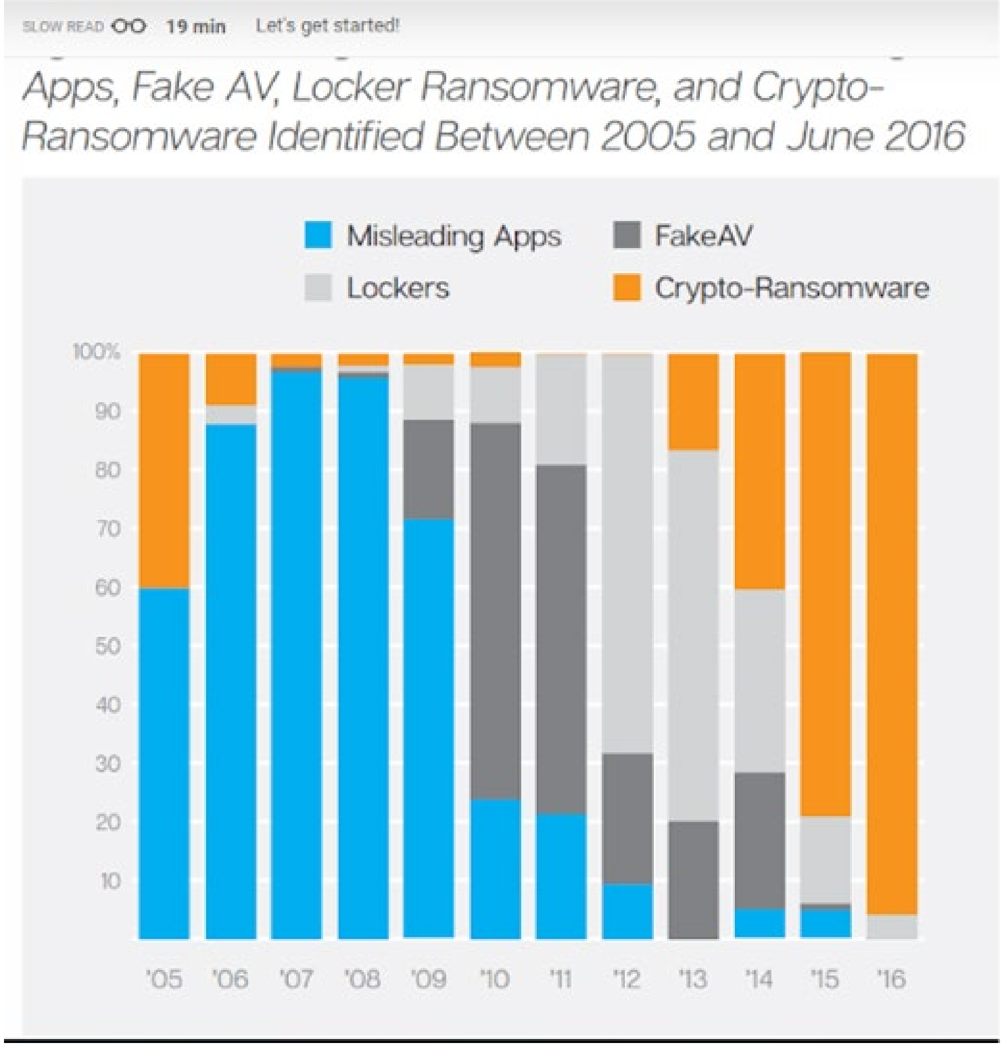
- Viruses that infect the Master Boot Record (MBR) and prevent system boot
- Viruses that allow boot, however lock the users out of their logins
- Viruses that encrypt specific files and leave the overall system running. CryptoLocker was an earlier virus that ran in 2004 and 2005.
    - These are the most popular and most dangerous.

The last type of attack acts more like a robbery the most recent is “WannaCry”

CryptoLocker style Ransomware is the currently trending attack

This shows the trend of attacks and how we are currently under a attack from CryptoLocker style attacks.

The most recent was the WannaCry virus

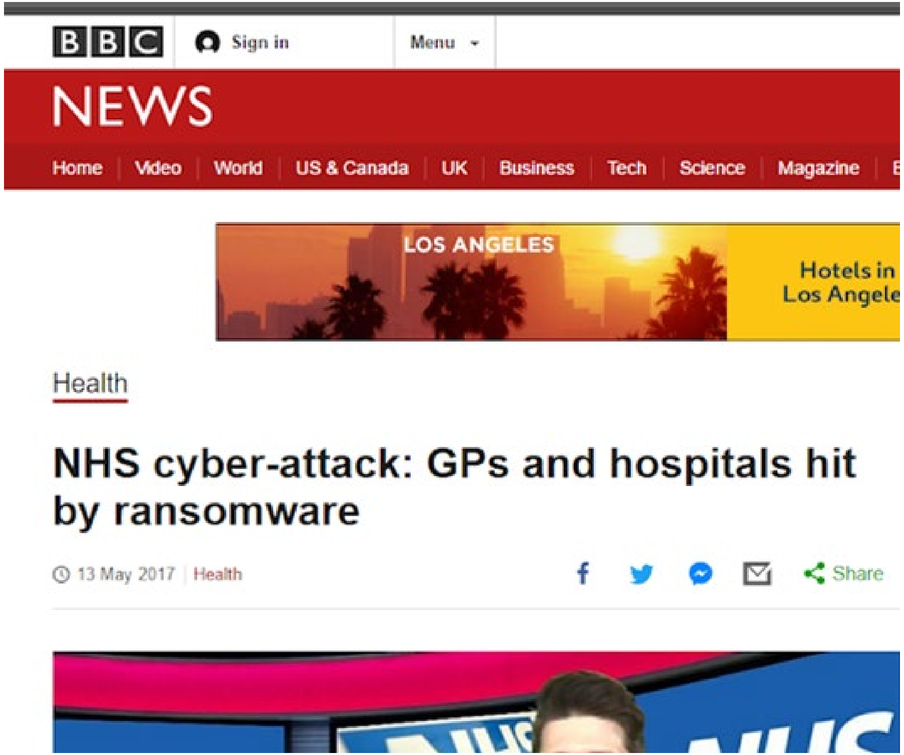


SLOW READ 19 min Let's get started!

