WannaCry

A Tale Still Resolving

Stephen Bookstaber
Rene Colo
Tesslyn Knapp
Jonathan Lee
Phoebe Sheahan

WHAT IS WANNACRY

RANSOMWARE

Ransomware is a **type of malware** that is used to **extort money from victims**.

Wannacry is a **form of crypto ransomware**, because the money being extorted was demanded in the **form of a bitcoin payment**.

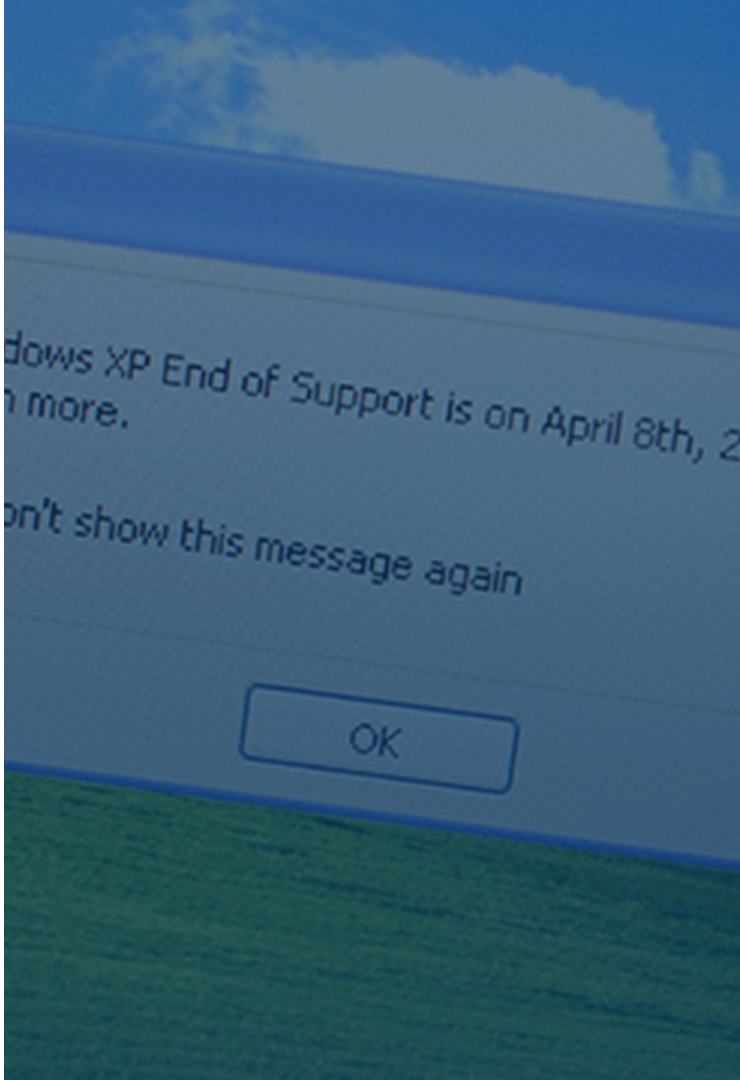
FACTS

Date:
May 2017

Targeted vulnerability in **Microsoft Operating Systems** including end-of-support **Windows XP**

Windows released patches for this vulnerability two months prior. **Users that did not update** their systems with the patch were **left vulnerable**.

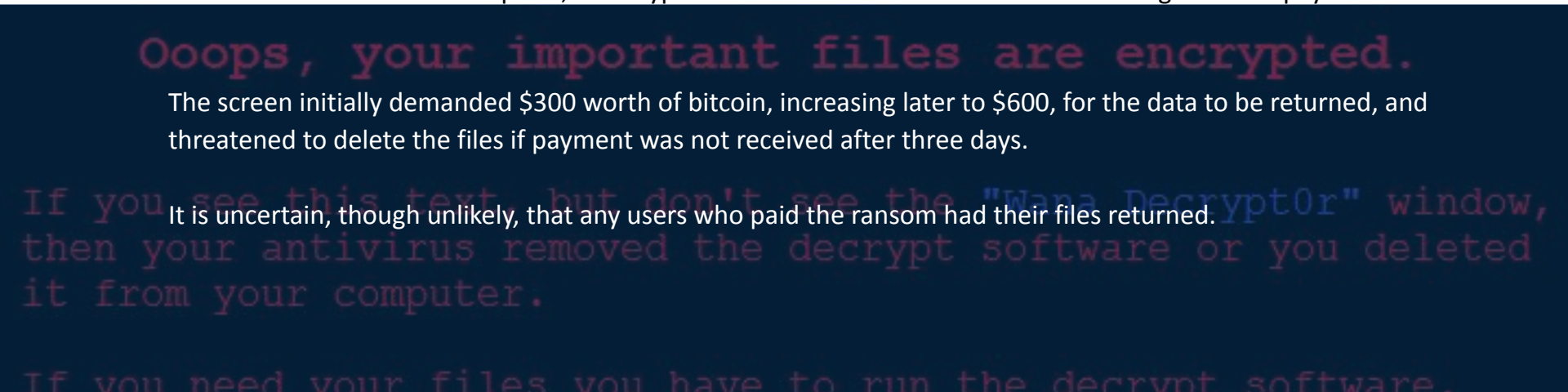
EternalBlue: the exploit to gain access to vulnerable Windows operating systems
DoublePulsar: a backdoor tool that enables execution of malicious code



