Ransomware Attacks

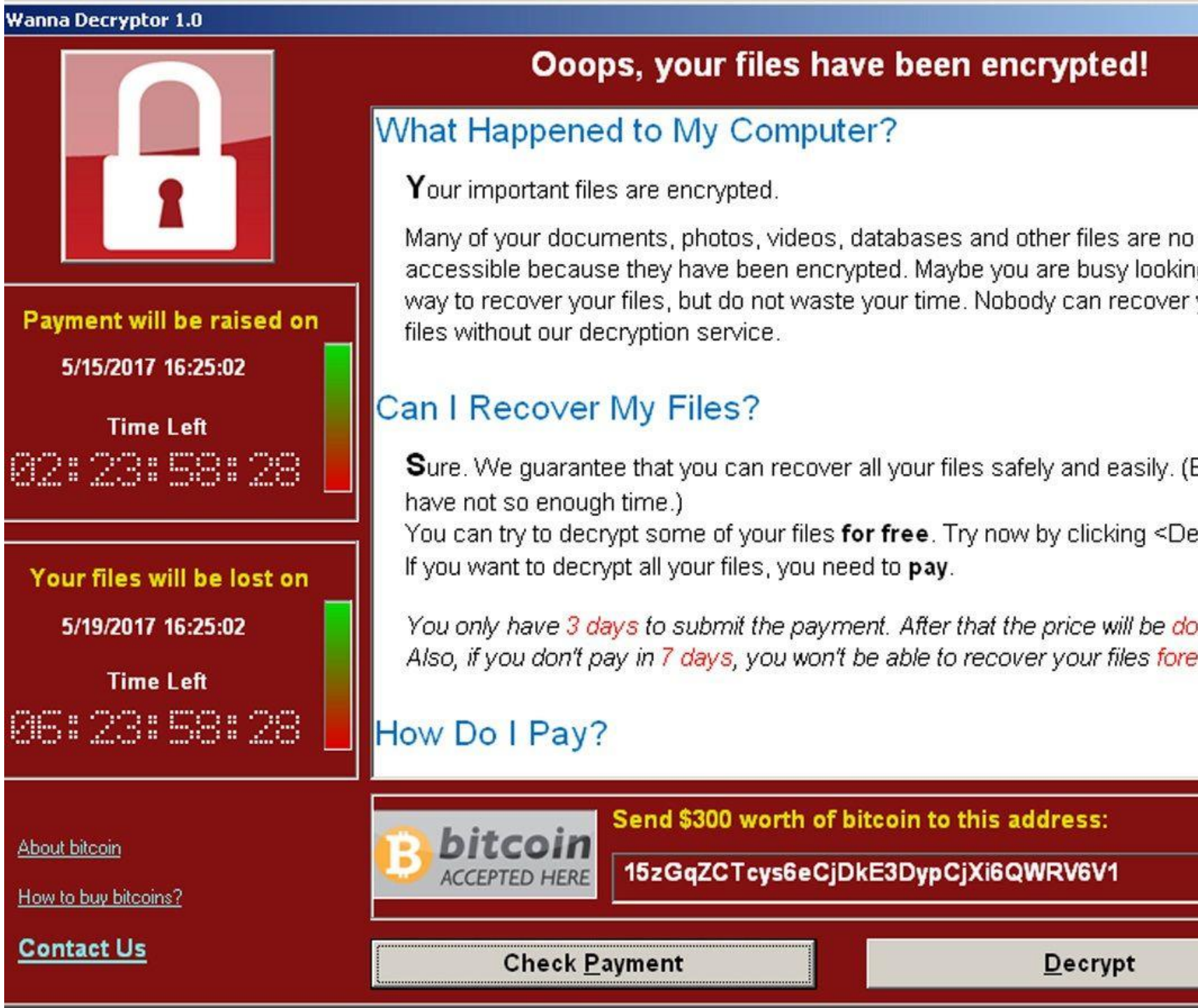
MICHAEL NICHOLSON

What is Ransomware?

Ransomware is malware that requires the victim to pay a ransom to access encrypted files.

