

# WannaCry Ransomware

Ted Gould  
@tedjgould

Allen Rotary  
May 17, 2017

# What happened?

Wana Decrypt0r 2.0

## Oops, your files have been encrypted!

English



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 GMT from Monday to Friday.  
Once the payment is checked, you can start decrypting your files immediately.

### Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

**Payment will be raised on**  
1/4/1970 00:00:00  
Time Left  
00:00:00:00

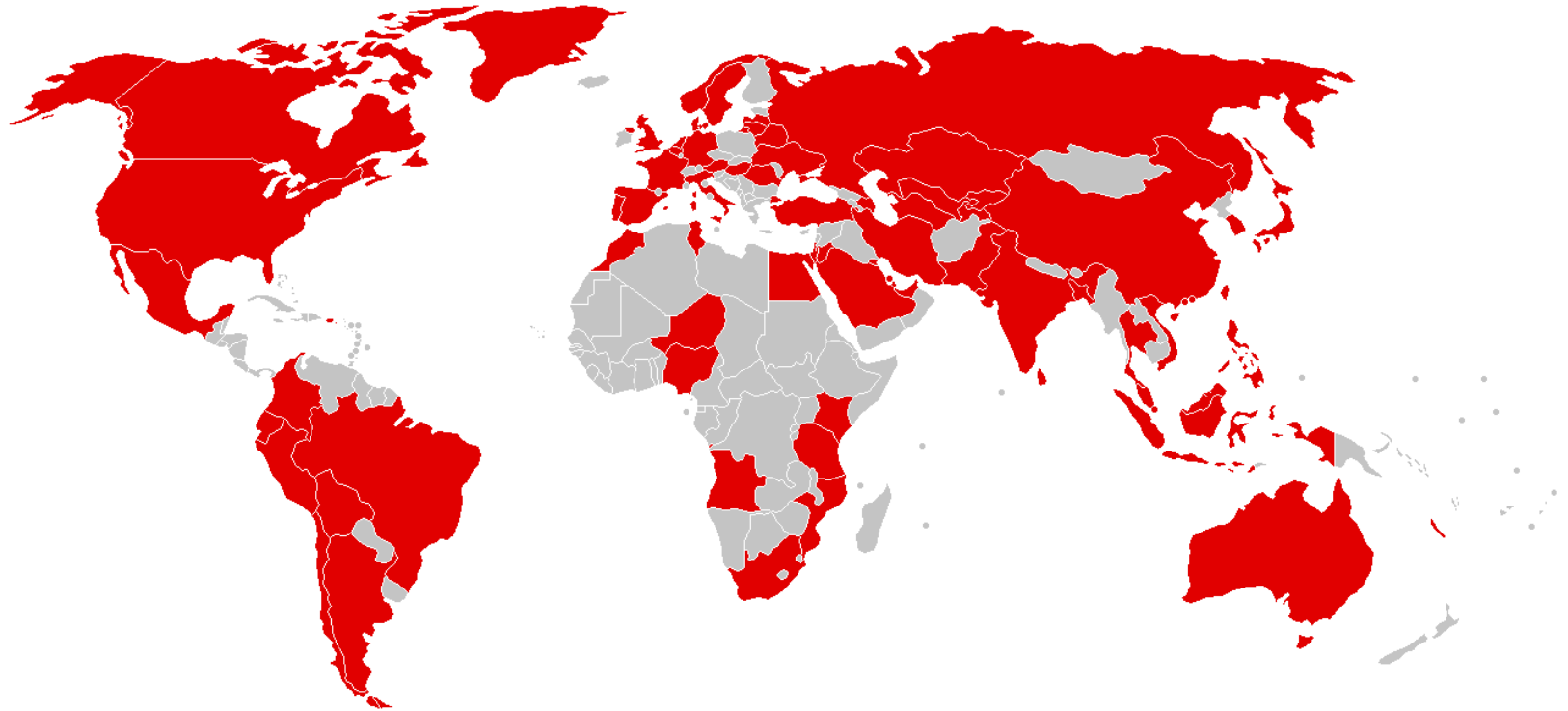
**Your files will be lost on**  
1/8/1970 00:00:00  
Time Left  
00:00:00:00