FACTS

Cryptoworm:
Starting from a single machine, it used the **EternalBlue** exploit to gain access to unpatched machines, installed the **Doublepulsar** exploit, and then used Doublepulsar execute the cryptoworm function. **Both were developed by the NSA** and stolen by a group called the ShadowBrokers.

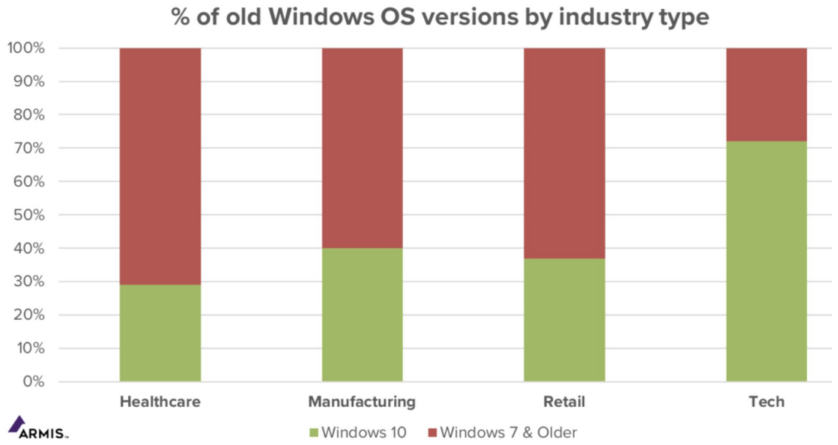
The Ransom:
When the virus infects a computer, it encrypts the data and flashes a screen demanding a bitcoin payment.



The screen initially demanded $300 worth of bitcoin, increasing later to $600, for the data to be returned, and threatened to delete the files if payment was not received after three days.

It is uncertain, though unlikely, that any users who paid the ransom had their files returned.

IMPACTS: OVERVIEW



$400,000 Ransomed

$4 Billion in Losses

300,000 Computers

150 Countries

Encrypts all data on machine > Stop use of device completely > Holds data hostage > **Organizations declare state of emergency.**

IMPACTS: INDUSTRY

GOVERNMENT

Mostly avoided WannaCry infections

Implementation of cybersecurity regulations

Blamed for hiding the security flaw after it was stolen earlier by hackers

Did not notify companies or institutions of possible vulnerabilities

BIG TECH

Microsoft was the most affected tech company

200,000 Windows Computers were infected

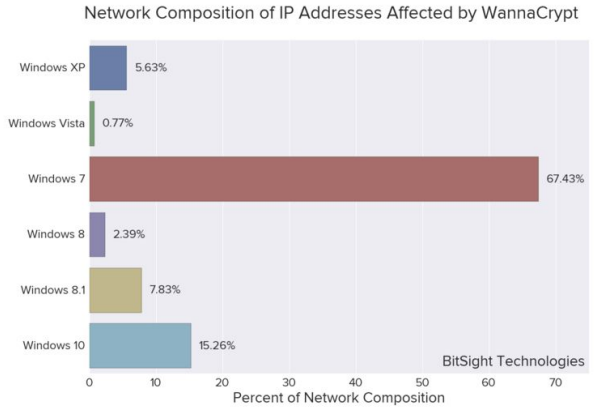
Failed to patch systems and stopped support

Big tech companies were blamed but the government relies on their security flaws for counter-terrorism and law enforcement.