Apps, Fake AV, Locker Ransomware, and Crypto-Ransomware Identified Between 2005 and June 2016

WannaCry attacked Hospitals in England.

From Wikipedia: “The [WannaCry] attack affected many National Health Service hospitals in England and Scotland, and up to 70,000 devices – including computers, MRI scanners, blood-storage refrigerators and theatre equipment – may have been affected. On 12 May [2017], some NHS services had to turn away non-critical emergencies, and some ambulances were diverted.”

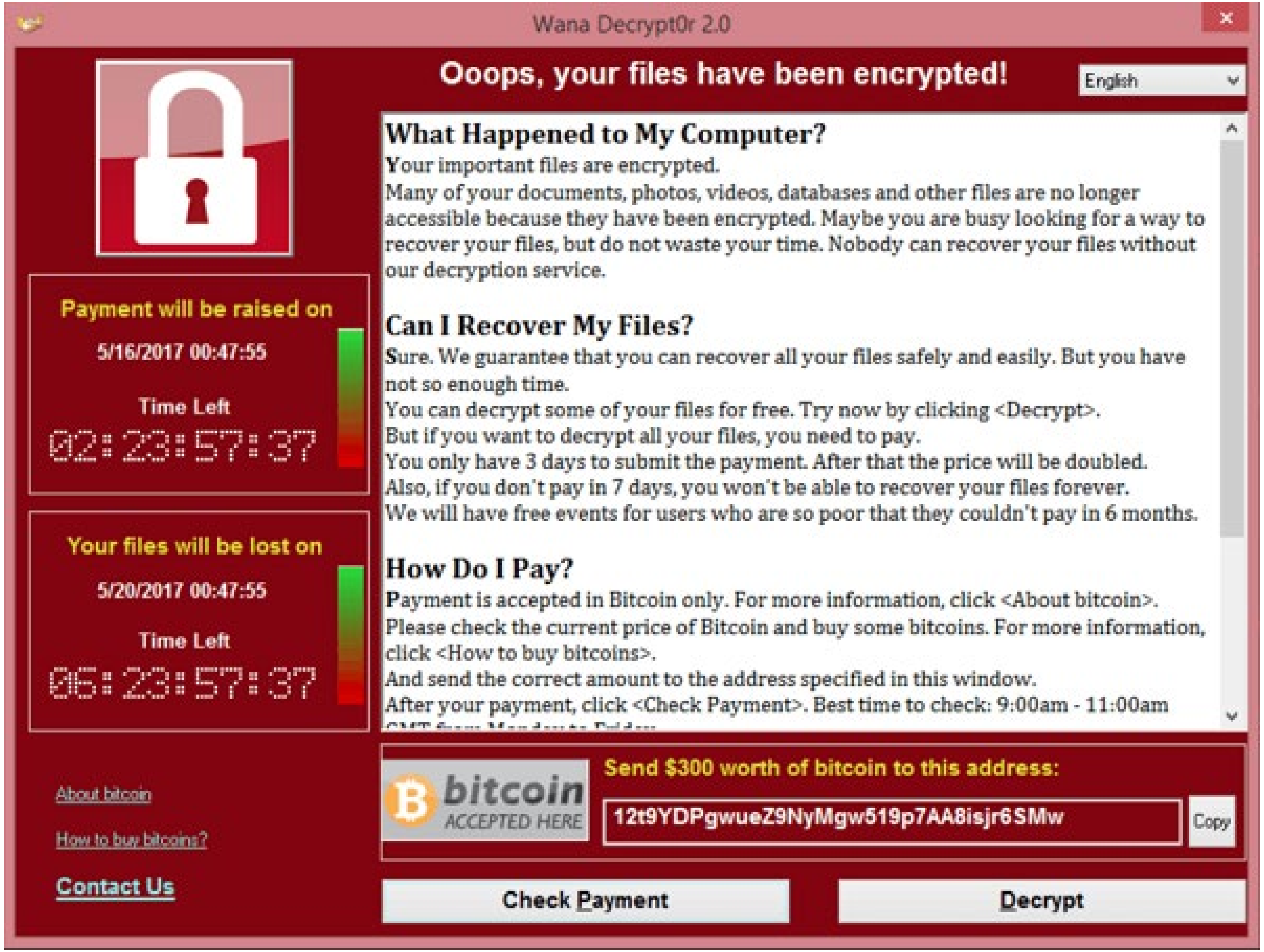


NHS cyber-attack: GPs and hospitals hit by ransomware

13 May 2017 | Health

WannaCry: the most recent ransomware

It is a CryptoLocker style virus that encrypts only data (non-system) files and demands payment to unlock the files. If you refuse to pay, it erases the files in 7 days.



Wana Decrypt0r 2.0

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.