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)

 **Send \$600 worth of bitcoin to this address:**  
 [Copy](#)

[Check Payment](#) [Decrypt](#)

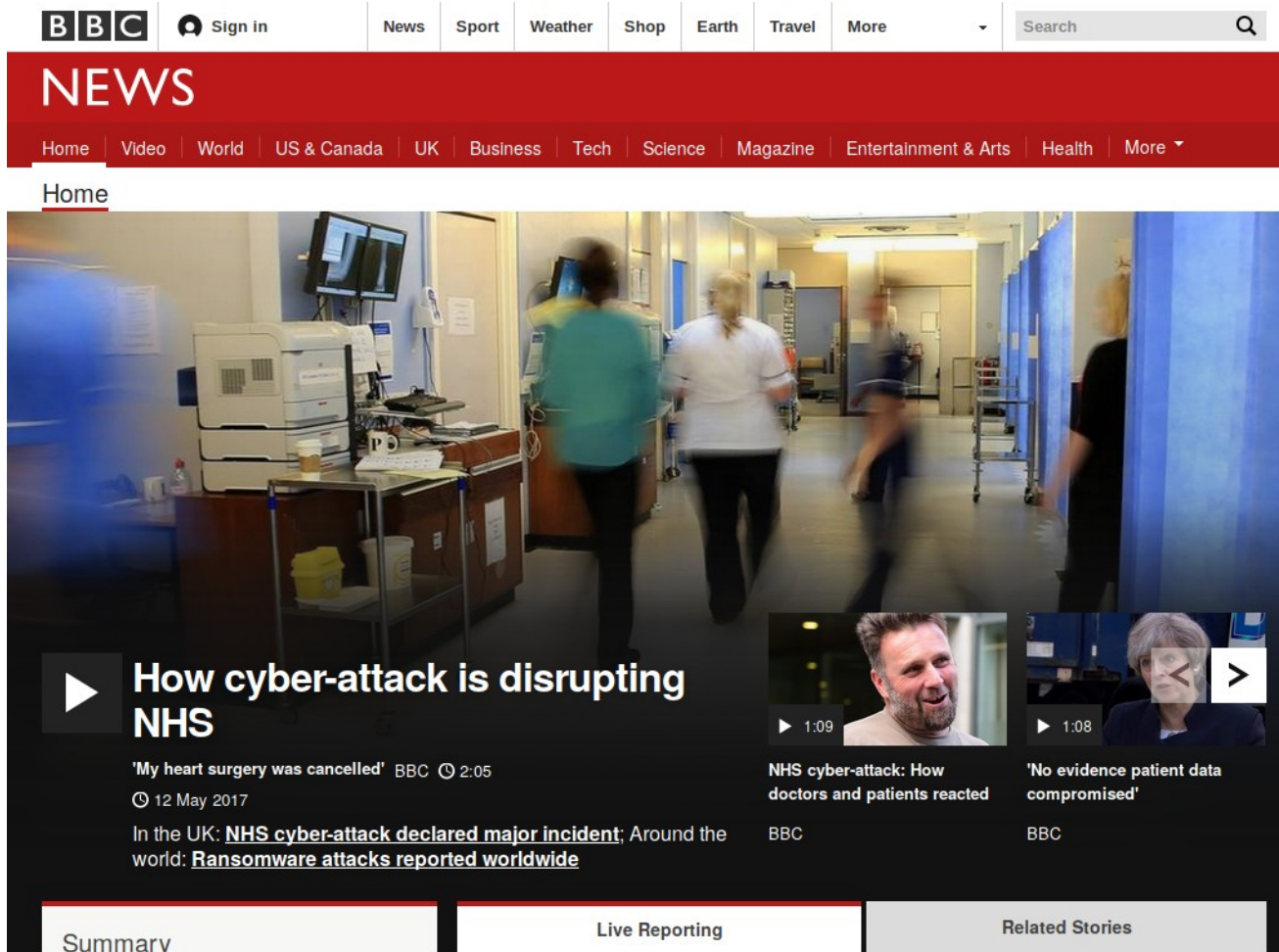
# Where?