Forced to release patches for unsupported systems

RETAIL

Point of sale devices



IMPACTS: REGULATIONS

REGULATIONS

Businesses who have outdated systems were required to meet certain regulations and agreements with vendors to continue to run these systems

Companies were held responsible when they had no way to counterattack due to regulations

Vulnerabilities Equities Process is a policy that addresses when agencies should notify companies about security flaws but it is only partially public

IMPACTS: HEALTHCARE 2017

WannaCry **crippled 81 out of 236 National Health Service** hospitals in England plus **603 primary care** and **595 medical practices**

Impacted up to **70,000 devices** including:

Computers, MRI scanners, blood-storage refrigerators, and theatre equipment

Infected **1,200 diagnostic devices** and caused many others to be temporarily taken out of service to prevent malware from spreading

Forced **5 UK hospitals' emergency departments to close** and divert patients

Costed NHS **$116.4 million** and lead to **19,000** cancelled appointments.

There are **surprisingly high numbers of unmanaged devices** running on outdated operating systems in the healthcare sector

Many medical devices themselves are based on outdated Windows versions and **cannot be updated without complete remodeling** and many don't run any endpoint security

Nearly 70% of healthcare organizations operated on Windows 7 or older platforms in 2019

The FBI considers WannaCry the **first ransomware attack to widely target vulnerabilities commonly found in medical devices**

IMPACTS: HEALTHCARE SINCE 2017

WannaCry continued to be an **active threat with 40% of healthcare organizations experiencing at least one** WannaCry attack in the first 6 months of 2019

Ransomware accounted for more than **70 percent of the successful cyber attacks on health care organizations each year** since 2017 despite hospitals being on high alert

NHS IT staff has since improved its security and only been hit by 6 successful ransomware attacks since 2017 in comparison to 203 from the three years prior to 2017

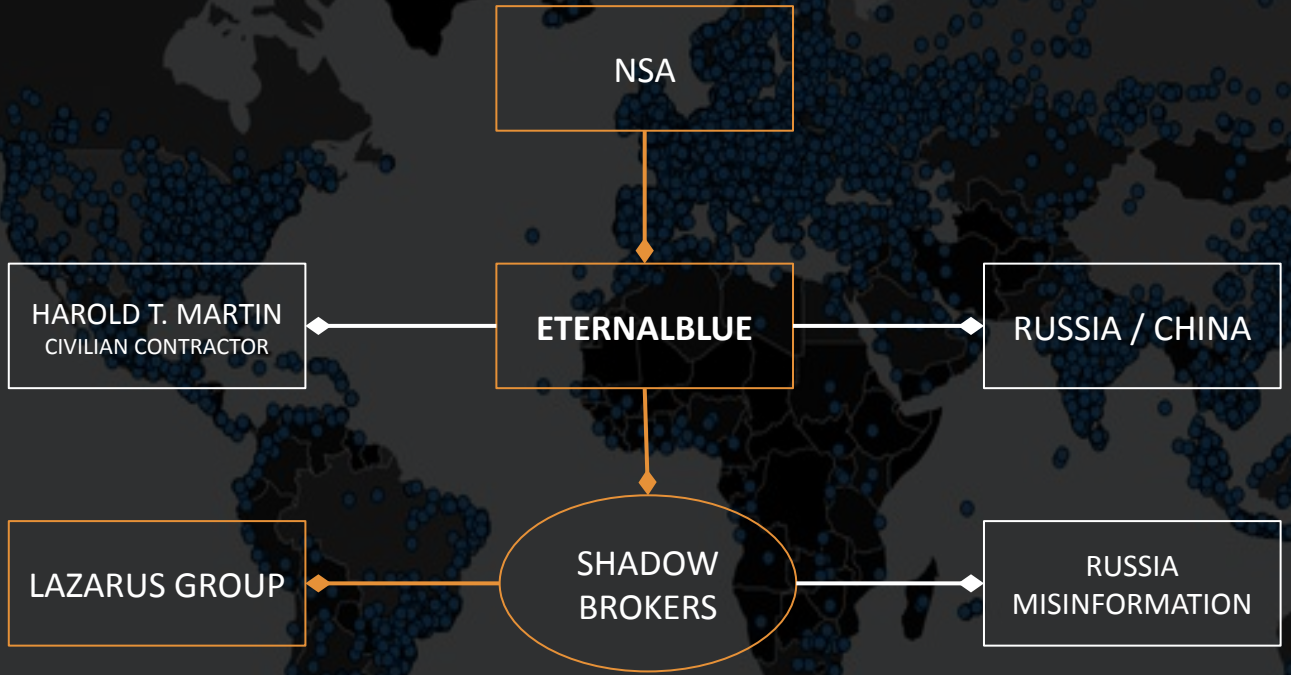
Ransomware attacks that cause hospitals to suspend patient care operations is **akin to a mass-casualty terrorist attack**

Like military attacks on hospitals, **cyber attacks on hospitals violate all internationally accepted norms of warfare**

WHAT CAN BE DONE?