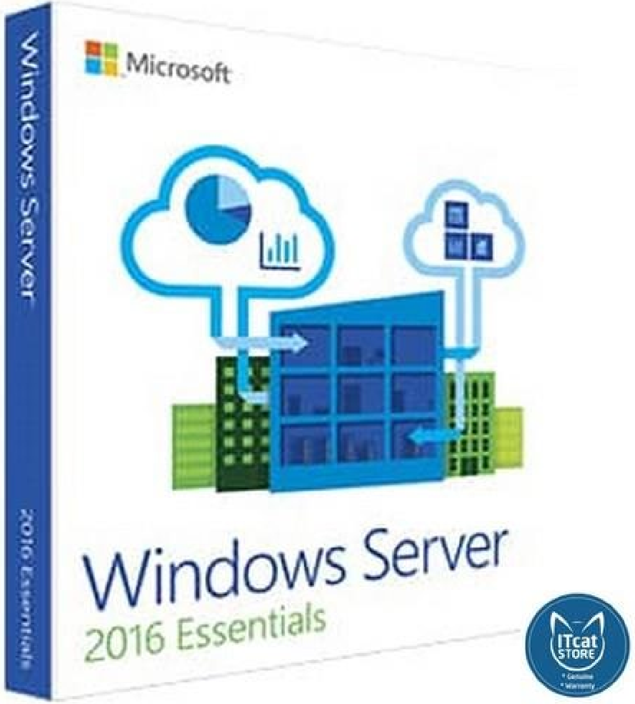
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

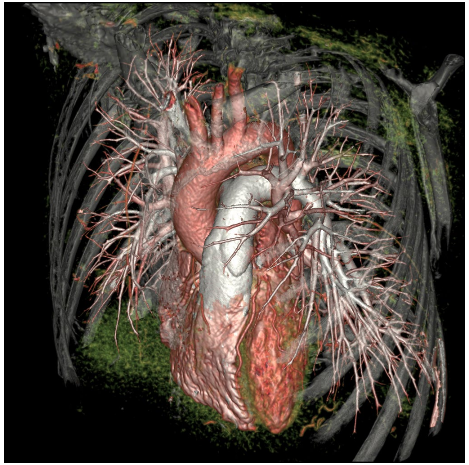
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

How WannaCry was spread

- Exploited a SMB protocol weakness - spread through open folders
    - This is the protocol used for WINS (Windows) , Appletalk, and Samba (Linux/ Android)
- Partially exploited a email phishing - unconfirmed
- People tried to “Share” a file with you, if you clicked on it, the virus used the click to get permission to install the WannaCry encryption.

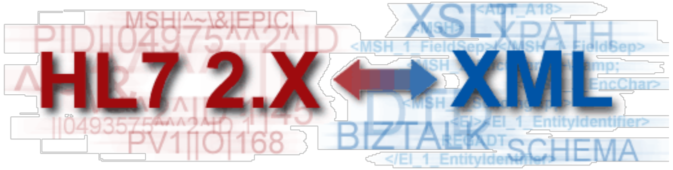


What does WannaCry encrypt?



It looks for and encrypts almost 190 different file types.

These files include: All of the Microsoft Office, Openoffice, and Adobe suite (.doc, .docx, .xls, .ppt, .txt ...), all pictures (.jpg, .gif, .tiff ...), All movies and audio files (.mp3, .mp4, .avi, .mov…), all database programs (SQL, XML, Access) , all compression file formats (.zip, .7zp, .rar …). **In short, everything personal.**



It charges a typical fee of $300 to decrypt the files.

We have gone from being held up on the street to being held up online.

How do we stop CryptoLockers (and other) attacks?

In short, get buy in from your support team. Remember to involve people

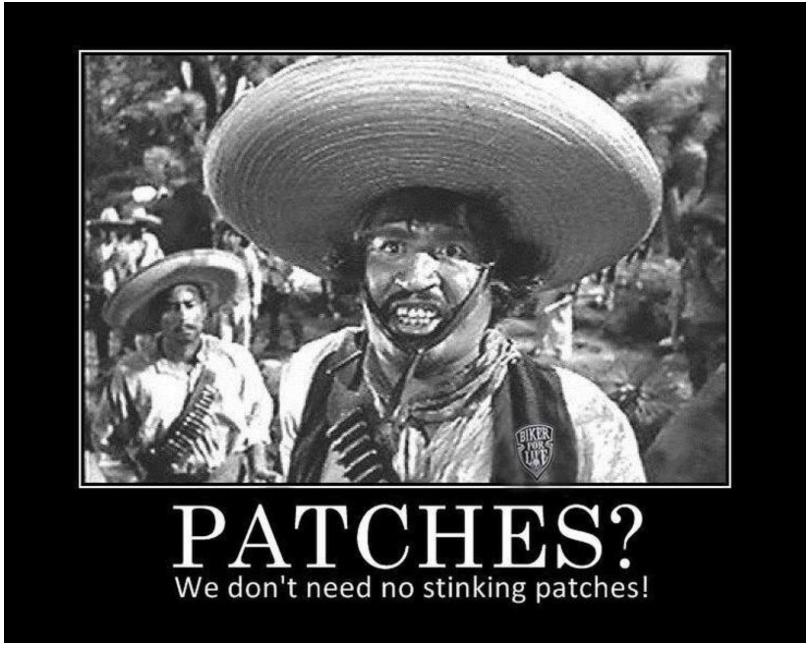
- Do not approach any solution without the OEM support.
  - If you patch it, you bought it. You assumed the liability. Check before installing.
  - Don’t be a cowboy doing your own thing.
- Involve Risk Management in decision making.
  - They can have more weight in Capital Equipment
- Ask IT for Help

What things should I ask the OEM for?