This specific interface is from the ransomware WannaCry.

WannaCry took advantage of the “EternalBlue” exploit in the Windows operating system. (Patched March 14, 2017)



What is EternalBlue?

EternalBlue is a cyberattack exploit developed by the U.S. National Security Agency (NSA) that exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol.

Effects Windows 95 through Windows XP

Microsoft even patched unsupported operating systems because many companies and organizations still use their outdated operating systems.

The NSA withheld the information about the EternalBlue exploit for 5 years and only told Microsoft about it when hackers began using it to install malware on computer systems.

How did WannaCry Use EternalBlue?

WannaCry specifically used Server Message Block (SMB) version 1 and TCP port 445.

SMB has a feature called “SMB Transactions” which enables for atomic read and write to be performed between an SMB client and server.

The vulnerability with the transactions is that if the message request is greater than the SMB MaxBufferSize, the messages that are left will be sent as Secondary Trans2 requests. This specifically effects the srv2.sys kernel driver and is triggered by malformed Secondary Trans2 requests.

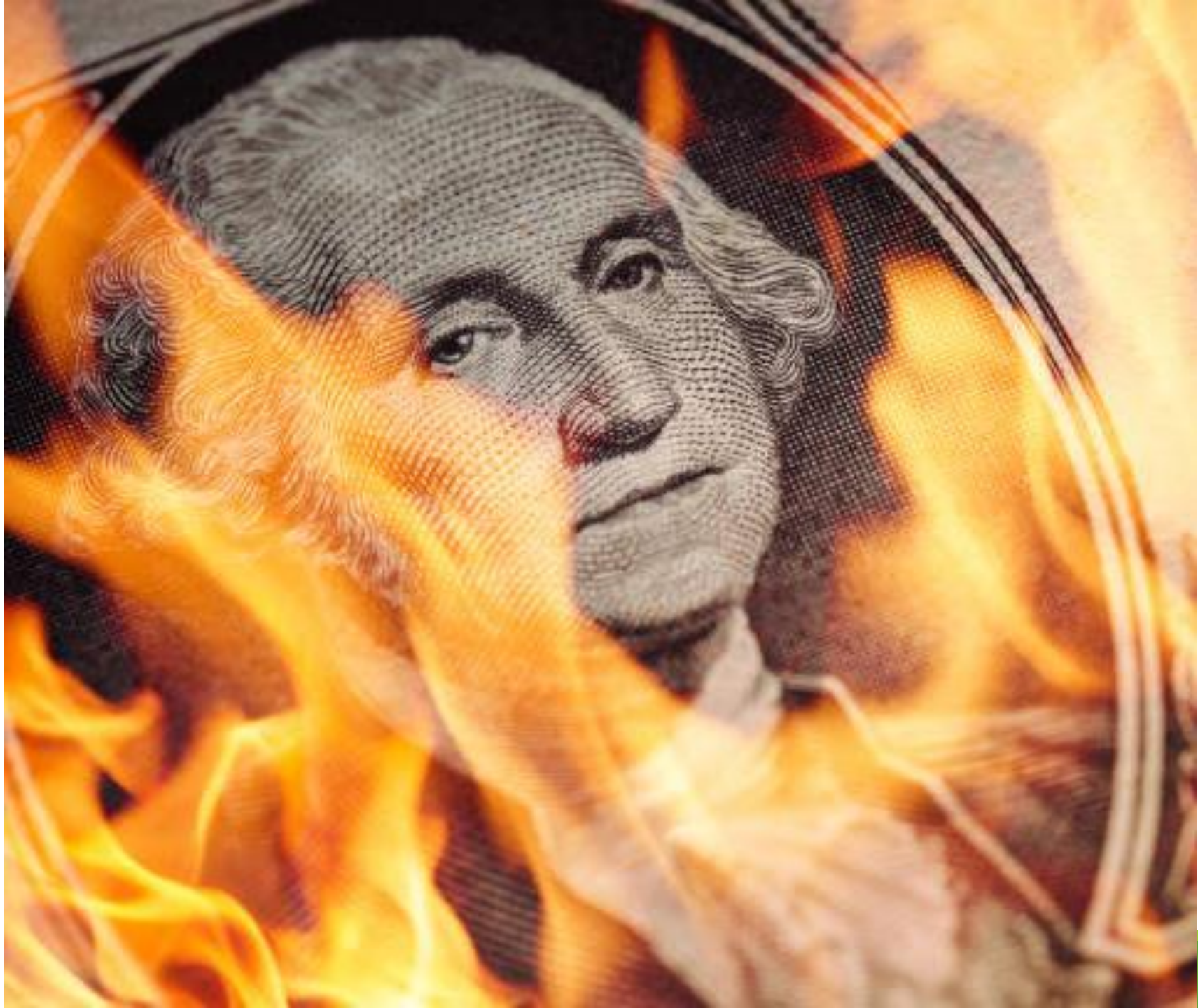
In simpler terms, a hacker sends a large amount of data to a computer which the computer cannot fully handle, so there is a protocol that separates the packets up so the computer can fully receive the information. The protocol is flawed, so the hacker can take advantage of the vulnerability by sneaking in packets of data that will go unnoticed by the receiving computer.