Since cyber risk to the healthcare sector is now directly influenced by the geopolitical climate, the effort to protect hospitals and patients must include **involving law enforcement, legislative, military, and intelligence assets in their defense**

ASSUMPTIONS: UNKNOWN



HACKER WHO STOPPED WANNACRY ARRESTED

2010
Marcus Hutchins approached by Vinny

2012
Completed UPAS Kit

2013
Coerced to start UPAS Kit 2.0

2014
Completed UPAS Kit 2.0 [*Kronos*]

2015
Started blogging about how to deconstruct root kits. Joined Kryptos Logic

2017/05/12
Marcus Hutchins found Killswitch. Began campaign to keep domain from being taken offline.

2017/08/12
Marcus Hutchins arrested by FBI in Las Vegas after DefCon in regards to Kronos

2019
"Full responsibility for my mistakes"
Pled guilty to 2 / 10 counts. Served 1 year of supervised release in LA

2010

2020

2013
NSA created Eternal Blue

2017/05/12
WannaCry Released

2017/01 - 2017/04
Jan: Shadow Brokers Release Exploits from Agencies
Mar: NSA updates Microsoft & Microsoft makes patches about Eternal Blue leak
Apr: Shadow Brokers Release Eternal Blue

RESPONSIBILITY OF ACTIONS

NSA

"Hoards vulnerabilities"

- Used for US defense as a deterrent as well as espionage

NO PUNISHMENT

Hack got leaked but no public tribunals and no public trials.

MARCUS HUTCHINS

One man who built rootkits was arrested

- Kronos was used and designed for malicious purposes

PUNISHMENT

The man who stopped the hack got arrested for a much smaller action.

INDIVIDUAL: RESPONSIBILITY

INCREASE KNOWLEDGE OF CYBERSECURITY

Gain more knowledge from classes or reading articles and journals online

KEEP SOFTWARE UP TO DATE

Double edged sword: **may introduce new vulnerabilities** or **introduce instability**, which may lead to **data loss**

BE WARY OF UNKNOWN WIFI

Networks are only as **secure as their weakest device**. Give your friends Guest WiFi. Be careful of Open WiFi.

BACK-UP YOUR DATA

Both hardware and software backups will help ensure that you are insulated from data corruption

U.S. USE CASE:
Everyone and every industry uses the internet

DIFFICULTY: MEANS AND ACCESS
Not everyone can afford, so what do you do?

Write your local, state, and federal politicians

We all need to be in this together

Individual Responsibility

United States Use Case: **Every one and every industry uses the internet**

Increase knowledge of cyber security

Keep software up to date on computers, devices, and network

- Double-edged sword:
  - Rarer: **Some updates have introduced new vulnerabilities**
  - **Introduce instability**, which may lead to unrecoverable data loss

Networks are only as **secure as their weakest device**

- Give your friends the Guest Wifi not your actual Wifi
- Be Wary of Open Wifis

Back up your data to other locations / devices

Difficulty: **means and access**

- Not everyone can afford a new computer / device
- Write to your local, state, and federal politicians

Stephen: What is ransomware? Tell direct factual story of what happened and what led up to it: How did Wannacry actual infect stuff (the technical aspects of the worm)?
Slides:

-

Phoebe: impacts: big tech, government, regulations

Tess: Impacts in healthcare

Rene: Assumptions (cybersecurity, government, NSA); why did they do it? Recommendations on cybersecurity/government
Slides:

Jon: Tell Marcus's story, the human element, post-2017 people updating their computers/security as a reaction to Wannacry. Recommendations for the personal.
Slides:

- The Hacker who Stopped It (And His Life) - Get Famous and Get Wrekt
- Individual responsibility (how can individuals keep up to date? Cost prohibitive?)

