NHS 70

Celebrating 70 years of the NHS – 1948 to 2018

Happy birthday!

#NHS70
WannaCry? You bet we wanted to!

STORIES FROM THE FRONT LINE (AN NHS PERSPECTIVE)

[ANNE GADSDEN, INFORMATION GOVERNANCE OFFICER REPORTING FROM A SECRET, UN-NAMED LOCATION]
A massive cyber-attack using tools believed to have been stolen from the US National Security Agency (NSA) has struck organisations around the world.

Cyber-security firm Avast said it had seen 75,000 cases of the ransomware - known as WannaCry and variants of that name - around the world.

There are reports of infections in 99 countries, including Russia and China.

Among the worst hit was the National Health Service (NHS) in England and Scotland.

The BBC understands about 40 NHS organisations and some medical practices were hit, with operations and appointments cancelled.

How did the cyber-attack unfold?

The malware spread quickly on Friday, with medical staff in the UK reportedly seeing computers go down "one by one".

NHS staff shared screenshots of the WannaCry program, which demanded a payment of $300 (£230) in virtual currency Bitcoin to unlock the files for each computer.
57,000 infections globally
$38,000 paid in ransom

UK: 61 NHS organizations
US: FedEx
Spain: Telefonica
France: Renault
Russia: 1,000 computers in interior ministry
China: Secondary schools and universities
India: Andhra Pradesh Police Departments
Indonesia: Hospitals in Jakarta
Ooops, your files have been encrypted!

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 GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

[Bitcoin address]

Check Payment  Decrypt
What is Ransomeware?
200,000+ Systems Affected by WannaCry Ransom Attack

The WannaCry ransomware attack in numbers

- Affected systems: >220,000
- Affected countries: 150
- Ransom per system: $300

Average ransom in past ransomware attacks

- 2014: $373
- 2015: $294
- 2016: $1,007

Approx. ransom in major ransomware threats

- Feb ’16 Locky: $965
- Mar ’16 Cerber: $1,200
- Apr ’16 CryptXXX: $500

Sources: Media reports, Symantec
**37 ENGLISH TRUSTS WHERE CYBER ATTACKERS STRUCK**

<table>
<thead>
<tr>
<th>Trusts</th>
<th>Trusts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Aintree Univ Hospitals</td>
<td>14 East Cheshire</td>
</tr>
<tr>
<td>2 Barnsley Hospital</td>
<td>15 E Lancashire Hospitals</td>
</tr>
<tr>
<td>3 Barts Hospital</td>
<td>16 Essex Partnership</td>
</tr>
<tr>
<td>4 Basildon and Thurrock Hospitals</td>
<td>17 George Eliot Hospital</td>
</tr>
<tr>
<td>5 Birmingham Community Trust</td>
<td>18 Hampshire Hospitals</td>
</tr>
<tr>
<td>6 Blackpool Teaching Hospitals</td>
<td>19 Ipswich Hospital</td>
</tr>
<tr>
<td>7 Burton Hospitals</td>
<td>20 Liverpool Community Health Trust</td>
</tr>
<tr>
<td>8 Central Manchester University Hospitals</td>
<td>21 Liverpool Women's</td>
</tr>
<tr>
<td>9 Cheshire and Wirral Partnership</td>
<td>22 London North West</td>
</tr>
<tr>
<td>10 Colchester Hospital</td>
<td>23 Mid Essex Hospital</td>
</tr>
<tr>
<td>11 Cumbria Partnership</td>
<td>24 North Staffordshire</td>
</tr>
<tr>
<td>12 Derbyshire Community Health Services</td>
<td>25 Northern Lincolnshire and Goole Trust</td>
</tr>
<tr>
<td>13 East And North</td>
<td>26 Northumbria Healthcare</td>
</tr>
<tr>
<td></td>
<td>27 North Cumbria University Hospital</td>
</tr>
<tr>
<td></td>
<td>28 Nottinghamshire Healthcare</td>
</tr>
<tr>
<td></td>
<td>29 Sherwood Forest Hospitals</td>
</tr>
<tr>
<td></td>
<td>30 Southport and Ormskirk Hospital</td>
</tr>
<tr>
<td></td>
<td>31 Royal Liverpool and Broadgreen Hospitals</td>
</tr>
<tr>
<td></td>
<td>32 United Lincolnshire Hospitals</td>
</tr>
<tr>
<td></td>
<td>33 University Hospitals of Morecambe Bay</td>
</tr>
<tr>
<td></td>
<td>34 University Hospitals of North Midlands</td>
</tr>
<tr>
<td></td>
<td>35 West Hertfordshire Hospitals</td>
</tr>
<tr>
<td></td>
<td>36 Wigan and Leigh Trust</td>
</tr>
<tr>
<td></td>
<td>37 York Teaching Hospital</td>
</tr>
</tbody>
</table>