- Windows Updates - install OEM verified Windows Patches. Sandbox updates.
- Disable Flash, Choose / Limit Web page access.
- Get rid of Flash Drives and front accessed USB ports - limit access
- Logins - Use groups - Verify hardware locations - Track liabilities
- May require setting permissions on a folder . You may have to use GPO - Get them to help.
- Turn off simple file sharing unless required
- Limit OEM VPN access. Ask the “Hard questions” about remote access to IT
- Ask IT about the segmentation of the network
- Get involved with Cyber Security settings, the Risk Management, and Capital Equipment Purchases. Only buy things with security approaches built in. **Embedded vs bolt on security.**

OEM need to verify the Patches

- Work with OEM’s to verify what software revisions you have and what patches are the most up to date.
- Microsoft of course recommends “Automatic Update” Be careful with Auto Update.
    - They may cause the system to shut down
- Yes, we need these “Stinking Patches”
- If it’s not verified, it's a “do at your own risk” - you may face a “you break it, you bought it” - Use a system as a sandbox.



Flash, Java, ASP and other glaring security holes

- Java uses a user security permissions (set by their login) to access the entire system
  - It is not very secure - got out of date easily
  - Buttons can be programed to do nearly anything
- Disable if possible - ask the OEM
- FYI: Flash is going away in 2020

- Shockwave and Flash give similar system access.
  - This is so bad that modern browsers use HTMLv5.2 or better - Solution, update browsers

Again, the answer is updating - check with the OEM

- ASP is a Windows proprietary version of Java

Seriously, disable the front facing USB ports

- Stop people from bringing in Flash Drives that can be infected
- Stop people from plugging their smartphones (a linux computer) up to a medical device.
- Stop vendors from hooking up unknown devices to a system
- Verify vendors are protecting their FSE machines from infections
- Know what hardware is connecting to your medical device. (I know this is time consuming, so is a crash.) Dodge the HIPAA fine!

Track sensitive hardware and operating systems

Tablets and Laptops can have VPN access.

Lost and stolen hardware accounts for up to 15% of breaches. Bring awareness to this.

More important - Know which machine is using what Operating systems - Know where your vulnerabilities are. NT, Xp, Vista, 7 or 8 ?

Put these things in your CMMS system and track them!

Use Stronger security measures

Have a policy for passwords using upper and lowercase characters, symbols, and numbers: Us3C@mm3lC@s3 = Use Camel Case

Have a policy to change passwords periodically

Keep in mind that up to 35% of breeches are email in nature.

Security is something you have, something you are, something you know.

- You have a FOB or Key card
- You know a password and login
- You have a biometric scanner (Cell phones are the future)

Control Logins - Do not use generic logins

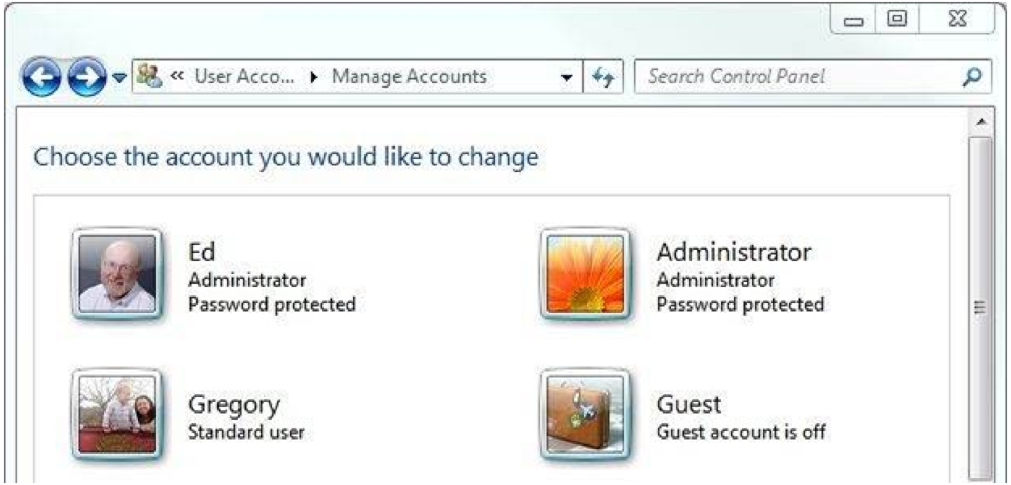
Authentication - Login control. Limit who can access the system

Authorization - What can you do? Not all logins are the same

- **Administrators** - can install programs and make changes to the system
- **Users** - can use the system - can't make system changes or install programs without an admin password.

Watch out for generic Administrator and Guest accounts.

All accounts should have a password.



Choose the account you would like to change

Ed
Administrator
Password protected

Administrator
Administrator
Password protected

Gregory
Standard user

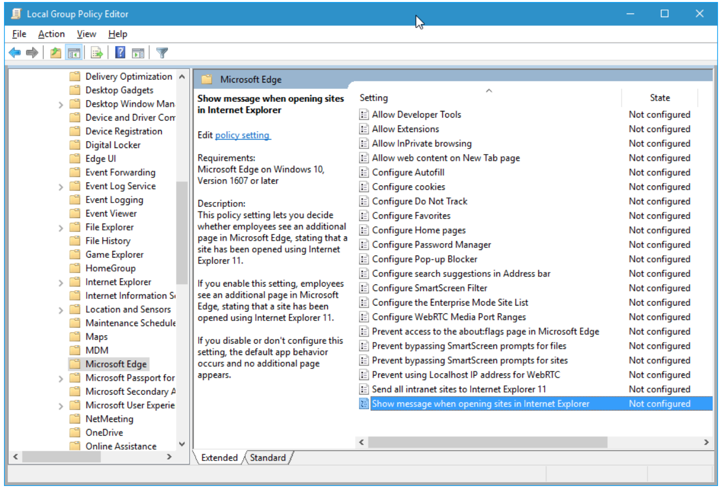
Guest
Guest account is off

Use GPO = Group Policy Object

GPO can be used to limit what a user (or admin) can do to a system. You can limit what they can or cannot run. Every function of windows can be individually controlled here. It is accessed through gpedit.msc

You can lock systems down to the most essential functions.