Intro

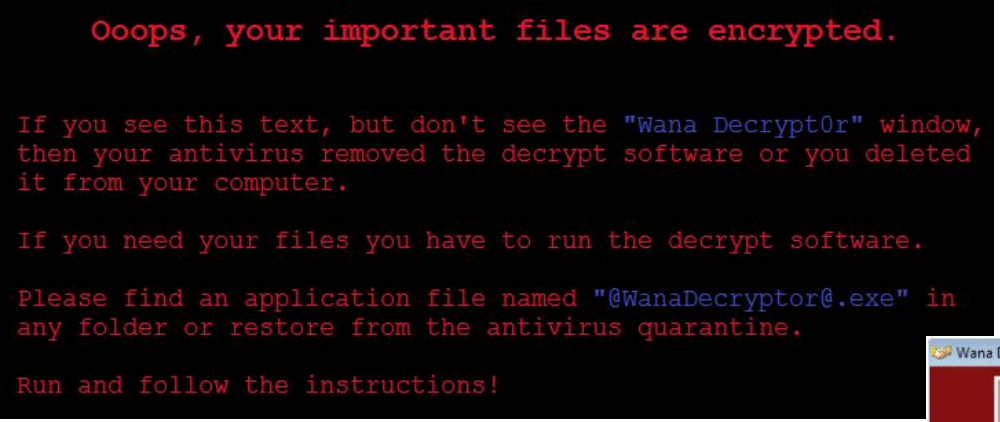
The Wannacry attack consisted of several components:

- Wannacry: the ransomware cryptoworm
- EternalBlue: the exploit to gain access to vulnerable systems Windows operating systems
- DoublePulsar: a backdoor tool that, once installed, enabled Wannacry , installed mechanism that installed and executed enabling Wannacry to install and execute

- Exploit targeted a Windows XP vulnerability. Microsoft released a patch two months earlier, but many people did not update their systems to install the patch.

- The hack to exploit this vulnerability, which enabled Wannacry to spread, was allegedly developed by the NSA and stolen by the perpetrators.

- The virus encrypted user's files and threatened to delete the files if a bitcoin payment was not received within three days.


Ooops, your important files are encrypted.
If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.
If you need your files you have to run the decrypt software.
Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.
Run and follow the instructions!


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
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
Payment will be raised on
5/16/2017 04:46:50
Time Left
02:23:59:42
Your files will be lost on
5/20/2017 04:46:50
Time Left
06:23:59:42
About bitcoin
How to buy bitcoins?
Contact Us
Send $300 worth of bitcoin to this address:
bitcoin ACCEPTED HERE
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Copy
Check Payment
Decrypt

Facts: Pre-2017

Facts:
Impacts: 2017

WANNACRY PROPAGATES

12/05 2017

- 230 000+ machine infected
  Worm + Cryptolocker
- Propagates through SMB protocol (445/TCP) - not by email (confusion with JAFF)
- Uses MS17-10
- Ransom : 300 to 600 USD per machine
- 98% of the victims are running Windows7
- 13/05/17:MS releases a patch for XP & 2003

MS PUBLISHES MS17-010

14/03 2017

Microsoft publishes a patch (MS17-010), this patch fixes the vulnerability used by EternalBue
No fix for XP & 2003 (end of support)

ETERNAL BLUE PUBLIC RELEASE

8/04 2017

On 08/04/17 & 14/04/17 Shadow Brokers publish new documents and release the password to read the archive "eqgrp-auction-file.tar.xz.gpg",those files contains, among others, the exploit Eternal Blue

The archive also contains other exploits (like EsteemAudit, targeting Terminal server) that could be worm-able!