Europol estimates ~200K computers in 150 countries

Map By User:Roke - File:BlankMap-World-v2.png, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=58863465>

# NHS Deminished Service



**BBC** Sign in News Sport Weather Shop Earth Travel More Search

## NEWS

Home Video World US & Canada UK Business Tech Science Magazine Entertainment & Arts Health More

### Home

**▶ How cyber-attack is disrupting NHS**

'My heart surgery was cancelled' BBC 2:05  
© 12 May 2017

In the UK: [NHS cyber-attack declared major incident](#); Around the world: [Ransomware attacks reported worldwide](#)

**▶ 1:09** NHS cyber-attack: How doctors and patients reacted  
BBC

**▶ 1:08** 'No evidence patient data compromised'  
BBC

**Summary**

- A cyber-attack on the NHS is affecting hospitals and GP surgeries across England and in Scotland
- Ransomware software that locks

**Live Reporting**

By Megan Fisher, Alex Therrien, John Hand and Bernadette McCague

**Related Stories**

[Get involved](#)

# What should you do right now?

- **Mac OS, Ubuntu, Chrome OS: Keep up-to-date**
- **Windows**
  - Apply all security updates (XP especially vulnerable)
  - Disable SMB1 if possible (Windows network sharing)
  - Update to supported versions of Windows (and other OSes) as soon as possible

# How does it work?

- **Encrypts documents on the computer**
- **Looks on the network for other computers to infect using the EternalBlue SMB exploit**
- **Requests Payment to a Bitcoin Wallet (\$300 to \$1000)**
- **Installs a backdoor in the machine**

# Encryption Stopped

The screenshot shows the top navigation bar of the Guardian website with links for 'sign in', 'become a supporter', 'subscribe', and 'search'. The 'theguardian' logo is on the right. Below is a secondary navigation bar with categories like 'US', 'politics', 'world', 'opinion', 'sports', 'soccer', 'tech', 'arts', 'lifestyle', 'fashion', 'business', 'travel', 'environment', and an 'all sections' menu. The article breadcrumb is 'home > tech'. The main headline is "'Accidental hero' halts ransomware attack and warns: this is not over". A sub-headline reads: "Expert who stopped spread of attack by activating software's 'kill switch' says criminals will 'change the code and start again'". Two bullet points highlight key facts: "Massive ransomware cyber-attack hits countries around the world" and "Criminals behind cyber-attack have raised just \$20,000, experts say". On the left, there are social media sharing icons (Facebook, Twitter, Email, Print) and a share count of "34k". The author information lists "Nadia Khomami in London and Olivia Solon in San Francisco" with the date "Saturday 13 May 2017 10.49 EDT". The main image shows a computer monitor displaying a "Statement on reported NHS cyber attack" from NHS Digital, with a yellow play button overlaid on the screen.

sign in | become a supporter | subscribe | search | jobs | US edition

theguardian

US | politics | world | opinion | sports | soccer | tech | arts | lifestyle | fashion | business | travel | environment | all sections

home > tech

**Cybercrime** | **'Accidental hero' halts ransomware attack and warns: this is not over**

Expert who stopped spread of attack by activating software's 'kill switch' says criminals will 'change the code and start again'

- [Massive ransomware cyber-attack hits countries around the world](#)
- [Criminals behind cyber-attack have raised just \\$20,000, experts say](#)

34k

Nadia Khomami in London and Olivia Solon in San Francisco

Saturday 13 May 2017 10.49 EDT

Statement on reported NHS cyber attack

<https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack>

# Who made EternalBlue?

- **Believed to be the NSA**
- **Leaked publicly (along with many other tools) on April 14<sup>th</sup>, 2017** (*some believe by a foreign adversary*)
- **NSA is believed to have other zero-day (unpatched) vulnerabilities**





# Should the US gov't have zero days?

**“Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today - nation-state action and organized criminal action.”**



<https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/>

# Should the US gov't pay for zero days?

SECTIONS HOME SEARCH The New York Times SUBSCRIBE NOW LOG IN

Web Defenders Detect Russian Hand in Iranians' Hacking Attempt

ITINERARIES Investing in Tech to Tackle an Awful Annoyance: Lost Luggage

All About Bitcoin, the Mysterious Digital Currency

BITS Daily Report: A Global Attack on the Internet. Again.