Ask the OEM about GPO and what it can do for you. If they do not know, you may want to bring this up on capital equipment purchases.



Show message when opening sites in Internet Explorer

Edit policy setting

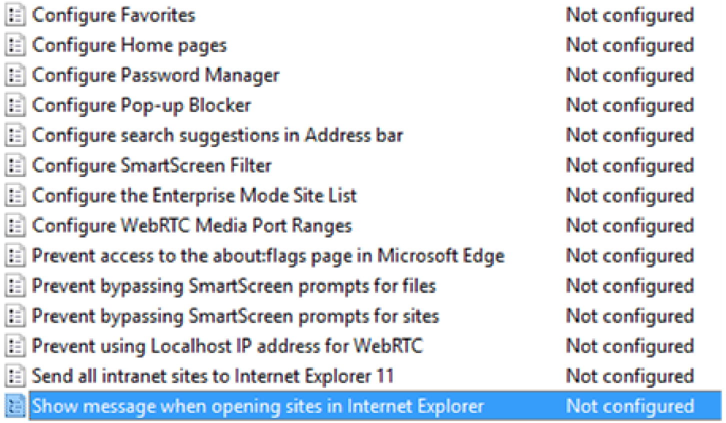
Requirements:
Microsoft Edge on Windows 10, Version 1607 or later

Description:
This policy setting lets you decide whether employees see an additional page in Microsoft Edge, stating that a site has been opened using Internet Explorer 11.

If you enable this setting, employees see an additional page in Microsoft Edge, stating that a site has been opened using Internet Explorer 11.

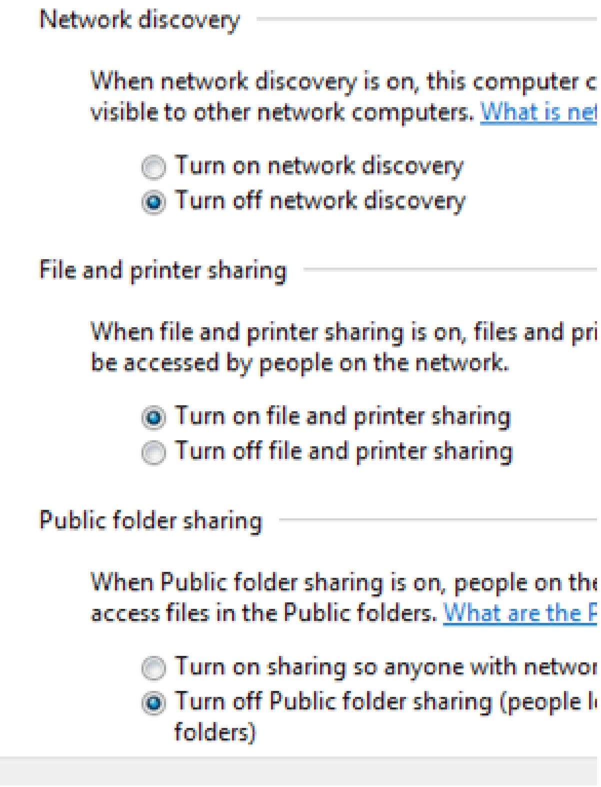
If you disable or don't configure this setting, the default app behavior occurs and no additional page appears.

Setting	State
Allow Developer Tools	Not configured
Allow Extensions	Not configured
Allow InPrivate browsing	Not configured
Allow web content on New Tab page	Not configured
Configure Autofill	Not configured
Configure cookies	Not configured
Configure Do Not Track	Not configured
Configure Favorites	Not configured
Configure Home pages	Not configured
Configure Password Manager	Not configured
Configure Pop-up Blocker	Not configured
Configure search suggestions in Address bar	Not configured
Configure SmartScreen Filter	Not configured
Configure the Enterprise Mode Site List	Not configured
Configure WebRTC Media Port Ranges	Not configured
Prevent access to the about:flags page in Microsoft Edge	Not configured
Prevent bypassing SmartScreen prompts for files	Not configured
Prevent bypassing SmartScreen prompts for sites	Not configured
Prevent using Localhost IP address for WebRTC	Not configured
Send all intranet sites to Internet Explorer 11	Not configured
Show message when opening sites in Internet Explorer	Not configured



Configure Favorites	Not configured
Configure Home pages	Not configured
Configure Password Manager	Not configured
Configure Pop-up Blocker	Not configured
Configure search suggestions in Address bar	Not configured
Configure SmartScreen Filter	Not configured
Configure the Enterprise Mode Site List	Not configured
Configure WebRTC Media Port Ranges	Not configured
Prevent access to the about:flags page in Microsoft Edge	Not configured
Prevent bypassing SmartScreen prompts for files	Not configured
Prevent bypassing SmartScreen prompts for sites	Not configured
Prevent using Localhost IP address for WebRTC	Not configured
Send all intranet sites to Internet Explorer 11	Not configured
Show message when opening sites in Internet Explorer	Not configured

Ask OEM's to use folder permissions on file shares



Network discovery

When network discovery is on, this computer c
visible to other network computers. What is ne