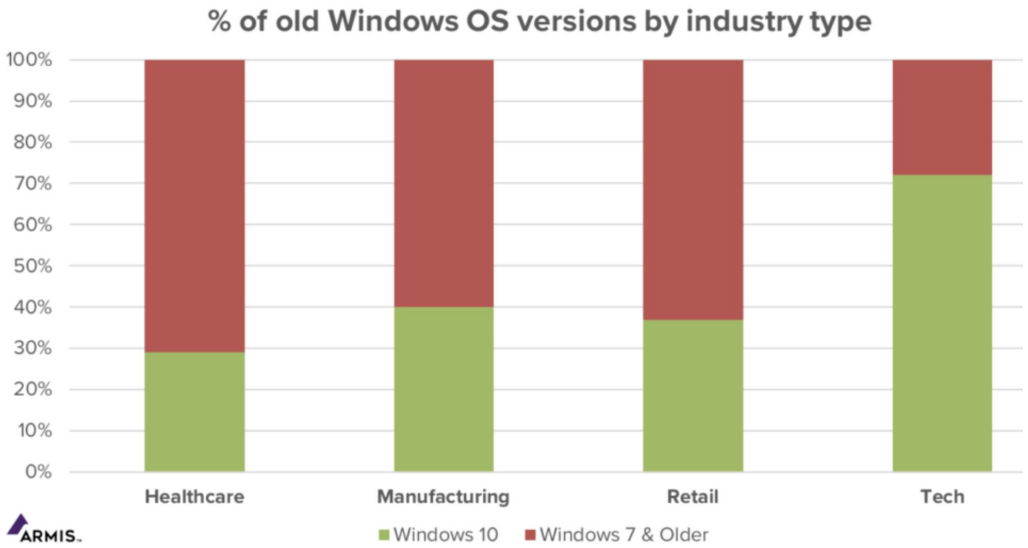
SHADOW BROKERS - MESSAGE FINALE

13/01 2017

The Shadow Brokers group publish a new archive "equation_drug.tar.xz.gpg" , this archive is password protected and is supposed to contain new exploits

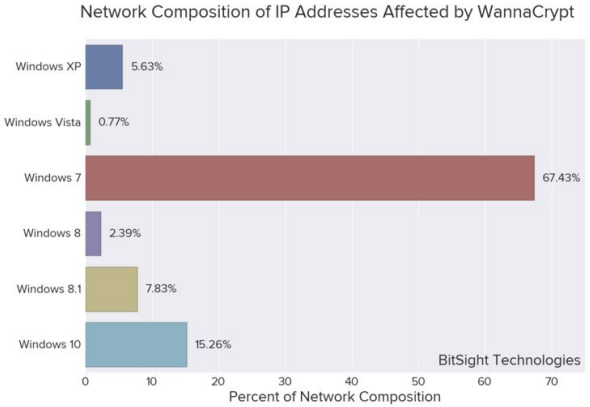
Impacts

- Estimated 4 billion in losses
- 300,000 computers
- 150 countries
- Ransom requested
- Encrypts all data on machine
    - Stopped from using the machine completely
    - Holds data hostage
- Many organizations forced to declare a state of emergency.



Impacts

- Government: Mostly avoided WannaCry infections
  - Implementation of cybersecurity regulations
  - Blamed for hiding the security flaw after it was stolen earlier by
  - Did not notify companies or institutions of possible vulnerabiliti
- Big Tech: Microsoft was the most affected tech company
  - 200,000 Windows Computers were infected
  - Failed to patch systems and stopped support
  - Big tech companies were blamed but the government relies or counter-terrorism and law enforcement.
  - Forced to release patches for unsupported systems
- Retail
  - Point of sale devices
- Regulations
  - Businesses who have outdated systems were required to meet certain regulations and agreements with vendors to continue to run these systems
  - Companies were held responsible when they had no way to counterattack due to regulations
  - "Vulnerabilities Equities Process" is a policy that addresses when agencies should notify companies about security flaws but it is only partially public



Impacts on Healthcare (2017)

- WannaCry crippled 81 out of 236 National Health Service hospitals in England plus 603 primary care and 595 medical practices
  - Impacted computers, MRI scanners, blood-storage refrigerators and theatre equipment
    - Infected 1,200 diagnostic devices and caused others to be temporarily taken out of service to prevent malware from spreading
  - Forced 5 UK hospitals' emergency departments to close and divert patients
  - Costed NHS $116.4 million
- Surprisingly high numbers of unmanaged devices running on outdated operating systems
  - 70% of healthcare organizations operated on Windows 7 or older platforms in 2019
- WannaCry was the first ransomware attack to widely target medical devices

Impacts on Healthcare (since 2017)