WannaCry's Impact

Over $4 billion dollars lost in 2017.

150 countries effected.

Over 200,000 computers effected.



Why is Ransomware so Dangerous?

It can effect computers that have very important jobs.

Servers owned by banks, company computers, hospital computers and machinery, and even government or military computers.

Ransomware can spread throughout company computers even though it may be one person's mistake.

Ransomware is Easy to Install

There is an endless amount of ways that malware can infect a computer system. Using an outdated operating system makes the computer more vulnerable.

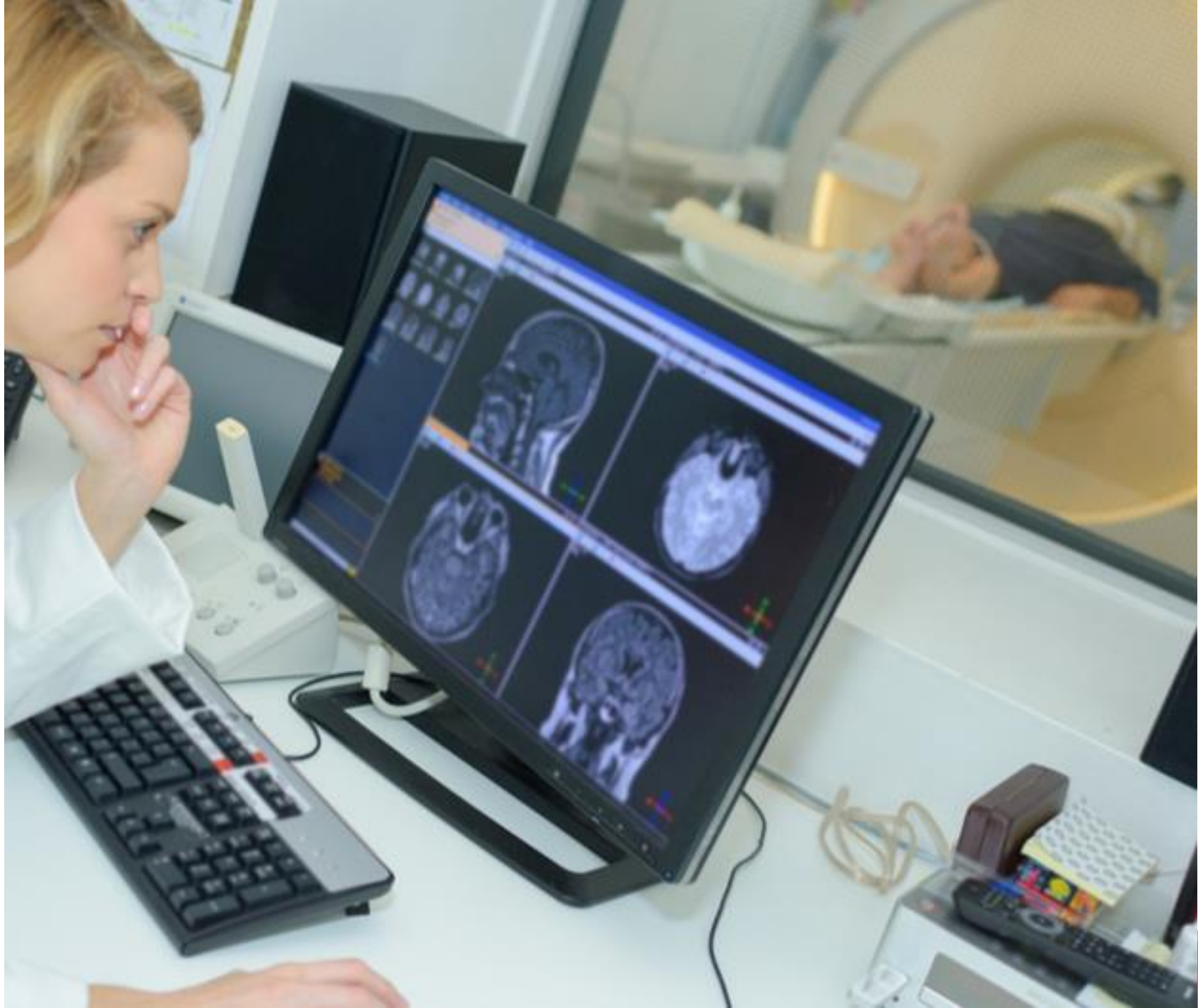
Trojan viruses, backdoor malware, email attachments, and fake download websites/buttons are just some of the ways that ransomware can be installed to a computer system.