○ Turn on network discovery
● Turn off network discovery

File and printer sharing

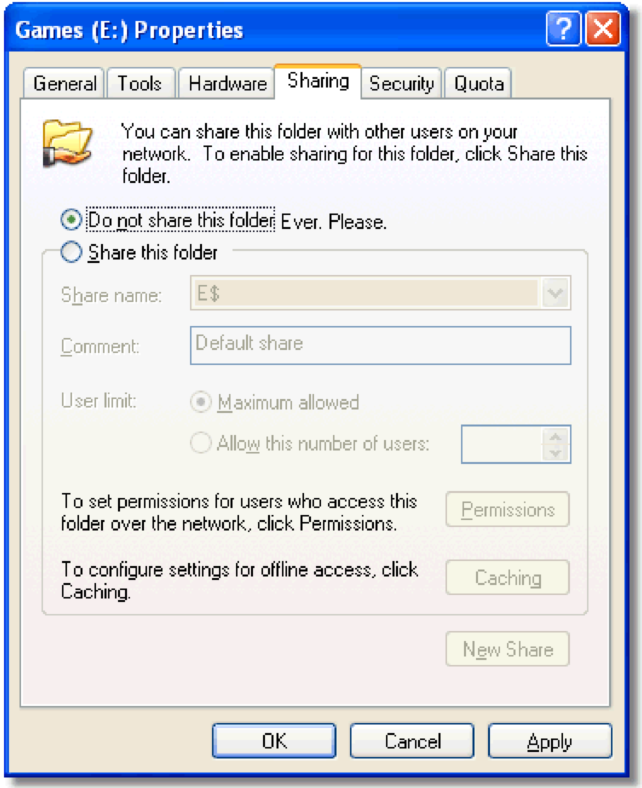
When file and printer sharing is on, files and pri
be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the
access files in the Public folders. What are the P

○ Turn on sharing so anyone with networ
● Turn off Public folder sharing (people l
folders)



Games (E:) Properties

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

● Do not share this folder Ever. Please.
○ Share this folder

Share name: E$

Comment: Default share

User limit: ● Maximum allowed
○ Allow this number of users:

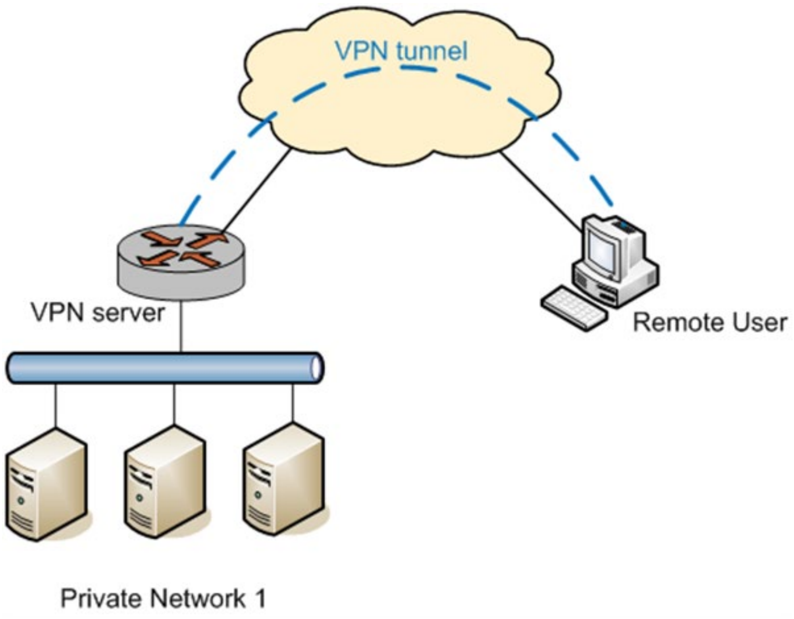
To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

You can set permissions to folders and control if users have read only access. Do not just leave a folder as a public share with no permissions.