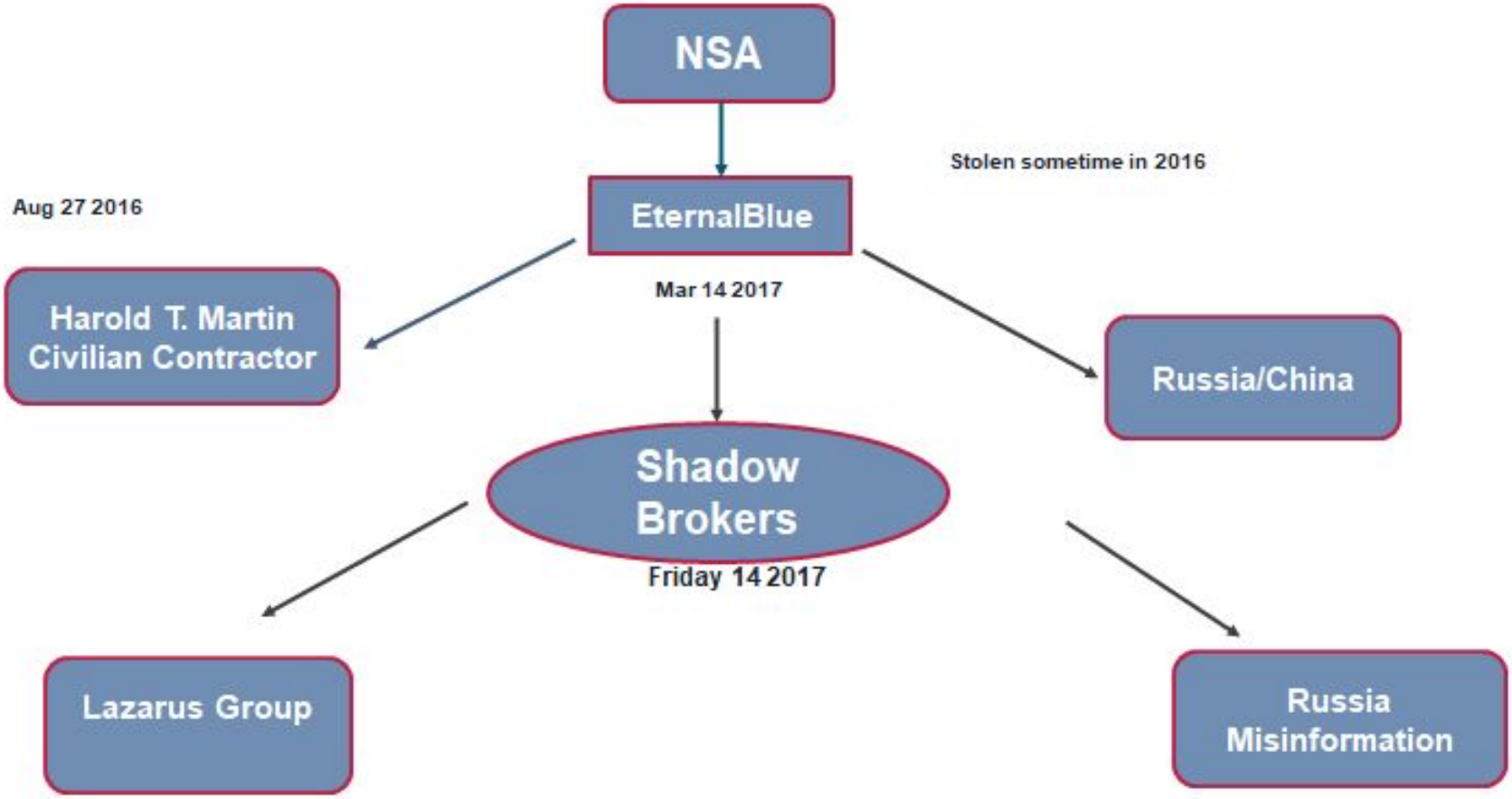
- 40% of healthcare organizations experiencing at least one WannaCry attack in 2019
- 70 percent of successful cyber attacks on health care organizations since 2017 are from ransomware
- NHS IT staff has only been hit by 6 successful ransomware attacks since 2017
    - 203 from the three years prior to 2017
- Ransomware attacks on hospitals is akin to a mass-casualty terrorist attack
    - Cyber attacks on hospitals violate all internationally accepted norms of warfare

What can be done?

- The effort to protect hospitals and patients must include involving law enforcement, legislative, military, and intelligence assets in their defense

150 Countries affected by WannaCry

Assumptions



Jon:

Tell Marcus’s story, the human element, post-2017 people updating their computers/security as a reaction to Wannacry. Recommendations for the personal.
Slides:

- The Hacker who Stopped It (And His Life) - Get Famous and Get Wrekt
- Individual responsibility (how can individuals keep up to date? Cost prohibitive?)