TECHNOLOGY

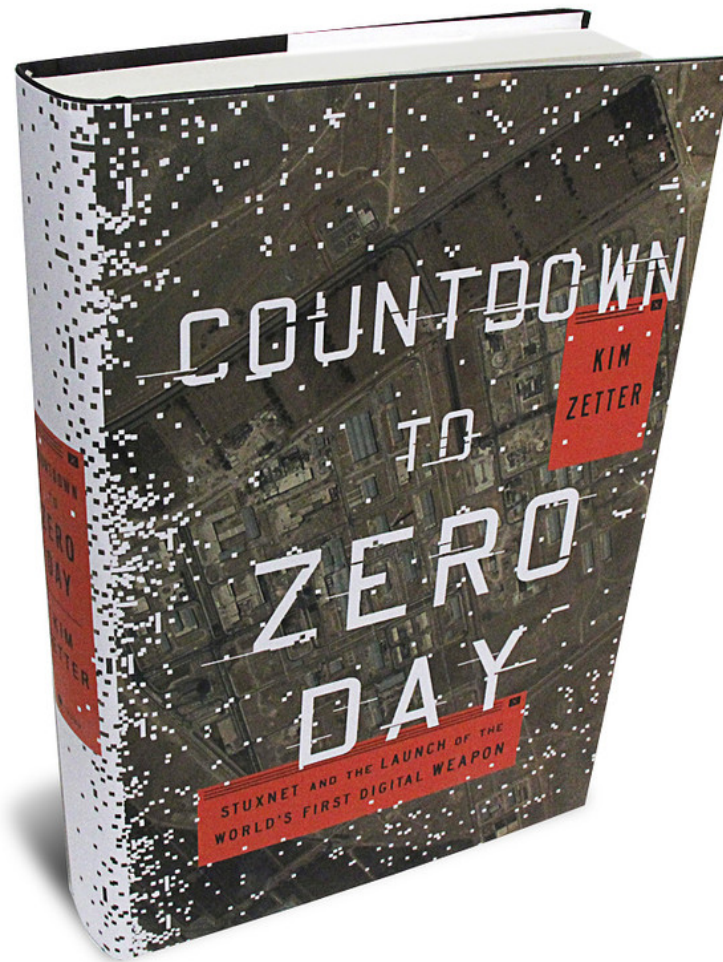
## Web Defenders Detect Russian Hand in Iranians' Hacking Attempt

By NICOLE PERLROTH MAY 15, 2017



<https://www.nytimes.com/2017/05/15/technology/web-defenders-detect-russian-hand-in-iranians-hacking-attempt.html>

# Book on Stuxnet (gov't viruses)



# Why?

- **Money?**

- Ransomware requires a fee to decrypt, sometimes paying that fee results in getting the decryption keys
- It appears people trying to pay overwhelmed the attackers (which would imply they weren't ready for the response)

- **Politics?**

- Since it was an NSA exploit someone may have been trying to embarrass the NSA or USA

- **Joy riders?**

- Information was publicly available, so literally anyone could have done it

# What to do about Ransomware?

# **BACKUPS!!!**

**(air gapped or offline if possible)**

# What if I get Ransomware?

- **Shutdown computer**

- Some ransomware may not have encrypted all files
- Worms may be continuing to look for additional targets on your network

- **Get help**

- Talk to a computer professional about how to fix the machine. This will likely including formatting (deleting all the data) the machine and returning it to a safe state

- **Notify customers via disclosure policy**

- You have a disclosure policy, right? Right? Important to let customers know similar to a physical break in.

# Questions?

Slides: <http://gould.cx/ted/presentations/>