*Image shows a map of the United Kingdom with numbers indicating the areas affected by cyber attacks.*
Impact of WannaCry cyber attack on the NHS

- 27 acute trusts infected (out of 236 trusts)
- 37 total trusts infected
- 44 trusts not infected but reporting disruption
- 21 trusts attempted to contact WannaCry but not locked out of devices

Source: National Audit Office
How the day unfolded

Head of IM&T
- Inform Executives
- Shut down the network
- Support the IM&T staff

Resilience Manager
- Keep NHS England informed
- Liaise between the Incident Room (“Gold Command”) and IM&T

A&E Matron
- Check A&E patients
- Bed Management meetings (patient flow)

Radiology IT Systems Manager
- Unplug the Imaging kit
- Start manual systems (burning images to disc)

On-call Business Manager
- Liaise with “gold command”
- Walk the wards
- Teleconference with clinicians
What did you feel?

• “**Murderous** – absolutely furious. I wanted to kill the person who did this”
• “I felt vulnerable and anxious about the impact on patients”
• “We made the right decisions and stopped the infection in its tracks”
• “We’re doing better now, thank you very much!”
• “What sort of person would do this!”
• “We’re trained to deal with this sort of thing, we got on and did it”
• “The team work was incredible”
• “It was intense, but it was a pleasure to work with everyone that day”
• “It was exhilarating”
IM&T Action

IM&T initiated NHS Digital’s Containment, Eradication and Recovery process:

1. Identified and quarantined all systems infected with the malware
2. Patched the vulnerability that enabled the malware to propagate throughout the network
3. Ensured all systems were updated with the latest AV (Anti-Virus) definitions
4. Implemented additional technical controls to prevent the malware from propagating
5. Recovery process
What did we learn?

- Be vigilant
- Have an IT priority switch-on list
- Identify different ways of communicating
- We know what we’re doing now - “yes we can do this, we’ve done this before”
- Go on the wards and have discussions face-to-face
- Use the whiteboards
- The face-to-face contact helped to build the team spirit
- Walking the floors, talking to people - it was actually fun
- Patient flow was a priority, and it worked.
- There was no patient harm, no clinics cancelled, no patients left un-scanned.
One year on: the NHS is still in the spotlight

18th April, 2018

- One year after WannaCry, zero NHS trusts pass cyber security assessment
  - Damning government report reveals NHS still fails to meet cyber security requirements
- The government's Public Accounts Committee has today released the findings of its report into the WannaCry ransomware which hit the NHS in May 2017, revealing that not one NHS trust is up to an acceptable standard of cyber security.
PAC criticises NHS’s lack of action on WannaCry measures

The NHS and Department of Health have been criticised by MPs for not taking enough action to improve cyber security measures following 2017’s WannaCry incident.
On the NHS tech team? Weep at ugly WannaCry post-mortem, smile as Health dept outlines plan

Apparently, senior NHS Trust managers will be held accountable… stop giggling

By John Leyden 2 Feb 2018 at 13:08
WannaCry is still with us: on 28\textsuperscript{th} March this year (2018), it attacked Boeing ...

Boeing is hit by WannaCry virus but contains the attack after panicked engineer sent memo warning it could 'spread to airplane software'
- Boeing commercial airplane factory in South Carolina was hit on Wednesday
- WannaCry is the same ransomware that crippled UK's National Health Service
- Panicked engineer sent out chilling alert calling for 'All hands on deck'
- By Wednesday evening Boeing said the attack was limited and contained

Statement: A number of articles on a malware disruption are overstated and inaccurate. Our cybersecurity operations center detected a limited intrusion of malware that affected a small number of systems. Remediations were applied and this is not a production or delivery issue.
Finally

- Planning and preparation is key to survival
- It’s not a matter of if, but when, the next attack comes
- It’s how you handle an event that is important

“Sh*t happens, deal with it.”