Hacker Who Stopped Wannacry Arrested

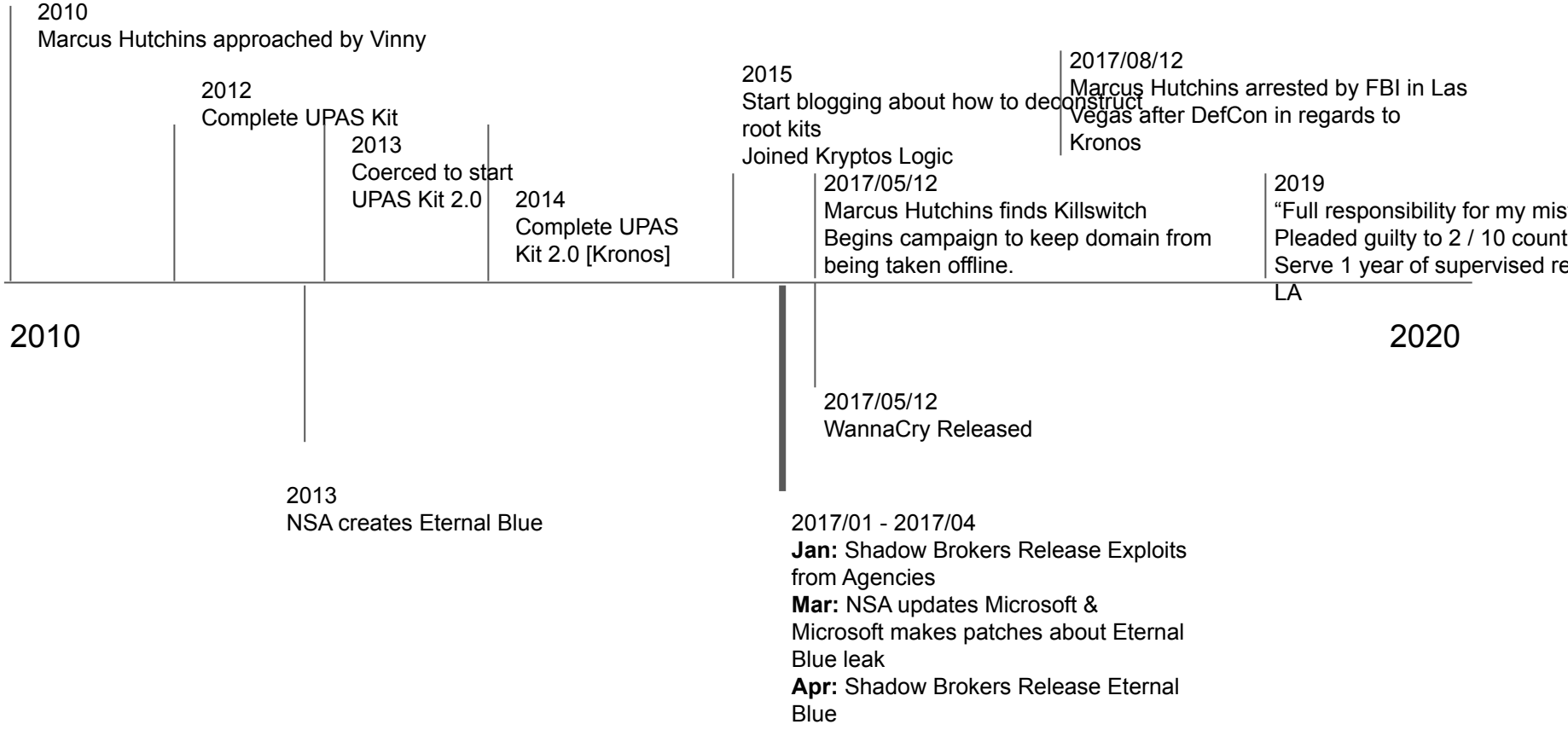
Marcus Hutchins - **22** in 2017

Found WannaCry “Killswitch” in the same day

Fend off attacks to undo the “Killswitch”

3 months later, **arrested for cybercrime** done as a teenager

Hacker Who Stopped Wannacry Arrested



Responsibility of Actions

NSA: “Hoards vulnerabilities” - finds and builds cyberattacks

- Used for US defense as a deterrent as well as espionage

Marcus Hutchins: one man who built a rootkit was arrested

- It was used and designed for malicious purposes

NSA’s hack got leaked, and there wasn’t any tribunals or punishments.

The man who stopped the hack got arrested for a much smaller action.

Individual Responsibility

United States Use Case: **Every one and every industry uses the internet**

Increase knowledge of cyber security

Keep software up to date on computers, devices, and network

- Double-edged sword:
  - Rarer: **Some updates have introduced new vulnerabilities**
  - **Introduce instability**, which may lead to unrecoverable data loss

Networks are only as **secure as their weakest device**

- Give your friends the Guest Wifi not your actual Wifi
- Be Wary of Open Wifis

Back up your data to other locations / devices

Difficulty: **means and access**

- Not everyone can afford a new computer / device
- Write to your local, state, and federal politicians

Articles

https://www.secureworldexpo.com/industry-news/hoarding-vulnerabilities-makes-me-wannacry