Disable simple file sharing when applicable

Limit VPN access



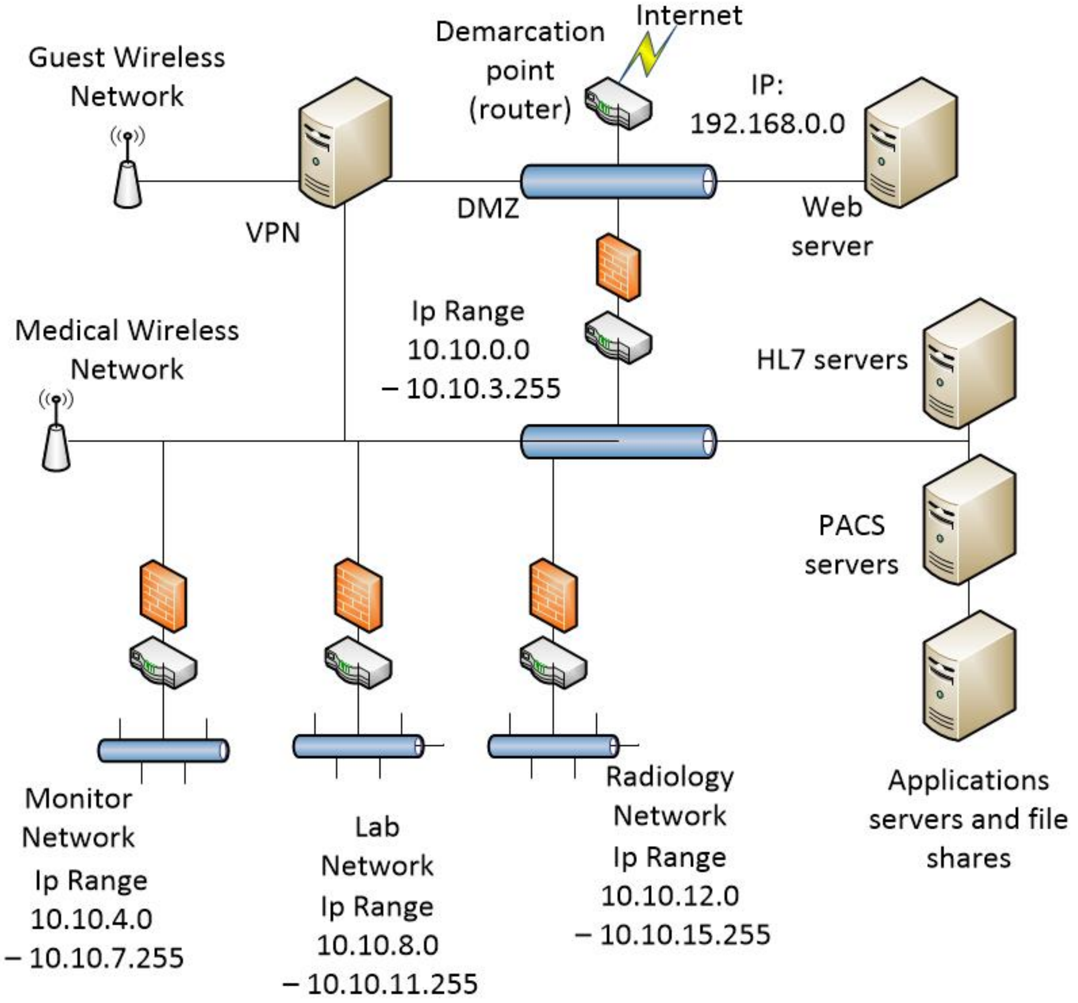
This is not popular with the OEM or vendors.

- Sometimes vendors need remote access and they ask for it from the Hospital IT.
- IT gives access after verifying the servicer or OEM
- Several redundant accounts can be created - creating vulnerabilities
- **VPN logins should be purged regularly.** What is your policy?
- Know who is getting into your network

Network Segmentation 101

Use routers to separate networks into smaller segments that operate independently of each other.

This protects the systems and controls the data flow.

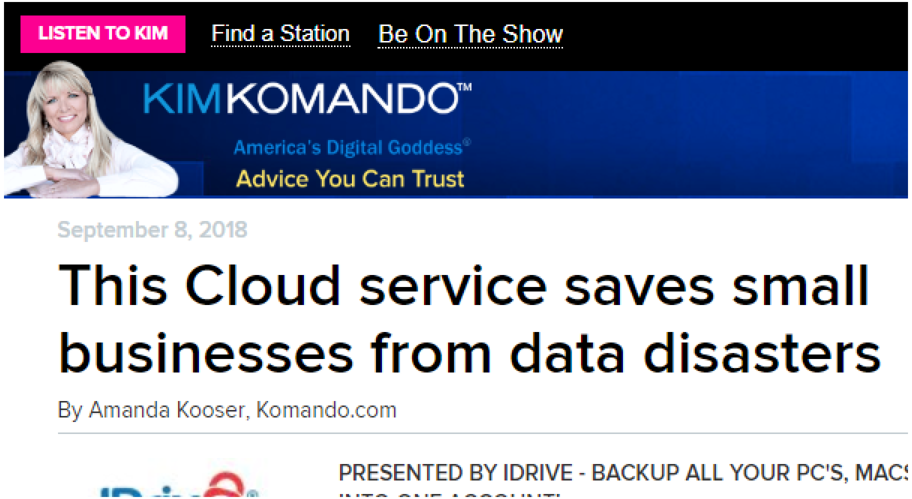

Internet
Demarcation point (router)
Guest Wireless Network
IP: 192.168.0.0
VPN
DMZ
Web server
Ip Range 10.10.0.0 – 10.10.3.255
Medical Wireless Network
HL7 servers
PACS servers
Monitor Network Ip Range 10.10.4.0 – 10.10.7.255
Lab Network Ip Range 10.10.8.0 – 10.10.11.255
Radiology Network Ip Range 10.10.12.0 – 10.10.15.255
Applications servers and file shares

As about Cloud applications and data storage

Newer technologies such as cloud applications allow hospitals to pool resources and ensure security with a 3rd party storage option, such as Iron Mountain.

Use Epic and other system integrations to push data to secure locations quickly.

Look for things like “Hosted on Amazon EC2 (AWS)”



September 8, 2018

This Cloud service saves small businesses from data disasters

By Amanda Kooser, Komando.com

PRESENTED BY IDRIVE - BACKUP ALL YOUR PC'S, MAC

Problem is… who owns it?
Remember: HIPAA keeps us honest

Get active on the purchasing of capital equipment

Check for the security breaches from a device before buying it.

Ask about Embedded security vs Bolt-on security.

Ask about the OEM support for updates and patches

Ask about further testing for cyber attacks from the OEM

FDA is addressing this by changing the 510K tests

SECURITY

FDA to Boost Medical Device Cybersecurity

Published on September 13, 2018

They are changing the 510K process to evaluate devices based on the cybersecurity risks from other OEM's in that device class.