The computer will appear to be normal until a specific task is formed or a certain amount of time has passed.

Ransomware Attacks in Hospitals

In most cases a ransomware attack can be considered non-life threatening. In hospitals it is a different story.

Imagine what could happen.



Brooklyn Hospital Incident

In July of 2019, a ransomware attack hit several computer systems at Brooklyn Hospital Center in New York City which caused permanent loss in patient information.

The malware also disrupted the operation of some hospital systems like dental and cardiac imaging.

There is no evidence that any data was compromised by the launchers of the ransomware, only permanent loss in some patient data.

Had to turn away many patients.

Ransomware attacks on hospitals are very effective because the data that is being held is invaluable to the lives of the patients. It is almost guaranteed that the hospital pays the ransom.

Reviews for this hospital are terrible. (2.8/5.0)

Park DuValle Health Center Incident

Had to pay $70,000 to get patient records unencrypted.

Data of over 20,000 patients held by the hackers for almost 2 months before the hospital paid the ransom.

Not the first time that this center has been attacked.

Costed the health center over a million dollars and damages.

Patients losing trust in organization because of their private information being compromised.

Reviews of this health center are bad. (3.1/5.0)

What is Learned from this?

Companies need to have better control of what their employees do on their computers.

Employees need to follow computer usage guidelines no matter what.

Computer users need to know how malware works and how easy it is to accidently download it.

Computer users need to know how to protect themselves from their data being compromised.

BACK UP YOUR FILES!!!

Sources

Basic Info About WannaCry: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Eternal Blue: https://en.wikipedia.org/wiki/EternalBlue

Explaining SMB Exploitation: https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html

WannaCry Economic Losses: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

Burning Money Pic: https://www.istockphoto.com/photos/money-burning?sort=mostpopular&mediatype=photography&phrase=money%20burning

WannaCry Screenshot: https://www.pbs.org/newshour/science/everything-need-know-wannacrypt-ransomware-attack

Hospital Computer Pic: https://www.insidescience.org/news/hospitals-hacks-malware-and-medical-safety

Brooklyn Hospital: https://www.fiercehealthcare.com/tech/ransomware-attack-at-brooklyn-hospital-center-results-permanent-loss-some-patient-data

Park DuValle Center: https://www.wdrb.com/in-depth/park-duvalle-health-center-pays-ransom-for-patient-records-in/article_68416546-af0b-11e9-ba4d-0bd49b023c3e.html