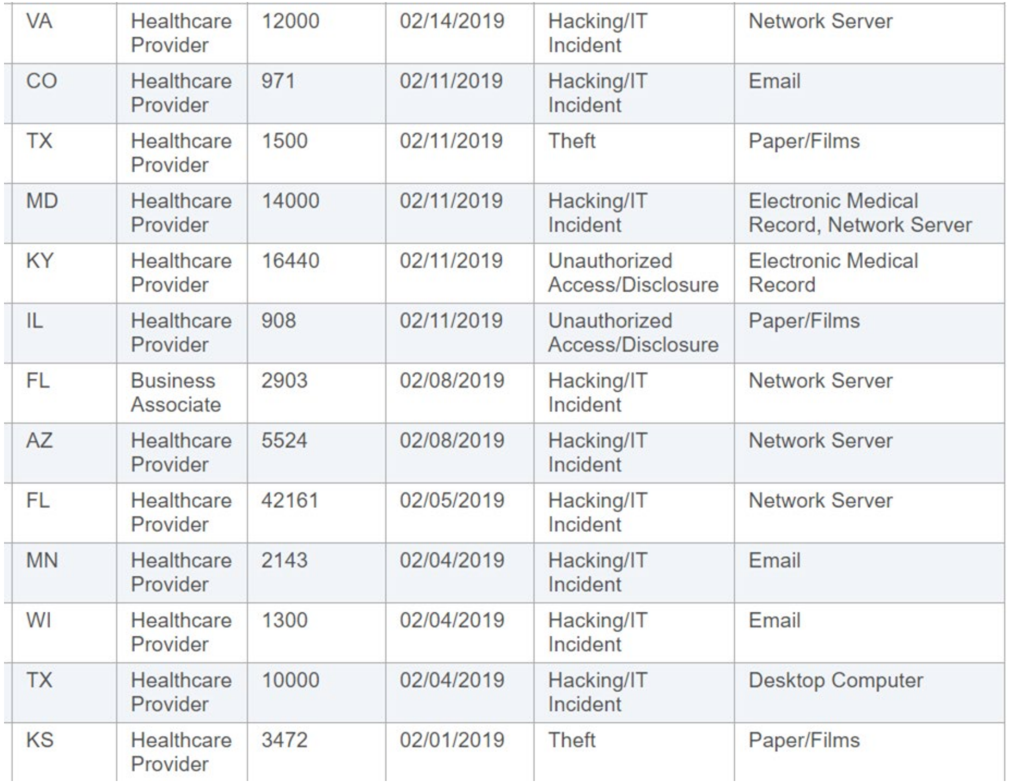
For example, if one company has a breach, the lessons from that will be applied to other companies as their devices are tested

Enforces embedded security over bolt-on security.

Risk Assessments on Equipment Cybersecurity

- Actually use a BET **Risk Assessment** to tell vulnerabilities
  - Tell what equipment is the most vulnerable
  - Tell how to segment networks
  - Tell where to go to defend against an attack or what machines to isolate first. Where are the vulnerabilities?
- Keep logs of **Operating Systems** for each machine
  - Patch revisions and Software Revisions
  - Security Packs / Windows Updates
  - Antivirus Updates (FDA is OK with it)
- Use this data when selecting **New Purchases**, get active.
  - Embedded security vs bolt on security and long term support
  - Remind people: We reduce loss, prevent breaches and fines
  - Ask the hard questions to the OEM and get them onboard

Ask Risk Management how they feel about this.



VA	Healthcare Provider	12000	02/14/2019	Hacking/IT Incident	Network Server
CO	Healthcare Provider	971	02/11/2019	Hacking/IT Incident	Email
TX	Healthcare Provider	1500	02/11/2019	Theft	Paper/Films
MD	Healthcare Provider	14000	02/11/2019	Hacking/IT Incident	Electronic Medical Record, Network Server
KY	Healthcare Provider	16440	02/11/2019	Unauthorized Access/Disclosure	Electronic Medical Record
IL	Healthcare Provider	908	02/11/2019	Unauthorized Access/Disclosure	Paper/Films
FL	Business Associate	2903	02/08/2019	Hacking/IT Incident	Network Server
AZ	Healthcare Provider	5524	02/08/2019	Hacking/IT Incident	Network Server
FL	Healthcare Provider	42161	02/05/2019	Hacking/IT Incident	Network Server
MN	Healthcare Provider	2143	02/04/2019	Hacking/IT Incident	Email
WI	Healthcare Provider	1300	02/04/2019	Hacking/IT Incident	Email
TX	Healthcare Provider	10000	02/04/2019	Hacking/IT Incident	Desktop Computer
KS	Healthcare Provider	3472	02/01/2019	Theft	Paper/Films

These are HIPAA Breaches from Feb 2019

- 29 breaches reported in Feb 2019
- 25 of the 29 were coded “Unauthorised Access” or “Hacking”
- 4 were coded “Theft”
- 14 direct system or server hacks
- 8 were email related hacks
- 50% increase in hacks from May 2017
- Involved over 2 million Patient records - 25 times increase from May 2017

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Is the sky falling? … No

- We are not at the front line of this defense.
- Thankfully, we do have a hospital IT security team to help
- We have OEM development teams who are talking about this stuff.
- We are not usually the repository of information the hackers are after…. yet.
- We are on the peripheral edge of the war on cybercrime.
- This is about minimizing risk, we are good at that.

Questions

Actually, I have some questions for you:

- How did your organization react to and handle the WannaCry event or other cyberattacks?
- How (within your ability to talk about it) was your facility affected by ransomware?
- What do you already do to reduce the liability and risk of a cyberattack?
- What training does your staff go through to accomplish the tasks in the above questions?
- How do you handle updates or sandboxing?
- Do you log equipment software information such as versions and Operating systems?
- What advice would you have to other technicians to better prepare themselves for the future?